

Meet unprecedented security challenges by leveraging MXDR services

By [Microsoft Security Experts](#)

July 10, 2023



Threat trends

Zero Trust

Microsoft Defender

Microsoft Defender Experts for XDR

Microsoft 365 Defender is now Microsoft Defender XDR. [Learn more.](#)

We know customers of every size face ever-increasing security risks. In just the last 12 months the speed of attackers leveraging breaches is also increasing, as it only takes 72 minutes on average for an attacker to access private data from the time a user falls victim to a phishing email.¹ Data breaches from insider threats have also risen 44 percent this last year.² Organizations need to be prepared to not only monitor their entire environment but have the experts in place to quickly analyze and respond.

Endpoint-focused detection and response are insufficient to protect against evolving threats

Historically, many customers begin their security journey focusing on endpoint security products. But in today's connected and dynamic world, organizations risk serious data breaches if they are not looking end-to-end. Specific pain points our customers often encounter include:

- **Inability to resource cybersecurity experts:** Teams may lack the skill sets needed to thoroughly investigate incidents and do not have the capacity for round-the-clock coverage. And even if organizations have the budget to hire internally, a resource gap in the industry can make it very difficult to hire the right talent in a timely fashion.
- **Triaging vast amounts of security alerts and data:** Many companies are dealing with alert fatigue, and they need to focus on the things that matter. They need help beyond just cleaning up minor incidents or false positive alerts. They need help enhancing their security posture to reduce the volume of alerts and incidents they see over time.
- **Ability to look end-to-end:** Many organizations have made the jump to endpoint detection and response (EDR), but they're not getting visibility into their environment beyond the endpoint. The advantage of Managed Extended Detection and Response (MXDR) over endpoint-focused managed detection and response (MDR) solutions is the ability to go beyond the endpoint to visualize and correlate threat data across domains and have that human-led expertise delivered quickly to help organizations accelerate or augment their security operations center capabilities.

Managed Extended Detection and Response changes how security work gets

done

Microsoft believes it's critical that customers not only have their environments well protected using [Zero Trust](#) principles leveraging advanced security technologies but also have the expertise available to them to fully triage events and respond to incidents 24 hours a day, 7 days a week.

Cybersecurity is a team sport. Too often, organizations play it outnumbered and outsmarted by the attacker. When your security team is challenged by a sophisticated adversary, an MXDR service provider can bring the power of best-in-class technologies and security know-how to tip the scales in your favor.

For most companies, cybersecurity is not their core business, and having the specialized resources to address these concerns can be a challenge. According to Gartner®, "by 2025, 60 percent of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30 percent today."³

How an MXDR service can work for you

A Managed Extended Detection and Response (MXDR) service is an extension of your team, empowering you to have specialist resources available around the clock. Monitoring your environment and triaging incidents that need immediate attention in a timely manner is critical to maintaining a healthy security posture. In the event your organization is affected by a critical incident, you will want to ensure you have the resources to investigate the incident, correlate the threat data to determine the root cause, and implement step-by-step response actions to contain and remediate the threat.

Microsoft-verified MXDR partner services

Most customers rely on a trusted security provider in some capacity to help them on their security journey. To assist customers as they consider MXDR services to further protect their organization, Microsoft has provided our Microsoft Cloud Partner Program members a way to receive Microsoft-verified MXDR partner status. This status means Microsoft engineers have reviewed and audited a partner's MXDR solution to meet the highest industry standards of round-the-clock security including proactive threat hunting, investigation, response, and prevention services. This verification can help you identify potential service partners who can help you secure your users and multicloud infrastructure.

Microsoft partners provide a full line of services and the ability to uniquely customize their offering to your needs. Service providers commonly protect across the breadth of your estate including Microsoft and other third-party security tools. Microsoft's partners also routinely provide customized service level agreements, data regulatory and industry specialization, and other specialized services aligned with the specific needs you may have, ranging from remotely managed supplementary services to your in-house team through full outsourcing services as required.

