IT Specialist eSENTIRE

eBOOK

Managed Detection and Response (MDR) for Microsoft Security

Industry-Leading Protection for Today's Productivity Apps, Cloud Services and Computing Ecosystems

I. Introduction: The Evolution of Microsoft Security

Microsoft has been the world's number one software provider for over 30 years, with approximately 90% of all computers currently running a version of the Windows operating system.[1] Over the past decade, as Microsoft transformed itself into a cloud company, it has doubled down on its security investments, acquiring best-of-breed product companies and strengthening its focus on research and development. Since 2015, Microsoft has spent approximately $1 billion per year on these efforts "to support a comprehensive, cross-company approach to cybersecurity."[2]

Now, Microsoft, the leading enterprise software company on the planet, is going all-in on security.

In August 2021, Microsoft announced a fourfold increase in its already high levels of cybersecurity investment. At the time, the company pledged to invest $20 billion over the next five years to advance its security offerings. It also promised to spend $150 million on helping U.S. government agencies upgrade their cyber defenses and expand security awareness training programs.[3]

Billed as a civic-minded initiative intended to help both public and private sector entities shore up their capabilities to counter a serious and pressing threat to national security, the move also positions Microsoft to assume a leadership role in the cybersecurity product market.

It's an opportune moment for Microsoft to take this step. Over 2020-2021, companies of all sizes and across industries began shifting more of their infrastructure to the cloud to support an increasingly remote workforce and enhance business agility. However, this shift involves change and investment.

Many organizations are also using this time of transformation as an opportunity to mitigate the problem of security vendor sprawl by consolidating their technology stack. There are many advantages to doing so, including ease of management, simplicity, and reduced costs. In fact, companies that choose Microsoft as their primary vendor gain access to a comprehensive set of capabilities that Microsoft describes as "end-to-end, best in breed and AI driven." [4] These capabilities are comparable to leading vendors' offerings in endpoint, email, identity, and cloud security.

However, maintaining a strong security posture requires far more than tools and technologies. Microsoft Security solutions also must be tuned, optimized, and properly managed. This means you need access to the right expertise 24/7.

> To truly make the most of your investment in Microsoft Security, and take full advantage of the visibility and control that these solutions deliver, you'll need high-quality prevention, detection, and response capabilities.

This support should be delivered by a team with industry-leading skills in threat hunting, detection engineering, data analysis, and event monitoring to create a complete picture of the attack chain, even across complex environments. More importantly, it should be enhanced with full-scale containment and rapid response capabilities to prevent minor incidents from progressing into business disrupting events.

[1] https://visual.ly/community/Infographics/business/just-how-big-microsoft
[2] https://blogs.microsoft.com/blog/2015/11/17/enterprise-security-for-our-mobile-first-cloud-first-world/
[3] https://www.reuters.com/world/us/cyber-threats-top-agenda-white-house-meeting-with-big-tech-finance-executives-2021-08-25/
[4] https://www.microsoft.com/en-us/security/business

In a world where 2.72 million information security jobs remain unfilled, and where the global cybersecurity workforce needs to grow by 65% to be able to effectively defend organizations' critical assets,[5] not every company has the in-house capabilities to protect their Microsoft ecosystem.

[5] (ISC)2 Cybersecurity Workforce Study, 2021

To gain ongoing access to the expertise that's essential for maximizing the value of Microsoft Security, a growing number of organizations are turning to Managed Detection and Response (MDR) services. With the right MDR partner, security programs get more than access to 24/7 Security Operations Center (SOC) capabilities. They also gain the ability to identify and stop threats at speed – before they become costly breaches or damaging operational disruptions.

The State of Cybersecurity by the Numbers

2.72M
Unfilled jobs in the global cybersecurity workforce[6]

65%
Rate that the cybersecurity workforce needs to grow by to defend organizations' critical assets[6]

39%
Security teams that report that they receive alerts from seven or more disparate tools[7]

[6] (ISC)2 Cybersecurity Workforce Study, 2021
[7] Neustar Cyber Threats and Trends Report, Jan – Jun 2020: Is This the New Normal?

