

eSentire MDR for Endpoint

Hunt and Isolate Endpoint Threats Fast, Before They Spread



Prevent Predictable Known Attacks

We identify suspicious behavior using predictive threat modeling to automatically block known, new and fileless cyber attacks.



Detect Unknown, Elusive Attacks

Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats.



Respond To and Remediate Threats

When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints preventing disruption to your business.



Build Resilience Against Future Attacks

We help you anticipate, withstand, and recover from critical cyber threats by determining the root cause of the incident and eradicating threat actor presence. As a result, your endpoints become resilient to even the most advanced cyberattacks.

Today's endpoints are located across vast physical and digital environments, making traditional, point-solution endpoint approaches incomplete. eSentire's comprehensive, multi-signal Managed Detection and Response (MDR) service provides advanced endpoint protection with 24/7 threat hunting, deep investigation and complete threat response. For the most elusive threats, our SOC Cyber Analysts and Elite Threat Hunters rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread and business disruption. We work alongside you to determine root cause and corrective actions, ensuring you are protected and hardened against future business disruption.

eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine Elite Threat Hunting with endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as:

- Commodity malware
- Ransomware
- Zero-day attacks
- Suspicious activity
- Abnormal behavior
- Fileless attacks
- Advanced Persistent Threats (APTs)
- Lateral movement

We go beyond standard MDR providers to provide complete endpoint response and remediation including:

- ⊕ Preventing infected endpoints from spreading to other machines
- ⊕ Isolating ransomware, data exfiltration and hands-on keyboard attackers
- ⊕ Quarantining malicious files and terminating processes
- ⊕ Stopping/removing service and registry keys
- ⊕ System reboots

How We Help	Your Outcomes
✓ Endpoint protection regardless of whether your users and data reside in the cloud, mobile, virtual or physical environments ✓ Automated blocking preventing known, unknown and fileless attacks ✓ Rapid human-led investigations ✓ Remote managed containment to lock down and isolate threat actors on your behalf, preventing lateral spread ✓ Remediation of infected endpoints to bring them back to full production	✓ Optimize and harden endpoint defenses ✓ Elimination of your physical and virtual endpoint blind spots ✓ Reduced attacker dwell time ✓ Mitigation of potential disruption to your business ✓ Satisfaction of your compliance requirements ✓ Minimized incident recovery time frame

Cost-Effective Endpoint Protection and Flexible Bring Your Own License Options

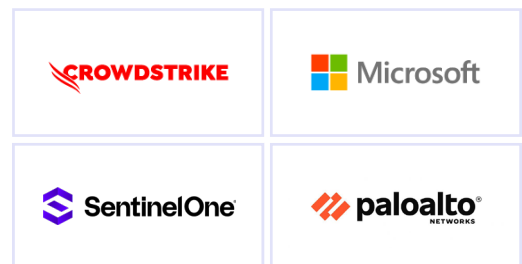
Get Proactive, Prevention-First Endpoint Protection with the eSentire Agent

The eSentire MDR Agent offers a cost-effective prevention-first approach to stop ransomware and malware attacks using proprietary deep learning technology with incredible efficacy. It delivers incredible cybersecurity value with complete flexibility as part of our value-rich, full-service bundles for small and medium-sized businesses.

[LEARN MORE ABOUT THE ESSENTIRE MDR AGENT →](#)

Our Best-of-Breed Ecosystem of Technology Partners

We also offer a flexible best-of-breed MDR approach that means we partner with leaders in endpoint, SIEM, cloud and vulnerability management including CrowdStrike, Microsoft, Sentinel One, Palo Alto Networks, Sumo Logic, and Tenable. We can easily maximize your existing investment in security tools through our bring your own license or subscription (BYOL/ BYOS) services to support even more cost-efficient options.



