eSENTIRE

Microsoft Solutions Partner
Security

Microsoft Intelligent Security Association
Microsoft
Microsoft Verified Managed XDR Solution

SOLUTION BRIEF

eSentire MDR for Microsoft

Complete Microsoft Ecosystem Visibility and Optimization

Centralize visibility and account for risks across your Microsoft cloud ecosystem. Get expert guidance and support from eSentire's Microsoft team to optimize your cybersecurity controls and overall posture.

Unparalleled Threat Response and Remediation

Build a resilient security operation by combining cutting edge XDR technology and our security expertise to stop and remediate cyber threats across endpoint, email, and identity vectors.

Maximum ROI on Microsoft Cloud Investments

Unlock the full potential of the controls and tools that exist within your investments in Microsoft Defender XDR and Microsoft Sentinel. Plus, our cybersecurity experts become a 24/7 extension of your team.

Highly Certified Microsoft Security Expertise

As an active member of the Microsoft Intelligent Security Association (MISA) we have achieved MXDR status with Microsoft and are a Microsoft Security Solutions Partner. We have managed over 250 Microsoft MDR deployments.

Your Challenges

1. You're dealing with vendor sprawl and budget constraints

Most organizations have to make sense of alerts from at least a half-dozen or more different security tools. At the same time, many are also re-evaluating IT spend and strategy to adjust to a post-COVID 19 pandemic operating environment.

This has led many organizations to replace legacy tools with Microsoft's advanced and highly integrated solutions that cover endpoint, email, cloud, identity and more. Microsoft bundles these tools in their enterprise licensing, offering their customers a cost-effective alternative to buying multiple separate security solutions.

39%

Of organizations reported they receive security alerts from seven or more different tools

(Neustar International Cybersecurity Council, 2020)

51%

Of organizations are concerned about security technology spend post-COVID 19

(ISC2 Cybersecurity Workforce Study, 2020)

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

Despite being familiar with Microsoft 365 or Microsoft Sentinel, your business may not have the in-house expertise and resources to properly optimize and manage these tools for ongoing threat detection and response.

3.1M

Global cybersecurity workforce skills gap

(ISC2 Cybersecurity Workforce Study, 2020)

The Solution

You need an experienced, and trusted partner to optimize and manage your Microsoft Security suite 24/7. Our Microsoft experts identify, contain, respond and remediate threats across Microsoft SIEM, endpoint, identity, email, and cloud security services stopping threats before they disrupt your business operations. Our MDR for Microsoft offerings include:

eSentire MDR with Microsoft Defender XDR

Stop advanced threats and minimize the risk of business disruption across your users, endpoints, and cloud applications.

- **Microsoft Defender for Endpoint**
  Endpoint protection, detection, response, and remediation
- **Microsoft Defender for Office 365**
  Mitigate the risk of phishing and business email compromise
- **Microsoft Defender for Identity**
  Investigate and respond to compromised identities and insider threats
- **Microsoft Defender for Cloud Apps**
  Rich visibility into data and user activity across your cloud SaaS applications

eSentire MDR with Microsoft Sentinel

Critical threat visibility and 24/7 monitoring across multi-cloud, and hybrid environments. Detect and investigate threats in:

