CRITICAL**START**®

Guide to Managed Detection and Response and Microsoft Security

Managed Detection and Response Deployment Strategies to Maximize Protection and Performance from Microsoft Security Tools

CRITICALSTART®

TOPICS INCLUDE

- ✓ **Understanding the critical role MDR plays when integrated with Microsoft Security tools**
- ✓ **Risks that must be considered when deploying a new MDR strategy**
- ✓ **The right questions to ask to aid in evaluating any MDR platform**
- ✓ **Microsoft 365 Defender, Microsoft Defender for Endpoint and Microsoft Sentinel comparisons to support decision making around Microsoft Security and MDR**
- ✓ **Critical Start's approach to the most effective utilization of MDR when integrating with Microsoft Security products**

Microsoft Security Offers Bold New Tools

Here's how to make them even better.

There's no denying that Microsoft Security is moving to stay ahead of constantly evolving security threats. Forrester recently named Microsoft a Leader in the 2021 Forrester Endpoint Security Software as a Service Wave. The organization has also updated several security products to help businesses move to a zero-trust security model. But with the hyper-complexity of today's security environment, combined with a weak security posture found in many enterprises, compounded by a shortage of cybersecurity talent, an aggressive and proactive approach to cybersecurity becomes critically important. With an attack surface that is constantly changing, where access roles are dynamic, and devices and applications request and keep more data, tools alone are not enough. Tools, talent and new process and methodology are needed for cross-enterprise isibility into threat detection, investigation, and remediation.

Microsoft makes great strides in this area, with a suite of products to not only identify a threat as it happens, but to deliver visibility as the threat attempts to move across an organization's security landscape. But many organizations still struggle to have the right talent and process to make the most effective use of this information. They might have a team that's strong at email security, but still doesn't know the best way to handle an alert that comes from an endpoint. What's needed is a team with the expertise and methodology to make sense of Microsoft's crossenterprise visibility threat detection and auto investigation capabilities to radically reduce alerts and actively respond to threats.

Putting Microsoft Security to Work the Right Way

At Critical Start, most security gaps we see today are around configuration and maintenance. Microsoft tools have the capability to close these gaps and extend the security umbrella, but organizations need support in operations and maintenance to use them effectively.

MDR is the Rosetta stone for Microsoft Security

MDR brings the talent, process, and expertise to put platforms like Microsoft 365 Defender, Microsoft Sentinel and Microsoft Defender for Endpoint to work as part of a unified security plan—a plan that closes gaps and provides a highly-agile response to alerts and potential breaches. By working with a security partner that utilizes their own analysts, tools, threat identification strategies and procedures to be proactive in responding to cyberattacks, damage from these attacks can be effectively mitigated for far less cost than an internally developed solution.

MDR helps maximize the value of Microsoft Security solutions, reports on security posture across the environment and protects a company's brand, revenue, and important assets, by reducing risk acceptance and accelerating return on investment. If configured properly, MDR can limit access to only what a user needs to do their job and alert analysts to suspicious actions based on the user's identity. It often utilizes artificial intelligence (**AI**) to prioritize alerts, consolidating everything onto one platform to provide comprehensive visibility to the Security Operations Center (**SOC**). Analysts can then decide on the alerts that represent a security threat and respond with direct action, such as isolating an endpoint, changing passwords, or whatever action in necessary to prevent the attack from moving within the network.

MDR is the latest evolution to protect organizations from a highly diverse, multifaceted threat environment, including everything from individual hackers to nation states. But perhaps its most important benefit is that a company can access the latest security expertise without hiring internally, and available resources can grow with the business without the need to add additional personnel.

MDR Growth

Frost and Sullivan forecasts that the MDR market will grow at Compound Annual Growth Rate of 16.4% over the next few years, reaching $1,907.9 million by 2024

How to select the right MDR partner

While MDR has a clear value in maximizing the performance of Microsoft Security solutions, this value will only be realized by working with a partner that intrinsically knows the technology—and their knowledge cannot simply be a snapshot in time.

The right MDR vendor is actively engaged with Microsoft on a continual basis. They work with Microsoft regularly, so they can track the trajectory that Microsoft is developing with certain products. That will enable them to develop a plan that makes the most of new capabilities as they become available.

Always consider the risks

But to find the right partner, you should consider not only their expertise, but also any policies that can open up new risk for your organization. As an example, there are MDR providers that will ask for almost unlimited permissions when provisioning their SOC users into a customer's system. But there is usually no reason for an MDR vendor to have that level of access into your critical systems and data. A good partner should be willing to set up service-level permissions and individual human level permissions that provide an audit trail and are limited to just what's needed to do the job effectively. For quality MDR with Microsoft Security, there's no reason to give away the keys to the castle.

