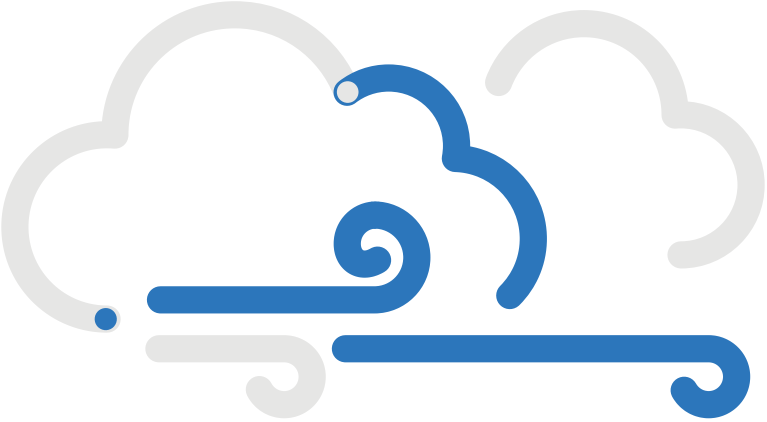
Microsoft Security

Your cybersecurity forecast calls for Managed XDR

Table of Contents



If there's one thing we know about the cloud, it's cloudy.

And a lack of full visibility into data, endpoints, identities, and other areas of your environment can leave your organization vulnerable. Today's security leaders are facing a perfect storm of challenges—including both an ongoing talent shortage that makes scaling security programs difficult and a growing attack surface coupled with an increase in cybersecurity threats.

As security leaders prepare to weather the volatile security climate ahead, managed services can provide the support and expertise they need to help address coverage gaps, add new capabilities, and augment their overall security operations.

This comprehensive guide covers the challenges facing security leaders now, the case for managed services, and a detailed view of Microsoft Defender Experts for XDR—a managed extended detection and response service that employs Microsoft experts to triage, investigate, and respond to incidents to help customers stop cyberattacks and prevent future compromise.

The cybersecurity forecast

For most organizations, cybersecurity is not their core business, and having the specialized resources to properly staff and respond to security challenges can be difficult. In the current environment, security leaders face growing complexity and a growing diversity of digital ecosystems that leaves many organizations vulnerable. Many are also managing hybrid workforce models, ongoing cloud migration, and a digital supply chain with multiple third-party partners and applications.

The forecast and priorities for each organization are different, but the trends they face may include many or all of the following challenges:

More frequent, sophisticated, and impactful cyberattacks, targeting organizations of all sizes and industries. The volume of password attacks has risen to an estimated 11,000 attacks every second, a tenfold increase from the same time last year.[1]

Attackers that use multiple vectors and techniques to evade detection, compromise systems, and exfiltrate data. Organizations struggle to maintain visibility and control over their diverse and distributed digital estate.

[1] 2023 Microsoft Digital Defense Report

A shortage of skilled and experienced security personnel.Despite a 9% increase in the global cybersecurity workforce, the workforce gap grew even faster by 13% to roughly 4 million, according to a workforce study from ISC2.

An overwhelming volume and complexity of alerts with a shortage of skills, tools, and processes to investigate and respond effectively.

Siloed, fragmented, or incompatible security solutions—creating gaps and inefficiencies in the security posture.

A rise in ransomware attacks targeting critical infrastructure, health care, education, and other sectors—and the need for a coordinated response and prevention strategy.[1]

The increasing sophistication and persistence of nation-state actors that use cyberattacks to advance their geopolitical interests, disrupt adversaries, and steal intellectual property.[1]

> "Microsoft has a much more global view of account activity, traversing the globe and ensuring my account doesn't become compromised. Whereas our prior vendor was focused on investigating current activities such as downloading a malicious file."
>
> **CIO, legal**

[1] 2023 Microsoft Digital Defense Report

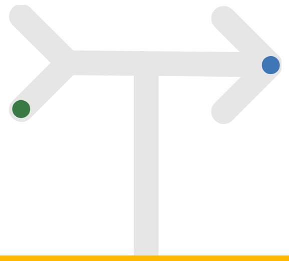
In this challenging environment, many organizations know they need to build more cyber resilience—which is the ability to anticipate, withstand, recover from, and adapt to cyber incidents, and the best practices and recommendations for building and maintaining resilience. But traditional security solutions are not enough to keep up with the evolving threat landscape and the complexity of modern IT environments. So, many security leaders are turning to managed security services like managed detection and response (MDR).

