SOPHOS

Verstärken Sie Microsoft Defender mit Sophos MDR

Reduzieren Sie Cyber-Risiken, schöpfen Sie Ihre Investition in Microsoft Security voll aus und verbessern Sie Ihre Konditionen bei Cyberversicherungen: Verstärken Sie den Schutz von Microsoft Defender mit 24/7 Bedrohungserkennung und -bekämpfung durch ein Expertenteam – von dem MDR-Anbieter, dem weltweit die meisten Kunden vertrauen.

Sophos-Whitepaper, Juli 2023

Einführung

Endpoint Security ist ein wesentlicher Bestandteil der Cyber-Abwehr, sie kann jedoch nicht alle Bedrohungen stoppen. Hochversierte Cyberkriminelle tarnen ihre Angriffe mit Taktiken, Techniken und Prozessen, um von Sicherheitstechnologien unerkannt zu bleiben. Dazu nutzen sie etwa ungepatchte Schwachstellen, bedienen sich gestohlener Anmeldeinformationen oder zweckentfremden legitime IT-Tools.

Um komplexe Ransomware-Angriffe und Datendiebstähle zu stoppen, ist es wichtig, den Schutz von Microsoft Defender rund um die Uhr durch expertengestützte Erkennungs- und Reaktionsmaßnahmen zu ergänzen. Doch angesichts der schieren Menge an Warnmeldungen von Microsoft-Security-Lösungen und zunehmend komplexeren Bedrohungen stoßen Sicherheitsteams in Unternehmen dabei schnell an ihre Grenzen.

Vor diesem Hintergrund setzen immer mehr Unternehmen auf Sophos MDR, dem MDR-Service, dem weltweit die meisten Kunden vertrauen, und optimieren so den Schutz von Microsoft Defender. Sophos-Analysten überwachen und untersuchen Microsoft-Sicherheitswarnmeldungen rund um die Uhr und ergreifen sofortige Maßnahmen, um bestätigte Bedrohungen zu stoppen. Außerdem erkennen und stoppen sie Bedrohungen, die von Microsoft Defender nicht erfasst werden – mit Sophos-eigenen Erkennungen, Threat Intelligence und manuellen Threat Hunts.

Sophos MDR überzeugt durch individuell anpassbare Service-Optionen, die sich auf vorhandene IT-/Cybersecurity-Lösungen und interne Ressourcen abstimmen lassen. Egal, ob Sie das Know-how Ihrer IT ergänzen, ihre Cyber-Abwehr außerhalb der Geschäftszeiten verstärken oder die Bedrohungserkennung und -reaktion komplett auslagern möchten – mit Sophos MDR sorgen Sie für effektiven Cyberschutz.

Verstärken Sie Microsoft Defender mit Sophos MDR

✓ Cyber-Risiken reduzieren

- Stoppen Sie komplexe Ransomware-Angriffe und Sicherheitsvorfälle, einschließlich manueller Angriffe, die von Microsoft Defender nicht erfasst werden

✓ Sicherheitsinvestitionen optimal nutzen

- Setzen Sie IT-Ressourcen für strategische Aufgaben frei
- Minimieren Sie die Wahrscheinlichkeit erheblicher Bereinigungskosten nach Vorfällen
- Steigern Sie den ROI vorhandener Investitionen

✓ Konditionen beim Versicherungsschutz verbessern

- Erhalten Sie bessere Versicherungsangebote, indem Sie Ihre Cyber-Risiken reduzieren

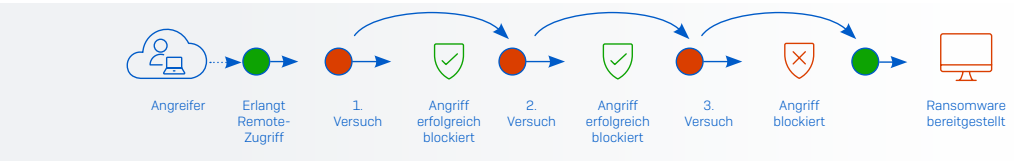
Technologie allein kann Angreifer nicht stoppen

Die Realität zeigt, dass Technologie-Lösungen, einschließlich Microsoft Defender, allein nicht jeden Cyberangriff verhindern können. Aktive Angreifer passen ihre Taktiken, Techniken und Prozesse (TTPs) in Echtzeit an Abwehrmaßnahmen von Sicherheitstechnologien und Bedrohungsexperten an, um unerkannt zu bleiben.

Diese Angriffe führen oft zu verheerenden Ransomware-Vorfällen und Datenschutzverletzungen und lassen sich nur sehr schwer stoppen. Zudem sind manuelle Angriffe mittlerweile weit verbreitet. So verzeichneten 23 % der kleinen und mittleren Unternehmen im vergangenen Jahr einen aktiven Angriff. Mit Hinblick auf die potenziell katastrophalen Auswirkungen dieser Angriffe geben 30 % der IT-/Cybersecurity-Experten an, dass sie aktive Angreifer als eine der besorgniserregendsten Cyberbedrohungen in 2023 einstufen.[1]

Mit Sicherheitstechnologien allein lassen sich aktive Angreifer nicht stoppen. Diese versierten, hartnäckigen Bedrohungsakteure bedienen sich verschiedenster, innovativer Angriffsmethoden und verfolgen dabei unter anderem folgende Ziele:

- Ausnutzen von Sicherheitslücken (gestohlene Zugangsdaten, ungepatchte Schwachstellen und Fehlkonfigurationen von Sicherheitstools), um die Unternehmensabwehr zu überlisten und sich lateral im Netzwerk zu bewegen.
- Zweckentfremden legitimer IT-Tools, um keine Erkennungen auszulösen, z. B. PowerShell, PsExec und RDP.
- Anpassen ihrer Angriffe in Echtzeit an Sicherheitskontrollen und Ausweichen auf neue Techniken, bis sie ihre Ziele erreichen.



Beispiel für eine aktive Angriffsstrategie

Indem sie autorisierte Benutzer nachahmen und sich Sicherheitslücken zunutze machen, können Angreifer automatisierte Erkennungstechnologien überlisten, die nicht zwischen legitimen Benutzern und Angreifern unterscheiden können.

Erschwerend kommt hinzu, dass moderne, finanzstarke Cyberkriminelle mit immer innovativeren Geschäftsmodellen arbeiten. „Cybercrime-as-a-Service" (Ransomware-as-a-Service, Phishing-as-a-Service und mehr) boomt und erleichtert den Einstieg in die Cyberkriminalität. Bedrohungsakteure sind zunehmend in der Lage, Angriffe im großen Stil auszuführen.

In der Folge sind die Datenverschlüsselungsraten bei Ransomware-Angriffen höher denn je: Bei mehr als drei Vierteln der Angriffe (76 %) konnten Cyberkriminelle Daten verschlüsseln[2].

Ransomware in Zahlen

- 66 % der Unternehmen wurden im letzten Jahr Opfer von Ransomware
- 76 % der Ransomware-Angriffe führten zu einer Verschlüsselung von Daten
- 30 % der Angriffe, bei denen Daten verschlüsselt wurden, gingen mit Datendiebstahl einher
- Angriffsursache Nummer 1: Ausgenutzte Schwachstellen (36 %)
- Angriffsursache Nummer 2: Kompromittierte Anmeldedaten (29 %)

1 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos.

2 Ransomware-Report 2023, Sophos.

24/7 Threat Detection and Response: Moderne Cybersecurity ist essenziell

Die gute Nachricht: Durch die Kombination aus Technologie und Experten-Knowhow lassen sich komplexe, manuelle Angriffe abwehren. Bei jeder Aktion, die ein Angreifer ausführt, wird ein Signal erzeugt. Die Verbindung von menschlicher Expertise, modernsten KI-basierten Machine-Learning-Modellen und Extended Detection and Response (XDR) Tools ermöglicht Sicherheitsanalysten, Daten von Security- und IT-Tools zu nutzen. So können sie hochkomplexe, von Hackern manuell gesteuerte Angriffe erkennen, analysieren und beseitigen, um Ransomware-Angriffe und Sicherheitsvorfälle zu verhindern.

24/7 Threat Detection and Response sind ein wesentlicher Bestandteil moderner Cybersecurity. Viele Unternehmen tun sich jedoch schwer, dies effektiv umzusetzen und sind daher anfällig für Angriffe. Sie sehen sich vor allem mit mangelnder Expertise und unzureichenden Kapazitäten konfrontiert.