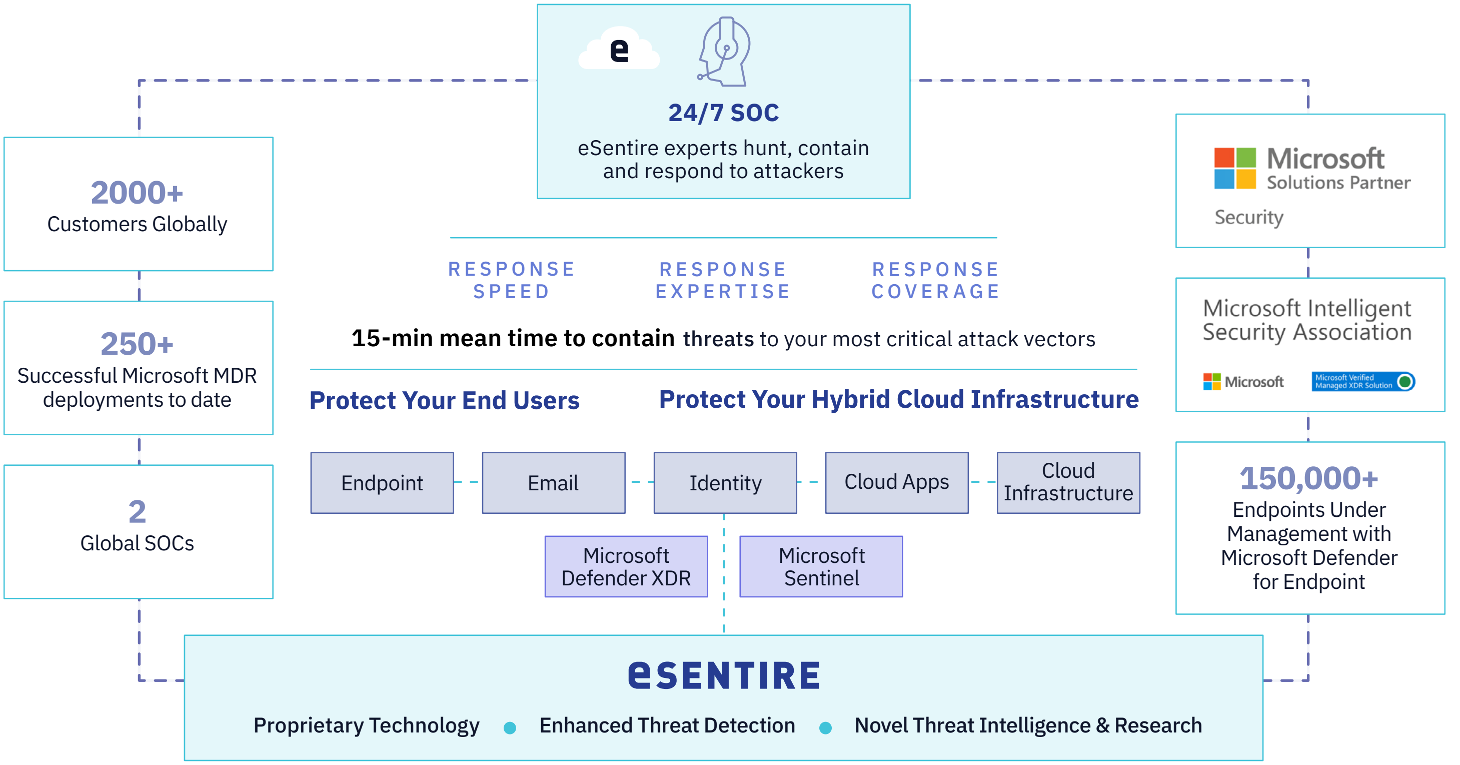
- Azure Active Directory
- Microsoft Defender For Cloud
- AWS
- Google Cloud Platform
- Google Workspace
- Existing Security Controls and Network Infrastructure

How It Works

Our dedicated Microsoft security experts help you operationalize Microsoft Defender XDR and Microsoft Sentinel to onboard our services. eSentire MDR directly and securely connects to your Microsoft environment, taking full advantage of the mature security provider controls that exist within Microsoft's platform. Additional software or hardware is not required, so we're able to deliver faster time to value and minimize complexity.

Once connected, eSentire ingests signals from your Microsoft Defender XDR and Microsoft Sentinel tools, enriching them with unique threat intelligence learned from new and emerging threat detections across our global customer base of 1500+ businesses globally. Our 24/7 SOC Cyber Analysts and Elite Threat Hunters rapidly respond to and investigate threats across your Microsoft environments, with a Mean Time to Contain of less than 15 minutes.

