eSENTIRE

Microsoft Solutions Partner
Security

Microsoft Intelligent Security Association
Microsoft
Microsoft Verified Managed XDR Solution

eSentire MDR for Microsoft for Healthcare Delivery Organizations

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 365 Defender and Microsoft Sentinel. Plus, our cybersecurity experts become a 24/7 extension of your team.

Highly Certified 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

The widespread reliance on the cloud and the use of electronic health records by healthcare providers such as patient clinics, hospitals, and business associates has turned healthcare delivery organizations (HDOs) into prime targets for cyberattacks.

In addition, third-party exposure, flexible access to patient care, human error, legacy operating systems, and the increasing adoption of internet-connected medical devices and other healthcare IoT are all contributing factors to an ever-expanding attack surface.

Skilled adversaries now target the healthcare sector over others due to the nature of the data that HDOs have access to– patients' electronic protected health information (ePHI). The severity of cyberattacks, in addition to how fast cybercriminals can breach the perimeter to exfiltrate healthcare data, means that your security team must be able to minimize attacker dwell time and reduce the overall scope of the damage.

Given that your team must be able to prioritize the speed of your threat response, how fast you can identify, contain, and respond to a threat becomes crucial in your ability to prevent, withstand, and recover from cyberattacks.

As a result, your HDO must take action to protect the critical assets from attack, understand the existing key areas of risk and vulnerabilities within your organization, and understand the barriers that occur when developing, and implementing, a security program.

Why Invest in Microsoft Security Solutions

Many healthcare delivery organizations are rapidly shifting to the cloud as they prioritize speed, flexibility, scalability, and taking a cost-effective approach. Part of this transition includes an investment in Microsoft 365, which includes the traditional Microsoft productivity applications and cybersecurity services, all based in the cloud.

There are three primary reasons why healthcare organizations are increasingly relying on Microsoft 365:

- ✓ **Security tool consolidation**: Microsoft's security products allow teams to consolidate their spend to secure their endpoints, email, identity, SIEM, and cloud environments by implementing a zero-trust approach to their cybersecurity program – all consolidated within a fully interoperable, easy-to-manage platform.
- ✓ **Cost-effective security solution:** Microsoft offers cost-effective Office 365 plans for the frontline workforce and healthcare organizations that are designed specifically for the unique needs of HDOs by creating a "holistic approach to data security, privacy, and compliance to prevent incidents that could disrupt patient care".
- ✓ 2 **threat detection and response:** Microsoft also gives security operations teams the power to identify, detect, and rapidly remediate attacks in their earliest stages. This enables your team to gain comprehensive visibility across the full ecosystem and the ability to initiate response actions directly within the tools themselves.

Introducing eSentire MDR for Microsoft

At eSentire, we share Microsoft's zero-trust approach to cybersecurity and firmly believe that you need a certified, experienced, and trusted partner to protect your investment in the Microsoft ecosystem. As part of eSentire MDR for Microsoft security solutions, we offer complete multi-signal MDR across your Microsoft Sentinel and Defender for Endpoint, Identity, Office 365, and Cloud Apps services.

