Lösungsbroschüre

Sophos Endpoint

Powered by Intercept X

Die branchenweit führende KI-gestützte Endpoint-Security-Lösung

Unsere auf der Technologie von Intercept X basierende Lösung bietet einzigartigen Schutz und verhindert komplexe Angriffe, bevor sie Ihre Systeme beeinträchtigen. Leistungsstarke EDR- und XDR-Tools (Endpoint/Extended Detection and Response) ermöglichen eine gezielte Suche und Analyse verdächtiger Aktivitäten und Angriffsindikatoren, damit Sie schnellstmöglich reagieren können.

Präventive Cybersecurity

Sophos Endpoint nutzt ein umfassendes Sicherheitskonzept, das auf präventiver Cybersecurity gründet, und verlässt sich nicht auf eine einzelne Sicherheitstechnologie. Mehrere Deep-Learning-KI-Modelle schützen vor bekannten und neuen Angriffen. Web, Anwendungs- und Peripherie-Kontrollen reduzieren Ihre Angriffsfläche und blockieren gängige Angriffsvektoren. Verhaltensanalysen, Anti-Ransomware, Anti-Exploit-Verfahren und weitere hochmoderne Technologien stoppen Bedrohungen schnell, bevor sie eskalieren, sodass IT-Teams mit begrenzten Ressourcen weniger Vorfälle analysieren und beheben müssen.

Lückenloser Ransomware-Schutz

Sophos Endpoint bietet die branchenweit zuverlässigste Zero-Touch-Endpoint-Abwehr gegen komplexe Ransomware. Die CryptoGuard-Technologie stoppt schädliche Verschlüsselungen in Echtzeit und setzt betroffene Dateien automatisch in ihren Ursprungszustand zurück, wodurch Auswirkungen auf den Geschäftsbetrieb minimiert werden.

Adaptive Abwehr

Branchenweit einmalige dynamische Abwehrmechanismen passen sich als Reaktion auf aktive Angreifer und manuell gesteuerte Angriffe an. Dadurch sind die Angreifer nicht mehr in der Lage, ihren Angriff auszuführen. Der Angriff wird unterbrochen und eingedämmt, und Sie gewinnen wertvolle zusätzliche Zeit, um Reaktionsmaßnahmen zu ergreifen.

Einfache Einrichtung und Verwaltung

Sophos Central ist eine leistungsstarke, cloudbasierte Cybersecurity-Management-Plattform für alle Sophos-Next-Gen-Sicherheitslösungen. Empfohlene Technologien und Funktionen sind standardmäßig aktiviert. So verfügen Sie sofort über den stärksten Schutz, ohne eine Feinabstimmung vornehmen zu müssen.

Bewährter Branchenführer im Bereich Endpoint Security

Sophos Endpoint erhält kontinuierlich Bestnoten von Kunden, Analysten und unabhängigen Testinstituten. Sophos ist zum 15. Mal ein „Leader" im Gartner® Magic Quadrant™ for Endpoint Protection Platforms und die beste Endpoint Protection Suite in den Winter-Reports 2025 von G2 Grid®.

Vorteile auf einen Blick

- Schutz vor bekannten und neuen Angriffen durch mehrere Deep-Learning-KI-Modelle
- Reduzieren der Angriffsfläche und Blockieren gängiger Angriffsvektoren mit Web-, Anwendungs- und Peripherie-Kontrollen
- Schnelles Stoppen von Bedrohungen, bevor sie eskalieren – mit Verhaltens-analysen, Anti-Ransomware, Anti-Exploit und weiteren modernen Technologien
- Sichere Daten dank erstklassigem Schutz vor lokalen und Remote-Ransomware-Angriffen
- Branchenweit einmalige dynamische Abwehr-mechanismen, die sich als Reaktion auf aktive Angreifer und manuell gesteuerte Angriffe automatisch anpassen
- Suche, Analyse und Stoppen verdächtiger Aktivitäten mit leistungsstarken EDR- und XDR-Tools

Präventive Cybersecurity reduziert die Angriffsfläche

Angriffe frühzeitig zu stoppen, ist weniger ressourcenintensiv als sie zu einem späteren Zeitpunkt in der Angriffskette zu überwachen und die Schäden zu beheben. Sophos Endpoint umfasst hochmoderne Schutztechnologien, die eine Vielzahl von Angriffen abwehren. Web-, Anwendungs- und Peripheriekontrollen reduzieren Ihre Angriffsfläche und blockieren gängige Angriffsvektoren. So haben Angreifer keine Chance, in Ihre Umgebung vorzudringen.

