# Microsoft Security Experts

## CY2023 Q2 – Microsoft Security Managed Services

# Contents

**Microsoft Security Experts** ..... **3**
Purpose of this document ..... 3
Microsoft Security Experts ..... 3
**Microsoft Defender Experts for XDR** ..... **4**
Overview ..... 4
**Microsoft Defender Experts for Hunting** ..... **5**
Overview ..... 5
**Additional Information** ..... **6**
Data Location, Usage, Retention ..... 6
Security, Compliance ..... 6
Availability ..... 6
Languages ..... 6
Additional resources ..... 7

# Microsoft Security Experts

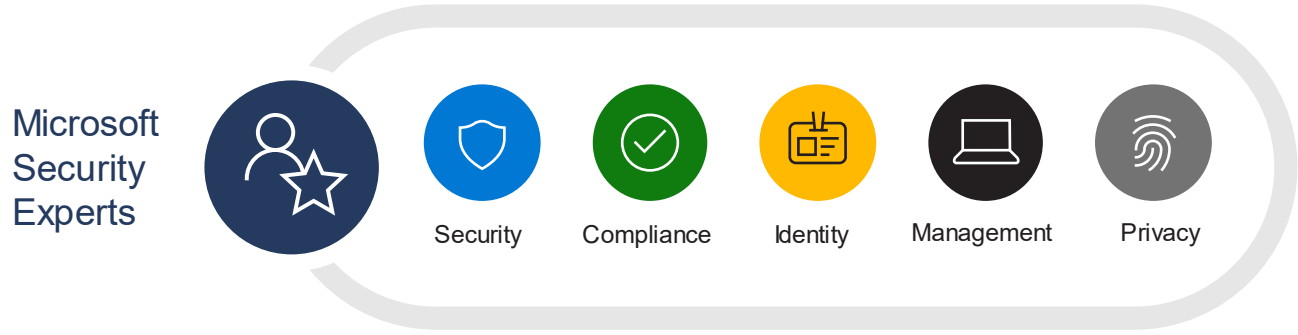
## Purpose of this document

Microsoft understands that customers who use our managed services entrust us with their most valued asset, their data. This document will provide additional clarity around how data is stored and used to deliver the services offered by **Microsoft Security Experts** (Security Experts). Specifically, this document covers our **Microsoft Defender Experts for XDR** (Defender Experts for XDR) and **Microsoft Defender Experts for Hunting** (Defender Experts for Hunting) managed services.

## Microsoft Security Experts

Today, cybersecurity has reached an inflection point, the United States is facing a cybersecurity talent shortage with nearly one in three—or 2.5 million—security jobs vacant[1] pushing time of detection for a breach to an alarming 277 days.[2] And, even when talent is available, access to highly skilled expertise remains a challenge.

Microsoft created Microsoft Security Experts to help customers achieve better security outcomes that span across Microsoft Security's product categories: security, compliance, identity, management, and privacy. Security Experts includes managed services, incident response, and advisory services. For more details refer to the announcement blog here.




[1] America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce, Brad Smith, Official Microsoft Blog, Microsoft. October 28, 2021.
[2] Cost of a Data Breach Report 2022, IBM.

