Ontinue

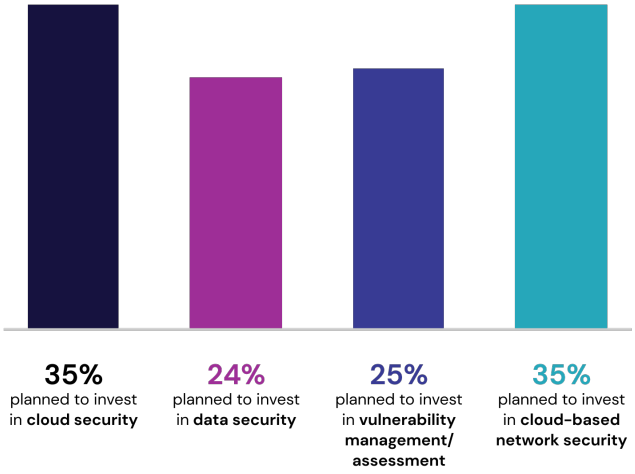
eBOOK

5 Capabilities of a Modern MXDR Service Provider

As businesses have accelerated their digital transformation initiatives, threat actors have also continued to launch debilitating attacks on organizations of all sizes. And these attacks continue to succeed even as organizations have invested in additional security tools.

The Flexera 2021 State of Tech Spend Report[1] surveyed CIOs and found that 86% expected the pace to increase somewhat or significantly. This trend will continue to increase challenges such as myriad security products overwhelming operators and driving costs up.

In response, organizations have shifted their investment priorities. A Microsoft Security Blog[2] article discussing a CISO survey noted that in 2022:



Today's Top Cybersecurity Challenges

Achieving a mature security posture is more than a mission-critical goal for many organizations, but they still face significant challenges when trying to achieve their security goals, including:

Complexity of the Environment

Modern cloud-based environments incorporate an overwhelming number of applications. Unlike on-premises software where updates can be pushed to a corporate-owned device sitting on a corporate network, software-as-a-service (SaaS) applications are code-based. Increased complexity comes from many other sources, such as the adoption of hybrid cloud infrastructure, the proliferation of end-user devices due to BYOD policies, as well as the increased number of employees working from home.

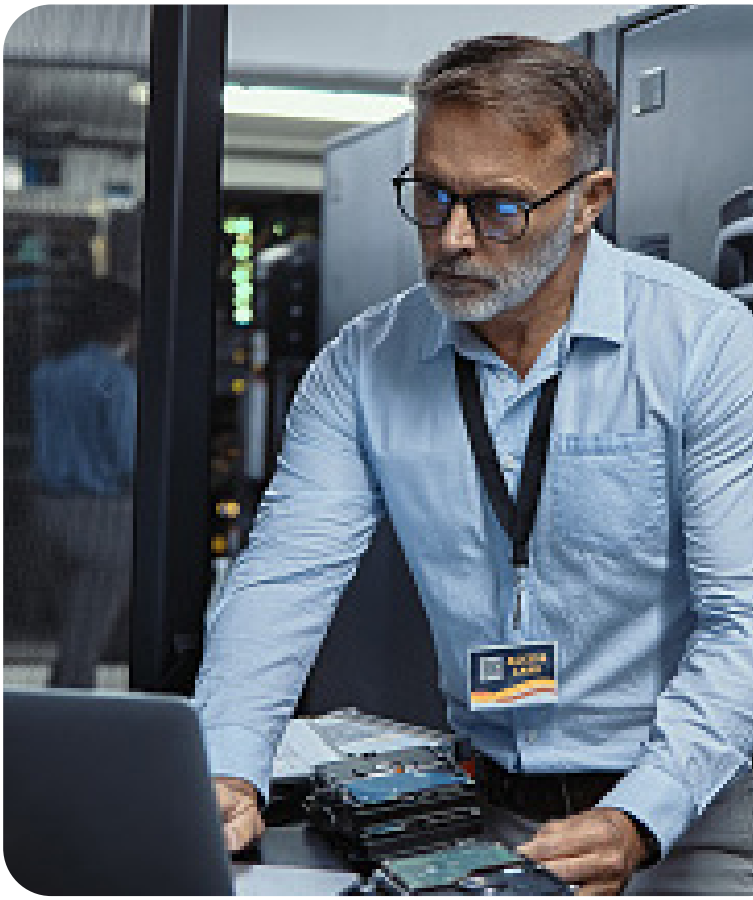
Too Many Tools, Too Little Visibility

In response, many organizations have invested heavily in cybersecurity technologies intended to enable a more robust posture. The pace of adoption, however, led to yet another problem: the rapid adoption of disconnected point solutions. These tools closed a specific security gap, but they created additional problems. For instance, overwhelmingly high number of alerts—and many false positives—can make it nearly impossible to follow incident response processes.

Too Few People

While organizations may have more tools, they often struggle to find experienced security staff. Cybersecurity requires not only technology, but also skilled people and effective processes. Even if an organization has sufficient budget, acquiring and retaining talent remains challenging—particularly for mid-sized companies.

To meet these challenges head on, a growing number of organizations have chosen to outsource their cybersecurity to improve effectiveness. A recent large survey found one of the primary motivating factors for engaging a security service provider was that "a managed service provider could do a better job than we can do on our own." [3]



Outsourcing: Enhanced Cybersecurity at a Reduced Cost

Bring-your-own-device (BYOD) and work-from-home (WFH) initiatives have massively expanded the attack surfaces of many organizations. Plus, tool-centric approaches have resulted in high cost and alert fatigue, which allows threats to sneak by without an analyst running them to ground. A tool-centric, manual, and premises-based approach also makes it harder to scale your security.

