eSENTIRE

Microsoft Partner Gold Security Microsoft

Member of Microsoft Intelligent Security Association Microsoft

DATA SHEET

eSentire MDR with Microsoft Defender for Endpoint

Prevent the Predictable. Hunt the Elusive.

Prevent The Predictable

Identify suspicious behavior using predictive threat modeling to automatically block expected, unexpected and fileless attacks.

Detect The Elusive

Find threats built to circumvent prevention leveraging proprietary machine learning and advanced analytics.

Hunt and Isolate Before Disruption

Minimize threat actor dwell time with elite eSentire threat hunters that identify, lock down and isolate compromised endpoints on your behalf.

Harden Against Future Attacks

Determine root cause and eradicate threat actor presence across your environment with full incident lifecycle support.

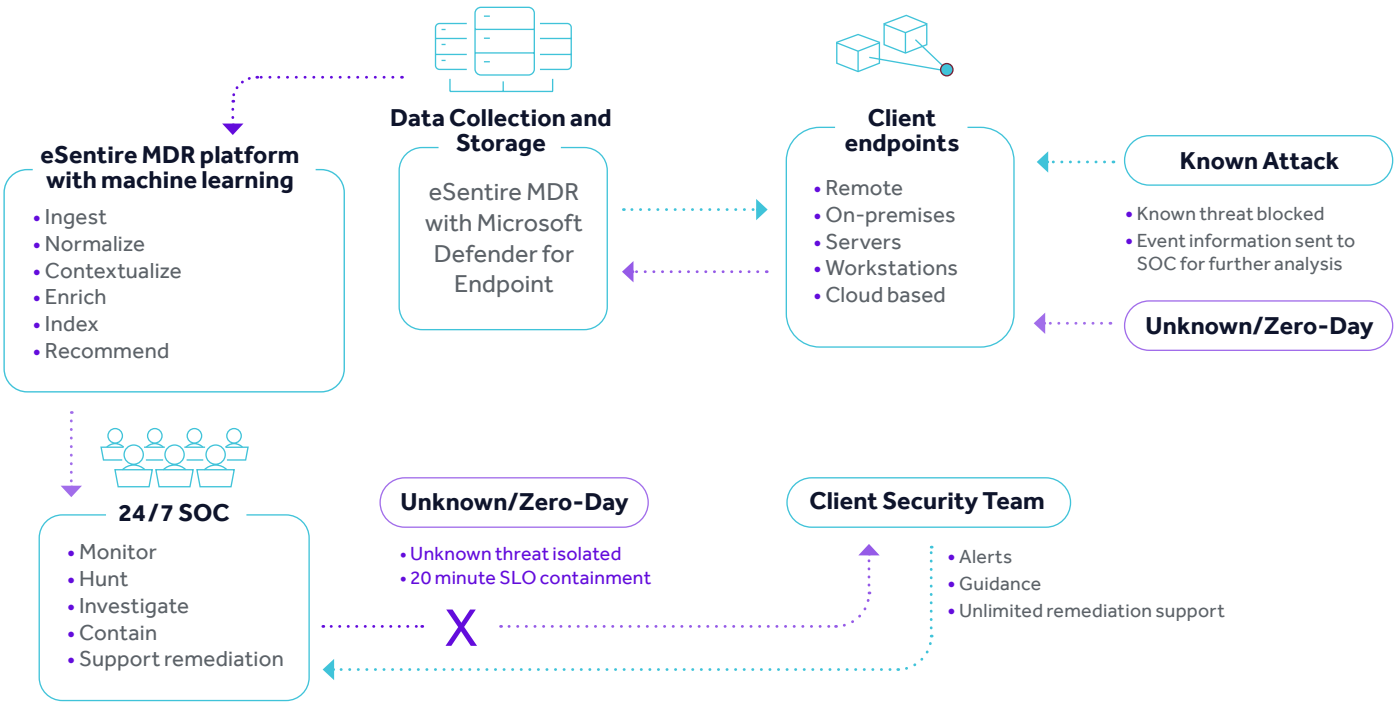
eSentire protects your assets 24/7 no matter where users or data reside. eSentire MDR combines elite threat hunting with the Microsoft Defender for Endpoint platform to eliminate blind spots. Leveraging Microsoft threat detection and intelligence as well as our predictive threat modeling and proprietary machine learning, our team of experts can identify potential unknown and zero-day threats. For the most elusive of threats, an elite team of eSentire threat hunters rapidly investigate and neutralize compromised endpoints on your behalf, preventing lateral spread. Supporting the full incident response lifecycle, we work alongside your security team to determine root cause and corrective actions, ensuring your environment is hardened against future business disruption.

