Microsoft Security

Microsoft Defender Experts for XDR

Go beyond the endpoint with managed XDR to help stop attackers and prevent future compromise

Why Managed Extended Detection and Response (MXDR)?

Expertise
Extend 24/7 coverage and close skill set gaps to improve SOC operations

Efficiency
Alleviate alert fatigue and focus on what matters to improve security posture

Scope
Go beyond the endpoint to gain a more complete picture of the attack story

Defender Experts for XDR

A managed extended detection and response (MXDR) service that gives security teams air cover to help stop attackers in their tracks and prevent future compromise.

Capabilities

Managed detection and response – Let our expert analysts manage your Microsoft 365 Defender incident queue and guide your response to incidents or handle triage, investigation, and response on your behalf.

Proactive threat hunting – Extend your team's threat hunting capabilities and prioritize significant threats with Defender Experts for Hunting built in.

Live dashboards and reports – Get a transparent view of our operations conducted on your behalf, along with a noise-free, actionable view into what matters for your organization, coupled with detailed analytics.

Proactive check-ins – Benefit from remote, periodic check-ins with your named SDM team to guide your MXDR experience and improve your security posture.

Fast and seamless onboarding – Get a guided baselining experience to ensure your Microsoft security products are correctly configured.

Scope

→ Microsoft 365 Defender

Availability

→ In public preview now

→ Commercial cloud

→ English language only

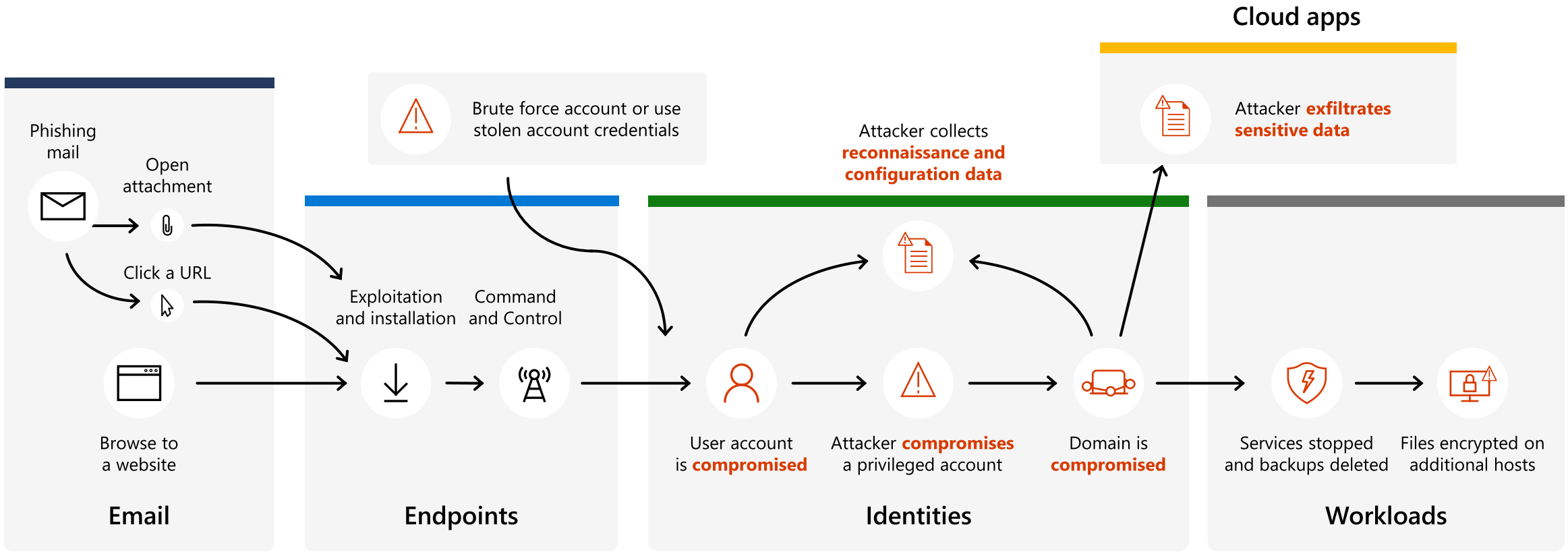
Requirements

→ 1 or more Microsoft 365 Defender product

- Microsoft Defender for Endpoint P2
- Microsoft Defender for Office P2
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

Endpoint-focused detection and response solutions are insufficient to protect against evolving threats

