eSENTIRE

DATA SHEET:

eSentire MDR for Insider Threat

Proactive Defense for Malicious Insiders and Advanced Persistent Threats

Comprehensive Insider And Advanced Persistent Threat Awareness

We automatically map hosts across on-premises and cloud environments, capturing vital east-west traffic, critical for visibility into advanced persistent and malicious insider threat activities.

Ongoing Adaptive Behavioral Baselines

Our team develops a deep understanding of your normal network activity making adjustments for changing business operations and the evolving insider cyber threat landscape.

Machine Learning Powered Detection Mapped To The Attack Kill Chain

We identify potential insider cyber threats with powerful machine learning technology that links host interactions and data movement to attack kill chain behaviors.

Complete Response with Elite Threat Hunting and Remediation

MDR for Insider Threat alleviates resource constraints with a dedicated team of Elite Threat Hunters that conduct investigations and support remediation that reduces cyber risk to your business operations.

eSentire MDR for Insider Threat identifies advanced persistent threats and malicious insiders that can evade traditional detection technologies. We maintain an understanding of what your normal network activity looks like and identify deviations that indicate attacker kill chain stages. Our Elite Threat Hunters investigate suspicious activity and work with your team to neutralize attacks minimizing time to contain and preventing disruption to your business.

We protect against:

- Threat behaviors vs. signatures
- Live-off-the-land techniques
- Malicious use of approved tooling
- Hackers leveraging east-west tactics, techniques, and procedures (TTPs)

How We Help

- 24/7 insider threat monitoring
- Increased east-west traffic visibility across cloud and on-premises environments
- Provide baseline network behavioral norms and maintain continuous situational awareness
- Provides access to ThreatCases® so you can understand the context and status of events
- Team eSentire is an extension of your team by hunting, investigating and remediating advanced persistent threats and malicious insiders already in your network

Your Outcomes

- Better visibility into your business ensuring continuous threat and risk awareness
- Identification of insider threats that elude signature-based detections
- Our experts understand your environment with unique context ensuring correlation across your complex environment
- Peace of mind that no insider threat goes unnoticed
- Alleviates resource constraints to investigate, confirm and respond to malicious insider threats

Detection Engineering Driven By Our Elite Threat Hunters

MDR for Insider Threat identifies malicious activity indicative of insider threats, leveraging proprietary machine learning processes developed by our Threat Response Unit (TRU) and Elite Threat Hunting to contain attackers before they can disrupt business operations.

From internal reconnaissance to data collection and exfiltration, attack stages are mapped to hosts that exhibit potential malicious behaviours. These attack stages are visualized with the involved suspicious hosts and relevant network activity in a ThreatCase®, summarizing the complete investigation and providing context to the attack. Your organization has complete access to all ThreatCases® and gains the expertise of our 24/7 Security Operations Center (SOC) Cyber Analysts & Elite Threat Hunters so you can understand attacks, respond in minutes, and harden your network.

Features

Automated Network Mapping

Automatically maps new and existing network hosts across your on-premises, cloud and hybrid environments.

Comprehensive Visibility

Provides unparalleled visibility into east-west traffic, capturing data movement between hosts critical to determining the legitimacy of traffic and the network norm.

Continuous Situational Awareness

We ingest data from high fidelity sources into our integrated machine learning platform that modifies and redefines understanding of the network norm over time, continually evolving to keep pace with the changing threat landscape and evolving nature of your network.

Consumable Attack Chain Visualizations

Plain language narratives aligned to ThreatCases® provide visual maps with linked evidence of insider threat campaigns unfolding inside your network.

Adaptive Human Context

Our Elite Threat Hunters work in tandem with your internal security teams to establish a deep understanding of network and security operations that improves accuracy and speed of investigations.

Elusive Insider Identification

Integrated machine learning looks deep within your network for entities exhibiting characteristics that match attack kill chain stages. From reconnaissance to data collection and exfiltration, host activity is mapped to attack stages that exhibit potential malicious behaviors traditional detections and triggers miss.

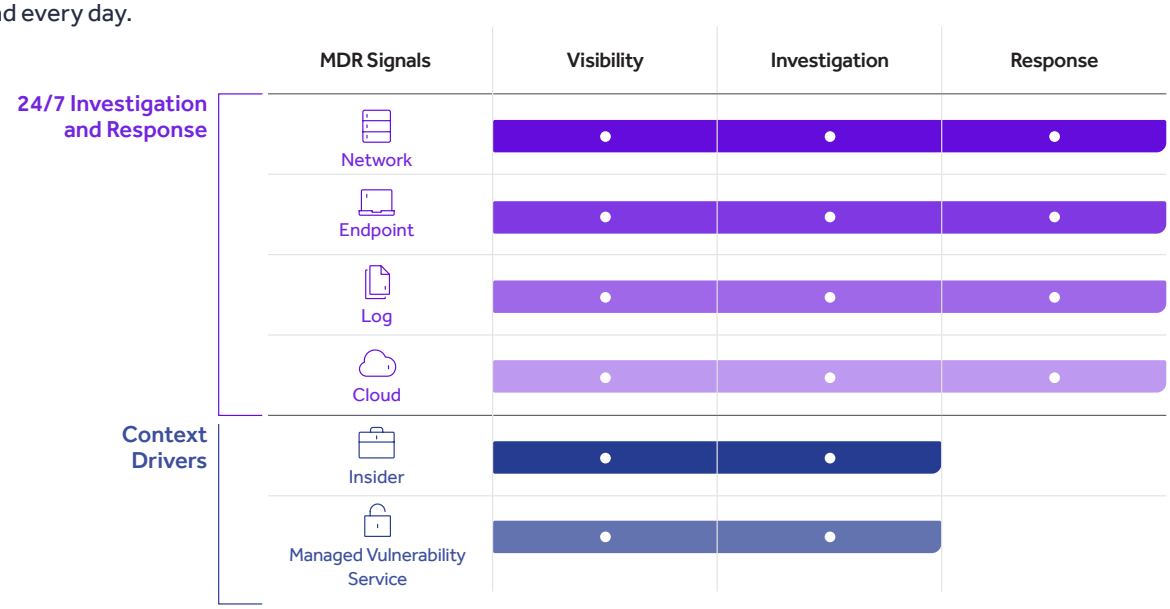
eSentire vs. other Insider Threat Protection

	Other Insider Threat Protection	eSentire
Uses attack chain stages across techniques, tactics and procedures (Recon, data collection and exfiltration)		✓
Unifies visibility across all east-west traffic		✓
Integrates data from virtually any sources		✓
Provides simple straightforward ThreatCases® for easy to interpret information at your fingertips		✓
Normalizes disparate datasets for analysis		✓
Applies user behavior analytics whether malicious or not	Limited	✓
Identifies suspicious behavior whether malicious or not	Limited	✓
Cloud operated and deployed	Limited	✓
Reactive and proactive threat hunting included	Limited	✓

Why Mutli-Signal MDR 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 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 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 & 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.



Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to demonstrate how eSentire Multi-Signal MDR stops threats before they disrupt your business.

Contact Us

If you're experiencing a security incident or breach contact us 1-866-579-2200

eSentire

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.