II. The Business Case for Microsoft

Today's cybersecurity vendor landscape is more crowded than ever. Nearly 3,500 distinct companies compete with one another in the United States alone, offering products and services ranging from cloud misconfiguration monitoring to deep learning-powered threat intelligence.[8]

In the midst of such a crowded marketplace, organizational security programs are responding to the emergence of new threats and attack vectors by adopting additional security solutions. Without the proper resources to monitor more data sources, many confront excessive numbers of false positive alerts, noise, and complexity in the market. In fact, 39% of security teams report that they receive alerts from seven or more disparate tools.[9]

As a result, many growing and maturing companies are upgrading from Microsoft 365 E3 licensing to Microsoft 365 E5 because it includes far more extensive security and compliance capabilities.

Capabilities	Microsoft 365 E3	Microsoft 365 E5
Office 365 Data Loss Prevention	✓	✓
Microsoft Defender for Endpoint, Plan 2		✓
Microsoft Defender for Identity		✓
Microsoft Defender for Cloud Apps		✓
Azure Active Directory	✓	✓

In terms of security functionalities, Microsoft E5 licensing provides full visibility across email, identity, and cloud applications as well as comprehensive response capabilities. Microsoft Defender makes it possible for security teams to:

- initiate actions to keep malware from spreading,
- terminate processes & sessions to prevent attackers from exploiting the environment or stealing data, and
- purge malicious files and email.

To obtain comparable prevention, detection, visibility, and response capabilities, an organization would need to purchase solutions from at least four distinct security vendors. By bundling their E5 licensing together with Microsoft 365 and Azure licensing, Microsoft Security users will save 50% to 60% over the costs of a multi-vendor best-of-breed security tool stack.

"In today's world, it makes a great deal of sense – both financially and logistically – to roll five or six security controls that a company would otherwise be buying separately into Microsoft licensing. It's a product that's very competitive with the market-leading vendors' offerings, and ***Microsoft has an advantage because it can incorporate security functionalities right into the operating system. There's no need for an agent. These are best-in-class tools that are already consolidated."***

- Mark MacDonald, Manager, Product Marketing at eSentire

[8] https://www.cyberdb.co/database/usa/
[9] Neustar Cyber Threats and Trends Report, Jan – Jun 2020: Is This the New Normal?

The cost savings alone is enough to make a compelling business case for the switch, but Microsoft also gives security operations teams the power to see, find, and rapidly remediate attacks in their earliest stages.

By moving to the Microsoft Security suite, your organization can leverage endpoint, email, identity, and cloud security capabilities as well as security information and event management (SIEM) and security orchestration, automation, and response (SOAR) functionalities – all consolidated within a fully interoperable, easy-to-manage platform.

This enables your team to gain comprehensive visibility across the full ecosystem and the ability to initiate response actions directly within the tools themselves. The fact that they're natively integrated with the Microsoft cloud platform inherently simplifies the task of monitoring them.

Choosing Microsoft in the Real World

Venerable is a leading organization in the insurance and annuity sector. From the outset, decision-makers wanted to adopt a cloud-native approach for all internal applications and architecture. Initially, Venerable relied heavily on Amazon Web Services (AWS), but chose to adopt Microsoft Azure and Microsoft 365 to decrease their reliance on a single cloud platform.

eSentire facilitated a seamless transition from Venerable's existing redundant endpoint licensing to Microsoft Defender for Endpoint to consolidate their security spending and to maximize their investment in Microsoft Office 365 E5 licensing. As part of the migration, eSentire provides 24/7 MDR services and leverages Venerable's own Defender for Endpoint licensing.

The transition to Microsoft enhanced the firm's disaster recovery efforts, while enabling the Venerable team to leverage technologies and platforms that are also used by their customers.

Since Venerable's security team is focused on moving ahead of the business roadmap based on the needs of their end customers, eSentire has shown the capability to outpace the market in terms of their innovative, and transparent roadmap of services.

In fact, from the very start, eSentire's differentiator has been the market leadership and specialization demonstrated by the team in the MDR space in addition to the cyber expertise shown continually by eSentire's team of security experts who are committed to 24/7 threat detection, eyes on glass capabilities, and immediate support in case of an incident.

"Being able to have someone you can reach out to if something's gone sideways and know they're a trusted partner who understands your environment and the MDR space was essential for us," said Simon Scully, Assistant Vice President, IT Security - Security Operations at Venerable.

