

Ron DeSantis, Florida Governor
Pedro Allende, Secretary
James Grant, Florida State Chief Information Officer

**AGENCY TERM CONTRACT
FOR
Endpoint Detection and Response
DMS-22/23-155D
BETWEEN
STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES
AND
MAINLINE INFORMATION SYSTEMS, INC.**

AGENCY TERM CONTRACT

This Contract is between the STATE OF FLORIDA, DEPARTMENT OF MANAGEMENT SERVICES ON BEHALF OF FLORIDA DIGITAL SERVICE (Department), with offices at 4050 Esplanade Way, Tallahassee, Florida 32399-0950, and MAINLINE INFORMATION SYSTEMS, INC. (Contractor), with offices at 1700 Summit Lake Dr., Tallahassee, FL 32317, each a "Party" and collectively referred to herein as the "Parties".

WHEREAS, the Contractor responded to the Department's Request for Quotes (RFQ), No: DMS-22/23-155, Endpoint Detection and Response; and

WHEREAS, the Department has accepted the Contractor's Quote and enters into this Contract in accordance with the terms and conditions of RFQ No. DMS-22/23-155.

NOW THEREFORE, in consideration of the premises and mutual covenants set forth herein, the Parties agree as follows:

1.0 Definitions

- 1.1 Agency Term Contract (ATC or Contract): A written agreement between the Department and the Contractor that is for use by the entire Department and under which Purchase Orders (PO) shall be issued.
- 1.2 Business Day: Any day of the week excluding weekends and holidays observed by State agencies pursuant to subsection 110.117(1)(a)-(j), Florida Statutes (F.S.).
- 1.3 Calendar Day: Any day in a month, including weekends and holidays.
- 1.4 Contract Administrator: The person designated pursuant to section 8.0 of this Contract.
- 1.5 Contract Manager: The person designated pursuant to section 8.0 of this Contract.
- 1.6 Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).
- 1.7 Purchaser: The agency as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this ATC.

2.0 Scope of Work

The services and/or commodities to be provided by the Contractor pursuant to this Contract are defined and described in Exhibits A and B.

3.0 Contract Term

This ATC shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying Alternate Contract Source (ACS), and shall begin on the last date on which it is signed by all Parties.

4.0 Renewal Terms

The Department reserves the right to renew the Contract in whole or in part, for a renewal term not to exceed three (3) years, or portions thereof, in accordance with section 287.057, F.S. and subject to any limitations based on the term of the underlying ACS, at the renewal pricing specified in the Contractor's Quote or upon mutual agreement of the Parties as set forth in the

Contract. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department.

5.0 Contract Documents and Hierarchy

All Exhibits attached to this Contract are incorporated in their entirety and form as part of this Contract. This Contract sets forth the entire understanding between the Parties and is comprised by the following documents:

1. Exhibit A: RFQ No. DMS-22/23-155;
2. Exhibit B: Contractor's Quote.

In the event that any of the Contract documents conflict, the order of precedence set forth in Section 17.0, of RFQ No. DMS-22/23-155 shall control.

In the event of any conflict between this Contract and any applicable federal or state statute, administrative rule or regulation; the statute, rule or regulation will control.

6.0 Amendments

Unless otherwise provided herein, all modifications to this Contract must be in writing and signed by both Parties, except changes to Section 8.0, below. Any future amendments of the Contract, which alter the definition of the services or scope of work, shall define the services or scope in the same format as Exhibit A and Exhibit B.

Notwithstanding the order listed in Section 5.0, amendments issued after Contract execution may expressly change the provisions of the Contract. If an amendment expressly alters the Contract, then the most recent amendment will take precedence.

7.0 Contract Notices

In addition to the provisions in Section 38 of Form PUR 1000 (10/06), Contract notices may be delivered by email to the Contractor's Representative as prescribed in Section 8.0. All notices by hand-delivery shall be deemed received on the date of delivery, and all notices by email shall be deemed received when they are transmitted and not returned as undelivered or undeliverable.

8.0 Contract Contacts

The Department may appoint a different Contract Administrator or Manager, which will not require an amendment to the Contract, by sending written notice to the Contractor. The Contractor shall address all communication relating to the Contract to the Contract Manager.

8.1 The Department employee who is primarily responsible for maintaining the Contract Administration file is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
Email: DMS.Purchasing@dms.fl.gov

The Department's Contract Administrator will perform the following functions:

1. Maintain the official Contract Administration file;
2. Maintain this Contract and all amendments; and
3. Maintain records of all formal contract correspondence between the Department and the Contractor as provided by the Contract Manager for filing in the Contract Administration file.

8.2 The Department's Contract Manager is:

Lacy Perkins
Procurement and Grants Manager
Florida Digital Service
2555 Shumard Oak Blvd.
Tallahassee, FL 32399
Telephone: (850) 274-4156
Email: Purchasing@digital.fl.gov

The Contract Manager will perform the following functions:

1. Maintain a Contract Management file;
2. Serve as the liaison between the Department and the Contractor;
3. Enforce performance of the Contract terms and conditions;
4. Monitor and evaluate the Contractor's performance to ensure services conform to the Contract requirements;
5. Request all amendments, renewals, and terminations of this Contract, and implement management of the Contract change;
6. Exercise applicable remedies, as appropriate, when the Contractor's performance is deficient;
7. Evaluate the Contractor's performance upon completion of this Contract. This evaluation will be placed in the Contract file and will be considered if this Contract is subsequently used as a reference in future procurements.

For each PO issued, the Purchaser's Contract Manager will perform the following functions:

1. Verify the Customer received the deliverables from the Contractor;
2. Review, verify, and approve invoices from the Contractor;
3. Monitor the quality of services and commodities being delivered;
4. Monitor the budget to ensure funds are available through the PO term; and
5. Serve as the liaison between the Department, the Customer, and Contractor relating to quality and delivery.

8.3 The Contractor has assigned the following individual(s) to serve as the Contractor's Representative for this Contract:

Felicity Lynch
Fed. Conts & Negotiations Manager
1700 Summit Lake Drive
Tallahassee, FL 32317
Telephone: (540) 522-1619
Email: felicity.lynch@mainline.com

The Department will direct all questions and customer service issues concerning this Contract to the Contractor's Representative above. It will be the Contractor's Representative's responsibility to coordinate with necessary Department, Purchaser, and Customer personnel, as required, to answer questions and resolve issues. The Contractor must provide written notice to the Department's Contract Manager if a new employee is designated as the Contractor's Representative for this Contract.

9.0 Assignment

The Contractor shall not assign its duties or rights under this Contract to another party without the prior written approval of the Department. The Department shall, at all times, be entitled to assign or transfer its rights, duties, and obligations under this Contract to another governmental agency of the State of Florida upon providing written notice to the Contractor.

10.0 Price Decreases

The Contractor shall apply to the Department any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department under the Contract. Price increases are rejected, unless otherwise stated.

11.0 Additions/Deletions

During the term of the Contract, the Department reserves the right to add or delete services and commodities, when considered to be in its best interest and general scope of the Contract. Pricing shall be comparable to the amounts awarded.

12.0 Cooperative Purchasing

Pursuant to their own governing laws, and subject to the agreement of the Contractor, other entities may be permitted to make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other purchaser.

13.0 Other Conditions

13.1 Independent Contractor Status

This Contract does not create an employee/employer relationship between the Parties. The Parties are independent contractors under this Contract and neither is the employee of the other for all purposes, including, but not limited to, the application of the Fair Labor Standards Act minimum wage and overtime payments, Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code, the State Workers' Compensation Act, and the State's unemployment insurance law. The Parties shall each retain sole and absolute discretion in the judgment of the manner and means of carrying out their Contract duties. Services and commodities provided by each Party under this Contract shall be subject to the supervision of the other Party. In performing this Contract, neither Party nor its agents shall act as officers, employees, or agents of the other Party. The Parties agree that they

are separate and independent business enterprises, and that each can pursue other opportunities.

This Contract shall not be construed as creating any joint venture or partnership between the Parties, and neither Party will be liable for any obligation incurred by the other Party, including, but not limited to, unpaid wages and overtime premiums.

13.2 Force Majeure

Neither Party shall be liable for loss or damage suffered as a result of any delay or failure in performance under this Contract or interruption of performance resulting directly or indirectly from acts of God, fire, explosions, earthquakes, floods, water, wind, lightning, civil or military authority, pandemics, acts of public enemy, war, riots, civil disturbances, insurrections, strikes, or labor disputes.

13.3 Cooperation with the Florida Senate and Florida House of Representatives

In accordance with section 287.058(7), F.S., the Contractor agrees to disclose any requested information, relevant to the performance of this Contract, to members or staff of the Florida Senate or Florida House of Representatives, as required by the Florida Legislature. The Contractor is strictly prohibited from enforcing any nondisclosure clauses conflictive with this requirement.

13.4 Employment of State Workers

During the term of the Contract, Contractor shall not knowingly employ, subcontract with or subgrant to any person (including any non-governmental entity in which such person has any employment or other material interest as defined by section 112.312(15), F.S.) who is employed by the State or who has participated in the performance or procurement of this Contract, except as provided in section 112.3185, F.S.

SIGNATURE PAGE IMMEDIATELY FOLLOWS

IN WITNESS THEREOF, the Parties hereto have caused this Contract to be executed by their undersigned officials as duly authorized.

MAINLINE INFORMATION SYSTEMS, INC.:

STATE OF FLORIDA
DEPARTMENT OF MANAGEMENT SERVICES:

DocuSigned by:
Brian Showman
9EB87387D388408...
Authorized Signature

DocuSigned by:
Pedro Allende
5E91A9D389EB47C...
Pedro Allende, Secretary

Brian Showman
Print Name

6/30/2023 | 8:25 PM EDT
Date

General counsel
Title

6/30/2023 | 8:24 PM EDT
Date

Exhibit "A"

Request for Quotes (RFQ)

DMS-22/23-155

Endpoint Detection and Response Solution

Alternate Contract Sources:

**Cloud Solutions (43230000-NASPO-16-ACS)
Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS)
Technology Products, Services, Solutions, and Related Products
and Services (43210000-US-16-ACS)**

1.0 **DEFINITIONS**

The following definitions shall apply throughout this RFQ:

Agency Term Contract (ATC): The written agreement resulting from the award of this Request for Quotes between the Department and the Contractor(s).

Contractor: The vendor awarded an ATC resulting for this Request for Quotes.

Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).

Department: The State of Florida, Department of Management Services (DMS), on behalf of the Florida Digital Service (FL[DS]).

Purchase Order: The authorization to begin providing services to a Customer under the terms of this RFQ and a resulting ATC, if applicable.

Purchaser: The agency as defined in section 287.012, F.S., or Eligible User, as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.), who issues a Purchase Order from this RFQ or a resulting ATC.

Quote: A vendor's response to this Request for Quotes.

Solution: An Endpoint Detection and Response (EDR) solution that collects and analyzes endpoint data to detect and respond to cyber security threats.

2.0 OBJECTIVE

Pursuant to section 287.056(2), F.S., the Department intends to purchase an EDR (endpoint detection and response) solution for use by the Department and Customers to collect and analyze endpoint data to detect and respond to threats as specified in this RFQ.

The Department also reserves the right to execute an Agency Term Contract (ATC), in the form attached hereto, with the awarded Contractor(s) for the commodities and services specified in this RFQ. The ATC will allow the Department and Customers to purchase the Solution at or below the pricing provided by the awarded Contractor(s) throughout the ATC term.

This RFQ is being issued under the following Alternate Contract Source (ACS) contracts:

- Cloud Solutions (43230000-NASPO-16-ACS)
- Software Value Added Reseller (43230000-23-NASPO-ACS)
- Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)

3.0 DESCRIPTION OF PURCHASE

The Department is seeking a Contractor(s) to provide an Endpoint Detection and Response (EDR) Solution for the Department and Customers on a statewide basis. The Solution shall include software, implementation, training, support, and integration services as described below. The Contractor will be responsible for providing the Solution to Customers. The Contractor shall be responsible for all aspects of providing the Solution to Customers, as provided herein.

4.0 BACKGROUND INFORMATION

In accordance with section 282.318, F.S., the "State Cybersecurity Act," the Department "is the lead entity responsible for establishing standards and processes for assessing state agency cybersecurity risks and determining appropriate security measures." Additionally, the statute states that the Department "shall adopt rules that mitigate risks; safeguard state agency digital assets, data, information, and information technology resources to ensure availability, confidentiality, and integrity; and support a security governance framework."

The Department is also responsible for implementing the recommendations of the February 1, 2021, Florida Cybersecurity Task Force Final Report which addresses key objectives related to the state's cybersecurity infrastructure, governance, and operations. The resulting initiatives, projects, and efforts constitute the Enterprise Cybersecurity Resiliency Program.

Additionally, in accordance with section 282.3185, F.S., the "Local Government Cybersecurity Act," "Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework." In the Fiscal Year 2022-2023 General Appropriations Act (line 2944A), the Department was tasked with administering a competitive grant program for local government cybersecurity technical assistance for municipalities and counties. The Department intends to provide access to solutions to equip Customers with resources compliant with the abovementioned cybersecurity standards.

5.0 TERM

The ATC(s) shall have an initial term of three (3) years, subject to any limitations based on the term of the underlying ACS. The Department also reserves the right to renew the ATC(s) in accordance with section 287.057, F.S, and subject to any limitations based on the term of the underlying ACS. Renewals are also contingent upon satisfactory performance by the Contractor, as determined by the Department. Purchase Orders (PO) will be issued in accordance with the RFQ and any applicable ATC as services are needed for Customers. Any POs issued pursuant to the RFQ will have the term identified in the PO.

6.0 SCOPE OF WORK

The Solution proposed in any Quote must not conflict with Chapter 282, F.S., Rule Title 60GG, Florida Administrative Code (F.A.C.), and cybersecurity best practices. The Solution must meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework. The Contractor shall provide services in the manner prescribed by this Scope of Work. The Scope of Work shall be delivered in accordance with the deliverables herein. The Department expects the services to be completed remotely and is not requiring the Contractor to travel. Unless otherwise specified within vendor's Quote, the Solution should include the following items within the Scope of Work, but not be limited to:

6.1. Software Solution/Specifications

The Solution shall detect and respond to threats on endpoint devices such as laptops, desktops, servers, and mobile devices. Endpoint Detection and Response (EDR) solutions typically use a combination of techniques such as behavioral analysis, machine learning, and threat intelligence to identify and respond to security incidents in real-time. The primary purpose of EDR is to detect and respond to advanced threats that have bypassed traditional security defenses such as firewalls and antivirus software. This is accomplished by collecting data from endpoint devices, analyzing it for signs of suspicious activity, and taking automated or manual actions to isolate and neutralize threats. EDR solutions can help organizations improve their overall security posture by providing visibility into the activities taking place on endpoint devices, helping security teams respond to incidents more quickly and effectively, and providing valuable information that can be used to improve security processes and policies.

6.1.1. Multi-Tenant

The Solution shall support a multi-tenant, multi-organization architecture. Each tenant must have its own instance and each instance must aggregate up to a single instance and view. The aggregated instance will support enterprise security operations. The Solution shall provide dashboards for single-source visibility into threats, investigations, and trends.

6.1.2. Scalability

The Solution shall provide the ability to scale to support a large number of tenants and their endpoints.

6.1.3. Cloud Management

The Solution shall be provided as software as a service via cloud-hosted infrastructure to keep current with the latest releases of management server and endpoint agent software. The Solution shall allow capacity extensibility in the cloud with minimal impact on agent or management infrastructure.

6.1.4. Managed Security Services

The Solution shall deploy and maintain managed security services to support Purchasers and Customers, particularly the advanced administration requirement of endpoint detection and response tools and incident response capabilities.

6.1.5. Prevention

The Solution shall block malware pre-execution using the platform's anti-malware prevention program.

6.1.6. Product Usability

The Solution shall provide easy to understand, user-friendly interfaces with intuitive designs to facilitate user engagement, and clear documentation and support resources which instruct on use of the Solution.

6.1.7. Administration and Management Usability

The Solution shall have an easy-to-use administration console and allow straightforward ongoing management that utilizes a lightweight agent with low impact on potential performance.

6.1.8. Endpoint Detection and Response

The Solution shall record system behaviors to detect suspicious events, investigate and block malicious activity, and contain malicious activity at the endpoint. The Solution shall use the data to investigate and provide remediation guidance for any affected systems.

6.1.9. Endpoint Protection Platform Suite

The Solution shall use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

6.1.10. Operating System Support

The Solution shall protect a wide range of operating systems, including Windows, MacOS and Linux, and mobile operating systems like iOS and Android. The Solution shall provide specific functions for cloud, virtual and container-based workloads.

6.1.11. Data Management and Storage

The Solution shall provide required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication.

6.1.12. Performance Management

6.1.12.1. The Solution shall provide proactive alerts on system events, as well as logging and resolution reporting on all issues.

6.1.12.2. The Solution shall provide the ability to identify unhealthy agents on endpoints and self-heal issues. Any endpoints that cannot be self-healed must be reported through the administration console and reports.

6.1.13. Security

The Solution shall offer configurable controls that extend data and transaction security and compliance to third-party platforms or hosting providers the Solution uses. The Solution shall document security policies, audits, attestations or evaluations for compliance needs.

6.1.14. Data Management

The Solution shall enable monitoring, reporting, and management of data sharing, as well encryption and security for data at rest and in motion.

6.1.15. Disaster Recovery and Backup

The Solution shall enable processes such as disaster recovery, rollbacks, and version control.

6.1.16. Identity and Access Management

The Solution shall provide capabilities such as user authentication, password policy management, two factor authentication, single sign on, and role-based access.

6.1.17. Network

The Solution shall leverage network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the Solution.

6.1.18. Compliance and Third-Party Certification

The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII)

data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.

6.1.19. Configuration and Customization

The Solution shall allow customization of the standard deployed solution with custom user interfaces, data tables, process components, and business logic.

6.1.20. Role-Based Access

The Solution shall provide the ability to create customizable role-based personas based on responsibility.

6.1.21. Data Export

The Solution shall provide the ability to generate a customizable export of data based on user filters for assets, services, and issues present within the platform.

6.1.22. Integration

6.1.22.1. The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions and security information and event management (SIEM) systems. The Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.

6.1.22.2. The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).

6.1.22.3. The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.

6.1.22.4. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.

6.1.22.5. Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.

6.1.23. Performance and Availability

The Solution shall perform in accordance with the approved Service Level Agreement (SLA) (see Section 10.2) and be available 99.999% of the time per month.

6.1.23.1. The performance and availability SLA shall provide information on performance and availability objectives for the Solution to perform successfully and be available 99.999% of the time per month.

6.1.23.2. The vendor shall propose meaningful financial consequences in the draft performance and availability SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2. Training and Support

Through the Solution, the Contractor shall provide all consulting, training, and support to the Customer and FL[DS] to ensure successful implementation of the Solution and ongoing support as necessary and as defined by FL[DS] to include, but not be limited to:

6.2.1. Consult with and the Department, the Purchaser, and the Customer to ensure the Department, the Purchaser, and the Customer have the information necessary for decision-making.

6.2.2. Adhere to the FL[DS]-approved training SLA that specifies the objectives, description of the materials/resources provided to meet the objectives, suggested method of training (in-person, live webinar, online course, etc.), and specific training suggested for each user roles.

6.2.2.1. The training SLA must specify Initial Training (included in Item No. 1 on Attachment A, Price Sheet) provided and Ongoing Training provided (included in Item No. 2 on Attachment A, Price Sheet).

6.2.2.2. The vendor shall propose meaningful financial consequences in the draft training SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.2.3. Adhere to the FL[DS]-approved SLA for support service which provides information on support objectives, resources, availability, response times, resolution times and issue criticality levels.

6.2.3.1. The vendor shall propose meaningful financial consequences in the draft support service SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.3. Kickoff Meeting

6.3.1. The Contractor shall conduct a kickoff meeting with the Purchaser to further clarify PO expectations.

6.3.2. If the PO covers more than just the Purchaser, the Contractor shall conduct a kickoff meeting for each Customer on a date and time agreed upon by the FL[DS] (if the Solution is being integrated into the CSOC) and the Customer.

The Contractor may hold a kickoff meeting with multiple Customers per meeting.

- 6.3.3. The kickoff meeting for the Customer should include a demonstration of the Solution, or prior to the kickoff meeting, a link may be provided to the Customer to demonstrate the Solution.

6.4. **Implementation**

The Contractor shall implement the Solution with each Customer upon the Purchaser's approval, FL[DS] approval (if the Solution is integrating with the CSOC), and the Customer's approval of the Implementation Plan. The Contractor shall collaborate with the Customer to develop an Implementation Plan addressing all items contained in **Section 6.0**, Scope of Work, and submit it to the Purchaser, FL[DS] as applicable, and the Customer for approval.

The Implementation Plan must include the following at a minimum:

- 6.4.1. All tasks are required to fully implement and complete Initial Integration of the Solution.
- 6.4.2. Identify if the Contractor, Purchaser, FL[DS] (if applicable), or other Customer is responsible for each task.
- 6.4.3. Dates that each task (or group of tasks) will be completed by, identify task dependencies, and tasks on the critical path to ensure timely project completion.
- 6.4.4. Describe necessary training, method of training (e.g., in-person, live webinar, online course), and training dates.
- 6.4.5. Describe the support available to ensure successful implementation and Initial Integration.
- 6.4.6. Provide Contractor contact information (name, title, email, and phone number) for the Contractor Representative who is assigned to oversee successful implementation and Initial Integration.
- 6.4.7. Document the frequency and method(s) for the Contractor to communicate the ongoing status of the Implementation Plan to the Purchaser and any other Customers.

6.5. **Reporting**

The Contractor shall provide the following reports to the Purchaser:

- 6.5.1. Quarterly Business Reviews (QBR) which will include, but not be limited to, performance reports and metrics on service level achievements. The Contractor shall schedule a quarterly meeting to review the QBR and document any financial consequences to be assessed as necessary.
- 6.5.2. Monthly Implementation Reports shall be provided to the Purchaser to document compliance with Final Implementation Plan(s) and document any financial consequences to be assessed as necessary.

- 6.5.3. Monthly Training Reports shall be provided to the Purchaser to document all training provided to the Purchaser and any other Customers and document any financial consequences to be assessed as necessary.
- 6.5.4. Monthly Service Reports shall be provided to the Purchaser to document Solution performance, availability, response times, and resolution times and document any financial consequences to be assessed as necessary.
- 6.5.5. Ad hoc reports as requested by the Purchaser.

6.6. Optional Services

6.6.1. Manage, Detect, and Respond (MDR)

If available, the vendor shall provide optional annual pricing along with an SLA to manage, detect, and respond to security issues detected by the Solution.

- 6.6.1.1. Adhere to the FL[DS]-approved MDR SLA which provides information on MDR objectives, resources, availability, response times, resolution times, and issue criticality levels.
- 6.6.1.2. The vendor shall propose meaningful financial consequences in the draft MDR SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

6.6.2. Future Integrations

If available, the vendor shall provide optional pricing along with an SLA for Application Programming Interfaces available for the Solution.

- 6.6.2.1. Adhere to the FL[DS]-approved SLA for future integrations which include services and solutions that augment, enhance, or expand the Solution in a meaningful way.
- 6.6.2.2. The vendor shall propose meaningful financial consequences in the draft future integrations SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences.

7.0 DELIVERABLES

Deliverables for each Purchase Order may be submitted earlier than the delivery dates listed in **Table 1**. All deliverables are subject to the approval and acceptance of the Purchaser. The Contractor shall provide the services identified in **Section 6.0**, Scope of Work, to complete the deliverables as described in **Table 1** below. The Contractor will not be compensated for the kickoff meetings, or any work performed before or during the development of the Implementation Plan. Once the Implementation Plan is approved in writing by the Purchaser, FL[DS] (if applicable), and the Customer, as applicable, the Contractor shall provide the Customer with access to the software in accordance with the approved Implementation Plan (Final Implementation Plan). Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will invoice the Purchaser at the pricing established in Attachment A, Price Sheet, within thirty (30) days. The Contractor will be compensated, annually, in advance, for the Solution for each PO in accordance with this RFQ. The Purchaser may waive or amend any due dates in writing at its sole discretion.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
1	The Contractor shall host a kickoff meeting with the Purchaser individually, and kickoff meeting with each additional Customer, and FL[DS] (if applicable) in accordance with the PO, and any applicable ATC.	The Contractor shall host the meeting within five (5) calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after deliverable due date.
2	The Contractor shall submit the Implementation Plan timely and in accordance with the PO and any applicable ATC.	The Contractor shall collaborate with the Customer and submit each Customer's Implementation Plan to the Purchaser and each additional Customer within 10 calendar days of PO issuance.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after the deliverable due date until the Customer Implementation Plan is received. Financial consequences shall also be assessed for a Customer's Implementation Plan submitted that is not in accordance with the PO and any applicable ATC, in the amount of \$500 for each incomplete Implementation Plan.
3	The Contractor shall provide Solution access and all services in the Final Implementation Plan in accordance with this PO and any applicable ATC.	The Contractor shall provide Solution access and complete all requirements established in the Final Implementation Plan timely and accurately.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the Final Implementation Plan, until the requirement is accurately completed. Financial consequences shall be assessed in the amount of \$200 per requirement for each instance services are not performed, or documentation is not received, in accordance with this RFQ and the Implementation Plan.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
4	The Contractor shall ensure the Solution is available in accordance with this PO and any applicable ATC.	The Solution must be available 99.999% of the time per month in accordance with the FL[DS]-approved SLA and. Compliance is calculated on a monthly basis for each Customer.	Financial Consequences shall be assessed against the Contractor in the amount of \$100 for each negative deviation from the thousandth decimal point. For example, a Customer's monthly uptime of 99.997% will result in a financial consequence of \$200, unless the Department accepts different financial consequence in the Contractor's Quote.
5	The Contractor shall ensure the Solution performs in accordance with the FL[DS]-approved SLA.	The Solution must perform in accordance with the FL[DS]-approved SLA.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.
6	The Contractor shall ensure training and support are provided in accordance with the FL[DS]-approved SLA.	Training and support must be provided in accordance with Section 6.2. of this RFQ and the FL[DS]-approved SLA for training and support.	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date specified in the FL[DS]-approved SLA, until the requirement is accurately completed, unless the Department accepts different financial consequence in the Contractor's Quote.

**TABLE 1
DELIVERABLES AND FINANCIAL CONSEQUENCES**

No.	Deliverable	Time Frame	Financial Consequences
7	The Contractor shall report accurate information in accordance with the PO and any applicable ATC.	<p>QBRs are due 15 calendar days after the end of the quarter (January - March, April - June, July - September, and October - December).</p> <p>Monthly Implementation Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Training Reports are due five (5) calendar days after the end of the month.</p> <p>Monthly Service Reports are due five (5) calendar days after the end of the month.</p> <p>Ad hoc reports are due five (5) calendar days after the request by the Purchaser.</p>	Financial consequences shall be assessed in the amount of \$100 per calendar day, beginning on the first calendar day after any due date, until an accurate report is received.

All deliverables are subject to the approval and acceptance of the Purchaser. Any deliverables rejected by the Purchaser will be subject to the applicable financial consequences in Table 1 until the Contractor resubmits and the Purchaser accepts the deliverable.

8.0 PERFORMANCE MEASURES

The Contractor shall perform all required services in a proper and satisfactory manner as determined by the Purchaser. The Contractor shall perform 100% of deliverable requirements to the satisfaction of the Purchaser, within the PO-required deadlines.

8.1 Performance Compliance

By submitting a response to this RFQ, the Contractor acknowledges and agrees that its performance under this SOW must meet the standards set forth above and that it will be bound by the conditions set forth herein. After executing an applicable financial consequence, the Purchaser may, at its sole discretion, allow additional time for the

Contractor to remedy the performance issues identified by the Purchaser; or, after giving the Contractor a reasonable opportunity to cure such performance issues, may proceed with default proceedings.

The Purchaser reserves the right to perform or assign the required services to another contractor, if the awarded Contractor is not achieving the required levels of service, after the Contractor has been duly notified of their inadequacy.

Where any applicable ATC(s) and PO(s) require the generation and submission of deliverables to the Purchaser, receipt by the Purchaser will not be construed to mean or imply acceptance of those deliverables. It is specifically intended by the Purchaser that acceptance of required deliverables constitute a separate act. The Purchaser may reject deliverables as incomplete, inadequate, or unacceptable according to the parameters set forth in this SOW.

By submitting a Quote, the vendor represents and warrants that the Solution substantially conforms or exceeds the specifications herein and will continue to substantially conform or exceed the specifications provided herein throughout the duration of any resultant ATC and PO. The Solution's failure to substantially conform or exceed these specifications may result in termination of any resultant ATC or PO(s).

9.0 FINANCIAL CONSEQUENCES

The Purchaser shall impose financial consequences upon the Contractor for failure to comply or submit evidence documenting compliance with the performance standard requirements, or deliverable deemed unacceptable by the Purchaser if the Contractor fails to resolve errors, as set forth in **Section 7.0**, Deliverables. If the Purchaser chooses to allow completion of Contract requirements after the time allowed, its allowance shall not act as a waiver of financial consequences. These financial consequences are not a penalty and are intended to incentivize successful performance of the specified requirements.

The financial consequences assessed will result in a payment or an automatic credit to the Purchaser, at the Purchaser's discretion. In the event the Purchaser disagrees with a financial consequence assessment by the Contractor, the Purchaser will make the final determination on the Contractor's compliance with the deliverables and financial consequence assessment.

10.0 RESPONSE CONTENT AND FORMAT

10.1 Responses are due by the date and time shown in **Section 11.0**, Timeline.

10.2 Quotes shall be concise, in an electronic Adobe PDF format, and prepared using the following outline:

- 1) Documentation to describe the endpoint detection and response Solution proposed and how it meets the requirements of this RFQ to include the following at a minimum:
 - a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.
 - b. A draft SLA for training and support which adheres to all provisions of this RFQ.

- i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).
 - c. A draft implementation plan for a Customer which adheres to all provisions of this RFQ.
 - d. A draft MDR SLA, if applicable, per section 6.6.1 with annual pricing.
 - e. A draft SLA for future integrations, if applicable, per section 6.6.2 with pricing.
 - f. A draft disaster recovery plan per section 32.5.
- 2) Documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.
 - 3) Documentation describing the vendor's capacity and ability to implement the Solution on a statewide basis.
 - 4) Detail regarding any value-added services.
 - 5) **Attachment A**, Price Sheet, containing pricing for all items and completed in accordance with the instructions provided in this RFQ.
 - 6) **Attachment B**, Contact Information Sheet, containing the contacts for the Quote and the resulting ATC(s) and PO(s).
 - 7) **Non-Disclosure Agreement** executed by the vendor.

If the vendor is utilizing subcontractors, the vendor shall identify all subcontractors the vendors will utilize to provide the services required by this RFQ and what services each subcontractor will provide.

10.3 All Quotes should be submitted via email to the Department's Procurement Officer, identified in **Section 12.0**. Quotes must remain valid for at least 180 calendar days.

Note: If the vendor considers any part of its response to the RFQ to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information"), it shall provide the Department with a copy of its response with such Confidential Information redacted in accordance with Section 19.

11.0 **TIMELINE**

EVENT	DATE
Release of the RFQ	May 10, 2023
Pre-Quote Conference Registration Link: https://us02web.zoom.us/meeting/register/tZMrf-2qqTgtEtUhsUQg5jjixaUSqJ9oFLS	May 15, 2023, at 2:00 p.m., Eastern Time
Responses Due to the Procurement Officer, via email	May 19, 2023, by 5:00 p.m., Eastern Time
Solution Demonstrations and Quote Negotiations	May 22-24, 2023
Anticipated Award, via email	May 24, 2023

12.0 PROCUREMENT OFFICER

The Procurement Officer for this RFQ is:

Alisha Morgan
Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950
DMS.Purchasing@dms.fl.gov

13.0 PRE-QUOTE CONFERENCE

The Department will hold a Pre-Quote Conference as indicated in **Section 11.0**, Timeline, above to answer vendor questions. The Department will use its best efforts to answer vendor questions during the Pre-Quote Conference.

14.0 SOLUTION DEMONSTRATIONS

If the Department requests a demonstration of the Solution, the vendor must be available to demonstrate the Solution to the Department during the timeframe specified in **Section 11.0**, Timeline.

15.0 QUOTE NEGOTIATIONS

The Department may schedule negotiation sessions with vendors to discuss the Quote if any aspects of the Quote are not in the best interest of the Department. These negotiations will be scheduled in the timeframe specified in **Section 11.0**, Timeline. The Department does not anticipate exceeding these timeframes. The Department may require the vendors to revise any terms and conditions in the vendor's Quote, including any SLAs, during this timeframe.

16.0 SELECTION OF AWARD

The Department intends to select one (1) or more vendor(s) that provide the overall best value to the State. The Department will consider all aspects of submitted Quotes when making a selection, including the proposed Solution, how it meets the requirements, benefits to the State, and price.