Check the Credentials

Always check the certifications of any vendor you're considering to truly understand their level of knowledge. Critical Start team members' certifications range from MS-500: Microsoft 365 Security Administration to SC200 and AZ-500: Microsoft Azure Security Technologies. The team also uses Microsoft Security Best Practices to deploy Microsoft Sentinel and Microsoft Defender 365 tools to optimize Microsoft content for both Scheduled Query Rules and Indicators of Compromise (IOCs).

Ask the right questions

There are questions you should be asking to ensure the MDR partner you select has the foundation in place to help you build a strong relationship with someone you can trust to help you get the most from your Microsoft Security products. Some of these questions include:

Are you experts with every aspect of Microsoft Security?

The MDR team you work with must regularly work with Microsoft to understand every capability and limitation of their products to improve SOC efficiency and reduce acceptance of risk. They need to use the unified Microsoft Security Information Event Management (**SIEM**) and Extended Detection and Response (**XDR**) stack effectively to quickly detect every alert, resolve every incident and respond to breaches across your organization. Beyond monitoring alerts, they need to bring shared responsibility for cyber incident response using Microsoft Sentinel, where security ownership must be clearly defined with each party maintaining complete control over the assets, processes, and functions they own. They also need to deploy the principle of least privilege, where users have only the minimal level of rights to perform their necessary job functions. And they need to maximize the value of your investment by applying their knowledge and experience to understand your Microsoft Security environment at a deeper level than other vendors. They need to help assess how modern attacks can impact your organization and design a customized strategy to better defend your environment against potential threats.

Can you help us deal with compromised identities?

The right MDR partner should be able to help you leverage Microsoft's automated investigations and actionable incidents to modulate and adapt for identity, check for globally trusted behaviors, and escalate for validation with enriched data warning signs such as risky sign-ins, logons from unfamiliar IPs, and impossible travel. An investigation can confirm if a user has been compromised or if the identity does not present any risk. If a user is deemed not risky, the MDR provider can dismiss the user's risk, allowing them access again. They can also confirm if a user has been compromised following an investigation.

Do you treat all alerts equally?

Many vendors practice alert suppression to reduce the overall volume of alerts while only focusing on alerts categorized as critical or high. And they may not even be able to effectively automate the process for closing these alerts. But here's the real problem: Ransomware attacks can often register only a medium- or low-priority alert. That's why we use the Critical Start Zero-Trust Analytics Platform® (**ZTAP**®) to investigate every alert. The Trusted Behavior Registry® (**TBR**) within ZTAP is designed to eliminate false-positives at the scale by resolving known-good and safely trusted alerts. A platform like ZTAP can consolidate visibility across the Microsoft Security ecosystem and across hybrid device types so that MDR analysts can focus on remediating the true positive alerts that might indicate a threat.

How many professional services do I need to buy from you outside of MDR?

At Critical Start, we provide a full suite of multi-spectrum security services including incident response, threat hunting, penetration testing and more. But we don't require a client to contract for our other services as the price of admission for MDR. Basically, you need to work with someone who can play well with other partners that are part of your security mix to offer just as much, or as little, security solutions that you need to round out your portfolio.

Ask the right questions

Are you providing a 24x7x365 service?

The need for this may seem obvious, but there are actually MDR vendors that view security as a 9x5 service. But when threats can come in from anywhere in the world at any time, day or night, the need for a vendor who can match the timing and pace of those threats becomes clear.

How many real humans will be protecting my environment?

Some MDR offerings provide a chatbot that notifies you of suspicious activity in Microsoft Sentinel and then simply give you a link to the issue. But would you rather deal with a chatbot, or a live MDR analyst that has identified the problem, taken direct action to mitigate the issue, and then is ready to make a full report to you over your mobile device? The right MDR vendor should offer you the mobile tools to empower you to take charge of your security from anywhere, and you should always be able to collaborate with industry-leading expertise when a threat is detected.

How extensive are your playbooks?

Some MDR offerings provide a chatbot that notifies you of suspicious activity in Microsoft Sentinel and then simply give you a link to the issue. But would you rather deal with a chatbot, or a live MDR analyst that has identified the problem, taken direct action to mitigate the issue, and then is ready to make a full report to you over your mobile device? The right MDR vendor should offer you the mobile tools to empower you to take charge of your security from anywhere, and you should always be able to collaborate with industry-leading expertise when a threat is detected.

Are you providing us just a Service Level Objective (SLO), or a true Service Level Agreement (SLA)?

Is any MDR offering you consider willing to commit their offered protection level to a contract, or are they simply talking about abstract goals around managing risk?

Other questions to ask

Beyond issues important to the successful deployment and use of Microsoft Security tools, there are other questions you should ask as indicators of how a vendor will perform when your organization is facing a threat:

How long does your team take to respond to alerts?

Are there contractual obligations around this?

