

Microsoft Defender Experts for Hunting

Proactive threat hunting that extends beyond the endpoint

[Click here to get started →](#)



Security

What is Defender Experts for Hunting?

Microsoft Defender Experts for Hunting is a managed threat hunting service that proactively looks for threats 24/7/365 across endpoints, email, identity, and cloud apps using Microsoft 365 Defender data. The service combines hunter-trained AI and human expertise to probe deeper to expose significant threats.

Technology is not enough to defend against cybercrime. Organizations need to proactively look for potential threats versus relying solely on disparate product alerts. Most security teams are not able to dedicate enough time to proactive threat hunting because they are at capacity with alert triage and improving their security posture.

Defender Experts for Hunting extends your team's threat hunting capabilities to add a layer of proactive threat detection to improve your overall SOC response.

Expertise on demand

Our experts extend your team's threat hunting capabilities for an additional layer of proactive threat detection.

Cross-domain hunting

Access leading threat intelligence and unparalleled visibility of the attack story as we reason over 43 trillion threat signals each day.

Fast deployment

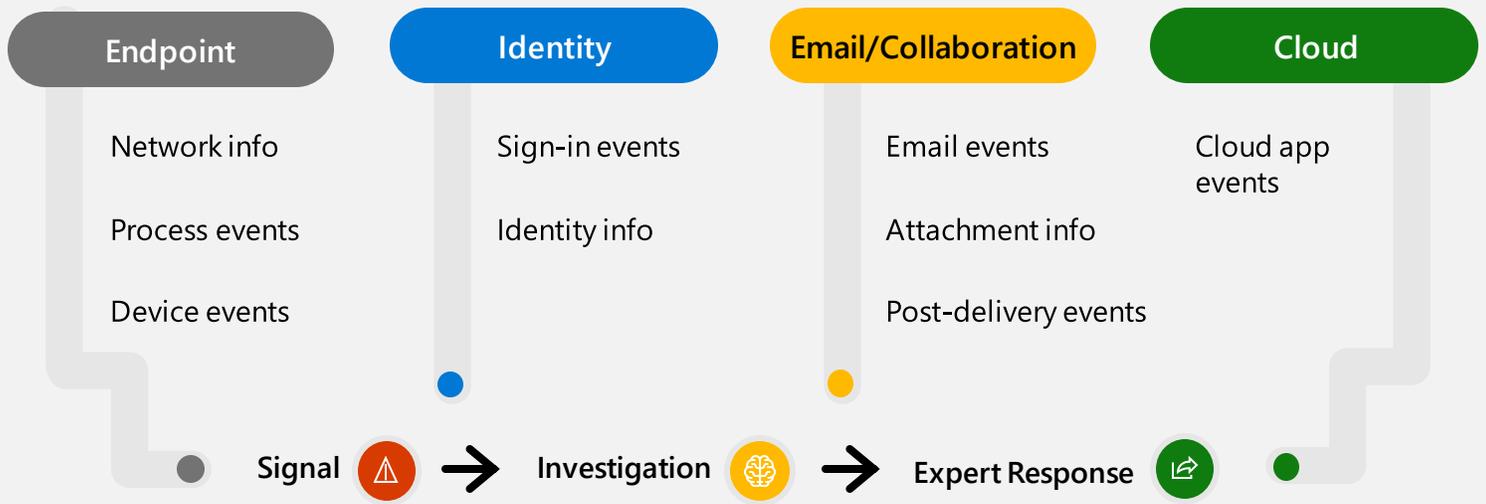
Deploy threat hunting in hours across all Microsoft 365 Defender products.

Straightforward pricing

Per-user pricing makes budget forecasting easier.



Unifying cross-domain signals paints the full picture of the attack story



Core Features



Threat hunting and analysis

Let Microsoft threat-hunting experts look deeper to expose advanced threats and correlate across the stack.



Hunter-trained AI

Improve threat discovery and prioritization with automated tools trained by our security experts based on their learnings.



Experts on demand

Ask a Defender Expert about a specific incident, nation-state actor, or attack vector.



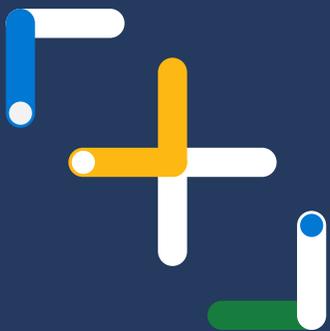
Defender expert notifications

Receive incident notifications to help improve your security operations center (SOC) response.



Reports

An interactive experience showing what we hunted and what we found.



“We haven’t found any company other than Microsoft that offers a coherent architecture that combines end-to-end security solutions with such a high and broad degree of productivity, hardware, and interoperability.”

Igor Tsyganskiy

Chief Technology Officer Bridgewater Associates

[Click here to get started →](#)