

DATA SHEET

eSentire MDR with Microsoft Azure Sentinel

24/7 Threat Visibility and Response Across Your Microsoft Ecosystem

Complete Multi-Cloud and Hybrid Environment Visibility

Get centralized visibility and account for risks across your Microsoft cloud ecosystem, other cloud service platforms, and traditional network security controls with Microsoft's cloud SIEM Azure Sentinel.

Unified MDR for Microsoft 365, Azure, and Beyond

We combine Security Orchestration, Automation, and Response (SOAR) technology with our Elite Threat Hunters and experienced Cyber Analysts to respond and contain threats across multiple vectors 24/7.

Integrated Detection Engineering

eSentire's Threat Response Unit (TRU) manages the entire detection engineering process, ensuring that your business keeps up with rapidly evolving attackers.

Highly Certified Microsoft Security Expertise

Team eSentire is Microsoft Security Gold-certified with cybersecurity experts to optimize your Azure Sentinel instance for MDR.

Your Challenges

Increased attack volume & sophistication

Detecting threats across an ever-expanding attack surface in multi-cloud and hybrid environments presents problems that aren't easily solved by technology alone.

62%

of organizations have 11 or more active cloud services and applications

(Cybersecurity Insiders 2020)

You're dealing with vendor sprawl and budget constraints

Security vendor and tool sprawl in combination with a post-pandemic operating environment has prompted many organizations to re-evaluate IT spend and strategy. Microsoft's integrated security tools including Azure Sentinel allow for consolidation.

39%

of organizations receive security alerts from 7 or more tools

(Neustar, 2020)

Your team lacks the cybersecurity resources to investigate and respond 24/7

The chances are your business does not have the in-house expertise and resources to properly optimize and manage tools like Azure Sentinel thanks to the perpetual global security skills shortage.

