

Sophos + Microsoft

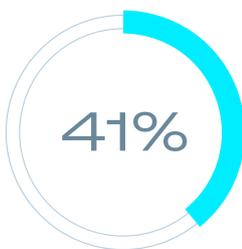
Stronger together for better security

Today's cyber threats demand stronger, more adaptive protection across Microsoft environments. Elevate protection, reduce risk, and maximize the return on your security investments, by combining Sophos' industry leading solutions with the Microsoft tools you already rely on.

Microsoft-centric organizations face critical security pressures

Threat actors increasingly target identities, exploit gaps in siloed security tools, and overwhelm teams with alerts. Business email compromise attacks and session hijacking frequently bypass MFA, turning identity into a primary threat vector across Microsoft environments. Meanwhile, remote ransomware encryption and hands-on-keyboard techniques allow adversaries to slip past Microsoft defenses. Combined with limited in-house expertise, these pressures create critical visibility and response gaps.

Accelerate security outcomes



The percentage of Sophos MDR threat cases that are triggered by Microsoft telemetry.



The number of attacks on Microsoft environments neutralized by Sophos MDR in 2025.



The average threat remediation time in Microsoft environments by Sophos MDR.

Benefits

- **Maximize your Microsoft investment:** Extend the value of your Microsoft tools with deeper insight, stronger threat detection, and expert-led response.
- **Elevate protection:** Close gaps attackers exploit, across identity, endpoint, email, and network.
- **Accelerate security outcomes:** Sophos MDR analysts can rapidly remediate threats on your behalf.
- **Reduce operational complexity:** Simplify security management with integrated intelligence, unified workflows, and expert guidance that lightens the load on your team.
- **Strengthen resilience:** Benefit from protection informed by telemetry from hundreds of thousands of Microsoft environments.

Better together means better protected

Sophos elevates the security and value of your Microsoft environment with deeper insight, faster action, and unmatched expertise.



Defense for every Microsoft plan: Whether you're on M365 Business Basic/Standard/Premium, E3, or E5, Sophos delivers advanced protection, detection and response.



Built-in community immunity: Learnings from defending hundreds of thousands of Microsoft customers continuously strengthen protection across the Sophos community.



Breadth to cover the stack: Endpoint, Email, Firewall, ITDR, MDR, Advisory Services, all integrated with Microsoft to reduce risks and stop active threats.



Deep, two-way integrations: Sophos ingests rich Microsoft telemetry to identify adversary behavior and executes response actions directly in your Microsoft 365 environment.



Outcome ownership, not alert forwarding: Sophos MDR analysts don't just notify you; they can take immediate action directly in your Microsoft tenant.



Microsoft Certified experts: Sophos MDR teams include Security Operations analysts specializing in detecting and responding to cyberattacks using custom Microsoft response playbooks.

How Sophos elevates your Microsoft stack

Sophos offers a full suite of security capabilities that work in concert with your Microsoft tools. Each solution adds depth, intelligence and resilience to your broader Microsoft strategy. From endpoints and identities to email, network and beyond, Sophos delivers cohesive protection designed to close the gaps that attackers rely on.

Sophos MDR for Microsoft environments

24/7 managed detection and response that combines proprietary detections, Microsoft signals, and expert analysts to shut down threats, fast. Ideal for organizations running Microsoft technologies, or mixed environments, that want an expert team to own cybersecurity outcomes, not just send alerts.

- Uses Microsoft signals to identify and protect against sophisticated attacks that technology alone cannot stop.
- Leverages telemetry from Microsoft Graph Security and Management Activity APIs to deliver deep detection value, even without E5 licensing.
- Includes integrations with both Microsoft and non-Microsoft solutions for complete coverage of your IT estate.
- Rapidly executes response actions directly in your Microsoft environment, including revoking user sessions, disabling signins, and suspending malicious inbox rules.
- Use with Sophos Endpoint (included) or Microsoft Defender for Endpoint – you choose.

Sophos MDR is a Microsoft-verified Small and Medium Business (SMB) Solution through the Microsoft Intelligent Security Association (MISA), validating deep integration with Microsoft Defender for Endpoint and Defender for Business to deliver stronger, faster protection across Microsoft environments.



Sophos ITDR for Entra ID

Sophos Identity Threat Detection and Response (ITDR) continuously scans Entra ID for misconfigurations and exposures, monitors for credential abuse including dark web findings, and enables analysts to take response actions in Entra ID to contain identity attacks, fast. Sophos ITDR elevates the native IAM capabilities of Entra ID with unmatched threat defense from Sophos.

Sophos Endpoint for superior ransomware protection

70%* of modern, human-operated ransomware attacks use remote encryption to avoid detection by tools including Microsoft Defender. Sophos Endpoint includes proprietary CryptoGuard technology to stop local and remote ransomware in its tracks. User-based licensing maximizes value when team members have multiple devices, including endpoints running legacy and out-of-support Windows operating systems.