17.0 RFQ HIERARCHY

The ATC(s) and PO(s) resulting from this RFQ will include the following Attachments which set forth the entire understanding of the Customer, the Contractor, and the Department and supersede all prior agreements. All Attachments listed below will be incorporated in their entirety into, and form part of any ATC(s) or PO(s) issued. In the event of a conflict between the documents that make up any ATC(s) and PO(s), priority shall be in the order listed:

- 1) The PO(s);
- 2) The ATC(s);
- 3) The Department's Non-Disclosure Agreement (NDA) or other Purchaser's NDA;
- 4) This RFQ;
- 5) Department's Purchase Order Terms and Conditions;
- 6) The ACS contract the vendor submitted their Quote in accordance with [ACS: Cloud Solutions (43230000-NASPO-16-ACS), Software Value Added Reseller (SVAR) (43230000-23-NASPO-ACS), or Technology Products, Services, Solutions, and Related Products and Services (43210000-US-16-ACS)]; and
- 7) The vendor's Quote.

18.0 DEPARTMENT'S CONTRACT MANAGER

The Department's Contract Manager who will oversee the Contractor's performance of its duties and obligations pursuant to the terms of any applicable ATC and any resultant PO and serve as a liaison with the Contractor, will be as follows:

To Be Determined
Florida Department of Management Services
Florida Digital Service
2555 Shumard Oak Blvd
Tallahassee, FL 32399
purchasing@digital.fl.gov

19.0 PAYMENT

- 19.1 The Contractor will be compensated in advance, annually, for all Deliverables per PO. Once the Implementation Plan is approved by the Purchaser, FL[DS] (if applicable) and the Customer in writing, the Contractor shall provide the Customer with access to the software in accordance with the Final Implementation Plan. Once software access is granted to the Customer, and the Customer confirms receipt, the Contractor will submit one (1) invoice to the Contract Manager specified in the PO indicating the date the Customer received the software access.
- 19.2 On each invoice, the Contractor shall certify that all costs and fees claimed in the invoice statement for payment are accurate and were performed in furtherance of the PO.
- 19.3 Contractor compensation will be exclusively made in accordance with the terms of this RFQ, any applicable ATC, and the PO. The Purchaser will not reimburse the Contractor for any other expenses associated with, or related to, any applicable ATC or resultant PO(s). For example, travel related expenses, including lodging, mileage, vehicle rental, and food, will not be subject to reimbursement.
- 19.4 Purchasers shall pay invoices in accordance with their governing laws and regulations, which shall govern the rights and obligations of the Purchaser and the Contractor. The Department shall pay invoices submitted by the Contractor in accordance with the provisions of section 215.422, F.S., which shall govern the rights and obligations of the Department and the Contractor.
- 19.5 The Contractor is responsible for the performance of all tasks and deliverables contained in any applicable ATC or PO.

20.0 PUBLIC RECORDS AND DOCUMENT MANAGEMENT

20.1 Access to Public Records

The Department may unilaterally cancel any applicable ATC or PO for failure by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F.S., made or received by the Contractor in conjunction with any applicable ATC or PO.

20.2 Contractor as Agent

Solely for the purposes of this section, the Contract Manager specified in the PO is the custodian of public records. If under the PO, the Contractor is providing services and is acting on behalf of a public agency, as provided by section 119.0701, F.S., the Contractor shall:

- 1) Keep and maintain public records required by the public agency to perform the service.
- 2) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time and at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
- 3) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the PO term and following the completion of the PO if the Contractor does not transfer the records to the public agency.
- 4) Upon completion of the PO, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the PO, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the PO, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Purchaser, upon request from the Purchaser's custodian of public records, in a format that is compatible with the information technology systems of the Purchaser.
- 5) **IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, F.S., TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE PURCHASE ORDER, CONTACT THE FOLLOWING CONTACTS:**

DEPARTMENT:

CUSTODIAN OF PUBLIC RECORDS

PHONE NUMBER: 850-487-1082

EMAIL: PublicRecords@dms.fl.gov

**MAILING ADDRESS: 4050 ESPLANADE WAY, SUITE 160
TALLAHASSEE, FL 32399.**

OTHER PURCHASER:

CONTRACT MANAGER SPECIFIED ON THE PO

20.3 Public Records Exemption

The Contractor may have access to cybersecurity information classified as confidential and exempt under section 119.0725, F.S. In the event that the Contractor has access to confidential and exempt information, the Contractor agrees to maintain the confidentiality as required in section 119.0725, F.S.

20.4 Document Management

The Contractor must retain sufficient documentation to substantiate claims for payment under the PO and all other records, electronic files, papers, and documents that were made in relation to the PO. The Contractor must retain all documents related to the PO for five (5) years after the expiration of the PO, or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at the Department of State's Records Management website.

21.0 IDENTIFICATION AND PROTECTION OF CONFIDENTIAL INFORMATION

Article 1, section 24, Florida Constitution, guarantees every person access to all public records, and section 119.011, F.S., provides a broad definition of "public records." As such, records submitted to an Agency as defined in section 119.011, F.S. (referred to for purposes of this Section 19 as "Agency") are public records and are subject to disclosure unless exempt from disclosure by law. If the vendor considers any portion of records it provides to an Agency (including those submitted in response to this RFQ) to be trade secret or otherwise confidential or exempt from disclosure under Florida or federal law ("Confidential Information"), the vendor shall mark the document as "confidential" and simultaneously provide that Agency with a separate, redacted copy of the record. For each portion redacted, the vendor should briefly describe in writing the grounds for claiming exemption, including the specific statutory citation for such exemption. The vendor shall only redact portions of records that it claims are Confidential Information.

In the event of a request for public records pursuant to Chapter 119, F.S., the Florida Constitution, or other authority, to which records that are marked as "confidential" are responsive, the Agency will provide the vendor-redacted copy to the requestor. If a requestor asserts a right to the redacted Confidential Information, the Agency will notify the vendor such an assertion has been made. It is the vendor's responsibility to take the appropriate legal action to assert that the information in question is exempt from disclosure under Chapter 119, F.S., or other applicable law.

If the Agency becomes subject to a demand for discovery or disclosure of documents that are marked as "confidential" in a legal proceeding, the Agency will give the vendor notice of the demand or request. The vendor shall take the appropriate legal action in response to the demand and to defend its claims of confidentiality. If the vendor fails to take appropriate and timely action to protect the records it has designated as Confidential Information, the Agency will provide the unredacted records to the requester.

The vendor shall protect, defend, and indemnify the Agency and any applicable Customer for all claims, costs, fines, and attorneys' fees arising from or relating to the vendor's determination that the redacted portions of its records are Confidential Information. If the vendor fails to submit a redacted copy in accordance with this section, of information it claims is Confidential Information, the Agency is authorized to produce the entire record submitted to the Agency in response to a public records request for, or demand for discovery or disclosure of, these records.

22.0 USE OF SUBCONTRACTORS

In providing services under the PO(s) and any applicable ATC, the Contractor is permitted to utilize subcontractors identified in its Quote. The Contractor shall notify the Contract Manager specified on the PO in writing of any subcontractors not identified in the Contractor's Quote who will be engaged to provide services for a PO 10 calendar days prior to their engagement.

During the term of the PO, subcontractors may be substituted with the prior written approval of the Contract Manager specified on the PO. The Purchaser reserves the right to reject a subcontractor with 10 calendar days advance notification to the Contractor.

The Contractor is fully responsible for the satisfactory completion of all subcontracted work and is required to ensure subcontractor's adherence to the terms set forth any PO.

The Contractor shall make all payments to subcontractors. If the Contractor utilizes a subcontractor, the Contractor shall pay the subcontractor within seven (7) Business Days after any payment is received from the Purchaser, per section 287.0585, F.S. It is understood, and agreed upon, that the Department shall not be held accountable to any subcontractor for any expenses or liabilities incurred under the subcontract, and that the Contractor is solely responsible to the subcontractor for all expenses and liabilities under the Contract. If the Contractor fails to pay the subcontractor within seven (7) Business Days, the Contractor shall pay the penalty to the subcontractor in the amount of one-half (1/2) of one percent (1%) of the amount due, per Calendar Day, from the expiration of the period allowed herein for payment. Such penalty shall be in addition to actual payments owed and shall not exceed 15% of the outstanding balance due.

23.0 LEGISLATIVE APPROPRIATION

Pursuant to section 287.0582, F.S., the State of Florida's performance and obligation to pay under any PO is contingent upon an annual appropriation by the Legislature.

24.0 MODIFICATIONS

The Department reserves the right to change, add or delete any requirement from this RFQ if the Department deems it to be in the best interest of the State of Florida. In addition, the Department reserves the right to withdraw and cancel this RFQ at any time, prior to a duly authorized and executed ATC or PO.

25.0 CONFLICT OF INTEREST

It is essential that the vendor and any subcontractors are independent and impartial and that the implementation of decisions made as it relates to consultation and services is not used for private gain or other remuneration. The Contractor shall not receive any monies for services provided under the PO aside from those paid pursuant to the PO.

26.0 DISCRIMINATORY, CONVICTED AND ANTITRUST VENDORS LISTS

The vendor is hereby informed of the provisions of sections 287.133(2)(a), 287.134(2)(a), and 287.137(2)(a), F.S., that identify the impacts to the vendor 's ability or its affiliates' ability to respond to the competitive solicitations of a public entity; to be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with a public entity; or to transact business with a public entity if it, or its affiliates, are placed on the Convicted Vendor, Discriminatory Vendor, or Antitrust Violator Vendor Lists of the Department of Management Services. The Contractor shall promptly notify the Purchaser if it or its suppliers, subcontractors, or consultants under any POs are placed on any such lists.

27.0 E-VERIFY

The Contractor (and its subcontractors) has an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By accepting the ATC or any PO(s), the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S. The Contractor must obtain an affidavit from its subcontractors in

accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of any applicable ATC(s) and any PO(s). The Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager specified on the PO within five (5) business days of issuance of the ATC or any PO(s). The Contract Manager will be designated on any applicable ATC and PO.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the ATC and any other Purchaser's obligation to terminate any PO(s) if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one (1) year after the date of such termination. The Department or any other applicable Purchaser will promptly notify the Contractor and order the immediate termination of any contract between the Contractor and a subcontractor performing work on its behalf under the ATCs and any PO(s) should the Department or any other applicable Purchaser develop a good faith belief that the subcontractor has knowingly violated section 448.095(1), F.S.

28.0 COOPERATION WITH INSPECTOR GENERAL

Pursuant to section 20.055(5), F.S., Contractor, and its subcontractors (if any), understand and will comply with their duty to cooperate with the Department's or any Purchaser's Inspector General in any investigation, audit, inspection, review, or hearing.

29.0 ACCESSIBILITY

The Contractor will comply with section 508 of the Rehabilitation Act of 1973, as amended and 29 U.S.C. s. 794(d), including the regulations set forth under 36 C.F.R. part 1194. Section 282.601(1), F.S., states that "state government shall, when developing, competitively procuring, maintaining, or using electronic information or information technology acquired on or after July 1, 2006, ensure that State employees with disabilities have access to and are provided with information and data comparable to the access and use by State employees who are not individuals with disabilities."

30.0 PRODUCTION AND INSPECTION

In accordance with section 216.1366, F.S., any public agency is authorized to inspect the: (a) financial records, papers, and documents of the contractor that are directly related to the performance of the contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of the contractor which the public agency determines are necessary to monitor the performance of the contract or to ensure that the terms of the PO are being met. The Contractor shall provide such records, papers, and documents requested by the public agency within 10 business days after the request is made.

31.0 SCRUTINIZED COMPANIES

In accordance with the requirements of section 287.135(5), F.S., the vendor certifies that it is not participating in a boycott of Israel. At the Department's or Purchaser's option, any applicable ATC or PO may be terminated if the Contractor is placed on the Quarterly List of Scrutinized Companies that Boycott Israel (referred to in statute as the "Scrutinized Companies that Boycott Israel List") or becomes engaged in a boycott of Israel. The State Board of Administration maintains the "Quarterly List of Scrutinized Companies that Boycott Israel" at the following link:

<https://www.sbafla.com/fsb/FundsWeManage/FRSPensionPlan/GlobalGovernanceMandates.aspx>.

32.0 BACKGROUND SCREENING

All Contractor employees and their subcontractors and agents performing work under the Contract must comply with all security and administrative requirements of the Department and the Purchaser.

32.1 Background Check

In addition to any background screening required by the Contractor as a condition of employment, the Contractor warrants that it will conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees or other person, hereinafter referred to as "Person" or "Persons," operating under their direction who directly perform services under the Contract, whether or not the Person has access to State of Florida Data, as well as those who have access, including indirect access, to State of Florida Data, whether or not they perform services under the PO. The Contractor warrants that all Persons will have passed the Background Screening described herein before they have Access to Data or begin performing services under the Contract. The look-back period for such background screenings shall be for a minimum of six years where six years of historical information is available.

"Access" means to review, inspect, approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any data, regardless of type, form, or nature of storage. Access to a computer system or network includes local and remote access.

"Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions, whether it is exempt, confidential, or personal health information. Data may be in any form, including but not limited to, storage media, computer memory, in transit, presented on a display device, or in physical media such as paper, film, microfilm, or microfiche. Data includes the original form of the Data and all metadata associated with the Data.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

- 1) Social Security Number Trace; and
- 2) Criminal Records (Federal, State and County criminal felony and misdemeanor, national criminal database for all states which make such data available).

32.2 Disqualifying Offenses

If at any time it is determined that a Person has a criminal misdemeanor or felony record regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) within the last six years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that Person from any position with

access to State of Florida Data or directly performing services under the Contract. The disqualifying offenses are:

- 1) Computer related or information technology crimes;
- 2) Fraudulent practices, false pretenses and frauds, and credit card crimes;
- 3) Forgery and counterfeiting;
- 4) Violations involving checks and drafts;
- 5) Misuse of medical or personnel records; or
- 6) Felony theft.

If the Contractor finds a Disqualifying Offense for a Person within the last six years from the date of the court's disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have access to State of Florida Data. The Contractor will consider the following factors only in making the determination: i.) nature and gravity of the offense, ii.) the amount of time that has elapsed since the offense, iii.) the rehabilitation efforts of the person, and iv.) relevancy of the offense to the job duties of the Person. If the Contractor determines that the Person should be allowed access to State of Florida Data, then Contractor shall maintain all criminal background screening information and the rationale for such access in the Person's employment file.

32.3 Refresh Screening

The Contractor will ensure that all background screening will be refreshed every five (5) years from the time initially performed for each Person during the Term of the Contract.

32.4 Self-Disclosure

The Contractor shall ensure that all Persons have a responsibility to self-report within three calendar days to the Contractor any updated court disposition regarding any disqualifying offense, regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict). The Contractor shall immediately reassess whether to disallow that Person access to any State of Florida premises or from directly performing services under the Contract. Additionally, the Contractor shall require that the Person complete an annual certification that they have not received any additional criminal misdemeanor or felony record regardless of adjudication (adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) for the Disqualifying Offenses and shall maintain that certification in the employment file.

In addition, the Contractor shall ensure that all Persons have a responsibility to self-report to the Contractor within three calendar days, any arrest for any Disqualifying Offense. The Contractor shall notify the Contract Manager specified on the PO and any applicable ATC within 24 hours of all details concerning any reported arrest.

32.5 Duty to Provide Security Data

The Contractor will maintain the security of State of Florida Data including, but not limited to, a secure area around any display of such Data or Data that is otherwise visible. The Contractor will also comply with all state and federal rules and regulations regarding security of information, including HIPPA when applicable. Data cannot be disclosed to any person or entity that is not directly approved to participate in the SOW set forth in any resulting ATC or PO.

The Contractor must deliver an attestation describing the classification of Customer data consumed by the Solution to ensure suitable controls are considered for classified data. Additionally, the Contractor will provide documentation and evidence describing the technical security controls commensurate with the data's classification as defined in Chapter 60GG-2, F.A.C. For any data identified as uniquely valuable to the Customer, the Contractor must provide a disaster recovery plan which must be approved by the Customer.

32.6 Screening Compliance Audits and Security Inspections

The Purchaser reserves the right to audit the Contractor's background screening process upon two (2) business days prior written notice to the Contractor during the Term of the PO and any applicable ATC. In the event of an incident as defined in section 282.0041, F.S., the Department will have the right to inspect to meet all applicable state and federal rules and regulations upon two (2) business days prior written notice to the Contractor to ensure that access to the State of Florida Data is secure and in compliance with any PO or applicable ATC.

32.7 Record Retention

The Customer will maintain ownership of all data consumed by the Solution. For all such data, Contractor shall comply with and grant all rights in Section 18.2 to each Customer.

The Contractor shall retain a list of all persons with Access to Data, including a statement confirming that each person has passed the background screening required herein. Such a statement shall not include the substance of the screening results, only that the person has passed the screening.

The Contractor shall create a written policy for the protection of Data, including a policy and procedure for Access to Data. The Contractor shall document and record, with respect to each instance of Access to Data:

- 1) The identity of all individual(s) who accessed data in any way, whether those individuals are authorized persons or not.
- 2) The duration of the individual(s)' access to Data, including the time and date at which the access began and ended.
- 3) The identity, form, and extent of Data accessed, including, but not limited to, whether the individual accessed partial or redacted versions of Data, read-only versions of Data, or editable versions of Data.
- 4) The nature of the access to Data, including whether Data was edited or shared with any other individual or entity during the duration of the access, and, if so, the identity of the individual or entity.

The Contractor shall retain the written policy and information required in this section for the duration of the Contract and a period of no less than five (5) years from the date of termination of the Contract and any Contract extensions. The written policy and information required in this section shall be included in Department's or the Purchaser's audit and screening abilities as defined in Section 30.6, Screening Compliance Audits and Security Inspections. The written policy and information required in this section shall also be subject to immediate disclosure upon written or

oral demand at any time by the Department, the Purchaser, or its designated agents or auditors.

Failure to compile, retain, and disclose the written policy and information as required in this section shall be considered a breach of any ATC(s) and PO(s). The resulting damages to the Department from a breach of this section are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Contractor, the Customer, and the Department acknowledge that these financial consequences are liquidated damages, exclusive of any other right to damages, not intended to be a penalty and solely intended to compensate for unknown and unascertainable damages. The Contractor therefore agrees to credit the affected Customer, the sum of **\$500.00** for each breach of this section.

32.8 Indemnification

The Contractor agrees to defend, indemnify, and hold harmless the Department and any applicable Customers, the State of Florida, its officers, directors and employees for any claims, suits or proceedings related to a breach of this section. The Contractor will include credit monitoring services at its own cost for those individuals affected or potentially affected by a breach of this section for a two-year period following the breach.

33.0 LOCATION OF DATA

In accordance with Rule 60GG-4.002, F.A.C., the Contractor, including its employees, subcontractor personnel, independent contractors, leased employees, volunteers, licensees, or other persons operating under their direction, are prohibited from (i) performing any of the services under any applicable ATC or PO outside of the continental United States, or (ii) sending, transmitting, storing, or accessing any State of Florida data, outside of the continental United States. The Parties agree that a violation of this provision will:

- a) Result in immediate and irreparable harm to the Purchaser, the Department, or the Customer, entitling the Purchaser, the Department, or the Customer to immediate injunctive relief, provided, however, this shall not constitute an admission by the Contractor to any liability for damages under subsection (c) below or any claims, liability, or damages to a third party, and is without prejudice to the Contractor in defending such claims.
- b) Entitle the Purchaser, the Department, or the Customer, as applicable, to a credit or payment, at the Purchaser's discretion, of \$50,000 per violation, with a cumulative total cap of \$500,000 per event. This credit or payment is intended only to cover the Purchaser's, the Department's, or the Customer's internal staffing and administrative costs of investigations and audits of the transmittal of State of Florida data outside the U.S.
- c) Entitle the Purchaser, the Department, or the Customer, as applicable, to recover damages, if any, arising from a breach of this subsection and beyond those covered under subsection b).

The credits or payments in subsection b) are a reasonable approximation of the internal costs for investigations and audits from a violation. The credits or payments are in the nature of liquidated damages and not intended to be a penalty. By executing any resulting ATC or performing under any resulting PO, the Contractor acknowledges and agrees the costs

intended to be covered by subsection b) are not readily ascertainable and will be difficult to prove. The Contractor agrees that it will not argue, and is estopped from arguing, that such costs are a penalty or otherwise unenforceable. For purposes of determining the amount of costs due hereunder, a group of violations relating to a common set of operative facts (e.g., same location, same time period, same off-shore entity) shall be treated as a single violation. The costs will be applied as a financial consequence and are exclusive of any other right to damages.

34.0 DATA TRANSMISSION

Solution data shall only be transmitted through secure transmission methods utilizing a National Institute of Standards and Technology approved means of electronic encryption as well as password protection and in a file format and layout determined by the Department or the Purchaser, as applicable. Solution data shall not be transmitted via any other means, including electronic mail. If applicable to any transmission of the Solution data, both transmitter and the receiver shall completely and permanently remove Solution data from any temporary transfer location within twenty-four (24) hours of receipt of the Solution data.

35.0 TERMS AND CONDITIONS

The Department shall not accept any unrequested terms or conditions submitted by a vendor, including any appearing in documents attached as part of the vendor's Quote or on documents submitted after award. In submitting its Quote, the vendor agrees that any additional terms or conditions, whether submitted intentionally or inadvertently, shall have no force or effect, though items that the Department identified herein as negotiable may be negotiated. The Department will not accept or comply with any automatic renewal language within the vendor's Quote or any associated document. Any automatic renewal language will be deemed null and void. All licenses purchased through this RFQ shall have a one-year term, which may only be renewed by the Department through a new purchase order. The aforementioned provision is non-negotiable.

36.0 COOPERATIVE PURCHASING

Pursuant to their own governing laws, and subject to the agreement of the Contractor, Customers may make purchases in accordance with the terms and conditions contained herein. The Department shall not be a party to any transaction between the Contractor and any other Purchaser.

37.0 PRICE ADJUSTMENTS

The Contractor shall apply to the Department and Purchaser any price decrease effectuated during the Contract term by reason of market change or special sales offered to other customers. Such a price decrease applies regardless of whether any related equipment is rented or leased by the Department or Purchaser under the Contract. Price increases are rejected, unless otherwise stated. All prices are firm and shall be held for the duration of the Contract term.

38.0 FINANCIAL STABILITY

The Contractor is required to have financial stability in accordance with section 287.057 (27)(b), F.S. The Department will not entertain terms and condition negotiations with third parties regarding financing or funding associated with this RFQ.

39.0 RFQ ATTACHMENTS

Attachment A, Price Sheet
Attachment B, Contact Information Sheet

Agency Term Contract (Redlines or modifications to the ATC are not permitted.)
Department's Purchase Order Terms and Conditions
Non-Disclosure Agreement (Redlines or modifications to the NDA are not permitted.)

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT A PRICE SHEET

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

- _____ 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services
- _____ 43230000-NASPO-16-ACS Cloud Solutions
- _____ 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the endpoint detection and response Solution for FL[DS] and all Customers. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of any applicable ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p><u>Initial Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	\$ _____
2	<p><u>Subsequent Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	SKU Description	Market Price	ACS Price

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VI. State of Florida Enterprise Pricing (Optional)

The Department is also seeking an optional annual fixed rate to provide the Solution and services to all potential FL[DS] Customers. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for endpoint detection and response, at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor’s behalf, as confirmed by the signature below.

Vendor Name

Signature

FEIN

Signatory Printed Name

Date

ATTACHMENT B
CONTACT INFORMATION SHEET

I. Contact Instructions

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
Name:		
Title:		
Address (Line 1):		
Address (Line 2):		
City, State, Zip Code		
Telephone (Office):		
Telephone (Mobile):		
Email:		

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 1. Purchase Order.

A. Composition and Priority.

The Contractor agrees to provide commodities or contractual services to the Agency within the manner and at the location specified in the Purchase Order, and any attachments to the Purchase Order. These Purchase Order Terms and Conditions, whether generic or specific, shall take precedence over any inconsistent or conflicting provision in the State of Florida, General Contract Conditions, PUR 1000. Additionally, the terms of the Purchase Order supersede the terms of any and all prior agreements with respect to this purchase.

B. Initial Term.

Unless otherwise specified, the Purchase Order begins on the date of issuance. Contractual services or commodities to be provided by the Contractor shall be completed by the date specified on the Purchase Order end date.

Section 2. Performance.

A. Performance Standards.

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Statement of Work and attachments to the Purchase Order. The Agency shall be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination shall be maintained by the Contractor with representatives of the Agency, or of other agencies involved in the project on behalf of the Agency.

B. Performance Deficiency.

If the Agency determines that the performance of the Contractor is unsatisfactory, the Agency may notify the Contractor of the deficiency to be corrected, which correction shall be made within a time-frame specified by the Agency. The Contractor shall provide the Agency with a corrective action plan describing how the Contractor will address all issues of contract non-performance, unacceptable performance, and failure to meet the minimum performance levels, deliverable deficiencies, or contract non-compliance. If the corrective action plan is unacceptable to the Agency, the Contractor will be assessed a non-performance retainage equivalent to 10% of the total invoice amount or as specified in the contractual documents. The retainage will be applied to the invoice for the then-current billing period. The retainage will be withheld until the Contractor resolves the deficiency. If the deficiency is subsequently resolved, the Contractor may invoice the Agency for the retained amount during the next billing period. If the Contractor is unable to resolve the deficiency, the funds retained will be forfeited.

Section 3. Payment and Fees.

A. Payment Invoicing.

The Contractor will be paid upon submission of properly certified invoice(s) to the Agency after delivery and acceptance of commodities or contractual services is

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

confirmed in writing by the Agency. Invoices shall contain detail sufficient for audit thereof and shall contain the Purchase Order and the Contractor's Federal Employer Identification Number or Social Security Number.

B. Payment Timeframe.

Section 215.422, Florida Statutes (F.S.), provides that agencies have five (5) working days to inspect and approve commodities or contractual services. Items may be tested for compliance with specifications. Items delivered not conforming to specifications may be rejected and returned at the Contractor's expense. Interest penalties for late payment are also provided for in section 215.422, F.S. A Vendor Ombudsman, whose duties include acting as an advocate for Vendors who may be experiencing problems obtaining timely payment(s) from an Agency, may be contacted at 850-413-5516, or Vendors may call the State Comptroller's Hotline at 1-800-848-3792.

C. MyFloridaMarketPlace Fees.

The following language is included pursuant to rule 60A-1.031, Florida Administrative Code:

The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), Florida Statutes. Payments issued by Agencies or Eligible Users to Vendors for purchases of commodities or contractual services are subject to Transaction Fees, as prescribed by rule 60A-1.031, Florida Administrative Code, or as may otherwise be established by law. Vendors shall submit monthly reports required by the rule. All reports shall be subject to audit. Failure to pay Transaction Fees or submit reports shall constitute grounds for default and exclusion from business with the State of Florida.

D. Payment Audit.

Records of costs incurred under terms of the Purchase Order shall be maintained and made available to the Agency upon request at all times during the period of the Purchase Order, and for a period of three years thereafter. Records of costs incurred shall include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Agency for audit.

E. Annual Appropriation and Travel.

Pursuant to section 287.0582, F.S., if the Purchase Order binds the State or an executive agency for the purchase of services or tangible personal property for a period in excess of one (1) fiscal year, the State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature. Travel expenses are not reimbursable unless specifically authorized in writing, and shall be reimbursed only in accordance with section 112.061, F.S.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 4. Liability.

A. Indemnity.

To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the State of Florida, its officers, employees and agents harmless from all fines, claims, assessments, suits, judgments, or damages, consequential or otherwise, including court costs and attorney's fees, arising out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Purchase Order, as well as for any determination arising out of or related to the Purchase Order, that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Agency. The Purchase Order does not constitute a waiver of sovereign immunity or consent by the Agency or the State of Florida or its subdivisions to suit by third parties.

B. Payment for Claims.

The Contractor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Contractor or any employee, agent, subcontractor, assignee or delegate in connection with the Purchase Order.

C. Liability Insurance.

The Contractor shall maintain insurance sufficient to adequately protect the Agency from any and all liability and property damage/hazards which may result from the performance of the Purchase Order. All insurance shall be with insurers qualified and duly licensed to transact business in the State of Florida. If required by the Agency and prior to commencing any work the Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in full force and showing the Agency to be an additional insured.

D. Workers' Compensation.

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law.

E. Performance Bond.

Unless otherwise prohibited by law, the Agency may require the Contractor to furnish, without additional cost to the Agency, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Agency shall determine the type and amount of security.

Section 5. Compliance with Laws.

A. Conduct of Business.

The Contractor shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor shall comply with Section 247A of the Immigration and Nationality Act, the

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Americans with Disabilities Act, Health Insurance Portability and Accountability Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

Pursuant to subsection 287.058(1), F.S., the provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference, to the extent applicable.

B. Lobbying.

In accordance with sections 11.062 and 216.347, F.S., the Purchase Order funds are not for the purpose of lobbying the Legislature, the judicial branch, or an Agency. Pursuant to subsection 287.058(6), F.S., the Purchase Order does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Purchase Order, after the Purchase Order's execution and during the Purchase Order's term.

C. Gratuities.

The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State officer or employee.

D. Cooperation with Inspector General.

Pursuant to subsection 20.055(5), F.S., Contractor, and any subcontractor to the Contractor, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Purchase Order. The Contractor shall retain such records for three (3) years after the expiration of the Purchase Order, or the period required by the General Records Schedules maintained by the Florida Department of State (available at: <http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>), whichever is longer. The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

F. Communications and Confidentiality.

The Contractor agrees that it shall make no statements, press releases, or publicity releases concerning the Purchase Order or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Purchase Order, or any particulars thereof, during the period of the Purchase Order, without first notifying the Agency's Contract Manager or the Agency's designated contact person and securing prior written consent. The Contractor shall maintain confidentiality of all confidential data, files, and records related to the services and/or commodities provided pursuant to the Purchase Order and shall comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures shall be consistent with the most recent version of the Agency's security policies, protocols, and procedures. The Contractor shall also comply with any applicable professional standards with respect to confidentiality of information.

G. Intellectual Property.

Unless specifically addressed in the Purchase Order, intellectual property rights to all property created or otherwise developed by the Contractor for the Agency will be owned by the State of Florida through the Agency at the completion of the Purchase Order. Proceeds to any Agency derived from the sale, licensing, marketing or other authorization related to any such Agency-controlled intellectual property right shall be handled in the manner specified by applicable state statute.

H. Convicted and Discriminatory Vendor Lists.

In accordance with sections 287.133 and 287.134, F.S., an entity or affiliate who is on the Convicted Vendor List or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Purchase Order with any Agency.

Section 6. Termination.

A. Termination for Convenience.

The Purchase Order may be terminated by the Agency in whole or in part at any time in the best interest of the Agency. If the Purchase Order is terminated before performance is completed, the Contractor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Purchase Order price as the amount of work satisfactorily performed. All work in progress shall become the property of the Agency and shall be turned over promptly by the Contractor.

B. Termination for Cause.

If the Agency determines that the performance of the Contractor is not satisfactory, the Agency shall have the option of (a) immediately terminating the Purchase Order, or (b)

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Purchase Order will be terminated at the end of such time, or (c) take other action deemed appropriate by the Agency.

Section 7. Subcontractors and Assignments.

A. Subcontractors.

The Contractor shall not subcontract any work under the Purchase Order without the prior written consent of the Agency. The Contractor is fully responsible for satisfactory completion of all subcontracted work.

B. Assignment.

The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Purchase Order without the prior written consent of the Agency. In the event of any assignment, the Contractor remains secondarily liable for performance of the Purchase Order, unless the Agency expressly waives such secondary liability. The Agency may assign the Purchase Order with prior written notice to the Contractor.

Section 8. RESPECT and PRIDE.

A. RESPECT.

In accordance with subsection 413.036(3), F.S., if a product or service required for the performance of the Purchase Order is on the procurement list established pursuant to subsection 413.035(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INsofar AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated nonprofit agency and the products it offers is available at <http://www.respectofflorida.org>.

B. PRIDE.

In accordance with subsection 946.515(6), F.S., if a product or service required for the performance of the Purchase Order is certified by or is available from Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE) and has been approved in accordance with subsection 946.515(2), F.S., the following statement applies:

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INsofar AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the products it offers is available at <http://www.pride-enterprises.org>.

Section 9. Miscellaneous.

A. Independent Contractor.

The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Agency and are not entitled to the benefits of State of Florida employees. The Agency shall not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all of its subcontracts under the Purchase Order.

B. Governing Law and Venue.

The laws of the State of Florida shall govern the Purchase Order. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Purchase Order. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Agency.

C. Waiver.

The delay or failure by the Agency to exercise or enforce any of its rights under the Purchase Order shall not constitute waiver of such rights.

D. Modification and Severability.

The Purchase Order may only be modified by a change order agreed to by the Agency and the Contractor. Should a court determine any provision of the Purchase Order is invalid, the remaining provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Purchase Order did not contain the provision held to be invalid.

