Lösungsbroschüre

Sophos Extended Detection and Response

Abwehr gegen aktive Angreifer mit KI-gestützter EDR und XDR

Angriffe schnell zu stoppen, ist entscheidend. Die offene, KI-native XDR-Plattform von Sophos bietet leistungsstarke Tools und Bedrohungsdaten, mit denen Sie verdächtige Aktivitäten in Ihrer gesamten IT-Umgebung erkennen, analysieren und proaktiv darauf reagieren können.

Branchenweit stärkster Schutz

Je mehr Bedrohungen im Vorfeld gestoppt werden, umso weniger Vorfälle müssen IT-Teams mit ihren oft begrenzten Ressourcen analysieren und beheben. Sophos kombiniert Extended Detection and Response mit dem branchenweit stärksten Endpoint-Schutz. Dieser blockiert Bedrohungen, bevor sie manuell analysiert werden müssen, und reduziert damit Ihre Arbeitslast.

Integrierte Endpoint Detection and Response (EDR)

Sophos XDR bietet umfassende EDR-Tools, einschließlich leistungsstarker, anpassbarer Suchfunktionen mit standardmäßigem Zugriff auf umfangreiche Endpoint- und Serverdaten der letzten 90 Tage sowie sicherem Remote-Zugriff auf Ihre Geräte. So können Sie Probleme beheben, Software installieren und deinstallieren, Prozesse beenden und vieles mehr.

Beschleunigen von Security Operations mit GenAI

Mit den weitreichenden generativen KI-Funktionen von Sophos XDR kann Ihr Team intelligente Entscheidungen treffen. So steigt das Vertrauen von Analysten und des Unternehmens in die Cybersicherheit. Der Sophos KI-Assistent führt Benutzer aller Kompetenzstufen durch jede Phase einer Bedrohungsanalyse und ermöglicht Ihnen, Angreifer schnell zu beseitigen.

Vollständige Transparenz über die Endpoint-Ebene hinaus

Je mehr Einblicke IT-Teams haben, desto schneller können sie reagieren. Ereignisse von Sophos- und Drittanbieter-Lösungen werden erfasst, gefiltert, korreliert und priorisiert. So haben Sie alle wichtigen Angriffsflächen im Blick und können aktive Angreifer schnell erkennen und stoppen. Sophos XDR ist mit Ihren vorhandenen Tools und Technologien kompatibel und bietet Integrationen mit Identity-, Netzwerk-, Firewall-, E-Mail-, Cloud-, Produktivitäts-, Backup- und Endpoint-Sicherheitslösungen.

Umfangreiche Sophos XDR-fähige Lösungen

Sophos-Technologien arbeiten nahtlos in der XDR-Plattform zusammen, um die bestmöglichen Sicherheitsergebnisse zu erzielen. Native Lösungsintegrationen umfassen Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email und Sophos Cloud Optix.

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten an allen wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette integrierter Lösungen
- Nutzung bereits vorhandener Tools und Investitionen mittels vielfältiger Integrationen von Drittanbieter-Technologien
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR

Mit maximaler Effizienz erkennen, analysieren und reagieren

Die Tools und Workflows von Sophos XDR unterstützen gezielt Sicherheitsanalysten und IT-Administratoren und sorgen für mehr Effizienz. Automatisch generierte Fälle ermöglichen Ihnen, das Ausmaß und die Ursache eines Vorfalls schnell zu erkennen und zu bestimmen, damit Sie so schnell wie möglich reagieren können.

KI-priorisierte Erkennungen für alle wichtigen Angriffsflächen

Erkennen Sie schnell und einfach verdächtige Aktivitäten, die sofortige Aufmerksamkeit erfordern. Sophos XDR priorisiert Erkennungen automatisch auf Grundlage des Risikos und liefert vollständigen Kontext.

Zuordnungen zum MITRE ATT&CK Framework

Erkennungen und Fälle werden automatisch MITRE ATT&CK-Taktiken zugeordnet, sodass Sie Lücken in Ihrer Abwehr leicht erkennen und Verbesserungen priorisieren können.

