LÖSUNGSBROSCHÜRE

Sophos Endpoint und EDR

Umfassende Endpoint Protection, Detection und Response

Die branchenweit führende KI-gestützte Endpoint-Security-Lösung

Sophos Endpoint bietet mit einem präventiven Cybersecurity-Konzept und branchenführender Endpoint Security einzigartigen Schutz von modernen Cyberangriffen. Sophos Endpoint Detection and Response (EDR) ist eine umfassende Schutz-, Erkennungs- und Reaktionslösung, die Sophos Endpoint umfasst und für Sicherheitsanalysten und IT-Administratoren konzipiert ist. Schützen und überwachen Sie Ihre Endpoints und Server auf verdächtige Aktivitäten – im Büro, remote oder in der Cloud.

Präventive Cybersecurity

Sophos Endpoint nutzt ein umfassendes Sicherheitskonzept, das auf präventiver Cybersecurity gründet, und verlässt sich zum automatischen Blockieren von Bedrohungen nicht auf eine einzelne Sicherheitstechnologie. Deep-Learning-KI-Modelle schützen vor bekannten und neuen Angriffen. Kontrollen reduzieren Ihre Angriffsfläche, während Verhaltensanalysen, Ransomware-Schutz, Anti-Exploit-Funktionen und weitere modernste Technologien Bedrohungen schnell stoppen, bevor sie eskalieren.

Adaptive Abwehr

Wenn Sophos Endpoint einen manuellen Angriff erkennt, werden dynamisch zusätzliche Abwehrmaßnahmen aktiviert, um Angreifer zu stoppen, bevor Schaden entsteht. Diese branchenweit einzigartige Funktion reduziert die Angriffsfläche und unterbricht und dämmt den Angriff ein. Dadurch werden Cyberkriminelle an weiteren Aktionen gehindert und Ihr Team erhält mehr Zeit zum Reagieren.

Einblick in evasive Bedrohungen

Sophos EDR bietet KI-priorisierte Bedrohungserkennungen, die verdächtige Aktivitäten hervorheben, die sofortige Aufmerksamkeit erfordern. Analysieren Sie Aktivitäten in Echtzeit – mit Zugriff auf umfangreiche Daten auf dem Gerät und Telemetrie im Sophos Data Lake, einschließlich historischer Aktivitäten, selbst wenn Geräte offline sind.

Schnellere und effektivere Workflows

Sophos EDR ist für IT-Generalisten und Sicherheitsanalysten konzipiert. Leistungsstarke Tools ermöglichen Ihrem Team, umfangreiche IT-Betriebsaufgaben schnell und einfach über eine direkte, sichere Verbindung zu Ihren Geräten zu erledigen. Ergebnisorientierte KI-Tools optimieren die Analyse und Reaktion, sodass Ihr Team verdächtige Aktivitäten und evasive Bedrohungen, die auf Ihre Endpoints und Server abzielen, schnell und präzise analysieren und beseitigen kann.

Vorteile auf einen Blick

- Präventive Cybersecurity, die Ihre Angriffsfläche reduziert und Bedrohungen schnell stoppt
- Sichere Daten dank erstklassigem Schutz vor lokalen und Remote-Ransomware-Angriffen
- Branchenweit einmalige dynamische Abwehrmechanismen, die sich als Reaktion auf aktive Angreifer und manuell gesteuerte Angriffe automatisch anpassen
- KI-priorisierte Erkennungen heben hervor, worauf Ihr Team sich konzentrieren sollte
- Ergebnisorientierte KI-Tools optimieren die Analyse und Reaktion auf verdächtige Aktivitäten und evasive Bedrohungen
- Leistungsstarke Tools für IT-Generalisten und Sicherheitsanalysten

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

Fängt ausgehende Browser-Verbindungen ab und blockiert Datenverkehr, der für schädliche oder verdächtige Websites bestimmt ist. Die Lösung stoppt Bedrohungen in der Bereitstellungsphase und verhindert, dass Benutzer auf Websites zur Malware-Bereitstellung oder Phishing-Websites umgeleitet werden.

