SOPHOS

SOPHOS AI DEFENSE

Schaffen Sie Transparenz über die KI-Nutzung.

Nutzen Sie KI sicher und souverän.

Unternehmen und Organisationen führen KI schneller ein, als sie deren Nutzung steuern können. Sensible Daten werden ausgetauscht, Agenten agieren ohne Transparenz und Sicherheitsteams fehlt oft der Überblick darüber, welche Tools im Einsatz sind. Sophos AI Defense basiert auf Sophos Fusion und hilft Ihnen dabei, die Nutzung von KI in Ihrer Umgebung zu erkennen, zu verstehen und zu kontrollieren.

69 %

Organisationen, die den Verdacht haben oder Beweise dafür besitzen, dass Mitarbeiter verbotene öffentliche KI-Dienste nutzen[1]

82 %

der Unternehmen und Organisationen stoßen bei Untersuchungen auf unbekannte KI-Tools oder -Workflows[2]

90 %

der IT-Entscheider äußern Besorgnis über Risiken durch Schatten-KI[3]

1,3 Mrd.

Vorhergesagte Zahl von KI-Agenten bis 2028[4]

WAS SOPHOS BIETET

KI erkennen. KI kontrollieren. KI absichern.

Sehen Sie, wie KI wirklich genutzt wird

Transparenz beginnt mit der tatsächlichen Nutzung von KI – nicht nur mit der genehmigten Nutzung.

- Ermitteln Sie, wie KI in Ihrem Unternehmen sowie in Ihren Tools und Workflows gesetzt wird.
- Prüfen Sie die zugelassenen Tools und decken Sie nicht genehmigte Nutzung auf.
- Erhalten Sie kontinuierliche Transparenz über Browser-, Endpoint- und Netzwerk-Interaktionspunkte.

Identifizieren Sie das KI-Verhalten, das die meisten Risiken birgt

Nicht jede KI-Aktivität birgt Risiken, aber ohne Kontext können Teams nicht zwischen genehmigter Nutzung und Verhalten, das ein Eingreifen erfordert, unterscheiden.

- Bewerten Sie die KI-Nutzung, einschließlich Identität, Verhalten und Datenkontext.
- Unterscheiden Sie zwischen akzeptabler KI-Nutzung und nicht verwalteten, überprivilegierten oder riskanten Aktivitäten.
- Priorisieren Sie wesentliche Risiken, anstatt auf isolierte oder geringfügige Ereignisse zu reagieren.

Wandeln Sie KI-Richtlinien in Kontrollen um

Mit zunehmender Verbreitung von KI stoßen statische Richtlinien an ihre Grenzen. Die Durchsetzung muss kontinuierlich und durchsetzbar sein.

- Wenden Sie Sicherheitseinstellungen auf die gesamte KI-Nutzung an, nicht nur auf deren Definition in Richtlinien
- Erzwingen Sie Kontrollen an wichtigen Interaktionspunkten, um die KI-Nutzung und den Datenaustausch mit Richtlinien und Vorschriften in Einklang zu bringen
- Reduzieren Sie Schatten-KI, indem Sie Benutzern genehmigte Tools anbieten

Integrieren Sie KI in Security Operations

KI erweitert Ihre Angriffsfläche und birgt neue Risiken in Bezug auf Prompts, Daten und agentengesteuerte Aktionen, die eine aktive Verwaltung erfordern.

- Erkennen Sie Fehlgebrauch, Missbrauch und Kompromittierungen von KI-Systemen in Ihren Erkennungs- und Analyse-Workflows.
- Integrieren Sie KI-Aktivitäten in die umfassendere Sicherheitstelemetrie
- Wenden Sie dieselben Playbooks, Tools und Eskalationswege an, die für Standardbedrohungen verwendet werden

SOPHOS AI DEFENSE AUF EINEN BLICK

- Ermitteln Sie, wie KI in Ihrem Unternehmen und Ihren Tools und Workflows genutzt wird – einschließlich Schatten-KI
- Identifizieren Sie riskantes Verhalten anhand von Identität, Datenoffenlegung und Nutzungskontext
- Wenden Sie Sicherheitseinstellungen für Browser-, Endpoint- und Netzwerk-Interaktionspunkte an
- Verhindern Sie die Weitergabe sensibler Daten an KI-Tools, indem Sie Prompts, Uploads und KI-Interaktionen in Echtzeit überprüfen
- Integrieren Sie KI-Risiken in Ihre Security-Operations-Workflows