Beschleunigte Bedrohungssuche und -analyse

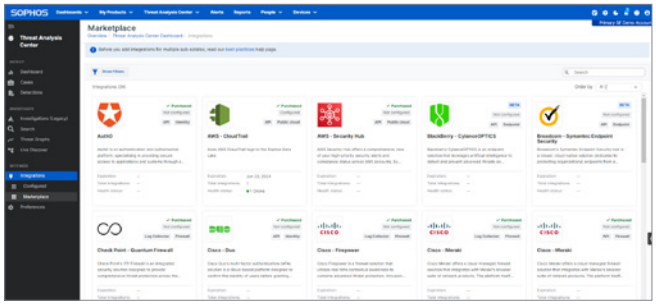
Mit leistungsstarken Suchfunktionen und vordefinierten Abfragevorlagen finden Sie benötigte Daten jetzt noch schneller – auch ohne SQL-Fachkenntnisse.

Automatisierte und beschleunigte Reaktionsmaßnahmen

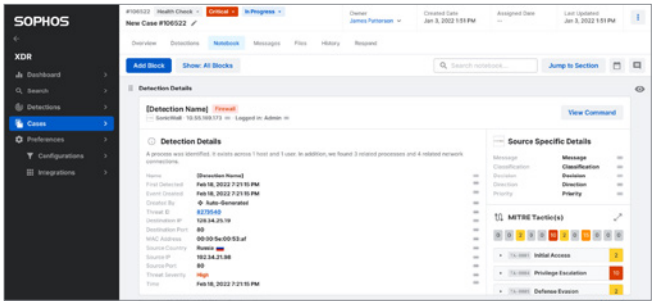
Mit automatisierten Aktionen wie Prozessbeendigung, Ransomware-Rollback und Netzwerk-Isolierung dämmen Sie Bedrohungen blitzschnell ein und sparen wertvolle Zeit.

Kollaboratives Fallmanagement

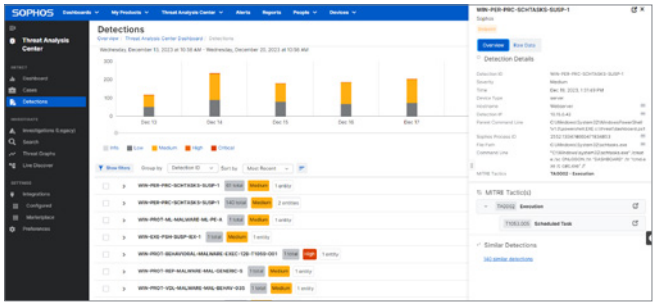
Die automatische Fallerstellung ermöglicht eine schnelle Analyse – mit umfassenden Fallmanagement-Tools zur Zusammenarbeit mit anderen Teammitgliedern.



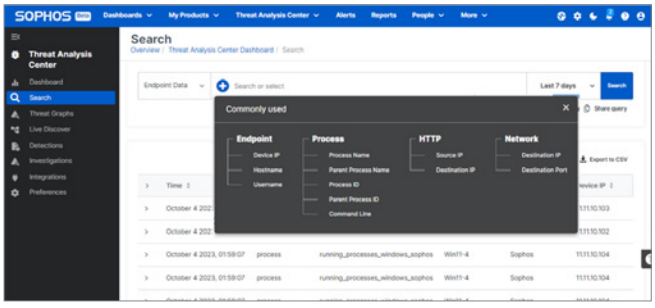
Kompatibel mit Sophos-Lösungen und Drittanbieter-Tools



Leistungsstarke Fallmanagement- und Collaboration-Tools



KI-priorisierte Erkennungen für alle wichtigen Angriffsflächen



Einfache und leistungsstarke Suche – keine SQL-Kenntnisse erforderlich

Beschleunigen von Security Operations mit GenAI

Mit den umfangreichen generativen KI-Funktionen von Sophos XDR kann Ihr Team intelligente Entscheidungen treffen. So steigt das Vertrauen von Analysten und des Unternehmens in die Cybersicherheit. Die GenAI-Funktionen werden optional angeboten, sodass Sie die volle Kontrolle über die KI-Implementierung erhalten.

KI-Assistent

Führt Benutzer aller Kompetenzstufen durch jede Phase einer Fallanalyse und maximiert die Effizienz, um Bedrohungen schnell zu stoppen.

