Ontinue

WHITE PAPER

How MXDR Can Solve Three of Your Biggest Security Challenges

For today's organizations, protecting an increasing amount of data and assets against cyberthreats is rife with challenges. The growing volume of attacks, an always-expanding attack surface, too many security controls, and a worldwide talent shortage have made 24/7 managed detection and response (MDR) services more appealing than ever. This is especially true among customers who have smaller infosec teams and don't plan to staff an in-house SOC.

First focused on endpoint detection and response (EDR) tools, MDR services later expanded to using XDR tools to offer visibility into workloads, networks, and identity – operating as managed extended detection and response (MXDR) solutions.

Despite the rapid adoption of early MDR and MXDR solutions over the years, organizations today still struggle to manage day-to-day security operations. According to a 451 Research report, "Customers indicate they continue to struggle with efficient security operations … more than 90% indicate they can't investigate all the security alerts they receive in a day."* Ultimately, those early MDR/MXDR solutions focused on managing tools (EDR and XDR) to reduce alert volumes, rather than reducing risk and mitigating threats – the outcomes customers actually need.

That need drove platforms and services that involve more than managing EDR or XDR tools. The next evolution of MDR/MXDR platforms and services focuses on managing a security "mission" or the "job to be done" – presumably to solve the very problem these tools were purchased for in the first place.

Solving security missions like mitigating ransomware holistically requires a more comprehensive approach that expands the scope of the problem beyond detection and response. At its core, today's MDR and MXDR platforms must address three core challenges that security teams face:

- **Too reactive:** Instead, the service needs to detect, respond – and prevent. That requires a deep understanding of the customer's environment and the ability to leverage insights learned from detection and response to continuously identify and mitigate potential security gaps and vulnerabilities with proactive preventive measures. The result is a stronger overall security posture, fewer incidents, and faster detection and response involving less effort.
- **Too slow:** Security is all about making decisions and taking decisive action – quickly. A modern MXDR service needs to enable much faster (and smarter) decision-making and execution using AI, data science, automation, collaboration, and localization. AI should be used not only for threat detection, but also to provide knowledge of the environment, the people, and processes in the organization, and to point the way toward improvements.
- **Too inefficient:** Security teams are inundated with tools and the resulting complexity is not only expensive, but it also increases risk. It's imperative that MXDR solutions enable security teams to do more with less and reduce complexity rather than contribute to it.

Complex Problems with Straightforward Solutions

Addressing the core challenges that persist despite the tools and services that organizations have available to them requires a complete rethinking of the operating model for managed detection and response. In order to be faster, more efficient, and more proactive, cybersecurity programs and their partners need to focus on five core characteristics: prevention, automation, collaboration, localization, and specialization.

* The Rise of Extended Detection and Response, 451 Research, June 2021

Elevating prevention: There is no faster way to mitigate a threat than avoiding it in the first place. By expanding the scope of the problem to include prevention, in addition to detection and response, a modern MXDR solution helps organizations reduce their overall risk while improving detection and response at the same time.

Prevention requires a deep understanding and comprehensive context of a customer's business and environment. An MXDR provider must understand each customer's underlying IT architecture, their workloads, and the applications running on top of them, as well as how they are interconnected. The provider must also marry their IT understanding with their understanding of the business so they can assess the criticality, posture, and risks of every asset in scope.

But asset inventories and business context aren't enough. Most managed security providers struggle with consistent process execution and decision-making within the process, as well as tracking the execution to ensure it meets all SLAs. They fail to operationalize preventive controls and vulnerability programs for their customers because they fail to understand the people and the processes involved beyond the security team.

Today's MXDR provider takes the organization's existing processes and teams into account, providing them with prioritized directions on where to focus, and mapping into the existing processes of the organization, rather than forcing the organization to adjust to a one-size-fits-all approach.

Today's MXDR provider takes the organization's existing processes and teams into account, providing them with prioritized directions on where to focus, and mapping into the existing processes of the organization, rather than forcing the organization to adjust to a one-size-fits-all approach.

