SOPHOS

SOPHOS AI DEFENSE

Bring AI out of the shadows.

Adopt and use AI with confidence.

Organizations are adopting AI faster than they can handle it. Sensitive data is being shared, agents operate without visibility, and security teams often lack insight into what tools are in use. Powered by Sophos Fusion, Sophos AI Defense helps you discover, understand, and control AI usage across your environment.

75% of employees use AI tools not sanctioned by IT[1]

82% of organizations discovered unknown AI tools or workflows[2]

90% of IT leaders express concern about shadow AI risk[3]

1.3B AI agents will expand attack surfaces by 2028[4]

WHAT SOPHOS DELIVERS

See AI. Control AI. Secure AI.

See what AI is really doing.

Visibility starts with what's actually happening, not just what's approved.

- Discover AI usage across your employees, tools, and workflows
- Validate approved tools and surface unsanctioned usage
- Gain continuous visibility across browser, endpoint, and network interaction points

Identify the AI behavior that matters most.

Not all AI activity introduces exposure, but without context, teams can't distinguish between approved usage and behavior that warrants action.

- Assess AI usage including identity, behavior, and data context
- Distinguish acceptable use from unmanaged, over-privileged, or risky activity
- Focus on meaningful exposure instead of reacting to isolated or low-impact events

Turn AI policy into control.

As AI adoption scales, static policies break down. Enforcement must be continuous and enforceable.

- Apply guardrails across how AI is used, not just how it's defined in policy
- Enforce controls at key interaction points to align AI usage and data sharing with policy and regulations
- Reduce shadow AI by guiding users toward approved tools

Bring AI into security operations.

AI expands your attack surface, with new risks across prompts, data, and agent-driven actions that require active management.

- Surface AI misuse, abuse, and compromise into detection and investigation workflows
- Integrate AI activity into broader security telemetry
- Apply the same playbooks, tools, and escalation paths used for standard threats

SOPHOS AI DEFENSE AT A GLANCE

- Discover AI usage across employees, tools, and workflows — including shadow AI
- Identify risky behavior using identity, data exposure, and usage context
- Apply guardrails across browser, endpoint, and network interaction points
- Prevent sensitive data from being shared with AI tools by inspecting prompts, uploads, and AI interactions in real time
- Integrate AI risk into security operations workflows

WHO SOPHOS AI DEFENSE IS FOR

- Security leaders who need visibility and control over AI usage
- Security operations teams responsible for identifying and responding to AI-driven risk
- Organizations seeking to adopt and deploy AI tools securely
- Businesses looking to extend existing security investments to manage AI risk

FOCUS ON REAL AI RISK

Practical AI security, built for how AI is actually used.

Solve today's AI risk, not future hypotheticals.

Most solutions secure models or applications. Sophos AI Defense addresses what's actually putting you at risk today:

- Unmanaged AI usage across the workforce
- Limited visibility into tools, agents, and workflows
- Sensitive data shared with external AI tools through prompts and automated workflows

Extend the security you already have.

Sophos AI Defense builds on your existing controls — coordinating them to deliver immediate, practical outcomes.

- Extends your Sophos Workspace Protection, EDR, Firewall, XDR, and MDR investment
- Connects control points into a unified AI policy framework
- Delivers immediate value — no new deployment or added resources required

Turn visibility into outcomes, not just more data.

Visibility alone isn't enough. Sophos AI Defense turns insight into action:

- Combine visibility, context, and enforcement into one system across AI usage, data movement, and agent activity
- Apply policy, prioritize issues, and respond within the same workflows
- Deliver controlled outcomes — not just more dashboards

INDUSTRY RECOGNITION

Validated by the analysts and organizations that matter most.

GARTNER 2026

Leader, Endpoint Protection

G2 SUMMER 2026

#1 rated XDR and MDR solutions

MITRE ATT&CK EVALS

100% detection coverage

GARTNER PEER INSIGHTS

A "Customers' Choice" for XDR and MDR

One system. Every control point. Defending as one.

Sophos AI Defense is part of Sophos Fusion, the world's most complete cyber defense system. It protects organizations from AI-enabled threats that move faster than defenders can respond.

sophos.com/ai-defense →

[1] Microsoft Work Trend Index Annual Report, 2025. [2] CSA, "The Shadow AI Agent Problem in Enterprise Environments," 2025. [3] Komprise IT Survey: AI, Data & Enterprise Risk. [4] IDC, "IDC Info Snapshot" (May 2025).

2026-07-13 · SB-EN (MC)

SOPHOS