US SIGNAL®

Protect Your Endpoints.

TABLE OF CONTENTS

ENDPOINTS AT RISK

In the business world, laptops, desktops, and servers are standard tools of the trade across just about every industry. Unfortunately, these user systems are also key targets for ransomware and other types of attacks.

That's because these endpoints often provide easy ways for cybercriminals to access an organization's network, shared folders, critical servers, cloud resources, and virtual machines. Once inside, they can steal invaluable data, deploy malware, or initiate other cyberattacks. That's not to say these devices are completely at the mercy of cyberattackers. Organizations have numerous tools that can help protect their endpoints, including antivirus, content filtering and the block-listing or allow-listing of applications.

Among the issues with these solutions, however, is that they tend to focus on prevention – not detection or response. None are 100% foolproof when it comes to prevention. This is where endpoint detection and response (EDR) solutions, including managed detection and response (MDR) – a fully managed version of EDR, come into play.

EDR solutions are vital components of a defense in depth (DiD) strategy, which entails layering on various security mechanisms to provide more comprehensive protection – including for endpoints. They give organizations and managed security services providers visibility into all endpoints, enabling them to reduce the time to detect, investigate and mitigate potential threats.

In this ebook, we discuss how EDR solutions work, their features and benefits, the advantages of the MDR version, and some of the factors to consider when choosing an EDR or MDR solution.

EDR: WHAT IT IS

Traditionally, endpoints were protected using endpoint protection platforms (EPP) and antivirus tools. The focus of these solutions was on preventing intruders inside network's perimeter – where the endpoints are.

An EDR solution is an advanced cybersecurity tool that focuses on active and potential security threats. It's designed to protect systems no matter where they are – on premises, in the cloud or wherever remote users may be. EDR can protect against traditional threats and new threats such as zero-day and fileless malware attacks. EDR gathers data from an organization's endpoints and, using machine learning, data analytics, behavioral based detection, and artificial intelligence (AI), it detects, identifies and quickly responds to threats.

EDR solutions can be self-managed or managed by a third party. The managed version is referred to managed detection and response or MDR.

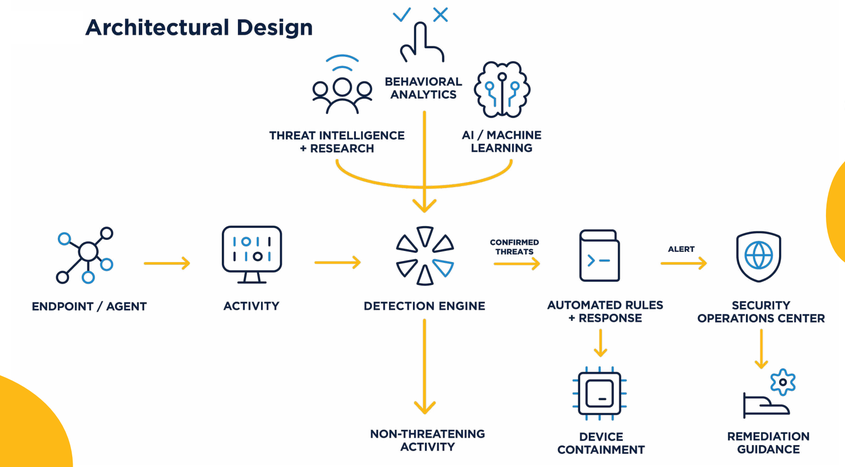
EDR: HOW IT WORKS

EDR solutions, including MDR, are typically cloud-based and delivered as Software-as-a-Service (SaaS). They monitor centralized endpoints regardless of location if the endpoint has internet connectivity.

In general, endpoint monitoring is conducted in real time. Pre-configured rules help identify when incoming data indicates a known type of threat actor behavior and triggers an automatic response. This includes containing and, as necessary, remediating the threat. Machine learning (ML) or artificial intelligence (AI) may also be used to detect anomalous behaviors and activities that don't fit a threat actor known profile of attack.

Many times, threats are stopped before they can execute. Non-threats can proceed without disrupting operations. All issues are analyzed, and information about threats and non-threats is used to further strengthen the solution's ability to detect and protect against future security issues.

In addition, EDR solutions generate alerts to help security operations analysts investigate issues. The best EDR solutions validate threats before sending alerts, helping to minimize the potential for alert fatigue that can cause many notifications to be ignored due to lack of time or understanding of the seriousness of the issue.



MDR: THE MANAGED VERSION OF EDR

While many EDR solutions can be self-managed, which means the organization employing the solution receives and responds to threat alerts, some organizations prefer to go with a what is known as a managed detection and response (MDR) solution.

