News Security management Microsoft Security Experts
5 min read

Expanded Microsoft Security Experts offerings provide comprehensive protection

By Microsoft Security Experts
Rani Lofstrom, Director, Security Incubations

October 9, 2023

Microsoft Defender Experts for Hunting

Microsoft Defender Experts for XDR

Microsoft Incident Response

Since we first introduced Microsoft Security Experts in May 2022, we've worked hard to expand our new security services category. In the past 16 months, we've launched new services, expanded our capabilities, and introduced new ways to buy. Our customers face an unprecedented number of security threats that introduce risk to the business. Also, our customers are facing a cybersecurity talent shortage; there is still a need for more than 3.4 million security professionals.[1] Combined with increasing international conflicts and an accelerating cyber arms race, the risk of cyberattacks has never been greater.[2]

At Microsoft, we aim to help our customers meet the range of today's security demands—together. In this environment, it is not a surprise that organizations are looking to do more with less and turning to managed security services to help their security teams.

Microsoft Defender Experts for XDR

In preview last year, Microsoft Defender Experts for XDR is now generally available. This managed extended detection and response (MXDR) service helps customers alleviate some of their most pressing pain points, including alert fatigue, scarce cybersecurity resources, and a limited ability to look end-to-end—beyond the endpoints—to visualize and correlate threat data across their entire digital environment. For most companies, security isn't their core business. Defender Experts for XDR can help customers drive security operations center (SOC) efficiency and add security expertise to their team quickly, freeing up their time to work on other security priorities.

Microsoft Defender Experts for XDR helps SOC teams focus on what matters, triaging and investigating prioritized incidents on your behalf. Our Defender Experts are available around the clock to chat about specific incidents or alerts, so your team can get immediate confirmation or clarification on a particular incident. Also, they provide detailed best practices and recommendations to

help your team prevent future attacks and improve your overall security posture.

To learn more about Defender Experts for XDR, read through our blog that walks through how the service works or watch our explainer video to see the service in action.

Microsoft Defender Experts for Hunting

Microsoft Defender Experts for Hunting is generally available for customers who look to Microsoft to proactively hunt for threats across Microsoft Defender data—including endpoints, email, cloud applications, and identity. Defender Experts for Hunting combines human expertise and hunter-trained AI to probe deeper to expose threats and correlate across your security stack. Improve your SOC response and prioritize significant threats with timely notifications and analysis by our expert threat hunters. And if you have questions, you can contact our Experts on Demand directly within your Microsoft Defender portal.

To learn more about how we approach active threat hunting, read through our Threat Hunting Survival Guide, or read about our participation in MITRE's first managed services evaluation.

Microsoft Incident Response

For customers that want help remediating a complex breach (or avoiding one altogether), Microsoft Incident Response (Microsoft IR) offers an end-to-end portfolio of proactive and reactive incident response services. We've been helping customers with their toughest incident response challenges since 2008. And we created Microsoft IR to be the first call for customers before, during, and after an incident. We operate in 190 countries and our incident responders are seasoned veterans with more than a combined 1,000 years of career experience resolving attacks from ransomware criminals to the most sophisticated nation-state threat actor groups.

Proactive services can help organizations identify and mitigate risks before they become incidents. This includes services such as compromise assessments, threat hunting, and incident response planning. We know companies that put proactive measures in place detect breaches 108 days faster than those without support (214 days compared to 322 days).[3] **Reactive services** can help organizations respond to a breach quickly and effectively to mitigate damage. This includes services such as incident investigation, containment, and remediation.

Since our last update, **Microsoft Incident Response Retainer is now generally available**. This new option is designed to give our customers a proactive way to get IR support from Microsoft and was designed to work with cyber insurance. The Microsoft IR Retainer is a flexible and scalable service that can help organizations of all sizes prepare for and respond to cyber incidents. The retainer includes pre-paid hours that provide organizations with peace of mind knowing that they have the resources they need to respond to an incident, regardless of its size or complexity. And if reactive services are not needed, the pre-paid hours can be reallocated to proactive services that help shore up the organization's security posture. The Microsoft Incident Response Retainer is a valuable tool for organizations of all sizes that want to be prepared for the unexpected. View the explainer video for more information.

To learn more about all our Incident Response services—including the newly available retainer—visit our Microsoft Incident Response webpage or go behind the scenes for an inside look at real-life cyberattack investigations in the Cyberattack Series.

Expert-led security transformation

Microsoft Security Enterprise Services (Enterprise Services), formerly known as Microsoft Security Services for Modernization, has restructured its offerings and is now more focused on helping customers meet modern security needs. These services are ideal for large enterprises that want to leverage Microsoft best practices and know-how as they continue their security transformation. Enterprise Services offers hands-on expertise and advisory services to assess and create your modern organizational cybersecurity strategy. These offerings provide planning and operations expertise to help you mitigate business risks and meet compliance requirements to ensure your business is future-ready. The services have recently been combined into two core expertise areas:

Security Cyber Resilience: End-to-end services to modernize and secure your digital estate including identities, data, applications, and devices across Microsoft Azure and multicloud environments. Microsoft Security Cyber Resilience helps safeguard your digital estate and create a transformation program of change, strategy, and operating models.

Security Operations: Secure your digital estate and safeguard critical information and assets with a security strategy and framework designed and implemented to respond to the modern threat landscape. Security Operations helps create—and action—a program of change for cybersecurity to make your digital estate more secure.

Working alongside our partners

Cybersecurity is a team sport. Too often, organizations play it outnumbered and outsmarted by the attacker. For most companies, cybersecurity is not their core business, and hiring specialized resources to address these concerns can be a challenge. Most customers rely on a trusted security provider in some capacity to help them on their security journey.

Microsoft partners provide robust 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. Microsoft Security Experts services were built to work alongside partner services, and we frequently partner with them on customer requests and design feedback for our solutions.

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

Looking to the future

As we continue to face new cybersecurity challenges, Microsoft will continue to evolve our Microsoft Security Experts services through our innovative engineering practices while leveraging the immense power of AI and other breakthrough technologies to help protect individuals, businesses, and more. Visit the Microsoft Security Experts page to learn more.

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] Revealing New Opportunities for the Cybersecurity Workforce, (ISC)2. 2022.

[2] Top Risks in Cybersecurity 2023, Bipartisan Policy Center. February 13, 2023.

[3] Cost of a Data Breach Report 2023, IBM. 2023.

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