E. Time is of the Essence.

Time is of the essence with regard to each and every obligation of the Contractor. Each such obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

F. Background Check.

The Agency may require the Contractor and its employees, agents, representatives and subcontractors to provide fingerprints and be subject to such background check as directed by the Agency. The cost of the background check(s) shall be borne by the Contractor. The Agency may require the Contractor to exclude the Contractor's employees, agents, representatives or subcontractors based on the background check results.

G. E-Verify.

In accordance with Executive Order 11-116, the Contractor agrees to utilize the U.S. Agency of Homeland Security's E-Verify system, <https://e-verify.uscis.gov/emp>, to verify the employment eligibility of all new employees hired during the term of the Purchase Order for the services specified in the Purchase Order. The Contractor shall also include a requirement in subcontracts that the subcontractor shall utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Purchase Order term.

H. Commodities Logistics.

The following provisions shall apply to all Purchase Orders unless otherwise indicated in the contract documents:

- 1) All purchases are F.O.B. destination, transportation charges prepaid.
- 2) Each shipment must be shipped to the address indicated on the face of the Purchase Order and marked to the attention of the individual identified, if any. Each shipment must be labeled plainly with the Purchase Order number and must show the gross, tare, and net weight. A complete packing list must accompany each shipment. This paragraph shall also apply to any third party who ships items on behalf of the Contractor.
- 3) No extra charges shall be applied for boxing, crating, packing, or insurance.
- 4) The following delivery schedule shall apply: 8:00 AM – 4:00 PM, Monday through Friday, excluding legal holidays.
- 5) If delivery to the specified destination cannot be made on or before the specified date, notify the Agency immediately using the contact information provided in the MyFloridaMarketPlace system.
- 6) The Agency assumes no liability for merchandise shipped to other than the specified destination.
- 7) Items received in excess of quantities specified may, at Agency's option, be returned at the Contractor's expense. Substitutions are not permitted.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



**State of Florida Department of
Management Services**

RFQ DMS-22/23-155 for Endpoint Detection
and Response Solution

Due: May 19, 2023

REVISED 6/13/2023

IMPROVE SERVICE. MANAGE COST. REDUCE RISK.



May 19, 2023

Alisha Morgan
State of Florida Department of Management Services
4050 Esplanade Way
Tallahassee, FL 32399-0950

Ms. Morgan:

Attached, please find the Mainline Information Systems, Inc. proposal for Endpoint Detection and Response Solution in response to the State of Florida Department of Management Services RFQ DMS-22/23-155. Mainline is an authorized VMware Enterprise Partner in good standing and has been providing quality information technology products and services with the highest degree of customer service available for over 30 years.

The Department is seeking a contractor to provide an endpoint detection and response (EDR) solution for the Department and customers on a statewide basis. The solution shall include software, implementation, training, support, and integration services as described in the subject RFQ. The contractor shall be responsible for all aspects of providing the solution to customers.

This proposal demonstrates our commitment to a successful, long-term relationship with State of Florida Department of Management Services. Mainline is a remarketer of third-party hardware, software products, and maintenance support services. Performance of hardware, software products, and maintenance support services are subject to the applicable end user terms for such and may be subject to a third-party agreement between State of Florida Department of Management Services and the OEM. Mainline reserves the right to negotiate or reject any terms and conditions not included as part of the solicitation that may be made part of any subsequent award. Mainline's offer is valid for 180 days.

Thank you for considering the attached proposal to meet your technology needs. I look forward to discussing the elements of this proposal with you in detail. Please feel free to contact me for any additional information.

Sincerely,

Doug Harrell

Doug Harrell
Regional Vice President of Sales – Florida
Mainline Information Systems, Inc.
Phone: (850) 294-2237
Email: (850) 294-2237@mainline.com

State of Florida Department of Management Services

RFQ DMS-22/23-155 for Endpoint Detection and Response Solution

Due Date: May 19, 2023

Prepared For:

Alisha Morgan
State of Florida Department of Management
Services
4050 Esplanade Way
Tallahassee, FL 32399-0950

Presented By:

Doug Harrell
Account Executive

Mainline Information Systems, Inc.
(850) 294-2237
(850) 294-2237@mainline.com



Table of Contents

Technical Proposal.....	5
Past Performance	28
Value Added Services	41
Price Proposal.....	45
Contact Information Sheet.....	57
Non-Disclosure Agreement	59
Attachment A – Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDRTM Service Offerings	65
Attachment B – VMware Production Support for Cloud Products.....	68
Attachment C – VMware Carbon Black Cloud Deployment	70
Attachment D – Carbon Black Cloud Global Resiliency	91
Attachment E – System and Organization Controls Report SOC 3®	94
Attachment F - VMware Carbon Black PS Consume Add-Ons Essentials	109
Attachment G – VMware Carbon Black EDR Administrator	117
Addendum to Mainline Response to Florida DMS RFQ DMS-2223-155.....	120

Technical Proposal

Mainline Information Systems is pleased to offer a VMware Carbon Black Cloud solution to the Florida Digital Service (FL[DS]) as a continuation of our support to the State of Florida.

See and stop more attacks with a cloud native endpoint and workload protection platform that adapts to the environment and the evolving threat landscape.

Proactively Detect and Stop Emerging Attacks



Fortify Endpoint and Workload Protection

Legacy approaches fall short as cybercriminals update tactics and obscure their actions. Get advanced cybersecurity fueled by behavioral analytics to spot minor fluctuations and adapt in response.



Recognize New Threats

Analyze attackers' behavior patterns to detect and stop never-before-seen attacks with continuous endpoint activity data monitoring. Don't get stuck analyzing only what's worked in the past.



Simplify Your Security Stack

Streamline the response to potential incidents with a unified endpoint agent and console. Minimize downtime responding to incidents and return critical CPU cycles back to the business.

VMware Carbon Black Cloud by the Numbers

- 379% ROI over 3 years
- 7.5 Hours saved per security incident.
- 94% Of customers saw significant improvement in security efficacy.

VMware Carbon Black Cloud Features



Next-Gen Antivirus and Behavioral EDR

Analyze attacker behavior patterns over time to detect and stop never-before-seen attacks, whether they are malware, fileless or living-off-the-land attacks.



Managed Alert Monitoring and Triage

Gain 24-hour visibility from our expert security operations analysts who provide validation, context into root cause, and automated monthly executive reporting.



Real-Time Audit and Remediation

Easily assess your current system state to track and harden the security posture of all your protected devices.

The following four (4) pages provide a brief overview of the proposed solution.

VMware Carbon Black Cloud

Endpoint protection that adapts to your business

A cloud native platform delivering best-in-class, next-generation antivirus and endpoint detection and response without compromising system performance.

Policy Action: No Action

Process Status: Ran

CMD sh

SHA-256 b494b5a5e3

PID 1000

Start time 11:15

TTPs attempted_client

Signed Software

Product -

CA Apple

Publisher -

Malware No

App Origin

Adaptive Prevention Delivers Better Protection

CYBERATTACKS MATURE

6 Trillion

Estimated damages from cybersecurity attacks by 2021 ¹

70%

Of attacks featured lateral movement ²

57X

Predicted increase in ransomware damages from 2015-2021 ³

56%

Of breaches took months or longer to discover ⁴

27%

Are confident that antivirus will protect them from ransomware ⁵

The majority of today's cyberattacks feature advanced tactics such as lateral movement and island hopping that target legitimate tools to inflict damage. These sophisticated hacking methods pose a tremendous risk to targets with decentralized systems protecting high-value assets, including money, intellectual property and state secrets.

VMware Carbon Black Cloud™ thwarts attacks by making it easier to:

- Analyze billions of system events to understand what is normal in your environment
- Prevent attackers from abusing legitimate tools
- Automate your investigation workflow to respond efficiently

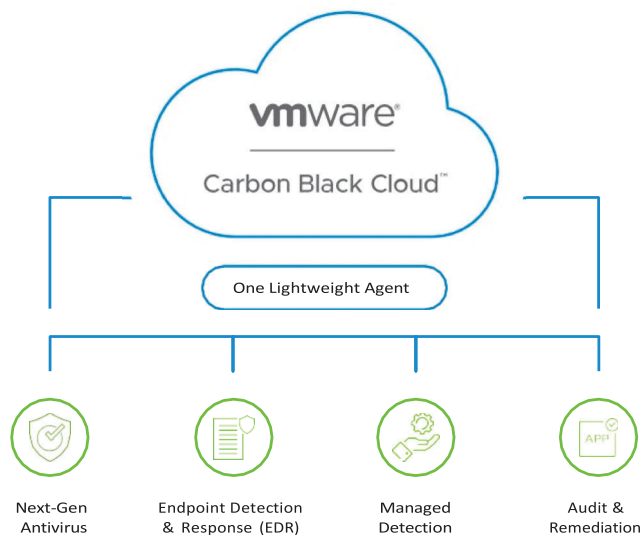
All of this is unified into one console and one agent, so that infrastructure and InfoSec teams have a single, shared source of truth to improve security together.

“VMware Carbon Black is essentially our Swiss army knife. We can do a lot of different things with a lot of information. The overall coverage and overall response times were greatly improved from what we had before. For us it was a no brainer.”

CARL ERICKSON, CISO, JOHNSON CONTROLS

One Platform for Your Endpoint Security Needs

VMware Carbon Black Cloud consolidates multiple endpoint security capabilities using one agent and console, helping you operate faster and more effectively. As part of VMware's intrinsic security approach, VMware Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats.



Endpoint standard – next-generation antivirus and behavioral EDR

Analyze attacker behavior patterns over time to detect and stop never-seen-before attacks, whether they are malware, fileless or living-off-the-land attacks.

Managed detection – managed alert monitoring and triage

Gain 24-hour visibility from our security operations center of expert analysts, who provide validation, context into root cause and automated monthly executive reporting.

Audit and remediation – real-time device assessment and remediation

Easily audit the current system state to track and harden the security posture of all your protected devices.

Enterprise EDR – threat hunting and containment

Proactively hunt for abnormal activity using threat intelligence and customizable detections.

Gartner

A VISIONARY

Gartner Magic Quadrant for
Endpoint Protection Platforms • August 2019
(as Carbon Black)



RATED 4.5 OUT OF 5

A Gartner Peer Insights
Customers' Choice for Endpoint Detection
and Response Solutions • 2020*



**MARKET LEADER IN MALWARE &
REAL-WORLD PROTECTION TESTS**

AV-Comparatives* April 2020

**MITRE
ATT&CK**

LEADER IN DETECTING THREATS

MITRE ATT&CK™ EDR Evaluation • 2020



**APPROVED CORPORATE ENDPOINT
PROTECTION**

AV-TEST Product Review and
Certification Report • 2020



**BEST CYBERSECURITY COMPANY
BEST ENDPOINT SECURITY SOLUTION**

Cybersecurity Excellence Awards • 2019

Start Learning More
Visit carbonblack.com >

¹ CSO Online, "Cybersecurity Business Report: Cybercrime Damages Expected to Cost the World 6 Trillion by 2021," Morgan, Steve. August 22, 2016, <https://www.csoonline.com/article/3110467/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html>

² Carbon Black, "Global Incident Response Threat Report: The Ominous Rise of "Island Hopping" & Counter Incident Response Continues", April , 2019, <https://cdn.www.carbonblack.com/wp-content/uploads/2019/04/carbon-black-quarterly-incident-response-threat-report-april-2019.pdf>

³ Cybercrime Magazine Online, "Global Ransomware Damage Costs Predicted to Reach 20 billion USD by 2021," Steve Morgan, October 21, 2019, <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

⁴ Verizon, "Verizon Data Breach Investigations Report," May, 2019, <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

⁵ Carbonite, "Rise of Ransomware," 2017, <https://www.carbonite.com/globalassets/files/white-papers/carbonite-rise-of-ransomware.pdf>

*Overall rating based on 74 total ratings as of 18 March 2020 in the EDR category. <https://www.carbonblack.com/resource/gartner-peer-insights-voice-of-the-customer-ep/>

The Gartner document is available upon request from Carbon Black. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. <https://www.carbonblack.com/resource/gartner-mq-2019/> The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved. <https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions>.



1) Documentation to describe the endpoint detection and response solution proposed and how it meets the requirements of this RFQ

Mainline Response:

Requirement	Response
<p>6.1. <u>Software Solution/Specifications</u></p> <p>The Solution shall detect and respond to threats on endpoint devices such as laptops, desktops, servers, and mobile devices. Endpoint Detection and Response (EDR) solutions typically use a combination of techniques such as behavioral analysis, machine learning, and threat intelligence to identify and respond to security incidents in real-time. The primary purpose of EDR is to detect and respond to advanced threats that have bypassed traditional security defenses such as firewalls and antivirus software. This is accomplished by collecting data from endpoint devices, analyzing it for signs of suspicious activity, and taking automated or manual actions to isolate and neutralize threats. EDR solutions can help organizations improve their overall security posture by providing visibility into the activities taking place on endpoint devices, helping security teams respond to incidents more quickly and effectively, and providing valuable</p>	<p>VMware Carbon Black Cloud™ (“VMware Carbon Black Cloud”) is a cloud-native Endpoint and workload protection platform that enables customers to protect, prevent, detect, and respond to cybersecurity attacks on their Endpoints and server workloads. VMware Carbon Black Cloud collects and consolidates a customer’s system data in a single platform to enable the customer to efficiently protect its environment from breaches. VMware Carbon Black Cloud pulls this information into a centralized data analytics platform, and provides the customer with analysis, alerts, and intelligence on vulnerabilities, suspicious activity, and blocked malware. Customers access the VMware Carbon Black Cloud service offerings through a web browser and by using scripts against a public API. VMware Carbon Black Cloud ingests a variety of data sources that are processed and stored as cybersecurity events, behaviors, and system state metrics that can be analyzed, visualized, and alerted upon for anomaly detection, incident investigation, and remediation of cybersecurity risks.</p>
<p>6.1.1. Multi-tenant</p> <p>The Solution shall support a multi-tenant, multi-organization architecture. Each tenant must have its own instance and each instance must aggregate up to a single instance and view. The aggregated instance will support enterprise security operations. The Solution shall provide dashboards for single-source visibility into threats, investigations, and trends.</p>	<p>The Carbon Black solution supports a multi-tenant organization in which each organization has its own instance. The roadmap is a more granular RBAC approach to allow a consolidation of threats and visibility across all organizations.</p>
<p>6.1.2. Scalability</p> <p><i>The Solution shall provide the ability to scale to support a large number of tenants and their endpoints.</i></p>	<p>Carbon Black is a Cloud SaaS platform that is flexible and modular with ability to scale.</p>

Requirement	Response						
<p>6.1.3. Cloud Management</p> <p>The Solution shall be provided as software as a service via cloud-hosted infrastructure to keep current with the latest releases of management server and endpoint agent software. The Solution shall allow capacity extensibility in the cloud with minimal impact on agent or management infrastructure.</p>	<p>The proposed solution is cloud hosted with minimal user impact.</p>						
<p>6.1.4. Managed Security Services</p> <p><i>The Solution shall deploy and maintain managed security services to support Purchasers and Customers, particularly the advanced administration requirement of endpoint detection and response tools and incident response capabilities.</i></p>	<p>Carbon Black MDR provides critical insight into attacks using automated ML to validate and prioritize alerts and uncover new threats as well as provide rapid response along with threat containment during an incident along with making policy recommendations to remediate threats.</p>						
<p>6.1.5. Prevention</p> <p>The Solution shall block malware pre-execution using the platform's antimalware prevention program.</p>	<p>VMware Carbon Black uses a 3 layered prevention compromised of Signature based prevention, Machine Learning, and Streaming Prevention (behavioral EDR).</p> <p>Create permission, blocking, and path denial rules to control what applications and behaviors the Carbon Black Cloud sensor prevents and allows in your environment.</p> <p>For Standard and Advanced default policies, many settings are activated out-of-the-box.</p> <p>Using wildcards in paths When adding a path, you can use wildcards to specify files or directories.</p> <table border="1" data-bbox="824 1404 1373 1812"> <thead> <tr> <th>Wildcard</th> <th>Description</th> <th>Example</th> </tr> </thead> <tbody> <tr> <td>*</td> <td>Matches 0 or more consecutive characters up to a single subdirectory level.</td> <td>C:\program files*\custom application*.exe Approves any executable files in: C:\program files\custom application\ C:\program files(x86)\custom</td> </tr> </tbody> </table>	Wildcard	Description	Example	*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files*\custom application*.exe Approves any executable files in: C:\program files\custom application\ C:\program files(x86)\custom
Wildcard	Description	Example					
*	Matches 0 or more consecutive characters up to a single subdirectory level.	C:\program files*\custom application*.exe Approves any executable files in: C:\program files\custom application\ C:\program files(x86)\custom					

Requirement	Response
	<p style="text-align: right;">application\ C:\Python27\Lib\site-packages**</p> <p>** Matches a partial path across all subdirectory levels and is recursive.</p> <p>Approves any files in that directory and all subdirectories.</p> <hr/> <p>? Matches 0 or 1 character in that position.</p> <p>C:\Program Files\Microsoft Visual Studio 1?.0**</p> <p>Approves any files in the MS Visual Studio version 1 or versions 10-19.</p> <ul style="list-style-type: none"> • Core Prevention The Carbon Black Threat Analysis Unit (TAU) crafts and publishes high-fidelity prevention rules to 3.6+ Windows sensors. These rules protect you from a variety of late-breaking, high-impact attacks without having to change policy configurations. • Set Permission Policy Rules Use permission rules to allow and log behavior, or to have the Carbon Black Cloud bypass a path entirely. Create permissions rules to set up exclusions for other AV/security products or to remove impediments for software developers' workstations. • Setting Antivirus Exclusion Rules You can create antivirus (AV) exclusion rules, including those specific to various endpoint platforms. • Set Blocking and Isolation Policy Rules You can create or edit a blocking and isolation rule to deny or terminate processes and applications. • USB Device Blocking You can control the access to USB storage devices, such as blocking the access to all unapproved USB devices. • Upload Paths

Requirement	Response
	<p>You can deny or allow sensors to send uploads from specific paths.</p> <ul style="list-style-type: none"> • Prevention Rules Capabilities for Linux Sensors <p>The Linux sensor supports essential malware prevention capabilities for supported Linux OS versions.</p> <ul style="list-style-type: none"> • Ransomware Policy Rules <p>The most secure ransomware policy is a default deny posture that prevents all applications, except those that are specifically approved, from performing ransomware-like behavior.</p>
<p>6.1.6. Product Usability</p> <p><i>The Solution shall provide easy to understand, user-friendly interfaces with intuitive designs to facilitate user engagement, and clear documentation and support resources which instruct on use of the Solution.</i></p>	<p>The proposed offering provides users with a simplified intuitive design. More detail is provided in the VMware Carbon Black User Guide.</p> <ul style="list-style-type: none"> • Section 1 Dashboard-pages 20-23 • Section 2 Alerts-pages 24-37 • Section 3: Investigating Events-pages 38-63 • Section 5: Enforce-pages 82-152
<p>6.1.7. Administration and Management Usability</p> <p><i>The Solution shall have an easy-to-use administration console and allow straightforward ongoing management that utilizes a lightweight agent with low impact on potential performance.</i></p>	<p>Carbon Black provides an easy-to-use intuitive console for users to quickly navigate and mitigate risk. Tabs are easily accessible and straightforward. Agent is lightweight and easy to deploy.</p>
<p>6.1.8. Endpoint Detection and Response</p> <p>The Solution shall record system behaviors to detect suspicious events, investigate and block malicious activity, and contain malicious activity at the endpoint. The Solution shall use the data to investigate and provide remediation guidance for any affected systems.</p>	<p>VMware Carbon Black EDR provides continuous and centralized recording of endpoint activity with attack chain visualization and search. The solution looks at TTPs and behavioral IOC to identify and block malicious activity. Additionally, providing a live response function for remote remediation.</p>
<p>6.1.9. Endpoint Protection Platform Suite</p> <p>The Solution shall use an extended portfolio of security tools, like endpoint firewalls, device and</p>	<p>The core Carbon Black Cloud Suite contains endpoint firewall, inventory, signature, vulnerability, and light sandboxing (with support for third party sandbox applications).</p>

Requirement	Response
application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.	Application management and control is best performed by VMware's AppC product line.
<p>6.1.10. Operation System Support</p> <p>The Solution shall protect a wide range of operating systems, including Windows, MacOS and Linux, and mobile operating systems like iOS and Android. The Solution shall provide specific functions for cloud, virtual and container-based workloads.</p>	<p>VMware Carbon Black supports a variety of OS's. Please refer to OS guide.</p> <p>For a complete list of supported operating systems, see the following sensor OERs:</p> <ul style="list-style-type: none"> • Carbon Black Cloud Windows Sensor on Windows Desktop OER • Carbon Black Cloud Windows Sensor on Windows Server OER • Carbon Black Cloud Linux Sensor OER • Carbon Black Cloud macOS Sensor OER
<p>6.1.11. Data Management and Storage</p> <p>The Solution shall provide required data storage capacity, file types, and locations, as well as processes such as disaster recovery, rollbacks, extraction, or eradication.</p>	<p>For the Carbon Black Cloud product, all storage, DR, and data is managed by VMware's Internal Cloud Infrastructure team and is provided as part of the service. These are also audited by a third party.</p>
<p>6.1.12. Performance Management</p> <p><i>6.1.12.1. The Solution shall provide proactive alerts on system events, as well as logging and resolution reporting on all issues.</i></p> <p><i>6.1.12.2. The Solution shall provide the ability to identify unhealthy agents on endpoints and self-heal issues. Any endpoints that cannot be self-healed must be reported through the administration console and reports.</i></p>	<p>6.1.12.1 Alerts can be setup within the Carbon Black system and triggered based on customizable thresholds. VMware also has a cloud monitoring system that can alert if there are general problems with the VMware cloud as a whole.</p> <p>6.1.12.2 The system has an inventory management screen that will depict out-of-date sensors. Future roadmap versions will add in additional self-healing capabilities and other device management features.</p>
<p>6.1.13. Security</p> <p><i>The Solution shall offer configurable controls that extend data and transaction security and compliance to third-party platforms or hosting providers the Solution uses. The Solution shall document security policies, audits, attestations, or evaluations for compliance needs.</i></p>	<p>Carbon Black has two main controls for extending data to third party platforms. VMware's secured API engine allows customer controlled direct API access using the published API Guide. VMware also has a data forwarding engine to export all and/or partial organization data to a customer owned AWS S3 bucket via SSL.</p> <p>Many of the Security and Auditing processes are documented in the VM Trust Center and SOC3/Attestations are available upon request</p>



Requirement	Response
<p>6.1.14. Data Management</p> <p>The Solution shall enable monitoring, reporting, and management of data sharing, as well encryption and security for data at rest and in motion.</p>	<p>with NDA</p> <p>All backend data follows strict SOC3 controls and is audited by an independent third party. These do include the monitoring, management, and encryption of the data in rest and in motion.</p> <p>This third-party audit is provided here in the System and Organization Controls Report SOC 3® included herein as Attachment E.</p> <p>VMware has aligned their Cloud Services Information Security Management System (ISMS) to support the following standards:</p> <p>ISO 27001 - Information Security Management ISO 27017 - Cloud Specific Information Security Guidance ISO 27018 - Cloud Specific standard for protecting Personally Identifiable Information (PII)</p>
<p>6.1.15. Disaster Recovery and Backup</p> <p>The Solution shall enable processes such as disaster recovery, rollbacks, and version control.</p>	<p>VMware as a whole supplies over 30 cloud-based products and adheres to all the industry best practices and certifications. Both ISO Certs and SOC3 (see Attachment E) reports have been audited by a third party to ensure the proper DR, rollbacks, and version control are in place</p>
<p>6.1.16. Identity and Access Management</p> <p>The Solution shall provide capabilities such as user authentication, password policy management, two factor authentication, single sign on, and role-based access.</p>	<p>With Carbon Black Cloud users have access to role-based access and access to permissions. API access and 2FA can also be set up.</p> <p>As an organization owner, user access to the organization and its resources is controlled. When users are invited to the organization, two types of role-based access are assigned:</p> <ul style="list-style-type: none"> • Access to one or more of the cloud services of the organization, such as Carbon Black Cloud. Users are granted access to the service by assigning one or more of the roles provided by the service. • Role-based access to the organization. As an organization owner with full access, or as an organization member with read-only access. <p>Assigning access permissions to groups is more efficient than assigning the same permissions to</p>

Requirement	Response
	<p>individual users one at a time. As an organization owner, the capability of determining the members that make up groups and what roles and permissions they are assigned to is possessed.</p> <ul style="list-style-type: none"> • Setting Up Enterprise Federation with VMware Cloud Services As an enterprise using VMware Cloud services, federations can be set up with multiple corporate domains. By federating corporate domains, the owner can enable single sign-on for users in the enterprise. Enterprise federation with VMware Cloud services is set up through a self-service workflow and supports integration with SAML 2.0 based identity providers. • Managing roles and permissions The organization owner can give VMware Cloud Services users two types of role-based access when invited to join the organization: organization role access and service role access. • Managing Active Users The organization owner can manage user access and determine the service and organization level permissions granted to users and groups. • Working with Groups Assigning roles to groups is more efficient than assigning the same permissions to individual users one at a time. The organization owner can create groups and determine the members that make up those groups and what roles they are assigned. • Setting up API Access The Carbon Black Open API platform can be used to integrate with a variety of security products, including SIEMs, ticket tracking systems, and custom scripts.
6.1.17. Network	VMware develops over 50 different onsite products, 30 different cloud products, and is a

Requirement	Response
<p>The Solution shall leverage network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the Solution.</p>	<p>leader in virtualization; using an extensive amount of both VM products as well as third party solutions to monitor the performance of existing systems.</p>
<p>6.1.18. Compliance and Third-Party Certification</p> <p>The Solution shall comply with relevant standards like General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act, Personally Identifiable Information (PII) DMS-22/23-155 Page 6 of 30 Endpoint Detection and Response Solution data requirements, Driver Privacy Protection Act, and third-party certifications such as Systems and Organizations Controls 2 (SOC 2) and International Organization for Standardization (ISO) 27001. The Department, Purchaser, or Customer may require Contractor(s) to execute security agreements, including but not limited to, CJIS riders or Business Associate Agreements as a condition of performance or purchase order issuance.</p>	<p>VMware gives customers confidence in the capabilities of their products by providing objective information around their capabilities in order to make the most informed decisions.</p> <p>VMware participates in testing to collaborate with the industry at large and share information that ultimately allows for the improvement of products. VMware wants to give customers confidence in the capabilities of their products by providing objective information around the capabilities.</p> <p>VMware participates in a diverse set of public, unbiased tests because it shows commitment to ensuring their products are equipped to handle a wide variety of real-world attack scenarios.</p> <p><i>Test Date: May 2020</i> <u>AV-Comparatives</u></p> <p>AV-Comparatives is an independent organization offering systematic testing for security software. Using one of the largest sample collections worldwide, it creates a real-world environment for truly accurate testing. VMware Carbon Black is a new entrant to AV-Comparatives testing and very proud to have received a 100% on malware, and 99.8% on the real-world protection tests, during the initial testing period (March-April 2020) and scoring better than most of direct competitors.</p> <p><i>Test Date: April 2020</i> <u>MITRE</u></p> <p>VMware Carbon Black is proud to be a two-time participant in the MITRE ATT&CK EDR evaluation. This test is built to exercise how well an EDR tool supplies its operators with the visibility and</p>

Requirement	Response
	<p>features they need to detect threats. Unlike other tests that measure automated prevention, this test reflects how threat hunters operate in the real world, pitting skilled professionals against a common set of threats.</p> <p><i>Test Date: June 2020</i> <u>AV-Test</u></p> <p>Although primarily malware focused, VMware believes participation in AV-Test is important because it provides a well-rounded sample and includes a robust false-positive test that paints a realistic picture of what running AV is like in production. Carbon Black has consistently achieved 100% blocking rate of prevalent malware set and 100% detection rate of all attacks in these tests.</p> <p><i>Test Date: June-July 2018</i> <u>OPSWAT</u></p> <p>The OPSWAT program abides by all industry standards and procedures, making the badge an industry-wide stamp of approval. This certification verifies that endpoint security products are supported by the OESIS Framework and therefore compatible with the many solutions that employ OESIS. It is for these reasons that VMware believes this program is an important one, which they are committed to participating in.</p> <p><i>Test Date: June 2018</i> <u>ICSA Labs</u></p> <p>As a security vendor, it's important to regularly check how products are performing in the market. For this reason, Carbon Black participates in the monthly ICSA Labs Anti-Malware test, where it is evaluated against the most current known malware. Carbon Black has consistently received a 100% prevention rating, validating its detection capabilities.</p>

Requirement	Response
	<p>When evaluating third-party test results, watch out for:</p> <ul style="list-style-type: none"> • Vendors who only participate in sponsored testing, where they control the test. • Vendors who opt out of rigorous prevention tests such as NSS Labs AEP • Vendors who don't adopt diversity in their testing strategy. • Tests that only exercise a limited portion of the attacker techniques across the entire killchain. <p>VMware thinks it is important tests are reflective of the reality of the current threat landscape, so an active role in evolving testing standards and methodologies that improve objectivity and relevance in testing has been taken.</p> <p><u>AMTSO</u></p> <p>Anti-malware testing isn't easy, and it can be biased or easily rigged. AMTSO's charter has been set to address the global need for improvement in the objectivity, quality, and relevance of anti-malware testing methodologies. VMware believes in AMTSO's mission of defining a set of standards that all vendors and testers should adhere to, so there can be truly unbiased, objective independent testing.</p> <p>Please see Attachment E for more information on SOC compliance.</p>
<p>6.1.19. Configuration and Customization</p> <p>The Solution shall allow customization of the standard deployed solution with custom user interfaces, data tables, process components, and business logic.</p>	<p>Carbon Black allows customization to dashboard and configuration changes.</p> <p>Users can select the data to display in the dashboard and add, remove, resize, or rearrange the widgets, keeping only widgets of interest and resizing them on the dashboard.</p> <p>Procedure</p> <ol style="list-style-type: none"> 1. Navigate to the upper right corner of the Dashboard page.

