Sophos Extended Detection and Response (XDR)

Schutz vor komplexen mehrstufigen Multi-Vektor-Angriffen

Angriffe schnell zu stoppen, ist entscheidend. Mit den leistungsstarken Tools und der Threat Intelligence von Sophos XDR erkennen, analysieren und bekämpfen Sie verdächtige Aktivitäten in Ihrem gesamten IT-Ökosystem – bereitgestellt über die adaptive, KI-native, offene Plattform von Sophos.

Legitime Zugangsdaten und unbekannte Schwachstellen werden in 55 % der Ransomware-Angriffe ausgenutzt, um sich Zugriff zu verschaffen.[1]

Die durchschnittliche Verweildauer von Angreifern bei Fällen, die vom Sophos Incident Response-Team untersucht wurden, beträgt insgesamt 7 Tage.[2]

Unterschiedliche Tools verursachen Datensilos und manuellen Aufwand. 76 % der Unternehmen/Organisationen erlebten im letzten Jahr ein Cybersecurity Burnout.[3]

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.

Überblick über alle Angriffsflächen

Je mehr Einblicke IT-Teams haben, desto schneller können sie reagieren. Unsere offene, erweiterbare Architektur bietet durch Integration von Bedrohungsdaten bereits vorhandener Lösungen in eine zentrale Detection and Response-Plattform Einblick in Ihre gesamte IT-Umgebung. Sophos XDR umfasst Integrationen mit einer umfangreichen Palette von Tools und Technologien.

Beschleunigen von Security Operations mit GenAI

Maximieren Sie die Effizienz von Analysten und beschleunigen Sie die Analyse und Reaktion. Die in Sophos XDR enthaltenen KI-basierten Tools optimieren Analysen, indem sie Echtzeit-Einblicke bieten, Bedrohungsdaten kontextualisieren und klare Empfehlungen geben.

Offene, auf Optimierung und Zentralisierung ausgelegte Plattform

Erhalten Sie eine zentrale Ansicht Ihres IT-Ökosystems und konzentrieren Sie sich bei Ihrer Analyse auf Elemente mit hoher Priorität statt auf irrelevante Warnmeldungen. Erkennen Sie schwerwiegende Bedrohungen mit KI-gestützter Priorisierung und Analytik und ermöglichen Sie mit robusten Analyse-Workflows und Fallmanagement-Tools eine effektive Teamarbeit.

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.

Lösung

Security & Identity

Produkt

XDR

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten und evasive Bedrohungen für alle wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette verfügbarer Integrationen
- Steigern des ROI von bereits getätigten Technologie-Investitionen
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR

1 Sophos Ransomware-Report 2025
2 Sophos Active Adversary Report 2025
3 Sophos Report – Cybersecurity Burnout im Jahr 2025

BERGT • working it-services • Kantstr. 53 • 14612 Falkensee

Sophos Extended Detection and Response (XDR)

Schnellere Reaktion durch intelligente XDR-Automatisierung

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

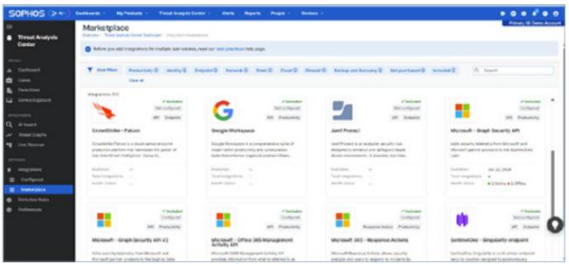
Zuordnungen zum MITRE ATT&CK Framework
Erkennungen und Fälle werden automatisch MITRE ATT&CK-Taktiken zugeordnet, sodass Sie Lücken in Ihrer Abwehr leicht erkennen und Verbesserungen priorisieren können.

Beschleunigte Bedrohungssuche und -analyse
Mit einfachen KI-Suchoptionen in natürlicher Sprache und vordefinierten Abfragevorlagen finden Sie für Analysen benötigte Informationen auch ohne SQL-Fachkenntnisse.

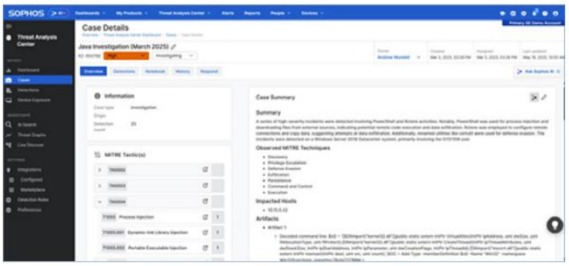
Automatisierte Reaktionsmaßnahmen
Mit automatisierten Aktionen wie Prozessbeendigung, Ransomware-Rollback, Netzwerk-Isolierung und adaptivem Angriffsschutz dämmen Sie Bedrohungen blitzschnell ein und sparen wertvolle Zeit.

