eSENTIRE | CROWDSTRIKE

DATA SHEET

eSentire MDR for Endpoint and Identity, Powered by CrowdStrike

Endpoint visibility that spans detection, response, and forensics

Delivers continuous, comprehensive endpoint visibility that spans detection, response, and forensics to ensure nothing is missed and potential breaches are stopped.

Stop identity-based attacks in real time

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.

Prevent known and unknown attacks

We identify suspicious behavior using predictive threat modeling, integrated threat modelling and predictive analytics to automatically block known, new and fileless cyberattacks.

Respond to and remediate threats

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.

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
- Geo and behavioral anomalies
- Credential abuse
- Suspicious activity
- Privilege escalation
- Fileless attacks
- Lateral movement
- Advanced Persistent Threats (APTs)

How We Help	Your Outcomes
24/7 monitoring and recording of endpoints and user identities	Optimized and hardened state of endpoint and identity defense
Endpoint and identity protection anywhere users and data reside — across cloud, mobile, virtual and physical environments	Elimination of your physical and virtual endpoint and identity blind spots
Rapid human-led investigations and managed threat hunting with	Mitigation of potential disruption to your business
CrowdStrike's Overwatch, offering detections based on the latest threat intelligence for the most recent global attacks	Reduction in your operating expenditure cost and resource demands
Machine learning and artificial intelligence to detect known and unknown malware and ransomware attacks	Satisfaction of your compliance requirements
Behavior-based indicators of attack (IOAs) to prevent sophisticated fileless and malware-free attacks	Minimized incident recovery time frame
Exploit blocking to stop the execution and spread of cyber threats	
Detecting and quarantining on write to stop and isolate malicious files	
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	

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*
• 24/7 monitoring and recording of endpoints	• 24/7 monitoring and investigation of identities across AD
• Endpoint protection anywhere users and data reside — across cloud, mobile, virtual and physical environments	• Full visibility across complex hybrid identity environments
• Machine learning and artificial intelligence to detect known and unknown malware and ransomware attacks at the endpoint level	• Reduce the attack surface with a complete picture of AD hygiene
• Behavior-based indicators of attack (IOAs) to prevent sophisticated fileless and malware-free attacks	• Detect abnormal user behavior and identity-based attacks like Kerberoasting, Golden Ticket, Pass-the-Hash
• Exploit blocking to stop the execution and spread of cyber threats	• Stop attacks in real-time by blocking authentication at the AD layer, even from unmanaged hosts
• Detect and quarantine potentially malicious files as they are written to devices, preventing them from executing and spreading within the environment	• Extend MFA to areas impossible to cover with traditional approaches, such as legacy systems
• Remote managed containment to lock down and isolate threat actors on your behalf, preventing lateral spread	• Identity-based segmentation: restrict users without needing to segment a network
• Remediation of infected endpoints to bring them back to full production	• Reduce noise by allowing users to approve their own access requests when there are deviations from normal behavior instead or generating an alert
	**available as an add-on to eSentire MDR for Endpoint, Powered by CrowdStrike*

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 2024 Global MSSP Partner of the Year. eSentire MDR for Endpoint and Identity leverages the industry-leading CrowdStrike Falcon® platform to deliver an endpoint and identity security solution that provides:

POWERED BY CROWDSTRIKE

- **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 2024 Global MSSP Partner of the Year
- 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