Herausforderung Nummer 1: Mangelnde Expertise

Bedrohungserkennung, -analyse und -reaktion sind hochspezialisierte Aufgaben, die eine umfassende Kenntnis von Angriffstechniken, Analysestrategien und Security-Tools voraussetzen. Nur wenige Unternehmen verfügen intern über dieses breitgefächerte und kostenintensive Spektrum an Kompetenzen. So bestätigen 93 % der Unternehmen, dass bereits grundlegende Sicherheitsaufgaben eine Herausforderung darstellen:

- Für 71 % ist das Ermitteln relevanter Signale und Warnmeldungen, die untersucht werden müssen, schwierig
- 71 % können nur mit Mühe ausreichende Daten erfassen, um festzustellen, ob ein Signal schädlich oder harmlos ist
- 75 % fällt es schwer, die Ursache eines Vorfalls zu ermitteln, d. h. wie der Angreifer sich Zugang verschaffen konnte

Das Ausmaß des Problems wird deutlich, wenn man die Daten betrachtet, die IT-Teams von Cybersecurity-Tools erhalten. Die folgende Tabelle zeigt Beispiele für Microsoft-Defender-Ereignisse und die entsprechende Ereigniskategorie.

Die Warnmeldungen zu verstehen, ist nur ein Teil der Bedrohungserkennung und -reaktion. Die IT-Security muss die Bedrohung mit kontextbasierten Daten und Threat Intelligence außerdem eingehend analysieren, um erforderliche Maßnahmen zu ermitteln.

EREIGNISBESCHREIBUNG	EREIGNISTYP
Auf verdächtigen Link geklickt	Initial Access
Schädliche Dateien oder Netzwerkverbindungen, die mit dem Prozess 3CXDesktopApp.exe verknüpft sind	Malware
Neues Benutzerkonto erstellt	Persistence
TS_BL_Suspicious Eventlog löschen oder Konfiguration mit Wevtutil	Defense Evasion
Privilegien-Eskalation verarbeiten	Privilege Escalation
Versuch, Microsoft Defender Antivirus-Schutz zu deaktivieren	Defense Evasion
Eine Datei oder Netzwerkverbindung, die mit dem Bedrohungsakteur Storm-0867 in Verbindung steht, erkannt	Credential Access
TS_BL_Script-Engines, die eine Verbindung zum Internet herstellen	Command and Control
Potenziell böswillige Aktivitäten, die manuell durchgeführt werden	Suspicious Activity
TS_BL_Malicious Payload-Download über Office-Binärprogramme	Ausführung
Neue Angreifergruppe DEV-0867 erkannt	Credential Access
Neue Angreifergruppe Citrine Sleet erkannt	Malware

Beispiele für Microsoft-Defender-Erkennungen, für die ein Fall erstellt wird

Herausforderung Nummer 2: Unzureichende Kapazitäten

Bedrohungserkennung, -analyse und -reaktion sind sehr zeitaufwändig. So beträgt die durchschnittliche Reaktionszeit auf Warnmeldungen bei Unternehmen mit 100 bis 3.000 Mitarbeitern 9 Stunden, bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sogar bis zu 15 Stunden.

IT-Teams benötigen unzählige Stunden für die Bearbeitung von Sicherheitswarnungen. Oft führt die Dringlichkeit der Arbeit dabei dazu, dass sich Teams nicht mehr auf strategisch wichtige Aufgaben konzentrieren können. Da Cyberkriminelle zu jeder Tageszeit zuschlagen können, müssen Unternehmen in der Lage sein, rund um die Uhr sofort auf Bedrohungen zu reagieren. Den meisten Unternehmen fehlen dazu schlichtweg die nötigen Kapazitäten.

Die Lösung: Eine robustere Cyber-Abwehr durch Managed Detection and Response (MDR)

52 % der IT-/Cybersecurity-Experten räumen ein, dass sie nicht mehr in der Lage sind, den zunehmend komplexen Cyberangriffen ohne Unterstützung von außen Herr zu werden. Daher setzen immer mehr Unternehmen auf spezialisierte MDR-Anbieter zur Ergänzung ihrer internen Cybersecurity-Ressourcen.

Was MDR konkret umfasst

MDR (Managed Detection and Response) ist ein 24/7 Fully-Managed Service, der durch ein Team von Sicherheitsexperten bereitgestellt wird. Diese sind auf das Erkennen und Bekämpfen von Cyberangriffen spezialisiert, gegen die reine Technologie-Lösungen machtlos sind.

Extended Detection and Response (XDR) ist eine Plattform, die Sicherheitsdaten aus mehreren Quellen kombiniert, um die Bedrohungserkennung, -analyse und -reaktion auf eine Weise zu automatisieren, die Einzellösungen überlegen ist.

Mit der Sophos-XDR-Plattform suchen, analysieren und beseitigen die MDR-Experten von Sophos Bedrohungen in Ihrem Auftrag für Sie. Zur Beschleunigung der Bedrohungssuche und -reaktion konsolidieren sie Signale aus der gesamten IT-Umgebung, einschließlich Firewall-, E-Mail-, Cloud- und mobilen Sicherheitslösungen.

Verstärken Sie Microsoft Defender mit Sophos MDR

Sophos MDR liefert effektive 24/7 Threat Detection and Response für Microsoft-Defender-Umgebungen. Sophos-Analysten überwachen und untersuchen Microsoft-Sicherheitswarnmeldungen rund um die Uhr und ergreifen sofortige Maßnahmen, um bestätigte Bedrohungen zu stoppen. Außerdem erkennen und stoppen sie Bedrohungen, die von Microsoft Defender nicht erfasst werden – mit Sophos-eigenen Erkennungen, Threat Intelligence und manuellen Threat Hunts.

Je mehr Einblicke wir haben, desto schneller können wir reagieren. Sophos MDR nutzt weitere Sicherheitsereignis-Quellen von Microsoft, die in E3- und E5-Lizenzen enthalten sind, sowie Signale von Firewall-, Cloud-, E-Mail-, Identitäts- und NDR (Network Detection and Response)-Tools und beschleunigt so die Bedrohungserkennung und -reaktion.

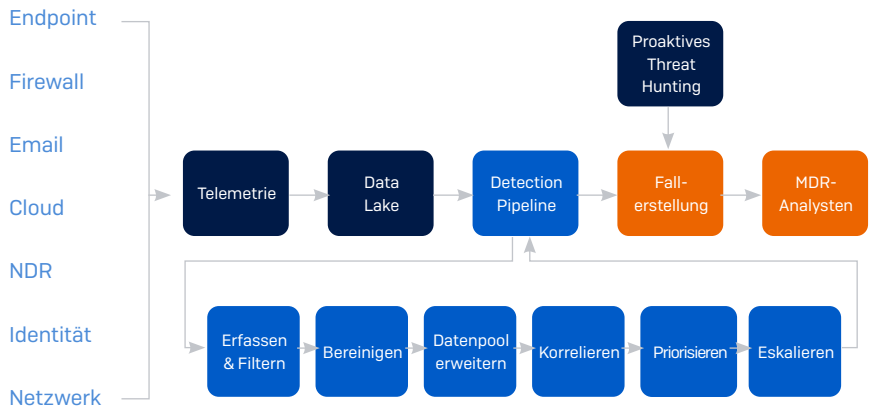
Benutzer von Microsoft Defender können unsere Security-Operations-Experten rund um die Uhr telefonisch erreichen und Reports zur Bedrohungsaktivität in der Sophos-Central-Plattform abrufen.

Sophos MDR für Microsoft Defender ist kompatibel mit Sicherheitsereignis-Quellen von Microsoft

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- MS 0365 Security & Compliance Center
- Microsoft Azure Sentinel
- Office 365 Management Activity (einheitliches Audit-Protokoll)

Sicherheitsereignis-Flow von Sophos MDR

Unser patentierter Sicherheitsereignis-Flow ist eine zentrale Komponente des Sophos-MDR-Services. Telemetriedaten aus der gesamten Sicherheitsumgebung, also auch von Microsoft Defender, werden vom Sophos Data Lake erfasst und über unsere Detection Pipeline verarbeitet. Die Pipeline verwandelt Warnmeldungen von Microsoft und Drittanbieter-Lösungen in aussagekräftige, priorisierte Daten für eine effektive Analyse und Reaktion.



Der Sicherheitsereignis-Flow von Sophos MDR

Erfassen & Filtern – Telemetriedaten werden erfasst und irrelevante Informationen herausgefiltert

Bereinigen – Daten werden in ein normalisiertes Schema umgewandelt und MITRE ATT&CK® zugeordnet

Datenpool erweitern – Threat-Intelligence-Daten von anderen Anbietern im jeweiligen geschäftlichen Kontext werden berücksichtigt

Korrelieren – Warnmeldungen werden nach Entitäten, MITRE-ATT&CK-Kategorie und Zeit in Cluster gruppiert

Priorisieren – Warnmeldungen und Cluster werden bewertet und nach Priorität sortiert

Eskalieren – Cluster werden anhand logischer Prozesse zu Fällen zur Analyse eskaliert

Rund um die Uhr aktiv – mit sieben globalen Security Operations Centern (SOCs)

Unser global aufgestelltes Team mit über 500 Threat Detection and Response-Experten ist auf sieben Security Operations Center (SOCs) verteilt: Diese befinden sich in den USA, Europa (UK/Irland und Deutschland), Asien und Australien. Unsere Experten sind spezialisiert auf alle Bereiche im Gebiet Cyberbedrohungen, darunter Malware, künstliche Intelligenz und Bedrohungsbereinigung. Damit haben Sie eine außerordentlich fundierte und breitgefächerte Expertise, die sich interne IT-Teams kaum aneignen können.