Web Protection

Blockiert ausgehenden Browser-Datenverkehr zu schädlichen Websites, stoppt Bedrohungen in der Bereitstellungsphase und blockt Phishing- und Malware-Websites.

Web Control

Blockiert den Zugriff auf unerwünschte und unangemessene Inhalte. Sorgt für eine richtlinienkonforme Internetnutzung in Ihrer Umgebung und schützt vor Datenverlusten.

Download Reputation

Analysiert heruntergeladene Dateien hinsichtlich Verbreitung, Alter und Quelle und bewertet ihre Reputation mithilfe der globalen Threat Intelligence aus den SophosLabs. Benutzer werden aufgefordert, Dateien mit geringer oder unbekannter Reputation zu blockieren.

Application Control

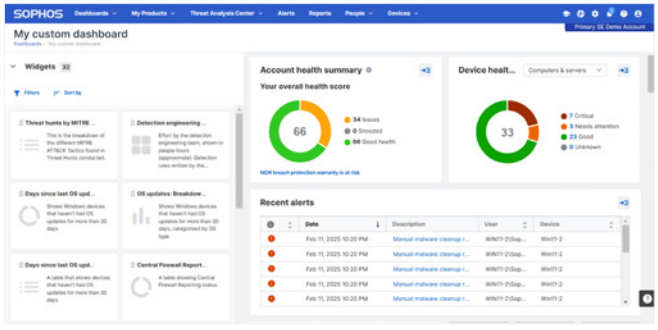
Blockiert anfällige oder ungeeignete Anwendungen mit vordefinierten Kategorien, sodass Apps nicht einzeln per Hash blockiert werden müssen.

Peripheral (Device) Control

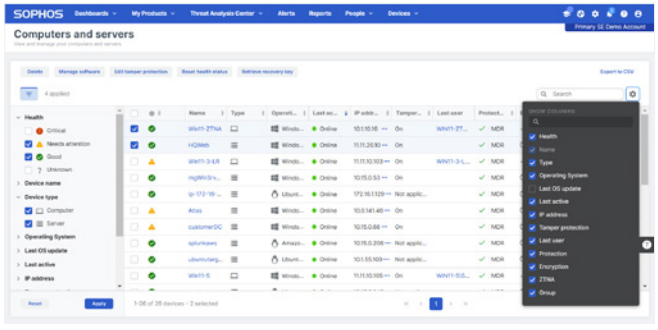
Überwacht und sperrt den Zugriff auf Wechselmedien, Bluetooth und Mobilgeräte, um zu verhindern, dass bestimmte Hardware eine Verbindung zu Ihrem Netzwerk herstellt.

Data Loss Prevention

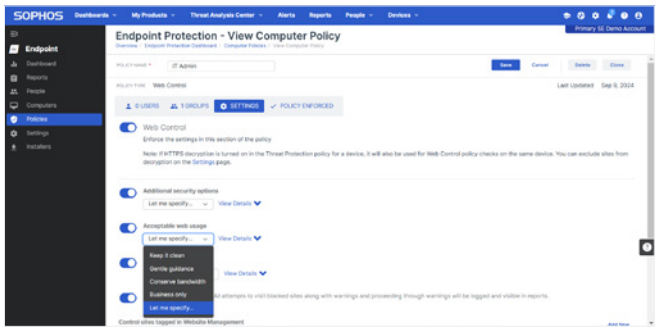
Überwacht oder beschränkt die Übertragung von Dateien mit sensiblen Daten. Beispielsweise wird verhindert, dass ein Benutzer eine vertrauliche Datei über webbasierte E-Mail-Programme versendet.



