Microsoft Security Experts

CY2022 Q3 – Microsoft Security Managed Services

Contents

Microsoft Security Experts

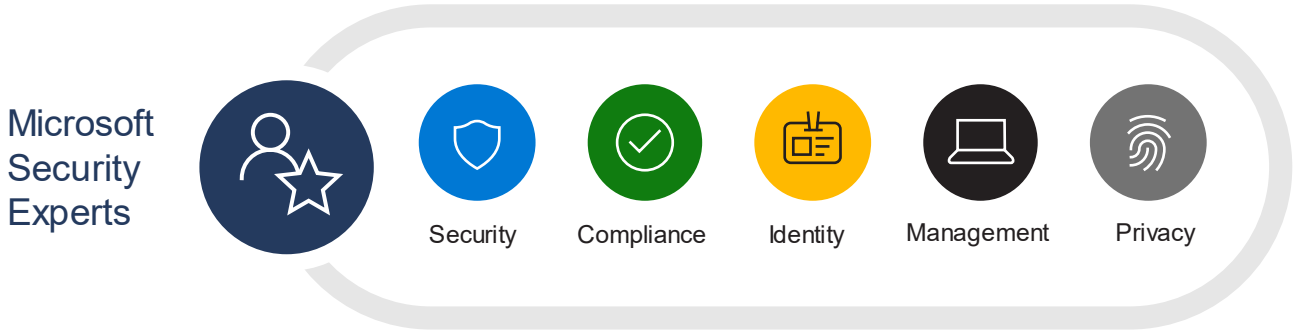
Purpose of this document

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 Hunting** (Defender Experts for Hunting) managed service.

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 287 days.[2] And, even when talent is available, access to highly skilled expertise remains a challenge.

Microsoft created Microsoft Security Experts, a new line of services to help customers achieve better security outcomes that spans 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.



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. [1] Cost of a Data Breach Report 2021, IBM. [2]

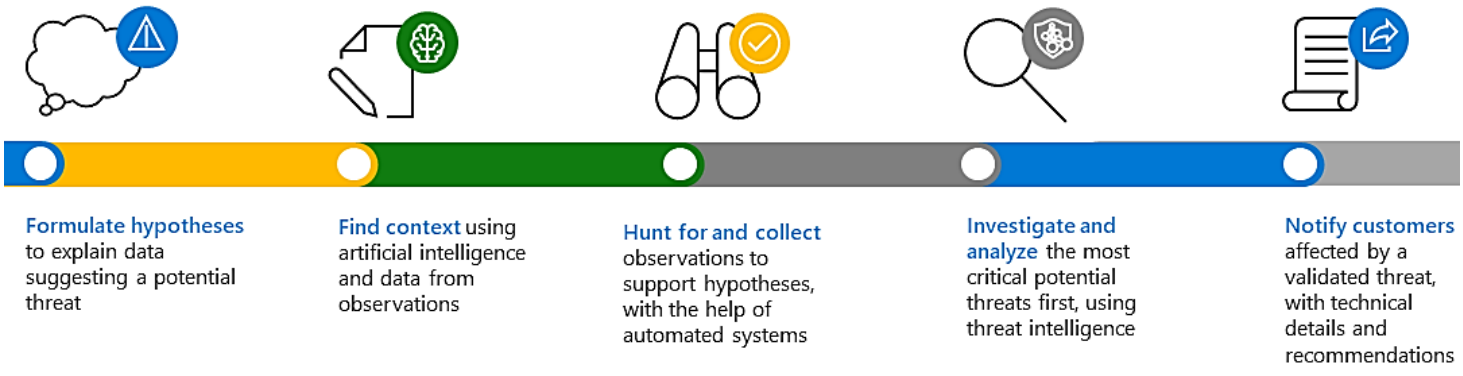
Microsoft Defender Experts for Hunting

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.

Data Location, Usage, Retention

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

Defender Experts for Hunting operational data, 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 less than 90 days after a customer leaves the service.

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 to Defender Experts for Hunting, they are granting permission to Microsoft experts to access the customer's advanced hunting data.

Defender Experts for Hunting has been developed in alignment with existing security and privacy standards and is working towards several certifications including ISO 27001 and ISO 27018.

Availability

The service is available for customers worldwide in our commercial public clouds. This service is currently not available to customers in government and sovereign clouds.

Languages

Defender Experts for Hunting is delivered in English language only at this time.

Additional resources

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