FAQ

ENDPOINT DETECTION AND RESPONSE (EDR/MDR)

QUICK JUMP MENU

+ What is an EDR solution?

Evolving beyond Next-Gen Anti-Virus, Endpoint Detection and Response (EDR) combines continuous monitoring, behavioral analytics, cloud based threat analysis, automated response capabilities and other tactics to detect, contain or mitigate threats such as ransomware or malware that target endpoints such as. laptops, servers and desktops.

+ What is an MDR solution?

A managed detection and response (MDR) solution enhances an EDR solution by providing qualified security professionals 24x7 with eyes on glass to manage the detection, response and mitigation of threats. Additionally, MDR provides support for endpoint lifecycle management, troubleshooting, and often proactive threat hunting. MDR solutions are ideal for organizations that may lack the necessary resources or expertise to manage an EDR solution, or those who want 24/7/365 coverage to respond to threats in real time.

+ How do US Signal's EDR and MDR solutions work?

Software agents are installed on individual endpoints to monitor activity and collect data — such as processes, connections, volume of activity, and data transfers—into a centralized portal and data lake. Baseline rules recognize when incoming data indicates a known type of security event and triggers an automatic response. The solution also uses machine-learning and AI technologies to detect anomalous actions in real time, including fileless attacks, exploits, bad macros, evil scripts, ransomware, and other types of attacks.

Threats are responded to by various techniques including alerting, killing the process, quarantining a file, or isolating an endpoint so that the threat is stopped before harm can occur. Non-threats can proceed without disrupting operations. Machine Learning uses the information gathered to strengthen the service's ability to detect and protect against security incidents.

+ What's the difference between US Signal's EDR and MDR solutions?

The primary difference is the responsibility for post-deployment monitoring and response. With the EDR solution, customers are responsible for receiving and responding to alerts. With the MDR solution, US Signal's Security Operations enter (SOC) team takes on the responsibility. MDR is ideal for customers that lack the resources to manage an EDR solution, have a small security team, or are interested in leveraging the expertise of third-party security experts like US Signal's SOC team.

In addition, the EDR solution is available with a standard or premium tier of protection; MDR is only available at the premium tier. (See more information here.)

+ What makes US Signal's EDR and MDR solutions standout from comparable solutions from other vendors?

The biggest differentiator is US Signal's Security Operations Center. They SOC team helps with setting up the solution, being trusted partners to the customer, and can provide guidance in integrating the platform with other security technologies deployed by the customer to build a comprehensive defense-in-depth security strategy. The US Signal SOC provides 24x7 monitoring of your environment and stands ready to respond should a security incident occur.

In addition, US Signal's solutions are flexible with different service levels to best meet customers' needs. They're also continually evolving to provide protection in an ever-changing threat landscape.

+ What's the difference between the Standard and Premium tier of service?

The Standard tier applies only to the unmanaged EDR solution. US Signal will guide the initial deployment; customers receive and respond to all security alerts. It features basic threat detection capabilities powered by AI, machine learning and other advanced technologies, including:

+ Global platform management
+ Protects while offline
+ Incident forensics reporting
+ Malware rollback
+ Automated threat blocking
+ Device control for USB
+ Installed application inventory
+ Alerts (to customer)
+ Remote worker protection
+ AI and behavioral-based detection
+ Signature-based detection
+ Anomaly-based detection
+ Firewall control
+ Device control for Bluetooth
+ Platform support and management

The Premium tier includes two options: Premium EDR and Premium MDR. Premium EDR is also a self-managed option, and is ideal for organizations seeking enterprise-grade EDR. As with Standard EDR, US Signal will guide the initial deployment; customers receive and respond to all security alerts. In addition to the Standard EDR features, Premium EDR offers:

+ Device containment
+ Visual kill chain representation
+ Custom detection rules
+ Complete endpoint visibility
+ Secure remote shell

Complete Endpoint Visibility is the primary selling point for the premium tier as this is what allows for collection of advanced telemetry from all endpoint agents, such as DNS lookups, URLS visited, process creation, and more. This telemetry can be crucial for understanding what happened during a security event – especially if there were no endpoint alerts triggered.

Premium MDR is US Signal's premium tier-level EDR service offered as a managed service. US Signal's Security Operations Center (SOC) team receives and responds to all security alerts, freeing up customers' internal resources and enabling them to leverage the SOC team's extensive security experience and expertise.

In addition to all the features provided in the premium level manage-it-yourself option, Premium MDR offers:

+ 24/7/365 monitoring and response
+ Advanced technical support
+ Agent lifecycle management
+ Automated quarantine
+ File and path exclusions
+ Remediation guidance
+ Deployment assistance
+ Quarterly account review
+ Policy configuration & compatibility assessment

+ What are the software agents used in US Signal's EDR and MDR solutions?

