

DATA SHEET

eSentire MDR for Endpoint and Identity Powered by CrowdStrike



<p>Endpoint visibility that spans detection, response, and forensics</p> <p>Delivers continuous, comprehensive endpoint visibility that spans detection, response, and forensics to ensure nothing is missed and potential breaches are stopped.</p>	<p>Stop identity-based attacks in real time</p> <p>Detect complex identity-based attacks across unified endpoint and identity telemetry to stop attacks in real time by combining the power of advanced AI, behavioral analytics, and a flexible policy engine to enforce risk-based conditional access.</p>	<p>Prevent known and unknown attacks</p> <p>We identify suspicious behavior using predictive threat modeling, integrated threat modelling and predictive analytics to automatically block known, new and fileless cyberattacks.</p>	<p>Respond to and remediate threats</p> <p>When a threat bypasses your controls, our 24/7 Elite Threat Hunters will act on your behalf to contain and remediate compromised endpoints preventing disruption to your business.</p>
---	---	--	--

The threat landscape is ever-evolving and adversaries are developing sophisticated approaches to establish a foothold on endpoints and exploit compromised credentials. Lack of visibility and response across endpoints and at the identity level can make it difficult to contain and remediate threats in order to minimize disruption to your business.

eSentire MDR for Endpoint and Identity, Powered by CrowdStrike, provides advanced endpoint and identity protection no matter where your users or data reside (on prem, cloud, hybrid) with 24/7 threat hunting, deep investigation and complete threat response. For the most elusive threats, Team eSentire rapidly investigates and isolates 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, eliminating blind spots and stopping:

- Commodity Malware
- Ransomware attacks
- Zero-day attacks
- Fileless attacks
- Privilege escalation
- Suspicious activity
- Geo & behavioral anomalies
- Advanced Persistent Threats (APTs)
- Lateral movement
- Credential abuse



How We Help	Your Outcomes
<ul style="list-style-type: none"> ✓ 24/7 monitoring and recording of endpoints and user identities ✓ Endpoint and identity protection anywhere users and data reside — across cloud, mobile, virtual and physical environments ✓ Machine learning and artificial intelligence to detect known and unknown malware and ransomware attacks ✓ Behavior-based indicators of attack (IOAs) to prevent sophisticated fileless and malware-free attacks ✓ Exploit blocking to stop the execution and spread of cyber threats ✓ Detecting and quarantining on write to stop and isolate malicious files ✓ 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 	<ul style="list-style-type: none"> ✓ Optimized and hardened state of endpoint and identity defense ✓ Elimination of your physical and virtual endpoint and identity blind spots ✓ Mitigation of potential disruption to your business ✓ Reduction in your operating expenditure cost and resource demands ✓ Satisfaction of your compliance requirements ✓ Minimized incident recovery time frame

The Solution

eSentire eSentire MDR for Endpoint and Identity, powered by CrowdStrike, stop endpoint and identity-based threats in real-time.

eSentire MDR for Endpoint, Powered by CrowdStrike	eSentire MDR for Identity, Powered by CrowdStrike**
<ul style="list-style-type: none"> • 24/7 monitoring and recording of endpoints • Endpoint protection anywhere users and data reside — across cloud, mobile, virtual and physical environments • Machine learning and artificial intelligence to detect known and unknown malware and ransomware attacks at the endpoint level • Behavior-based indicators of attack (IOAs) to prevent sophisticated fileless and malware-free attacks • Exploit blocking to stop the execution and spread of cyber threats • Detect and quarantine potentially malicious files as they are written to devices, preventing them from executing and spreading within the environment • 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 	<ul style="list-style-type: none"> • 24/7 monitoring and investigation of identities across AD • Full visibility across complex hybrid identity environments • Reduce the attack surface with a complete picture of AD hygiene • Detect abnormal user behavior and identity-based attacks like Kerberoasting, Golden Ticket, Pass-the-Hash • Stop attacks in real-time by blocking authentication at the AD layer, even from unmanaged hosts • Extend MFA to areas impossible to cover with traditional approaches, such as legacy systems • Identity-based segmentation: restrict users without needing to segment a network • Reduce noise by allowing users to approve their own access requests when there are deviations from normal behavior instead of generating an alert <p><small>** available as an add-on to eSentire MDR for Endpoint, Powered by CrowdStrike</small></p>

Best in Breed CrowdStrike Endpoint and Identity Detection and Response Technology

eSentire is an Elite CrowdStrike Powered Service Provider and was selected as CrowdStrike's 2023 Global MSSP Partner of the Year, with more than 500 mutual customers. eSentire MDR for Endpoint and Identity leverages the industry-leading CrowdStrike Falcon® platform to deliver an endpoint and identity security solution that provides:



- **Powerful Protection:** The CrowdStrike Falcon® platform delivers immediate, effective prevention against, and detection of all types of attacks — both malware and malware-free — regardless of whether endpoints are online or offline.
- **Unrivaled Visibility:** Gain complete visibility into what is happening on endpoints — nothing is missed. The Falcon platform helps to discover and investigate current and historic endpoint activity in seconds and initiate fast, effective remediation.
- **Ease of Use:** The cloud-delivered Falcon platform is easy to deploy, configure and maintain — all via a single, lightweight agent — to seamlessly deliver effective endpoint protection as a service.

Why eSentire

The eSentire MDR for Endpoint and Identity Difference means you're:

- ✓ Partnering with CrowdStrike's 2023 Global MSSP Partner of the Year, with over 500 mutual customers
- ✓ Receiving the flexibility of Bring Your Own License (BYOL) or leveraging a completely managed solution
- ✓ Gaining certified expertise across your MDR for Endpoint and Identity platform
- ✓ Receiving 24/7 service expertise including onboarding, threat hunting and complete response and remediation
- ✓ Benefiting from 24/7 multi-signal coverage beyond endpoint and identity, with threat correlation across network, endpoint, log, and cloud, deep investigation and complete response

Ready to Get Started?

Reach out to connect with an eSentire security specialist and 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

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).