ZIELGRUPPE VON SOPHOS AI DEFENSE

- Security-Verantwortliche, die Transparenz und Kontrolle über die KI-Nutzung benötigen
- Security Operations Teams, die KI-bezogene Risiken erkennen und darauf reagieren müssen
- Unternehmen und Organisationen, die KI-Tools sicher einführen und bereitstellen möchten
- Unternehmen, die ihre bestehenden Sicherheitsinvestitionen auch für die Absicherung von KI-Risiken nutzen möchten

FOKUS AUF REALE KI-RISIKEN

Praxisorientierte KI-Sicherheit – entwickelt für die tatsächliche KI-Nutzung

Lösen Sie heutige KI-Risiken, nicht zukünftige hypothetische Szenarien.

Die meisten Lösungen sichern Modelle oder Anwendungen. Sophos AI Defense geht die tatsächlichen Risiken an, denen Sie heute ausgesetzt sind:

- Nicht verwaltete KI-Nutzung in der gesamten Organisation
- Eingeschränkte Transparenz über Tools, Agenten und Workflows
- Übertragung sensibler Daten über Prompts und automatisierte Workflows an externe KI-Tools

Erweitern Sie Ihre bestehenden Sicherheitsvorkehrungen.

Sophos AI Defense baut auf Ihren bestehenden Kontrollmechanismen auf und koordiniert diese, um sofortige, praktische Ergebnisse zu erzielen.

- Ergänzt Ihre bestehenden Investitionen in Sophos Workspace Protection, EDR, Firewall, XDR und MDR
- Führt Kontrollpunkte in einem einheitlichen KI-Richtlinien-Framework zusammen
- Bietet unmittelbaren Mehrwert – ohne zusätzliche Implementierung oder weitere Ressourcen

Wandeln Sie Transparenz in Ergebnisse um – nicht nur in mehr Daten.

Transparenz allein genügt nicht. Sophos AI Defense setzt Erkenntnisse in konkrete Maßnahmen um:

- Kombinieren Sie Transparenz, Kontext und Durchsetzung in einem System für KI-Nutzung, Datenbewegungen und Agentenaktivität
- Setzen Sie Richtlinien durch, priorisieren Sie Risiken und reagieren Sie im selben Workflow
- Erzielen Sie kontrollierte Ergebnisse – statt lediglich zusätzlicher Dashboards

ANALYSTENBEWERTUNGEN

Anerkannt von den wichtigsten Analysten und Organisationen.

GARTNER 2026

Leader,
Endpoint Protection

G2 SOMMER 2026

Die am besten bewertete XDR- und MDR-Lösung

MITRE ATT&CK EVALS

100 % Erkennungsrate

GARTNER PEER INSIGHTS

„Customers' Choice" für XDR und MDR

Ein System. Verschiedenste Kontrollpunkte. Eine zentrale Abwehr.

Sophos AI Defense ist Teil von Sophos Fusion, dem weltweit umfassendsten Cyber-Abwehrsystem. Es schützt vor KI-gestützten Bedrohungen, die sich schneller bewegen, als die Cyberabwehr reagieren kann.

sophos.de/ai-defense →

[1] Gartner, Schatten-KI erfordert strengere Endpoint Application Control, 25. Mai 2026. [2] CSA, „Das Problem der Schatten-KI-Agenten in Unternehmensumgebungen", 2025. [3] Komprise IT-Umfrage: AI, Data & Enterprise Risk. [4] IDC Info Snapshot, gesponsert von Microsoft, 1,3 Milliarden KI-Agenten bis 2028, #US53361825, Mai 2025.

Gartner Peer Insights geben die subjektiven Meinungen einzelner Enduser wieder, die auf deren eigenen Erfahrungen basieren. Sie sind in keinem Fall als Tatsachenfeststellung zu werten und repräsentieren nicht die Ansichten von Gartner oder seinen verbundenen Unternehmen. Gartner befürwortet in dieser Publikation keine bestimmten Hersteller, Produkte oder Dienstleistungen und übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seiner verbundenen Unternehmen in den USA und international; PEER INSIGHTS ist eine eingetragene Marke von Gartner, Inc. und/oder seiner verbundenen Unternehmen und werden hier mit Genehmigung verwendet. Alle Rechte vorbehalten. Gartner®, Peer Insights™, Voice of the Customer for Extended Detection and Response, Peer Contributors, 23. Mai 2025 Gartner®, Peer Insights™, Voice of the Customer for Managed Detection and Response, Peer Contributors, 31. März 2026.

2026-09-15 SB-DE (MC)

SOPHOS