Lösungsbroschüre

Sophos Extended Detection and Response

Effektive Abwehr aktiver Angreifer mit umfassender EDR und XDR

Angriffe schnell zu stoppen, ist entscheidend. Sophos XDR 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 Zugriff auf Endpoint- und Serverdaten der letzten 90 Tage sowie sicherem Remote-Zugriff auf Geräte. So können Sie Probleme beheben, Software installieren/deinstallieren, Prozesse beenden und vieles mehr.

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.

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.

Kompatibel mit Ihren vorhandenen Tools und Technologien

Telemetriedaten von unterschiedlichen Sicherheits-Tools anderer Anbieter (d. h. nicht von Sophos) können problemlos genutzt werden. So steigern Sie den ROI Ihrer Cybersecurity-Investitionen und beschleunigen gleichzeitig Ihre Sicherheitsprozesse. Integrationen umfassen unter anderem Identity-, Netzwerk-, Firewall-, E-Mail-, Cloud-, Produktivitäts- und Endpoint-Security-Lösungen.

Vorteile auf einen Blick

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

Beschleunigte Erkennung, Analyse und Reaktion

Die Tools und Funktionen von Sophos XDR unterstützen gezielt Sicherheitsanalysten und IT-Administratoren und sorgen für maximale Effizienz. KI-gesteuerte Analysen 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

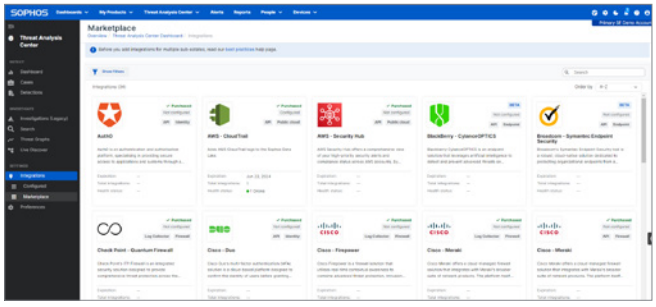
Mit leistungsstarken Suchfunktionen und vordefinierten Abfragevorlagen finden Sie benötigte Daten jetzt noch schneller – auch ohne SQL-Fachkenntnisse.

Automatisierte und beschleunigte Reaktionsmaßnahmen

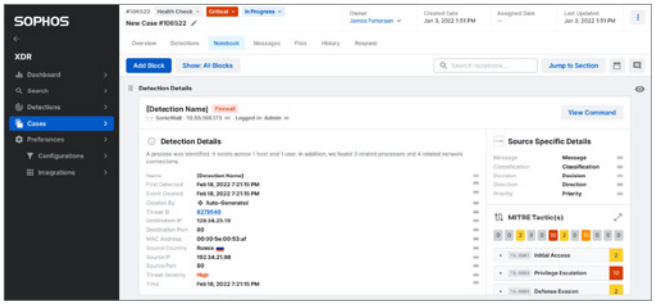
Mit automatisierten Aktionen wie Prozessbeendigung, Ransomware-Rollback und Netzwerk-Isolierung dämmen Sie Bedrohungen blitzschnell ein und sparen wertvolle Zeit.

Kollaboratives Fallmanagement

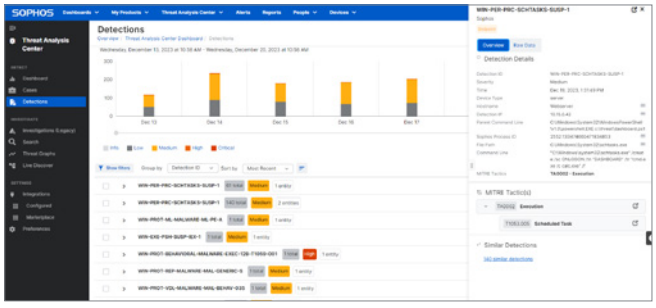
Die automatische Fallerstellung ermöglicht eine schnelle Analyse – mit umfassenden Fallmanagement-Tools zur Zusammenarbeit mit anderen Teammitgliedern.