	Endpoint Prevention	Endpoint Detection and Response
Focus	Optimize and adapt next-generation antivirus platform to prevent incidents from happening	Minimize detection-to-containment time frame of threats that bypass preventative controls

What Does Esentire MDR With Microsoft Defender For Endpoint Detect?

- Malware
- Known attacks
- Suspicious activity
- Abnormal behavior
- Fileless attacks
- Advanced persistent threats
- Lateral movement
- Zero-day attacks

How It Works



Features

24/7 Coverage

Monitors endpoints on and off the network around the clock with eSentire's global Security Operations Centers (SOCs).

Single Agent

Reduces complexity and management with a single lightweight agent that collects all endpoint data without sacrificing operational performance.

Endpoint Anywhere Visibility

Protects your endpoints anywhere users and data reside–across cloud, mobile, virtual and physical environments.

Endpoint Activity Recording

Accelerates forensic investigation, acting as a "black box" flight recorder that continuously records, centralizes and retains vital endpoint activity.

Automated Blocking

Prevents known, unknown and fileless attacks using predictive threat modeling and behavioral analysis.

Advanced Detection of Unknown and Zero-Days

Catches what prevention misses with proprietary machine learning layered with attack pattern and behavioral analytics.

Integrated Expertise

Speeds deployment and continuously adapts and hardens endpoints, alleviating resource constraints.

Elite Threat Hunting

Pursues elusive threat actors and performs rapid forensic investigation, enabling timely containment and root cause determination.

Remote Managed Containment

Locks down and isolates threat actors on your behalf preventing lateral spread and potential business disruption.

Full Incident Lifecycle Support

Eradicates threat actor presence with co-managed remediation from initial detection to confirmation of hardening and monitoring for reentry.

The eSentire Difference

	Other EDR	eSENTIRE MDR
24/7 continuous monitoring, recording and centralizing of activity	✓	✓
Prevention of known attacks	✓	✓
Alerting of confirmed threats and suspicious behavior	✓	✓
Co-remediation and hardening recommendations	✓	✓
Continuous management, tuning and refinement of detection platform	Varies (May Require Add-on to Service)	✓
Singular agent	Varies	✓
Detection of unknown attacks using machine learning and advanced analytics	Limited	✓
Active threat hunting	Limited (May Require IR Retainer)	✓
Tactical threat containment on customer's behalf via host isolation to stop lateral spread	Varies	✓
Root cause determination	Varies (May Require IR Retainer)	✓
Full incident lifecycle support	Requires IR Retainer	✓

Make The Case - eSentire MDR With Microsoft Defender for Endpoint

- Rapid deployment and quick time to value
- Optimized and hardened state of endpoint defense
- Elimination of physical and virtual endpoint blind spots
- Blocking of known, unknown and fileless attacks
- Detection of elusive attackers and zero-day threats
- Isolation of compromised endpoints, preventing lateral spread
- Reduction in operating expenditure cost and resource demands
- Minimized incident recovery timeframe
- Improvement in overall security posture
- Mitigation of potential business disruption
- Satisfaction of compliance requirements

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 Thre at 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**.