Requirement	Response						
	<p>2. Click the Configure Dashboard icon. The available widgets are displayed at the bottom of the page.</p> <p>3. Click the Add icon on the available widget. The widget appears in the dashboard.</p> <p>4. Locate the blue corner on the bottom-right of the widget and drag the border frame to resize it. This step can be applied to any of the available widgets on the dashboard.</p> <p>5. Optionally, click the trash () icon to delete the widget.</p> <p>6. Click the Save configuration () icon to apply the changes.</p> <p>Users can filter the available data based on a specific period of time, alert severity, by including or excluding group alerts, and dismissed alerts.</p> <p>Procedure</p> <ol style="list-style-type: none"> 1. Navigate to the upper left corner of the Dashboard page. 2. Click the filter icon. 3. Select from any of the following options. <table border="1" data-bbox="922 1150 1323 1808"> <thead> <tr> <th data-bbox="922 1150 1060 1203">Option</th> <th data-bbox="1063 1150 1323 1203">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="922 1207 1060 1724">Time frame bubbles</td> <td data-bbox="1063 1207 1323 1724">By default, All. Set the time frame to view data specifically during that window. Select an existing window or create a custom one. Selecting All displays the last 13 months of data, if available. Note:Filters are not applied on few widgets.</td> </tr> <tr> <td data-bbox="922 1728 1060 1808">Policy type</td> <td data-bbox="1063 1728 1323 1808">By default, All policies. View the</td> </tr> </tbody> </table>	Option	Description	Time frame bubbles	By default, All. Set the time frame to view data specifically during that window. Select an existing window or create a custom one. Selecting All displays the last 13 months of data, if available. Note: Filters are not applied on few widgets.	Policy type	By default, All policies. View the
Option	Description						
Time frame bubbles	By default, All. Set the time frame to view data specifically during that window. Select an existing window or create a custom one. Selecting All displays the last 13 months of data, if available. Note: Filters are not applied on few widgets.						
Policy type	By default, All policies. View the						

Requirement	Response	
	<p>drop-down menu</p>	<p>dashboard data for all policies, your default policy, or just for a required policy. Select the required option from the drop-down menu. You can also type a name of the policy and filter your search results.</p>
	<p>Alert severity</p>	<p>By default, 3. Set the severity score to show only a certain range of values. All alerts with the selected or higher severity score are displayed.</p>
	<p>Group Alerts</p>	<p>By default, Off. Click the Group alerts toggle to view similar alerts collectively or individually. Set the toggle to On or Off.</p>
	<p>Include dismissed alerts</p>	<p>By default, disabled. Alerts that have been previously dismissed.</p>
	<p>Results The data in the widgets updates based on users filtering choices.</p>	
<p>6.1.20. Role-Based Access</p> <p>The Solution shall provide the ability to create customizable role-based personas based on responsibility.</p>	<p>The Carbon Black Cloud console comes with six pre-defined, built-in roles to assign to users.</p> <p>View All Users can view pages, export data, and add notes and tags. Suitable for new users or users in an oversight capacity. Permissions include:</p>	

Requirement	Response
	<ul style="list-style-type: none"> • View dashboard data • Investigate alerts and view analysis • View endpoints, workloads, policies, reputations <p>Analyst 1 Users monitor, investigate, and respond to potential threats. Users can also triage alerts and place devices in or out of quarantine. Permissions include:</p> <ul style="list-style-type: none"> • View and quarantine devices • Analyze and dismiss alerts <p>Analyst 2 Users monitor, investigate, and respond to potential threats. Users can also effect change on endpoints or workloads through Live Response, file deletion, and quarantine. Permissions include all Analyst 1 permissions in addition to:</p> <ul style="list-style-type: none"> • Manage background scans • Delete hashes from endpoints or workloads <p>Analyst 3 Users monitor, investigate, and respond to potential threats. Users can also use Live Response to manage application reputations, and certificates. Users can use all Live Response features including process execution, memory dump, and removal from endpoints or workloads. Permissions include all Analyst 2 permissions in addition to:</p> <ul style="list-style-type: none"> • Live Query access • Live Response access • Approve/Ban applications • Manage trusted certs <p>System Admin Users are responsible for daily admin activities including adding users, managing sensors, and enabling bypass. Users in this role cannot change global settings, delete files, or use Live Response.</p> <p>Super Admin Users have all permissions, including console setup and configuration, Live Response, and policy management, API keys, and sensor group rules.</p>

Requirement	Response
	<p>Kubernetes Security DevOps Users are responsible for configuring Kubernetes security. This includes setting up Kubernetes policies, scopes, and Kubernetes clusters in the Carbon Black Cloud console. Users can monitor the health of the Kubernetes environment, investigate workloads and violations, and take actions accordingly.</p>
<p>6.1.21. Data Export</p> <p>The Solution shall provide the ability to generate a customizable export of data based on user filters for assets, services, and issues present within the platform.</p>	<p>With VMware Carbon Black cloud users have access to reporting to capture reporting for future or offline needs via the dashboard</p> <p>With the Carbon Black Cloud reporting functions, users can generate a report to capture details related to current or predicted resource needs. The report can be downloaded in a PDF or CSV file format for future and offline needs. A full report from is downloaded from the Dashboard page, or a partial report from a single widget.</p> <p>Procedure</p> <ol style="list-style-type: none"> 1. Navigate to the upper right corner of the Dashboard page. 2. Click the Export (↓) icon and select CSV or PDF Report. <ul style="list-style-type: none"> ○ The CSV file is available for download under the Notifications drop-down menu. ○ The PDF file downloads to your device. 3. Optionally, click the Export (↓) icon in a widget of your choice to export any individual data set. <p>The CSV file downloads to your device.</p>
<p>6.1.22. Integration</p> <p><i>6.1.22.1. The Solution shall integrate with the Department's existing security tools such as firewalls, antivirus software, endpoint management solutions and security information and event management (SIEM) systems. The</i></p>	<p>VMware Carbon Black extends rich analytics and response actions to the rest of the security stack through integrations and open API's.</p> <p>VMware Carbon Black Integration Network Through 140+ ecosystem partnerships and integrations, Carbon Black is able to fit into and</p>

Requirement	Response
<p><i>Customer shall determine if the Solution is able to integrate with the Customer's security tools. The Contractor shall take any steps necessary to support Customer integration.</i></p> <p><i>6.1.22.2. The Solution shall be capable of data integration through common exchange techniques and frameworks such as RESTful Application Programming Interfaces (APIs).</i></p> <p><i>6.1.22.3. The Solution shall be capable of integrating with a variety of identity and access management (IAM) systems to meet Customer current and future needs.</i></p> <p><i>6.1.22.4. Initial Integration shall include connecting each Customer to the state Cybersecurity Operations Center (CSOC) and validating with FL[DS] that all Solution data is properly integrated, as requested by the Customer.</i></p> <p><i>6.1.22.5. Integration Maintenance may be required after initial integration to ensure that the Solution properly exchanges data between Customers and the CSOC. The Contractor shall address any concerns that FL[DS] has regarding integration issues.</i></p>	<p>enrich current security and IT workflows.</p> <p><u>Enhance Workflows</u> Fits into and enhances existing workflows across security and IT tools.</p> <p><u>Increase Visibility</u> Extends visibility and remediation across endpoints, networks, workloads, and containers.</p> <p><u>Amplify Investments</u> Get more value out of Carbon Black and other security and IT investments through extended visibility and automation.</p> <p>Next-Gen SOC Alliance In partnership with the industry's leading SIEM/SOAR players, VMware is setting a strong vision for the modern SOC and delivering unprecedented visibility and remediation capabilities across endpoints, networks, workloads, and containers.</p> <p> exabeam</p> <p> splunk</p> <p> IBM</p> <p> sumo logic</p> <p> Chronicle</p> <p> Secureworks</p> <p>Open APIs Open APIs for the Carbon Black Cloud platform unlock opportunities for integration and enrichment across different security and IT workflows. Using developer tools, such as the</p>

Requirement	Response
	Carbon Black Cloud Event Forwarder, users can customize integrations and build connections that streamline security & IT workflows.
<p>6.1.23. Performance and Availability</p> <p>The Solution shall perform in accordance with the approved Service Level Agreement (SLA) (see Section 10.2) and be available 99.999% of the time per month.</p> <p>6.1.23.1. The performance and availability SLA shall provide information on performance and availability objectives for the Solution to perform. successfully and be available 99.999% of the time per month.</p> <p>6.1.23.2. The vendor shall propose meaningful financial consequences in the draft performance and availability SLA submitted with their Quote, which will be incorporated in the FL[DS]-approved financial consequences</p>	Please see Attachment A – Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDRTM Service Offerings.

to include the following at a minimum:

a. A draft SLA for Solution performance and availability which adheres to all provisions of this RFQ.

Mainline Response: Please see Attachment A – Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDRTM Service Offerings.

b. A draft SLA for training and support which adheres to all provisions of this RFQ.

i. The training SLA must specify initial training (included in Item No. 1 on Attachment A, Price Sheet) provided and ongoing training provided (included in Item No. 2 on Attachment A, Price Sheet).

Mainline Response: Please see Attachment B – VMware Production Support for Cloud Products.

SLAs related to implementation / training as SLAs are not applicable to the proposed offering. Training credits expire within one year of purchase. Customers have access to use these on any online course, and availability is based upon dates with certain courses even offering on-demand.- [VMware Learning](#). Training credits are quoted on a rate per single credit. Nine (9) credits are required for the following courses for a single individual: Carbon Black Control Administrator Training, Carbon Black Advanced Administrator Training, Carbon Black EDR Advanced Administrator Training, Carbon Black EDR Advanced Analyst Training, Carbon Black Cloud Endpoint Standard Training, Carbon Black Cloud Audit and Remediation, Carbon Black Cloud Enterprise EDR. 17 credits are required for Carbon Black Cloud: Plan and

Deploy Training. 19 credits are required for Carbon Black Cloud: Advanced Operations and Troubleshooting

Implementation SKUs expire within one year of purchase. Customers have access to engage with a PM immediately upon purchase.

Additional information is provided as Attachment G – VMware Carbon Black EDR Administrator.

c. A draft implementation plan for a Customer which adheres to all provisions of this RFQ.

Mainline Response: Please see Attachment C – VMware Carbon Black Cloud Deployment.

d. A draft MDR SLA, if applicable, per section 6.6.1 with annual pricing.

Mainline Response: The Carbon Black Cloud Managed Detection and Response team analyzes Carbon Black analytics alerts from the Carbon Black Cloud Endpoint Standard product of severity level 5 alerts and higher. Severity level 8 alerts or higher have an SLO of two hours. Severity level 5-7 alerts are best effort.

Users receive notifications through email for alerts, typically due to potential threats. For any actionable alert, an analyst sends an email to the identified points of contact within the user's organization. In cases of major incidents, the CSM and sales team are also notified to ensure timely communication about the incident.

If Carbon Black Cloud Managed Detection and Response cannot reach users by email, the Carbon Black Cloud Managed Detection and Response team reaches out to the CSM and sales team.

For Carbon Black Cloud Managed Detection and Response, emails contain a two-way communication feature between the user's organization and the Carbon Black Cloud Managed Detection and Response team. Users can respond to the initial alert email to begin two-way communication.

Carbon Black Cloud Managed Detection and Response emails include IOCs, such as registry edits, hashes, IP addresses, and root causes if they are known. Emails also include initial remediation action and applicable policy recommendations. These are:

- True positives alerts.
- Better policy tuning.
- Alert response notifications by email.
- For Carbon Black Cloud Managed Detection and Response customers:
 - The action taken by analysts.
 - The team can potentially provide advice on the overall network environment. However, analysts do not have access to additional networking tools.

What is considered an actionable alert?

An actionable alert is an alert users can act on. Typically, actionable alerts are likely threats to the user's environment. Carbon Black Cloud Managed Detection and Response provides recommendations and instructions for deleting malicious, suspicious, or unwanted files from the user's device.

Can I directly contact the Carbon Black Cloud Managed Detection and Response team?

The only direct contact available between a Carbon Black Cloud Managed Detection and Response customer and the Carbon Black Cloud Managed Detection and Response team is through a two-way communication initiated by an incident email. Responses sent in daily summaries are not received by the team. If the customer does not have the Carbon Black Cloud Managed Detection and Response product, no direct communication is available.

To contact the team outside of an active incident investigation, contact the CSM. CSMs can then reach out to the Carbon Black Cloud Managed Detection and Response team for answers to questions.

Please note, the MDR operates on an SLO as opposed to an SLA.

e. A draft SLA for future integrations, if applicable, per section 6.6.2 with pricing.

Mainline Response: Pricing for future integrations is unknown and will not be determined until those integrations are made available for sale.

f. A draft disaster recovery plan per section 32.5.

Mainline Response: Please see Attachment D – Carbon Black Cloud Global Resiliency.

Past Performance

2) Documentation describing any experience providing the Solution, or similar Solution, on a statewide basis or across a large geographic region.

3) Documentation describing the vendor's capacity and ability to implement the Solution on a statewide basis.

Mainline Response: Information detailing successful implementations of the Carbon Black solution within the state of Florida is included on the following 12 pages.



Creating a Future-Ready Security Operations Center

Whether they have a formal security operations center (SOC) or a small team of one or two cybersecurity personnel, states and local governments and education institutions face a changing world when it comes to monitoring for, identifying and responding to today's threats. An explosion of new devices and endpoints; the expansion of organizational boundaries; and a nonstop volley of phishing, ransomware and other attacks have put enormous pressures on security analysts. Traditional tools such as signature-based detection are not sufficient for detecting today's threats, and analysts' jobs overwhelmingly focus on managing low-fidelity alerts rather than proactive, coordinated threat hunting.

Given the severity and impact of today's attacks, security operations teams need to identify suspicious behavior as far in advance of an actual attack as possible. If an attack does occur, they need to detect and stop it within minutes or seconds.

The Infrastructure Investment and Jobs Act (IIJA) provides an important opportunity for organizations to invest in technology such as advanced endpoint detection and response (EDR) to modernize security operations. Advanced EDR solutions help organizations modernize security operations, reduce risks and alleviate pressure on staff by enabling analysts to

proactively detect, investigate and respond to true threats earlier in the threat cycle and more easily support audit and compliance efforts. Senior security managers can keep their business safe while helping their team do more with less, and CISOs and other leaders can meet goals for improving threat intelligence capabilities and the organization's security posture.

➤ New Drivers Put Focus on the Function of the SOC

Several trends are driving the need to enhance threat hunting capabilities and modernize security operations. Many of these have recently been cited as top concerns by the National Association of State CIOs.

Expanding attack surface. The attack surface continues to spread beyond traditional network perimeters as remote work, cloud environments, software-as-a-service (SaaS), mobile devices, Internet of Things (IoT) sensors and other endpoints proliferate. Security analysts are using multiple, siloed tools to monitor endpoints, applications and the cloud, which complicates their jobs and increases response times and risk.

What is Advanced EDR?

Advanced endpoint detection and response (EDR) systems offer a critical first line of defense against outside threats. A comprehensive EDR solution:

- **Provides visibility into the full security stack and records every system event** (even if an endpoint is offline). Analysts can identify, detect, protect and respond to and recover from threats via one integrated platform.
- **Helps detect known and unknown threats.** Unlike static, signature-based threat detection tools that rely on known information, advanced EDR uses artificial intelligence and machine learning to identify anomalous behavior and other threats that outdated detection approaches miss.
- **Provides real-time intelligence and context.** An advanced EDR solution draws on a vast data lake of human intelligence and threat telemetry from internal systems and trusted third parties. Analysts use this consolidated threat intelligence to obtain more comprehensive insights and detect, analyze and verify threats more quickly and accurately.
- **Enables rapid remediation and reduces attack dwell time.** Faster time to detection and intelligent automation allow security professionals to respond to and remediate attacks within minutes. Personnel can safely contain ongoing attacks and then access affected endpoints to execute response and remediation tasks — all from a single platform.

Advanced, targeted attacks. Attackers are using sophisticated tactics to evade defenses, conduct reconnaissance and attack targets. Lateral movement — where attackers breach a system and then leverage internal resources to further penetrate networks and distribute attacks — is an increasingly common tactic, appearing in more than 25% of attacks reported by respondents in one recent survey.² In the same survey, zero-day exploits were reported by 62% of respondents, and nearly 60% of respondents had experienced a ransomware attack. The September 2022 Los Angeles Unified School District ransomware attack, in which cybercriminals accessed data, compromised critical systems and then demanded ransom, is one of many school-focused ransomware attacks making headlines.³

Stringent cyber insurance requirements. Cyber insurance rates are soaring, as insurers move to address rising losses associated with ransomware and other attacks. For example, Horry County, South Carolina, saw its premium triple from one year to the next.⁴ In 2021, one major insurer announced that it had increased its cybersecurity insurance rates globally by 40%.⁵ Requirements to qualify for cyber insurance are also more stringent, with many insurers requiring full implementation of robust controls such as multifactor authentication, endpoint detection and response for all endpoints, data backups and more.

Low-fidelity alerts. Security operations analysts spend the majority of their day opening and closing tickets for low-fidelity alerts. More than 70% of analysts investigate more than 10 alerts per day,⁶ which leaves little time for proactive threat hunting and contributes to high job dissatisfaction among security analysts.

Talent gaps/high turnover. Attracting and retaining cybersecurity professionals is often thwarted by stress and job dissatisfaction. In a recent survey of cybersecurity and incident response professionals, 47% of respondents said they experienced burnout or extreme stress in the past 12 months, and 69% of respondents reporting these symptoms said they've considered leaving their job as a result.⁷

Insufficient cybersecurity funding. Despite forthcoming funding from the IIJA, states and local governments as well as K-12 districts and higher education institutions chronically struggle with paying for cybersecurity. In a survey of state educational technology directors and other education professionals, for instance, only 6% of respondents indicated their state provides ample cybersecurity funding.⁸

Enhancing security operations

Forward-looking governments and education institutions are modernizing their cybersecurity strategy to efficiently and proactively detect and respond to threats in their increasingly complex environments. Visibility and context, along with automated processes, are essential components of their modern cybersecurity strategy.

Given the uptick in zero-day exploits and the impact of today's ransomware and other attacks, organizations

Capabilities to look for in an advanced EDR solution

The following features should be part of any advanced EDR solution:

- **Easy integration across the full security stack.** To provide comprehensive visibility and intelligence, the EDR platform should easily integrate with endpoints, containers, workloads, virtual desktop infrastructure (VDI) and modern application development tools as well as critical security systems across the organization's network, including firewalls, security information and event management (SIEM) solutions, cloud-based security tools and other network security technology.
- **Ease of use.** To ensure everyone has the intelligence they need, the platform should be easy for all levels to use, including lower-tier analysts and new team members.
- **Minimal false positives.** An advanced EDR solution allows analysts to find real threats without having to sift through a lot of "noise." Look for vendor metrics that demonstrate a low rate of false positives.
- **Federal Risk and Authorization Management Program (FedRAMP) High Authorization.** This designation means that the Department of Defense (DoD), Department of Homeland Security (DHS) and General Services Administration (GSA) have vetted the EDR solution for adherence to the highest security and compliance standards and cleared it for use on a government-wide scale.

cannot risk waiting for an attack to happen. To detect, protect and respond immediately and appropriately to cyber threats, organizations need complete, accurate data.

A modern security strategy requires in-depth visibility and context across every user, application, device, endpoint and workload. Organizations must be able to detect anomalies and proactively hunt for threats far out on the horizon, as well as inspect and correlate network traffic in real time — both as it moves in and out of the network and as it moves laterally throughout the network — to stop attacks before they do damage. In addition, security professionals must be able to draw on and consolidate internal and publicly available threat intelligence to maintain a comprehensive, up-to-date understanding of the threat environment. With full visibility and context, analysts can then make well-informed decisions about what they see.

Automation also plays a crucial role. With the volume of threats today and an ongoing shortage of analysts, it's practically impossible to rely on human intervention and manual processes to detect, analyze and respond to alerts. Automating specific processes within the organization's incident response playbook — for example, emergency patching or traffic filtering

— frees up analysts' time for higher order tasks and alleviates the stress and errors associated with time-consuming, repetitive manual processes.

An advanced EDR solution enables comprehensive visibility and automates core incident response functions to help organizations efficiently and proactively detect and respond to zero-day and other threats — often before an incident occurs. It continually monitors, records and stores network and endpoint activity data so analysts can analyze, investigate and hunt threats in real time, visualize the entire attack structure (e.g., point of breach, lateral movement, installation of malicious code, and exfiltration or destruction of data) and respond efficiently and authoritatively.

Ensuring success and sustainability

The following best practices help ensure security operations modernization is successful and sustainable.

Define desired outcomes. Clarify and document desired outcomes. Then identify the tools, processes and talent needed to achieve those outcomes.









Invest in your analysts. Ensure analysts obtain the necessary training for certification and proficiency in the tools they use. Make sure they can understand the intelligence they receive and have procedures and playbooks in place to respond appropriately.

Manage talent to reduce burnout. Develop a deep bench so people can be rotated to give them a break from highly stressful tasks. Offer flexible hours, coaching, therapy and continued education to keep employees in their desired job and targeted career path.

Continually test controls. Have red (attacker role), blue (defender role) and purple (both roles together) teams test specific use cases — ransomware, for example — against controls.

Cultivate a security mindset enterprisewide. Educate the overall organization on the impact of cloud and hybrid operations on security operations and the security operations team. Reinforce the fact that cybersecurity is everyone's job and build in processes to reduce organizational silos.

See More, Stop More

Use Case	Enhance Security Operations	Advanced EDR Solution
 Users	Identity & access management	<ul style="list-style-type: none"> ✓ User risk scoring/access control policies/identity federation
 Endpoints /devices	Endpoint & server protection	<ul style="list-style-type: none"> ✓ Access the complete activity record of every endpoint ✓ Isolate infected systems & remove malicious files
 Network	Network protection	<ul style="list-style-type: none"> ✓ Lateral security, service mesh, SASE, vulnerability management
 Infrastructure	Multicloud	<ul style="list-style-type: none"> ✓ Real-time identification & mitigation ✓ Cross-cloud remediation at scale ✓ Workload protection
 Application	Application security	<ul style="list-style-type: none"> ✓ Kubernetes security, posture management ✓ API security, application control ✓ Vulnerability management
 Data	Data security	<ul style="list-style-type: none"> ✓ Threat hunting ✓ Audit & remediation ✓ Ransomware prevention & recovery
 Visibility & analytics	Advanced correlation/global monitoring & detection	<ul style="list-style-type: none"> ✓ Advanced detection & monitoring of threats ✓ End-to-end attack visibility
 Automation & orchestration	Automation, orchestration & response	<ul style="list-style-type: none"> ✓ Consolidate threat intelligence to automatically detect suspicious behavior ✓ Automatically collect & store detailed forensic data for investigation

Work with a trusted provider. Given the complexity of creating and maintaining a high-performing security operations center, many organizations rely on private sector partners to provide SOC functions. In particular, small and midsized organizations with fewer available resources may find it useful to partner with providers for Managed Detection and Response (MDR) services or even embrace a full Managed Security Service Provider (MSSP) model. Talk to your peers in other jurisdictions about their experience with outsourcing SOC functions, and make sure your contract terms include appropriate metrics on functionality and performance.

Ask the right questions. When considering SOC modernization, security leaders may want to ask these questions:

- ✓ What gaps do we have in our ability to identify risk and resolve threats?
- ✓ How do we learn about new attacks?
- ✓ How are we reducing operational overhead when mitigating risks?

Conclusion

The stakes are mounting. As state and local governments and education institutions move more critical data and operations online, cybercriminals continue to innovate new ways of circumventing defenses. To maintain resilience and reduce exposure in their increasingly complex digital environments, security leaders must act swiftly to enhance security operations. An advanced endpoint detection and response (EDR) solution empowers security professionals to do their job effectively and efficiently by providing the tools, processes and automation to see more and stop more — and to catch threats earlier, before they can do harm.

This piece was written and produced by the Government Technology Content Studio, with information and input from VMware Carbon Black.

Endnotes:

1. <https://www.nascio.org/resource-center/resources/2022-cyber-study/>
2. VMware. Global Incident Response Threat Report. 2022.
3. <https://abc7.com/lausd-ransom-cyberattack-los-angeles-unified-school-district/12246624/>
4. <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/07/27/cyber-insurance-price-hike-hits-local-governments-hard>
5. <https://www.reuters.com/article/aig-results-cyber-idCNL1N2PD1AJ>
6. Center for Digital Government interview with Fawaz Rasheed, Field CISO, VMware. September 2022.
7. VMware. Global Incident Response Threat Report. 2022.
8. <https://www.setda.org/priorities/state-trends/>
9. <https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local>

Produced by:  CENTER FOR
DIGITAL
GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com.

Optimizing Available Funding

State and local government and education organizations have a tremendous opportunity to secure funding for EDR solutions. For example, the IIJA provides \$1 billion over four years to the State and Local Cybersecurity Grant Program.⁹

“There is a lot to think about when it comes to enhancing security operations,” says Patrick Loughlin, U.S. SLED director in the Security Business Unit of VMware Carbon Black. “With Carbon Black, we factor in fulfilling cyber insurance requirements; enabling comprehensive telemetry by pulling metadata from both workloads and endpoints; and aligning with the industry’s best MSSPs, incident response firms and security partners. This has been a formula for achieving customer success with both government and education entities.”

Additional best practices to keep in mind include:

- **Create a formal cybersecurity plan** to protect against, detect, respond to and recover from threats
- **Implement an advanced endpoint detection and response solution** to manage and mitigate threats
- **Improve resiliency** through disaster recovery-as-a-service (DRaaS), which ensures data availability and rapid recovery in the event of attacks
- **Modernize legacy apps and move to the cloud** to reduce technical debt, improve security and accelerate delivery of constituent services
- **Establish digital equity** by leveraging cloud technologies and private 5G technology to provide internet access to underserved communities

Sponsored by: 

VMware gives government agencies the smartest path to the cloud, edge, and app modernization, in order to deliver citizen services and meet mission demands. With VMware’s Cross-Cloud services, you can control all apps and clouds through one management platform, where you can set unified security policies and quickly develop and deploy apps without refactoring. For more information visit: <https://www.vmware.com/products/carbon-black-cloud-endpoint.html>.



Build custom workflows
to fit with the security stack



Minimal effort required
so you can focus on
what matters



Seamless deployment
in just days

City of Venice, Florida Works with VMware to Secure Their Digital Environment

The City of Venice IT department's goal is to empower a transparent and agile digital government. Florida has been a prominent target of ransomware attacks during the 2020 pandemic, and the city's IT department has continued to strengthen their security stack to stay on top of events in their digital environment. Fortunately, for a small IT team with multiple duties and responsibilities, the VMware Carbon Black Cloud™ platform has provided them with the ability to customize the platform to their specific workflows, giving the team peace of mind.

Challenges to unifying security

The City of Venice has roughly 350 employees and an IT department of six that serves many departments in the city, including public safety. As with many small teams, IT director Christophe St. Luce and his employees must wear multiple hats. The group covers frontline support calls, acquisition of new laptops, management of the network and server infrastructure, and more.

Previously, IT for the City of Venice was haphazard. Different departments purchased their own tools and software, creating little to no cohesion. St. Luce faced the challenge of consolidating all the needs of the departments, and finding an endpoint security solution that would satisfy the needs of multiple stakeholders and keep the organization secure. Before partnering with VMware, the City of Venice chose Malwarebytes for their endpoint



Venice is a city on Florida's Gulf Coast with roughly 24,000 full-time residents and approximately 5,000 visitors each year. Their government office has about 350 employees covering all departments within the city, including public safety.

INDUSTRY

Government/Public Sector

HEADQUARTERS

Venice, Florida

VMWARE FOOTPRINT

VMware Carbon Black Cloud
Endpoint™ Standard



protection. However, the city uses high-end laptops for various systems, and Malwarebytes was slowing them down. With a slower environment, the City of Venice lacked agility when preventing advanced attacks.

St. Luce and his team knew they needed a security solution that could solve their evolving challenges, was easier to use, and required less overhead. After a demo of VMware Carbon Black Cloud Endpoint Standard, the choice was clear for St. Luce and his team: Partner with VMware.

“VMware Carbon Black Cloud Endpoint Standard is a different tier of system than I’ve seen demos of before,” explains St. Luce. “The single cloud platform was powerful, yet intuitive to deploy.”

With full support from finance, the IT department moved forward with VMware Carbon Black Cloud Endpoint Standard.

Customized to their workflows

Implementation of their VMware Carbon Black Cloud solution was completed in just three and a half days by St. Luce himself. With a lot of infrastructure at the City of Venice, St. Luce utilized the Microsoft System Center Configuration Manager (SCCM) platform for the smooth transition over from Malwarebytes. VMware Carbon Black Cloud was automatically rolled out to all the company’s servers, domain controllers, and desktop computers.

Since deploying the product, St. Luce has been “very pleased at how minimally invasive [VMware Carbon Black Cloud] is, yet intuitive, and how quickly it can stop potential threats.” Like with any type of agent, there is minor tweaking that St. Luce will occasionally have to perform, but “it’s been a very quiet platform that sits in the background,” says St. Luce. He can check the console every so often on his own time and verify if updates are needed. “I haven’t had to make any adjustments to it in probably the last two and a half months,” says St. Luce. “It’s been working fantastically ever since.”

With a dynamic console, the city can use VMware Carbon Black Cloud to see everything they need to know immediately. Increased visibility means greater insight into identifying the root cause of an attack, seeing where it came from, who was affected, and where it could spread.

Securing a distributed workforce

The City of Venice had deployed VMware Carbon Black Cloud at the beginning of 2020. By the time they started using the product in their environment, the government office had about 50 out of their 350 employees working from home. St. Luce’s main concern was making sure the organization’s endpoints would be protected when they were on and off the City of Venice’s network. When the pandemic brought on a shift to an entirely remote workforce, St. Luce was prepared and confident that his users would be protected on their own networks. With a strong confidence in their systems in place, the city has been able to boost overall productivity.

It’s important that each department within the City of Venice understands the value the IT organization brings and how they are keeping everyone safe. Previously, St. Luce did a speaking tour within the government’s departments and explained what ransomware and malicious actors do, and why his team does what they do. He educated each team about threats in the cybersecurity world and assured them that the City of Venice is always on the offense, but they have a good defense as well. With VMware Carbon Black Cloud, the IT team is confident they have the right solution to prevent advanced attacks while remaining agile.

“I’m very pleased at how minimally invasive [VMware Carbon Black Cloud] is, yet intuitive, and how quickly it can stop potential threats.”

CHRISTOPHE ST. LUCE
IT DIRECTOR, CITY OF VENICE

Looking ahead

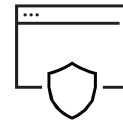
The partnership between VMware and the City of Venice has delivered immeasurable value, according to St. Luce. VMware Carbon Black Cloud has helped St. Luce keep systems in check with little to no threats warranting concern to their environment. The insight into their network and the ease of use for a small team has helped them deliver on their goal of empowering a transparent and agile digital government. With the VMware partnership in place, they look forward to continuing to secure the City of Venice’s digital environment. “I am very happy with [VMware Carbon Black Cloud] and hope to keep it for many years,” St. Luce says.



Complies with national law enforcement regulations to secure data and applications



Reduces load on IT staff by centrally managing hundreds of devices in the field



Improves deputies' access to information while protecting law enforcement data with intrinsic security

Osceola County Sheriff's Office Enhances Responsiveness and Public Safety with VMware



OSCEOLA COUNTY SHERIFF'S OFFICE
SHERIFF RUSS GIBSON

Modern law enforcement involves more technology than ever, from body cameras to rugged mobile data computers used by officers in the field. Osceola County Sheriff's Office actively incorporates cutting-edge technology to help deputies perform their duties quickly, safely and efficiently.

As the number of technologies and connected devices used by the sheriff's office grows, security becomes more complicated. The agency now complies with rigid security standards by using VMware solutions to deliver intrinsic security and modernize its data center infrastructure.

Meeting FBI security standards

Osceola County Sheriff's Office must comply with many technology standards, including Florida Department of Law Enforcement (FDLE) and FBI Criminal Justice Information Services (CJIS) standards. The office prioritized several initiatives to comply with standards, including improving micro-segmentation for virtualized applications. With that goal in mind, the office's IT team worked with SPJ Solutions, a VMware Partner, on a CJIS security compliance initiative and evaluation of solutions that could help the sheriff's office meet micro-segmentation requirements while supporting growing technology needs.

"VMware is a leader in micro-segmentation, so it made sense to look at VMware NSX Data Center as the way forward to comply with standards," says Daniel Caban, director of information technology at Osceola County Sheriff's Office. "Beyond micro-segmentation, VMware does so much for security, virtualization and endpoint management that it seemed like a smart move to switch to VMware."

Osceola County Sheriff's Office serves the 360,000 residents of Osceola County, Florida. Its 500 officers and 300 civilian support staff work with the community to provide a safe and secure environment to live, work and visit.

ABOUT SPJ SOLUTIONS

SPJ Solutions, a VMware Partner, specializes in the design, deployment, support and training of software-defined network and data center technologies. SPJ Solutions is the creator of *clTopus*, a VMware NSX automation and management tool.

INDUSTRY

Public Sector

HEADQUARTERS

Kissimmee, Florida

VMWARE FOOTPRINT

VMware NSX® Data Center
VMware Carbon Black Cloud™
VMware Workspace ONE®
VMware vSphere®
VMware vRealize® Operations™
VMware vRealize Network Insight™
VMware vRealize Log Insight™
VMware vCenter® Converter™
VMware Professional Services



Fast migration to a more secure environment

Osceola County Sheriff's Office decided to deploy NSX Data Center for its micro-segmentation capabilities in addition to its software-defined firewall functionality. The agency also migrated its virtual machines to VMware vSphere as part of the NSX deployment for greater security and performance, with VMware vRealize Operations for performance and capacity optimization as well as monitoring and management of the new environment. VMware vCenter Converter helped ease the transition by quickly converting and migrating existing virtual machines.

"My staff was impressed by how easy it was to migrate to vSphere using vCenter Converter," says Caban. "We had little to no downtime during the migration."

To make the transition to VMware as seamless as possible, the sheriff's office enlisted the help of VMware Professional Services to work together with SPJ Solutions and internal staff for the deployment of NSX Data Center. SPJ Solutions tested different environment scenarios with ciTopus, its NSX automation and management tool. ciTopus, a visual network topology design tool, helps automate deployments and management of NSX environments.

The team also leveraged the network visibility capabilities of VMware vRealize Network Insight, which played an important role during the deployment of NSX Data Center by helping the team better see traffic and understand communication between virtual servers.

VMware Carbon Black Cloud adds another layer to the intrinsic security strategy. In recent years, local governments have seen an increase in ransomware and other sophisticated cyberattacks. VMware Carbon Black helps keep Osceola County Sheriff's Office ahead of malicious actors by providing end-to-end cybersecurity protection for law enforcement data.

"We feel VMware Carbon Black and its machine learning capabilities help fortify the security posture of the sheriff's office. The ease of use of VMware Carbon Black® Cloud Managed Detection™ takes a significant burden off my staff to ensure each endpoint and service is secured. Having the ability to know the exact process a threat takes to compromise a device enables my staff to analyze and take future actions so a threat cannot happen again," says Caban.

Osceola County Sheriff's Office also took advantage of the powerful vSphere environment to upgrade from VMware AirWatch® to VMware Workspace ONE. While AirWatch was only deployed on mobile devices, Workspace ONE—an industry leader in unified endpoint management—delivers digital workspaces across 500 laptops, 800 desktops and 550 mobile devices.

VMware Professional Services also conducted NSX Data Center, vSphere and Workspace ONE training with the team to bring all employees up to date and ease the transition.

"The response to VMware from our IT staff has been excellent," says Caban. "Compared to the previous environment, they're finding that VMware has more powerful capabilities and is much easier to use."

