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 24x7x365 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.

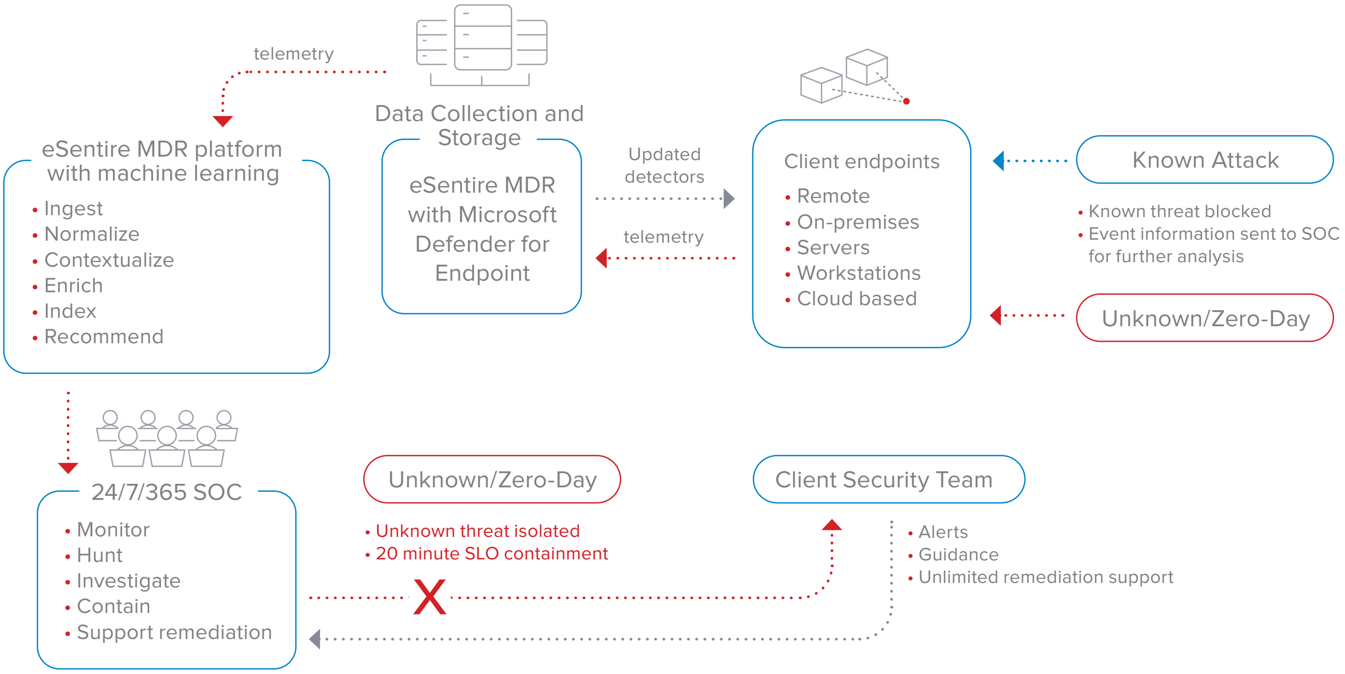
	Endpoint Prevention	Endpoint Detection and Response
Focus	Optimize and adapt next-generation antivirus platform to prevent incidents from happening	Minimize detection-to-containment time frame of threats that bypass preventative controls

[1,2,3] Ponemon: 2018 State of Endpoint SecurityRisk

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



telemetry

Data Collection and Storage

eSentire MDR platform with machine learning

- Ingest
- Normalize
- Contextualize
- Enrich
- Index
- Recommend

eSentire MDR with Microsoft Defender for Endpoint

Updated detectors

telemetry

Client endpoints

- Remote
- On-premises
- Servers
- Workstations
- Cloud based

Known Attack

- Known threat blocked
- Event information sent to SOC for further analysis

Unknown/Zero-Day

24/7/365 SOC

- Monitor
- Hunt
- Investigate
- Contain
- Support remediation

Unknown/Zero-Day

- Unknown threat isolated
- 20 minute SLO containment

Client Security Team

- Alerts
- Guidance
- Unlimited remediation support

FEATURES

24x7x365 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
24x7 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

Ready to get started? We're here to help.

Reach out and schedule a meeting to learn more.

eSENTIRE

Member of
Microsoft Intelligent Security Association
Microsoft

eSentire, Inc., founded in 2001, is the category creator and world's largest **Managed Detection and Response (MDR)** company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, **visit www.esentire.com** and follow **@eSentire**.