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

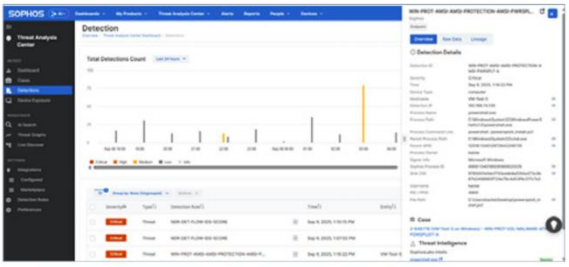
Reaktionsmaßnahmen für Analysten
Ergreifen Sie eine Vielzahl von Reaktionsmaßnahmen, um Bedrohungen schnell einzudämmen und zu beseitigen, auch in Microsoft 365-Umgebungen.



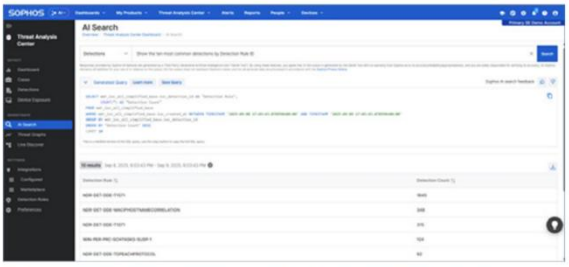
Umfasst Integrationen mit Lösungen von Sophos und anderen Anbietern.



Leistungsstarke Fallmanagement- und Collaboration-Tools.



KI-priorisierte Erkennungen für alle wichtigen Angriffsflächen.



KI-Suche in natürlicher Sprache – keine SQL-Kenntnisse erforderlich.

Lösung

Security & Identity

Produkt

XDR

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten und evasive Bedrohungen für alle wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette verfügbarer Integrationen
- Steigern des ROI von bereits getätigten Technologie-Investitionen
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR

Sophos Extended Detection and Response (XDR)

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. GenAI-Funktionen sind standardmäßig in Sophos XDR enthalten.

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 natürliche 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

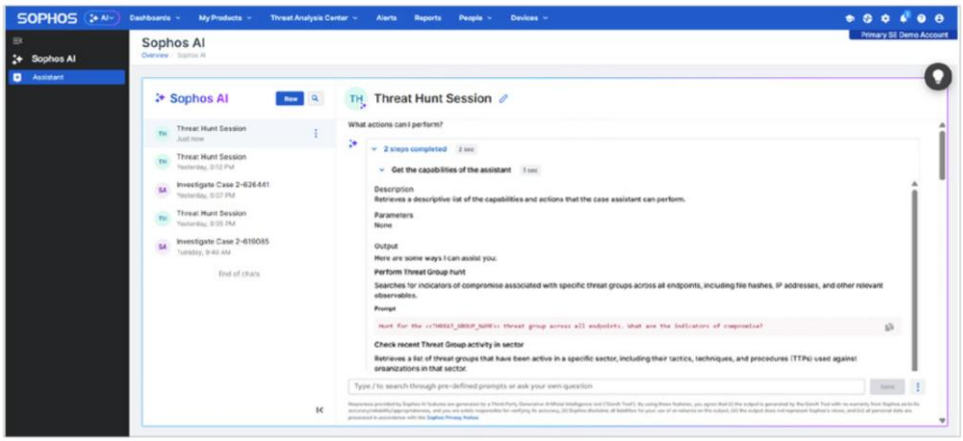
Mit dem Sophos KI-Assistenten können alle Benutzer – von IT-Generalisten bis hin zu Tier-3-SOC-Analysten – die Informationen abrufen, die sie benötigen, um Bedrohungsanalysen durchzuführen und Angreifer schnell zu beseitigen.

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.

Entwickelt in Zusammenarbeit mit den Sicherheitsanalysten von Sophos
Profitieren Sie von praxiserprobten Workflows und der Erfahrung von Sophos MDR-Experten.

Stellen Sie Fragen in Alltagssprache oder verwenden Sie vordefinierte Prompts von Sophos-Bedrohungsexperten. Erhalten Sie übersichtliche Zusammenfassungen und empfohlene nächste Schritte.

Kontinuierliche Aktualisierung basierend auf der Bedrohungslandschaft
Stellt den Zugriff auf die neuesten Analysetechniken und Bedrohungsinformationen von Sophos X-Ops sicher.



Lösung

Security & Identity

Produkt

XDR

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten und evasive Bedrohungen für alle wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette verfügbarer Integrationen
- Steigern des ROI von bereits getätigten Technologie-Investitionen
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR

BERGT • working it-services • Kantstr. 53 • 14612 Falkensee

Sophos Extended Detection and Response (XDR)

Sophos „XDR-fähige" Produktintegrationen

Sophos-Lösungen arbeiten nahtlos zusammen, um die bestmöglichen Sicherheitsergebnisse zu erzielen. Die breite Palette preisgekrönter Produkte, darunter Endpoint, Firewall, NDR, ZTNA, E-Mail, Cloud und Mobile, ist vollständig in die XDR-Plattform integriert – und der erstklassige Schutz von Sophos Endpoint ist standardmäßig enthalten.

Sophos Endpoint

Blockieren Sie komplexe Bedrohungen auf Ihren Endpoints und Servern, einschließlich raffinierter Ransomware-Angriffe.