MDR solutions layer on the expertise of a 24/7/365 Security Operations Center (SOC) to the EDR solution. The SOC provides qualified security professionals around the clock to manage the detection, response and remediation of threats. Their extensive security knowledge and experience helps them to better understand the data provided by the EDR solution and to accurately prioritize alerts and respond them appropriately and effectively. That's especially beneficial given that many organizations lack the highly specialized in-house security expertise required for dealing with the wide range of existing and emerging endpoint threats.

In addition, MDR solutions include support for endpoint lifecycle management, troubleshooting and, in many cases, proactive threat hunting.

MDR solutions are not only ideal for organizations that lack the necessary resources or expertise to manage an EDR solution. They also work well for those that want 24/7/365 coverage to respond to threats in real time.

AGENT OR AGENTLESS EDR

As noted earlier, EDR solutions can use agents (software) or employ an agentless approach.

EDR solutions that use agents install them on individual endpoints. They run autonomously on each device, and sit at the kernel level. Agents installed directly on endpoints can capture a considerable amount of data on user activity no matter what device is used to login to the network. They also can quickly implement actions to contain or mitigate threats.

Among the downsides of using agents is that they may not work on endpoints with unsupported operating systems. This is often the case with Internet of Things (IoT) devices that don't use standard operating systems. IoT devices also may not have powerful processors or large amounts of memory; agents can introduce CPU and RAM utilization overhead.

With agentless EDR solutions, no agent software is installed on endpoints. Instead, the EDR tool passively monitors traffic coming onto and passing through the network as it flows between users' client machines and the servers they're accessing. Because there are no agents to install, deployment is faster. However, agentless EDR solutions don't capture local user activity on endpoints, or anything about locally running processes, hardware elements or other details of the device itself.

Data about endpoints can't be gathered when they're not connected to the corporate network. Encrypted data traffic is also difficult to monitor and analyze. The biggest drawback is that without a presence on the endpoint device, the response portion of EDR may be limited.

SIEM INTEGRATION

Among the questions that inevitably arise is how an EDR solution works with security information and event management (SIEM) platforms.

SIEM provides a single central location for storing and analyzing data, coming from many different log sources. This data may be generated by applications, databases, infrastructure, sensitive assets, manufacturing systems or security systems.

Structurally, a SIEM then utilizes an EDR as another log source providing valuable information. EDR helps investigate, uncover, prioritize, and remediate complex attacks specifically using end-point data. That's why SIEM and EDR or MDR are often paired as complementary security tools to provide a multilayer, more effective defense system.

THE BENEFITS OF EDR AND MDR

EDR and MDR solutions offer numerous benefits over other security tools such as antivirus. For example, unlike legacy antivirus tools that perform scans daily or weekly, EDR and MDR solutions monitor in real-time. They immediately provide alerts of potential threats or intrusions. This allows you to respond faster and mitigate attacks before they do any significant damage.

Among the biggest benefits of EDR and MDR solutions are the insights they provide. **By providing visibility into a problem, an EDR or MDR solution delivers information regarding where the issue originated and the different data and applications it interacted with so appropriate actions can be taken – including rolling back to a pre-infected state.** In addition, visibility into what's happening on endpoints can also help IT security teams eliminate vulnerabilities so they can strengthen overall network and endpoint security.

MDR solutions offer even more benefits. Among them: 24/7/365 management, the expertise of dedicated security professionals, and support for endpoint lifecycle management, troubleshooting and, in many cases, proactive threat hunting.

EDR AND MDR FEATURES

EDR and MDR solutions vary in the features they offer, and the most desirable features are those that best meet an organization's specific needs and use cases. In general, look for solutions that:

+ Cover the operating systems used in your endpoints; at a minimum, most EDR tools provide support for Windows (including older versions), Mac OS and Linux.
+ Provide centralized real-time monitoring and visibility.
+ Make use of advanced technologies such as machine learning to deliver the most up-to-date threat intelligence.
+ Monitor and provide remote logging and analysis of endpoint behaviors.
+ Collect a wide range of security-related event data from each endpoint, including process creation, registry changes and disk access.
+ Perform behavioral analysis on the data to uncover potential threats as well as malicious activity that is already in progress.
+ Detect, prioritize, and track Indicators of Compromise (IOCs), Indicators of Attack (IOAs) and advanced threats, such as fileless attacks, zero-day exploits and others, in real time.
+ Generate alerts when a threat is detected; even better, generate alerts for validated threats.
+ Offer a "managed" option if you don't have the resources to respond to alerts
+ Allow for interactive IOC/IOA searching across all endpoints.
+ Integrate with, forensics case management, security information and event management (SIEM), and security orchestration, automation and response (SOAR), and other security tools.
+ Support network quarantine to lockdown communication between suspicious nodes and the SaaS management console.
+ Provide playbooks and configurable automated responses.
+ Employ various steps to remediate or contain an attack, including:
    - Quarantining files and blocking the spread of suspicious files
    - Terminating suspicious processes
    - Isolating the endpoint on the network to prevent lateral movement of the attack
    - Automatic or manual execution of suspicious payloads in a sandbox
    - Remote script execution on the endpoint
    - Rolling back to a pre-infected state
+ Include a vetted 24/7/365 Security Operations Center (SOC) to handle alert response and overall management (MDR only).

