Best practices SIEM and XDR Microsoft Defender Experts for XDR
5 min read

Microsoft Defender Experts for XDR helps triage, investigate, and respond to cyberthreats

By Microsoft Security Experts

July 24, 2023

Microsoft Defender

Microsoft Defender Experts for Hunting

Microsoft Defender XDR

Microsoft Security Experts

It has been an eventful time since the introduction of Microsoft Security Experts.[1] We launched Defender Experts for Hunting, our first-party managed threat hunting service for customers who want Microsoft to help them proactively hunt threats across endpoints, Microsoft Office 365, cloud applications, and identity.[2] We also participated in the inaugural 2022 MITRE Engenuity ATT&CK® Evaluations for Managed Services, where Microsoft demonstrated industry-leading results.[3] And finally, we announced the general availability of Microsoft Defender Experts for XDR, our first-party Managed Extended Detection and Response (MXDR) service.[4] We're excited about the launch of our newest service, so let's take a deeper look at Defender Experts for XDR and how it works.

Defender Experts for XDR builds on Microsoft's industry-leading XDR suite

Industry-leading technologies serve as the backbone of any managed security service, and Defender Experts for XDR builds on the defining benchmark that Microsoft 365 Defender has set in the extended detection and response space. Microsoft was named a Leader in The Forrester New Wave™: Extended Detection and Response (XDR), Q4, 2021, one of only two providers to be named a Leader.[5] Microsoft 365 Defender was rated as "differentiated" in seven criteria including detection, investigation, response, and remediation. Forrester noted that our decision to regulate inputs into XDR, specifically to rich, native telemetry, yields tailored detection, investigation, response, and mitigation capabilities.

Forrester notes that "there is a deep divide in the XDR market between those far along the path and those just starting to deliver on the vision of XDR" and those mature providers "combine the best elements of their portfolios, including industry-leading products, to simplify incident response and build targeted, high-efficacy detections."

The right and leading technologies are crucial to implementing managed services. Microsoft has a leading endpoint detection and response (EDR) solution, and while EDR is important and serves a valuable purpose, it is insufficient as the only method to protect against evolving threats.[6] In addition, "too many tools, or worse, duplicate tools in the SOC [security operations center] need to be rationalized and managed security services like MDR [managed detection and response] are increasingly seen as not only a cost savings opportunity but also as a way to rapidly mature their capabilities."[7] With Microsoft's XDR solution coupled with Defender Experts for XDR, we can deliver end-to-end protection and expertise.

How Microsoft Defender Experts for XDR works

Our Defender Experts team delivers the essential human element that complements the power of our Microsoft 365 Defender suite. They are the tip of the spear—taking unparalleled access to data and intelligence across nation-state and e-crime activity, new vulnerability data, newly observed tactics and techniques, and more to analyze and curate a hypothesis-led hunting strategy to find emerging, suspicious activities, and in turn deliver expertise to your security team immediately to help address coverage gaps and augment your overall security operations.