Branchenweit führende Analyse- und Reaktionszeiten

Dank der einzigartigen Kombination aus menschlicher Expertise, Technologie und Bedrohungserfahrung bereinigt Sophos MDR Bedrohungen in durchschnittlich nur 38 Minuten und sorgt so für effektiven Cyberschutz.

- Durchschnittliche Zeit bis zur Erkennung (Mean Time To Detect, MTTD): 1 Minute
- Durchschnittliche Zeit für die Analyse (Mean Time To Investigate, MTTI): 25 Minuten
- Durchschnittliche Zeit bis zur Reaktion (Mean Time To Respond, MTTR): 12 Minuten

Wer nutzt Sophos MDR?

Unsere MDR-Services werden von Tausenden Unternehmen und Einrichtungen in allen Branchen genutzt – von kleinen Unternehmen mit begrenzten IT-Ressourcen bis hin zu Großkonzernen mit eigener SOC-Abteilung. Die drei beliebtesten Response-Modelle von Sophos MDR sind:

- Sophos MDR verwaltet die Reaktion auf Bedrohungen komplett für den Kunden
- Sophos MDR arbeitet mit dem IT-Team des Kunden zusammen und koordiniert gemeinsam die Reaktionsmaßnahmen
- Sophos MDR unterstützt und ergänzt die interne IT-Security, meldet Vorfälle, die Maßnahmen erfordern, und liefert Informationen zu Bedrohungen sowie Empfehlungen zur Reaktion

Bedrohungsfall: Command-and-Control mit Microsoft Defender erkennen

BRANCHE
Dienstleistungen

HAUPTSITZ
USA

MITARBEITER
750

SERVICESTUFE
Sophos MDR for Microsoft Defender

MIT SOPHOS MDR INTEGRIERTE TELEMETRIE-QUELLEN

✓ Endpoint	X Identität
✓ Firewall	X Cloud
X Email	✓ Netzwerk

Was ist Command-and-Control?

Command-and-Control (auch C&C oder C2) umfasst Techniken, mit denen Angreifer mit den von ihnen kontrollierten Systemen in einem kompromittierten Netzwerk kommunizieren und Befehle an sie senden.

Command-and-Control-Kanäle zwischen einer Zielumgebung und der Infrastruktur des Angreifers können verschiedene Ursachen haben, z. B. Phishing-E-Mails, Social Engineering, Malware, Lücken in Browser-Plugins und vieles mehr. Angreifer nutzen häufig vorhandene Ressourcen und ahmen erwarteten Netzwerkverkehr nach, um unerkannt zu bleiben und keinen Verdacht zu erregen.

ERKENNUNG

Microsoft Defender generiert eine Warnmeldung zur Kommunikation mit einer verdächtigen IP-Adresse.

Die Microsoft-Warnmeldung wird automatisch mit Ereignissen im Sophos XDR Data Lake korreliert, um festzustellen, ob der Angriff von der Firewall des Kunden blockiert wurde und ob mehrere Endpoints betroffen sind.

ANALYSE

Die Analysten von Sophos MDR bestätigen, dass die schädliche Verbindung aus der Microsoft-Defender-Warnmeldung blockiert und die unmittelbare Bedrohung eingedämmt wurde.

Mit SophosLabs Intelix werden die Angriffsfamilie, Indicators of Compromise (IoCs) und bekannte IP-Adressen und Domänen, die von den Angreifern verwendet werden, identifiziert.

Die ursprüngliche Warnmeldung von Microsoft wird mit diesen Bedrohungsdaten angereichert, damit sie für die Ursachenanalyse verwendet werden kann.

REAKTION

Das kompromittierte Gerät wird isoliert und der Angriff eingedämmt.

Sophos MDR bestätigt, dass der Erstzugriff von einer Phishing-E-Mail ausging.
Eine Analyse wird durchgeführt, um die Zusammensetzung der Phishing-E-Mail zu ermitteln und sicherzustellen, dass keine anderen Benutzerkonten gefährdet sind.