Over the previous 12 months, more than 40 partners in the Microsoft Cloud Partner Program with Security designations have now received this engineering verification. If you are considering adding MXDR services, Microsoft recommends reviewing one of [Microsoft's verified MXDR service partners](#).

Microsoft Defender Experts for XDR

Microsoft is committed to ensuring customers have all the help they need. In addition to customizable partner offerings that work for the full range of global customer needs, for customers that require XDR products and managed services from a single platform provider, Microsoft is excited to announce the general availability of [Microsoft Defender Experts for XDR](#), a first-party MXDR offering that gives security teams air cover with leading end-to-end protection and expertise. Powered by [Microsoft's best-in-class XDR suite](#), Defender Experts for XDR helps security teams triage, investigate, and respond to incidents related to email, cloud applications, endpoint, and identity to stop attackers in their tracks and prevent future compromise.

Capabilities include:

- **Managed detection and response**—Let our expert analysts manage your Microsoft 365 Defender incident queue and guide your response to incidents or handle triage, investigation, and response on your behalf.
- **Proactive threat hunting**—Extend your team's threat-hunting capabilities and prioritize significant threats with [Microsoft Defender Experts for Hunting](#) built in.
- **Live dashboards and reports**—Get a transparent view of our operations conducted on your behalf, along with a noise-free, actionable view of what matters for your organization, coupled with detailed analytics.
- **Proactive check-ins**—Benefit from remote, periodic check-ins with your named service delivery manager to guide your

MXDR experience and improve your security posture.

- **Fast and seamless onboarding**—Get a guided baselining experience to ensure your Microsoft security products are correctly configured.

Microsoft Defender Experts for XDR

Meet the new first-party MXDR services from Microsoft with end-to-end protection and expertise.

[Learn more >](#)

Learn more

To learn more about this service, visit the [Defender Experts for XDR product page](#) and visit the [Microsoft Defender Experts for XDR documentation page](#).

To learn more about Microsoft Security solutions, visit our [website](#). Bookmark the [Security blog](#) to keep up with our expert coverage on security matters. Also, follow us on LinkedIn ([Microsoft Security](#)) and Twitter ([@MSFTSecurity](#)) for the latest news and updates on cybersecurity.

¹[Anatomy of a modern attack surface: Six areas for organizations to manage](#), Microsoft. May 5, 2023.

²[2022 Cost of Insider Threats: Global Report](#), The Ponemon Institute. 2022.

³Gartner®, Market Guide for Managed Detection and Response Services, Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies. February 14, 2023.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

[Learn more](#)

Connect with us on social



What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

[Copilot in Windows](#)

[Explore Microsoft products](#)

[Windows 11 apps](#)

Microsoft Store

[Account profile](#)

[Download Center](#)

[Microsoft Store support](#)

[Returns](#)

[Order tracking](#)

[Certified Refurbished](#)

[Microsoft Store Promise](#)

[Flexible Payments](#)

Education

[Microsoft in education](#)

[Devices for education](#)

[Microsoft Teams for Education](#)

[Microsoft 365 Education](#)

[How to buy for your school](#)

[Educator training and development](#)

[Deals for students and parents](#)

[Azure for students](#)

Business

[Microsoft Cloud](#)

[Microsoft Security](#)

[Dynamics 365](#)

[Microsoft 365](#)

[Microsoft Power Platform](#)

[Microsoft Teams](#)

[Copilot for Microsoft 365](#)

[Small Business](#)

Developer & IT

[Azure](#)

[Developer Center](#)

[Documentation](#)

[Microsoft Learn](#)

[Microsoft Tech Community](#)

[Azure Marketplace](#)

[AppSource](#)

Company

Careers

About Microsoft

Company news


Privacy at Microsoft


Investors

Diversity and inclusion

Accessibility

Sustainability

 English (United States)

 Your Privacy Choices

Consumer Health Privacy