Read the Full Case Study

III. Microsoft Security Capabilities

As successful ransomware and software supply chain attacks continue to grow,[6] there is much work to be done in securing an organization's increasingly distributed infrastructures. Unfortunately, cybersecurity teams continue to fight a losing battle to keep up with the expansion of the attack surface along with more complex business requirements. While traditional security controls and managed security services were once adequate, they're no longer enough.

Microsoft Security solutions give security teams with the proper expertise and resources the visibility and threat disruption capabilities they need to achieve these outcomes. Microsoft describes its approach to security as providing comprehensive, unified management across the entirety of the IT ecosystem. The emphasis is on multi-signal coverage that's as extensive as possible, in keeping with Microsoft's Zero Trust approach.

Microsoft offers strong user identity and device health verification capabilities as well as least-privilege access to resources and services. According to Microsoft, Zero Trust is enforced with data insights that security teams can leverage to reduce the risk of unauthorized lateral movement across the network. [7][8]

To contain today's growing cyber threats, defenders must take a multi-signal approach that protects the entirety of the attack surface. They also need rapid response and containment capabilities that can stop even the most sophisticated adversaries at any stage of the attack lifecycle. This is exactly what leading Managed Detection and Response (MDR) solutions offer.

Mapping Microsoft Security Coverage onto the Attack Vectors Most Frequently Exploited in Real-World Breaches

- **Phishing** played a role in over 80% of the breaches analyzed in the 2021 Verizon Data Breach Investigations Report (DBIR), while sending emails under false pretenses (including Business Email Compromise) was involved in 15% of attacks.[12] **Microsoft Defender for Office 365** includes robust filtering capabilities to prevent these attacks, AI-based detections to identify suspicious content and attack patterns, email-focused investigation and threat hunting capabilities, and the ability to automatically purge malicious emails and files.

- **Privilege abuse** was part of the attack sequence in 75% of the breaches investigated in the 2021 DBIR. In nearly all breaches, attackers must obtain elevated credentials if they are to move laterally across the environment to discover and exfiltrate valuable data. **Microsoft Defender for Identity** leverages Azure Active Directory or on-premises Active Directory to apply advanced analytics to monitor user and entity behavior, identify suspicious activities and enable rapid containment by suspending or locking out access or temporarily revoking privileges.

- **Malware** was used by threat actors to gain an initial foothold in an environment in only 20% of breaches examined in the DBIR but played a role during or immediately prior to data exfiltration in over 60% of the breaches. **Microsoft Defender for Endpoint** enables vulnerability and misconfiguration management on endpoint devices as well as threat monitoring and analysis. It also allows defenders to isolate ransomware, stop data exfiltration, and block hands-on keyboard attackers by quarantining malicious files, terminating processes, or rebooting affected systems.

[6] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[7] https://www.microsoft.com/en-us/insidetrack/transitioning-to-modern-access-architecture-with-zero-trust
[8] Verizon Data Breach Investigations Report

"The Microsoft Defender stack is comprised of an endpoint security solution, an identity solution, an email solution, and a cloud security solution," says Kurtis Armour, Vice President of Product Management at eSentire. "Together, those capabilities encompass everything you need to be able to stop a threat. From phishing and social engineering to lateral movement and initial code execution, the vectors that are exploited in nearly 100% of attacks are covered by Microsoft Security. These tools enable us to do deep-dive investigations of any incident that took place in any of our customers' environments."

What sets Microsoft's approach apart is that all these different enforcement and visibility points are seamlessly correlated and integrated – with standardized data schemas – within a single platform. In addition, Microsoft Sentinel provides cloud SIEM and SOAR capabilities that enable log monitoring and response to events generated by sources across the Microsoft cloud ecosystem, including Azure Active Directory, as well as non-Microsoft signal sources.

"Microsoft Security solutions provide a special set of first-class citizen signals that we have a deep, bi-directional connection to," says Mark Gillett, Vice President of Product Management at eSentire. "This gives us a ton of power and visibility to be able to detect and respond at a wide array of enforcement points. Tools like Microsoft Defender for Identity have a huge advantage because Active Directory is so widely used. It contains a broad array of behavioral detections, as well as a set of response buttons we can push to lock out a user who's behaving suspiciously."

