SOPHOS

SOPHOS XDR + NEXT-GEN SIEM

Security Operations und Compliance für das agentische Zeitalter.

Stoppen Sie KI-gesteuerte Angriffe und vereinfachen Sie Compliance – ganz ohne zusätzliche Komplexität.

Da KI die Angriffsfläche vergrößert und Angriffe beschleunigt, haben fragmentierte Sicherheitslösungen Schwierigkeiten, mitzuhalten. Sophos XDR mit Next-Gen SIEM vereint Schutz, Erkennung, Analyse und Reaktion – und unterstützt Ihre regulatorischen Anforderungen in einem einheitlichen KI-basierten Cybersecurity-Abwehrsystem.

55 %
der Ransomware-Angriffe verwenden legitime Zugangsdaten oder nutzen Schwachstellen aus[1]

76 %
der Unternehmen/ Organisationen erleben aufgrund von Alerts ein Cybersecurity Burnout[2]

80 %
der CISOs bemängeln redundante Compliance-Maßnahmen aufgrund isolierter Workflows[3]

1,3 Bio.
prognostizierte KI-Agenten bis 2028, die Ihre Angriffsfläche vergrößern[4]

WAS SOPHOS BIETET

KI-Architektur. Intelligentere, beschleunigte Reaktion.

Ermöglichen Sie jedem Analysten, großflächig zu agieren.

KI-Tools und Automatisierung verkürzen die Einarbeitungszeit, verringern die Arbeitsbelastung und sorgen für eine effizientere Erkennung, Analyse und Reaktion – so können Analysten mehr leisten, schneller arbeiten und dabei voll auf ihre Fähigkeiten vertrauen

- KI-Assistenten beschleunigen Analysen und Threat Hunting
- Fallorientierte Workflows gruppieren, priorisieren und kontextualisieren zusammengehörige Aktivitäten automatisch
- Integrierte Automatisierungs-Playbooks beschleunigen Reaktionsmaßnahmen und beseitigen manuelle Aufgaben

Threat Intelligence, die sich ständig erweitert.

Sophos XDR wird mit jeder Bedrohung intelligenter und nutzt dabei weltweite Erkenntnisse aus der Praxis, um die Erkennung und Reaktion zu verbessern.

- Daten von mehr als 625.000 geschützten Unternehmen und Organisationen fließen in KI-Modelle und die Erkennungslogik ein
- Erkenntnisse aus jährlich über 380.000 MDR-Analysen
- Erkenntnisse werden automatisch in Echtzeit angewendet

Erkennen, analysieren, reagieren, speichern

Vermeiden Sie doppelten Aufwand. Sophos XDR mit Next-Gen SIEM bietet moderne Security Operations und langfristige Compliance – komplett vereint durch einzigartiges Design.

- Schutz-, Erkennungs-, Analyse-, Reaktions- und Audit-Workflows in einem System
- Speicherung von sicherheits- und complianceorientierten Telemetriedaten für bis zu 10 Jahre
- Planbare Kosten dank Lizenzierung auf Basis der Benutzer- und Server-Anzahl, nicht auf dem Datenvolumen

Nutzen Sie Ihren eigenen Stack oder unseren.

Von Grund auf anbieterunabhängig. Erfassen Sie alles – von Sicherheitssignalen bis hin zu complianceorientierten Telemetriedaten von Tools, die Sie bereits nutzen.

- Umfangreiche, KI-gestützte Integrationen liefern Telemetriedaten aus Sicherheits- und Compliance-Datenquellen
- Bidirektionale Integrationen ermöglichen Reaktionsmaßnahmen direkt in Ihren vorhandenen Tools
- Sophos Endpoint und das Sophos E-Mail Monitoring System (EMS) sind für besseren Schutz enthalten

AUF EINEN BLICK

- Vereinigen Sie Security Operations (Bedrohungsschutz, -erkennung, -analyse und -reaktion) und Compliance-Maßnahmen in einem zentralen System
- Beschleunigen Sie Analysen und Reaktionsmaßnahmen mit KI-Tools und -Assistenten
- Erkennen Sie mehrphasige Angriffe auf Endpoint-, Identity-, E-Mail-, Cloud- und Netzwerk-Ebene sowie in Produktivitätstools
- Automatisieren Sie die Bedrohungsreaktion mit integrierten SOAR Playbooks
- Bleiben Sie Bedrohungen immer einen Schritt voraus – mit integrierter Angreifer-Intelligence von Sophos X-Ops

ZIELGRUPPE

- Sicherheitsteams, die von der Alert-Flut und manuellen Analysen überfordert sind
- Unternehmen und Organisationen, die ihre Security Operations als Reaktion auf moderne KI-basierte Bedrohungen modernisieren möchten
- Unternehmen, die Threat Respone- und Compliance-Workflows vereinheitlichen möchten
- Compliance-Teams, die Audit-Anforderungen ohne die Komplexität und Kosten eines traditionellen SIEM erfüllen möchten
- MSPs und Reseller, die skalierbare Premium-Lösungen für SecOps anbieten

UPGRADE AUF SOPHOS MDR

Profitieren Sie von einem erstklassigen SOC, ohne selbst eines aufbauen zu müssen.

24/7 Fully Managed Threat Response.

Sophos XDR und Next-Gen SIEM können für von Experten geleitete Analysen und Reaktionsmaßnahmen nahtlos auf Sophos MDR upgegradet werden

Schneller durch KI. Entscheidungen durch menschliche Experten.

Sophos MDR ist das weltweit größte agentische SOC – KI analysiert und reagiert in Sekundenschnelle, Analysten tragen die Verantwortung für die Ergebnisse.

Expertise im globalen Maßstab.

Erweitern Sie Ihr internes Team um globale Sophos-Sicherheitsexperten, darunter Analysten, Threat Hunter, Forscher, Response-Experten und KI-Engineers.

ANALYSTENBEWERTUNGEN

Validiert von den wichtigsten Analysten und Organisationen.

GARTNER 2026
17 x Leader, Endpoint Protection

G2 SOMMER 2026
Nr. 1 bei XDR-Lösungen

MITRE ATT&CK EVALS
100 % Erkennungsrate

GARTNER PEER INSIGHTS
Eine „Customers' Choice“ für XDR

Ein System. Verschiedenste Kontrollpunkte. Eine zentrale Abwehr.

Sophos XDR mit Sophos Next-Gen SIEM 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.com/XDR →**

[1] Sophos Ransomware-Report 2026. [2] Sophos, Cybersecurity Burnout im Jahr 2025.. [3] CISO Society 2025 State of Continuous Controls Monitoring Report. [4] IDC Info Snapshot, 2025.

2026-07-27 SB-DE (AT)

SOPHOS