eSentire MDR with Microsoft 365 Defender

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

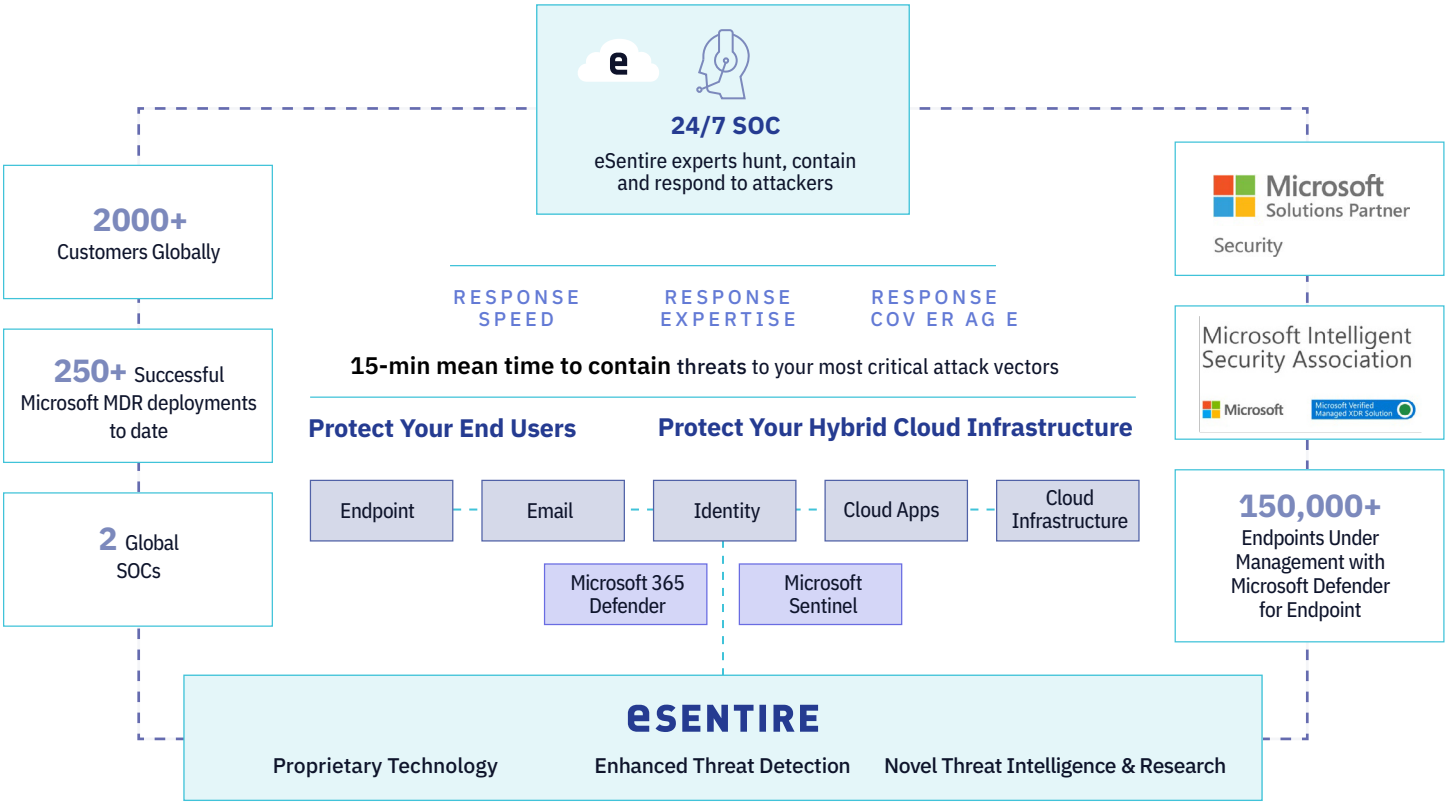
eSentire MDR with Microsoft Sentinel

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

Our dedicated Microsoft security experts help you operationalize Microsoft 365 Defender 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 365 Defender and Microsoft Sentinel tools, enriching them with unique threat intelligence learned from new and emerging threat detections across our global customer base of 2000+ 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.



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 365 Defender 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

Managed Detection and Response Services that Meet Cybersecurity Insurance Requirements

eSentire's MDR services have been specifically designed to rapidly identify and contain advanced threats to reduce cyber risk. We maintain partnerships with leading cyber insurance providers as an MDR provider of choice and offer complete threat protection that meets insurance requirements and can reduce policyholder costs for HDOs that are already grappling with budget constraints. Underwriters at cyber insurance organizations are looking to reduce policyholder risk and many times require policyholders to work with MDR providers like eSentire to develop and implement strong cybersecurity controls and governance.

Why Choose eSentire to Secure Your Microsoft Ecosystem

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry—financial services. Over the last two decades, we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale.

With two 24/7 Security Operations Centers (SOCs), hundreds of cyber experts, and 2000+ customers across 80+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in securing healthcare delivery organizations.