Will my company have access to your SOC as needed or is that an additional charge?

Is there any hardware associated with this service?

If my company grows quickly can the MDR tool you're using scale quickly?

Can this tool help me respond to both SIEM and Endpoint Detection and Response (**EDR**) alerts from one console?

Can we investigate and respond to alerts natively from our phones?

The last two questions are particularly important, as they can determine what kind of control and visibility you will have in determining the direction of your new security environment. Information on alerts needs to be accessible from one device and one platform, and it should be accessible at any time and place to ensure critical threat and response information is always available as it happens.

How Critical Start approaches Microsoft Security

MDR For Microsoft 365 Defender

Microsoft has built a best-in-class security portfolio to stop attacks across Microsoft 365 services. Unlike our competitors who practice alert suppression, Critical Start MDR services built a comprehensive integration with Microsoft 365 Defender to quickly detect every event, resolve every alert, and respond to breaches across all your resources.

Our service integration leverages the power of ZTAP and the TBR which eliminates false positives at scale. And ZTAP strengthens our investigation of unknown alerts to ensure the escalation of the alerts that really require the attention of your security team.

We take every alert from the Microsoft 365 Defender security suite into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the Critical Start SOC investigates the alert.

We take an all-in security approach as our integration is focused on principles of least privilege. Azure Active Directory is used as an identity provider, single signon and privileged access manager for SOC access. Our service leverages cross-operating systems and Microsoft automated investigations and actionable incidents to speed up investigation and response.

IOC Management is on us

A key feature of the MDR service for both Microsoft Defender for Endpoint and Microsoft 365 Defender is IOC management. Microsoft is the fastest moving security company today. IOCs are published and updated hourly across different locations. The process of publication and application of additional detections can be hard to manage and a full-time job, so we added this feature in the service for no additional cost.

Simply Smarter

Critical Start MDR services for Microsoft 365 Defender leverage:

- ✓ Microsoft Security Best Practices to deploy Microsoft Sentinel and Microsoft Defender 365 tools to optimize Microsoft content for both Scheduled Query Rules and IOCs
- ✓ Microsoft User and Entity Behavior Analytics (**UEBA**) in every escalated alert, which increases the likelihood of detecting a true positive at multiple parts of the kill chain
- ✓ Azure Active Directory as an identity provider, single signon, and privileged access management for SOC access

IOC Management is on us

A key feature of the MDR service for both Microsoft Defender for Endpoint and Microsoft 365 Defender is IOC management. Microsoft is the fastest moving security company today. IOCs are published and updated hourly across different locations. The process of publication and application of additional detections can be hard to manage and a full-time job, so we added this feature in the service for no additional cost.

How Critical Start approaches Microsoft Security

MDR for Microsoft Defender for Endpoint

Starting with endpoints, Critical Start built an MDR service with Microsoft Defender for Endpoint that goes beyond monitoring alerts to helping customers, and our SOC analysts, see attacks across hybrid device types and operating systems so we can investigate the context and remediate the true positives. At the same time, this platform is built on deep insights into operating system threats and shared signals across devices, identities, and information. Leveraging Microsoft automated alerts and actionable incidents, focus time on what really needs security expertise—deciding what to prioritize next on your Microsoft Roadmap. Leave the research, false positives, and containment of infected devices to Microsoft and Critical Start.

We take every alert from Microsoft Defender for Endpoint into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the Critical Start SOC investigates and proactively responds to stop the attack on your behalf. Our analysts then collaborate with you to remediate in minutes.

Redefining Integration

Unlike other MDR providers, Critical Start MDR services with Microsoft Defender for Endpoint leverage:

- ✓ Cross-operating system (Windows, Mac, Linux) IOCs
- ✓ Azure Active Directory as an identity provider, single signon, and privileged access management for SOC access
- ✓ Cross-signal context in device timeline investigations
- ✓ Ability to pivot directly to the device timeline from any generated IOC

Wave goodbye to portal fatigue

A comprehensive integration means you can speed up investigation and response with access to Microsoft Defender for Endpoint or Microsoft 365 Defender. Get Entities, get Secure Score, Sign-In Details, and related alerts all in one portal. For each type of data source, such as email, identity, and endpoint, we have built queries within this single portal, so you can fetch other information for additional context.

How Critical Start approaches Microsoft Security

MDR for Microsoft Sentinel

Most SIEM solutions are leveraged for compliance, but only partially optimized for threat detection. Critical Start MDR services integrate with Microsoft Sentinel to detect every event, resolve every alert, and escalate only the alerts that matter to you. We provide you full operating potential for threat detection and response, while providing your security operations team increased efficiency and productivity gains.

Our Threat Detection Engineering team has a collective 100+ years of experience and over 50PB of data management experience, including environments greater than 20PB in size. We manage, maintain, and curate Microsoft Sentinel out-of-box detections and IOCs and our services include Critical Start proprietary detections and IOCs.