Increasing security maturity requires reviewing the previous month's incidents to help you identify unresolved risk – creating a virtuous cycle of security in which detection and response informs prevention. You can use that knowledge to make changes, increase your prevention capabilities, and avoid fighting the same problems over and over.

While some MXDR providers do provide prevention-focused services, such as vulnerability management, these services are generally delivered completely separately from the service provider's core MXDR service. This prevents the MXDR service from leveraging the insights generated by the vulnerability management service, and vice versa. When evaluating MXDR vendors, it's important to ask the provider how their services interoperate and contribute to an overall stronger security posture.

Automation driven by data science and AI: Data science has traditionally been used in the security industry to model threat behavior to improve detection. Today, understanding what we defend and how defenders operate has become the new imperative – and that understanding should fuel improvement. It should drive what becomes automated next and how. It should drive changes to training and process. Using AI and ML to monitor and predict threat actor behaviors isn't new.

But today's MXDR service providers need to use AI to monitor every aspect of defense – from the steps involved in detection and investigation, to the communications between defenders during a response, to the response workflows themselves – and use the information to improve workflows and speed up the process. That's the next evolution of applying intelligence to security.

AI-driven Automation is the key to speed, consistency, and accuracy – since pushing humans to complete complex manual processes results in more errors. Automating parts of a process, or even entire processes end to end, also allows staff (on both at the customer's organization and at the MXDR service provider) to focus on more complex activities that can't be automated. Or, they can focus on alerts and data that are more ambiguous but have the potential to have a greater impact. Increasingly, providers can automate triage capabilities that not only auto-close noisy alerts, but also apply intelligence to automatically prioritize incidents based on context to ensure that SOC analysts focus on what matters most. By automating Tier 1 analysis and prioritization, the SOC analysts can spend more time investigating complex threats.

Increasingly, providers can automate triage capabilities that not only auto-close noisy alerts, but also apply intelligence to automatically prioritize incidents based on context to ensure that SOC analysts focus on what matters most.

To further increase the speed of the SOC, a more innovative MXDR service provider will also automate aspects of the investigation process. This lowers the chances of human error and reduces the mean time to respond for the SOC.

Real-time collaboration is clearly needed between your MDR service provider and security team, but security is operationalized by IT, application teams, and even end users, as well. We believe that security is a team sport, and communication and alignment between all of the teams involved in security operations fosters collaboration. For example, let's say an alert is triaged by the MDR provider who sees that Bob, an employee in a customer's organization, has opened a malicious file. The next step in triage is communicating with Bob to see if he opened the file – or if it was something else. Using collaboration with Microsoft Teams enables the MDR provider to reach out directly to Bob, and act as an extension of the organization's Security team, instead of using the security team as a middle person/go between.

When people have the right information presented at the right time in a way that is easy to consume, they can make decisions faster and with more confidence. Everyone needs a "single source of the truth" even if they consume it in different ways. Every MDR service provider has some sort of portal that is useful for reporting and checking metrics, but for many customers this is just another in an endless array of portals and dashboards. Portals also fall short for real-time collaboration, which is required during a critical security incident. Successful collaboration demands the ability for the MDR service, the customer's security team, and the end users to communicate – through text, audio, or video, on desktop and mobile devices – during an incident.

Risk-based localization: Tailoring protection requires a deep understanding of an organization's unique environment, business operations and teams – and it's critical to speeding up decision-making and execution. Understanding the customer's people (who does what?), process (what should you escalate to in various situations?), and technology (what assets are important? How do we best secure their unique infrastructure and apps?) is imperative to making optimal decisions and taking actions that don't cause collateral damage. Most MDR service providers and MSSPs fail to deliver, offering a generic service instead of one tailored the customer's environment. And because they don't understand the environment they're protecting, the effectiveness of prevention and response suffers.

Instead, knowing what a specific alert or threat means to a specific customer is more valuable than actioning an alert based on its generic impact. So localization reduces the number of false positives, escalations to end users and security people, and results in a better signal-to-noise ratio. This minimizes disruption while achieving security goals.