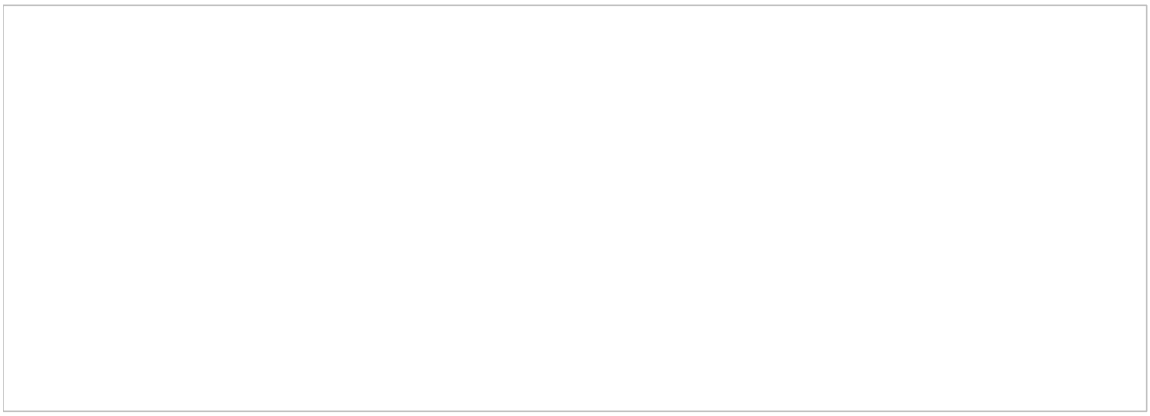

Figure 1. This diagram describes how Microsoft conducts its four-step Defender Experts for XDR process. It starts with triage and prioritizing Microsoft 365 Defender incidents and alerts to alleviate alert fatigue. Microsoft investigates and analyzes the most critical incidents first, documenting the process and findings. In the response step, Microsoft helps contain and mitigate incidents faster by delivering step-by-step guided and managed response, with Defender Experts available on-demand by live chat. Detailed recommendations and best practices are then provided to prevent future attacks. This process delivers continuous security posture improvements around the clock.

As an extension of your team, Defender Experts for XDR empowers you to respond with confidence. Our Defender Experts work around the clock, monitoring your environment and triaging the incidents that need immediate attention. In the event your organization is being affected by a critical incident, our team will investigate it, correlate the threat data to determine the root cause, and provide step-by-step response actions you need to take to contain and remediate the threat. You can take it further and give us permission to contain and remediate the threat for you.

Figure 2. This graphic shows a multistage incident in Microsoft 365 Defender. It includes the attack story of the active alerts related to the incident as well as the Defender Experts section that shows the guided response that includes the actions needed to resolve the incident immediately.

This is all available to you in a turnkey experience, where you can get up and running in hours, with the help of your dedicated service delivery manager (SDM)—your trusted advisor, who is available to you at any given time. And if you have any questions or need additional context on a particular incident, you can access our experts around the clock through live chat. Our detailed, real-time reporting shows you the comprehensive details of investigations into critical incidents, and how long it takes for our team to conduct the investigations on your behalf.

Figure 3. The graph highlights the number of hours that a customer spent completing guided response tasks and the potential time

savings a customer can realize if Defender Experts for XDR handles response on their behalf.

"Defender Experts for XDR found a shadow IT detection on the first day of service," said Mike Johnson, Global Cyber Threat and Incident Response Security Operations Center Manager at Verifone. "I was impressed that they found a real issue for us so fast—none of our other tools alerted us about it."

Defender Experts for XDR also provides recommendations on how your team can be proactive to prevent the next attack and reduce the number of incidents over time to improve your security posture. "Organizations who need to augment their SOC with 24/7 coverage and immediate access to expertise that will help them quickly triage, investigate, and respond to incidents should explore a managed XDR service," said Craig Robinson, Vice President of Security Services at IDC Research. "Microsoft's new MXDR service positions them to support the needs of organizations facing talent shortages who need to scale their security programs quickly, address coverage gaps, and protect their environment."

Learn more about Microsoft Defender Experts for XDR

Defender Experts for XDR can quickly deliver expertise to your security teams, help address coverage gaps, and add capabilities like proactive threat hunting to augment your overall security operations. Our customers and partners have been instrumental in the development of Defender Experts for XDR and your continued trust in us drives our team to listen, learn, and adapt to meet your evolving needs. We're excited about the road ahead and look forward to being a part of your security journey and building a safer world for everyone.

To learn more about the service, visit the Microsoft Defender Experts for XDR web page, read the Defender Experts for XDR docs page, download the datasheet, or watch a short video.

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]Building a safer world together with our partners—introducing Microsoft Security Experts, Vasu Jakkal. May 9, 2022.

[2]Microsoft Defender Experts for Hunting proactively hunts threats, Microsoft Security Experts. August 3, 2022.

[3]Microsoft Defender Experts for Hunting demonstrates industry-leading protection in the 2022 MITRE Engenuity ATT&CK® Evaluations for Managed Services, Ryan Kivett. November 9, 2022.

[4]Meet unprecedented security challenges by leveraging MXDR services, Microsoft Security Experts. July 10, 2023.

[5]Forrester Research, Inc., The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021, Allie Mellen, Joseph Blankenship, Alexis Tatro, Peggy Dostie. October 13, 2021.

[6]Microsoft is named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms, Rob Lefferts. March 2, 2023.

[7]Applying the Lessons Learned from 2022 Is Vital for Security Service Providers to Secure Growth in 2023, Doc #US50206623, IDC. February 2023.

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

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy