Endpoint Detection and Response Solution
DMS 22/23-155 Solution Summary

Managed FortiEDR with a 24/7 U.S. SOC, Implementation, Training, Integration, Maintenance, and Support included.
Optional –
- **Managed and Monitored SIEM**
- **Forensic and Remediation Services**

FortiEDR offers an enhanced Threat Detection that enables real-time monitoring for suspicious activity, detecting potential threats and signs of compromise. With our **Rapid Incident Response**, our SOC swiftly contains and mitigates security incidents, minimizing potential breach impacts. All while providing you with **full management access**.

We offer **Proactive Threat Hunting**, empowering our SOC team to search for hidden threats or signs of advanced persistent threats (APTs) that evade traditional security measures. Our Forensic Investigation capabilities allow detailed analysis of endpoint activities, crucial for incident investigation, root cause analysis, and **compliance purposes**. Additionally, FortiEDR reports on detected vulnerabilities running in your application environment.

FortiEDR automates **Endpoint Remediation**, restoring the running process by removing malicious elements and repairing a compromised system. We have up-to-date Threat Intelligence Integration that enhances detection capabilities by integrating with threat intelligence feeds, allowing quick identification and response to emerging threats.

Along with our SOC, you have full access to a Centralized Management and Reporting controls with all your endpoint security measures available from a unified dashboard, simplifying administration, monitoring, and compliance reporting. Continuous Monitoring by our SOC and AI enhanced Protection ensures a high level of security against evolving threats, while Compliance and Audit Readiness facilitates adherence to regulations and security best practices.

FortiEDR provides innovative endpoint security with real-time visibility, protection, and remediation. It proactively **shrinks the attack surface**, prevents malware infections, and defuses potential threats in real time, with automated responses to halt attacks and restore systems to a secure state. FortiEDR is unique as it operates as a Kernel replacement, not a Kernel hook, as most endpoint tool's function. This allows for a **lightweight endpoint agent** utilizing less than 1% CPU, under a 120 MB of RAM, and less than 20 MB of disk space, all while generating minimal network traffic. Our lightweight endpoint agent supports **Windows, macOS, and several Linux operating systems,** providing offline protection, and requiring minimal resources. With native cloud infrastructure, FortiEDR can be deployed as a **cloud-native, hybrid, or on-premises** solution, even in air-gapped environments.

FortiEDR also **remotely remediates** affected endpoints including **virtual patching** that can prevent many vulnerabilities caused by missed patches. Our **AI powered machine learning** anti-malware engine blocks attacks before execution, ensuring robust and efficient endpoint protection across multiple platforms.