Sophos liefert Empfehlungen, um die Wahrscheinlichkeit weiterer Phishing-Angriffe in Zukunft zu minimieren.

Vorteile für Kunden

Ganz gleich, ob Sie Ihr internes Security Operations Team ergänzen und unterstützen oder 24/7 Managed Detection and Response durch ein Experten-Team ohne internes Security Operations Center in Anspruch nehmen möchten – Sophos MDR kann helfen. Unternehmen, die Microsoft Defender durch Sophos MDR ergänzen, erzielen bessere Cybersecurity-Ergebnisse: Sie reduzieren ihre Cyber-Risiken, schöpfen ihre Sicherheitsinvestitionen voll aus und verbessern ihre Konditionen beim Versicherungsschutz.

Komplexe Bedrohungen stoppen – mit Microsoft + Sophos MDR

24/7 Überwachung und Reaktion durch ein Experten-Team
Analysten von Sophos MDR überwachen und priorisieren Warnmeldungen von Microsoft Defender 24/7 und reagieren darauf, indem sie sofortige Maßnahmen ergreifen und bestätigte Bedrohungen stoppen

Erkennen und stoppen Sie Bedrohungen, die von Microsoft Defender nicht erfasst werden
Sophos-eigene Erkennungen, Threat Intelligence und manuelle Threat Hunts bieten zusätzlichen Schutz

Verbessern Sie die Transparenz und kontextualisieren Sie Microsoft-Defender-Warnmeldungen
Zusätzliche, in Ihrer E3- oder E5-Lizenz enthaltene Microsoft-Quellen von Sicherheitsereignissen lassen sich integrieren

Unsere Security-Operations-Experten sind für Sie da
Die Analysten von Sophos MDR bieten 24/7 Telefonsupport. Außerdem stehen detaillierte Reports zur Bedrohungsaktivität in Sophos Central zur Verfügung

Cyber-Risiken reduzieren

Einer der Hauptvorteile von MDR-Services als Ergänzung zu Microsoft Defender ist der bessere Schutz vor Ransomware und anderen komplexen Cyberbedrohungen.

Sophos-Analysten verfügen über einen weitreichenden Erfahrungsschatz, den sich interne IT-Teams kaum aneignen können. Zudem sind sie routiniert im Umgang mit Threat-Hunting-Tools und der Auswertung von Telemetriedaten. So können sie in allen Phasen des Prozesses schnell und gezielt reagieren – vom Erkennen wichtiger Signale bis hin zum Analysieren potenzieller Vorfälle und Beseitigen schädlicher Aktivitäten.

Sophos MDR schützt mehr Unternehmen und Einrichtungen als alle anderen Anbieter. So erreichen wir eine gemeinschaftliche Immunität. Sicherheitsrelevante Erkenntnisse können auch auf andere Kunden angewendet werden, die dem gleichen Zielprofil entsprechen. Auf diese Weise können wir ähnliche Angriffe in dieser Community proaktiv verhindern.

★★★★★

„Die Pentester waren fassungslos, dass sie keine Eintrittspforte finden konnten. Ab da wussten wir, dass wir dem Service von Sophos voll vertrauen können."
University of South Queensland

★★★★★

„Mit Sophos MDR können wir viel schneller auf Bedrohungen reagieren."
Tata BlueScope Steel

★★★★★

„Wir werden in Echtzeit über alle Bedrohungen benachrichtigt."
Bardiani Valvole

Sicherheitsinvestitionen optimal nutzen

Mit Sophos MDR steigern Sie die Effizienz Ihrer Sicherheits-Tools und Ihres IT-Security-Teams.

Die Bedrohungserkennung und -reaktion beansprucht IT-Kapazitäten stark. Sophos MDR schafft hier Abhilfe und setzt wertvolle IT-Ressourcen für strategische Aufgaben frei. MDR-Kunden können unsere Security-Operations-Experten rund um die Uhr telefonisch erreichen und Reports zur Bedrohungsaktivität in der Sophos-Central-Plattform abrufen. So können sie schneller und genauer auf Warnmeldungen reagieren.

Dank Telemetriedaten Ihrer Sicherheitstools von Microsoft und anderen Anbietern beschleunigt Sophos MDR die Bedrohungserkennung und -reaktion, verstärkt Ihre Cyber-Abwehr und steigert gleichzeitig den Return on Investment vorhandener Lösungen.

