eSENTIRE

DATA SHEET

eSentire MDR for Log

24/7 active log monitoring to deliver critical visibility, compliance and a system of record, across your multi-cloud and hybrid environments.

Multi-Signal Ingestion And Full Threat Visibility

Gain multi-signal visibility across your network assets, endpoints, applications and cloud apps enabling data correlation and deep investigation regardless if your data is in the cloud, on premises or in between.

Proactive Threat Hunts

Stay ahead of the ever-evolving threat landscape with hundreds of proprietary runbooks, cutting-edge detections, and new IOCs developed and updated by our Threat Response Unit (TRU).

Applied Analysis and Investigations

Easily search your log system of record for security incident details, satisfying insurance, compliance and regulatory requirements. We provide log management capabilities to support and enrich threat hunts and investigations.

Rapid Threat Detection and Response in Multi-Cloud and Hybrid Environments

Our 24/7 SOC Cyber Analysts leverage ML-enabled behavioral detections and proprietary runbooks to detect threats within your environment in real-time and deliver a Mean Time to Contain of 15 minutes.

eSentire MDR for Log delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management. Our best-of-breed log monitoring technology ingests and stores logs across AWS, Microsoft 365, Azure, and your existing security controls to provide complete attack surface visibility and help you satisfy insurance, regulatory and compliance requirements such HIPAA, PCI, GDPR, etc.

We aggregate meaningful and actionable intelligence from multi-signal ingestion across your network assets, endpoints, applications and cloud services to accelerate our investigations and enable complete response against cyber threats.

We detect a multitude of attack types and techniques, including but not limited to:

- Phishing and business email compromise attacks
- Data exfiltration
- Insider threats
- Suspicious or unusual user behavior
- Cloud service misconfigurations
- Modular malware
- Privilege escalations and alterations
- Cryptojacking
- Suspicious VPN activity
- Defense evasion

How We Help

- ✓ 24/7 threat detection mapped to the MITRE ATT&CK framework
- ✓ Detect threats that traditional logging technologies miss with proactive threat hunts and continuous intelligence from our Threat Response Unit (TRU)
- ✓ Multi-signal visibility from your network assets, endpoints, applications and cloud services
- ✓ Rapid human-led investigations
- ✓ Configurable, economic log consumption, analysis and storage options
- ✓ Global threat sweeps across your logs under management by our Threat Response Unit

Your Outcomes

- ✓ Enhanced threat detection and response capabilities
- ✓ Decreased threat actor dwell time
- ✓ Decrease in false positives for your security team
- ✓ Expertise from the eSentire Blue Team in planning, building and maintaining your SIEM -Access to best-of-breed log monitoring, log management and cloud SIEM technology and expertise at a fraction of the cost of a DIY approach
- ✓ System of record for insurance mandates
- ✓ Regulatory compliance with logging requirements within HIPAA, PCI, GDPR, etc. -Decreased risk of business disruption

Our Best-of-Breed Ecosystem of Technology Partners

Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM. We can also leverage your existing investment in bring your own license (BYOL) service scenarios.

sumo logic

Microsoft

Detection Engineering Driven By Our Elite Threat Hunters

eSentire MDR for Log is powered by dynamic threat detections and runbooks. Our Threat Response Unit (TRU) builds more than 150 novel proprietary detectors and runbooks mapped to the MITRE ATT&CK Framework each quarter, enabling you to stay ahead of the threat landscape.

Based on Threat Intel Research and MITRE Mapped

We investigate the latest threat actor tactics, techniques and procedures on an ongoing basis through original research, leveraging enriched threat intelligence, and the MITRE ATT&CK framework.

Developed to Proactively Identify Threats and Streamline Investigations

Our open XDR platform provides visibility and early detections for emerging attacks with proprietary security content and new IOCs are continuously updated by our Threat Response Unit (TRU). Early detections are investigated, correlated across signal types to identify potential attacker movement across environments, and where necessary, active threats are rapidly contained within a 15-minute Mean Time to Contain.

Measurement and Continuous Improvement of Detections

We track all security content for accuracy and efficacy after deployment, implementing adjustments and decommissioning as necessary for optimized operational efficiency.

DETECTION ENGINEERING SPOTLIGHT:

Malkara

With more employees working remotely than ever before, most organizations use VPNs or similar network access mechanisms to facilitate remote access. This presents an opportunity for attackers with valid account credentials to leverage your VPNs or network gateways to “walk in the front door” of your network undetected. The MITRE ATT&CK Framework 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, the eSentire TRU team developed a proprietary machine learning model code-named Malkara as part of eSentire’s MDR for Log service. This tool leverages VPN log data and applies ML models to identify malicious VPN behaviors across cloud and on-premises environments using valid account credentials. Our 24/7 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.

Robust Hybrid Environment Coverage

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

CLOUD INFRASTRUCTURE

Google Cloud · Azure · aws

CLOUD APPLICATIONS

Google Workspace · Azure

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

- EDR/EPP tools
- VPN providers
- Network security technology
- Web gateway solutions
- Email security platforms
- Identity providers

We continuously expand our log ingestion capabilities by adding new runbooks for SaaS platforms and enterprise applications. When suspicious activity is detected, we stitch together context-free log telemetry to identify similar attacker tactics in your environment.

SAAS PLATFORMS AND SECURITY INFRASTRUCTURE

CROWDSTRIKE · Microsoft · SentinelOne · LACEWORK · eSENTIRE · sumo logic · tenable

Barracuda · CloudGuard SaaS · citrix · cisco · Dropbox · DUO · f5

FURTINET · mimecast · okta · paloalto · salesforce · proofpoint

slack · Gmail · TREND MICRO · SOPHOS · zscaler · Qualys

Features

24/7 Monitoring

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

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.

Machine Learning-powered Detection Engineering

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

Cloud SIEM Implementation and Maintenance

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

Unlimited Logs **Available only as part of eSentire Atlas MDR Packages*

Our streamlined log management solution enables unlimited critical log ingest focused on threat hunting and detection, making incident investigation more effective and response faster, while meeting your retention and compliance needs.

Simplified Compliance Management

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

We Do More than Managed Log - 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 Open XDR Cloud Platform prevents 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 minimise the risk of business disruption.

At eSentire we recognise that the attack surface is continuously evolving and expanding. While our MDR service protects your organisation from modern attackers and the vectors they target most often, we are continuously analysing and developing new services & detections to outpace the adversaries. In our 20+ year history, we pride ourselves on the fact that no eSentire customer has experienced a business disrupting breach. With over 2000 customers across 80+ 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
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, 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.