Attacks are crossing modalities



Typical Human-Operated Ransomware Campaign

Our unique view helps customers with the most challenging attacks

Identity compromise

Respond to phishing, password brute force attacks, account takeover

Device-to-cloud pivoting

Correlate cloud activity originating from on-premises compromise

Cloud application breach

Detect Cloud Application breaches, lateral movement

O365 tenant compromise

Detect Office 365 tenant compromise/ business email compromise

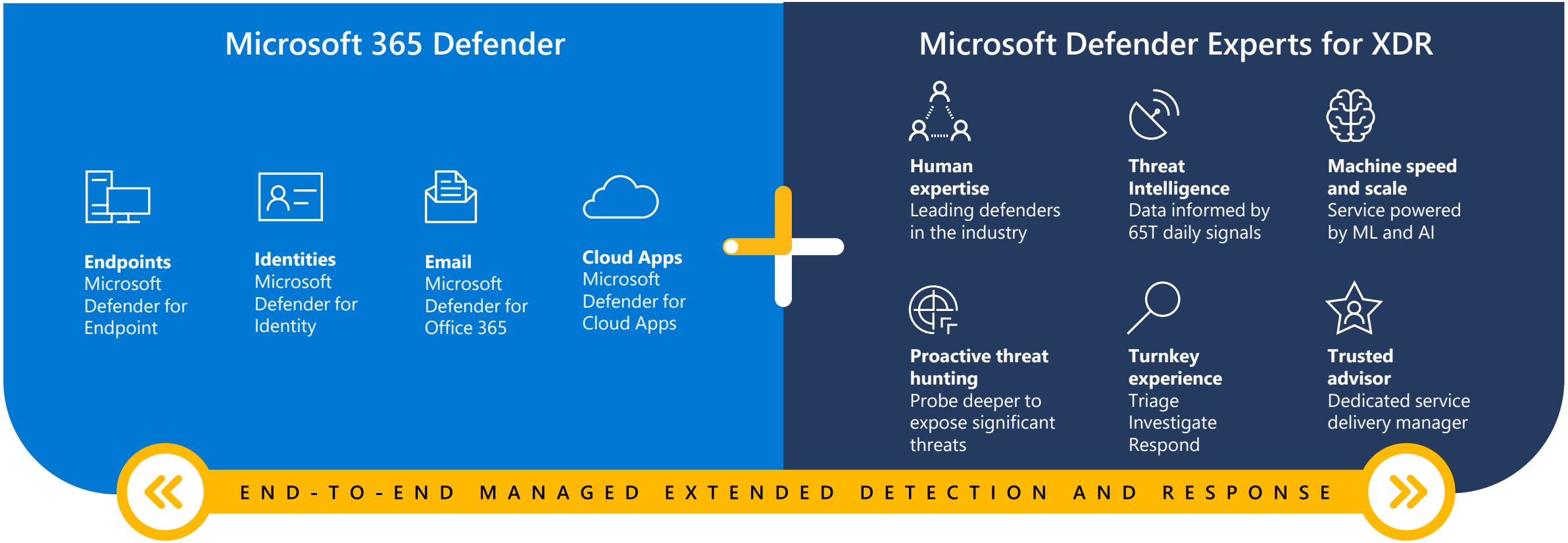
Cloud data theft

Detect cloud data exfiltration

In addition to device-focused scenarios across device compromise, malware, ransomware

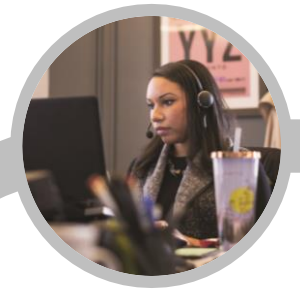
Defender Experts for XDR

A true MXDR solution that delivers comprehensive detection and response for customers using industry-leading Defender workloads



How Defender Experts for XDR works

Jumpstart your SOC with **24/7/365** coverage



Triage

Filter the noise to prioritize Microsoft 365 Defender 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 by delivering step-by-step guided and managed response, and **consult on-demand via chat**

Prevent

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

CONTINUOUS SECURITY POSTURE IMPROVEMENTS


Defender Experts
for Hunting

Defender Experts for Hunting

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 to prioritize significant threats and improve your overall SOC response.

Capabilities

Threat hunting and analysis - Expose advanced threats and identify the scope and impact of malicious activity associated with human adversaries or hands-on-keyboard attacks.

Defender Expert Notifications – Notifications show up as incidents in Microsoft 365 Defender to help improve your SOC response with specific information about scope, method of entry, and remediation instructions.

Experts on Demand – Click the 'Ask Defender Experts' button in the Microsoft 365 Defender portal to ask for help on a specific incident, nation-state actor, or attack vector.

Hunter-trained AI – Microsoft experts feed their learning back into the automated tools they use to improve threat discovery and prioritization.

Reports – Interactive reports show what we found and investigated, adversary tactics according to the MITRE framework, and threat categorization based on behavior, characteristics, and impact.

Scope

- Microsoft 365 Defender

Availability

- Generally Available
- English language only
- Commercial cloud

Pricing

- per user per month (List price)

Requirements

- 1 or more Microsoft 365 Defender products
  - Microsoft Defender for Endpoint P2
  - Microsoft Defender for Office P2
  - Microsoft Defender for Identity
  - Microsoft Defender for Cloud Apps
- 1,000 minimum users recommended

Defender Experts Comparison

Category	Capability	Defender Experts for Hunting *24/7 managed threat hunting*	Defender Experts for XDR *24/7 managed extended detection and response (MXDR)*
Security Technology	Coverage	Endpoint, O365, Applications, Identity	Endpoint, O365, Applications, Identity
Proactive Hunting	Managed Threat Hunting	✓	✓
	Reports and Insights	✓	✓
	Experts on Demand	✓	✓
Detection & Response	Alert Monitoring	×	✓
	Incident Triage and Handling	×	✓
	Managed Response	×	✓
Proactive Engagements	Onboarding	×	✓
	Proactive Check-ins	×	✓
	Proactive Tuning Guidance	×	✓

Augment your team with Microsoft expertise

Get a seamless, stress-free experience with your assigned Service Delivery Manager (SDM)

Comprehensive onboarding

Go through a thorough onboarding experience that assesses and enhances your security posture

Close alignment

Engage in regular touch points with a named security expert from Microsoft

Strategic engagement

Give feedback and get recommendations to continuously strengthen your security posture