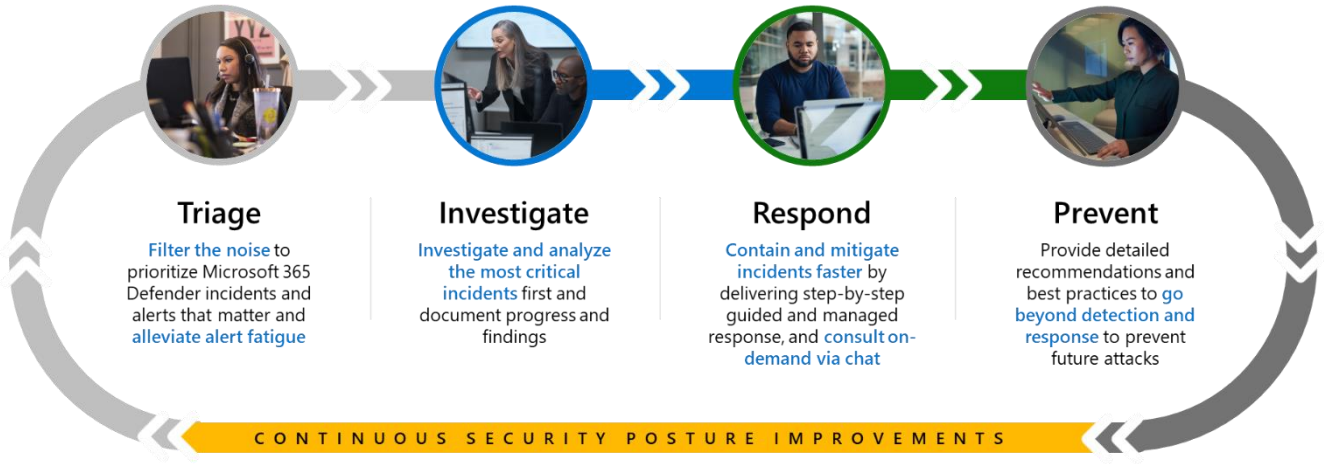
# Microsoft Defender Experts for XDR

## Overview

Microsoft Defender Experts for XDR (Defender Experts for XDR) is a managed extended detection and response service that gives security teams air cover with leading end-to-end protection and expertise. Defender Experts for XDR helps triage, investigate, and respond to incidents for customers who use one or more of the following Microsoft 365 Defender services: Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and Azure Active Directory (Azure AD). Defender Experts for XDR augments your security operations center (SOC) with Microsoft expertise to stop attackers in their tracks, prevent future compromise, and improve your security posture.

To carry out managed extended detection and response on behalf of the customer, Microsoft analysts need access to customers' M365 Defender portal alerts, incidents, and advanced hunting data. Defender Experts for XDR is sold separately from other Defender products. By purchasing and onboarding the service, the customer is providing consent to Microsoft to triage and investigate incidents and provide guided response or act on their behalf. During onboarding, the customer can configure the desired level of access.

Below is a diagram that shows how this service works.




*This diagram describes how Microsoft conducts its four-step Defender Experts for XDR process. It starts with triage 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 via live chat. Detailed recommendations and best practices are then provided to prevent future attacks. This process delivers continuous security posture improvements around the clock.*

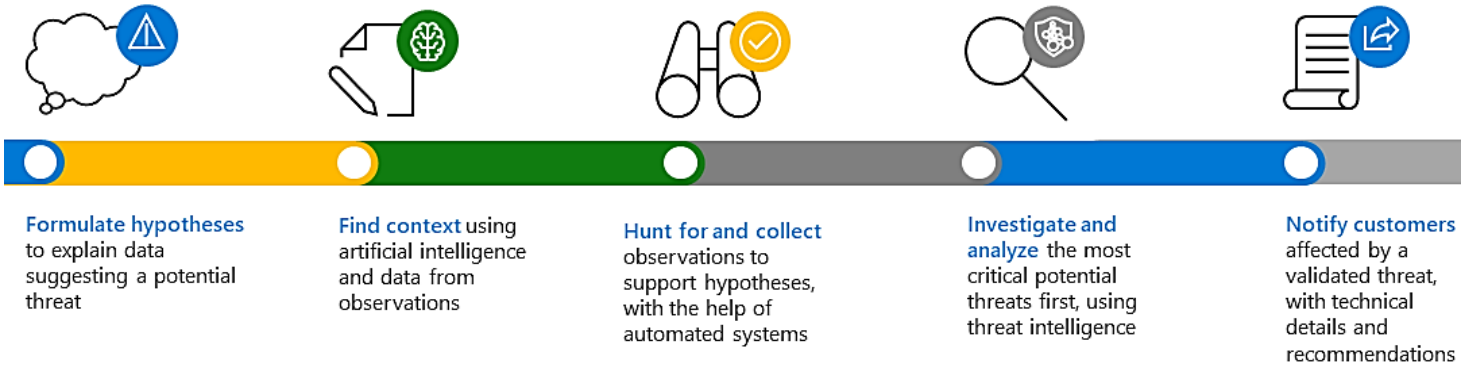
# Microsoft Defender Experts for Hunting