Sophos Email for Microsoft 365

Sophos Email integrates with Exchange Online to stop phishing and business email compromise attacks and adds user awareness training and phishing simulations, all without disrupting mail flow or Microsoft security policies.

Sophos Firewall for Microsoft environments

Sophos Firewall is optimized for Microsoft environments, with flexible hardware, virtual, and cloud deployment options (including Azure and Hyper-V), Entra ID integration for zero-trust remote access, and Azure Virtual WAN integration for SD-WAN overlay network deployments.

Taegis XDR with Next-Gen SIEM for Microsoft E5 + Sentinel

For enterprises that need SIEM-grade retention and cross-stack detection with predictable data storage economics, Taegis unifies Microsoft and non-Microsoft telemetry, integrates with Sentinel, and avoids variable events-per-second billing.

Sophos Intelix for Microsoft Copilot

Sophos Intelix brings Sophos X-Ops' threat intelligence into Microsoft Security Copilot and Microsoft 365 Copilot, delivering smarter security, seamlessly within Microsoft environments. These integrations make advanced cyber intelligence instantly accessible where defenders, IT admins, and business users already operate.

Choosing the right Sophos and Microsoft combination

Strengthening your Microsoft environment starts with choosing the right pairing of Sophos capabilities and Microsoft technologies. Whether you want to build on your existing Microsoft plan or address a specific security challenge, Sophos offers clear paths that maximize protection, simplify operations, and deliver stronger outcomes.

Align with your Microsoft plan

Identify the strongest combination of Sophos and Microsoft capabilities based on your M365 subscription. Each combination is designed to enhance visibility, improve threat response, and close the gaps attackers rely on.

For M365 Business Basic, Business Standard, O365 E1 and O365 E3	For M365 Business Premium, M365 E3, and E5 with Microsoft Defender solutions
<p>Organizations using these Microsoft productivity focused plans often need stronger endpoint, email, and detection capabilities to defend against modern threats.</p> <p>Recommended Sophos additions:</p> <ul style="list-style-type: none">• Sophos MDR — delivers 24/7 detection and expert-led response using Microsoft telemetry.• Sophos Endpoint — advanced protection, including robust remote ransomware protection.• Sophos Email — enhanced phishing and business email compromise (BEC) protection.	<p>These plans introduce more built-in protection tools, but teams often need stronger detection, response, and validation of their organization’s security posture.</p> <p>Recommended Sophos additions:</p> <ul style="list-style-type: none">• Sophos MDR with Microsoft Defender for Endpoint (or switch to Sophos Endpoint).• Sophos Advisory Services — identify security gaps with penetration testing and assessments.• Sophos Email Monitoring System — layered visibility and detection on top of Microsoft 365 email.• Taegis XDR with Next-Gen SIEM — cross-stack detection with predictable extended data retention costs.

Align with your security needs

Sophos offers targeted combinations built to address the threats most common in Microsoft environments. Close security gaps across identity, endpoint, email, and network.

Identity-based threats	Remote ransomware
<p>Attackers increasingly target Entra ID and user identities to gain a foothold in your environment.</p> <p>Recommended combination:</p> <ul style="list-style-type: none">• Microsoft Entra ID + Sophos MDR<ul style="list-style-type: none">- Add Sophos ITDR for proactive identity risk discovery and response.	<p>70%* of modern, human-operated ransomware attacks use remote encryption to avoid detection by tools like Microsoft Defender.</p> <p>Recommended combination:</p> <ul style="list-style-type: none">• Sophos Endpoint + Sophos MDR<ul style="list-style-type: none">- Or Microsoft Defender for Endpoint + Sophos MDR if Defender is already deployed.
Business email compromise (BEC)	Security posture and risk reduction
<p>BEC attacks rely on impersonation, inbox rule manipulation, and MFA-bypass techniques.</p> <p>Recommended combination:</p> <ul style="list-style-type: none">• Microsoft 365 Email + Sophos Email + Sophos MDR	<p>Organizations looking to strengthen their resilience benefit from proactive security testing delivered by security experts.</p> <p>Recommended combination:</p> <ul style="list-style-type: none">• Sophos Advisory Services to uncover weaknesses<ul style="list-style-type: none">- Plus Microsoft and Sophos solutions to address identified risks.

Speak with an expert today to build the right security approach for your Microsoft estate. Our team will help you identify the ideal combination of Sophos and Microsoft capabilities for your M365 subscription and ensure you're getting the full value from your Microsoft investments.

Learn more: [Sophos.com/Microsoft](https://sophos.com/Microsoft)

* Microsoft 2024 Digital Defense report.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-03-02 BR-EN (TA) CRE-4588