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

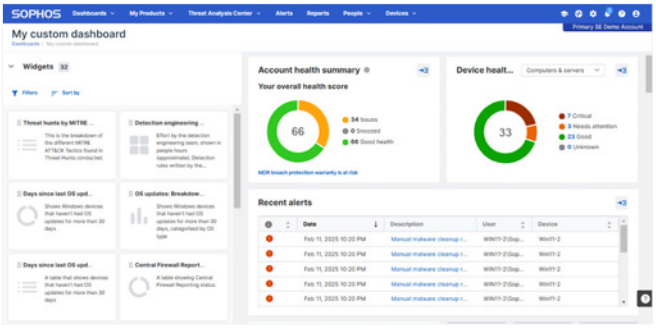
Blockiert Anwendungen, die möglicherweise anfällig bzw. für Ihre Umgebung ungeeignet sind oder für kriminelle Zwecke missbraucht werden könnten. Sophos bietet vordefinierte Kategorien zum Blockieren und Überwachen von Anwendungen, wodurch das zeitaufwendige Blockieren einzelner Anwendungen per Hash entfällt.

Peripheral (Device) Control

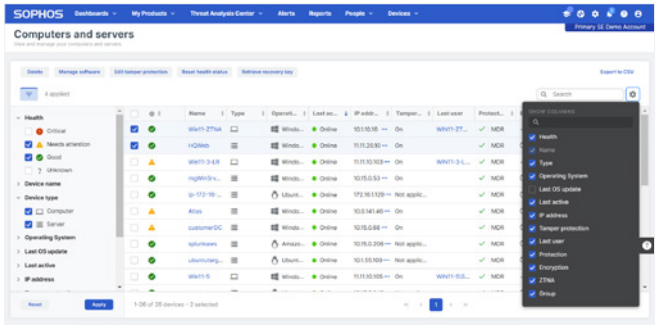
Überwacht und sperrt den Zugriff auf Wechselmedien, Bluetooth und Mobilgeräte, um zu verhindern, dass bestimmte Hardware eine Verbindung zu Ihrem Netzwerk herstellt.

Data Loss Prevention

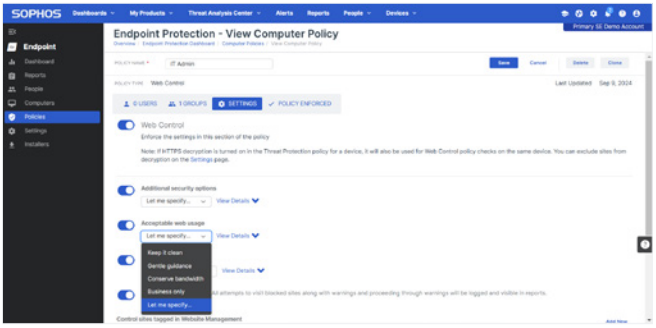
Überwacht oder beschränkt die Übertragung von Dateien mit sensiblen Daten. Beispielsweise wird verhindert, dass ein Benutzer eine vertrauliche Datei über webbasierte E-Mail-Programme versendet.



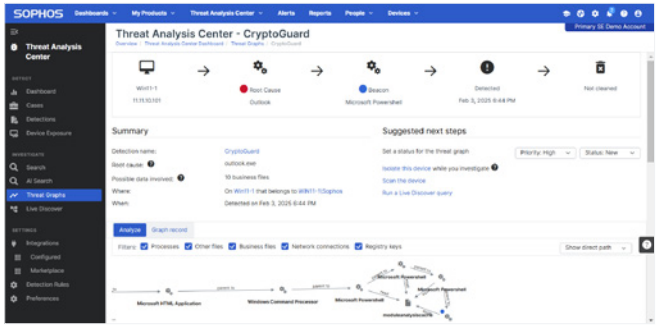
Passen Sie die Dashboards ganz nach Ihren Anforderungen individuell an.