In fact, by 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today.[1] A managed detection and response (MDR) service provides customers with 24/7 monitoring, analysis, and response capabilities for their security incidents. By adding an MDR service, customers reduce time and effort required to contain and remediate threats and minimize the risk and impact of cyberattacks.

EDR	MDR	XDR	MXDR
(threat) detection and response for endpoints	managed detection and response for endpoints	extended detection and response for endpoints plus identity, cloud, data and more	managed extended detection and response for endpoints plus identity, cloud, data and more

[1] Meet unprecedented security challenges by leveraging MXDR services

The case for managed extended detection and response (MXDR)



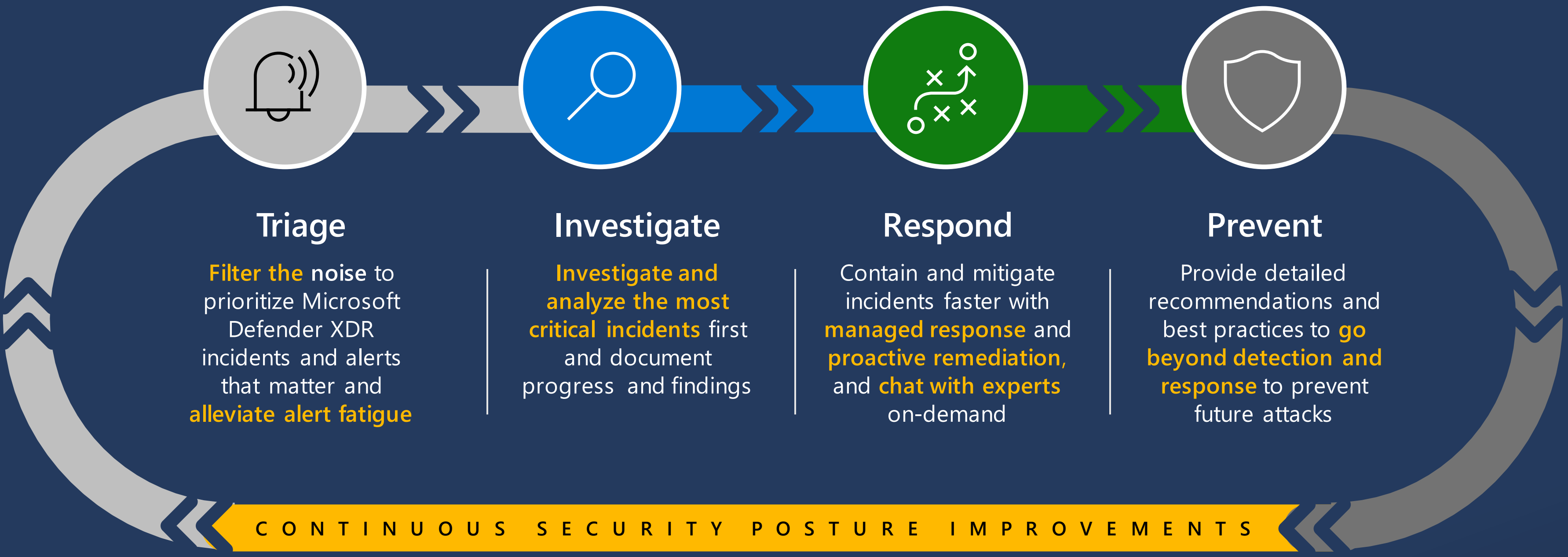
Extended detection and response (XDR) is a newer approach to security that integrates data and capabilities across multiple domains—such as endpoint, identity, cloud, and data. This integration enables security teams to gain a holistic and contextual view of their environment, detect and prioritize threats, and automate and orchestrate response actions.

XDR can help organizations improve their security efficiency, effectiveness, and resilience, and reduce the impact of cyberattacks. But it also requires a high level of expertise, resources, and maturity to implement and operate successfully. That's where a managed XDR service can help.

Managed XDR is a service that provides customers with access to a team of experts who can help them leverage the full potential of XDR. As a managed service, the added expertise can help organizations overcome the challenges of skills shortage, alert fatigue, and operational complexity, and enhance their security capabilities and outcomes.