Endpoint Threat Detection Engineering Driven by Industry Experts

We also go beyond other MDR providers by developing custom detection engineering based on our threat intelligence and proprietary Machine Learning (ML) applications that hunt and respond to endpoint threats.

eSentire's Threat Response Unit (TRU) delivers counter-threat research and proprietary content to stay ahead of attackers targeting endpoints. TRU builds proprietary detectors for Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs), all mapped to the MITRE ATT&CK framework. We publish original research and security advisories so you're up to date on the latest cyber landscape and endpoint security risks.

Machine Learning Innovation: BlueSteel

eSentire feeds your endpoint telemetry through the BlueSteel engine. Advanced analytics and machine learning are then used to identify signs of malicious activity. We leverage BlueSteel to continuously enhance our endpoint detection capabilities and empower our Elite Threat Hunters to disrupt, contain and remediate endpoint threats.

BlueSteel in Action Against PowerShell

Following initial intrusion, many attackers pivot to PowerShell as a means to advance their objectives. PowerShell commands are easily obfuscated, meaning it's easy for an attacker to hide malicious commands within script that otherwise appears normal. Using this technique, attackers can evade detection from endpoint protection technologies.

To solve this problem, eSentire's TRU team created a proprietary application called BlueSteel, which analyzes all PowerShell commands from customer endpoints and classifies them as either malicious or benign. The BlueSteel technique is similar to SPAM classification, utilizing frequency analysis with terms and characters to differentiate between good and bad. The goal is to increase the accuracy of PowerShell threat detection beyond what endpoint protection provides using machine learning.

As PowerShell attacks continue to be leveraged by attackers, BlueSteel continues to learn and enhance its threat detection capabilities. Combining advanced machine learning models with elite threat hunting, eSentire MDR ensures you can anticipate and withstand Powershell attacks.

Features

24/7 Protection

Monitors endpoints around the clock across eSentire's global SOC's.

Hybrid and Cloud Environment Visibility

Protects your endpoints anywhere users and data reside—across cloud, mobile, virtual and physical environments.

Endpoint Activity Recording

Accelerates forensic investigation, acting as a “black box” flight recorder that continuously records, centralizes and retains vital endpoint activity.

Advanced Threat Detection

Catches what preventative controls miss with proprietary machine learning layered with attack pattern and behavioral analytics.

Automated Blocking

Prevents known, unknown and fileless attacks using predictive threat modeling and behavioral analysis.

Elite Threat Hunting

Pursues elusive threat actors and performs rapid forensic investigation, enabling timely containment and root cause determination.

Threat Containment

Locks down and isolates threat actors on your behalf preventing lateral spread and potential business disruption.

Remediation

eSentire experts manage the remediation of infected endpoints to bring them back to full production.

	Other Managed Endpoint Providers	eSentire MDR for Endpoint
24/7 continuous monitoring, recording and centralizing of activity	✓	✓
Prevention of known attacks	✓	✓
Alerting of confirmed threats and suspicious behavior	✓	✓
Tactical threat containment on customer's behalf via host isolation to stop lateral spread	Varies	✓
Active threat hunting	Limited	✓
Continuous management, tuning and refinement of detection platform	Varies	✓
Root cause determination	Varies	✓
Detection of unknown attacks using machine learning and advanced analytics	Limited	✓
Remediation	Limited	✓

We Do More than Managed EDR - And Multi-Signal Matters

Our multi-signal approach ingests endpoint, network, log, cloud, identity, and vulnerability data that enables complete attack surface visibility. Automated blocking capabilities built into our eSentire XDR Cloud Platform prevent attackers from gaining an initial foothold while our expert Elite Threat Hunters can initiate manual containment at multiple levels of the attack surface. Through the use of host isolation, malicious network communication disruption, identity-based restriction and other measures, we can stop attackers at multiple vectors and help you build a more resilient security operation.

MDR Signals	Visibility	Investigation	Response
 ENDPOINT			
 NETWORK			
 LOG			
 CLOUD			
 IDENTITY			
 VULNERABILITY			

Ready to get started?

Connect with an eSentire Security Specialist to learn how we can help you build a more resilient security operation and prevent disruption.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US  1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow [@eSentire](https://twitter.com/eSentire).