Achieving compliance with ease

Working with the VMware environment has transformed network performance and security for the sheriff's office. The agency now meets all micro-segmentation requirements by separating criminal justice data from data not covered by CJIS standards. The solution also provides eye-opening insights into traffic moving through the network, which allows IT staff to create appropriate port rules and better lock down traffic.

"One of the biggest benefits of adopting VMware is how all of the solutions integrate together so seamlessly. With just a click of a button, solutions start working together to give us the compliance and performance we need."

DANIEL CABAN
DIRECTOR OF INFORMATION TECHNOLOGY,
OSCEOLA COUNTY SHERIFF'S OFFICE

CJIS suggested that the sheriff's office implement a log management system to capture events and maintain those logs for a year. The IT staff discovered that while there are many logging solutions on the market, it was often costly to maintain logs for 12 months. VMware vRealize Log Insight balances log maintenance with cost efficiency to comply with the CJIS recommendation.

The sheriff's office gains the benefit of intrinsic security across the solution, including the strong end-to-end security controls of Workspace ONE that verify device compliance and deploy conditional access controls before seamlessly connecting to the data center via NSX Data Center. "One of the biggest benefits of adopting VMware is how all of the solutions integrate together so seamlessly," says Caban. "With just a click of a button, solutions start working together to give us the compliance and performance we need."



Standardizing on Workspace ONE improves productivity for IT staff by simplifying deploying applications, delivering updates and onboarding new employees. Employees simply log on to a device, and their digital workspace is loaded automatically. The staff no longer needs to spend time installing, configuring and updating individual computers.

"We have hundreds of deputies working in the field. Workspace ONE greatly streamlines managing remote devices and provides officers with an outstanding experience," says Caban. "If a device is lost or damaged in the field, Workspace ONE also makes it easy to wipe the device remotely and protect sensitive law enforcement information."

Looking ahead

The sheriff's office continues to look at other ways to improve the digital environment by implementing VMware solutions. The VMware Horizon® virtual desktop solution may be a good solution for a situation such as the 911 center, where each device may serve multiple users.

"Our IT staff is extremely happy with our experiences with VMware," says Caban. "VMware offers advanced technology and a strong solution portfolio that will support us as we grow and evolve our technology stack."



Learn how @OsceolaSheriff uses #VMware to comply with law enforcement standards and support deputies in the field.



Polk County Schools Protects Data Centers with VMware Carbon Black Cloud Workload

Polk County School District is the seventh largest district in Florida, covering more than 106,000 students and 14,000 employees. For every school and program within the district, the students always come first.

Industry

Education

Strategic priorities

- Gained authoritative context and scaled response in less than two weeks
- Reduced time spent remediating by hours
- Increased visibility across servers

VMware footprint

- VMware Carbon Black Cloud Workload™ Advanced
- VMware vSphere®

With their motto of “Students First,” the Polk County School District’s (PCSD) mission is to provide a high-quality education for all students. For their IT team, providing that high-quality education means ensuring students’ data privacy and protection while avoiding any disruptions to the learning process. Ranking as the seventh largest district in Florida, Polk County covers more than 130 schools with 106,000 students and 14,000 faculty/staff. Acknowledging the continually growing threat landscape, Polk County called on VMware Carbon Black Cloud Workload to secure their data centers and give them the visibility they need to prevent unwanted threats in their environment.

The looming threat of ransomware

At the height of the pandemic in 2020, PCSD was approached by vendors expressing concern over the multitude of school districts being hit with ransomware. When businesses around them started to get hit, Polk County began focusing on what they could do to prevent ransomware. The district had recently upgraded their infrastructure, and there was a strong emphasis on security and how it should be prioritized. The majority of their security existed at the firewall and with traditional measures; they had limited resources in place to protect the workloads in their data centers. Like most school districts, Polk County was in need of a solution that provided industry-standard data center protection and was also easy to implement, maintain and absorbable by existing staff, regardless of size.



Simplified workload protection

Through working with VMware for more than a decade using VMware vSphere, VMware vRealize® Operations™, and VMware vCenter®, Polk County knew their first call would be to VMware. The VMware team has always been very responsive to any issues that arise for Senior Manager of Network Operations Mike Chiavuzzi and his team. Armed with the familiarity of their environment and technology stack, the VMware team presented a demo of how Carbon Black Cloud Workload can easily and quickly isolate a server all from within their current vSphere Client™ console. Chiavuzzi appreciated the simple user interface and capabilities that would help make their jobs easier and more efficient.

Workload security bridges the gap between IT admins and security operations. In the case of Polk County, workload security helps teams that wear various hats manage both responsibilities of IT and security. As a customer of vSphere, Polk County was able to turn on their security with just a click of a button in the same vSphere console they use every day. Tightly integrated with vSphere, Carbon Black Cloud Workload provides a seamless lifecycle management experience that alleviates installation and management overhead. By having osquery and vulnerability assessment within a single console, the team can focus on simplifying their approach to assess their server environment and maintain their overall IT hygiene.

“It’s a good value for what you’re providing,” said Chiavuzzi. “With VMware and Carbon Black married up, it had to be good. It was a pretty easy decision.”

After embracing VMware more than 10 years ago, Polk County is now a complete VMware shop for their data center.

A speedy deployment with the help of VMware Professional Services

In assessing their deployment, Polk County took advantage of the Quick Start Deployment services with the VMware Professional Services team.

“I just can’t say enough about the ease of getting [Carbon Black Cloud Workload] set up. It’s a pretty good turnaround for what you get out of it,” says Chiavuzzi.

From onboarding, integration and testing through training Polk County’s IT team, the VMware Professional Services team ensured everything stayed on track. Network Administrator Terry Arnold was able to get the product stood up and running within a week and a half on the elected servers. From there, it took two weeks for Carbon Black Cloud Workload to scan all their servers running under a standard policy. By testing a few pilot use cases with Professional Services, Arnold was able to determine the best policies to keep their servers secure. Having that link to Professional Services also meant Arnold had weekly meetings with the VMware team to walk through troubleshooting and drill down into what was really going on in their environment.

“We know we’re catching things, we can see it, and we can monitor [what is happening] so [VMware Carbon Black Cloud Workload] gives us another layer of comfort and security that we never had before.”

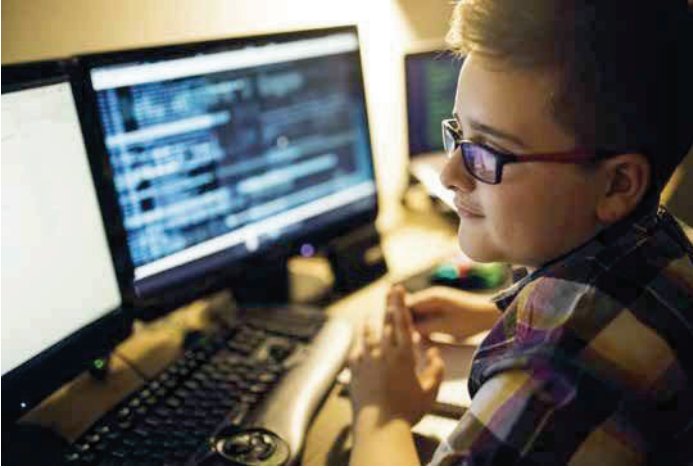
Mike Chiavuzzi, Senior Manager of Network Operations,
Polk County School District

An extra layer of comfort and security

Once the solution was up and running, the team could quickly identify any unsanctioned changes and program modifications on their servers. “9 out of 10 times, that is how ransomware will get through, and I like how [Carbon Black Cloud Workload] will stop it,” says Arnold.

Thanks to the new policy the VMware team helped set up, Polk County is now protected from security risks that could arise internally or externally via changes to programs without IT’s knowledge.

Polk County Schools Protects Data Centers with VMware Carbon Black Cloud Workload



With a school district like Polk County, gaining full visibility in a large environment can be challenging, but according to Chiavuzzi, Carbon Black Cloud Workload has been the key to an enhanced security stance not achievable previously. “We know we’re catching things, we can see it, and we can monitor [what is happening] so it gives us another layer of comfort and security that we never had before,” says Chiavuzzi.

The monitoring and threat protection from Carbon Black Cloud Workload minimizes operational footprint, reducing performance impact on traditional antivirus (AV) scans and giving Polk County the authoritative context to surgically remove vulnerabilities. This allows the team the flexibility to determine the best way to respond to a server. These decisions cannot be made in silos. Carbon Black Cloud Workload gives the PCSD team a single pane of glass to see everything throughout their data centers. If a change or an update breaks something, they would know the root cause for more effective remediation.

Customers like PCSD have greatly reduced the time spent hunting down the root causes of problems with Carbon Black Cloud Workload. “It’s fast,” says Arnold. “It will take us a couple of hours at the most. Most of the time, it doesn’t take that long. If [Carbon Black Cloud Workload] blocked and alerted us to vulnerabilities or threats, then we know where we have to go into.”

“What we like the most is it’s cloud-based. If [Carbon Black Cloud Workload] discovers something new in ransomware, it’s automatically being scanned [in the cloud],” says Arnold. “We don’t have to download anything or update all the servers. It’s being monitored through your cloud base. That’s the part I like.”

Looking ahead

Securing the data center is a top priority for the Polk County IT team, and their partnership with VMware has been the catalyst for building out their new security vision. Chiavuzzi acknowledges they have more work to do when it comes to security, but he is eager to explore the possibilities with VMware. Although faced with increasing threats and broadening responsibilities, they believe that the VMware security vision can provide them with the people, processes and technology to get them to where they need to be.

“Everything from support on in has been spot on. No complaints,” remarks Chiavuzzi. “I guess that’s why we’ve been a VMware customer for so long.”

Value Added Services

4) Detail regarding any value-added services.

Mainline Response: VMware hosts a vast array of SKU based services designed to augment and accent the Carbon Black Solution. Quickly deploy products and add-ons, perform health checks, and migrate applications. Leverage delivery specialists for product installation and configuration. Delivered remotely or on-site, SKU services enable fast onboarding of VMware products.

Multi-Cloud

VMware Cloud on Any Cloud

Including Azure VMware Solution, Google Cloud VMware Engine, Oracle Cloud VMware Solution, and VMware Cloud on AWS

- [VMware Cloud Readiness for VMware Cloud on AWS GovCloud \(US\)](#)
- [VMware Cloud Activation Essentials](#)
- [VMware Cloud Activation Standard](#)
- [VMware Cloud Activation Advanced](#)
- [VMware Cloud Activation Add-On](#)
- [VMware Cloud Migration Essentials](#)
- [VMware Cloud Migration Standard](#)
- [VMware Cloud Migration Advanced](#)
- [VMware Cloud DRaaS Essentials](#)
- [VMware Cloud DRaaS Standard](#)
- [VMwareCloud DRaaS Advanced](#)

VMware Cloud Foundation

- [VMware Cloud Foundation Small-Scale Deployment \(4 Host\)](#)
- [VMware Cloud Foundation Small-Scale Deployment \(8 Host\)](#)
- [VMware Site Reliability Engineering for Cloud Infrastructure](#)

VMware Cloud Foundation on VxRail

- [VMware Cloud Foundation on VxRail Design Review Essentials](#)
- [VMware Cloud Foundation on VxRail Design Review Standard](#)
- [VMware Cloud Foundation on VxRail Design Review Advanced](#)

VMware Aria Universal Suite

(Formerly VMware vRealize Cloud Universal)

- [VMware Fast Time to Value Standard](#)
- [VMware Fast Time to Value Advanced](#)
- [VMware Fast Time to Value Enterprise](#)

VMware Aria Automation

- [VMware Aria Automation Integration 8.x—Standard Service](#)

VMware Aria Operations

- [VMware Performance and Capacity Management Deploy Standard](#)

VMware Aria Cost powered by CloudHealth

(Formerly CloudHealth)

- [VMware Implementation Service](#)
- [VMware Cloud Governance Service](#)
- [VMware Cloud Optimization Service](#)
- [VMware Billing Rules Service](#)

VMware Cloud Provider Platform

- [VMware Cloud Provider Platform Upgrade Planning Essentials](#)
- [VMware Cloud Provider Platform Plan and Upgrade Standard](#)
- [VMware Cloud Provider Platform Plan and Upgrade Advanced](#)
- [VMware NSX Migration Essentials for VMware Cloud Director](#)
- [VMware NSX Migration Standard for VMware Cloud Director](#)
- [VMware NSX Migration Add-on for VMware Cloud Director](#)

vSAN

- [VMware vSAN Small Scale Health Check Essentials](#)
- [VMware vSAN Small Scale Health Check Standard](#)
- [VMware vSAN Small Scale Health Check Advanced](#)
- [VMware vSAN Small Scale Deployment \(4 host\)](#)
- [VMware vSAN Small Scale Deployment \(8 host\)](#)
- [VMware vSAN Small Scale Deployment \(12 host\)](#)
- [VMware vSAN Small Scale Deployment \(16 host\)](#)
- [VMware vSAN Deployment](#)
- [VMware vSAN Health Check Enterprise Small](#)
- [VMware vSAN Health Check Enterprise Medium](#)
- [VMware vSAN Health Check Enterprise Large](#)

vSphere

- [VMware Virtualization Small Scale Health Check Essentials](#)
- [VMware Virtualization Small Scale Health Check Standard](#)
- [VMware Virtualization Small Scale Health Check Advanced](#)
- [VMware Virtualization Deployment](#)
- [VMware Virtualization Health Check Enterprise Small](#)
- [VMware Virtualization Health Check Enterprise Medium](#)
- [VMware Virtualization Health Check Enterprise Large](#)
- [VMware vSphere Upgrade](#)

Site Recovery Manager

- [VMware Disaster Recovery Deployment](#)

Specialized Assistance

- [Delivery Specialist](#)
- [Commercial Residency](#)
- [Federal Residency](#)
- [VMware Day 2 Operations for Multi-Cloud Service](#)



Price Proposal

The following 11 pages contain Mainline's price proposal as well as Attachment A, Price Sheet, of the RFQ. Due to the structure of VMware's pricing model for the Carbon Black solution, please reference the modified pricing tables and the additional provided Excel spreadsheet.



**ATTACHMENT A
PRICE SHEET**

I. Alternate Contract Source (ACS)

Check the ACS contract the Quote is being submitted in accordance with:

- 43210000-US-16-ACS Technology Products, Services, Solutions, and Related Products and Services
- 43230000-NASPO-16-ACS Cloud Solutions
- 43230000-23-NASPO-ACS Software Value Added Reseller (SVAR)

II. Pricing Instructions

The vendor shall provide fixed rates quoted at or below the rates in the applicable ACS contract selected in Section I above. FL[DS] anticipates purchasing the endpoint detection and response Solution for FL[DS] and all Customers. No matter the quantity, the vendor may not exceed the quoted unit price. The Department reserves the right to utilize the quoted unit pricing during the term of any applicable ATC and PO. Prices are ceiling rates inclusive of any and all costs associated with providing services.

III. Pricing

Initial Term Pricing (Years 1-3)		
Item No.	Description	Rate Per Device
1	<p><u>Initial Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	
2	<p><u>Subsequent Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Please reference the modified pricing tables following the signature block. ¶

Optional Renewal Term Pricing (Years 4-6)		
Item No.	Description	Rate Per Device
1	<p>Initial Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	\$ _____
2	<p>Subsequent Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	\$ _____

Please reference the modified pricing tables following the signature block. ¶

IV. ACS Price Breakdown

In the table below, the vendor shall provide the pricing breakdown to document the pricing is in accordance with the applicable ACS contract. The vendor shall provide the ACS SKU Numbers, ACS SKU Descriptions, Market Price, and ACS Price that encompass the services as described in the RFQ:

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price

Please reference the modified pricing tables following the signature block. ¶

Item No. 2 – ACS Pricing Breakdown (without implementation)			
ACS SKU Number	SKU Description	Market Price	ACS Price

Please reference the modified pricing tables following the signature block. ¶

V. Waterfall Pricing (Optional)

The Department is seeking an optional waterfall pricing model which leverages volume discounts. Vendors are encouraged to provide a pricing structure which specifies a volume range at which larger discounts could be applied. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VI. State of Florida Enterprise Pricing (Optional)

The Department is also seeking an optional annual fixed rate to provide the Solution and services to all potential FL[DS] Customers. This alternative pricing shall be in addition to the pricing provided in Section III and IV of this attachment.

VII. Value-Added Services (Optional)

If vendors are able to offer additional services and/or commodities for endpoint detection and response, at no additional cost to the Department, the vendor may offer the Department value-added services, in addition to the services and/or commodities expressly sought by this RFQ.

Per **Section 31.0**, Scrutinized Companies, a vendor submitting a Quote must certify that their company is not participating in a boycott of Israel. By signing below, the vendor so certifies. Additionally, the person submitting the quote and pricing is authorized to respond to this RFQ on the vendor’s behalf, as confirmed by the signature below.

Mainline Information Systems, Inc.

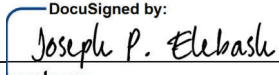
 Vendor Name

59-2960721

 FEIN

6/13/2023

 Date

DocuSigned by:


 Signature

Joseph P. Elebash

 Signatory Printed Name

Carbon Black Endpoint Standard - 1 Year Prepaid			
Initial Term Pricing (Years 1-3)			
Item No.	Description	Rate Per Device	
1	<p>Initial Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>(1-100 Licenses) \$23.00 per license \$3,390.00 per entity</p> <p>(101-500 Licenses) \$20.91 per license \$855.00 per entity</p> <p>(501-1,000 Licenses) \$19.17 per license \$855.00 per entity</p> <p>(1,001-5,000 Licenses) \$17.69 per license \$855.00 per entity</p>	<p>(5,001-10,000 Licenses) \$16.43 per license \$855.00 per entity</p> <p>(10,001-20,000 Licenses) \$13.86 per license \$855.00 per entity</p>
2	<p>Subsequent Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p>(1-100 Licenses) \$23.00 per license \$0.00 per entity</p> <p>(101-500 Licenses) \$20.91 per license \$0.00 per entity</p> <p>(501-1,000 Licenses) \$19.17 per license \$0.00 per entity</p>	<p>(1,001-5,000 Licenses) \$17.69 per license \$0.00 per entity</p> <p>(5,001-10,000 Licenses) \$16.43 per license \$0.00 per entity</p> <p>(10,001-20,000 Licenses) \$13.86 per license \$0.00 per entity</p>

Optional Renewal Term Pricing (Years 4-6)			
Item No.	Description	Rate Per Device	
1	<p>Initial Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>(1-100 Licenses) \$23.00 per license \$3,390.00 per entity</p> <p>(101-500 Licenses) \$20.91 per license \$855.00 per entity</p> <p>(501-1,000 Licenses) \$19.17 per license \$855.00 per entity</p> <p>(1,001-5,000 Licenses) \$17.69 per license \$855.00 per entity</p>	<p>(5,001-10,000 Licenses) \$16.43 per license \$855.00 per entity</p> <p>(10,001-20,000 Licenses) \$13.86 per license \$855.00 per entity</p>
2	<p>Subsequent Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p>(1-100 Licenses) \$23.00 per license \$0.00 per entity</p> <p>(101-500 Licenses) \$20.91 per license \$0.00 per entity</p> <p>(501-1,000 Licenses) \$19.17 per license \$0.00 per entity</p>	<p>(1,001-5,000 Licenses) \$17.69 per license \$0.00 per entity</p> <p>(5,001-10,000 Licenses) \$16.43 per license \$0.00 per entity</p> <p>(10,001-20,000 Licenses) \$13.86 per license \$0.00 per entity</p>

Carbon Black Endpoint Advanced - 1 Year Prepaid			
Initial Term Pricing (Years 1-3)			
Item No.	Description	Rate Per Device	
1	<p>Initial Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>(1-100 Licenses) \$34.50 per license \$3,390.00.00 per entity</p> <p>(101-500 Licenses) \$26.54 per license \$855.00 per entity</p> <p>(501-1,000 Licenses) \$24.64 per license \$855.00 per entity</p> <p>(1,001-5,000 Licenses) \$23.00 per license \$855.00 per entity</p>	<p>(5,001-10,000 Licenses) \$22.40 per license \$855.00 per entity</p> <p>(10,001-20,000 Licenses) \$20.06 per license \$855.00 per entity</p>
2	<p>Subsequent Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p>(1-100 Licenses) \$34.50 per license \$0.00 per entity</p> <p>(101-500 Licenses) \$26.54 per license \$0.00 per entity</p> <p>(501-1,000 Licenses) \$24.64 per license \$0.00 per entity</p>	<p>(1,001-5,000 Licenses) \$23.00 per license \$0.00 per entity</p> <p>(5,001-10,000 Licenses) \$22.40 per license \$0.00 per entity</p> <p>(10,001-20,000 Licenses) \$20.06 per license \$0.00 per entity</p>

Optional Renewal Term Pricing (Years 4-6)			
Item No.	Description	Rate Per Device	
1	<p>Initial Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>(1-100 Licenses) \$34.50 per license \$3,390.00 per entity</p> <p>(101-500 Licenses) \$26.54 per license \$855.00 per entity</p> <p>(501-1,000 Licenses) \$24.64 per license \$855.00 per entity</p> <p>(1,001-5,000 Licenses) \$23.00 per license \$855.00 per entity</p>	<p>(5,001-10,000 Licenses) \$22.40 per license \$855.00 per entity</p> <p>(10,001-20,000 Licenses) \$20.06 per license \$855.00 per entity</p>
2	<p>Subsequent Software Year</p> <p>One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p>(1-100 Licenses) \$34.50 per license \$0.00 per entity</p> <p>(101-500 Licenses) \$26.54 per license \$0.00 per entity</p> <p>(501-1,000 Licenses) \$24.64 per license \$0.00 per entity</p>	<p>(1,001-5,000 Licenses) \$23.00 per license \$0.00 per entity</p> <p>(5,001-10,000 Licenses) \$22.40 per license \$0.00 per entity</p> <p>(10,001-20,000 Licenses) \$20.06 per license \$0.00 per entity</p>

Carbon Black Endpoint Enterprise - 1 Year Prepaid			
Initial Term Pricing (Years 1-3)			
Item No.	Description	Rate Per Device	
1	<p><u>Initial Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p><u>(1-100 Licenses)</u> \$51.75 per license \$3,390.00 per entity</p> <p><u>(101-500 Licenses)</u> \$39.81 per license \$855.00 per entity</p> <p><u>(501-1,000 Licenses)</u> \$36.96 per license \$855.00 per entity</p> <p><u>(1,001-5,000 Licenses)</u> \$32.35 per license \$855.00 per entity</p>	<p><u>(5,001-10,000 Licenses)</u> \$30.44 per license \$855.00 per entity</p> <p><u>(10,001-20,000 Licenses)</u> \$29.07 per license \$855.00 per entity</p>
2	<p><u>Subsequent Software Year</u> One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p><u>(1-100 Licenses)</u> \$51.75 per license \$0.00 per entity</p> <p><u>(101-500 Licenses)</u> \$39.81 per license \$0.00 per entity</p> <p><u>(501-1,000 Licenses)</u> \$36.96 per license \$0.00 per entity</p>	<p><u>(1,001-5,000 Licenses)</u> \$32.35 per license \$0.00 per entity</p> <p><u>(5,001-10,000 Licenses)</u> \$30.44 per license \$0.00 per entity</p> <p><u>(10,001-20,000 Licenses)</u> \$29.07 per license \$0.00 per entity</p>

Optional Renewal Term Pricing (Years 4-6)			
Item No.	Description	Rate Per Device	
1	<p>Initial Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • implementation • initial training • initial Integration • integration maintenance • support services 	<p>(1-100 Licenses) \$51.75 per license \$3,390.00 per entity</p> <p>(101-500 Licenses) \$39.81 per license \$855.00 per entity</p> <p>(501-1,000 Licenses) \$36.96 per license \$855.00 per entity</p> <p>(1,001-5,000 Licenses) \$32.35 per license \$855.00 per entity</p>	<p>(5,001-10,000 Licenses) \$30.44 per license \$855.00 per entity</p> <p>(10,001-20,000 Licenses) \$29.07 per license \$855.00 per entity</p>
2	<p>Subsequent Software Year One year of endpoint detection and response software Solution as described in the RFQ per device. To include:</p> <ul style="list-style-type: none"> • ongoing training • integration maintenance • support services 	<p>(1-100 Licenses) \$51.75 per license \$0.00 per entity</p> <p>(101-500 Licenses) \$39.81 per license \$0.00 per entity</p> <p>(501-1,000 Licenses) \$36.96 per license \$0.00 per entity</p>	<p>(1,001-5,000 Licenses) \$32.35 per license \$0.00 per entity</p> <p>(5,001-10,000 Licenses) \$30.44 per license \$0.00 per entity</p> <p>(10,001-20,000 Licenses) \$29.07 per license \$0.00 per entity</p>

Item No. 1 - ACS Pricing Breakdown (including implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price
<p style="color: red; text-align: center;">Please see the following page and the provided Excel spreadsheet for a full listing of all SKUs, including implementation and training, as well as Market and ACS prices.</p>			

Item No. 2 - ACS Pricing Breakdown (without implementation)			
ACS SKU Number	ACS SKU Description	Market Price	ACS Price



SKU	Description	List Price	NASPO Price	100 Licenses	500 Licenses	1,000 Licenses	5,000 Licenses	10,000 Licenses	20,000 Licenses
Carbon Black - Standard									
VSEC-CBES-DIR-W-US-1Y-C	Carbon Black Endpoint-Standard - 1 Year Prepaid	\$ 40.00	\$ 38.60	\$ 23.00	\$ 20.91	\$ 19.17	\$ 17.69	\$ 16.43	\$ 13.86
Carbon Black - Advanced									
VSEC-CBEA-DIR-W-US-1Y-C	Carbon Black Endpoint-Advanced - 1 Year Prepaid	\$ 60.00	\$ 57.90	\$ 34.50	\$ 26.54	\$ 24.64	\$ 23.00	\$ 22.40	\$ 20.06
Carbon Black - Enterprise									
VSEC-CBEE-DIR-W-US-1Y-C	Carbon Black Endpoint Enterprise - 1 Year Prepaid	\$ 90.00	\$ 86.85	\$ 51.75	\$ 39.81	\$ 36.96	\$ 32.35	\$ 30.44	\$ 29.07
Carbon Black - Services									
VSEC-CBC-PS-DP-ESSL	Carbon Black Cloud Deployment Essentials Services (see attachment for details)	\$ 2,600.00	\$ 2,535.00	\$ 2,535.00	Included	Included	Included	Included	Included
Training/Education									
EDU-CR-0	Learning Credits - Prepaid	\$ 100.00	\$ 97.50	\$ 95.00	\$ 95.00	\$ 95.00	\$ 95.00	\$ 95.00	\$ 95.00
		<u>Learning Credit Price</u>	<u>QTY of Credit required for course</u>	<u>Extended Price</u>					
All Education Pricing is PER USER		\$ 95.00	9	\$ 855.00					
	*Carbon Black Control Administrator Training	\$ 95.00	9	\$ 855.00					
	*Carbon Black Advanced Administrator Training	\$ 95.00	9	\$ 855.00					
	*Carbon Black EDR Advanced Administrator Training	\$ 95.00	9	\$ 855.00					
	*Carbon Black EDR Advanced Analyst Training	\$ 95.00	9	\$ 855.00					
	*Carbon Black Cloud Endpoint Standard Training	\$ 95.00	9	\$ 855.00					
	*Carbon Black Cloud Audit and Remediation	\$ 95.00	9	\$ 855.00					
	*Carbon Black Cloud Enterprise EDR	\$ 95.00	9	\$ 855.00					
	*Carbon Black Cloud: Plan & Deploy Training	\$ 95.00	17	\$ 1,615.00					
	*Carbon Black Cloud: Advanced Operations & Troubleshooting	\$ 95.00	19	\$ 1,805.00					
Carbon Black - Optional Components									
VSEC-XDR-US-1Y-C	Carbon Black XDR - 1 Year Prepaid (Requires Carbon Black EDR Enterprise)	\$ 30.00	\$ 28.95	\$ 17.25	\$ 15.69	\$ 13.27	\$ 12.32	\$ 10.79	\$ 10.14
VSEC-MDR-DIR-US-1Y-C	Carbon Black Managed Detection and Response - 1 Year Prepaid	\$ 24.00	\$ 23.16	\$ 13.80	\$ 12.55	\$ 10.61	\$ 9.86	\$ 8.12	\$ 7.67
VSEC-HFW-US-1Y-C	Carbon Black Host-based Firewall(SaaS) - 1 Year Prepaid	\$ 3.00	\$ 2.90	\$ 1.73	\$ 1.56	\$ 1.32	\$ 1.23	\$ 1.01	\$ 0.95
Carbon Black - Optional Services									
VSEC-CB-PS-ADDON-ESSL	Carbon Black PS Consume Add-Ons-Essentials Services (Optional for additional consulting hours - see attachment for detail)	\$ 2,600.00	\$ 2,535.00	\$ 2,535.00	\$ 2,535.00	\$ 2,535.00	\$ 2,535.00	\$ 2,535.00	\$ 2,535.00
	These Services recommended for any purchase of the above Carbon Black Optional Components								
VSEC-CBC-PS-DP-STD	Carbon Cloud Cloud Deployment Standard Services (see Attac	\$ 5,000.00	\$ 4,875.00	\$ 4,793.15					
VSEC-CBC-PS-DPCON-ADV	Carbon Black Deploy & Consume Advanced Services (see Atta	\$ 18,000.00	\$ 17,550.00	\$ 16,988.44					
VSEC-CBC-PS-DPCON-PRO	Carbon Black Deploy & Consume Professional Services (see At	\$ 38,000.00	\$ 35,001.00	\$ 34,723.10					

Contact Information Sheet

The following page contains Attachment B, Contact Information Sheet, of the RFQ containing the contacts for the Quote and the resulting ATC(s) and PO(s).



**ATTACHMENT B
CONTACT INFORMATION SHEET**

I. Contact Instructions

The vendor shall provide the contact information for the Quote and a contact for the resulting ATC and PO contact in the table below.

II. Contact Information

	Contact for Quoting Purposes	Contact for the ATC and PO (if awarded)
Name:	Doug Harrell	Felicity Lynch
Title:	RVP of Sales - Florida	Fed. Confs & Negotiations Mgr
Address (Line 1):	1700 Summit Lake Drive	1700 Summit Lake Drive
Address (Line 2):		
City, State, Zip Code	Tallahassee, FL 32317	Tallahassee, FL 32317
Telephone (Office):	(850) 294-2237	(540) 522-1619
Telephone (Mobile):	(850) 294-2237	(540) 522-1619
Email:	doug.harrell@mainline.com	felicity.lynch@mainline.com

Non-Disclosure Agreement

The following five (5) pages contain the Non-Disclosure Agreement executed by the Mainline.



Attachment A – Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDRTM Service Offerings

The following two (2) pages contain the Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDRTM Service Offerings.



Service Level Agreement for VMware Carbon Black Cloud™ and VMware Carbon Black® Hosted EDR™ Service Offerings

Dated as of: 15 January 2020

VMware Carbon Black Cloud and VMware Carbon Black® Hosted EDR™ service offerings (each, as applicable, a **“Service”**) are cloud-based Endpoint security services.

VMware warrants that a Service will perform in accordance with and subject to this Service Level Agreement (“SLA”), which sets forth a customer’s sole and exclusive remedy for any breach of this warranty.

Availability

VMware will use commercially reasonable efforts to ensure that, during any given month of the Subscription Term, a Service achieves 100% Availability (as defined below). If the Availability Percentage (as defined below) during a given month is less than 99.9%, a customer will be eligible for a credit as provided below (“Service Credit”). This SLA applies only to a customer’s production environment of the Service, and not to any non-production environment, including, without limitation, testing, staging, evaluation, or proof of concept.

Unless otherwise provided in this SLA, this SLA is subject to the terms of the Agreement as defined in the Terms of Service. Capitalized terms not defined in this SLA will have the meaning specified in the Agreement.

Definitions

“Available” or **“Availability”** means when the user interface for the Service can be logged into. Availability excludes any period of time that the Service cannot be logged into due to: (i) a failure between the customer’s computing environment, computer(s), or system(s) and the Internet; (ii) factors outside of VMware’s reasonable control; (iii) any action or inaction of Customer or a Customer user, administrator, or anyone acting on behalf of Customer; or (iv) scheduled maintenance periods and necessary but unscheduled Emergency Maintenance.

“Availability Percentage” is calculated by subtracting from 100% the percentage of minutes during the month in which a Service was not Available.

“Emergency Maintenance” is unscheduled maintenance that is necessary, in VMware’s reasonable judgment, to address a recently-discovered issue in the Service that could, if left unresolved, materially threaten the security or usability of the Service, Customer Data, or the customer’s systems.

“Maintenance” is the scheduled or unscheduled time where a Service will be updated in order to deploy enhancements or fix issues. If the Service will not be Available for more than eight (8) hours in a given month as a result of scheduled Maintenance, VMware will notify the customer at least thirty (30) days in advance. In any case prior to performing scheduled Maintenance which is expected to result in the Service not being Available, VMware will notify the customer twenty-four (24) hours in advance. In the event of Emergency Maintenance, VMware will notify the customer as soon as practical if the Service is expected to not be Available. All notices under this SLA will be provided to the customer via the VMware Carbon Black User Exchange customer community.

