eSENTIRE

DATA SHEET

eSentire MDR for Identity

Go beyond identity and access management with real-time threat detection and response at the identity level to stop insider-threats and compromised credential attacks across your hybrid cloud environments, 24/7.

Correlate identity-related events with broader security incidents

eSentire XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents.

Our multi-signal approach ingests and correlates data from various sources including logs, network data, cloud, and endpoints to investigate and respond to identity-based threats.

Flexible, seamless integration with best-of-breed identity protection technology

Leverage your existing technology stack with flexible BYOL options or select one of our best-of-breed identity solutions without any limitations or constraints.

Regardless of the solution you choose, eSentire MDR for Identity stops identity and insider threats before they disrupt your business.

24/7 threat detection and response against identity-based threats

Whether threats originate on-premises or in the cloud, our open XDR platform automatically disrupts high fidelity threats and provides enriched telemetry to our 24/7 SOC to investigate and respond to identity-based attacks in real-time.

Additionally, the eSentire Threat Response Unit (TRU) regularly conducts proactive, hypothesis-driven threat hunts to improve your response capabilities against emerging identity and insider threats.

Your Challenges

The adoption of a remote and hybrid workforce forced many organizations to increase their reliance on cloud and SaaS applications for business operations and growth. As a result, security leaders are challenged with securing their organizations against identity-based threats, such as theft of valid user credentials. What's more, cybercriminals are actively exploiting vulnerabilities found in identity and access management (IAM) tools so they can gain initial access into the corporate environment.

In addition, humans are known to be the weakest link in cybersecurity, making it critical for security leaders to continuously monitor, update, and enhance their security protocols to mitigate the risks associated with identity-related threats.

Our Solution

eSentire MDR for Identity integrates and enhances insights from your security tooling to provide identity and insider threat context. We detect and respond to the following threats:

- Attacks on Active Directory
- Compromised Identities
- Ransomware
- Credential Weakness and Theft
- Unauthorized Access
- NTLM/LDAPS Protocol Threats
- Insider Threats

How We Help

- Monitor users, entity behavior, and activities with learning-based analytics for authentication and authorization
- 24/7 monitoring and investigation of identities
- Identify unused accounts, unused permissions, scenarios of over-permissions, and unnecessarily large compromised identity blast radius.
- Disable suspicious or compromised users
- Force a password reset
- Detects potential malicious insider activity

Your Outcomes

- Visibility into advanced persistent and malicious insider threat activities
- Correlate identity-related events with broader security incidents from various sources including logs, network, and endpoint
- Reduced alert noise
- Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)
- Improvement of overall security posture
- Mitigation of potential business disruption
- Complete response to identity and insider threats with elite threat hunting and remediation support

Our Best-of-Breed Technology Partners

We offer a flexible, best-of-breed MDR approach that means we partner with leaders in identity management and protection, including CrowdStrike and Microsoft. We also offer identity and authentication provider support for enrichment and swift response, along with a wide array of native integrations with cloud tooling to provide support regardless of where your environment and identities live. 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 to meet cyber insurance requirements.

CROWDSTRIKE

eSentire is an elite CrowdStrike Powered Service Provider with over 650 mutual customers and was selected as CrowdStrike's 2024 Global MSSP Partner of the Year. We have also been certified as a partner of choice by CrowdStrike, delivering differentiated MXDR offerings built on the CrowdStrike Falcon platform®.

Microsoft

eSentire is a Microsoft Security Solutions Partner, designated MXDR Partner and Microsoft Intelligent Security Association (MISA) member.

Identity Providers

eSentire integrates with leading Identity Providers to enhance your security posture with comprehensive identity enrichment and swift response capabilities. This integration enhances visibility, reduces threat dwell time, and minimizes operational disruptions.

Additionally, eSentire supports open integrations for popular cloud and Cloud Native Application Protection Platform (CNAPP) vendors. These integrations allow us to ingest information and logs from various sources, enabling detection and response.

Key Features

24/7 Visibility and Monitoring: Get a comprehensive view of all identities across your environment, including AD, Entra ID, and hybrid deployments.

Reduce Alert Fatigue: Reduce noise by allowing users to approve their own access requests when there are deviations from normal behavior instead or generating an alert.

Look Beyond Initial Access: Stay ahead of insider threats and identity store threats with threat detections that cover the complete cyber kill chain, mapped to the MITRE ATT&CK Framework, to include persistence, privilege escalation, credential access, discovery, and lateral movement.

- **Insider threats:** Detect potential malicious insider activity by following data movements, linking behaviors with different meta-goals, and using machine learning to understand which activities are expected and consistent for each network.

24/7 Threat Detection, Investigation, and Response: Get expert-level support from our Elite Threat Hunters and team of SOC Cyber Analysts, who respond on your behalf against threats that bypass your controls so you can prevent business disruption.

Why Choose eSentire?

- Benefit from 24/7 multi-signal coverage that extends beyond endpoints and identity with threat correlation across network, endpoint, log, cloud, and vulnerability data with deep threat investigation and complete response.
- Partner with a trusted advisor with demonstrated commitment to delivering industry-leading security services.
- Maximize your existing investment in security tools through our flexible Bring Your Own License (BYOL) offering or leverage a completely managed solution with our best-of-breed technologies.
- Get 24/7 service expertise including onboarding, unlimited threat hunting and incident handling, and complete response and remediation against sophisticated cyber threats.

Ready To Get Started?

We're here to help! Submit your information and an eSentire representative will be in touch to discuss how eSentire MDR can help you build a more resilient security operation today.

CONTACT US

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

eSENTIRE