> "Defender Experts for XDR gave us so much more visibility beyond what our security team used to have and freed our team up to focus on the threats that actually demand our attention."
>
> **Head of IT, Education**

Microsoft Defender Experts for XDR



Triage

Filter the noise to prioritize Microsoft Defender XDR incidents and alerts that matter and alleviate alert fatigue

Investigate

Investigate and analyze the most critical incidents first and document progress and findings

Respond

Contain and mitigate incidents faster with managed response and proactive remediation, and chat with experts on-demand

Prevent

Provide detailed recommendations and best practices to go beyond detection and response to prevent future attacks

CONTINUOUS SECURITY POSTURE IMPROVEMENTS

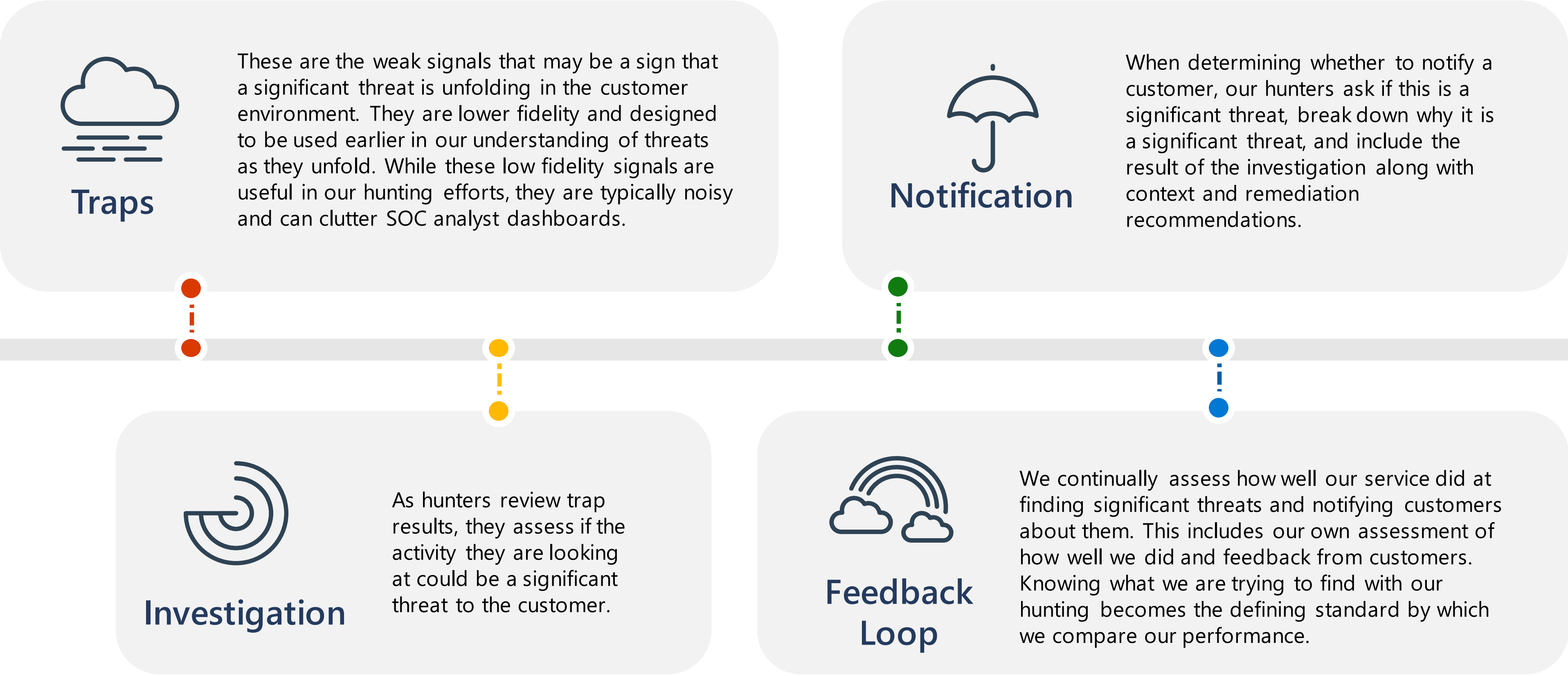
Defender Experts for XDR is a first-party managed XDR offering that provides security teams with leading end-to-end protection and expertise.

Powered by Microsoft's best-in-class XDR suite, Defender Experts for XDR helps security teams triage, investigate, and respond to incidents to help stop attackers in their tracks and prevent future compromise.

Cloudy with a chance of threats?