## Overview

Microsoft Defender Experts for Hunting (Defender Experts for Hunting) is a managed threat hunting service that proactively hunts for threats, on behalf of the customer, across their endpoints, email, identity, and cloud apps by using advanced hunting data from Microsoft 365 Defender (Microsoft Defender for Endpoint P2, Microsoft Defender for Office P2, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps). Defender Experts for Hunting will proactively hunt and investigate anything they find, then provide validated alert notifications along with remediation instructions, so that customers can quickly respond.

To carry out hunting on behalf of the customer, Microsoft analysts need access to customers M365 Defender advanced hunting data. Defender Experts for Hunting is sold separately from other Defender products. By purchasing and onboarding to the service, the customer is providing consent to Microsoft to access hunting data on their behalf and carry out the threat hunting activity.

Below is a diagram that shows how this service works.




*This diagram describes how Microsoft hunts beyond endpoints and provides recommendations in a five-step process. Starting with formulating a hypothesis to explain data suggestion a potential threat, then finding context using Artificial Intelligence and observations. Microsoft then hunts and collects more data to investigate and analyze the most critical threats and notifies customers of the findings with recommendations.*

# Additional Information

## Data Location, Usage, Retention

All data in existing Defender services will continue to reside in the customer's original Microsoft 365 Defender service storage location (See Microsoft 365 data locations).

Operational data for both **Defender Experts for XDR** and **Defender Experts for Hunting**, such as case tickets and analyst notes, are generated and stored in a Microsoft datacenter in the US region for the length of the service, irrespective of the Microsoft 365 Defender service storage location. Data generated for reporting dashboard is stored in customer's Microsoft 365 Defender service storage location. Reporting data and operational data will be retained for a grace period of no more than 90 days after a customer's subscription expires. If the customer terminates their subscription, data will be deleted within 30 days.

Microsoft experts hunt over advanced hunting logs in Microsoft 365 Defender advanced hunting tables. The data in these tables depend on the set of Defender services the customer is enabled for (e.g., Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, Azure Active Directory). Experts also leverage a large set of internal threat intelligence data to inform their hunting and automation.

## Security, Compliance

When a customer purchases and onboards **Defender Experts for XDR**, they are granting permission to Microsoft experts to access their Defender portal alerts, incidents, and advanced hunting data. Customer can configure the access permission level that is granted.

When a customer purchases and onboards **Defender Experts for Hunting**, they are granting permission to Microsoft experts to access the customer's advanced hunting data.

Both **Defender Experts for XDR** and **Defender Experts for Hunting** have been developed in alignment with existing security and privacy standards and are working towards several certifications including ISO 27001 and ISO 27018.

## Availability

Both **Defender Experts for XDR** and **Defender Experts for Hunting** are available for customers worldwide on our commercial public clouds. Both Defender Experts for XDR and Defender Experts for Hunting are not currently available to customers in government or sovereign clouds.

## Languages

Both **Defender Experts for XDR** and **Defender Experts for Hunting** are delivered in English language only at this time.

## Additional resources

Microsoft Security Experts webpage: https://aka.ms/MicrosoftSecurityExperts

Microsoft Defender Experts for XDR webpage: https://aka.ms/DefenderExpertsForXDR

Microsoft Defender Experts for Hunting webpage: https://aka.ms/DefenderExpertsForHunting

Microsoft Privacy Statement: https://aka.ms/privacy

Microsoft Product Terms: https://www.microsoft.com/licensing/terms/

Microsoft Data Protection Addendum: https://aka.ms/dpa