“Monthly Service Fee” is the fee applicable to a month of the Service, and is calculated by taking the annual subscription fee for the Service and dividing by 12.

“**Service Credit**” is a percentage credit applicable against the Monthly Service Fee, based on the actual Availability Percentage during the applicable month as detailed in the following table:

Availability Percentage	Service Credit
99.5% or over, but below 99.9%	5%
97% or over but below 99.5%	10%
95% or over but below 97%	25%
Below 95%	100%

Service Credit Request

To request a Service Credit, a customer must file a support request at <https://my.vmware.com> within thirty (30) days after the Service was first not Available in the month in question. The claim must include:

- the words “**SLA Service Credit Request**” in the subject line; and
- the dates and times of each period during which the Service was not Available in the month in question and for which Customer is claiming the Service Credit.

Upon receipt of a claim for a Service Credit, VMware will use reasonable efforts to confirm the claim. If the claim is confirmed by VMware, based on VMware’s data and records, then VMware will approve the Service Credit. Customer may not claim more than one Service Credit for any month.

A customer may apply the Service Credits only to its future payments for the Service that is the basis for the Service Credit. Service Credits will not entitle Customer to any refund or other payment from VMware and cannot be applied towards other VMware products or service offerings. Service Credits may not be transferred or applied to any other account. Service Credits will expire twelve (12) months after issuance or when the Subscription Term for the Service expires or terminates, whichever first occurs.

Attachment B – VMware Production Support for Cloud Products

The following page contains information concerning support for the proposed VMware Carbon Black solution.



VMware Production Support for Cloud Products

Focused, 24-hour support for cloud deployments

KEY BENEFITS

- Global, 24x7 support for Severity 1 issues
- Unlimited number of support requests
- Up to 6 Administrators
- Online access to documentation and technical resources, knowledge base articles, and discussion forums
- Cloud updates

ADDITIONAL INFORMATION

Purchase information can be found by dialing one of VMware's [toll free](#) numbers and choosing the Sales Option or contacting one of [VMware's resellers](#).

Additional information about VMware's support policies and offerings can be found in the [VMware Technical Support Welcome Guide](#).

TERMS AND CONDITIONS

VMware Cloud Services are governed by the applicable [VMware Cloud Service Offerings Terms of Service](#).

VMware may, at its discretion, decide to end availability of any Service Offering and related Cloud Support from time to time. VMware has no obligation to provide Cloud Support after the End of Support for the Service Offering. Refer to [VMware Lifecycle Policies](#) for more information.

Overview

VMware® Production Support for Cloud Services is designed with your access to cloud service products in mind. We are committed to delivering enterprise-class, worldwide support with a focus on a single objective: your success. Our global support centers are staffed around the clock to ensure that you can access the products from a Web browser anywhere the Internet is available. VMware handles software deployment and maintenance, enabling you to focus on running your business.

OVERVIEW	
Hours of Operation	24 hours/day, 7 days/week, 365 days/year
Self Help Access: KB Articles, Product Documentation & Communities	Yes
Online Access to Product Updates & Upgrades	Yes
Length of Contract Engagement	1, 2, or 3 years
Products Supported	All
Business Hours	Monday - Friday
Number of Support Requests	Unlimited
Number of Individual Support Administrators	6
Root Cause Analysis	Only available with VMware Premier Support and VMware Success 360
Target Response Times for Initial Response	Severity 1 within 30 minutes or less, 24 hrs/day 7 days/week
	Severity 2 - 4 business hours 10 hrs/day, 5 days/week
	Severity 3 - 8 business hours, 10 hrs/day, 5 days/week
	Severity 4 - 12 business hours 10 hrs/day, 5 days/week



Attachment C – VMware Carbon Black Cloud Deployment

The following 20 pages contain detailed information on various levels of deployment for the VMware Carbon Black Cloud solution.



VMware Carbon Black Cloud Deployment Essentials

AT A GLANCE

The primary objective of this service is to implement the VMware Carbon Black Cloud solution based on your desired outcomes.

This service is conducted jointly with your team members to enhance the learning experience during the deployment.

KEY BENEFITS

- Rapid time to value on your newly purchased VMware Carbon Black Cloud SaaS product
- Deploy a best practice based, foundational Carbon Black Cloud implementation
- Develop key skills to be able to support a CB Cloud security platform
- Consolidate multiple endpoint security capabilities using one agent and console

SKU

VSEC-CBC-PS-DP-ESSL

Service Overview

The VMware Carbon Black Cloud Deployment Essentials service introduces you to the products and assists you with the sensor deployment strategy, administration console UI walkthrough and policy/rules review.

The implementation will follow a phased approach with phases defined as follows: 1) Plan, 2) Execute, and 3) Close.

Services include basic configuration and sensor deployment best practices for one (1) customer's VMware Carbon Black Cloud instance via knowledge transfer workshops for up to a total of 1,000 Carbon Black endpoints and virtual workloads.

Estimated Schedule

Professional services are performed during normal business hours and workdays (weekdays and non-holidays) remotely. VMware will deliver the Remote Consulting Services using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the Consultant(s).

Project Schedule begins from the first Execute meeting and will run for a maximum of six (6) consecutive weeks (exception for the last week of December when VMware offices are closed).

Project Scope

- Carbon Black Cloud Endpoint Sensor Deploy (2)
- Workload appliance Deploy (1) (if applicable)
- Containers protection Deploy (1) (if applicable)
- Admin Console Setup (1)
- Policies, rules and alerts triage (15)
- Web UI Walkthrough on purchased features
- UEX intro

Responsibilities

All supplier and Customer responsibilities are listed in the Deliverables section. The ownership is defined as follows:

- VMware: VMware is responsible for delivery, with minimal assistance from the Customer's project team.

- Joint: VMware and the Customer's project team are jointly responsible for delivery
- Customer: The Customer is responsible for delivery, with minimal assistance from VMware.

Deliverables:

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
PHASE 1: PLAN				
1.1	Kick-Off Meeting	Solution Overview presentation	Joint	Initial meeting to discuss project scope, objectives, impact assessment, and teams
1.2	Review Datasheet	-	CUSTOMER	Understand service assumptions, scope, and completion criteria
1.3	Review Pre-Installation Requirements	Operating Environment Requirements (OER) document	Joint	Minimum system requirements
1.4	Review Change Management Strategy	-	CUSTOMER	Customer determines a change management process for agent testing and installation
PHASE 2: EXECUTE				
2.1	Pilot Deployment	Deploy up to two (2) Carbon Black Cloud sensors	CUSTOMER	Customer defines an end-user communication plan for pilot user community
2.2	Register Appliance in the vCenter Server (if applicable)	Deploy up to one (1) Carbon Black Cloud Workload appliance	Joint	Generate the API ID and key to establish connection between appliance and Carbon Black Cloud
2.3	Kubernetes Cluster Operator(s) (if applicable)	Deploy up to one (1) Kubernetes Cluster Operator(s)	Joint	Assist with deployment of Kubernetes Cluster Operator(s) (if applicable)
2.4	Configuration Assistance	Create up to fifteen (15) policies and/or rules	Joint	Assist analyzing event data, define reputation rules, behavioral rules, and permission rules

2.5	Product Adoption Document	Product adoption guide	VMware	High-level operational guide
2.6	Production Deployment	Deploy remaining Carbon Black Cloud sensors	CUSTOMER	Customer deploys solution to production endpoints
2.7	Alerts and Unexpected Blocks	Review and triage up to fifteen (15) alerts and unexpected blocks	Joint	Assist with alert notifications and triage
PHASE 3: CLOSE				
3.1	Customer Support Transition	Project closure email	VMware	Transition to support

Completion Criteria

The project is deemed complete upon ONE of the following criteria – whichever comes first:

1. Completion of all service deliverables in the Deliverables section.
2. After six (6) consecutive weeks from date the project is moved to Phase 2 Execute (Deliverable 2.1).
3. After 12 months from purchase date.
4. If the services were purchased using PSO credits the services expire the same time the credits expire unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Out of Scope

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines.
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control.
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by the Customer.
- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.

- Customer solution training other than the defined knowledge transfer session.

Carbon Black Cloud

- Remediation/removal of unauthorized, malicious, or unwanted files.
- Investigation and analysis of potential malware and threats.
- Configuring more than one administration console.
- Building of custom scripts or feeds.
- Performing custom threat feed configuration.
- Customer solution training other than the defined in scope services.
- Developing custom documentation.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues.

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

Contact a Professional Services expert at vmware.com/company/contact.html.

Service Assumptions

CUSTOMER RESOURCES: Should the Customer request VMware to perform tasks that are dependent upon the Customer resources or decisions, the Customer will make such resource available or decisions final in a timely manner.

HARDWARE PROCUREMENT: Procurement and installation of hardware is the responsibility of the Customer. VMware will provide recommendations and assistance.

WORKING HOURS: Engagements that require consultants to work in excess of 40 hours per week, to work on weekends or major national holidays and/or to travel outside of this schedule will be considered exceptions to this policy and will be reviewed and approved by VMware and the Customer as required.

PREREQUISITES: Pre-requisites must be completed for all installation components before any installation activities will be performed. Should the Customer not purchase the associated software for deployment, the services deliverable line items associated with those software components will not be delivered.

PROJECT MANAGEMENT: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis.

DELIVERABLE LANGUAGE: All work, documentation and work product(s) will be provided in English.

USE-CASE SCOPE: The scope of the use-cases will be considered locked upon completion of Deliverable 1.1 (See Deliverables section above) and will be delivered within a single production deployment phase. Any alteration to the use-case scope thereafter may necessitate a change request.

TERMS AND CONDITIONS

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

If you purchase this packaged service outside of the ELA, the service must be delivered and accepted within the first 12 months of the purchase, or the service will be forfeited. For detailed pricing, contact your local VMware representative.



VMware Carbon Black Cloud Deployment - Standard

AT A GLANCE

The primary objective of this service is to implement the VMware Carbon Black Cloud solution based on your desired outcomes.

This service is conducted jointly with your team members to enhance the learning experience during the deployment.

KEY BENEFITS

- Rapid time to value on your newly purchased VMware Carbon Black Cloud SaaS product
- Deploy a best practice based, foundational Carbon Black Cloud implementation
- Develop key skills to be able to support a CB Cloud security platform
- Consolidate multiple endpoint security capabilities using one agent and console

SKU

VSEC-CBC-PS-DP-STD

Service Overview

The VMware Carbon Black Cloud Deployment Standard service assists you with the sensor deployment strategy, administration console UI walkthrough, policy/rules review, best practices on using the features you purchased.

The implementation will follow a phased approach with phases defined as follows: 1) Plan, 2) Execute, and 3) Close.

Services include configuration and sensor deployment best practices for one (1) VMware Carbon Black Cloud instance via knowledge transfer workshops for up to a total of 5,000 Carbon Black endpoints and virtual workloads.

Estimated Schedule

Professional services are performed during normal business hours and workdays (weekdays and non-holidays) remotely. VMware will deliver Remote Consulting Services using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the Consultant(s).

Project Schedule begins from the first Execute meeting and will run for a maximum of nine (9) consecutive weeks (exception for the last week of December when VMware offices are closed).

Project Scope

- Carbon Black Cloud Endpoint Sensor Deploy (5)
- Workload appliance Deploy (1) (if applicable)
- Containers protection Deploy (1) (if applicable)
- Admin Console Setup (1)
- Web UI Walkthrough on purchased features
- Policies, rules and alerts triage (25)
- UEX intro

Responsibilities

All supplier and Customer responsibilities are listed in the Deliverables section. The ownership is defined as follows:

- **VMware:** VMware is responsible for delivery, with minimal assistance from the Customer's project team.
- **Joint:** VMware and Customer's project team are jointly responsible for delivery.

- CUSTOMER: The Customer is responsible for delivery, with minimal assistance from VMware.

Deliverables

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
PHASE 1: PLAN				
1.1	Kick-Off Meeting	Solution Overview presentation	Joint	Initial meeting to discuss project scope, objectives, impact assessment, and teams
1.2	Review Datasheet	-	CUSTOMER	Understand service assumptions, scope, and completion criteria
1.3	Review Pre-Installation Requirements	Operating Environment Requirements (OER) document	Joint	Minimum system requirements
1.4	Review Change Management Strategy	-	CUSTOMER	Customer determines a change management process for agent testing and installation
PHASE 2: EXECUTE				
2.1	Pilot Deployment	Deploy up to five (5) Carbon Black Cloud sensors	CUSTOMER	Customer defines an end-user communication plan for pilot user community
2.2	Register Appliance in the vCenter Server (if applicable)	Deploy up to one (1) Carbon Black Cloud Workload appliance	Joint	Generate the API ID and key to establish connection between appliance and Carbon Black Cloud
2.3	Kubernetes Cluster Operator(s) (if applicable)	Deploy up to one (1) Kubernetes Cluster Operator(s)	Joint	Assist with deployment of Kubernetes Cluster Operator(s) (if applicable)
2.4	Configuration Assistance	Create up to twenty-five (25) policies and/or rules	Joint	Assist analyzing event data, define reputation rules, behavioral rules, and permission rules
2.5	Product Adoption Document	Product adoption guide	VMware	High-level operational guide

2.6	Production Deployment	Deploy remaining Carbon Black Cloud sensors	CUSTOMER	Customer deploys solution to production endpoints
2.7	Alerts and Unexpected Blocks	Review and triage up to twenty-five (25) alerts and unexpected blocks	Joint	Assist with alert notifications and triage
PHASE 3: CLOSE				
3.1	Customer Support Transition	Project closure email	VMware	Transition to support

Completion Criteria

The project is deemed complete upon ONE of the following criteria - whichever comes first:

1. Completion of all service deliverables in the Deliverables section.
2. After nine (9) consecutive weeks from date the project is moved to Phase 2 Execute (Deliverable 2.1).
3. After 12 months from purchase date.
4. If the services were purchased using PSO credits the services expire the same time the credits expire unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Out of Scope

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines.
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control.
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by the Customer.
- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.
- Customer solution training other than the defined knowledge transfer session.

Carbon Black Cloud

- Remediation/removal of unauthorized, malicious, or unwanted files.
- Investigation and analysis of potential malware and threats.
- Configuring more than one administration console.
- Building of custom scripts or feeds.
- Performing custom threat feed configuration.
- Customer solution training other than the defined in scope services.
- Developing custom documentation.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues.

Carbon Black Cloud Deployment Standard

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

Contact a Professional Services expert at vmware.com/company/contact.html.

Service Assumptions

CUSTOMER RESOURCES: Should the Customer request VMware to perform tasks that are dependent upon the Customer resources or decisions, the Customer will make such resource available or decisions final in a timely manner.

HARDWARE PROCUREMENT: Procurement and installation of hardware is the responsibility of the Customer. VMware will provide recommendations and assistance.

WORKING HOURS: Engagements that require consultants to work in excess of 40 hours per week, to work on weekends or major national holidays and/or to travel outside of this schedule will be considered exceptions to this policy and will be reviewed and approved by VMware and Customer as required.

PREREQUISITES: Pre-requisites must be completed for all installation components before any installation activities will be performed. Should the Customer not purchase the associated software for deployment, the services deliverable line items associated with those software components will not be delivered.

PROJECT MANAGEMENT: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis.

DELIVERABLE LANGUAGE: All work, documentation and work product(s) will be provided in English.

USE-CASE SCOPE: The scope of the use-cases will be considered locked upon completion of Deliverable 1.1 (See Deliverables section above) and will be delivered within a single production deployment phase. Any alteration to the use-case scope thereafter may necessitate a change request.

TERMS AND CONDITIONS

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

If you purchase this packaged service outside of the ELA, the service must be delivered and accepted within the first 12 months of the purchase, or the service will be forfeited. For detailed pricing, contact your local VMware representative.



VMware Carbon Black Cloud Deploy and Consume Advanced

AT A GLANCE

The primary objective of this service is to implement the VMware Carbon Black Cloud solution based on your desired outcomes.

This service is conducted jointly with your team members to enhance the learning experience during the deployment.

KEY BENEFITS

- Rapid time to value on your newly purchased VMware Carbon Black Cloud SaaS product
- Deploy a best practice based, foundational Carbon Black Cloud implementation
- Develop key skills to be able to support a CB Cloud security platform
- Consolidate multiple endpoint security capabilities using one agent and console

SKU

VSEC-CBC-PS-DPCON-ADV

Service Overview

The VMware Carbon Black Cloud Deploy and Consume Advanced service assists you with the sensor deployment strategy, administration console UI walkthrough, policy/rules review, best practices on alerts tuning, audit and remediation usage, and threat intelligence/watchlists from pilot to production.

The implementation will follow a phased approach with phases defined as follows: 1) Plan, 2) Execute, and 3) Close.

Services include configuration and sensor deployment best practices for one (1) customer's VMware Carbon Black Cloud instance via knowledge transfer workshops for up to 10,000 Carbon Black endpoints and virtual workloads.

Estimated Schedule

Professional services are performed during normal business hours and workdays (weekdays and non-holidays) remotely. VMware will deliver the Remote Consulting Services using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the Consultant(s).

Project Schedule begins from the first Execute meeting and will run for a maximum of thirteen (13) consecutive weeks (exception for the last week of December when VMware offices are closed).

Project Scope

- Carbon Black Cloud Endpoint Sensor Deploy (up to 100)
- Workload Appliance Deploy (up to 5) (if applicable)
- Container protection Deploy (up to 5) (if applicable)
- Admin Console Setup (1)
- Web UI walkthrough on purchased features
- Policies, rules and alerts triage (up to 50)
- UEX Intro

Responsibilities

All supplier and Customer responsibilities are listed in the Deliverables section. The ownership is defined as follows:

- VMware: VMware is responsible for delivery, with minimal assistance from the Customer's project team.

- Joint: VMware and the Customer's project team are jointly responsible for delivery.
- CUSTOMER: The Customer is responsible for delivery, with minimal assistance from VMware.

Deliverables

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
PHASE 1: PLAN				
1.1	Kick-Off Meeting	Solution Overview presentation	Joint	Initial meeting to discuss project scope, objectives, impact assessment, and teams
1.2	Review Datasheet	-	CUSTOMER	Understand service assumptions, scope, and completion criteria
1.3	Review Pre-Installation Requirements	Operating Environment Requirements (OER) document	Joint	Minimum system requirements
1.4	Review Change Management Strategy	-	CUSTOMER	Customer determines a change management process for agent testing and installation
Phase 2: Execute				
2.1	Pilot Deployment	Deploy up to one hundred (100) Carbon Black Cloud sensors	CUSTOMER	Customer defines an end-user communication plan for pilot user community
2.2	Register Appliance in the vCenter Server (if applicable)	Deploy up to five (5) Carbon Black Cloud Workload appliance	Joint	Generate the API ID and key to establish connection between appliance and Carbon Black Cloud
2.3	Kubernetes Cluster Operator(s) (if applicable)	Deploy up to five (5) Kubernetes Cluster Operator(s)	Joint	Assist with deployment of Kubernetes Cluster Operator(s) (if applicable)
2.4	Configuration Assistance	Create up to fifty (50) policies and/or rules	Joint	Assist analyzing event data, define reputation rules, behavioral rules, and permission rules

2.5	Product Adoption Document	Product adoption guide	VMware	High-level operational guide
2.6	Production Deployment	Deploy remaining Carbon Black Cloud sensors	CUSTOMER	Customer deploys solution to production endpoints
2.7	Alerts and Unexpected Blocks	Review and triage up to fifty (50) alerts and unexpected blocks	Joint	Assist with alert notifications and triage
2.8	Alerts Investigation	Investigate alerts and provide improvement plan	VMware	Access to customer cloud Instance to Investigate alerts and provide Improvement plan (upon customer's approval)
Phase 3: Close				
3.1	Customer Support Transition	Project closure email	VMware	Transition to support

Completion Criteria

The project is deemed complete upon ONE of the following criteria – whichever comes first:

1. Completion of all service deliverables in the Deliverables section.
2. After thirteen (13) consecutive weeks from date the project is moved to Phase 2 Execute (Deliverable 2.1).
3. After 12 months from purchase date.
4. If the services were purchased using PSO credits the services expire the same time the credits expire unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Out of Scope

The following are the out of scope items for this project.

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines.
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control.

- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer.
- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.
- Customer solution training other than the defined knowledge transfer session.

Carbon Black Cloud

- Remediation/removal of unauthorized, malicious, or unwanted files.
- Investigation and analysis of potential malware and threats.
- Configuring more than one administration console.
- Building of custom scripts or feeds.
- Performing custom threat feed configuration.
- Customer solution training other than the defined in scope services.
- Developing custom documentation.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues.

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

Contact a Professional Services expert at vmware.com/company/contact.html.

Service Assumptions

CUSTOMER RESOURCES: Should the Customer request VMware to perform tasks that are dependent upon Customer resources or decisions, the Customer will make such resource available or decisions final in a timely manner.

HARDWARE PROCUREMENT: Procurement and installation of hardware is the responsibility of the Customer. VMware will provide recommendations and assistance.

WORKING HOURS: Engagements that require consultants to work in excess of 40 hours per week, to work on weekends or major national holidays and/or to travel outside of this schedule will be considered exceptions to this policy and will be reviewed and approved by VMware and the Customer as required.

PREREQUISITES: Pre-requisites must be completed for all installation components before any installation activities will be performed. Should the Customer not purchase the associated software for deployment, the services deliverable line items associated with those software components will not be delivered.

PROJECT MANAGEMENT: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis.

DELIVERABLE LANGUAGE: All work, documentation and work product(s) will be provided in English.

USE-CASE SCOPE: The scope of the use-cases will be considered locked upon completion of Deliverable 1.1 (See Deliverables section above) and will be delivered within a single production deployment phase. Any alteration to the use-case scope thereafter may necessitate a change request.

TERMS AND CONDITIONS

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

If you purchase this packaged service outside of the ELA, the service must be delivered and accepted within the first 12 months of the purchase, or the service will be forfeited. For detailed pricing, contact your local VMware representative.



VMware Carbon Black Cloud Deploy and Consume Professional

AT A GLANCE

The primary objective of this service is to implement the VMware Carbon Black Cloud solution based on your desired outcomes.

This service is conducted jointly with your team members to enhance the learning experience during the deployment.

KEY BENEFITS

- Rapid time to value on your newly purchased VMware Carbon Black Cloud SaaS product
- Deploy a best practice based, foundational Carbon Black Cloud implementation
- Develop key skills to be able to support a CB Cloud security platform
- Consolidate multiple endpoint security capabilities using one agent and console

SKU

VSEC-CBC-PS-DPCON-PRO

Service Overview

The VMware Carbon Black Cloud Deploy and Consume Professional service assists you with the sensor deployment strategy, administration console UI walkthrough, policy/rules review, best practices on alerts tuning, Audit and Remediation usage, and threat intelligence/watchlists, from pilot to production.

The implementation will follow a phased approach with phases defined as follows: 1) Plan, 2) Execute, and 3) Close.

Services include configuration and sensor deployment best practices for one (1) Customer's VMware Carbon Black Cloud instance via knowledge transfer workshops for up to 20,000 Carbon Black endpoints and virtual workloads.

Estimated Schedule

Professional services are performed during normal business hours and workdays (weekdays and non-holidays) remotely. VMware will deliver the Remote Consulting Services using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the Consultant(s).

Project Schedule begins from the first Execute meeting and will run for a maximum of seventeen (17) consecutive weeks (exception for the last week of December when VMware offices are closed).

Project Scope

- Carbon Black Cloud Endpoint Sensor Deploy (up to 200)
- Workload appliance Deploy (up to 10) (if applicable)
- Containers protection Deploy (up to 10) (if applicable)
- Admin Console Setup (1)
- WebUI Walkthrough on purchased features
- Policies, rules and alerts triage (up to 100)
- UEX Intro

Responsibilities

All supplier and Customer responsibilities are listed in the Deliverables section. The ownership is defined as follows:

- VMware: VMware is responsible for delivery, with minimal assistance from the Customer's project team.

- **Joint:** VMware and the Customer's project team are jointly responsible for delivery.
- **CUSTOMER:** The Customer is responsible for delivery, with minimal assistance from VMware.

Deliverables

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
PHASE 1: PLAN				
1.1	Kick-Off Meeting	Solution Overview presentation	Joint	Initial meeting to discuss project scope, objectives, impact assessment, and teams
1.2	Review Datasheet	-	CUSTOMER	Understand service assumptions, scope, and completion criteria
1.3	Review Pre-Installation Requirements	Operating Environment Requirements (OER) document	Joint	Minimum system requirements
1.4	Review Change Management Strategy	-	CUSTOMER	Customer determines a change management process for agent testing and installation
PHASE 2: EXECUTE				
2.1	Pilot Deployment	Deploy up to two hundred (200) Carbon Black Cloud sensors	CUSTOMER	Customer defines an end-user communication plan for pilot user community
2.2	Register Appliance in the vCenter Server (if applicable)	Deploy up to ten (10) Carbon Black Cloud Workload appliance	Joint	Generate the API ID and key to establish connection between appliance and Carbon Black Cloud
2.3	Kubernetes Cluster Operator(s) (if applicable)	Deploy up to ten (10) Kubernetes Cluster Operator(s)	Joint	Assist with deployment of Kubernetes Cluster Operator(s) (if applicable)
2.4	Configuration Assistance	Create up to one hundred (100) policies and/or rules	Joint	Assist analyzing event data, define reputation rules, behavioral rules, and permission rules

2.5	Product Adoption Document	Product adoption guide	VMware	High-level operational guide
2.6	Production Deployment	Deploy remaining Carbon Black Cloud sensors	CUSTOMER	Customer deploys solution to production endpoints
2.7	Alerts and Unexpected Blocks	Review and triage up to one hundred (100) alerts and unexpected blocks	Joint	Assist with alert notifications and triage
2.8	Alerts Investigation	Investigate alerts and provide improvement plan	VMware	Access to customer cloud Instance to Investigate alerts and provide Improvement plan (upon customer's approval)
PHASE 3: CLOSE				
3.1	Customer Support Transition	Project closure email	VMware	Transition to support

Completion Criteria

The project is deemed complete upon ONE of the following criteria – whichever comes first:

1. Completion of all service deliverables in the Deliverables section.
2. After seventeen (17) consecutive weeks from date the project is moved to Phase 2 Execute (Deliverable 2.1).
3. After 12 months from purchase date.
4. If the services were purchased using PSO credits the services expire the same time the credits expire unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Out of Scope

The following are the out of scope items for this project.

General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines
- Operating system administration including the operating system itself or any operating system features or components.
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within the Customer's control.
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer.

- Installation or configuration of VMware products not included in the scope of this document.
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components.
- Configuration of VMware products used for the service other than those implemented for the mutually agreed to use cases.
- Customer solution training other than the defined knowledge transfer session.

Carbon Black Cloud

- Remediation/removal of unauthorized, malicious, or unwanted files.
- Investigation and analysis of potential malware and threats.
- Configuring more than one administration console.
- Building of custom scripts or feeds.
- Performing custom threat feed configuration.
- Customer solution training other than the defined in scope services.
- Developing custom documentation.
- Troubleshooting integration or infrastructure issues when deemed to be non-Company product issues.

LEARN MORE

Visit vmware.com/services.

FOR MORE INFORMATION

Contact a Professional Services expert at vmware.com/company/contact.html.

Service Assumptions

CUSTOMER RESOURCES: Should the Customer request VMware to perform tasks that are dependent upon Customer resources or decisions, the Customer will make such resource available or decisions final in a timely manner.

HARDWARE PROCUREMENT: Procurement and installation of hardware is the responsibility of the Customer. VMware will provide recommendations and assistance.

WORKING HOURS: Engagements that require consultants to work in excess of 40 hours per week, to work on weekends or major national holidays and/or to travel outside of this schedule will be considered exceptions to this policy and will be reviewed and approved by VMware and the Customer as required.

PREREQUISITES: Pre-requisites must be completed for all installation components before any installation activities will be performed. Should the Customer not purchase the associated software for deployment, the services deliverable line items associated with those software components will not be delivered.

PROJECT MANAGEMENT: VMware and the Customer's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis.

DELIVERABLE LANGUAGE: All work, documentation and work product(s) will be provided in English.

USE-CASE SCOPE: The scope of the use-cases will be considered locked upon completion of Deliverable 1.1 (See Deliverables section above) and will be delivered within a single production deployment phase. Any alteration to the use-case scope thereafter may necessitate a change request.

TERMS AND CONDITIONS

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

If you purchase this packaged service outside of the ELA, the service must be delivered and accepted within the first 12 months of the purchase, or the service will be forfeited. For detailed pricing, contact your local VMware representative.



Attachment D – Carbon Black Cloud Global Resiliency

The following two (2) pages contain an overview of Carbon Black Cloud’s Global Resiliency program. More information regarding the disaster recovery aspects of the Carbon Black solution can be made available upon execution of a mutual non-disclosure agreement.





Global Resiliency Program

VMware is a provider of virtualization and virtualization-based cloud infrastructure solutions. Our solutions address a range of IT issues, including facilitating access to cloud computing capacity, business continuity, software lifecycle management, and corporate end-user computing device management. Our solutions are organized into three main product groups: cloud infrastructure and management, cloud application platform, and end-user computing.

VMware developed a global resiliency program that outlines how we respond to events that threaten to disrupt our business. While every business disruption poses unique problems based on external factors (for example, time of day or month, severity, nature of disaster, or geographic impacts), we are committed to our customers and doing what it takes for us to deliver the same quality service for which we're known.

Our resiliency program identifies what preparations must be made in advance of a disruption, as well as the steps to be taken when an event occurs. The program is reviewed periodically to determine the most critical business processes and the resources—people, equipment, records, computer systems and office facilities—required for operation. All documented resiliency plans and processes follow an annual standard maintenance and assessment schedule.

There are an incalculable number of events or circumstances that could result in a significant business disruption, and their impact may vary in size, scope, duration, severity and geographic location. Significant business disruptions may result in degrees of harm to human life and regional/national infrastructure (such as power, transportation and communications), which could impact VMware's recovery efforts.

While diligent in our efforts to plan for unexpected events, it is impossible to consider every possible scenario and develop detailed responses to each. VMware, in our sole discretion, reserves the right to flexibly respond to any disruption in a situation-specific and prudent manner. This document is not intended to provide a guarantee or warranty regarding the actions or performance of VMware, our computer systems or our personnel in the event of a significant business disruption. This information is provided solely to our customers and vendors. No further distribution or disclosure is permitted without our prior written consent. No person other than our customers and vendors may rely on any statement herein.

In the event of an actual declared disaster (including a force majeure event) and such disasters not fully addressed in the company's business continuity/disaster recovery plans, VMware will use commercially reasonable efforts to restore service to our customers as quickly as possible.

Key aspects of the resiliency program

Business continuity management

The business continuity management (BCM) program is under the direction of the chief information officer. The BCM steering committee—comprised of executive management across all lines of business—meets quarterly to review the overall program and provide any direction needed. Business continuity plans are developed and maintained to support the adequate performance of critical business functions. Business continuity plans and the business impact analysis are updated at least once per year to address major operational changes.

Disaster recovery

VMware has a backup data center located in a different geographic location than the primary data center. In the event of a disaster, critical functions will be recovered at the alternate location. This enterprise-grade data center is secured with restricted access; has redundant uninterruptible power supply units; and is monitored for temperature, humidity and other environmental conditions. Disaster recovery exercises are conducted each quarter.

Crisis management/crisis communications

VMware has emergency preparedness plans that provide additional emergency response, preparedness, instructions and guidelines to protect the safety and well-being of our employees and guests in the event of major disruptions and emergencies. Once activated, the crisis management team—comprised of select executives and senior managers from key departments—evaluates the severity of the event and responds accordingly.

Exercise and maintenance

VMware conducts exercises to identify gaps in documentation or processes. Exercise findings and areas identified as requiring attention are documented and assigned to the appropriate subject matter experts for resolution.

Staffing

All employees will be dedicated to restoring customer services as quickly as possible after a disruption. Teams are located globally and can continue operations if their primary offices are unavailable. Procedures are also in place to relocate employees, if needed.

Pandemic planning

Aligned with World Health Organization guidelines, a plan has been implemented across the enterprise to address pandemic concerns.

Attachment E – System and Organization Controls Report SOC 3®

The following 14 pages include the SOC 3 Report for Carbon Black Cloud.





Carbon Black Cloud

System and Organization Controls Report SOC 3[®]

Report on Management's Description of
VMware, Inc.'s Carbon Black Cloud System and
on the Suitability of the Design and Operating
Effectiveness of Controls Relevant to Security,
Availability, and Confidentiality

For the period of April 1, 2021 to March 31, 2022

Table of Contents

SECTION I: Independent Service Auditor’s Report	1
SECTION II: Assertion of VMware Inc.’s Management	4
ATTACHMENT A: Description of the Boundaries of the System Provided by VMware Inc	6
System Overview	7
Company Background	7
Carbon Black Cloud Service	7
Components of the Carbon Black Cloud System	8
Infrastructure.....	8
Software	8
People	8
Procedures.....	9
Data	10
Subservice Organization	10
ATTACHMENT B: Principal Service Commitments and System Requirements	11
Service Commitments and System Requirements	12

SECTION I:

Independent Service Auditor's Report



INDEPENDENT SERVICE AUDITOR'S REPORT

To: VMware Inc.