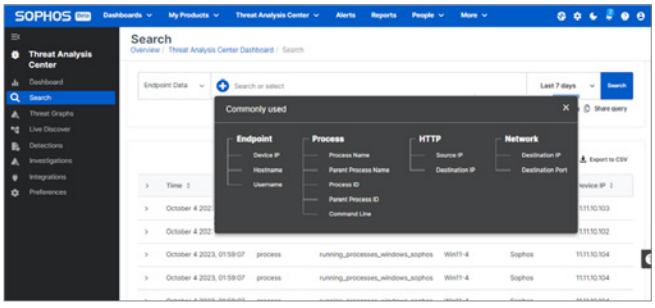
Kompatibel mit Sophos-Lösungen und Drittanbieter-Tools



Leistungsstarke Fallmanagement- und Collaboration-Tools



KI-priorisierte Erkennungen für alle wichtigen Angriffsflächen



Einfache und leistungsstarke Suche – keine SQL-Kenntnisse erforderlich

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; ohne Aufpreis integriert

Sophos Firewall

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

Produkt separat erhältlich; ohne Aufpreis integriert

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; ohne Aufpreis integriert

Sophos Cloud

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

Produkt separat erhältlich; ohne Aufpreis integriert

Sophos ZTNA

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

Produkt separat erhältlich; ohne Aufpreis integriert

Endpoint-Schutz von Drittanbietern

Kompatibel mit:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ kompatibel mit anderen Lösungen mit dem Sophos „XDR Sensor"-Agent

Microsoft Security Tools

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

90 Tage Datenspeicherung

Speichert Daten von Sophos-Produkten und Drittanbieter-Lösungen (nicht Sophos) im Sophos Data Lake.

Mit optionalem Add-on auf 1 Jahr erweiterbar

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

Kompatibel mit:

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

Netzwerk

Kompatibel mit:

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

Identity

Kompatibel mit:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Microsoft-Integration ohne Aufpreis inbegriffen

E-Mail

Kompatibel mit:

- Proofpoint
- Mimecast

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

Cloud

Kompatibel mit:

- Orca Security

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

Sicherung und Wiederherstellung

Kompatibel mit:

- Acronis
- Veeam

1 Jahr Datenspeicherung

Speichert Daten von Sophos-Produkten und Drittanbieter-Lösungen (nicht Sophos) im Sophos Data Lake.

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 Intercept X Endpoint, das modernsten Schutz vor Ransomware und Exploits sowie KI-gestützten Malware-Schutz bietet. Mit kontextsensitiven Abwehrmechanismen wird dabei der Schutz dynamisch angepasst.

Weitere Informationen finden Sie unter: sophos.de/endpoint

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-priorisierte Erkennungen und gesteuerte Analysen	✓
Fallmanagement, Collaboration und Reaktionsmaßnahmen	✓
Einfache und leistungsstarke Suchfunktionen für Threat Hunts und Analysen	✓
Sophos Endpoint- und Workload-Protection-Lösungen (Intercept X Advanced)	✓
Endpoint Detection and Response (EDR) Tools	✓
Speicherung von Cloud-Daten	90 Tage (auf bis zu 1 Jahr verlängerbar)
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	✓
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 wurde 2023 zum 14. Mal in Folge im Gartner® Magic Quadrant™ for Endpoint Protection Platforms als Leader eingestuft.

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 Sommer-Reports 2024 von G2 Grid®

OMDIA

Sophos war 2023 der am besten bewertete und einzige Leader im Omdia Universe for Comprehensive XDR

MITRE ENGENUITY | ATT&CK® Evaluations

Ein „Strong Performer" bei den MITRE Engenuity ATT&CK Evaluations für Managed Services

SE Labs

Sophos erzielt in unabhängigen Tests 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

2024-07-18 DS-EN (PS)

SOPHOS