We provide expert guidance around how to deploy Microsoft Sentinel in your environment and optimize your log data sources for effective threat detection with the Microsoft Defender Security suite or with other third party security tools in your environment.

With MDR for Microsoft Sentinel, you can:

- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency & productivity
- ✓ Take advantage of limitless amounts of detection content
- ✓ Accelerate value from Microsoft Sentinel

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILE**SOC**® application. An industry-leading first, MobileSOC puts the power of our ZTAP platform in your hands, allowing you to contain breaches right from your phone. Our iOS and Android app features 100 percent transparency, with full alert detail and a timeline of all actions taken.

Critical Start Managed Detection and Response Service Comparison for Microsoft Products

	Microsoft 365 Defender	Microsoft Defender for Endpoint	Microsoft Sentinel
Automatically resolve false positives at scale with the Critical Start Trusted Behavior Registry®	•	•	•
Contractually guaranteed Service Level Agreement for Time to Detect and Mean Time to Resolution for all alerts regardless of severity level	•	•	•
ZTAP® dashboard provides complete and aggregated visibility into every alert with full details on the investigation and each action taken	•	•	•
Curate the new and updated detections being released daily by Microsoft	•	•	•
Management, curation, and maintenance of out-of-the-box detections and IOCs released by Microsoft	•	•	•
Curation of original and third- party threat intelligence, combined with real-time threat analysis to create a high-fidelity, actionable view of existing and emerging threats	•	•	•
Continuous development and enrichment of new threat detections and Indicators of Compromise (IOCs based on the latest evolving security landscape)	•	•	•
Threat detection content mapped to MITRE ATT&CK® Framework	•	•	•
Disable and logout of all signed in sessions for compromised accounts	•	•	•
ZTAP supports organizations with multiple tenants using parent/child hierarchy	•	•	•
Granular-level audit capabilities	•	•	•
Enhanced and optimized API ingestion	•	•	•
Service Specific Capabilities	**Microsoft 365 Defender**	**Microsoft Defender for Endpoint**	**Microsoft Sentinel**
Investigate, remediate, and resolve alerts for Microsoft Defender for Identity	•	N/A	N/A
Investigate, remediate, and resolve alerts for Azure Active Directory Identity Protection	•		
Investigate, remediate, and resolve alerts for Microsoft Defender for Office 365	•		
Investigate, remediate, and resolve alerts for Microsoft Defender for Cloud Apps	•		
Investigate and respond to suspicious email phishing alerts and email reported by users	•		
Optional capability to send an email to the user informing them of the outcome of the investigation of their reported emails, positive or negative	•		
Notification templates used to provide investigation results of reported email are customizable	•		
Delete phishing emails from user's mailbox, Confirm user accounts as risky, Lock user, Reset Session, Revoke Access and Force Logoff, Force Password Reset	•		
Remediation actions directly from ZTAP and MOBILE**SOC**® app	•	•	
Investigate, remediate, and resolve alerts for Microsoft Defender for Endpoint	•	•	
Maintain block and allow lists for file hashes, processes, IP addresses	•	•	
Investigate and monitor multi-source security events (Active Directory, Windows, Linux, Applications, Firewalls)			•

How Critical Start approaches Microsoft Security

Going the extra mile

Another question to ask your MDR service provider is what types of services they offer above and beyond traditional MDR.

An MDR provider should be fluent in threat identification and active mitigation strategies. They must be able to analyze an environment and make recommendations not limited to what the vendor is comfortable with, but instead focus on the needs of the client. This includes supporting implementation, optimization, and monitoring to ensure that all tools work together in concert to deliver maximized efficiency and protection.

How to measure success

When working with an MDR provider, if they have the right team, tools, methodology and process to protect your organization, then over 99 percent of security alerts should be resolved effectively.

We've also found that many companies accept dwell times, or the time from when an incident is first detected to the final resolution, of 100 days or more. With the right MDR in place, we've found that dwell time should be 22 minutes on average.

According to the Cost of a Data Breach Report 2021, the global average cost of a data breach is now $4.24M, up significantly from $3.86M reported in the 2020 report, with the United States being the top country for average total cost of a data breach for the eleventh year in a row.

Ready to learn more?

Microsoft Security has the tools to take protection of your environment to the next level. But this overview is only intended as a guide for your Microsoft strategy moving forward. To learn how to get highest performance and protection from Microsoft tools, contact a Critical Start representative so we can learn about your unique security situation and how you can leverage our trust-oriented approach platform to help you resolve every alert and stop breaches.

CRITICALSTART®

Member of
Microsoft Intelligent
Security Association

Microsoft

For more information, contact us at:
https://www.criticalstart.com/contact/

Request a Free Assessment