Microsoft Security

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 was created for customers who have a robust security operations center and want Microsoft to help them proactively find for threats. Our experts will hunt across your Microsoft 365 Defender data and investigate anything they find. Then, they will hand off validated alert information along with remediation instructions, so you can quickly respond.

Proactive threat hunting is time consuming and requires deep expertise in both hunting tactics and data structure. Most security teams are not able to dedicate enough time to this task because they are at capacity with alert triage and improving their security posture.

We believe that Defender experts for Hunting are in the best position to help our customers hunt across their Microsoft 365 Defender environment, because we're the people who built the products you use every day.

Expertise on demand

Let our experts handle threat investigation and provide you with remediation instructions.

Cross domain hunting

Get a full picture of the attack story as we reason over 24 trillion cross-domain threat signals each day.

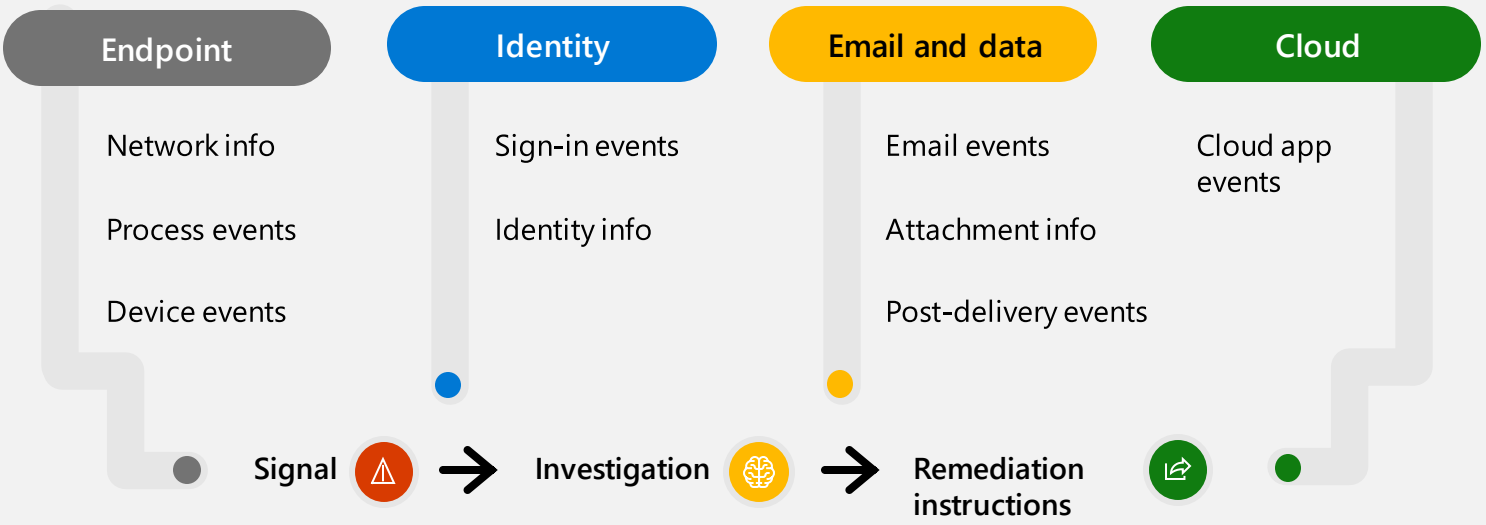
Fast deployment

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 →