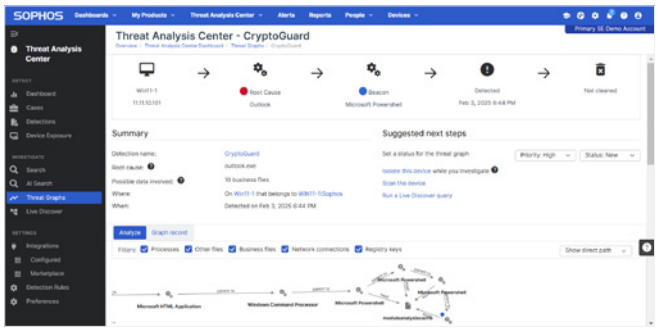
Passen Sie die Dashboards ganz nach Ihren Anforderungen individuell an.



Die Endpoint-Sicherheit lässt sich einfach einrichten und verwalten.



Empfohlene Einstellungen sind in den konfigurierbaren Richtlinien standardmäßig aktiviert.



Durch die Analyse von Bedrohungen können Sie deren Ursache einfach ermitteln.

Präventive Cybersecurity stoppt Bedrohungen schnell

Durch die frühzeitige Erkennung und Beseitigung von Bedrohungen können Sie Ihr Gefährdungspotenzial signifikant senken. Sophos Endpoint stoppt Bedrohungen schnell, bevor sie eskalieren, sodass IT-Teams mit begrenzten Ressourcen weniger Vorfälle analysieren und beheben müssen. Sophos bietet starke Funktionen zur Bedrohungsabwehr, die in unabhängigen Sicherheitstests regelmäßig Bestnoten erhalten.

Lückenloser Ransomware-Schutz

Laut Microsoft Digital Defense Report von 2024 kommt mittlerweile bei 70 % der erfolgreichen Angriffe Remote-Ransomware zum Einsatz, wobei 92 % aller Remote-Verschlüsselungsangriffe auf nicht verwalteten Geräten im Netzwerk starten. Sophos Endpoint bietet die stärkste Zero-Touch-Endpoint-Abwehr sowohl gegen lokale als auch Remote-Ransomware und erkennt Verschlüsselungsversuche dank modernster CryptoGuard-Technologie unabhängig von deren Ursprung.

- Blockiert neue und neuartige Ransomware-Varianten.
- Überprüft Dateiänderungen in Echtzeit, um schädliche Verschlüsselungen zu erkennen.
- Verhindert, dass Remote-Ransomware Dateien remote über das Netzwerk verschlüsselt.
- Setzt verschlüsselte Dateien automatisch in ihren unverschlüsselten Ursprungszustand zurück – mit proprietärer Technologie, die nicht auf den Windows Shadow Copy Service angewiesen ist.
- Schützt alle Dateitypen und -größen praktisch ohne Auswirkungen auf die Performance
- Bewahrt den Master Boot Record (MBR) vor komplexen Angriffen auf die Festplatte.

KI-gestützte Deep Learning Malware Prevention

Erkennt und blockiert sowohl bekannte als auch unbekannte Malware durch Analyse von Dateiattributen und prädiktives logisches Denken zum Erkennen von Bedrohungen.

Anti-Exploit-Funktionen

Schützt die Prozessintegrität durch Speicherhärtung und mehr als 60 Anti-Exploit-Verfahren, die nicht manuell optimiert werden müssen und nativen Windows-Funktionen und anderen Sicherheitslösungen überlegen sind.

Behavioral Protection

Überwacht Prozess-, Datei- und Registry-Ereignisse, um schädliche Aktivitäten zu erkennen und zu stoppen. Scannt den Speicher, prüft laufende Prozesse auf verborgene Bedrohungen und erkennt Angreifer, die schädlichen Code injizieren, um die Erkennung zu umgehen.

Synchronized Security

Sophos Endpoint tauscht Status- und Integritäts-Informationen mit der Sophos Firewall, Sophos Zero Trust Network Access (ZTNA) und anderen Produkten aus, um die Transparenz über Bedrohungen und die Anwendungsnutzung zu erhöhen und kompromittierte Geräte automatisch zu isolieren.

