SOLUTION BROCHURE

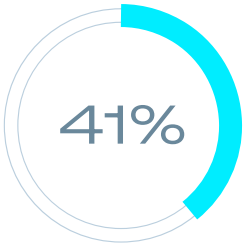
Taegis MDR + Microsoft E5 and Sentinel

Stronger together for better security

Enterprises with strong Microsoft investments in E5 licensing, the Defender suite, and Sentinel often reach a maturity plateau where visibility is strong, but operational capacity and resiliency gaps remain. Taegis MDR delivers a complementary and independent cross-security stack detection and response layer that unifies operations, enhances real-world security outcomes, and preserves Sentinel's strategic value without adding complexity or cost risk.

Microsoft-centric organizations face critical security pressures

Microsoft-centric enterprise organizations are under intense pressure as identity-driven attacks, AI-enhanced threats, and cloud sprawl converge on the same stack they rely on for email, collaboration, identity, and infrastructure. Threat actors increasingly target identities, exploit gaps in siloed or misconfigured security tools, and overwhelm teams with excessive noise and alerts. Additionally, the lack of insights from non-Microsoft security tools, along with the tough choices between maintaining security visibility and managing budget constraints, can lead to late detection of attacks or, in some cases, complete oversight of security breaches.



of MDR cases are triggered by Microsoft telemetry.

advanced attacks on Microsoft environments were neutralized by Sophos in 2025.

The average threat remediation time in Microsoft environments by Sophos.

Benefits

- **Maximize your Microsoft investment** with deeper insight, stronger threat detection, and expert-led response.
- **Defend Microsoft and hybrid environments** with a consistent operating model that works across current and future security tools.
- **Predictable data storage economics** by unifying Microsoft and non-Microsoft telemetry at scale.
- **Elevate protection** by closing attacker gaps across identity, endpoint, email, and network.
- **Holistically defend Microsoft and hybrid environments** with a stable operating model, regardless of your current and future security tools.

Better together means better protected

Taegis MDR elevates your defenses and helps you unlock the advanced security value of your Microsoft E5 licenses. Together, they implement an adaptive security posture that continuously improves and is resilient by design.

Architectural resilience
Relying on a single vendor creates correlated risk. Taegis MDR adds independent detection and response, providing redundancy and resilience during vendor-wide incidents.

Right tool for the job
Sentinel excels at Microsoft-native correlation, Azure environments, and compliance reporting. Taegis MDR delivers cross-stack detection and response, and unified operations.

Outcome ownership
Taegis MDR analysts don't just notify you; they can take immediate action directly in your Microsoft tenant, with your prior approval.

Freedom from SIEM cost constraints
Taegis MDR allows broad telemetry ingestion without cost tradeoffs, sending only high-value signals to Sentinel for retention, analytics, governance, and compliance without exceeding budgets.

Future-proofing the SOC
Whether deepening Microsoft adoption or keeping a hybrid stack, Taegis MDR stabilizes SOC operations and avoids costly replatforming.

Microsoft Certified experts
Security Operations analysts specializing in detecting and responding to cyberattacks using custom Microsoft response playbooks.

How Taegis MDR elevates your Microsoft stack

Taegis MDR offers a full suite of security capabilities that complements your existing Microsoft investment, adding operational capacity and resilience to your broader Microsoft strategy.

Taegis MDR with NextGen SIEM for Microsoft E5 + Sentinel

24/7 managed detection and response that combines proprietary detections, Microsoft signals, and decades of service delivery experience with an open platform to deliver measurable security outcomes. Whether fully managed or operated in collaboration with your security analysts, Taegis MDR accelerates your security maturity and delivers superior detection and response with predictable, cost-effective retention of Microsoft and non-Microsoft telemetry.

- An independent detection and response layer that leverages Microsoft telemetry and reduces single vendor/platform risk.
- Extensive telemetry ingestion of Microsoft and non-Microsoft technology solutions for complete coverage of your IT estate.
- Operates alongside Sentinel, offering predictable costs and flexible scaling, enhancing hunting and triage workflows, and collaborating with Sentinel-tuning partners.
- Uses Microsoft signals to identify and protect against sophisticated attacks.
- Taegis MDR Enhanced handles Sentinel incidents through a unified workflow, allowing analysts to easily pivot to Sentinel for enrichment or validation.
- An open platform that allows you to choose Microsoft Defender for Endpoint, Sophos Endpoint (included), or any third-party endpoint protection solution.

Taegis MDR can ingest data from the following Microsoft Products	
• Microsoft Defender for Endpoint • Microsoft Defender for Office 365 • Microsoft Defender for Cloud Apps • Microsoft Defender for Identity • Microsoft 365 Defender • Microsoft Entra ID Protection • Microsoft Purview Data Loss Prevention • Microsoft Purview Insider Risk Management	• Microsoft Azure Activity Log • Microsoft Azure Application Gateway • Microsoft Azure Event Hubs • Microsoft Azure Firewall • Microsoft Azure Front Door • Microsoft Azure Network Watcher Flow Logs • Microsoft Azure Storage Account

Sophos Endpoint for superior ransomware protection

Seventy percent of modern, human-operated ransomware attacks use remote encryption to avoid detection by tools including Microsoft Defender.

Sophos Endpoint is natively integrated and included with Taegis MDR. As an open platform, Taegis MDR allows organizations to use their existing endpoint protection solution or optionally upgrade to Sophos Endpoint for elevated protection.

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.

Additional Sophos solutions for Microsoft Environments

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 identity to email, network, and beyond, Sophos delivers cohesive protection designed to close the gaps that attackers rely on.

Sophos Identity Threat Detection and Response (ITDR) for Entra ID

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 protection from Sophos.

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.

Sophos Intelix for Microsoft Copilot

Sophos Intelix brings Sophos XOps' 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.

Sophos Email for Microsoft 365

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.

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.

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

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

2026-03-02 BR-EN (NP) CRE-4736