

eSentire MDR Foundations

Broad Visibility Across Your Users and Applications with 24/7 Threat Prevention, Detection, and Response



Full Threat Visibility & Investigation

With MDR Foundations you gain multi-signal visibility across your network assets, endpoints, applications, and cloud services enabling data correlation and deep investigation whether your data is in the cloud, on premises or hybrid.



24/7 Threat Hunting & Disruption

Integrated proprietary machine learning and advanced analytics identify and automatically block cyber threats built to bypass preventative defenses.

If a threat does get through, Elite Threat Hunters take action to contain and remediate compromised endpoints, preventing business disruption.



Reduce Risk and Harden Against Future Attacks.

Our 24/7 SOC Cyber Analysts and Elite Threat Hunters gain necessary context to respond to threats. We detect threats in seconds and deliver a Mean Time to Contain of 15 minutes.

We support the incident response lifecycle by determining root cause and eradicating threat actor presence. Your endpoints become resilient to new and repeat attacks.

Today's businesses operate in cloud, on-premises, and hybrid environments making traditional point-solutions in endpoint detection and response (EDR) incomplete. eSentire MDR Foundations combines the advanced protection of eSentire MDR for Endpoint with eSentire MDR for Log, enabling 24/7 multi-signal ingestion and complete threat visibility across your endpoints, applications, and cloud services.

Our SOC Cyber Analysts and Elite Threat Hunters investigate log and endpoint data and rapidly isolate compromised endpoints leveraging your existing EDR, endpoint protection (EPP), and next-gen antivirus (NGAV) licenses in a bring your own license (BYOL) model that helps you get the most out of your security investments.

You get a team of experts who aggregate meaningful and actionable intelligence from multiple signals, accelerating investigations and enabling complete response against cyber threats. MDR Foundations eliminates blind spots, to detect a multitude of attack types and techniques including but not limited to:

- Commodity Malware
- Ransomware
- Zero-day attacks
- Advanced Persistent Threats (APTs)
- Suspicious activity
- Abnormal behavior
- Fileless attacks
- Lateral movement
- Phishing Attacks
- Data Exfiltration
- Insider Threats
- Defense evasion
- Cloud Service Misconfigurations
- Modular malware
- Privilege escalations and alterations
- Cryptojacking
- Suspicious VPN activity

How We Help	Your Outcomes
<ul style="list-style-type: none"> • Multi-signal visibility from your network assets, endpoints, applications and cloud services • Rapid human-led investigations • Protection anywhere users and data reside- across cloud, mobile, virtual and physical environment. • Remote managed containment to lock down and isolate threat actors on your behalf, preventing lateral spread • Automated blocking preventing known, unknown and fileless attacks • 24/7 monitoring and recording of endpoints • Remediation of infected endpoints to bring them back to full production • 24/7 threat detection mapped to the MITRE ATT&CK framework • Detect threats that traditional logging technologies miss with continuous innovation from our Threat Response Unit (TRU) • Flexible log consumption, analysis and storage options 	<ul style="list-style-type: none"> • Mitigation of potential disruption to your business • Reduction in your operating expenditure cost and resource demands Optimized and hardened state of endpoint defense • Decrease threat actor dwell time • Decrease false positives and increase true positives for your security team • Elimination of your physical and virtual endpoint blind spots • Efficiencies and cost savings versus DIY security analytics • Minimized incident recovery time frame • Account for risk across your network assets • Satisfy and report on logging regulatory requirements from frameworks such as HIPAA, PCI, GDPR, etc.

Robust Hybrid Environment Coverage

Detect and respond to threats across the big three cloud providers:

Cloud Infrastructure



Further counter threat TTPs leveraging common security infrastructure and tools (including but not limited to):

- Mitigation of potential disruption to your business
- EDR/EPP tools (VMware® Carbon Black, CrowdStrike, Trend Micro, etc.)
- Network security technology (Palo Alto, Cisco, etc.).
- Email security platforms (Outlook, Gmail, Proofpoint, etc.)
- VPN providers (Palo Alto, Cisco, etc.)
- Web gateway solutions (Citrix)

Features

24/7 Monitoring

Human-led investigations and correlation from expert analysts in our 2 global Security Operations Centers (SOCs) across modern enterprise environments.