KI-Suche

Beschleunigt tägliche Aufgaben durch Suchen in natürlicher Sprache und senkt die technologischen Hürden für Security Operations.

KI-Fallzusammenfassung

Bietet einen leicht verständlichen Überblick über alle Erkennungen und empfohlene nächste Schritte, sodass Analysten schnell intelligente Entscheidungen treffen können.

KI-Befehlsanalyse

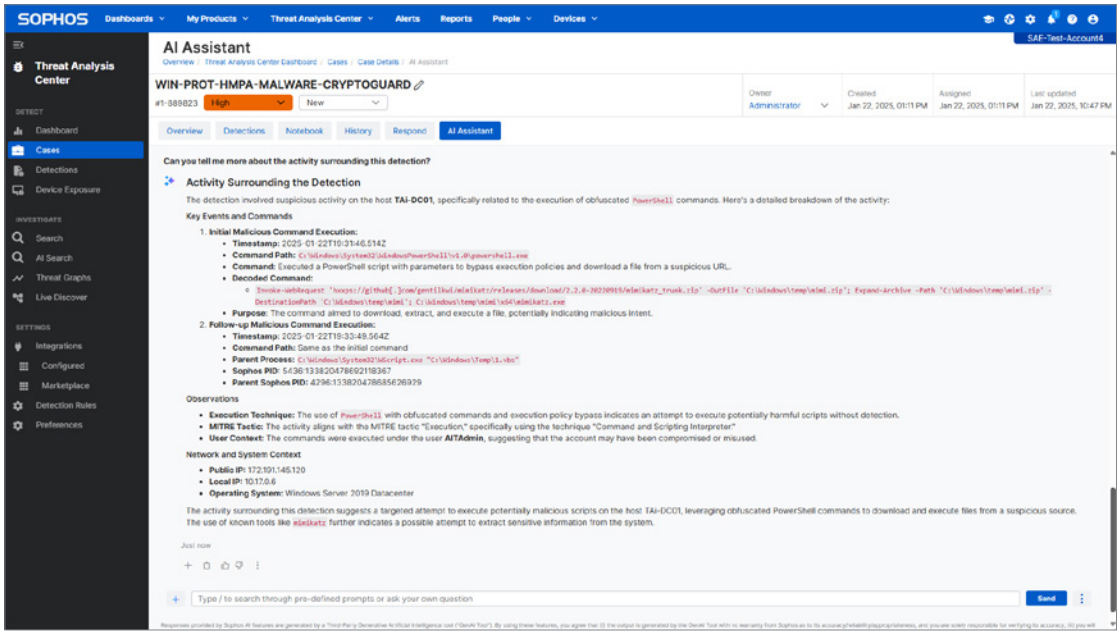
Analysiert komplexe Befehlszeilenargumente, um deren Bedeutung und Auswirkungen zu ermitteln – mit Erklärungen in einfacher Sprache.

Sophos KI-Assistent

Mit dem Sophos KI-Assistenten können alle Benutzer – von IT-Generalisten bis hin zu Tier-3-SOC-Analysten – die Informationen abrufen, die sie benötigen, um Bedrohungsanalysen durchzuführen und Angreifer schnell zu beseitigen.

- **Führen Sie eine breite Palette von SecOps-Aufgaben durch:** Analysieren Sie verdächtige Befehle, listen Sie Kompromittierungs-Indikatoren auf, ergänzen Sie Daten mit Bedrohungsinformationen, erstellen Sie detaillierte Reports und vieles mehr.
- **Stellen Sie Fragen in Alltagssprache** oder verwenden Sie vordefinierte Prompts von Sophos-Bedrohungsexperten. Erhalten Sie übersichtliche Zusammenfassungen und empfohlene nächste Schritte.
- **Entwickelt in Zusammenarbeit mit den Sicherheitsanalysten von Sophos:** Profitieren Sie von praxiserprobten Workflows und der Erfahrung von Sophos MDR-Experten.
- **Kontinuierliche Aktualisierung basierend auf der Bedrohungslandschaft:** Stellt den Zugriff auf die neuesten Analysetechniken und Bedrohungsinformationen von Sophos X-Ops sicher.

Der Sophos KI-Assistent ist kein gewöhnliches KI-Tool – in diesen intelligenten Assistenten ist die gesamte Expertise unseres weltweit führenden Managed Detection and Response Service eingeflossen.