Specialization and expertise in the security ecosystem of choice – especially for customers who want to standardize on the Microsoft security stack – it's critical to partner with an MXDR provider that knows how to maximize their investment. The broad range of security products and tools on the market today has forced service providers to support many different products – making it challenging to become expert or even proficient in any of them. Many providers claim to specialize in one particular product, yet still support a wide range of security tools, which dilutes their focus. Whenever possible, partnering with a provider who focuses on your specific tooling will provide the most robust and cost-effective security program.

It is no secret that security teams are inundated with products. In fact, a September 2022 survey from Gartner found that 75% of organizations are looking to consolidate vendors. Lack of interoperability and integration between disparate products can lead to gaps in an organization's security posture.

Where some MDR providers often bring their own proprietary technologies and products, today's innovative MXDR providers know they must focus on leveraging the security tools that organizations have already invested in. Furthermore, modern providers should actively help with the vendor consolidation effort by finding ways to maximize the value that organizations can get from their tools, enabling them to remove redundant or superfluous products.

AN ILLUSTRATIVE EXAMPLE

How an Innovative MXDR Service Provider Delivers

To illustrate the difference between the different types of MDR providers, let's look at a hypothetical attack where the attackers have breached a privileged account.

1. **Early stage MDR:** It's likely one of the original MDR providers wouldn't detect the initial breach, as early MDR services were largely limited to endpoint telemetry and would struggle to initially correlate the identity activity and anomalous endpoint behavior. Depending on the attacker's methods, it may take some time for an EDR to trigger an alert. Once the attacker began attempting executing commands to add additional permissions, modify account settings, or other moves to gain persistence that hit the endpoints, the EDR would trip.

2. **Mid-stage MDR:** As MDR providers evolved, they would recognize the attack using additional log sources, use cases that monitor Active Directory (either on premise or in Azure), or other identity services that would trigger alerts on the account change. At that point, the SOC would correlate these alerts together with the EDR, identify the privileged account using the existing customer asset inventory or naming convention, and investigate the path that allowed the attacker to compromise the account.

   The SOC would escalate to the customer security team, recommending an account lockout for all compromised accounts, then follow up with further in-depth investigation of the evidence. The attack would be stopped, but crucial time is lost with manual processes including manual handoffs between the MDR provider's SOC and the customer.

3. **Innovative MXDR leaders:** Today, a leading MXDR provider would automatically correlate the alerts coming through Active Directory along with the signals coming from the EDR and a variety of other sources. The compromised account (or accounts) would be automatically locked out. Simultaneously, an escalation would be sent automatically to the customer via the communication and collaboration systems the organization's security teams already use for their day-to-day workflows.

   The SOC would already be focusing on the in-depth investigation, collecting as much evidence as possible, as quickly as possible, to identify the vulnerabilities. Through both automated machine learning processes and manual knowledge transfer, this information would be fed back into the security program, hardening it against future attacks. Additionally, this MXDR leader would monitor how the security analyst and the client teams interact with the system, finding opportunities to streamline the process for everyone involved, minimizing clicks and automating more of both the detection and the response processes.

Conclusion

The demand for MDR services has skyrocketed among organizations seeking to protect their data, their assets, and their business – without having to staff their own SOC. MXDR service providers can operationalize cybersecurity for their customers by expanding into prevention, enabling greater speed, and leveraging the customer's existing tools, resulting in a virtuous lifecycle. By offering this new model of extended managed detection and response, modern MXDR providers bring about a more robust service for organizations who need to protect an ever-expanding attack surface 24/7, while optimizing the investments they've made in the Microsoft security suite.

CONTACT US LEARN MORE

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue ION is the MXDR service of choice for Microsoft security customers that want to accelerate MTTR, proactively reduce risk, and reduce costs. Together, the Ontinue ION Platform and designated cyber defense experts build a deep understanding of your organization's risk posture that focuses prevention, detection and response efforts to reduce risk and mitigate threats.

AI-driven automation delivers fast, accurate investigation and response. Our one-of-a-kind Microsoft Teams interface provides real-time access to our 24/7 ION Cyber Defense Center to resolve every incident.

As the 2022 Microsoft Security MSSP of the year, Ontinue knows how to optimize your Microsoft investments, simplifying your technology stack and improving ROI.