Every step of the way you are backed by Team eSentire, an experienced team of cybersecurity veterans, Elite Threat Hunters, and industry-renowned threat research experts who work together to put your business ahead of disruption.



24/7 SOC

eSentire experts hunt, contain and respond to attackers

2000+ Customers Globally

250+ Successful Microsoft MDR deployments to date

2 Global SOCs

RESPONSE SPEED · RESPONSE EXPERTISE · RESPONSE COVERAGE

15-min mean time to contain threats to your most critical attack vectors

Protect Your End Users · **Protect Your Hybrid Cloud Infrastructure**

Endpoint · Email · Identity · Cloud Apps · Cloud Infrastructure

Microsoft Defender XDR · Microsoft Sentinel

Microsoft Solutions Partner Security

Microsoft Intelligent Security Association

150,000+ Endpoints Under Management with Microsoft Defender for Endpoint

eSENTIRE

Proprietary Technology • Enhanced Threat Detection • Novel Threat Intelligence & Research

Response and Remediation at Critical Attack Vectors

At eSentire, we are proud to go beyond the market's capabilities in Response. We don't just detect and investigate threats across your Microsoft ecosystem – we actively respond and remediate them as well.

We deliver complete response across critical vectors including endpoint, email, cloud and identity. These vectors map to the most common attacker actions observed in successful breaches according to Verizon's annual data breach report.

Here's what you should expect from eSentire's complete response across your Microsoft environment:

Top Defined Attacker Actions Observed in Breaches:

Attack Vector	Response
Phishing	Email + Endpoint
Use of Stolen Credentials	Identity + Endpoint
Ransomware	Endpoint
Pretexting (Social Engineering)	Identity + Email

We hunt for threats across these Microsoft Services	We respond to threats at these vectors	Detect	Investigate	Isolate and Contain	Response and Remediation Outcomes
Microsoft Defender XDR • Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Microsoft Defender for Identity • Microsoft Defender for Cloud Apps **Microsoft Sentinel**	**Endpoint**	✓	✓	✓	• Prevent infected endpoints from spreading to other machines • Isolate ransomware, data exfiltration and hands-on keyboard attackers • Quarantine malicious files and terminate processes • Stop/remove service and registry keys • System reboot
	Email	✓	✓	✓	• Phishing attempts reported, investigated, and remediated • Facilitated retroactive malicious email and file and purges
	Identity	✓	✓	✓	• User-behavior based detections • Track log in and access activity across cloud SaaS applications • Response via AD credential suspension, locking out the user organization-wide

Maximize Your Investment in the Microsoft Security Stack with eSentire MDR

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

Total Economic Impact of MDR for Microsoft

~35%
Technology cost savings

~50%
Reduction in total implementation and management costs

~80%
Reduction in total management costs

~50%
Reduction in overall threat detection and response TCO

Why Choose eSentire to Secure Your Microsoft Ecosystem

Response and Remediation

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 isolate hosts, contain threats and remediate security incidents across your Microsoft suite.

Certified and Experienced

We are a Microsoft Security Solutions Partner and are proud Microsoft Intelligent Security Association (MISA) members, demonstrating our leadership in multi-cloud security and Microsoft expertise. We've overseen 250+ successful Microsoft MDR deployments to date.

Unique Intelligence, Powered by Our Threat Response Unit

Supercharge your Microsoft security investments with improved detection and response capabilities, our proprietary threat content, runbooks, and AI/ML innovations created by our elite Threat Response Unit (TRU).

Time to Value

Zero-install onboarding with time to value in days, not weeks or months. Disciplined service deployment and robust escalation processes to ensure complete response.

Complete Coverage

End-to-end cyber risk mitigation and coverage across our Exposure Management, Managed Detection and Response and Incident Response services.

Cost-Effective

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

Ready to Get Started?

Learn how eSentire MDR for Microsoft can help you secure your Microsoft ecosystem and build a more resilient security operation.

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**.