Get Microsoft Defender for Hunting

Our Defender Experts for Hunting service, which is included in Defender Experts for XDR, finds significant threats based on attacker behaviors. These threats are significant because of who may be behind them, how severe the activity may already be, or how severe we predict the activity may become. This objective becomes a guide for each phase of our service design:



Traps

These are the weak signals that may be a sign that a significant threat is unfolding in the customer environment. They are lower fidelity and designed to be used earlier in our understanding of threats as they unfold. While these low fidelity signals are useful in our hunting efforts, they are typically noisy and can clutter SOC analyst dashboards.

Investigation

As hunters review trap results, they assess if the activity they are looking at could be a significant threat to the customer.

Notification

When determining whether to notify a customer, our hunters ask if this is a significant threat, break down why it is a significant threat, and include the result of the investigation along with context and remediation recommendations.

Feedback Loop

We continually assess how well our service did at finding significant threats and notifying customers about them. This includes our own assessment of how well we did and feedback from customers. Knowing what we are trying to find with our hunting becomes the defining standard by which we compare our performance.

Field-tested human expertise

Adding human cybersecurity expertise helps customers reduce the time, cost, and risk of managing their security operations to achieve better security outcomes. Defender Experts for XDR is powered by a team of Microsoft experts who have over 600 combined years of cybersecurity, government and defense industry experience. They utilize AI-powered threat intelligence to proactively hunt for threats, validate and prioritize incidents, and respond to incidents for our customers.

What does a Defender Experts analyst do in a typical day?

A typical day in the life of a Defender Experts for XDR analyst is anything but typical. But they do whatever it takes to improve customer resilience each day, on tasks that include:

- Investigating incidents from Defender XDR and other sources.
- Conducting threat hunting within customer environments to identify and prioritize significant threats.
- Executing managed response to contain and remediate threats.
- Communicating and collaborating with customers and internal teams via real-time chat.
- Identifying vulnerabilities, misconfigurations, and other security issues in customer environments to improve their security posture.
- Documenting and reporting the findings and outcomes.

Read the 'day in the life' blog here

A seamless experience with native integration

Defender Experts for XDR provides customers with a seamless and integrated experience within the Microsoft Defender XDR platform—providing one place for all Defender Experts workflows. Our managed response is linked to each related Defender XDR incident with one-click actions for quicker alert resolution. And our one-of-a-kind, 24/7 real-time chat with our analysts is embedded in the Defender portal and in Microsoft Teams for smoother communications for customers. We have native integration with Microsoft Sentinel to enable automation for Defender Experts updates, which are also accessible within the Defender APIs for integrations with third party SIEM and case management tools.

And finally, our insights and reports are part of the Defender reporting framework, without requiring another BI or analytics software. These built-in features make it easy for customers to review, communicate and track our MDR operations without using a separate set of portals and apps. Our unique visibility allows us to identify weaknesses being exploited through attack methods like credential theft and phishing campaigns to stop threats higher up in the kill chain.

Accelerate your SOC operations

Let our experts' triage and investigate prioritized incidents that require immediate attention.

Protect with confidence

Contain incidents faster with human-led managed response and proactive remediation done on your behalf.

Access Defender Experts on-demand

Chat with Defender Experts around the clock about specific incidents or alerts.

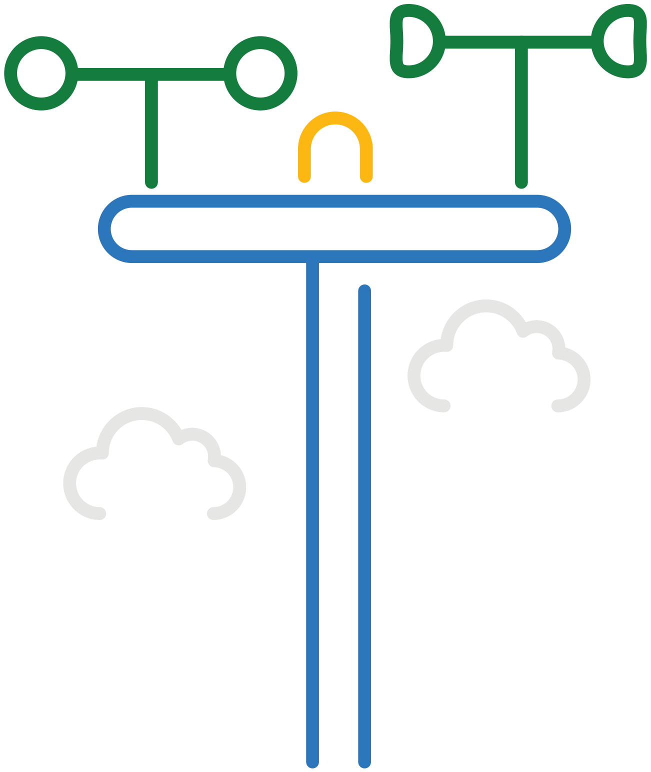
Prevent future attacks

Reduce incidents over time with detailed recommendations to improve your overall security posture.