However, many organizations lack the resources required to navigate the new security challenges 24/7. So, they increasingly choose to outsource their cybersecurity monitoring, detection, and response functions, whether in whole or in part.

Outsourcing also rides another wave—a growing cloud-first mentality. A new generation of security experts came of age in a world of cloud-native services, driven by APIs—as opposed to one centered around tools.

These outsourced services comprise four main types.

Managed Service Provider (MSP)

Generally business arms of the large telecommunications or IT companies, MSPs provide a wide array of services that include networking or business applications. MSPs generally fall into two categories, those that:

- Supply staff but purchase cybersecurity technologies developed by other companies.
- Offer prevention layer software but rely on their partner ecosystem or the customer to supply staff.

Managed Security Service Provider (MSSP)

MSSPs vary widely in their security offerings—from network to endpoint security—often including some SOC augmentation services. Those offering detection and response capabilities offer a set of services easily scaled across a large customer base, resulting in a generic, one-size-fits-almost-all model.

Managed Detection and Response

Managed Detection and Response (MDR) is an independent category providing outsourced security response through security operations centers (SOCs), which differentiates them from MSSPs.

Managed Extended Detection and Response

Managed extended detection and response (MXDR) provides protection for both endpoints and networks. It can also extend coverage to IoT devices or operational technology (OT) networks.

The Modern MXDR Service Provider: Ready for Today's Threats

Despite the rapid adoption of MDR services, organizations still struggle to manage day-to-day security operations. Primarily designed to detect threats by leveraging tools (EDR and XDR), traditional MDR and MXDR services send alerts, but then largely leave the response up to the customer to execute.

While helpful in reducing the overall number of alerts that security teams need to field, this tool-centric approach often fails to address the underlying gaps that prevent security organizations from maturing and scaling. And these, after all, were the primary motivations for security leaders to adopt the service in the first place. As a result, many organizations find themselves:

- **Slow** to detect and respond to threats
- **Reactive** to address threats and risk
- **Inefficient** as overworked teams try to do more with less, which includes reducing their tool count

A modern MDR/MXDR service provider increases protection across your attack surface. Leveraging both human analysis and automation, it provides 24/7 monitoring and detection, rapid investigation, and mitigation. It also increases efficiency, freeing up experts for threat identification and hunting.

Today, an MDR/MXDR services provider must take control of proactive risk mitigation, continuous monitoring, and incident response activities, taking end-to-end responsibility for operationalizing your security.

The right MDR/MXDR solution employs a rich set of capabilities to understand each organization's specific attack surface and operational constraints to deliver a strong, tailored threat response.

When evaluating service providers, you should expect a vendor who claims to be a modern MXDR service provider to offer the following five key capabilities.

1. **AI-driven Automation**
   Leveraging data science and AI-driven automation to accelerate numerous security operation tasks, from triage to resolution. Ideally, the MXDR service should have a level of automation that is capable of resolving and automatically closing a high percentage of high-severity threats – confidently. A vendor should also be able to measure all aspects of security operations and should provide opportunities for automation and optimization.
2. **Real-time collaboration**
   The right people in your organization should have access to the right information in real time, ideally using collaboration tools you're already using, such as Microsoft Teams, instead of a separate vendor portal. That way, people can easily be brought into the conversation to collaborate in real time over any device. Better yet, they don't need to be granted access to yet another system.
3. **Risk-based, localized protection**
   You need a tailored, risk-based approach to cybersecurity – so any MXDR vendor should understand your environment, operations, and teams at a fundamental level. Nobody wants a one-size-fits-all approach when it comes to security, yet that's what many MDR providers offer. Assess any vendor for the ability to tailor the protection specifically to your environment, your business operations, and your teams. Any ongoing detection and response efforts need to be able to determine where to focus preventive measures, including proactive threat hunting.
4. **Specialized Microsoft expertise**
   If your organization has invested in Microsoft security, you'll want to find an MXDR service provider whose solution is purpose-built to leverage every component of the Microsoft security and collaboration ecosystem. A vendor that is hyper-focused on Microsoft can help you realize the full potential in the Microsoft security stack.
5. **Prevention**
   Beyond having the basic detection and response functions, a modern MXDR provider should be staffed with experts who can proactively improve your security posture through continuous assessment. They should be able to review your organization's incident history, environment, posture and risk profile to guide prevention activities.

Conclusion

Today's MXDR represents a radical departure from its predecessors because it stems from a new mindset. From frontline analysts to CISOs, dealing with today's elevated threat environment has moved people's thinking beyond detection and response to include prevention, as well. With the right MXDR provider, organizations can go beyond detecting and responding to security incidents and build robust security that proactively reduces risk.

When organizations choose an MXDR service provider, they're choosing more than a service. They're choosing a long-term partner. The relationship between an MXDR provider and its customers should be based on shared values and goals.

References

[1] Flexera. (2021). State of Tech Spend 2021 https://resources.flexera.com/

[2] Jakkal, V. (2022, March 9). How CISOs are preparing to tackle 2022 Microsoft Security Blog https://www.microsoft.com/

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.