3.1M

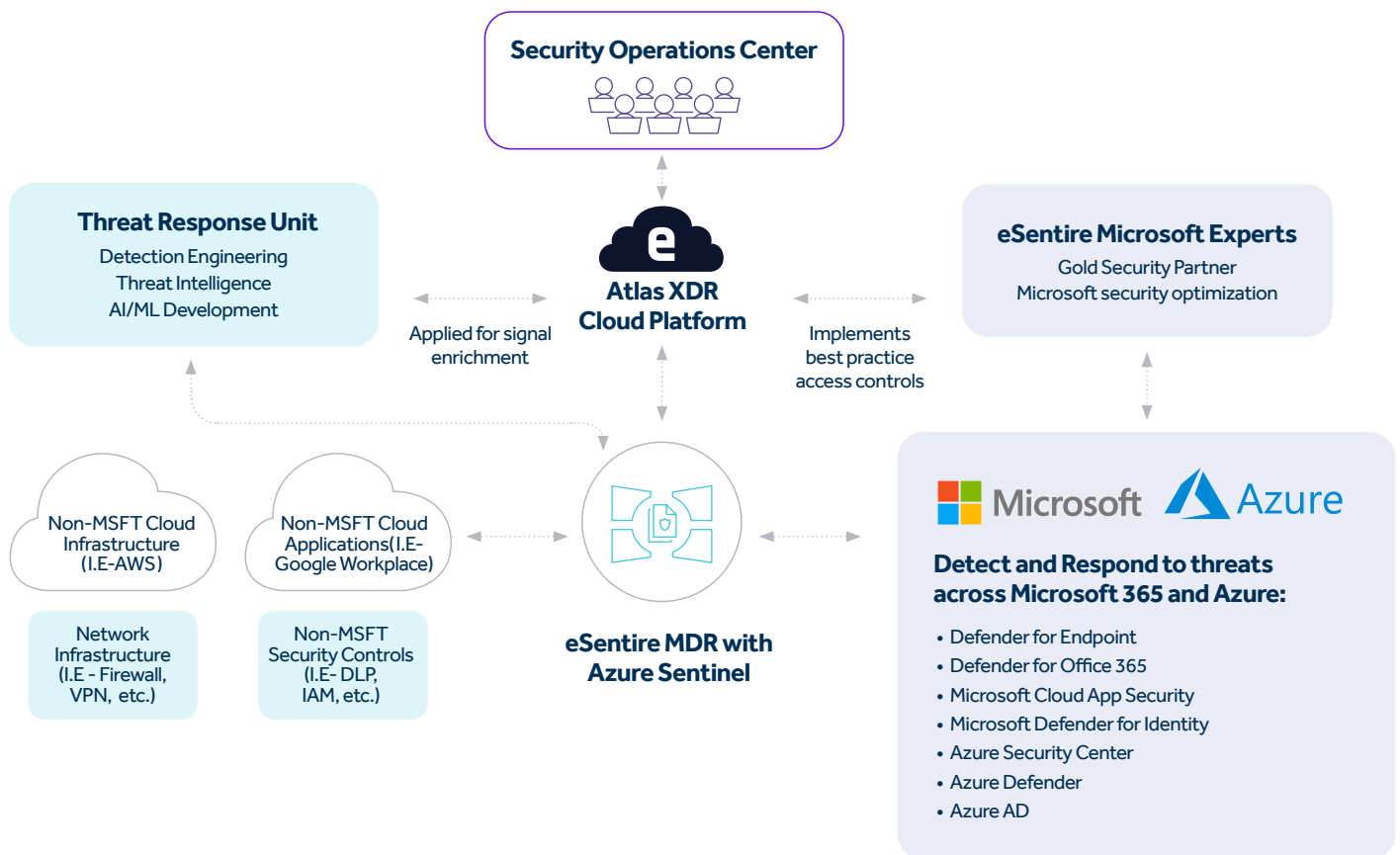
Global security skills gap

(ISC2, 2020)

The Solution

eSentire MDR with Azure Sentinel delivers critical threat visibility and 24/7 monitoring across Microsoft 365, Azure, multi-cloud, and hybrid environments. We leverage your existing investment in Azure Sentinel, Microsoft’s leading cloud SIEM platform, to provide our SOC cyber analysts important investigative context required to detect and contain threats before they impact your business. eSentire MDR’s integration with Microsoft 365 Defender XDR and Azure cloud security tools enables and streamlines rapid response to threats at multiple attack vectors including endpoint, email, and identity.

How it Works



Robust Multi-Cloud and Hybrid Environment Coverage

Detect threats across Microsoft 365 and Azure (including but not limited to):

- Microsoft 365 Defender
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Office 365
 - Microsoft Cloud App Security
 - Microsoft Defender for Identity
- Azure Sentinel
 - Azure Defender
 - Azure Security Center
 - Azure Active Directory

Detect threats in non-Microsoft cloud infrastructure and applications (including but not limited to):

- AWS
- Google Cloud Platform
- Google Workspace

Detect threats leveraging common security and network infrastructure tools (including but not limited to):

- Network security technology (Palo Alto, Cisco, etc)
- Email security platforms (Mimecast, Proofpoint, etc.)
- VPN providers (Palo Alto, Cisco, etc)
- Web gateway solutions (Citrix)

Not All MDR for Microsoft is Created Equal

	Other MSSP/MDR Providers	eSentire
24/7 monitoring of Microsoft 365 and Azure resources	✓	✓
24/7 monitoring of multi-cloud resources (AWS, GCP)	✓	✓
24/7 monitoring of legacy security and network infrastructure (i.e. – NGFW, VPN, email security)	✓	✓
Professional services delivered by Certified Microsoft Security Experts	Varies	✓
Integrated Response with Microsoft 365 Defender through an XDR platform – endpoint, email, and identity	Limited	✓
Full incident response support including remediation from our 24/7 SOC cyber analysts and threat hunting team	Limited	✓
Detection engineering from eSentire's TRU team – custom, proprietary threat content development for Microsoft, extensive runbooks, and Machine Learning-driven detections	Limited	✓

Maximize Your Investment in the Microsoft Security Stack with eSentire MDR

eSentire MDR with Azure Sentinel combines our multi-signal detection, 24/7 threat hunting, deep investigation, and complete response capabilities with your existing investment in the Microsoft's leading cloud SIEM. You can significantly reduce overall security spend and maximize ROI while substantially reducing the risk of suffering a business-disrupting breach.

Total Economic Impact of Azure Sentinel

67%

Faster time to deployment

79%

Reduction in false positives

79%

Cost reduction in SIEM costs (licencing, storage, and infrastructure spend with Azure Sentinel)

Forrester, 2020

Why Choose eSentire to Secure Your Microsoft Ecosystem



Response

We prioritize the R in MDR. We actively respond to threats on your behalf while the other guys overload you with alerts to investigate. That means we are actively containing threats and remediating security incidents across your environment.



Certified

We are certified as a Gold Microsoft partner and are proud Microsoft Intelligent Security Association (MISA) members demonstrating our leadership in multi-cloud security and Microsoft expertise.



Detection Engineering

Improved detection and response capabilities with our proprietary threat content, runbooks, and innovation in Artificial Intelligence & Machine Learning models, created by our industry renowned Threat Response Unit (TRU).



Time to Value

Leveraging the mature MSSP/MDR provider controls available via Azure Lighthouse results in faster time to value and minimized complexity. Our zero-install onboarding delivers value in hours not days or weeks. eSentire's disciplined service deployment and robust escalation processes ensure complete response when you need it most.




Cost Effective

Leverage your existing licenses and investment in Azure Sentinel to optimize your security posture with enhanced visibility, controls and response capabilities.

Are you ready to get started?

We're here to help! Speak with an eSentire Security Specialist to learn about eSentire MDR for Microsoft.

Get Started

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 Threat 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](https://twitter.com/eSentire).