Unparalleled threat intelligence and analysis into complex attacks

The Microsoft Threat Intelligence community is made up of more than 10,000 world-class experts, security researchers, analysts, and threat hunters analyzing 78 trillion signals daily to discover threats and deliver timely and hyper-relevant insight to protect customers.

With access to this unparalleled threat intelligence plus the cross-domain signals they analyze in customer environments, the Defender Experts team can detect and mitigate complex attacks—like the recent QR code phishing and attacker adversary-in-the-middle (AiTM) campaigns—quickly deriving insights on threat actors and their techniques and securing customers from major disruptions.



> "I see a benefit in correlation. For example, if an incident happens and a machine is infected with malware and credentials are stolen, then you see the login with those credentials from a location that is unfamiliar. Microsoft has all the data in one place, which is easier for us to correlate the whole picture."
>
> **Incident response team lead, travel**

Chasing the AiTM perfect storm

Adversary in the middle (AiTM) campaigns are some of the most prevalent and difficult to detect attacks. But with AI-powered threat intelligence, coupled with the ability to conduct in-depth threat hunting, the Defender Experts team can quickly correlate cross-domain threat data and stop these attacks.

1.

Hunting for user behavior

Defender Experts will correlate how a user accesses an email with image or document attachments with risky sign-in attempts from non-trusted devices in closer proximity.

2.

Hunting for sender patterns

Defender Experts will correlate email from non-prevalent domains in the organization with impersonation intents.

3.

Hunting for subject patterns

Defender Experts will track emails with suspicious keywords or personalization in subject lines.

4.

Hunting for attachment name patterns

Defender Experts will identify emails with randomly named attachments from the same sender to multiple recipients.

5.

Hunting for user signals/ clusters

Defender Experts will identify large scale campaigns sent to 1,000+ users with subjects and contents based on similar preferences.

6.

Hunting for suspicious sign-in attempts

Defender Experts will identify sign-in attempts from non-managed devices, untrusted devices with unusual characteristics, or from known malicious IPs

7.

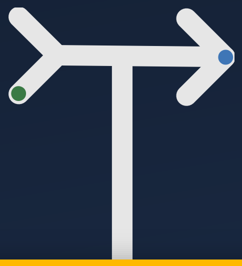
Mitigations

Deploy our Defender Experts services to stay ahead of these threats with proactive threat hunting and managed extended detection and response. Apply mitigations across your Microsoft products to reduce their impact.

Get started with Microsoft Defender Experts for XDR

Self-service is the easiest way to get started. You'll be assigned a service delivery manager and grant permissions to our experts. With permissions set, our experts can then sign into your tenant and deliver services based on assigned security roles.

After onboarding, your service delivery manager (SDM) will serve as your trusted advisor and set up remote, periodic check-ins to guide your **Defender Experts for XDR** experience and help improve your security posture. You also have 24/7 access to Experts on Demand, where you can ask the Defender Experts team for additional context on a particular incident. These proactive engagement opportunities will help you get the most out of your **Defender Experts for XDR** experience.