To contain today's growing cyber threats, defenders must take a multi-signal approach that protects the entirety of the attack surface. They also need rapid response and containment capabilities that can stop even the most sophisticated adversaries at any stage of the attack lifecycle. This is exactly what leading Managed Detection and Response (MDR) solutions offer.

IV. Protecting Your Investment in Microsoft from Rising Threats

Given that Microsoft products are so widely deployed, it's no surprise that they're a prized target for attackers. With an estimated 1.5 billion people around the world using the Microsoft Windows operating system daily, any zero-day vulnerabilities that adversaries uncover may potentially allow them to breach an enormous number of systems.[9]

Over the past year alone, multiple zero-day vulnerabilities in Microsoft software have been publicized, both by Microsoft and by independent security researchers. One such vulnerability, CVE-2021-26855, involved Microsoft Exchange Server, and opened the possibility that a remote attacker could compromise the confidentiality of a user's email with no interaction from that user.

Another vulnerability, CVE-2021-31959,[10] made it possible for a remote attacker to seize full control of a targeted Windows computer without help from the end user. At the time of its discovery, it had already been exploited in the wild.[11]

Microsoft's responses to, and handling of, these security incidents has drawn praise from industry experts, who note that "they probably have the finest-honed security process around."[12] Nonetheless, the fact that these code-base vulnerabilities continue to be discovered speaks to the fact that organizations cannot rely on application-level security to be infallible, however diligent its vendor might be.

This is why a multi-layered approach to security that also includes rapid detection, response, and remediation capabilities is so important – no matter how robust your protections are.

To ensure this multi-layered approach to security, your organization requires human expertise. You need people who can monitor, support, tune, optimize, integrate, investigate, and respond within the Microsoft Security ecosystem to maximize its value.

This is where MDR comes in. A top-notch MDR provider gives your organization access to the skills and expertise you need to operationalize Microsoft's capabilities and harden your defenses across the entirety of the Microsoft Security ecosystem.

Organizations should look to partner with providers that highly certified, active members of the Microsoft Intelligent Security Association (MISA) and are certified as a Microsoft Security Partners. MISA members have demonstrated expertise in managing, and securing, the entire Microsoft Security suite 24/7.

As a Microsoft Gold Security Partner, eSentire has demonstrated deep response capabilities. eSentire detects and investigates threats across an organization's Microsoft ecosystem, in addition to actively responding by isolating hosts, containing threats, and remediating security incidents on the customers' behalf.

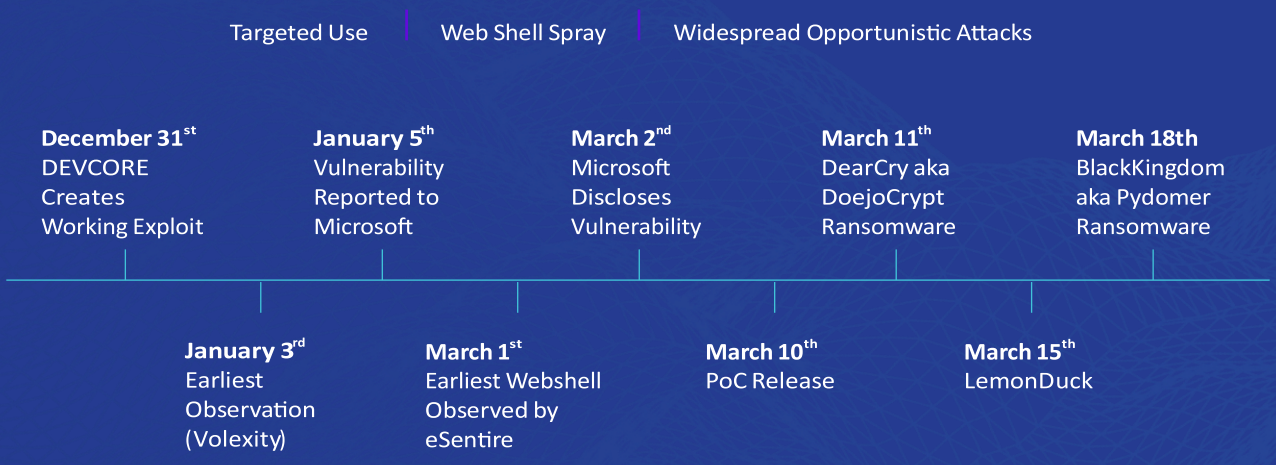
[9] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
[10] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31959
[11] https://krebsonsecurity.com/2021/06/microsoft-patches-six-zero-day-security-holes/
[12] https://www.csoonline.com/article/3635849/microsofts-very-bad-year-for-security-a-timeline.html?page=2