In Sophos XDR enthaltene Integrationen

Sicherheitsdaten aus den folgenden Quellen können ohne Aufpreis in die Sophos XDR-Plattform integriert werden. Telemetriequellen werden verwendet, um die Transparenz in Ihrer Umgebung zu erhöhen, neue Bedrohungserkennungen zu generieren, die Genauigkeit vorhandener Bedrohungserkennungen zu verbessern, Threat Hunts durchzuführen und zusätzliche Reaktionsmaßnahmen zu ermöglichen.

Sophos Endpoint

Blockieren Sie komplexe Bedrohungen und erkennen Sie schädliche Verhaltensweisen auf Ihren Endpoints.

Produkt im Preis von Sophos XDR enthalten

Workload Protection

Modernster Schutz und Bedrohungserkennung für Windows- und Linux-Server und -Container.

Produkt im Preis von Sophos XDR enthalten

Sophos Mobile

Schützen Sie Ihre iOS- und Android-Geräte und -Daten vor den neuesten Bedrohungen.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos Firewall

Überwachen und filtern Sie ein- und ausgehenden Netzwerkverkehr, um komplexe Bedrohungen zu stoppen, bevor sie Schaden anrichten können.

Produkt separat erhältlich; Xstream Protection Subscription erforderlich; ohne Aufpreis enthalten

Sophos Email

Schützen Sie Ihren Posteingang mit modernster KI vor Malware. Diese verhindert Phishing-Angriffe sowie gezielte Angriffe, bei denen eine falsche Identität vorgetäuscht wird.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos Cloud Optix

Verhindern Sie Cloud-Sicherheitsverstöße und gewinnen Sie Einblick in Ihre kritischen Cloud Services, einschließlich AWS, Azure und GCP.

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos ZTNA

Ersetzen Sie Remote Access VPN durch „Least Privilege"-Zugriff, um Ihre Benutzer sicher mit Ihren Netzwerk-Anwendungen zu verbinden.

Produkt separat erhältlich; Integration ohne Aufpreis

Endpoint-Schutz anderer Anbieter

Integrationen umfassen:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Kompatibel mit anderen Endpoint-Protection-Lösungen mit dem Sophos „XDR Sensor"-Agent

Microsoft Security Tools

- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

90 Tage Datenspeicherung

Speichert Erkennungsdaten standardmäßig 90 Tage im Sophos Data Lake.

Microsoft Office 365 Management Activity

Liefern Informationen über Benutzer-, Admin-, System- und Richtlinienaktionen und -ereignisse, die über die Office 365-Verwaltungsaktivitäts-API erfasst werden.

Google Workspace

Erfasst Sicherheitstelemetrien von der Google Workspace Alert Center API.

Add-On-Integrationen

Sicherheitsdaten aus den folgenden Quellen können durch Zukauf von Integration Packs in die Sophos XDR-Plattform integriert werden. Telemetriequellen werden verwendet, um die Transparenz in Ihrer Umgebung zu erhöhen, neue Bedrohungserkennungen zu generieren, die Genauigkeit vorhandener Bedrohungserkennungen zu verbessern, Threat Hunts durchzuführen und zusätzliche Reaktionsmaßnahmen zu ermöglichen.

Sophos NDR

Überwachen Sie kontinuierlich die Aktivitäten in Ihrem Netzwerk und erkennen Sie verdächtige Aktionen zwischen Geräten, die sonst unbemerkt ablaufen.

Per SPAN Port Mirroring mit jedem Netzwerk kompatibel

Firewall

Integrationen umfassen:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

Netzwerk

Integrationen umfassen:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Identity

Integrationen umfassen:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft-Integration ohne Aufpreis inbegriffen

E-Mail

Integrationen umfassen:

- Mimecast
- Proofpoint
- Trend Micro

Microsoft-365- und Google Workspace-Integrationen sind ohne Aufpreis enthalten

Cloud

Integrationen umfassen:

- Orca Security

AWS-, Azure- und GCP-Integrationen sind über das separat erhältliche Produkt „Cloud Optix" verfügbar.