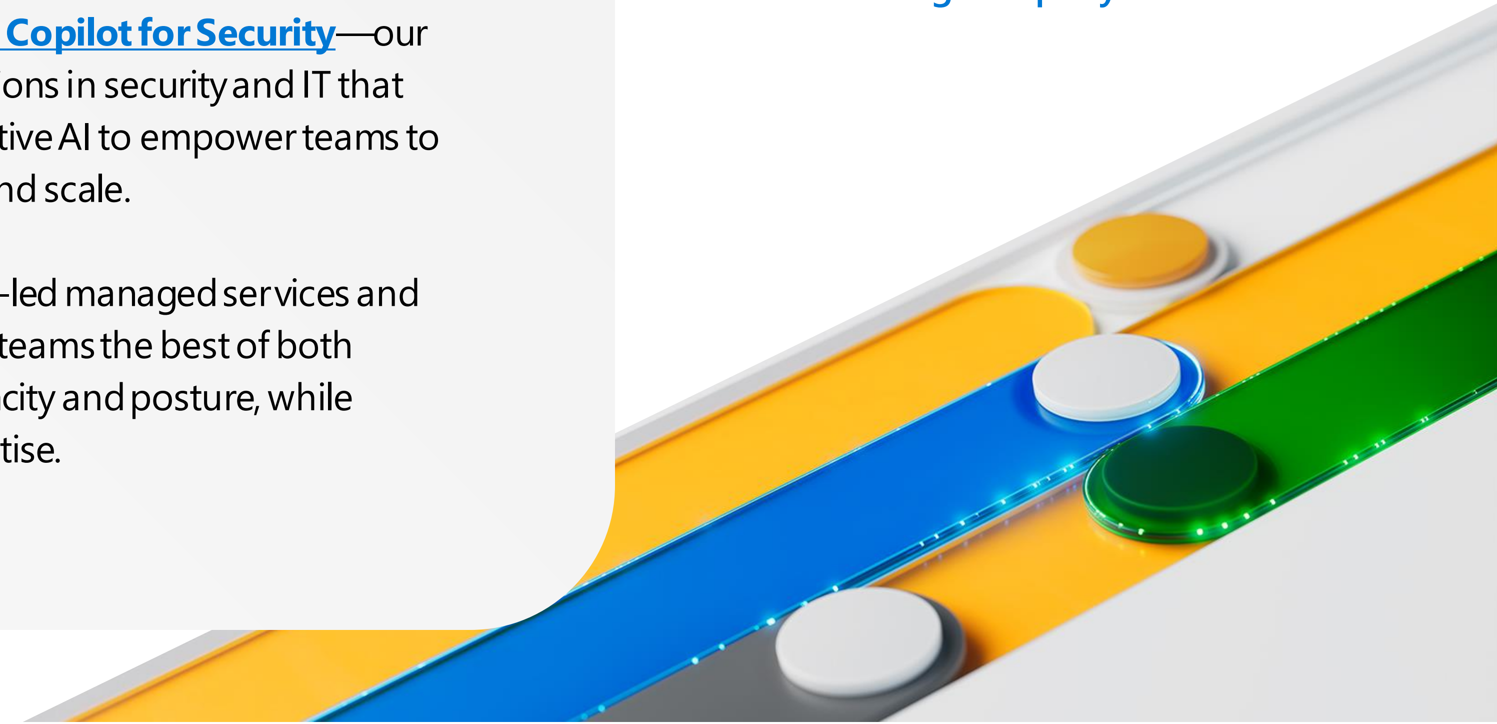
For more detailed information and step-by-step screenshots of the process, visit How to use the Microsoft Defender Experts for XDR service | Microsoft Learn

Defender Experts and Copilot for Security – better together

Our Defender Experts team was **one of the earliest teams to utilize Microsoft Copilot for Security**—our AI assistant for daily operations in security and IT that brings the power of generative AI to empower teams to defend at machine speed and scale.

The combination of human-led managed services and generative AI will give SOC teams the best of both worlds: improved SOC capacity and posture, while strengthening overall expertise.

> "By implementing Microsoft Defender Experts for Hunting, we enhanced our cybersecurity posture by having experts who continuously look for hidden threats, ensuring the safety of our data, reputation, and customer trust."
>
> Chief Information Security Officer, IT consulting company



Get results that matter

- Our expert analysts have resolved over 20,000 incidents for customers in any given month.

- See how our experts can strengthen your security posture and close any gaps with actionable insights from our service.

- Read how a study found a projected return on investment of 43% to 254% over three years and a projected net present value of $1.0M to $6.1M with Defender Experts for XDR. Calculate a high-level estimate of your projected ROI based on the study methodology.

- See how we are a Leader in the 2022 MITRE Engenuity ATT&CK® Evaluations for Managed Services.

- Microsoft is named a Leader in the Frost Radar™: Managed Detection and Response, 2024 report.

- Visit one of our **Microsoft-verified MXDR partners** and see how we work better together.

> "Defender Experts for XDR found a shadow IT detection on the first day of service. I was impressed that they found a real issue for us so fast. None of our other tools alerted us about it."
>
> Incident Response Manager, electronic payment solutions

Learn More

For more information about Microsoft Defender Experts for XDR, check out these resources or contact your account manager:

Microsoft Defender Experts for XDR

What is Microsoft Defender Experts for XDR offering | Microsoft Learn