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 Malware-Abwehr auf Basis von Deep Learning

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

Anti-Exploit-Funktionen

Schützen die Prozessintegrität, indem sie den Anwendungsspeicher härten und bei der Ausführung von Laufzeitcode sogenannte Guardrails anwenden. Sophos Endpoint umfasst über 60 standardmäßig aktivierte Anti-Exploit-Techniken, die keine Schulung oder Feinabstimmung erfordern. Diese Techniken bieten Schutz, der dem von Windows und den meisten anderen Endpoint-Security-Lösungen gebotenen Schutz bei Weitem überlegen ist.

Behavioral Protection

Überwacht Prozess-, Datei- und Registrierungsereignisse im Zeitverlauf, um schädliche Verhaltensweisen und Prozesse zu erkennen und zu stoppen. Außerdem werden Speicher-Scans durchgeführt, laufende Prozesse auf schädlichen Code überprüft, der nur während der Prozessausführung sichtbar wird, und Angreifer erkannt, die schädlichen Code in den Speicher eines laufenden Prozesses einschleusen, um die Erkennung zu umgehen.

Synchronized Security

Sophos Endpoint tauscht Status- und Integritäts-Informationen mit der Sophos Firewall, Sophos Wireless, 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 umfassenden 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. Unsere hoch spezialisierte Bedrohungsforschung liefert zusätzliche Live-Informationen aus dem umfangreichen Produkt-Portfolio und dem globalen Kundenstamm von Sophos.

Application Lockdown

Verhindert den Missbrauch von Browsern und Anwendungen durch das Blockieren von Aktionen, die normalerweise nicht in Verbindung mit diesen Prozessen beobachtet werden (z. B. ein Webbrowser oder eine Office-Anwendung, die versucht, PowerShell zu starten).

Antimalware Scan Interface (AMSI)

Das Windows Antimalware Scan Interface (AMSI) bestimmt, ob Skripte (z. B. PowerShell oder Office-Makros) sicher sind (u. a. ob sie verschleiert sind oder zur Laufzeit generiert werden), und blockiert dateilose Angriffe, bei denen Malware direkt aus dem Speicher geladen wird. Sophos verfügt außerdem über proprietäre Funktionen zur Abwehr von Malware, die versucht, die AMSI-Erkennung zu umgehen.

Malicious Traffic Detection

Erkennt Geräte, die versuchen, mit einem Command-and-Control(C2)-Server zu kommunizieren, indem sie Datenverkehr von Nicht-Browser-Prozessen 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. Die adaptiven Abwehrmaßnahmen blockieren Aktionen, die in einem typischen Kontext möglicherweise unbedenklich erscheinen, aber während eines Angriffs gefährlich sein können. So können Sie dynamisch auf aktive Angriffe reagieren und das Angriffsgeschehen unterbrechen – selbst wenn Angreifer bereits Fuß gefasst haben, und das alles, ohne Alarm auszulösen oder auf bösartigen Code angewiesen zu sein.

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.