Live Protection

Erweitert starken Schutz auf dem Gerät mit Echtzeit-Abfragen aktueller globaler Bedrohungsinformationen aus den SophosLabs. Dies bietet zusätzlichen Dateikontext und unterstützt die Entscheidungsüberprüfung, False-Positive-Unterdrückung und Reputationprüfung.

Application Lockdown

Verhindert den Missbrauch von Browsern und Anwendungen durch das Blockieren von Aktionen, die normalerweise nicht in Verbindung mit diesen Prozessen beobachtet werden.

Antimalware Scan Interface (AMSI)

Das Windows Antimalware Scan Interface (AMSI) blockiert dateilose Angriffe, bei denen Malware direkt aus dem Speicher geladen wird. Sophos Endpoint umfasst zudem auch eine proprietäre Abwehrfunktion gegen die Umgehung der AMSI-Erkennung.

Malicious Traffic Detection

Erkennt Geräte, die mit Command and Control(C2)-Servern kommunizieren, indem sie Nicht-Browser-Datenverkehr abfängt und analysiert, ob dieser für eine schädliche Adresse bestimmt ist.

Adaptive Abwehr

Sophos Endpoint nutzt branchenweit einmalige dynamische Abwehrmechanismen, die den Schutz automatisieren, indem sie sich in Echtzeit an aktive Angreifer und manuell gesteuerte Angriffe anpassen. Sophos Endpoint blockiert Aktionen, die normalerweise nicht unbedingt schädlich sind, im Kontext eines Angriffs jedoch gefährlich werden. Diese Funktion reagiert dynamisch auf aktive Angriffe, bei denen Angreifer Fuß fassen konnten, ohne Warnsignale auszulösen oder schädlichen Code zu verwenden. Dadurch wird der Angriff unterbrochen.

Adaptive Attack Protection

Aktiviert dynamisch verstärkte Abwehrmaßnahmen auf Endpoints, wenn ein manuell gesteuerter Angriff erkannt wird. Dadurch wird das Angriffsgeschehen unterbrochen und Sie haben mehr Zeit, angemessen zu reagieren.

Critical Attack Warning

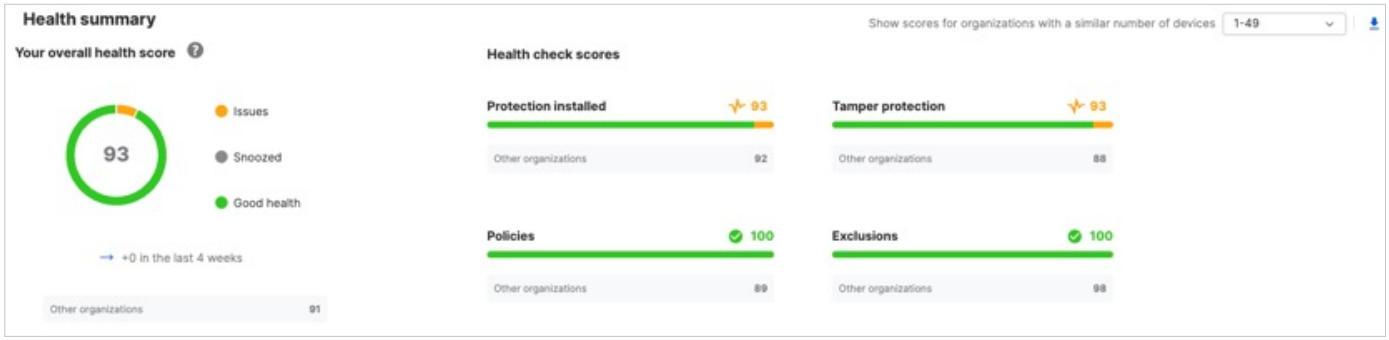
Benachrichtigt Administratoren über akute Angriffsaktivitäten auf mehreren Endpoints – basierend auf umgebungsweiten Bedrohungserkennungen.