Elite Threat Hunting

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

Threat Detection Across Hybrid and Cloud Environments

We detect threats based on business rules, MITRE ATT&CK techniques, user behaviors, the promotion of detections from existing security tools, and more.

Threat Containment

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

Machine Learning-powered Detection Engineering

Atlas XDR machine learning-powered security force multipliers that hunt and respond to elusive threats through vast amounts of data.

Hybrid and Cloud Environment Visibility

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

Remediation

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

Endpoint Activity Recording

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

Cloud SIEM Implementation and Maintenance

Included configuration and ongoing maintenance services from experienced SIEM practitioners for supported Cloud SIEM technologies.

Flexible Log Consumption, Analysis and Storage Options

Focus on the data that matters the most to your business in order to maximize your investment.

Simplified Compliance Management

Satisfy and report on the logging regulatory requirements of frameworks such as HIPAA, PCI, GDPR, etc.

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.

Our Best-of-Breed Ecosystem of Technology Partners

Our best-of-breed MDR approach means we partner with the leading technology platforms in EPP and EDR, data analytics, log management, and cloud SIEM helping you maximize your existing investment with either our BYOL model or by selecting licensing included options. Additionally, **MDR Foundations includes Sumo Logic log analytics**, and no SIEM or additional log licensing is needed.

Bring your own best of breed endpoint license select eSentire Atlas Agent powered by award-winning technology* for your endpoint solution.



eSentire MDR Foundations vs. Other Managed Endpoint and SIEM Solutions

	Other Solutions	eSentire
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	✓
Forensic Investigation	Limited	✓

Detection Engineering Driven by Our Elite Threat Response Unit

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. BlueSteel continuously enhances 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 to advance their objectives. With PowerShell commands, 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.

eSentire's proprietary application called BlueSteel analyzes all PowerShell commands from customer endpoints and classifies them as either malicious or benign. As PowerShell attacks continue to be leveraged by attackers, BlueSteel continues to learn and enhance its threat detection capabilities. Combining machine learning with elite threat hunting and applying it to eSentire's MDR capabilities, our Security Operation Center (SOC) analysts are empowered to disrupt, contain and remediate threats like PowerShell every day.

Detection Engineering Spotlight: Malkara
























With more employees working remotely than ever before, most organizations have VPN or similar network access mechanisms in place to facilitate remote access. Attackers who have obtained valid account credentials can leverage VPNs or network gateways as a way to "walk in the front door" of your network undetected. MITRE ATT&CK classifies this technique as T1078 – Valid Accounts and it's typically one of the more difficult techniques to identify before it's too late.

To take on this challenge, eSentire's TRU developed a proprietary machine learning model code-named Malkara as part of eSentire's Log service. The model analyzes all remote access to identify any anomalous activity and the end user who triggered the alert. eSentire SOC Cyber Analysts follow investigative runbooks to determine the validity of the event and if the activity is determined to be malicious, take action available to them to contain the threat.

Multi-Signal Matters

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

At eSentire we recognize that the attack surface is continuously evolving and expanding. While our MDR service protects your organization from modern attackers and the vectors they target most often, we are continuously analyzing and developing new services & and detections to outpace the adversaries. In our twenty+ year history, we pride ourselves on the fact that no eSentire client has experienced a business disrupting breach. With over 1000 customers across 70 countries, we don't just claim to deliver complete response. We prove it and are proud to earn our global reputation as the Authority in Managed Detection and Response, each and every day.

MDR Signals	Visibility	Investigation	Response
 NETWORK			
 ENDPOINT			
 LOG			
 CLOUD			
 IDENTITY			
 VULNERABILITY			

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. eSentire's award-winning global **e3 partner ecosystem**, representing experience, expertise, eSentire, has been awarded a 5-Star rating in the Partner Program Guide by CRN®, a brand of The Channel Company, for five consecutive years. The e3 ecosystem focuses on mapping partner engagement, productivity and overall experience to how business leaders choose to consume best-in-class cybersecurity services through marketplaces, global Managed Services Providers (MSPs), Managed Security Services Providers (MSSPs), Value Added Resellers (VARs), and Technology Service Brokers. For more information and to become a partner, visit: www.eSentire.com/Partners and follow [@eSentire](https://twitter.com/eSentire).