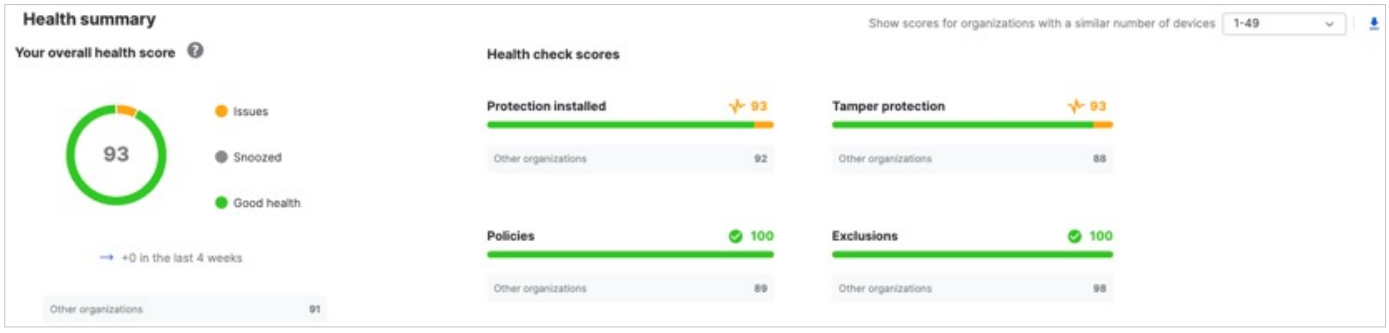
	BEHAVIORAL PROTECTION	ADAPTIVE ATTACK PROTECTION	CRITICAL ATTACK WARNING
UMFANG	EINZELGERÄT	EINZELGERÄT	GESAMTE UMGEBUNG
VORTEILE	Die verhaltensbasierte Engine blockiert die frühen Phasen aktiver Angriffe	Verstärkt die Schutzfunktion, um Angriffe zu vermeiden	Warnt Sie bei Angriffen, auf die sofort reagiert 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

Starke Standardrichtlinien und Erkennen von Änderungen am Sicherheitsstatus

Standardmäßig sind in Sophos Endpoint unsere empfohlenen Schutztechnologien aktiviert, sodass Sie sofort über die stärksten Schutzeinstellungen verfügen. Es ist keine komplizierte Konfiguration oder Anpassung erforderlich. Bei Bedarf besteht jedoch die Möglichkeit, für eine besonders granulare Kontrolle individuelle Anpassungen vorzunehmen.

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

Beschleunigte Erkennung, Analyse und Reaktion

Sophos EDR ist eine umfassende Schutz-, Erkennungs- und Reaktionslösung, die für IT-Generalisten und Sicherheitsanalysten entwickelt wurde. Sophos EDR reduziert Ihr Sicherheitsrisiko durch die Möglichkeit, auf evasive Bedrohungen zu reagieren und die potenziellen Auswirkungen auf Ihr Unternehmen zu minimieren. Sophos Endpoint ist in Sophos EDR enthalten und nativ integriert.

KI-priorisierte Erkennungen

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

Reaktionsmaßnahmen von Sicherheitsanalysten

Ihr Team kann Endpoints isolieren, während Analysen verdächtiger Aktivitäten manuell adaptiven Angriffsschutz aktivieren u.v.m.

KI-Fallzusammenfassung

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

Automatisierte Reaktionsmaßnahmen

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

KI-Suche

Beschleunigt tägliche Aufgaben durch natürliche Sprache und senkt die technologischen Hürden für Security Operations.

KI-Befehlsanalyse

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

Live Response

Sophos EDR ermöglicht IT-Generalisten und Sicherheitsanalysten, IT-Betriebsaufgaben effizient zu erledigen und Bedrohungen schnell und präzise zu beseitigen. Über eine direkte, sichere und geprüfte Verbindung zu Ihren Endpoints und Servern können Sie potenzielle Probleme direkt in der Sophos-Konsole analysieren und beheben.

Per Remote-Zugriff auf Geräte können Sie folgende Aufgaben erledigen:

- Software installieren und deinstallieren
- Skripts und Programme ausführen
- Konfigurationsdateien bearbeiten
- Herunterfahren/neu starten
- Forensische Tools von Drittanbietern ausführen
- Und viele weitere Aufgaben

Gerätegefährdung

Identifizieren Sie schnell riskante, veraltete und anfällige Geräte in Ihrer Umgebung. Die Funktion „Gerätegefährdung“ informiert Sie über Geräte, die besonders anfällig für Bedrohungen sind, und ermöglicht Ihnen, Maßnahmen für Geräte zu ergreifen, auf denen seit Längerem keine Betriebssystem-Updates mehr durchgeführt wurden.