	BEHAVIORAL PROTECTION	ADAPTIVE ATTACK PROTECTION	CRITICAL ATTACK WARNING
UMFANG	EINZELGERÄT	EINZELGERÄT	GESAMTE UMGEBUNG
VORTEILE	Die verhaltensbasierte Engine blockiert die frühen Phasen aktiver Angriffe	Verstärkt die Schutzfunktion, um Angriffe zu vermeiden	Warnt Sie bei Angriffen, auf die sofort reagiert werden muss
AUSLÖSER	Verhaltensregeln	Hacking-Toolsets erkannt	Relevante Indikatoren aktiver Angreifer, einschließlich Korrelationen und Schwellenwerte auf Organisationsebene
ANALOGIE	Schutzschild aktiviert	Schutzschild hoch	Alarmstufe Rot

Adaptive Abwehr in Sophos Endpoint

Änderungen am Sicherheitsstatus erkennen

Schlecht konfigurierte Richtlinien-Einstellungen, Ausschlüsse und andere Faktoren können Ihre Sicherheit beeinträchtigen. Der Account Health Check erkennt Sicherheitsprobleme und risikoreiche Fehlkonfigurationen, die Sie mit einem Klick beheben können.



Account Health Check

Zusätzliche Schutzschichten (Add-ons)

Sophos ZTNA

Ermöglichen Sie Ihren Nutzern sicheren Zugriff auf Ihre Anwendungen – mit der überlegenen Alternative zum klassischen VPN. Sophos ZTNA ist die einzige Lösung für Zero Trust Network Access, die nahtlos mit Next-Gen Endpoint Protection verknüpft ist.

Geräteverschlüsselung

Täglich gehen Geräte verloren oder werden gestohlen. Eine Festplattenverschlüsselung ist daher unerlässlich. Die in Sophos Endpoint integrierte Geräteverschlüsselung ermöglicht eine effektive Verwaltung von BitLocker (Windows) und FileVault (macOS).

Beschleunigte Erkennung, Analyse und Reaktion

Sophos Endpoint blockiert die meisten Bedrohungen bereits automatisch im Vorfeld, sodass weniger Ereignisse analysiert werden müssen. Für verdächtige Aktivitäten und Bedrohungen, die von Experten analysiert werden müssen, bietet Sophos leistungsstarke Lösungen, mit denen Sie alle wichtigen Angriffsvektoren schnell erkennen, analysieren und darauf reagieren können.

Sophos XDR

Mit Sophos Extended Detection and Response (XDR) können Sie in Ihrer gesamten Umgebung nach verdächtigen Aktivitäten und mehrphasigen Angriffen suchen, diese analysieren und darauf reagieren. Unsere leistungsstarken GenAI-basierten Tools wurden von Sicherheitsanalysten für Benutzer aller Kompetenzstufen entwickelt und ermöglichen es allen – von IT-Generalisten bis hin zu hochqualifizierten SOC-Analysten –, Bedrohungen schnell zu analysieren und Angreifer zu beseitigen.

Sophos XDR bietet schlüsselfertige Integrationen mit einem umfangreichen Ökosystem aus Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identity-, Produktivitäts-, Cloud- und Backup-Lösungen, mit denen Sie den ROI Ihrer bereits vorhandenen Sicherheitstools deutlich steigern können.

Weitere Infos unter sophos.de/xdr

Sophos MDR

Unternehmen, die nicht über die notwendigen internen Ressourcen verfügen, um die Bedrohungserkennung und -reaktion selbst zu bewerkstelligen, können Sophos Managed Detection and Response (MDR) in Anspruch nehmen, unseren 24/7 Threat Detection and Response Service, der von einem Expertenteam bereitgestellt wird. Sophos MDR nutzt Telemetriedaten von Sicherheitstechnologien anderer Hersteller und Sophos-Lösungen und erkennt und beseitigt so selbst die raffiniertesten Bedrohungen.

Sophos MDR lässt sich individuell auf Ihre Bedürfnisse zuschneiden – mit mehreren Servicestufen und Reaktions-Optionen sowie Möglichkeiten zum Einbinden bereits vorhandener Tools und Technologien.

