LÖSUNGSBESCHREIBUNG

Sophos Endpoint

KI-gestützte Cybersecurity verhindert Sicherheitsverstöße, Ransomware-Angriffe und Datenverluste

Sophos Endpoint bietet mit erstklassigen Endpoint-Security-Funktionen einzigartige Abwehrmaßnahmen gegen komplexe Cyberangriffe. Mit umfassenden Abwehrmaßnahmen, die auch lückenlosen Ransomware-Schutz umfassen, stoppen Sie die meisten Bedrohungen bereits automatisch, bevor sie Ihre Systeme beeinträchtigen. KI-gestützte Detection- und Response-Tools ermöglichen Ihrem Team, verdächtige Aktivitäten und komplexe Bedrohungen, die auf Ihre Endpoints und Server abzielen, schnell und präzise zu analysieren und zu beseitigen.

Anwendungsfälle

1 | PRÄVENTIVE CYBERSECURITY

Gewünschtes Ergebnis: Mehr Bedrohungen bereits im Vorfeld stoppen, um Risiken zu minimieren und den Arbeitsaufwand zu reduzieren

Lösung: 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. 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.

2 | ADAPTIVE ABWEHR

Gewünschtes Ergebnis: Aktive Angreifer mit dynamischem Schutz stoppen, der sich automatisch an das Angriffsgeschehen anpasst

Lösung: 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.

3 | EINFACHE VERWALTUNG

Gewünschtes Ergebnis: Auf Bedrohungen konzentrieren statt auf die Verwaltung

Lösung: Sophos Central ist eine cloudbasierte, KI-native Cybersecurity-Management-Plattform für alle Sophos-Next-Gen-Sicherheitslösungen. Starke Standard-Richtlinieneinstellungen gewährleisten, dass ohne zusätzliche Schulungen und Feinabstimmungen die empfohlenen Schutzeinstellungen aktiviert sind. Der Account Health Check („Kontointegrität“) in Sophos Central erkennt Konfigurationsprobleme und bietet Klick-to-Fix-Funktionen zur Problembehebung, mit denen Sie Ihren Sicherheitsstatus einfach optimieren.

4 | DETECTION AND RESPONSE

Gewünschtes Ergebnis: Evasive Angriffe beseitigen, die durch Technologie allein nicht gestoppt werden können

Lösung: Mit unseren EDR(Endpoint Detection and Response)-Funktionen finden, analysieren und bekämpfen Sie verdächtige Aktivitäten auf Ihren Endpoints und Servern. Sophos XDR (Extended Detection and Response) erweitert EDR und bietet durch Integration von Bedrohungsdaten bestehender und neu erworbener Sicherheitslösungen Transparenz über Ihre gesamte Angriffsfläche. Bei begrenzten internen Ressourcen können Sophos Managed Detection and Response (MDR) Services in Anspruch genommen werden. Diese Services werden von globalen Cybersecurity-Experten bereitgestellt, die Ihre Umgebung rund um die Uhr auf Bedrohungen überwachen.

Gartner

Zum 16. Mal in Folge ein Leader im Gartner® Magic Quadrant™ for Endpoint Protection Plattforms

Gartner Peer Insights Customers' Choice 2025

Customers' Choice im Gartner® Voice of the Customer Report für Endpoint Protection Platforms 2025

SE Labs

Branchenführende Ergebnisse in unabhängigen Schutztests

Nr. 1

Die zuverlässigste Zero-Touch-Endpoint-Abwehr gegen Remote-Ransomware

Mehr erfahren und kostenlos testen:

sophos.de/endpoint

2025-09-17 SB-DE (NP)