Die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs belaufen sich derzeit auf 1,85 Mio. US$. Zudem bestätigen 84 % der Unternehmen, die von Ransomware betroffen waren, dass sie dadurch Geschäftseinbußen oder Umsatzverluste verzeichneten.[2] Durch die Investition in einen Service, wie Sophos MDR, senken Unternehmen die Gesamtkosten für die Cybersecurity-Bereitstellung.

★★★★★

„Seit der Einführung von Sophos konnten wir im operativen Bereich erheblich Zeit einsparen. So haben unsere Teams wieder mehr Kapazitäten, um sich Aufgaben zu widmen, die den Studierenden zugutekommen und deren Zufriedenheit erhöhen."

London South Bank University

★★★★★

„Sophos MDR meldet, behebt und entfernt Bedrohungen schnell und zuverlässig. So haben wir mehr Zeit, uns auf wertschöpfende Aufgaben zu konzentrieren."

Tomago Aluminium

Konditionen beim Versicherungsschutz verbessern

Mit Sophos MDR erfüllen Unternehmen viele Kontrollmechanismen, die Versicherer an ihre besten Angebote knüpfen, z. B. 24/7 Detection and Response, Incident-Response-Pläne, Protokollierung und Monitoring, und mehr.

Unsere Kunden schildern uns, dass Versicherer ihnen bessere Konditionen beim Versicherungsschutz bieten, weil sie Cyber-Risiken reduzieren.

★★★★★

„Durch unsere Zusammenarbeit mit Sophos for XDR und MDR konnten wir unsere Cyberversicherungs-Prämien senken, obwohl uns zu Beginn der Partnerschaft gesagt wurde, dass sich die Prämien verdoppeln würden. Das ist ein großer Erfolg, der einen echten Mehrwert darstellt. Sogar unser CFO bedankte sich für unseren Einsatz und MDR trug entscheidend dazu bei."

Bob Pellerin, CISO, The Fresh Market

2 Ransomware-Report 2023, Sophos.

Branchenweit führender MDR-Service

Sophos ist der weltweit führende MDR-Anbieter und schützt mehr Unternehmen als alle anderen Anbieter vor Ransomware, Sicherheitsvorfällen und anderen Bedrohungen, die Technologien allein nicht stoppen können.

Sophos MDR schützt Tausende von Unternehmen aller Branchen weltweit und bietet eine beispiellose Tiefe und Breite an Expertise zu branchenspezifischen Cyberbedrohungen. Dank dieser umfassenden Telemetriedaten erreichen wir eine gemeinschaftliche Immunität: Von einem einzelnen Unternehmen gewonnene Erkenntnisse erhöhen den Schutz für alle Kunden mit einem ähnlichen Profil.

Am wichtigsten sind natürlich die Cybersecurity-Ergebnisse, die wir für unsere Kunden erzielen. Sophos ist die am besten und häufigsten bewertete MDR-Lösung bei Gartner® Peer Insights™ mit einer durchschnittlichen Bewertung von 4.8/5 (300 Bewertungen insgesamt, Stand: 14. Juni 2023). 97 % der Kunden würden uns weiterempfehlen.

Außerdem ist Sophos Leader im G2 Grid® Report für Managed Detection and Response und Leader im G2 Grid für MDR allgemein, für Midmarket und für Enterprise.

Mehr dazu, wie Microsoft-Defender-Kunden von Sophos MDR profitieren können, erfahren Sie unter sophos.de/mdr

Von allen Anbietern die meisten Kunden

Über 17.000 Unternehmen nutzen Sophos MDR (Q2, 2023)

Am besten bewertet

Unabhängige Kundenbewertung von 4.8/5

Am häufigsten bewertet

300 Bewertungen auf Gartner Peer Insights in den letzten 12 Monaten

Starker Schutz dank Sophos Endpoint Protection

Sophos Intercept X Endpoint Protection arbeitet für Sie und mit Ihnen und passt Ihre Abwehr als Reaktion auf einen Angriff an.

Die Lösung bietet leistungsstarken, mehrschichtigen Schutz vor Ransomware und komplexen Bedrohungen in allen Phasen der Angriffskette. Verhaltensbasiertes Ransomware-Rollback, 60 Exploit-Mitigations und mehr sind standardmäßig aktiviert und müssen nicht erst konfiguriert werden.

Unsere innovative Adaptive Attack Protection reagiert dynamisch auf manuelle Angriffe und stellt automatisch zusätzliche Abwehrmechanismen bereit, um Angreifer zu stoppen und IT-Teams Zeit für die Reaktion zu verschaffen.