The Need for Speed Against Zero-Day Attacks

By definition, zero-day vulnerabilities are those that are known to adversaries but not to the software's vendor. There are no patches in existence that users can apply to repair these vulnerabilities. Unfortunately, as vendors begin to develop and release patches quickly, threat actors are striving to move even faster to beat vendors' time-to-patch. In this race, speed is of the essence.

The timeline of the ProxyLogon zero-day vulnerability provides an illustrative example that shows how MDR can improve upon the capabilities of vendors' vulnerability management programs.

- The ProxyLogon zero-day vulnerabilities were discovered on December 31, 2020.
- On March 1, 2021, eSentire's Threat Response Unit (TRU) began detecting post-compromise WebShell activity.
- Although the vulnerability was reported to Microsoft in January 2021, it wasn't until March 2, 2021 that Microsoft disclosed the vulnerability – one full day after eSentire had already begun a Global Threat Hunting operation.
- In March, Microsoft reported that the advanced persistent threat (APT) group HAFNIUM was behind the exploitation that had occurred prior to public disclosure.
- As a result, 22 true positives were detected and remediated in customer environments.



Because zero-day attacks cannot be prevented through patching, well-developed detection and response capabilities are critical for identifying and blocking post-exploitation activities.

Protecting your Microsoft environment from attacks leveraging undiscovered vulnerabilities requires more than high-caliber detection and response capabilities. You need a team of highly skilled elite threat hunters who work as an extension of your team, developing sophisticated hunting tools and new detections enriched by original threat intelligence research on your side to keep you ahead of zero-day attacks.

In this case, eSentire's Threat Response Unit discovered a critical vulnerability before Microsoft disclosed it publicly, so eSentire's customers were always one step ahead of their peers – in terms of both knowledge and protection.

V. MDR: An Essential Partner to Microsoft Security

For a security team to achieve high-quality 24/7 threat detection, investigation, and response, two essential elements are needed:

- High-quality tools
- High-quality expertise

Microsoft provides the high-quality tools, but they still need to be configured properly and monitored 24/7. Organizations have traditionally sought out managed security services providers (MSSPs) for this support, but that presents limitations.. For one, traditional MSSPs inundate security teams with alerts and false positives. Moreover, MSSPs focus on preventative measures and a high-level overview of security posture. Actively responding to threats isn't their forte.

Top-tier Managed Detection and Response (MDR), on the other hand, goes much further than the alerting that MSSPs offered in the past, providing complete response and remediation capabilities. This is especially important considering how organizations' security needs are currently shifting.

Organizations are now seeking managed security services that provide multi-signal coverage, ongoing threat hunting conducted by experts, and rapid response capabilities that go beyond merely isolating an infected endpoint or alerting the customer that an incident has taken place.

Today's industry leading MDR providers can achieve full incident resolution at speed, and scale, on behalf of their clients. This goes all the way to getting IT assets back to a "good as new" or "ready to work" state.

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

There are five core capabilities that an MDR solution must have for robust protection: Threat intelligence, Visibility, Automation, Human-led threat detection, response and remediation, and Risk reduction over time.

1

An effective security strategy requires threat intelligence – an in-depth, current understanding of the "known bad" so that these attack tactics can be automatically blocked. In addition, all blocking rules need ongoing tuning or curation. A fine balance must be achieved to limit the number of false positives and block as much malicious activity as possible.

MDR enables an organization to keep pace with the evolution of the threat landscape by staying informed about the latest trends in attack tactics, techniques, and procedures (TTPs). A first-rate provider will go one step further, conducting extensive threat intelligence research so the organization's security team can always stay one step ahead of industry news sources and intel feeds.

Their clients will also benefit from security network effects: if, for instance, the MDR provider becomes aware of a vulnerability that has impacted one Microsoft customer, it will rapidly move to ensure that all others in the global customer base are protected from the same vulnerability.