Sicherung und Wiederherstellung

Integrationen umfassen:

- Acronis
- Rubrik
- Veeam

1 Jahr Datenspeicherung

Erkennungsdaten werden 1 Jahr lang im Sophos Data Lake gespeichert

Weltweit einzigartige Endpoint Protection

Erleichtern Sie Ihre Analysearbeit, indem Sie Sicherheitsverstöße schon im Vorfeld verhindern. Bei den meisten XDR-Produkten müssen IT-Teams wertvolle Zeit mit der Analyse von Vorfällen verbringen, die ihre Schutzlösung eigentlich blockieren sollte. Sophos kombiniert XDR mit dem branchenweit stärksten Endpoint-Schutz. Dieser blockiert Bedrohungen, bevor sie manuell analysiert werden müssen, und reduziert damit Ihre Arbeitslast.

Sophos XDR Subscriptions umfassen Sophos Endpoint, das modernsten Schutz vor Ransomware und Exploits sowie KI-gestützten Malware-Schutz bietet. Mit adaptiven Abwehrmechanismen wird dabei der Schutz als Reaktion auf einen akuten Angriff dynamisch erhöht.

Weitere Informationen finden Sie unter: sophos.de/endpoint

Erhalten Sie Detection and Response als Fully-Managed-Service

Erkennen und analysieren Sie selbst mit Sophos XDR Bedrohungen oder nehmen Sie unseren umfassenden 24/7 Managed Service in Anspruch. Mit Sophos Managed Detection and Response (MDR) kann unser Expertenteam Ihnen ein sofort einsatzbereites Security Operations Center zur Seite stellen, das bei Vorfällen auch umfassende Reaktionsmaßnahmen für Sie ergreift.

Weitere Informationen finden Sie unter: sophos.de/mdr

In Sophos XDR Subscriptions enthalten

	Sophos XDR
KI-generierte Bedrohungs-Scores und priorisierte Erkennungen	✓
Fallmanagement, Collaboration und Reaktionsmaßnahmen	✓
Einfache und leistungsstarke Suchfunktionen für Threat Hunts und Analysen	✓
GenAI-basierte XDR-Funktionen (optional): KI-Assistent, KI-Fallzusammenfassung, KI-Befehlsanalyse, KI-Suche	✓
Sophos Endpoint- und Workload-Protection-Lösungen	✓
Endpoint Detection and Response (EDR) Tools	✓
Erkennungsdaten werden im Sophos Data Lake gespeichert (standardmäßig 90 Tage)	✓
Umfangreiche Endpoint- und Serverdaten auf dem Gerät	✓
Integrationen mit Sophos-Lösungen: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud Optix	✓
Sophos Network Detection and Response (NDR)	Optionales Add-on
Integrationen mit Endpoint-Protection-Lösungen anderer Anbieter	✓
Integrationen mit Microsoft-Lösungen	✓
Integration in die Produktivitätslösung „Google Workspace“	✓
Integrationen mit Firewall-, Netzwerk-, E-Mail-, Cloud-, Identity-, Backup- und Recovery-Lösungen anderer Anbieter	Optionale Add-ons

Darum entscheiden sich Kunden für Sophos XDR

Sophos ist ein etablierter Marktführer im Bereich Extended Detection and Response und erhält regelmäßig unabhängige Auszeichnungen, die dies untermauern.

Gartner

Sophos ist 2024 zum 15. Mal in Folge im Gartner® Magic Quadrant™ for Endpoint Protection Platforms ein „Leader“

Gartner Peer Insights Customers' Choice 2024

Sophos platziert als Gartner® Peer Insights™ Customers' Choice 2024 für Endpoint Protection Plattformen und Netzwerk-Firewalls

G2 Leader

Sophos ist ein Leader für Endpoint Protection, EDR, XDR, Firewall und MDR in den Winter-Reports 2025 von G2 Grid®

MITRE | ATT&CK® Evaluations

Sophos hat bei den MITRE ATT&CK Evaluations: Enterprise für EDR/XDR-Lösungen 2024 herausragende Ergebnisse erzielt

SE Labs

Sophos erzielt in unabhängigen Sicherheitstests von SE Labs durchweg branchenführende Schutzergebnisse

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter sophos.de/xdr

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2025-02-10 DS-DE (PS)

SOPHOS