In Sophos XDR enthalten

Sophos EDR

Erkennen, analysieren und bekämpfen Sie verdächtige Aktivitäten und evasive Bedrohungen, die Ihre Endpoints ins Visier nehmen.

In Sophos XDR enthalten

Sophos ITDR

Überwachen Sie Ihre Umgebung auf Identitätsrisiken und erhalten Sie Informationen aus dem Darknet zu kompromittierten Zugangsdaten.

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 NDR

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

Produkt separat erhältlich; Integration ohne Aufpreis. Per SPAN Port Mirroring mit jedem Netzwerk kompatibel

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

Sophos Mobile

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

Produkt separat erhältlich; Integration ohne Aufpreis

Sophos E-Mail

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

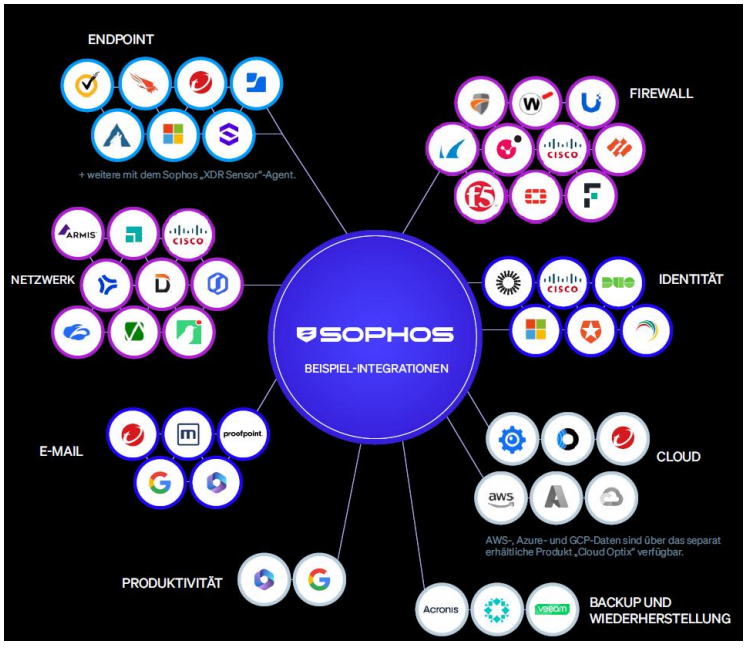
Sophos Cloud Optix

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

Produkt separat erhältlich; Integration ohne Aufpreis

Schöpfen Sie das Potenzial bereits getätigter Technolgie-Investitionen optimal aus

Steigern Sie den ROI Ihrer derzeitigen Sicherheitstools, indem Sie diese in unsere offene Plattform einbinden. Sophos XDR umfasst schlüsselfertige Integrationen mit einem umfangreichen Ökosystem von Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identity-, Backup-, Cloud-Security- und Produktivitätstools anderer Anbieter, einschließlich Microsoft 365.



SOPHOS

Lösung

Security & Identity

Produkt

XDR

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten und evasive Bedrohungen für alle wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette verfügbarer Integrationen
- Steigern des ROI von bereits getätigten Technologie-Investitionen
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR

Sophos Extended Detection and Response (XDR)

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.

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, dass bei Vorfällen auch umfassende Reaktionsmaßnahmen für Sie ergreift.

In Sophos XDR Subscriptions enthalten

	Sophos XDR
KI-generierte Bedrohungs-Scores und priorisierte Erkennungen	✓
Fallmanagement, Collaboration und Reaktionsmaßnahmen	✓
Leistungsstarke Suchfunktionen in natürlicher Sprache für Threat Hunts und Analysen	✓
GenAI-basierte XDR-Funktionen:	✓
KI-Assistent, KI-Fallzusammenfassung, KI-Befehlsanalyse, KI-Suche	✓
Sophos Endpoint inklusive (oder nutzen Sie Ihre bestehende Endpoint-Lösung eines anderen Anbieters)	✓
Erkennungsdaten werden im Sophos Data Lake gespeichert (standardmäßig 90 Tage)	✓
1 Jahr Datenspeicherung erhältlich	Optionales Add-On
Native Integrationen mit Sophos-Lösungen: Sophos Endpoint, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud Optix	✓
Integrationen mit Endpoint-, Firewall-, Netzwerk-, E-Mail-, Cloud-, Identity-, Backup-, Microsoft 365- und Google Workspace-Lösungen anderer Anbieter.	✓
Sophos Network Detection and Response (NDR)	Optionales Add-On
Sophos Identity Threat Detection and Response (ITDR)	Optionales Add-On

Lösung

Security & Identity

Produkt

XDR

Vorteile auf einen Blick

- Einblick in verdächtige Aktivitäten und evasive Bedrohungen für alle wichtigen Angriffsflächen
- Offene XDR-Plattform mit einer breiten Palette verfügbarer Integrationen
- Steigern des ROI von bereits getätigten Technologie-Investitionen
- Schnelle Analyse und Bekämpfung von Bedrohungen mit priorisierten Erkennungen und KI-gestützten Tools
- Branchenführende Endpoint Protection und EDR