



EBOOK

Expert security, always on

Unlock the full value of your
Microsoft investment with the
world's largest Agentic SOC



Overwhelmed and under attack

AI-powered attacks and rising cybercrime costs are outpacing what lean IT teams can handle alone.

AI is rewriting the threat landscape

Attackers are using AI to phish, map environments, script exploits, and move faster across endpoints, cloud, identity, and email — often using legitimate credentials and trusted Microsoft tools to evade traditional defenses. At the same time, Copilots, agents, and LLM-powered workflows are expanding the attack surface, giving adversaries more ways to reach sensitive data and exfiltrate it at machine speed.

For SMBs, the pressure is especially acute. Small teams can't staff around the clock, can't investigate every alert, and can't match the speed of AI-driven attackers with manual processes alone.

96%

of SMBs struggle to investigate security alerts - allowing threats to go undetected

Source: [Sophos](#)

75%

of cyber attacks on SMBs resulted in losses of \$250,000 or more.

Source: [Identity Threat Resource Center](#)

88%

of ransomware attacks strike outside business hours.

Source: [Sophos](#)

Effective defense now requires an Agentic SOC

Modern attacks demand AI-accelerated operations that combine always-on expertise, deep threat intelligence, and accountable response to hunt, investigate, and stop threats at speed and scale.

An Agentic SOC for your Microsoft environment

Sophos Managed Detection and Response (MDR) is the world's largest Agentic SOC, integrating deeply with your Microsoft stack to detect and stop cyberattacks that tools alone can't block. AI handles speed and scale. Humans provide judgment and accountability.



Free up your team with 24/7 AI-accelerated threat monitoring

Sophos MDR monitors your Microsoft environment around the clock using agentic AI and deep human expertise — including the nights, weekends, and holidays when most attacks are deliberately timed to strike. Autonomous agents investigate and prioritize alerts in seconds, so your team only sees what matters.



Catch sophisticated attacks fast — before a compromised account becomes a business crisis

When AI can act alone, it does. When judgment is needed, a human is already there. Sophos MDR takes action directly inside your Microsoft environment, neutralizing advanced cyberattacks in just 12 minutes on average — no delay, no manual handoff, no opportunity for the attack to progress.



Turn your existing Microsoft solutions into an integrated security powerhouse — without replacing what you already own

Sophos MDR unlocks the full value of your Microsoft solutions by extracting and using threat telemetry to detect attacks — regardless of your plan or license level. It's part of a unified AI-native architecture where endpoint, identity, email, cloud, and more share a common data fabric to accelerate security outcomes.

24/7 expert monitoring

**Attacks are timed to maximize damage.
Stop them before they start.**

Today's threat actors log in with stolen credentials, move through your environment using your own tools, and blend in with normal activity. Increasingly, they're using AI to accelerate every stage — from reconnaissance to execution. No malware to flag. No signature to catch. Businesses, no matter their size, need someone monitoring for threats 24/7, 365.

Sophos MDR can help

As the world's largest Agentic SOC, Sophos MDR monitors your Microsoft environment around the clock using agentic AI and deep human expertise — including the nights, weekends, and holidays when most attacks are deliberately timed to strike. Alerts are investigated and prioritized by autonomous AI agents with human accountability. AI-powered, expert-led triage cuts through noise, freeing your team to focus on strategic work without expanding headcount. Every response follows your approved guardrails, always governed by expert oversight and accountability.



Did you know?

52% of Sophos MDR cases are resolved end-to-end by AI, in an average of 89 seconds from alert to automated response.

sophos

Rapid threat response

Response times are compressing as adversaries adopt AI

AI-driven phishing, credential abuse, and automated reconnaissance flood SMB environments with an ever-increasing volume of attacks and alerts to sift through. Adversaries are using AI to execute more polished attacks, compressing response times and increasing pressure on staff. Defending against AI-speed attacks requires AI-speed response, with human accountability for every outcome.

Sophos MDR can help

When AI can act alone, it does. When judgment is needed, a human is already there — the right response, from the right responder, every time, AI or human, decided in seconds. Sophos MDR takes action directly inside your Microsoft environment, neutralizing threats in just 12 minutes on average — and just 89 seconds when end-to-end AI.

Through bidirectional integration with Microsoft, Sophos MDR enables autonomous agents and expert analysts to investigate and respond directly inside the tenant. Responses follow your approved guardrails: fully automated where pre-authorized, analyst-led where needed, and always governed by expert oversight.



Did you know?

Sophos MDR includes
unlimited incident
response hours
— no retainers, no
surprise costs.

sophos

From siloed tools to unified defense

Upgrade your security stack to a cyber defense system

Your productivity and security operate in silos, each generating its own alerts and logs, creating a fragmented view of risk. That fragmentation drives duplicate work, weak visibility, and a nagging sense the stack should deliver more. And when budget conversations start, it can be difficult to prove ROI.

Sophos MDR can help

Whatever your plan or license level, Sophos MDR unlocks the full value of your Microsoft solutions by ingesting rich Microsoft telemetry to identify adversary behavior and execute response actions directly in your Microsoft 365 environment.

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 and Defender for Business to deliver stronger, faster protection across Microsoft environments.

Beyond Microsoft, Sophos MDR correlates deep threat intelligence across your entire network, regardless of vendor. With more than 350 third-party integrations, there are no blind spots – so even the most advanced attacks are identified and contained before they disrupt the business. And because Sophos defends 600,000+ organizations worldwide, every threat we see makes your next defense stronger.



Did you know?

Sophos MDR integrates with more than 350 third-party tools and software, ingesting telemetry, logs, and security alerts from across your environment.

sophos

Microsoft-optimized security for your business

AI speed. Human judgment. One team protecting your Microsoft environment 24/7.

Ready to see what Microsoft-optimized security looks like?

Discover how Sophos MDR can expand your team, unlock the full value of your Microsoft investments, and defend your organization in the Agentic AI era.

[Learn more about
Sophos MDR](#)

[Explore Sophos MDR on
the Microsoft Marketplace](#)

Member of
**Microsoft Intelligent
Security Association**



Microsoft Verified
SMB Solution