Funktionsumfang von Sophos Endpoint und Sophos EDR

	Sophos Endpoint	Sophos EDR
Next-Gen Endpoint Protection Malware-Schutz auf Basis von Deep Learning (KI-gestützt), Ransomware-Schutz, Verhaltensanalyse, Anti-Exploit-Funktionen u.v.m.	✓	✓
Adaptive Abwehr Adaptiver Angriffsschutz, Warnung vor kritischen Angriffen	✓	✓
Reduzierung der Angriffsfläche von Endpoints Web-Schutz, Web Control, Peripheral Control, App Control und Data Loss Prevention	✓	✓
Endpoint Detection and Response (EDR) Erkennung und Analyse von Angriffen auf Endpoints und Server sowie Reaktionsmaßnahmen		✓
Live Response und Gerätegefährdung Leistungsstarke Tools für IT-Generalisten und Sicherheitsanalysten		✓
Speicherung von Erkennungsdaten im Sophos Data Lake (standardmäßig 30 Tage)		✓ (Upgrade auf 1 Jahr möglich)
Sophos Endpoint for Legacy Platforms Umfassende Sicherheit für ältere und nicht mehr unterstützte Windows- und Linux-Betriebssysteme	Optionales Add-on	Optionales Add-on
Sophos Device Encryption Zentrale Verwaltung der nativen Festplattenverschlüsselung auf Windows- und macOS-Geräten	Optionales Add-on	Optionales Add-on
Sophos Incident Response (IR) Services Retainer Expertenteam, auf das Sie im Ernstfall jederzeit zurückgreifen können	Optionales Add-on	Optionales Add-on

Sophos XDR

Sophos Extended Detection and Response (XDR) bietet Transparenz über die Endpoint- und Server-Ebene hinaus. Mit den leistungsstarken Tools und der Threat Intelligence erkennen, analysieren und beseitigen Sie Bedrohungen in Ihrem gesamten IT-Ökosystem – bereitgestellt über die adaptive, KI-native, offene Plattform von Sophos.

Unsere offene, erweiterbare Architektur bietet durch Integration von Bedrohungsdaten bestehender und neu erworbener Sicherheitslösungen Transparenz über Ihre gesamte Angriffsfläche. Sophos XDR umfasst schlüsselfertige Integrationen mit einem umfangreichen Ökosystem von Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identity-, Backup-, Cloud-Security- und Produktivitätslösungen.

Weitere Infos unter sophos.de/xdr

Sophos MDR

Mit den Managed Detection and Response (MDR) Services von Sophos bleiben Sie Angreifern immer einen Schritt voraus – egal, in welchem Stadium Ihrer Cybersecurity-Implementierung Sie sich befinden. Wir kombinieren benutzerfreundliche, KI-basierte Technologien mit hochkarätigen Sicherheitsexperten, die Bedrohungen rund um die Uhr überwachen, abwehren, erkennen und auf sie reagieren.

Über verschiedene Service-Level und Reaktions-Optionen passen Sie Sophos MDR individuell an Ihre Anforderungen an. Sophos MDR integriert Bedrohungsdaten bestehender und neu erworbener Sicherheitslösungen.

Weitere Infos unter sophos.de/mdr

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 2025 im Gartner® Magic Quadrant™ for Endpoint Protection Platforms zum 16. Mal in Folge ein Leader.

SE Labs

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

Leader

Sophos ist der einzige Anbieter, der in den G2 Overall Grid® Reports vom Frühjahr 2025 für Endpoint Protection Suites, EDR, XDR, Firewall-Software und MDR als ein Leader eingestuft wurde.

IDC

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

Gartner Peer Insights Customers' Choice 2025

Sophos ist ein Gartner® Peer Insights™ „Customers' Choice“-Anbieter im Voice of the Customer Report für Endpoint Protection Platforms 2025.

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

© Copyright 2025. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

2025-09-17 BR-DE (NP)

SOPHOS