Sophos-MDR-Kunden mit Microsoft Defender können jederzeit zu Sophos Endpoint Protection wechseln. Dies sorgt für maximale Flexibilität und zukunftssichere Performance Ihrer Security-Lösungen.

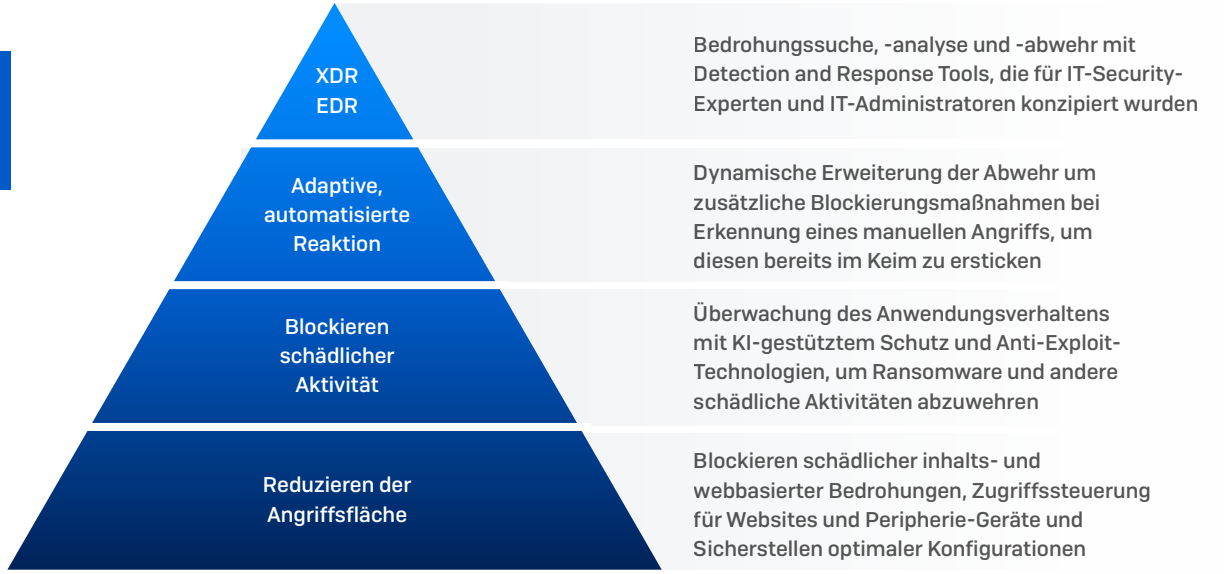
Weitere Informationen und eine kostenlose Testversion finden Sie auf sophos.de/endpoint

✓ Gartner Leader in 13 Reports in Folge
Seit 2008 positionierte sich Sophos in allen Reports als Leader im Gartner Magic Quadrant für EPP

✓ Top-Bewertungen auf Gartner Peer Insights
Unabhängige Kundenbewertung von 4.8/5

✓ G2 Leader für Enterprise, Midmarket und SMB
Basiert ausschließlich auf Kundenbewertungen

✓ Volle Punktzahl bei Schutz – SE Labs
AAA-Bewertung für Enterprise und Small Business Security



Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31. Dezember 2022
GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seiner verbundenen Unternehmen in den USA und international; Magic Quadrant und PEER INSIGHTS sind eingetragene Marken von Gartner, Inc. und/oder seiner verbundenen Unternehmen und werden hier mit Genehmigung verwendet. Alle Rechte vorbehalten.
Gartner befürwortet in seinen Forschungsbeiträgen keine bestimmten Hersteller, Produkte oder Dienstleistungen und rät Technologie-Nutzern nicht ausschließlich zu Anbietern mit besten Bewertungen. Forschungsbeiträge von Gartner sind als Meinungsäußerungen des Gartner Forschungsinstituts einzustufen und in keinem Fall als Tatsachenfeststellung zu werten. Gartner übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.
Gartner Peer Insights geben die subjektiven Meinungen einzelner Enduser wieder, die auf deren eigenen Erfahrungen basieren. Sie sind in keinem Fall als Tatsachenfeststellung zu werten und repräsentieren nicht die Ansichten von Gartner oder seinen verbundenen Unternehmen. Gartner befürwortet in dieser Publikation keine bestimmten Hersteller, Produkte oder Dienstleistungen und übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2023-06-27 (WP-NP)

SOPHOS