An agent is a software program that is deployed to each endpoint. It runs autonomously on each device, without reliance on an internet connection. The agent sits at the kernel level. Using a dynamic behavior tracking engine, it monitors all processes in real time. Premium EDR allows customers to see exactly what happened on an endpoint at each stage of execution, including threat origin, patient zero, process and file activity, registry event, network connections, and forensic data. While the EDR agent will provide protection when no Internet connection is present, centralized alerting and the full benefits of the platform are realized when the full cloud-based intelligence can be used to protect the endpoint.

+ Who is responsible for installing the software agents on the individual endpoints?

US Signal will provide a virtual, guided deployment for all service tiers led by an experienced member of US Signal's Security Operations Center team. If further assistance is desired, US Signal can provide on-site support for deployment at an additional cost.

+ What endpoints (devices) are covered?

Both the EDR and MDR solutions can be used for laptops, desktops, and servers running Microsoft Windows, Apple Mac OS X, and most current Linux OS types.

+ Do these solutions work for IoT devices?

IoT devices are not covered at this time.

+ Will US Signal's EDR and MDR solution agents slow down my endpoints?

The solution agent won't slow down the endpoint it's installed on. Unlike antivirus products that require constant ".dat" file signature updates and daily disk scans, US Signal's software agents use static file AI and behavioral AI. This saves on CPU, memory and disk I/O, providing end users with better performance. Note: System resource consumption will vary depending on system workload.

+ How do US Signal's EDR and MDR solutions help ensure endpoint compliance with security and compliance standards?

For customers subject to CJIS, GDPR, HIPAA, PCI, or GLBA Anti-Virus or modern day EDR that automatically updates signatures is either a required or addressable control that must be implemented. US Signal's EDR and MDR offerings address these requirements.

+ Do US Signal's EDR and MDR solutions offer protection when users are offline?

Yes. The agent on the endpoint performs static and dynamic behavioral analysis pre- and on-execution. These two methods are the principal prevention and detection methods in use and don't require internet connectivity. When the agent is online, in addition to the local checks, it may also send a query to the cloud for further checking. Alerting, remote quarantine ability, administrative visibility, and functionality of the console is lost until the device is back online.

+ Are US Signal's EDR and MDR solutions cloud-based?

Yes. They are considered Software-as-a-Service (SaaS) solutions. However, their agent prevention, detection, and response logic are performed locally on the software agent, meaning the agent detection and protection capabilities are not cloud-reliant. Some EDR platforms rely on real-time upload of indicator telemetry to the cloud for purposes of identifying attacks – this is not the case for US Signal's solution.

This eliminates the large time gap between infection and cloud detection and response time that is associated with cloud-centric solutions.

+ Are these solutions meant to replace anti-virus or other similar endpoint security solution? Do I need to uninstall my existing antivirus program?

US Signal's solution can replace your antivirus or other anti-malware solution. It can also be used in conjunction with them, so you can decide if you want to uninstall them or not.

+ Will the EDR and MDR solutions easily integrate with other security tools such as a security incident and event management (SIEM) platform?

Yes. Logs and Alert can be forwarded from the EDR platform the customers SIEM platform and will be discussed during the Implementation phase of EDR or MDR.

+ Do US Signal's EDR and MDR solutions protect against ransomware?

Yes. They offer multiple capabilities to protect against ransomware including:

+ The ability to kill offending processes
+ Remediation (reversal) of unwanted changes
+ Auto or manual device network containment while preserving the administrator's ability to maintain interaction with the endpoint via the console
+ File and script quarantine
+ Rollback of Windows systems to their prior state

+ Does US Signal's EDR solution provide malware prevention?

US Signal's EDR solution prevents a wide range of attacks, including those from malware. The EDR solution analyzes executable files pre-execution and examines any process execution or child process execution for abnormal behavior. This eliminates the need for traditional signatures, which are easily bypassed, require constant updating, and require resource-intensive scans on the device. Analysis is performed anytime a file is opened or an application is executed on an endpoint to evaluate the behavior and activity of the file compared to expected normal behavior.

+ Can US Signal's EDR solution detect in-memory attacks?

Yes. It's integrated with hardware-based Intel® Threat Detection Technology (Intel TDT) for accelerated memory scanning capabilities.

+ Is the machine learning feature configurable?

No, but there's no need to "train" the AI within your environment. The data science team behind the solution trains the machine learning models in the development lab to help improve detection and protection, and reduce the false positive rate. New models are periodically introduced as part of agent code updates.

+ Are US Signal's EDR and MDR solutions scalable?

Yes. They can scale to protect large environments of hundreds or even thousands of endpoints.

+ Do the EDR and MDR solutions receive frequently updated signatures and models designed to detect advanced attacker tactics, techniques, and procedures (TTPs)?

Yes. Updated information is provided frequently.

+ What kind of device control do US Signal's EDR and MDR solutions offer?

There is the ability to restrict the use of USB removable media and Bluetooth devices with the EDR and MDR solution.

+ What is the cost/pricing for US Signal's EDR?

Pricing includes a one-time set up fee and monthly charge per endpoint.

US SIGNAL®