We protect over $6.5 trillion in assets across highly regulated industries, including healthcare institutions, medical technology, and pharmaceuticals. **In fact, more than 2.5 million patients pass through healthcare facilities that are protected by eSentire.** This includes defending our healthcare customers from a 200% increase in cyberattacks during the COVID-19 pandemic.

At eSentire, we go beyond the market's capability in threat response and specifically address cybersecurity risks for the healthcare sector. Our multi-signal MDR approach ingests endpoint, network, log, cloud, asset, and vulnerability data to enable complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit (TRU) are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. Our SOC Cyber Analysts, and Elite Threat Hunters are mission-driven to put HDOs ahead of business disruption. Powered by our industry-leading XDR cloud platform and unique threat intelligence, eSentire can detect and respond to cybersecurity threats in HDOs with a Mean Time to Contain of 15 minutes.

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.

At eSentire We Support Healthcare Delivery Organizations By:

- ✓ Preventing operational disruption of internal and constituent-facing services through a combination of 24/7 Managed Detection and Response, Exposure Management Services, and Incident Response Services
- ✓ Protecting your patients' electronic protected health information (ePHI) from ransomware attacks, third-party risk, data theft and exposure, and insider threats
- ✓ Mitigating third-party supply chain risk and supporting patient care with 24/7 threat detection, investigation, and complete response
- ✓ Ensuring that any regulatory penalties and third-party costs associated with data breaches are minimized
- ✓ Ensuring your HDO, and your business associates, remain compliant with stringent cybersecurity compliance and regulatory mandates, such as the HIPAA Security Rule
- ✓ Reducing your overall organizational risk by helping your team identify your critical sources of value, discover existing vulnerabilities, and address them based on what would have the worst impact to your organization

Whether your assets are stored in the cloud, on-premises, or in a hybrid environment, we detect and contain threats that other MDR providers miss. Our global 24/7 SOCs have discovered instances of ransomware gangs targeting our healthcare customers and have interrupted their activities before they could establish a foothold by:

- ✓ Using endpoint protection to prevent the disabling of defenses
- ✓ Detecting malicious administrative activity through remote access tools using proprietary machine learning algorithms
- ✓ Blocking active attempts to deploy user credential collection tools, malware payloaders, and multiple ransomware attacks

Key Healthcare Industry Challenges	How eSentire Managed Detection & Response Helps
Protecting Patient Healthcare Information	We are adept at securing all forms of sensitive data, such as electronic protected healthcare information (ePHI), HIPAA protected data, along with financial information (PII) and credit card or payment transfer services (PCI). Our 24/7 Elite Threat Hunters and SOC Cyber Analysts actively hunt for threats across your environment. We detect intrusions and contain attacks before data can be exfiltrated.
Operational Disruption and the Cost of Downtime	We detect malicious administrative activity through remote access tools and stop intrusions before malware can be deployed throughout your environment.
Protecting Against Supply Chain and Third-Party Vendor Risk	We identify core services, including electronic medical records (EMR), drug management, time tracking, file share and document signing, and prioritize these services for monitoring. We mitigate supply chain and third-party vendor risk. • eSentire Exposure Management Service experts support in creating a third-party risk management program for your business and support securing M&A and digital transformation activities. • eSentire MDR has repeatedly caught and stopped vendor compromises before the vendor reported the vulnerability.
Preventing Ransomware Attacks	We monitor your attack surface 24/7 to discover intrusion attempts, preventing the pervasive deployment of malware and ransomware. • We support multi-signal coverage ensuring visibility across endpoint, network, log, cloud, and other data sources for deep investigation and kill-switch response capabilities. • We offer endpoint protection to prevent your defenses from being disabled.
Avoiding Regulatory and Compliance Violations	Our MDR and Exposure Management services are designed to help you navigate the complexity of HIPAA Security Standards and put corrective controls in place. Our 24/7 Global SOCs leverages proven run books which include detectors mapped to requirements and reporting measures for PCI DSS, CCPA, GLBA, SOX, NYCRR, HIPAA, as well as state-level regulations.

eSENTIRE