2

Although Microsoft's suite of security products allows your team to gain this visibility using Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft Sentinel, you still need human expertise to translate this visibility into value, including the ability to accurately detect and rapidly contain malicious or suspicious activities.

MDR providers that embrace a multi-signal approach can also ingest other log sources, multi-cloud data signals, network signals, vulnerability data, and more to further their investigations and drive response across multiple points. Ultimately, collecting and correlating data across multiple signals is what enables security analysts and threat hunters to gain a deep, contextually enriched understanding of what's going on in your IT environment to drive rapid investigation and actionable intelligence.

3

When it comes to preventing a data breach, time is of the essence. The automated response capabilities derived from an AI and ML-driven XDR platform enable an MDR provider to enhance threat investigation and detection, gain necessary context around alerts, eliminate noise, and rapidly take containment actions when an alert is a true positive. This means that when MDR is built on a foundation of XDR, it can deliver faster and more comprehensive response capabilities.

4

Accurate detection requires rich signals, but it also demands expertise in content engineering. While Microsoft may allow your security operations team to isolate and contain a threat, you need human-led security expertise to decide when, and how, to initiate these responses with context – and when to rely on automation-driven capabilities. In short, you must evaluate how quickly your team can investigate, respond to, and remediate threats. First-rate MDR providers will go beyond Microsoft-provided content to refine the platform with additional detections and custom content on an ongoing basis.

5

Risk Reduction over Time

Taking proactive steps to keep threats out of the environment is important. An industry leading MDR provider should leverage data and lessons learned from their ongoing MDR operations to continuously reduce their clients' risk over time. Security teams will benefit from mapping the detections created by their threat intelligence teams to industry standard frameworks like the MITRE ATT&CK, which can then be leveraged to quantify your organizational cyber risks and inform the overall cybersecurity strategy. This approach allows you to reduce risk by allocating budgets to the areas where they're most vulnerable.

VI. What to Look for in an MDR Provider for Microsoft

With so many MDR providers on the market today, it can be challenging to make sure you're getting the protection your business truly needs. Here are five questions to ask prospective MDR for Microsoft providers:

1

Can you handle all the technologies that are in use in my environment, including those that aren't from Microsoft?

Although Microsoft Sentinel is a powerful security analytics solution, and although it can handle data from nonMicrosoft sources, it still prioritizes signals from Microsoft tools. Keep in mind that Microsoft Defender doesn't work with older versions of Windows (which can be problematic if you have highly customized legacy systems that you can't easily upgrade). If you are running legacy security tools like on-premises firewalls, non-standardized operational technology (OT) systems, Internet of Things (IoT) sensors, or edge computing devices, how will the provider monitor these parts of your infrastructure?

Look for an MDR provider who has the expertise and technology infrastructure needed to derive value from all the signals in your environment, not just those that come from Microsoft. Typically, this comes from having access to an extended detection and response (XDR) platform. XDR is an innovative technology that enables high-fidelity detection, faster and more accurate investigation, and automated response across a broad range of security tools and signal types.

2

Do you have expertise in security monitoring, threat hunting, incident containment, and response across both Microsoft and non-Microsoft environments?

Attackers' TTPs aren't radically different for Microsoft customers. In addition, very few organizations are running only Microsoft solutions. It's far more common to have resources in multiple cloud platforms, Software-as-a-Service (SaaS) applications, and legacy systems, even if you are striving to become a 100% Microsoft shop.

3

How many other Microsoft customers do you work with?

Network effects have powerful benefits in information security: if a security operations team is seeing something like the Exchange Server vulnerability being exploited in the wild in one client's environment, they'll know to proactively look out for this threat in others' environments.

4

What does "Response" mean to you as an MDR provider? How will you take action on my behalf?

There are major differences among providers when it comes to the quality of response. Many MDR providers will offer nothing more than lightweight tactical isolation. They will limit the response actions they're willing to take on their clients' behalf to simply isolating infected systems or the suspending accounts harboring suspicious user behaviors. This leaves the client to deal with the aftermath of the cyberattack on their own.