Scope

We have examined VMware Inc. (VMware or service organization) accompanying assertion titled "Assertion of VMware Inc.'s Management" (assertion) that the controls within VMware's Carbon Black Cloud System (system) were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

VMware is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that VMware's service commitments and system requirements were achieved. VMware has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, VMware is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls were not effective to achieve VMware's service commitments and system requirements based on the applicable trust services criteria

SECTION I: Independent Service Auditor's Report

- Performing procedures to obtain evidence about whether controls within the systems were effective to achieve VMware's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within VMware's Carbon Black Cloud System were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Crowe LLP

Crowe LLP

Columbus, Ohio
May 31, 2022

SECTION II:

Assertion of VMware Inc.'s Management



VMware, Inc. (877) 486-9273 toll free
3401 Hillview Ave. (650) 427-5000 main
Palo Alto, CA 94304 (650) 427-5001 fax www.vmware.com

May 31, 2022

ASSERTION OF VMWARE INC.'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within VMware Inc.'s (VMware or service organization) Carbon Black Cloud System throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that VMware's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. VMware's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that VMware's service commitments and system requirements were achieved based on the applicable trust services criteria.

VMware Inc.

ATTACHMENT A:

Description of the Boundaries of the System Provided by VMware Inc.

System Overview

COMPANY BACKGROUND

VMware, Inc. was founded on January 1, 1998, and currently has more than 35,000 employees worldwide. VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver applications on cloud environments. With more than 500,000 customers and 75,000 partners, VMware provides infrastructure, services, and cloud solutions to organizations of all sizes. Headquartered in Palo Alto, California, and strategic business offices around the globe, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.

CARBON BLACK CLOUD SERVICE

VMware Carbon Black is the security business unit (SBU) within VMware that provides clients a comprehensive portfolio of security solutions, including VMware's Carbon Black Cloud System.

Carbon Black Cloud is an extensible platform that leverages unfiltered data and streaming analytics to power multiple security services. Services that are included with this platform include the following:

- **Endpoint Standard:** Next-generation antivirus and Behavioral Endpoint Detection and Response (EDR).
- **Audit and Remediation:** Real-time endpoint query and remediation.
- **Managed Detection and Response:** Managed threat alert and response service.
- **Enterprise EDR:** Incident response and threat hunting for security operations center teams.
- **Workload Protection:** Advanced security and risk management for cloud workloads.
- **Container Security:** Identification of risks associated with container environments.
- **Vulnerability Management:** Identification of vulnerabilities associated with endpoints and workloads.

Components of the Carbon Black Cloud System

The boundaries of Carbon Black Cloud are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Carbon Black Cloud.

The components that directly support the services provided to customers are described in the subsections below.

INFRASTRUCTURE

The Carbon Black Cloud production system is hosted by a third-party provider at multiple locations. Carbon Black Cloud allows customers to select which region will host their service at the time of provisioning.

SOFTWARE

Carbon Black Cloud is a software application developed internally at VMware. There are many software and ancillary software products used to build, support, secure, maintain, and monitor Carbon Black Cloud.

PEOPLE

Carbon Black Cloud is managed by the following teams.

TEAM	DESCRIPTION
SBU Engineering	Responsible for development, documentation, and system test plans.
SBU Production Engineering team	Responsible for automation, upgrades and patch management, monitoring, maintenance, and troubleshooting.
SBU Product Security Team	Responsible for software and infrastructure as code security, vulnerability response and remediation, implementation of corporate security policies and services, assisting with compliance certification, security audits, and risk management of Carbon Black products and services.

Carbon Black Cloud is supported by the following Corporate teams:

TEAM	DESCRIPTION
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Human Resources	Responsible for human resources (HR) policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, pre-employment screening, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

ATTACHMENT A: Description of the Boundaries
of the System Provided by VMware Inc.



TEAM	DESCRIPTION
Security and Resiliency	Responsible for managing the enforcement, development, and maintenance of information security policies and standards to help ensure VMware Information Assets are preserved in a secure environment, in accordance with generally accepted best practices, focusing on VMware business and risk objectives.
Risk Management	Responsible for managing the annual performance of risk assessments, maintenance of a centralized risk register, and tracking and reporting of risk mitigation activities throughout the organization.
Enterprise Resiliency Business Continuity	Responsible for managing the organization's overall approach to business continuity, including the annual performance of Business Impact Assessments and testing and maintenance of Business Continuity Plans for VMware lines of business.
Security Operations Center	Responsible for intake of reported security events, including gathering, triaging, and providing first response. Security incidents are escalated to the VMware Security Incident Response Team.
Security Incident Response Team	Responsible for centrally managing all information security incidents for VMware, including ensuring proper collection of evidence, coordinating cross-functional incident teams, and developing effective response strategies for incident remediation.
Red Team	Responsible for performing penetration testing for VMware products and services, including tracking and escalation of remediation of test findings.
Data Center Operations	Responsible for managing the operations of VMware data center facilities, including reviewing and approving physical access and maintaining an inventory of physical assets.
Facilities Team	Responsible for performing regular equipment maintenance and managing the building management system for VMware data center facilities.
Global Support Services	Responsible for handling customer support issues and inquiries.
Colleague Support Team	Responsible for the distribution, replacement, and collection of VMware-issued end user devices.

PROCEDURES

VMware has established policies and procedures to support the achievement of its service commitments and the applicable AICPA Trust Services Categories and Criteria for Security . These include policies and procedures include guidance for how the service is designed and developed, how the system is operated, how the internal business systems are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific processes required in the operation and development of the service.

The Corporate Information Security Policies & Procedures are defined, approved, published, and communicated to users and relevant third parties. These documents are stored in a central repository accessible to employees and other appropriate staff and define the roles and responsibilities for the information security program. The information security policies are reviewed, updated, and approved at least annually to help ensure their continuing suitability and effectiveness.

DATA

Carbon Black Cloud does not store, process, or transmit critical data (i.e., data that is directly related to the transaction or business function between the customer and the business, such as card data, Personally Identifiable Information [PII], or financial details) on behalf of user entities to provide its function as a security solution. Furthermore, Carbon Black Cloud's data collection attributes can be configured by user entities to collect only the data that the user deems necessary for its business function and to exclude other data. All customers can be provided Carbon Black Data Collection Guides upon request.

Subservice Organization

The Company uses a subservice organization for application hosting services. The Company's controls related to Carbon Black Cloud cover only a portion of the overall internal controls for each user entity of Carbon Black Cloud. The description does not extend to the application hosting services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Controls are expected to be in place at the subservice organization related to physical security and environmental protection, as well as backup, recovery, redundancy controls related to availability. The subservice organization's physical security controls mitigate the risk of unauthorized access to the hosting facilities. The subservice organization's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management reviews the third-party examination reports for the subservice organization to assess its achievement of controls relevant to the entity's commitments. In addition, through its operational activities, Company management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to subservice organization management.

ATTACHMENT B:

Principal Service Commitments and System Requirements

Service Commitments and System Requirements

The processes and procedures managed by Carbon Black Cloud are implemented to help ensure the security of its service offering. Carbon Black Cloud has communicated its End User License Agreement commitments to customers within documentation posted on the publicly available VMware website.

VMware makes the following commitments regarding the security of information within service level agreements (“SLAs”) and the system description posted on the VMware website.

CATEGORY	PRINCIPAL SERVICE COMMITMENTS	RELATED SYSTEM REQUIREMENTS
Common Criteria Relevant to Security, Availability, and Confidentiality	<ul style="list-style-type: none"> • Protect the information systems used to deliver the service offering over which VMware has sole administrative level control. • Monitor security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the service over which VMware has sole administrative control. This responsibility stops at any point where the customer has some control, permission, or access to modify an aspect of the service. • Maintain the systems used to deliver the service, including the application of patches for the target systems. • Perform routine vulnerability scans to surface risk areas for the systems used to deliver the service offering and address vulnerabilities in a timely manner. • Encrypt production data at rest and while in transit. • Maintain commercially reasonable administrative, technical, organizational, and physical measures to protect the security of customer data against anticipated threats or hazards. • Maintain a security incident response plan. 	<ul style="list-style-type: none"> • Logical access standards • Employee provisioning and deprovisioning standards • Risk and vulnerability management standards • Incident handling standards • Change management standards • Vendor management
Availability	<ul style="list-style-type: none"> • Host production infrastructure within multiple geographically diverse data centers. 	<ul style="list-style-type: none"> • System monitoring • Backup and recovery standards

VMware has also identified control processes to help achieve their principal service commitments – the primary control processes for each commitment are summarized above as “Related System Requirements.”

Attachment F - VMware Carbon Black PS Consume Add-Ons Essentials

The following seven (7) pages contain information on key optional add-ons available.





VMware Carbon Black PS Consume Add-Ons Essentials

At a glance

Directed and managed by you, our Security Consultants bring VMware Carbon Black technology experience and best practices gained from hands-on experience and the collective knowledge of VMware Professional Services to help your team reach your desired outcomes faster.

Key benefits

- Skilled resources available to supplement customer teams
- Experts in VMware Carbon Black technologies
- Wide variety of assistance available

SKU

VSEC-CB-PS-ADDON-ESSL

Service Overview

VMware Professional Services provide you with seasoned Security Consultants, carefully matched to your requirements that become embedded, integral members of your team. We will provide a maximum of ten (10) consulting hours remotely for a duration of six (6) consecutive weeks.

Project Scope

VMware Security Consultants will work at the direction of the Customer and will have experience in their areas of focus. The assistance provided may focus on one (1) of the following VMware technologies:

Technology	Offshore (AMER, APJ, or EMEA)
VMware Carbon Black® Cloud (All Editions)	✓
VMware Carbon Black® App Control	✓*
VMware Carbon Black® EDR™ or CB Hosted EDR™	✓

Leverage Our Experts to Reach Your Goals Faster

The experts of VMware Professional Services can help you install, deploy, integrate, and operationalize VMware Carbon Black solutions. Call on them to help you accelerate project timelines, overcome challenges, empower your team via knowledge transfer, basically fill any gap where additional VMware Carbon Black knowledge and best practices would be useful.

You're in Charge; Set the Direction and We'll Make a Match

VMware Security Consultants are directed and managed by you; so you tell them what you'd like to achieve and they will help you get there.

Our ready workforce has a wide range of skill sets across the VMware Carbon Black portfolio of solutions and will be matched with your organization based on your unique objectives.

VMware Security Consultants can provide expert installation, configuration, usage, optimization, and administrative assistance. VMware Security Consultants may

perform the following VMware Carbon Black technology related tasks as time permits:

- Accelerate adoption, strengthen your team's capabilities, and sustain success
- Making recommendations for service-level and technical improvements that can encompass environments
- Product-specific knowledge transfer to your operational, engineering, and security teams
- Assisting with development of documentation of standard operating procedures for your environment
- Performance monitoring and tuning
- Health check, upgrade, and migration assistance

VMware Professional Services has the experience, best practices, proven methodologies, and deep knowledge of VMware technology that can help you reduce risk and complexity, minimize disruption, and experience predictable outcomes.

From deploying sensors and integrating your environment, to implementing operations and management, we can help you realize outcomes faster.

Our Security Consultants are armed with best practices that will help you expedite project completion, improve operational reliability and efficiency, and build the self-sufficiency of your team.

Frequently Asked Questions

Q. I need assistance with multiple VMware Carbon Black technologies. Will I need to purchase a separate SKU for each technology?

A. Not necessarily. The type and expertise of Security Consultant that will best meet your needs will be determined via a discussion with VMware Professional Services Sales.

Q. Can a Security Consultant help develop and design a new architecture?

A. No, Security Consultants are not focused on developing design and architecture.

Q. Can I add a Security Consultant to another service?

A. Yes, the Security Consultant can be added as a separate work stream to a primary service.

Service Assumptions

1. VMware makes no representation or warranty that the services provided will yield any specific deliverable(s) or assumed result(s). The Consultant's time delivered, and technical knowledge are the assumed requirements for fulfillment of the service.
2. The service will be provided for a duration of six (6) contiguous weeks, without pause for up to ten (10) consulting hours.
3. Customer may request to consume Security Consultant allocations planned in future weeks. Such requests will be granted based on resource availability.
4. Service will be initiated within 30 days of purchase.
5. VMware expects Customer to provide systems access as required for resource to perform activities and delays created by resource not having access will be the responsibility of Customer.
6. Customer is responsible for, and assumes any risk associated with any problems resulting from the content, completeness, accuracy and consistency of any data, materials and information supplied by the Customer.
7. Completion of any work will be limited by the resource allocated procured by the Customer.
8. VMware will assist with the installation/configuration of environment or feature type will be implemented based on the license type purchased by the Customer.
9. Any changes to the scheduling to compress the schedule will be mutually agreed and documented in writing.
10. Customer is responsible for ensuring configurations and policies align to their requirements. VMware will provide recommendations and assistance.
11. Configuration of software other than VMware software is the responsibility of the Customer.
12. Review of the settings and features will be provided throughout the configuration; however, formal training is out of scope.
13. Services or products that have been deprecated or reached end of life are out of scope.
14. Any work that may require custom configuration, scripting, or coding are out of scope.
15. Complex solution and architecture design is out of scope.
16. Pre-requisites must be completed for all components before any installation or configuration activities will be performed.
17. VMware reserves the right to assign Consultant(s) to the engagement in accordance with the skills levels required to perform the work described in this Datasheet.
18. VMware and the Customer will work closely together to ensure that project scope remains consistent, and issues are resolved in a timely manner.
19. All work will be delivered remotely via screen-share. On-site travel is out of scope.
20. All work will be conducted during VMware local business hours: 8am to 6pm UTC - 5:00 Eastern Time (US and Canada) or UTC +00:00 Dublin, London.
21. All work will be provided in English.

22. Any feature or technology not listed in Section 2. Activities is out of scope, unless agreed in writing with the Professional Services Team prior to purchase.
23. The scope of the services is deemed complete upon ONE of the following criteria - whichever comes first:
 - Upon consumption of the total resource allocation procured
 - After six (6) weeks from the date the project is initiated
 - The period of performance is limited to 12 months from purchase date

If the services were purchased using PSO credits, the services expire at the same time the credits expire unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Project Management

Customers that are engaging in a project and will leverage a resource on this effort should note that VMware will limit their project management responsibilities to the activities listed below. All other project management responsibilities and activities will be the Customer's responsibility as identified in the following table.

	VMware Responsibility	Customer Responsibility
Project Setup and Initiation		
Conduct kick-off conference call with key stakeholders and Project Team	✓	n
Develop high-level project schedule and contact list	n	✓
Develop project plan	n	✓
Scope Management		
Identify and manage any activities associated with Customer's project	n	✓
Identify and maintain a Work Breakdown Structure (WBS) of any activities	n	✓
Schedule Management		
Create, maintain, and manage a project schedule	n	✓
Financial Management		
Track and manage project time	n	✓
Review invoices for accuracy	✓	n
Quality Management		
Establish and execute Customer's project readiness at key checkpoints	n	✓
Identify, manage, and document requirements for user testing, operational readiness, or process changes	n	✓
Risk and Issue Management		
Track and manage project issues and risks (product, process or technical)	n	✓
Resource Management		
Identify and assign qualified VMware resources	✓	n
Define, document, and manage a project resource plan if required	n	✓
Integrate VMware and Customer resources into the project schedule	n	✓
Manage and identify any changes to resource skills and communicate to VMware	n	✓
Identify and execute project change request for a different skill set if a change is required	✓	✓
Communications Management		
Weekly VMware status report(s)	✓	n
Weekly status meeting(s)	n	✓
Facilitate, host, and manage Customer meeting(s)	n	✓

Attend periodic stakeholder meeting(s)	n	✓
Host executive update(s)	n	✓
Project Closure		
Host a project closure conference call	n	✓
Complete a Customer Satisfaction Survey	n	✓
Facilitate "Lessons Learned" session	n	✓

Learn more

Visit vmware.com/services.

Customer Responsibilities

Customer is responsible for task assignment and prioritization of the supplied resource(s).

VMware Responsibilities

VMware will provide the resource(s) described in this Datasheet.

Terms and conditions

This datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. All VMware service engagements are governed by the VMware Professional Services [General Terms and Conditions](#). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.

Attachment G – VMware Carbon Black EDR Administrator

The following two (2) pages contain additional training information.





VMware Carbon Black EDR Administrator

Course Overview

This one-day course teaches you how to use the VMware Carbon Black® EDR™ product and leverage the capabilities to configure and maintain the system according to your organization's security posture and policies.

This course provides an in-depth, technical understanding of the Carbon Black EDR product through comprehensive coursework and hands-on scenario-based labs.

Course Objectives

By the end of the course, you should be able to meet the following objectives:

- Describe the components and capabilities of the Carbon Black EDR server
- Identify the architecture and data flows for Carbon Black EDR communication
- Describe the Carbon Black EDR server installation process
- Manage and configure the Carbon Black EDR sever based on organizational requirements
- Perform searches across process and binary information
- Implement threat intelligence feeds and create watchlists for automated notifications
- Describe the different response capabilities available from the Carbon Black EDR server
- Use investigations to correlate data between multiple processes

Target Audience

System administrators and security operations personnel, including analysts and managers

Prerequisites

There are no prerequisites for this course.

Course Delivery Options

- Classroom
- Live Online
- [Onsite](#)
- [On Demand](#)

Product Alignment

- VMware Carbon Black EDR

Course Modules

- 1 Course Introduction
 - Introductions and course logistics
 - Course objectives
- 2 Planning and Architecture
 - Hardware and software requirements
 - Architecture
 - Data flows
 - Server installation review
 - Installing sensors
- 3 Server Installation & Administration
 - Configuration and settings
 - Carbon Black EDR users and groups
- 4 Process Search and Analysis
 - Filtering options
 - Creating searches
 - Process analysis and events
- 5 Binary Search and Banning Binaries
 - Filtering options
 - Creating searches
 - Hash banning
- 6 Search best practices
 - Search operators
 - Advanced queries
- 7 Threat Intelligence
 - Enabling alliance feeds
 - Threat reports details
 - Use and functionality
- 8 Watchlists
 - Creating watchlists
 - Use and functionality
- 9 Alerts / Investigations / Response
 - Using the HUD
 - Alerts workflow
 - Using network isolation
 - Using live response

Contact

If you have questions or need help registering for this course, click [here](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
© 2020 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.

Addendum to Mainline Response to Florida DMS RFQ DMS-2223-155

Mainline presents the following information to the State for clarification of pricing included in Mainline's original response to the State of Florida DMS RFQ DMS-2223-155 as well as information clarifying transferability. Mainline has also included VMware's end user terms.

Transferability

VMware Carbon Black is modular, and subscription based; license transfer from end customer to affiliate is permitted and license transfer from end customer to a customer divested entity is permitted with business operations approval. The transferring party agrees to transfer to transferee all software, including any and all associated materials, such as media, manuals, proof-of-purchase certificates, software critical bug notices (if any), upgrades, patches, and updates of software (and any copies thereof). The transferee shall accept the aforesaid software and materials transferred from the transferring party and transferee agrees to comply with all the terms specified in the applicable order and the applicable license agreement and/or partner agreement in place between the transferee and Carbon Black. The transferee acknowledges and agrees that, unless transferee has a negotiated master agreement with Carbon Black for the purchase of the software, transferee's use of the software is subject to the EULA or Terms of Service (as applicable), and that such EULA or Terms of Service governs the transferee's use of the software. Licenses must be transferred before time of renewal. Expired licenses cannot be transferred.

Pricing

Mainline has included a revised pricing table. An Excel spreadsheet has also been provided.

Mainline is a remarketer of third-party hardware, software products, and maintenance support services. Performance of hardware, software products, and maintenance support services are subject to the applicable end user terms for such and may be subject to a third-party agreement between the end user and VMware.

A copy of VMware's general terms and conditions has been included on the following six (6) pages.





VMWARE GENERAL TERMS

Last updated: 16 June 2022

By downloading or using an Offering, Customer agrees to be bound by the terms of the Agreement.

1. OFFERINGS.
 - 1.1. Applicable Terms. The terms of the Order and these General Terms, including applicable Exhibits and Offering-specific Notes (collectively, the "Agreement") govern Customer's use of the Offerings. The following descending order of precedence applies: (a) the Order; (b) the General Terms; (c) the Exhibits; and (d) the Offering-specific Notes.
 - 1.2. Users. Customer is responsible for its Users' compliance with the Agreement.
 - 1.3. Restrictions. Customer may use the Offerings only for its internal use and for the benefit of its Affiliates. Affiliates may not use the Offerings. Customer may not resell or sublicense its rights to the Offerings. Customer may not use the Offerings in an application service provider, service bureau, hosted IT service, or similar capacity for third parties.
 - 1.4. Benchmarking. Customer may use the Offerings to conduct internal performance testing and benchmarking studies. Customer may only publish or distribute study results with VMware's approval. Customer may submit requests to VMware by emailing benchmark@vmware.com.
 - 1.5. Evaluations. Evaluations are for 30 days (unless VMware specifies otherwise in writing). Customer may not have access to data in the Evaluation after it ends. Evaluations are provided "AS IS" without indemnification, support, service level commitment, or warranty of any kind, express or implied.
2. ORDERS AND PAYMENTS.
 - 2.1. Orders. Orders are binding when VMware accepts them, which is deemed to occur on Delivery.
 - 2.2. Purchase Orders. Purchase orders do not have to be signed to be valid. Terms contained in any purchase order or other business form do not apply.
 - 2.3. No Refunds. All Orders are non-refundable and non-cancellable except as expressly provided in the Agreement.
 - 2.4. Overages. Customer must pay all fees for use of the Offerings, including amounts for add-on features and fees incurred based on usage. VMware may bill Customer directly for metered or overage fees, even if Customer originally purchased the Offerings through a VMware authorized reseller.
 - 2.5. Direct Orders. This section 2.5 (Direct Orders) applies only to Orders placed directly with VMware. If Customer purchases entitlements to the Offerings through a VMware authorized reseller, different terms regarding invoicing, payment, and taxes may apply.
 - 2.5.1. Payments. Except as listed in an Order, fees for the Offerings will be governed by the applicable price list at the time of invoicing. Customer must pay all undisputed fees and approved expenses within 30 days from the date of invoice. After 30 days, interest will accrue at the lesser of 1.5% per month or the highest lawful rate.
 - 2.5.2. Disputes. To dispute any fees in good faith, Customer must notify VMware in writing of the reasons for the dispute before the payment due date. The parties must negotiate in good faith to resolve the dispute as soon as reasonably practicable. VMware will not suspend or terminate Customer's access to any Offering because of any unpaid, disputed fees while Customer and VMware are negotiating to resolve the dispute.
 - 2.5.3. Taxes. Fees are exclusive of Taxes. Customer must pay or reimburse VMware for all Taxes. If Customer is required to withhold any Tax, Customer must gross up its payments so that VMware receives all sums due in full. If Customer's address is outside of the United States, VMware will treat the Customer's "bill to" address as the place of supply for VAT purposes.
3. TERM.
 - 3.1. Term. The Agreement applies to the Offerings from the effective date of the Order until the expiration or termination of Customer's entitlement to the Offerings as set forth in this Agreement.
 - 3.2. Temporary Suspension. In the event of a security risk to a Service or its users, VMware may suspend Customer's use of that Service.
 - 3.3. Termination for Cause. Either party may terminate the Agreement (in whole or in part) or Customer's entitlement to an Offering under the Agreement effective immediately upon written notice if the other party: (a) materially breaches any provision of the Agreement and fails to cure within 30 days after receiving written notice; or (b) becomes insolvent or subject to any form of bankruptcy proceeding.



- 3.4. Effect of Termination. Upon termination of the Agreement or part of it: (a) all entitlements to the applicable Offerings immediately end; (b) Customer must stop using, and destroy any copies of, those Offerings; and (c) each party must return or destroy any Confidential Information of the other party in its control (other than information that must be retained by law). Any provision that is intended by the parties to survive termination of the Agreement will survive.
4. CONFIDENTIAL INFORMATION.
- 4.1. Protection. Recipient must protect Discloser's Confidential Information with at least the same care as it protects its own Confidential Information but not less than reasonable care. Recipient may not use Discloser's Confidential Information except to exercise its rights and perform its obligations under the Agreement. Recipient may disclose Confidential Information only to Recipient's Affiliates, employees and contractors who need to know the Confidential Information for purposes of the Agreement and who have a duty of confidentiality no less restrictive than this section 4 (Confidential Information).
- 4.2. Exceptions. Recipient's obligations under section 4.1 (Protection) do not apply if the information: (a) is rightfully known by Recipient at the time of disclosure without any obligation of confidentiality; (b) is lawfully disclosed to Recipient by a third party without confidentiality restrictions; (c) becomes publicly available through no fault of Recipient; or (d) is independently developed by Recipient without access to or use of Discloser's Confidential Information.
- 4.3. Injunctive Relief. Nothing in the Agreement limits a party's right to seek equitable relief for breach of this section 4 (Confidential Information).
5. OWNERSHIP.
- 5.1. Customer Content. Customer retains all Intellectual Property Rights in and to Customer Content.
- 5.2. VMware IP. VMware retains all Intellectual Property Rights in and to the Offerings, including any improvements, enhancements, modifications, and derivative works. If Customer provides any feedback about the Offerings, VMware may use that feedback without restriction.
- 5.3. Reservation of Rights. Except as expressly stated in the Agreement, the Agreement does not grant either party any rights, implied or otherwise, to the other party's content or intellectual property.
6. LIMITED WARRANTIES.
- 6.1. Software and Cloud Services. VMware warrants that Software and Cloud Services will substantially conform with the Documentation: (a) for Software, for 90 days following Delivery; or (b) for Cloud Services, for the Subscription Term. Customer must properly install and use the Offerings without modification and in accordance with the Documentation. Customer must notify VMware of an alleged breach of this warranty within the applicable warranty period. As Customer's sole remedy for a breach of this warranty, VMware must either: (1) correct any reproducible error in the Software or Cloud Service; or (2) terminate the Software or Cloud Service and refund applicable license fees (for Software) or unused, prepaid fees (for Cloud Services).
- 6.2. Professional Services and Support Services. VMware warrants that Professional Services and Support Services will be performed in a professional manner following industry standards. Customer must notify VMware within 30 days of an alleged breach of this warranty. As Customer's sole remedy for a breach of this warranty, VMware must either: (a) rectify the breach; or (b) terminate the applicable Service and refund any unused, prepaid fees for that Service.
- 6.3. Disclaimer of Warranties. Except for the limited warranties in this section 6 (Limited Warranties), to the maximum extent permitted by law, VMware, for itself and on behalf of its suppliers, disclaims all warranties and conditions whether express, implied, or statutory, including any warranties of merchantability, satisfactory quality, fitness for a particular purpose, title, non-infringement, and any warranty arising from course of dealing or course of performance, relating to the Offerings. Neither VMware nor its suppliers warrant that the Offerings will operate uninterrupted, that Offerings will be free from defects or errors, or that the Offerings will meet (or are designed to meet) Customer's requirements.
7. INDEMNIFICATION.
- 7.1. Defense and Indemnification. Subject to the remainder of this section 7 (Indemnification), VMware will: (a) defend Customer against any Infringement Claim; and (b) indemnify Customer from amounts finally awarded against Customer by a court of competent jurisdiction or a government agency, or agreed to in a settlement, for the Infringement Claim.
- 7.2. Requirements. Customer must provide VMware with prompt notice of any Infringement Claim and reasonably cooperate with VMware's requests for assistance. VMware will have sole control of the defense and settlement of the Infringement Claim.



- 7.3. Exclusions. VMware has no obligation under this section 7 (Indemnification) with respect to an Infringement Claim based on: (a) combination of Indemnified Materials with non-VMware materials; (b) use of an older version of Indemnified Materials when use of a newer version would have avoided the infringement; (c) any modification to Indemnified Materials other than those made by VMware; (d) any Deliverable provided by VMware in accordance with Customer's specifications; (e) any claim relating to open source software or freeware technology that is not embedded by VMware into the Offerings; or (f) any Indemnified Material provided on a no-charge, beta, or evaluation basis.
- 7.4. Remedies. If Indemnified Materials become, or in VMware's reasonable opinion are likely to become, the subject of an Infringement Claim, VMware must, at its option and expense, either: (a) procure the necessary rights for Customer to keep using the Indemnified Materials; or (b) modify or replace the Indemnified Materials to make them non-infringing. If those remedies are not commercially feasible, VMware may terminate Customer's entitlement to the Indemnified Materials and refund any applicable:
- (1) prepaid fees for Cloud Services or Subscription Software, prorated for the remaining portion of the then-current Subscription Term;
 - (2) fees paid for Perpetual Licenses or Deliverables, less straight-line depreciation over a three-year useful life; and
 - (3) unused, prepaid fees for discontinued Support Services.
- 7.5. Sole Remedy. This section 7 (Indemnification) states Customer's sole remedy and VMware's entire liability for Infringement Claims.
8. LIMITATION OF LIABILITY.
- 8.1. Disclaimer. To the maximum extent permitted by law, neither party will be liable for lost profits or business opportunities, loss of use, loss of data, loss of goodwill, business interruption, or any indirect, special, incidental, or consequential damages under any theory of liability. This limitation will apply regardless of whether a party has been advised of the possibility of those damages and regardless of whether any remedy fails of its essential purpose.
- 8.2. Cap on Monetary Liability. Each party's aggregate liability under this Agreement will not exceed amounts paid or payable by Customer for the Offering giving rise to the claim in the 12 months prior to the event giving rise to the claim, except for Perpetual Licenses, where each party's aggregate liability will not exceed the license fees paid for the Software giving rise to the claim. VMware's aggregate liability for an Evaluation will not exceed \$5,000 USD.
- 8.3. Exclusions. The limitations of liability in sections 8.1 (Disclaimer) and 8.2 (Cap on Monetary Liability) will not apply to: (a) VMware's indemnification obligations under section 7 (Indemnification); (b) either party's infringement of the other party's Intellectual Property Rights; (c) Customer's violation of section 2 of the Cloud Services Exhibit (Acceptable Use); or (d) any liability that may not be limited by law.
- 8.4. Further Limitations. VMware's liability for any third-party software embedded into the Software or Cloud Services is subject to this section 8 (Limitation of Liability). VMware's suppliers have no liability under the Agreement, and Customer may not bring claims directly against them. VMware has no liability with respect to any Third-Party Content.
9. DATA USE AND PRIVACY.
- 9.1. Personal Data. If VMware acts as a processor of Personal Data, VMware will process Personal Data in accordance with the Data Processing Addendum.
- 9.2. Account, Operations, and Usage Data. VMware collects Customer contact and purchase information to manage Customer's account and to fulfill Orders. VMware also processes: (a) information necessary to facilitate delivery and operation of the Offerings, verify compliance with the terms of the Agreement, invoice, and provide Support Services; and (b) configuration, performance, and usage data to improve VMware products and services, and other analytics purposes as detailed in the Offering-specific Notes. To the extent any of that data includes information that identifies an individual, VMware will process that information in accordance with VMware's Products & Services Privacy Notice available at www.vmware.com/help/privacy.html.
- 9.3. Support Requests and Professional Services. Customer is responsible for taking steps necessary to protect any sensitive information or Personal Data that it provides to VMware while receiving Support Services or Professional Services. Those steps may include obfuscating or removing such information or working with VMware at the time of submission to limit disclosure.
- 9.4. Required Disclosures. VMware may disclose Customer Content or Confidential Information if VMware is required by law or by order of a judicial or administrative body of competent jurisdiction



(a “Demand”). Unless legally prohibited from doing so, VMware must provide Customer with notice and a copy of the Demand. If the Demand relates to Cloud Services, VMware must (i) inform the relevant authority that VMware is a service provider acting on Customer’s behalf and all requests for access to Customer Content should be directed in writing to the contact Customer identifies (or if no contact is timely provided, to Customer’s legal department) and (ii) only provide access to Customer Content with Customer’s authorization. If Customer requests and at Customer’s expense, VMware must take reasonable steps to contest the Demand. If VMware is legally prohibited from notifying Customer of the Demand, VMware must evaluate the validity of the Demand, and, if VMware does not believe the Demand is legal, VMware must challenge the Demand. VMware must limit the scope of any disclosure to the minimum information required to comply with the Demand.