THE US SIGNAL APPROACH TO MDR

US Signal offers an MDR solution, with the US Signal Security Operations Center (SOC) team responsible for post-deployment monitoring and response of the MDR solution. The SOC team provides 24/7/365 coverage for customers, assists with proper configuration and rule creation, and leads the response and remediation efforts.

The solution uses software agents installed on individual endpoints to monitor activity, and perform static and dynamic behavioral analysis pre- and on-execution. They're the principal prevention and detection methods and don't require a network connection. This saves on CPU, memory and disk I/O, and ensures users are covered even when they're offline.

Data — such as processes, connections, volume of activity, and data transfers — is collected into a centralized portal and data lake. Baseline rules recognize when incoming data is a known type of security event and triggers an automatic response. The solution also uses AI technologies to detect anomalous actions in real time, such as fileless attacks, exploits, bad macros, evil scripts, and ransomware.

Various techniques are used to respond to threats, including alerts, 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 information gathered to strengthen the service's ability to detect and protect against future security incidents. The solution can be layered with SIEM solutions to further strengthen defenses.

MDR FEATURE OVERVIEW

FEATURES	PREMIUM MDR
Global Platform Management	✓
Remote Worker Protection	✓
AI Behavioral Based Detection	✓
Machine Learning Based Detection	✓
Malware Rollback	✓
Firewall Control	✓
Device Control for USB, Bluetooth	✓
Device Containment	✓
Complete Endpoint Visibility	✓
Visual Killchain Representation	✓
Secure Remote Shell	✓
Custom Detection Rules	✓
Automated Quarantine	✓
Advanced Technical Support	✓
Alert Response	✓
Agent Lifecycle Management	✓
Remediation Guidance	✓
Quarterly Account Review	✓
24x7x365 US Signal SOC Monitoring	✓

US SIGNAL MDR FAQS

A list of frequently asked questions about US Signal's MDR solution – and answers to them – can be found at on the US Signal website. Here are a few that may be of interest:

+ What endpoints (devices) are covered?
US Signal's MDR solution can be used for laptops, desktops, and servers running Microsoft Windows, Apple Mac OS X, and most current Linux OS types. Mobile devices and IoT devices are not covered at this time.

+ Can US Signal's MDR solution help ensure endpoint compliance with security and compliance standards?
For customers subject to CJIS, GDPR, HIPAA, PCI, or GLBA Anti-Virus, automatically updates signatures is either a required or addressable control that must be implemented. US Signal's EDR and MDR offerings address these requirements.

+ Does US Signal's MDR solution offer protection when users are offline?
Yes. The agent on the endpoint performs static and dynamic behavioral analysis pre- and on-execution which doesn'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. However, alerting, remote quarantine ability, administrative visibility and functionality of the console is lost until the device is back online.

+ Does US Signal's MDR solution protect against ransomware?
Yes. They offer multiple capabilities to protect against ransomware, including:

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

+ Does US Signal's MDR solution provide malware prevention?
Yes. They analyze executable files pre-execution and examine 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 MDR solution detect in-memory attacks?
Yes. They're integrated with hardware-based Intel® Threat Detection Technology (Intel TDT) for accelerated memory scanning capabilities.

+ Does US Signal's MDR solution receive frequently updated signatures and models designed to detect advanced attacker tactics, techniques and procedures (TTPs)?
Yes. Updated information is provided frequently.

+ Is US Signal's MDR solution scalable?
Yes. They can scale to protect large environments of hundreds or even thousands of endpoints

+ What is the cost/pricing for US Signal's MDR solution?
Pricing includes a one-time set up fee and monthly charge per endpoint.

PROTECT YOUR ENDPOINTS **AND MORE**

An EDR solution like US Signal's MDR is just one aspect of a comprehensive IT security strategy, but it's an important one. For more information on this and other security solutions that will enable you to implement a DiD security approach, scan the QR code below or contact US Signal by email at **info@ussignal.com** or call **866.2.SIGNAL**.

ussignal.com/edr

ABOUT US SIGNAL

Learn how US Signal can help you safeguard your business assets from ransomware and other malware, pre-emptively detect security gaps mitigate data loss if a disaster occurs, and keep mission-critical applications operational.

US Signal offers a comprehensive service portfolio of disaster recovery and business continuity options to ensure data availability while mitigating IT-related business disruptions. All services are powered by the company's own resilient private fiber network and PCI- and HIPAA-compliant infrastructure.

US Signal is audited for compliance with or holds certifications for numerous regulatory requirements and industry standards. Among them:

HIPAA COMPLIANT · PCI · AICPA SOC 2 · AICPA SOC · CJIS READY · ITAR · GDPR