Industry leading MDR providers, on the other hand, orchestrate remediation across the entirety of the attack lifecycle, with little customer involvement needed at all. They leverage Microsoft Security's capabilities to go beyond containment

actions and into full incident remediation efforts by removing all traces of the attackers' presence from the environment and restoring systems to full working order.

5 **Which certifications do you hold?**
Microsoft Security Competency certifications are difficult to obtain and represent true expertise in managing and working with the platform. To become a Microsoft Gold Partner, an MDR provider must meet performance requirements and have multiple security administers and engineers on staff who have validated their skills by passing examinations. Look for an MDR provider that belongs to the Microsoft Intelligent Security Association (MISA), since these organizations share threat intelligence and product integrations.

VII. Conclusion

There's little doubt that Microsoft Security provides powerful threat detection, investigation, and response capabilities. Growing numbers of organizations are replacing legacy security tools with Microsoft's advanced and cost-effective cybersecurity solution suite. In fact, making the move to Microsoft Security can simplify your security tool stack while saving you money and enhancing centralized visibility.

Given the ongoing shortage of skilled cybersecurity professionals, though, few organizations have access to the in-house expertise and resources needed to properly manage and optimize these tools.

To realize the full value of your investment in Microsoft Security, you need an experienced, certified, and trustworthy partner who can manage these solutions 24/7 to shrink attacker dwell times and reduce the risks of business disruption. Combining first-rate MDR with your existing investment in the Microsoft ecosystem can significantly reduce your overall security spend and put your business ahead of threat disruption.

Not All MDR for Microsoft is Created Equal

Leverage your existing investment in the Microsoft ecosystem and accelerate your security program with eSentire's 24/7 Managed Detection and Response (MDR) service to shrink threat actor dwell time and reduce the risk of business disruption.

At eSentire, we don't just detect and investigate threats across your Microsoft environment, we provide complete and robust response. This means we not only isolate and contain threats, but we fully remediate incidents on your behalf. Here's what you can expect from eSentire MDR for Microsoft:

We hunt for threats across threat Microsoft Services	We respond at these vendors	Detect	Investigate	Isolate and Contain	Response and Remediation Outcomes
Microsoft 365 Defender • Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Microsoft Defender for Cloud Apps • Microsoft Defender for Identity	**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** • Retroactive malicious email and file purges

Microsoft Sentinel	**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**

We operate Microsoft Sentinel in conjunction with our own Atlas XDR Cloud Platform, a proprietary cloud-native solution that leverages patented machine learning models to eliminate noise and ensure alert fidelity. With this architecture, we're able to handle a full complement of Microsoft and non-Microsoft signals. And we can orchestrate response actions in whichever platform has the greatest control and efficiency.

Unlike MSSPs, eSentire MDR doesn't just deliver alerts. Instead, our focus is on delivering superior security outcomes. We provide the expertise, resources, and supplemental capabilities you need to optimize and manage Microsoft Security's full set of functionalities. We share Microsoft's vision of a Zero Trust approach to cybersecurity, and believe that skilled, ongoing monitoring is critical for successful security outcomes.

Our Commitment to You:

- **Complete Microsoft Ecosystem Visibility and Optimization:** Centralize visibility and account for risks across your Microsoft cloud ecosystem. Expert guidance and support from eSentire's Microsoft team to optimize your cybersecurity controls and overall posture.
- **Unparalleled Threat Response, Remediation, and Containment:** 24/7 MDR leveraging our Atlas XDR platform, Microsoft Security tools, threat hunting and cloud security experts. We respond to 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 existing investments in Microsoft 365 and Azure. Plus, engage our cybersecurity experts as a 24/7 extension of your team.
- **Highly Certified Expertise:** We are an active member of the Microsoft Intelligent Security Association (MISA) and are certified as a Microsoft Gold Security Partner.

Ready to get started?

It's time to reclaim the advantage and put your business ahead of disruption.
Build a more responsive security operation today with eSentire MDR for Microsoft.

Contact Us

If you're experiencing a security incident or breach contact us **1-877-317-2414**

eSENTIRE ITSpecialist

IT Specialist Advisory Services is an IT procurement firm specializing in cloud computing, cybersecurity, and managed services. We help organizations save time, money and resources in the acquisition of information technology from leading service providers in the U.S and abroad .

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries 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**.