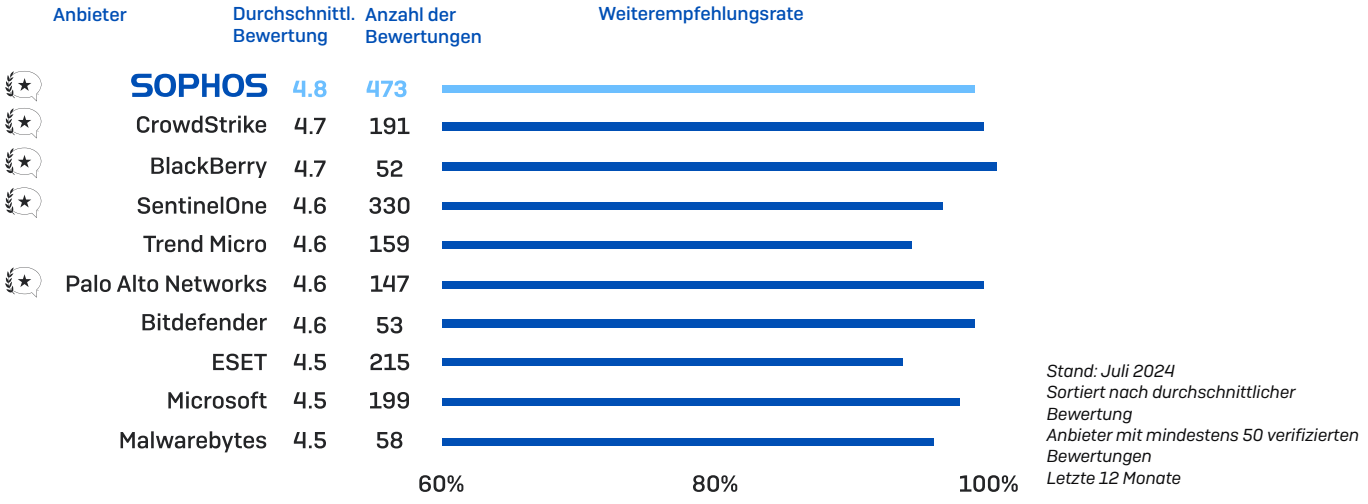
Weitere Infos unter sophos.de/mdr

	Sophos Endpoint	Sophos XDR	Sophos MDR
Next-Gen Threat Protection KI-gestützter Deep Learning-Malware- und Web-Schutz	✓	✓	✓
Blockieren schädlicher Aktivitäten Anti-Ransomware, Anti-Exploit, adaptive Abwehr	✓	✓	✓
Reduzierung der Angriffsfläche DLP, Web, Peripheral und Application Control	✓	✓	✓
Detection and Response Leistungsstarke Tools zur Bedrohungsanalyse und -reaktion		✓	✓
Transparenz über alle wichtigen Angriffsflächen Integrationen für Technologien von Sophos und anderen Anbietern		✓	✓
Managed Detection and Response 24/7 Threat Monitoring and Incident Response durch Experten			✓

Die am besten und am häufigsten bewertete Endpoint-Protection-Lösung

Im „Voice of the Customer Report“ von Gartner für Endpoint Protection Platforms 2024 erhielt Sophos die höchste Anzahl von Bewertungen unter allen Anbietern und erzielte eine Bewertung von 4,8/5,0. Darüber hinaus wurden wir in allen elf Branchensegmenten als „Customers’ Choice“ 2024 ausgezeichnet.

Endpoint Protection Platforms



Stand: Juli 2024
Sortiert nach durchschnittlicher Bewertung
Anbieter mit mindestens 50 verifizierten Bewertungen
Letzte 12 Monate

Darum entscheiden sich Kunden für Sophos Endpoint

Sophos ist ein etablierter Marktführer im Bereich Endpoint Security 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“.

SE Labs

Sophos erzielt in unabhängigen Endpoint-Security-Tests durchweg branchenführende Schutzergebnisse.

G2 Leader

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

IDC

Sophos ist ein Leader im IDC MarketScape 2024 in der Kategorie „Worldwide Modern Endpoint Security for Small and Midsize Businesses“.

Jetzt kostenfrei testen

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

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

2025-03-04 SB-DE (NP)

SOPHOS