10. OPEN SOURCE SOFTWARE. Open source software is licensed to Customer under the open source software’s own applicable license terms, which can be found in either the open_source_licenses.txt file accompanying the Offerings, the Documentation, or at www.vmware.com/download/open_source.html. These license terms are consistent with the license granted in the Agreement and may contain additional rights benefiting Customer. The open source license terms take precedence over the Agreement to the extent that the Agreement imposes greater restrictions on Customer than the applicable open source license terms. To the extent the license for any open source software requires VMware to make the corresponding source code and/or modifications (the “Source Files”) available to Customer, Customer may obtain a copy of the applicable Source Files at www.vmware.com/download/open_source.html or by sending a written request, with name and address, to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date Customer acquires its entitlement to the Offering.
11. MISCELLANEOUS.
 - 11.1. Transfer and Assignment. Customer may not assign the Agreement or any Order without VMware’s consent. Once validly assigned, the Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.
 - 11.2. Notice. All notices must be in writing. Notices to Customer will be given: (a) by email to the email address associated with Customer’s account, if Customer has subscribed to email notices; or (b) by posting in the VMware customer portal. Legal notices to VMware will be given to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.
 - 11.3. Waiver. Waiver of a breach of the Agreement will not constitute a waiver of any later breach.
 - 11.4. Severability. If any part of the Agreement is held to be invalid or unenforceable, all remaining provisions will remain in force to the extent feasible to effectuate the intent of the parties.
 - 11.5. Insurance. VMware will carry insurance for the term of the Agreement. VMware’s Memorandum of Insurance may be viewed at www.vmware.com/agreements.
 - 11.6. Compliance with Laws. Each party must comply with all applicable laws.
 - 11.7. Export Control. The Offerings are subject to the U.S. Export Administration Regulations (including “deemed export” and “deemed re-export” regulations), and may be subject to the export control laws of other countries. Customer represents and warrants that: (a) Customer and any User, are not, and are not acting on behalf of: (1) any person who is a citizen, national, or resident of, or who is controlled by, the government of any country to which the United States has prohibited export transactions; or (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List, or any similar applicable designated persons list; (b) Customer, and any User, will not permit the Offerings to be used for any purposes prohibited by law, including any prohibited development, design, manufacture, or production of missiles or nuclear, chemical, or biological weapons; and (c) Customer, and any User, are not subject, either directly or indirectly, to any order issued by any agency of the United States government revoking or denying, in whole or in part, Customer’s United States export privileges. Customer must notify VMware promptly if Customer or any User becomes subject to any order of that type.
 - 11.8. Governing Law. The Agreement is governed by the laws of the State of California and U.S. federal laws, if the billing address for Customer’s Order is in the United States, and by the laws of Ireland if the billing address for Customer’s Order is outside the United States. Conflict of law rules are expressly disclaimed. The United Nations Convention on Contracts for the International Sale of Goods does not apply.
 - 11.9. U.S. Public Sector End User. If Customer is a U.S. Public Sector End User, the U.S. Public Sector Exhibit available at www.vmware.com/agreements supersedes or modifies the referenced provisions of the Agreement.



- 11.10. Third Party Rights. Other than as expressly stated, the Agreement does not create any rights for any person who is not a party to it. Only persons who are parties to the Agreement may enforce or rely on any of its terms.
- 11.11. Force Majeure. Except for Customer's payment obligations, neither party will be liable for any delay or failure to perform due to any cause beyond the party's reasonable control, including labor disputes, industrial disturbances, systemic utility failures, acts of nature, pandemics, embargoes, riots, government orders, acts of terrorism, or war.
- 11.12. No Agency. Nothing in the Agreement is intended to constitute a fiduciary relationship, agency, joint venture, partnership, or trust between the parties. No party has authority to bind the other party.
- 11.13. Translation. This non-English version of these General Terms is provided only as a courtesy, and Customer's use of the Offerings is governed by the English version of these General Terms, published at www.vmware.com/agreements.
- 11.14. Counterparts. The Agreement may be signed electronically or in counterparts, in which case each signed copy will be deemed an original as though both signatures appeared on the same document.
- 11.15. Entire Agreement. The Agreement contains the entire agreement of the parties and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings, and agreements, whether written or oral, between the parties regarding its subject matter. The Agreement may be amended only in writing and signed by both parties.
12. DEFINITIONS.

Affiliate means an entity that is directly or indirectly controlled by, is under common control with, or controls that party, where "control" means an ownership, voting, or similar interest representing more than 50% of the total interests outstanding of that entity at that time.

Cloud Service means the VMware cloud service specified in Customer's Order.

Cloud Services Guide means the then-current VMware Cloud Services Guide, available at www.vmware.com/agreements.

Confidential Information means information or materials provided by a party ("Discloser") to the other party ("Recipient") that: (a) is in tangible form and labelled "confidential" or similar; or (b) information which a reasonable person knew or should have known to be confidential. Confidential Information includes: (1) license keys; (2) VMware pricing, product roadmaps or strategic marketing plans; (3) non-public materials relating to the Offerings; and (4) Customer Login Credentials.

Customer means the entity identified in the Order as "Customer".

Customer Content means content uploaded by Customer or any User into the Cloud Service or provided to VMware as a part of Support Services, but does not include Third-Party Content or account information. For purposes of this definition, "content" means any data, including all text, sound, video, or image files, and software (including machine images).

Data Processing Addendum means the then-current VMware Data Processing Addendum, available at www.vmware.com/agreements.

Deliverables means any reports, analyses, scripts, templates, code, or other work results delivered by VMware as specified in the applicable SOW for Professional Services.

Delivery means: (a) for Cloud Services, when VMware emails the Login Credentials to the email address associated with Customer's account; (b) for Software, when VMware notifies Customer of availability of Software for download; (c) for Support Services, upon VMware's issuance of an invoice for those Support Services; (d) for Professional Services, as specified in the applicable SOW; (e) for purchasing program credits, when VMware makes the fund balance available in the applicable portal; and (f) for shipping and delivery of physical objects, Ex Works VMware's regional fulfillment facility (INCOTERMS 2020™).

Documentation means the product documentation describing the features, functionality, and use of the Offerings published and updated by VMware from time to time at docs.vmware.com.

Evaluation means an Offering (or part of an Offering) made available free of charge, for evaluation, trial, proof of concept, or similar purpose.

Exhibits means the exhibits to these General Terms (Software, Cloud Services, Professional Services, U.S. Federal, and VMware Entities) available at www.vmware.com/agreements.

Indemnified Materials means the Cloud Services, Software, and Deliverables.



Infringement Claim means any claim by a third party that the Indemnified Materials infringe any patent, trademark, or copyright of that third party, or misappropriate a trade secret (only to the extent that misappropriation is not a result of Customer's actions).

Intellectual Property Rights means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, know-how, inventions, patents, patent applications, moral rights, and all other proprietary rights, whether registered or unregistered.

Login Credentials means any passwords, authentication keys, or security credentials that enable Customer's access to and management of the Cloud Service.

Offering(s) means, collectively, Services or Software.

Offering-specific Notes means the applicable license notes or services notes found in the Product Guide, the Cloud Services Guide, and the Support Services Guide.

Order means an enterprise order, SOW, quote, or other ordering document for Offerings, issued by Customer to VMware or to Customer's VMware authorized reseller and accepted by VMware described in section 2 of these General Terms (Orders and Payments).

Perpetual License means a license to the Software with a perpetual term.

Personal Data is defined in the Data Processing Addendum.

Product Guide means VMware's then-current Product Guide available at www.vmware.com/agreements.

Professional Services means those services described in the applicable SOW.

Service Level Agreement means the then-current version of the applicable service level agreement for a Cloud Service, available at www.vmware.com/agreements.

Service(s) means Cloud Services, Support Services, or Professional Services.

Software means the VMware computer programs that Customer licenses under an Order, together with any related software code VMware provides as part of Support Services and that is not subject to a separate license agreement.

SOW means a written agreement between Customer and VMware containing project-specific details of the Professional Services or VMware online datasheet.

Subscription Software means Software that is licensed for a specific term.

Subscription Term means the period Customer is permitted to use a Cloud Service or Subscription Software, stated in the applicable Order. For any on-demand Cloud Services, Subscription Term means the period during which Customer uses the Cloud Service.

Support Services means VMware support and subscription services that are purchased under an Order or included with purchase of Subscription Software or Cloud Services.

Support Services Guide means VMware's then-current Support Services Guide, available at www.vmware.com/agreements.

Tax means any sales, consumption, VAT, GST, use, gross receipts, business and occupation, withholding, and other taxes (other than taxes on VMware income), export and import fees, customs duties, and similar fees imposed by any government or other authority.

Third-Party Agent means a third party delivering information technology services to Customer under a contract with Customer.

Third-Party Content means content provided by a third party that interoperates with a Cloud Service, but that is not part of the Cloud Service. Third-Party Content is optional and is subject to the third-party terms accompanying the Third-Party Content.

U.S. Public Sector End User means a U.S. Federal End User or a U.S. State or Local Government End User, as those terms are defined in the U.S. Public Sector Exhibit.

User means an employee, contractor, or Third-Party Agent that Customer authorizes to use the Offerings as permitted under the Agreement or under Customer's Login Credentials.

VMware means VMware, Inc., a Delaware corporation, if the billing address for the Order is in the United States, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for the Order is outside the United States, except if the billing address for the Order is in the United Kingdom, Australia, or New Zealand or the Pacific Islands, in which case VMware means the applicable entity identified in the VMware Entities Exhibit found at www.vmware.com/agreements.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 1. Purchase Order.

A. Composition and Priority.

The Contractor agrees to provide commodities or contractual services to the Agency within the manner and at the location specified in the Purchase Order, and any attachments to the Purchase Order. These Purchase Order Terms and Conditions, whether generic or specific, shall take precedence over any inconsistent or conflicting provision in the State of Florida, General Contract Conditions, PUR 1000. Additionally, the terms of the Purchase Order supersede the terms of any and all prior agreements with respect to this purchase.

B. Initial Term.

Unless otherwise specified, the Purchase Order begins on the date of issuance. Contractual services or commodities to be provided by the Contractor shall be completed by the date specified on the Purchase Order end date.

Section 2. Performance.

A. Performance Standards.

The Contractor agrees to perform all tasks and provide deliverables as set forth in the Statement of Work and attachments to the Purchase Order. The Agency shall be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof. Coordination shall be maintained by the Contractor with representatives of the Agency, or of other agencies involved in the project on behalf of the Agency.

B. Performance Deficiency.

If the Agency determines that the performance of the Contractor is unsatisfactory, the Agency may notify the Contractor of the deficiency to be corrected, which correction shall be made within a time-frame specified by the Agency. The Contractor shall provide the Agency with a corrective action plan describing how the Contractor will address all issues of contract non-performance, unacceptable performance, and failure to meet the minimum performance levels, deliverable deficiencies, or contract non-compliance. If the corrective action plan is unacceptable to the Agency, the Contractor will be assessed a non-performance retainage equivalent to 10% of the total invoice amount or as specified in the contractual documents. The retainage will be applied to the invoice for the then-current billing period. The retainage will be withheld until the Contractor resolves the deficiency. If the deficiency is subsequently resolved, the Contractor may invoice the Agency for the retained amount during the next billing period. If the Contractor is unable to resolve the deficiency, the funds retained will be forfeited.

Section 3. Payment and Fees.

A. Payment Invoicing.

The Contractor will be paid upon submission of properly certified invoice(s) to the Agency after delivery and acceptance of commodities or contractual services is

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

confirmed in writing by the Agency. Invoices shall contain detail sufficient for audit thereof and shall contain the Purchase Order and the Contractor's Federal Employer Identification Number or Social Security Number.

B. Payment Timeframe.

Section 215.422, Florida Statutes (F.S.), provides that agencies have five (5) working days to inspect and approve commodities or contractual services. Items may be tested for compliance with specifications. Items delivered not conforming to specifications may be rejected and returned at the Contractor's expense. Interest penalties for late payment are also provided for in section 215.422, F.S. A Vendor Ombudsman, whose duties include acting as an advocate for Vendors who may be experiencing problems obtaining timely payment(s) from an Agency, may be contacted at 850-413-5516, or Vendors may call the State Comptroller's Hotline at 1-800-848-3792.

C. MyFloridaMarketPlace Fees.

The following language is included pursuant to rule 60A-1.031, Florida Administrative Code:

The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), Florida Statutes. Payments issued by Agencies or Eligible Users to Vendors for purchases of commodities or contractual services are subject to Transaction Fees, as prescribed by rule 60A-1.031, Florida Administrative Code, or as may otherwise be established by law. Vendors shall submit monthly reports required by the rule. All reports shall be subject to audit. Failure to pay Transaction Fees or submit reports shall constitute grounds for default and exclusion from business with the State of Florida.

D. Payment Audit.

Records of costs incurred under terms of the Purchase Order shall be maintained and made available to the Agency upon request at all times during the period of the Purchase Order, and for a period of three years thereafter. Records of costs incurred shall include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Agency for audit.

E. Annual Appropriation and Travel.

Pursuant to section 287.0582, F.S., if the Purchase Order binds the State or an executive agency for the purchase of services or tangible personal property for a period in excess of one (1) fiscal year, the State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature. Travel expenses are not reimbursable unless specifically authorized in writing, and shall be reimbursed only in accordance with section 112.061, F.S.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Section 4. Liability.

A. Indemnity.

To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the State of Florida, its officers, employees and agents harmless from all fines, claims, assessments, suits, judgments, or damages, consequential or otherwise, including court costs and attorney's fees, arising out of any acts, actions, breaches, neglect or omissions of the Contractor, its employees, agents, subcontractors, assignees or delegates related to the Purchase Order, as well as for any determination arising out of or related to the Purchase Order, that the Contractor or Contractor's employees, agents, subcontractors, assignees or delegates are not independent contractors in relation to the Agency. The Purchase Order does not constitute a waiver of sovereign immunity or consent by the Agency or the State of Florida or its subdivisions to suit by third parties.

B. Payment for Claims.

The Contractor guarantees the payment of all just claims for materials, supplies, tools, or labor and other just claims against the Contractor or any employee, agent, subcontractor, assignee or delegate in connection with the Purchase Order.

C. Liability Insurance.

The Contractor shall maintain insurance sufficient to adequately protect the Agency from any and all liability and property damage/hazards which may result from the performance of the Purchase Order. All insurance shall be with insurers qualified and duly licensed to transact business in the State of Florida. If required by the Agency and prior to commencing any work the Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in full force and showing the Agency to be an additional insured.

D. Workers' Compensation.

The Contractor shall maintain Workers' Compensation insurance as required under the Florida Workers' Compensation Law.

E. Performance Bond.

Unless otherwise prohibited by law, the Agency may require the Contractor to furnish, without additional cost to the Agency, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Agency shall determine the type and amount of security.

Section 5. Compliance with Laws.

A. Conduct of Business.

The Contractor shall comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor shall comply with Section 247A of the Immigration and Nationality Act, the

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

Americans with Disabilities Act, Health Insurance Portability and Accountability Act, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status.

Pursuant to subsection 287.058(1), F.S., the provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference, to the extent applicable.

B. Lobbying.

In accordance with sections 11.062 and 216.347, F.S., the Purchase Order funds are not for the purpose of lobbying the Legislature, the judicial branch, or an Agency. Pursuant to subsection 287.058(6), F.S., the Purchase Order does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Purchase Order, after the Purchase Order's execution and during the Purchase Order's term.

C. Gratuities.

The Contractor shall not, in connection with this or any other agreement with the State, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State officer or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State officer or employee.

D. Cooperation with Inspector General.

Pursuant to subsection 20.055(5), F.S., Contractor, and any subcontractor to the Contractor, understand and will comply with their duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor shall provide any type of information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but shall not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Purchase Order. The Contractor shall retain such records for three (3) years after the expiration of the Purchase Order, or the period required by the General Records Schedules maintained by the Florida Department of State (available at: <http://dos.myflorida.com/library-archives/records-management/general-records-schedules/>), whichever is longer. The Contractor agrees to reimburse the State for the reasonable costs of investigation incurred by the Inspector General or other authorized State official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State which results in the suspension or debarment of the Contractor. Such costs shall include, but shall not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees.

E. Public Records.

To the extent required by the Florida Public Records Act, Chapter 119, F.S., the Contractor shall maintain and allow access to public records made or received in

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

conjunction with the Purchase Order. The Purchase Order may be terminated for cause by the Agency for the Contractor's refusal to allow access to public records.

F. Communications and Confidentiality.

The Contractor agrees that it shall make no statements, press releases, or publicity releases concerning the Purchase Order or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Purchase Order, or any particulars thereof, during the period of the Purchase Order, without first notifying the Agency's Contract Manager or the Agency's designated contact person and securing prior written consent. The Contractor shall maintain confidentiality of all confidential data, files, and records related to the services and/or commodities provided pursuant to the Purchase Order and shall comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures shall be consistent with the most recent version of the Agency's security policies, protocols, and procedures. The Contractor shall also comply with any applicable professional standards with respect to confidentiality of information.

G. Intellectual Property.

Unless specifically addressed in the Purchase Order, intellectual property rights to all property created or otherwise developed by the Contractor for the Agency will be owned by the State of Florida through the Agency at the completion of the Purchase Order. Proceeds to any Agency derived from the sale, licensing, marketing or other authorization related to any such Agency-controlled intellectual property right shall be handled in the manner specified by applicable state statute.

H. Convicted and Discriminatory Vendor Lists.

In accordance with sections 287.133 and 287.134, F.S., an entity or affiliate who is on the Convicted Vendor List or the Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Purchase Order with any Agency.

Section 6. Termination.

A. Termination for Convenience.

The Purchase Order may be terminated by the Agency in whole or in part at any time in the best interest of the Agency. If the Purchase Order is terminated before performance is completed, the Contractor shall be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Purchase Order price as the amount of work satisfactorily performed. All work in progress shall become the property of the Agency and shall be turned over promptly by the Contractor.

B. Termination for Cause.

If the Agency determines that the performance of the Contractor is not satisfactory, the Agency shall have the option of (a) immediately terminating the Purchase Order, or (b)

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

notifying the Contractor of the deficiency with a requirement that the deficiency be corrected within a specified time, otherwise the Purchase Order will be terminated at the end of such time, or (c) take other action deemed appropriate by the Agency.

Section 7. Subcontractors and Assignments.

A. Subcontractors.

The Contractor shall not subcontract any work under the Purchase Order without the prior written consent of the Agency. The Contractor is fully responsible for satisfactory completion of all subcontracted work.

B. Assignment.

The Contractor shall not sell, assign or transfer any of its rights, duties or obligations under the Purchase Order without the prior written consent of the Agency. In the event of any assignment, the Contractor remains secondarily liable for performance of the Purchase Order, unless the Agency expressly waives such secondary liability. The Agency may assign the Purchase Order with prior written notice to the Contractor.

Section 8. RESPECT and PRIDE.

A. RESPECT.

In accordance with subsection 413.036(3), F.S., if a product or service required for the performance of the Purchase Order is on the procurement list established pursuant to subsection 413.035(2), F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INsofar AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about the designated nonprofit agency and the products it offers is available at <http://www.respectofflorida.org>.

B. PRIDE.

In accordance with subsection 946.515(6), F.S., if a product or service required for the performance of the Purchase Order is certified by or is available from Prison Rehabilitative Industries and Diversified Enterprises, Inc. (PRIDE) and has been approved in accordance with subsection 946.515(2), F.S., the following statement applies:

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INsofar AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the products it offers is available at <http://www.pride-enterprises.org>.

Section 9. Miscellaneous.

A. Independent Contractor.

The Contractor and its employees, agents, representatives, and subcontractors are not employees or agents of the Agency and are not entitled to the benefits of State of Florida employees. The Agency shall not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all of its subcontracts under the Purchase Order.

B. Governing Law and Venue.

The laws of the State of Florida shall govern the Purchase Order. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Purchase Order. Further, the Contractor hereby waives any and all privileges and rights relating to venue it may have under Chapter 47, F.S., and any and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to those based on convenience. The Contractor hereby submits to venue in the county chosen by the Agency.

C. Waiver.

The delay or failure by the Agency to exercise or enforce any of its rights under the Purchase Order shall not constitute waiver of such rights.

D. Modification and Severability.

The Purchase Order may only be modified by a change order agreed to by the Agency and the Contractor. Should a court determine any provision of the Purchase Order is invalid, the remaining provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the Purchase Order did not contain the provision held to be invalid.

E. Time is of the Essence.

Time is of the essence with regard to each and every obligation of the Contractor. Each such obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

**Purchase Order
Terms & Conditions
Effective September 1, 2015**

F. Background Check.

The Agency may require the Contractor and its employees, agents, representatives and subcontractors to provide fingerprints and be subject to such background check as directed by the Agency. The cost of the background check(s) shall be borne by the Contractor. The Agency may require the Contractor to exclude the Contractor's employees, agents, representatives or subcontractors based on the background check results.

G. E-Verify.

In accordance with Executive Order 11-116, the Contractor agrees to utilize the U.S. Agency of Homeland Security's E-Verify system, <https://e-verify.uscis.gov/emp>, to verify the employment eligibility of all new employees hired during the term of the Purchase Order for the services specified in the Purchase Order. The Contractor shall also include a requirement in subcontracts that the subcontractor shall utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Purchase Order term.

H. Commodities Logistics.

The following provisions shall apply to all Purchase Orders unless otherwise indicated in the contract documents:

- 1) All purchases are F.O.B. destination, transportation charges prepaid.
- 2) Each shipment must be shipped to the address indicated on the face of the Purchase Order and marked to the attention of the individual identified, if any. Each shipment must be labeled plainly with the Purchase Order number and must show the gross, tare, and net weight. A complete packing list must accompany each shipment. This paragraph shall also apply to any third party who ships items on behalf of the Contractor.
- 3) No extra charges shall be applied for boxing, crating, packing, or insurance.
- 4) The following delivery schedule shall apply: 8:00 AM – 4:00 PM, Monday through Friday, excluding legal holidays.
- 5) If delivery to the specified destination cannot be made on or before the specified date, notify the Agency immediately using the contact information provided in the MyFloridaMarketPlace system.
- 6) The Agency assumes no liability for merchandise shipped to other than the specified destination.
- 7) Items received in excess of quantities specified may, at Agency's option, be returned at the Contractor's expense. Substitutions are not permitted.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



4050 Esplanade Way
Tallahassee, FL 32399-0950

Ron DeSantis, Governor
Pedro Allende, Secretary

**CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND
MAINLINE INFORMATION SYSTEMS, INC.**

This Confidentiality and Non-Disclosure Agreement (“Agreement”) is between the Florida Department of Management Services (“Department”), a state agency, and Mainline Information Systems, Inc. (“Recipient”), referred to herein collectively as the “Parties” and individually as a “Party.”

WHEREAS, Recipient has or will enter into a Purchase Order or Agency Term Contract under Request for Quote No. DMS-22/23-155, Endpoint Detection and Response Solution (“Solution”);

WHEREAS, in furtherance of providing these services and/or commodities, Recipient may access, receive, or create Confidential Information from the Department or any third-party beneficiaries; and

WHEREAS, the Department maintains certain protections on such Confidential Information and desires to set forth the terms Recipient is required to adhere to.

NOW THEREFORE, for the mutual and valuable consideration acknowledged by both Parties, the Parties agree as follows:

1. Definitions.

- (a) **Access**: Means the ability or authorization to create, inspect, transmit, approach, instruct, communicate with, store, retrieve, or otherwise make use of any Confidential Information, regardless of type, form, or nature of storage. “Access” to a computer system or network includes local and remote access.
- (b) **Affiliates**: Any agents, affiliates, partners, subcontractors, resellers, distributors, dealers, or other entities associated with Recipient that have Access to the Confidential Data.
- (c) **Agreement-related Materials**: Materials created or provided by Recipient while performing the Agreement.
- (d) **Confidential Information**: Information that is restricted from public disclosure based on federal or State laws and regulations including, but not limited to, those related to privacy, confidentiality, security, personally identifying information, personal health, business or trade secret information, and other information exempt from state public records law. “Confidential Information” includes information disclosed, orally or otherwise, before, on, or after this Agreement effective date by the Department to Recipient, and whether or not marked, designated, or otherwise identified as “confidential.” Any information derived from Confidential Information and/or created by Recipient pursuant to this Agreement which must be restricted from public disclosure based on federal or State laws and regulations shall be considered Confidential Information subject to the restrictions set forth in this Agreement.

Specifically, Recipient will receive and may create or learn of information which include network schematics, hardware and software configurations, or encryption, or which identify detection, investigation, or response practices for suspected or confirmed IT security incidents, including suspected or confirmed breaches, the disclosure of which would facilitate unauthorized access, modification, disclosure, or destruction of information, IT resources, or information relating security, which are confidential and exempt from public disclosure pursuant to section 282.318(5), Florida Statutes (F.S.).

- (e) Customer: Agencies as defined in section 287.012, Florida Statute (F.S.), and Eligible Users as defined in Rule 60A-1.001, Florida Administrative Code (F.A.C.).
- (f) State: The State of Florida.

2. **Term and Termination.** This Agreement is effective upon signature by both Parties. This Agreement may be terminated by the Department when determined to be in the best interest of the State of Florida by providing Recipient with advance written notice.
3. **Intended Third Party Beneficiary.** Customers receiving services under the Solution are intended third party beneficiaries of this Agreement, entitled to enforce any rights hereunder for their benefit.
4. **Confidential Information Use.** Use of the Confidential Information shall be limited to the provisions set forth herein and to the extent necessary to provide the services and/or commodities. The Department retains full rights and title to all Confidential Information provided by it, and any information derived therefrom. Recipient has no ownership rights to the Confidential Information provided under this Agreement, or any information derived therefrom.
5. **Recipient Obligations.** Recipient shall: 1) maintain the confidentiality of all the Confidential Information pursuant to this Agreement, as required herein, 2) comply with all federal and State laws and regulations related to information privacy and security, and 3) ensure that any Affiliates comply with the preceding two requirements as to any Confidential Information shared with or otherwise Accessed by the Affiliate. Recipient shall take all measures necessary to protect against improper Access to and/or disclosure or theft of the Confidential Information and will ensure only those individuals performing services contemplated in this Agreement will be permitted to Access the Confidential Information. Recipient shall perform the following measures to preserve the privacy, security, confidentiality, integrity, and accessibility of the Confidential Information which includes, but is not limited to:
 - (a) Using the Confidential Information only to provide services and/or commodities as contemplated in this Agreement and not otherwise using the Confidential Information for Recipient's own benefit or the benefit of others, or in violation of any applicable laws or regulations;
 - (b) Not creating derivative works based upon the Confidential Information, copying the Confidential Information, or publishing or disclosing the Confidential Information to any individual or entity except in accordance with this Agreement;
 - (c) Implementing and maintaining protective administrative, technical, and organizational security measures appropriate to the nature of the Confidential Information to safeguard against unauthorized Access, disclosure, or theft of the Confidential Information;
 - (d) Maintaining the confidentiality of the Confidential Information under this Agreement in accordance with Department policies and procedures and applicable State and federal laws and regulations;

- (e) Storing and safeguarding the Confidential Information in a physically and electronically secure location where Access is limited to authorized persons;
- (f) Maintaining an up-to-date list of individuals who are authorized to Access the Confidential Information;
- (g) Instructing and requiring all individuals authorized to Access the Confidential Information to adhere to the confidentiality requirements set forth in this Agreement prior to being granted Access to the Confidential Information;
- (h) Not allowing, through action or inaction, any Confidential Information to be sent by any medium, transmitted, or to be Accessed outside of the United States. For the purposes of this restriction, "Access" does not include remote support sessions for devices that might contain the Confidential Information; however, during the remote support session the Department requires Recipient to escort the remote support access and maintain visibility of the actions taken during the remote support access. Requests for remote access will be submitted to the Department's Contract Manager. With approval, third parties may be granted time-limited terminal service access to information technology resources as necessary for fulfillment of related responsibilities. Remote connections are subject to detailed monitoring via two-way log reviews and the use of other tools; and
- (i) Performing all actions necessary to assist with all tasks in furtherance of the Department's efforts to comply with the obligations under Chapters 60FF and 60GG, Florida Administrative Code, as applicable.

6. Liability. By signing this Agreement, Recipient acknowledges Recipient shall be responsible and liable for the acts and omissions of any of Recipient's employees and/or the Affiliate(s) that result in a violation of this Agreement as if such acts or omissions were Recipient's acts or omissions. Recipient represents that it will enter into a written agreement with an Affiliate with Access to Confidential Information wherein it shall require the Affiliate agree to be bound by and adhere to the terms of this Agreement.

7. Notice of Breach. Recipient must notify the Department as expeditiously as practicable, but in all instances no later than within one (1) business day, in the event Recipient discovers any incident that involves, or which Recipient reasonably believes may involve, a breach of the Confidential Information which includes any unauthorized Access to or disclosure of the Confidential Information and/or which compromises the security, integrity, or confidentiality of the Confidential Information. Additionally, if the Department or Customer shares with Recipient information that is covered by section 501.171, F.S., Recipient is responsible for fulfilling all applicable requirements of section 501.171, F.S., including those that would otherwise be the responsibility of the Department or Customer. Recipient agrees to provide the Department and applicable Customers with all details associated with all breaches or suspected breaches and to work with the Department or the applicable Customer to investigate and resolve any breach, implement any necessary remedial measures, and perform all tasks to ensure full compliance with section 501.171, F.S., including, where applicable, providing any breach notifications to comply with this statutory requirement.

8. Indemnification. Recipient shall defend, indemnify, and hold harmless the Department, the Customer, and the State against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, in connection with any third-party claim, suit, action, or proceeding arising out of or resulting from a violation of any obligation set forth in this Agreement by Recipient (including its employees) or its Affiliates. The Agreement does not constitute a waiver of sovereign immunity or consent by the Department, Customers, or the State or its subdivisions to suit by third parties. The obligations of this paragraph shall survive the Agreement.

- 9. Contractual Remedies.** Recipient acknowledges that a breach of this Agreement, including disclosure of any of the Confidential Information, will cause irreparable injury to the Department or the Customer and will entitle the Department or the Customer, if applicable, to liquidated damages commensurate with the Department's or the Customer's internal staffing and administrative costs associated with addressing the breach. This will not preclude the Department or the Customer from recovering other damages it may suffer as a result of such a violation or seeking other legal remedies that may be available during or after the Agreement term, including obtaining injunctive relief against the breach or threatened breach of these Agreement terms.
- 10. Data Destruction.** Prior to the termination of this Agreement, Recipient shall assist the Department or the applicable Customer in exporting and extracting or destroying, at the Department's or the applicable Customer's direction, all information obtained from the Department or the applicable Customer by Recipient or created for the Department or the applicable Customer by Recipient pursuant to this Agreement at no cost, in a format acceptable to the Department or the applicable Customer without the need to purchase additional services and/or commodities. Additionally, when the Agreement is terminated, Recipient shall transfer to the Department, or the Customer as applicable, all such information in all its forms from the Department or the applicable Customer and shall destroy duplicate records in accordance with section 501.171(8), F.S., and, if applicable, section 119.0701, F.S. This obligation to transfer and destroy information survives the term of this Agreement.

Recipient shall adhere to established information destruction standards, such as those established by the National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization" (2014), in destroying duplicate information provided by the Department or the applicable Customer. See <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>. Recipient shall provide the Department, or the Customer as applicable, with written confirmation of destruction of Confidential Information in accordance with these standards. If Recipient is permitted by the Department or the applicable Customer to keep Confidential Information upon termination of this Agreement, Recipient shall continue to protect and maintain the confidentiality of the Confidential Information in accordance with applicable State and federal laws, rules, and regulations and such obligations set forth herein shall survive this Agreement.

- 11. Severability and Waiver.** If a court of competent jurisdiction deems any term or condition of this Agreement void or unenforceable, the other provisions are severable to that void provision, and will remain in full force and effect. However, to the fullest extent permitted by law, this Agreement shall be construed as if the scope or duration of such provision had been more narrowly drafted so as not to be invalid or unenforceable.

The delay or failure by the Department or the Customer to exercise or enforce any of its rights under this Agreement shall not constitute a waiver of such rights.

- 12. Governing Law and Venue.** The laws of the State of Florida govern the Agreement. The Parties submit to the jurisdiction of the courts of the State exclusively for any legal action related to the Agreement which arises during or after the Agreement term. Further, Recipient hereby waives all privileges and rights relating to venue it may have under Chapter 47, F.S., and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to, those based on convenience. Recipient hereby submits to venue in the county chosen by the Department or the applicable Customer.

13. Entire Agreement. This Agreement contains the entire understanding of the Parties regarding the matters set forth herein and shall supersede any prior negotiations or agreements, whether written or oral, with respect thereto.

IN WITNESS WHEREOF, the Parties agree to the terms and conditions of this Agreement and have duly authorized their respective representatives to sign it on the dates indicated below.

**FLORIDA DEPARTMENT
OF MANAGEMENT SERVICES**

MAINLINE INFORMATION SYSTEMS, INC.

DocuSigned by:
Pedro Allende
5E91A9D369EB47C...
By: _____
Name: Pedro Allende
Title: Secretary
Date: 6/14/2023 | 4:58 PM EDT

DocuSigned by:
Joseph P. Elebash
A9FC98822028481...
By: _____
Name: Joseph P. Elebash
Title: Chief Financial Officer
Date: 6/13/2023