Lösungsbeschreibung

Sophos Endpoint

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

Sophos Endpoint bietet einzigartige Abwehrmaßnahmen gegen komplexe Cyberangriffe und lückenlosen Ransomware-Schutz, um die meisten Bedrohungen bereits zu stoppen, bevor sie Ihre Systeme beeinträchtigen. GenAI-gestützte EDR- und XDR-Tools ermöglichen Ihrem Team, komplexe mehrphasige Bedrohungen schnell und präzise zu erkennen, zu analysieren und darauf zu reagieren.

Anwendungsfälle

1 | PRÄVENTIVE CYBERSECURITY

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

Lösung: 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.

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 automatisch zusätzliche Abwehrmaßnahmen aktiviert, um den Angreifer zu stoppen, bevor Schaden entsteht. In diesem erhöhten Schutzmodus werden verdächtige Aktivitäten wie Downloads von Remote-Verwaltungstools sofort blockiert, sodass Ihr Team mehr Zeit für die Reaktion erhält.

3 | DETECTION AND RESPONSE

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

Lösung: Unsere leistungsstarken EDR- und XDR-Tools können mit Security-Produkten von Sophos und anderen Herstellern genutzt werden. Sie ermöglichen Ihnen, verdächtige Aktivitäten zu erkennen, zu analysieren und darauf zu reagieren. Unternehmen und Organisationen mit begrenzten internen Ressourcen können den Service Sophos Managed Detection and Response (MDR) in Anspruch nehmen oder den Sophos Incident Response Service Retainer nutzen, um im Falle eines Sicherheitsvorfalls schnell auf unsere Experten zurückgreifen zu können.

4 | 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 stellen sicher, dass in Ihrem Unternehmen oder Ihrer Organisation 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.

Gartner

Zum 15. Mal in Folg ein Leader im Gartner® Magic Quadrant™ for Endpoint Protection Plattforms

Gartner Peer Insights Customers' Choice 2024

Customers' Choice im Gartner® Voice of the Customer Report für Endpoint Protection Platforms 2024

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

2025-02-03 SB-DE (MP)

SOPHOS