SOPHOS

Endpoint Security Buyer's Guide

Cyberbedrohungen werden immer komplexer – damit wächst auch der Druck, sich mit der richtigen Endpoint-Lösung optimal zu schützen. Mittlerweile gibt es im Bereich Endpoint Security allerdings so viele verschiedene Anbieter und Tools, dass es immer schwerer wird, die richtige Lösung für die unternehmensspezifischen Sicherheitsanforderungen zu finden.

Dieser Guide verschafft Ihnen Klarheit, führt Sie durch die wichtigsten Funktionen einer Endpoint-Protection-Lösung und erklärt Ihnen, was Sie zum Schutz vor modernen, komplexen Bedrohungen benötigen. Mit diesen Erkenntnissen sind Sie bestens gerüstet, um eine Entscheidung für Ihr Unternehmen zu treffen.

Sophos-Whitepaper, Juni 2024

Die heutige Bedrohungslandschaft

Wie aus unserer unabhängigen Umfrage unter 3.000 IT-/Cybersecurity-Entscheidern in 14 Ländern hervorgeht, bewegen sich Angreifer in einer anderen Geschwindigkeit als Unternehmen mit ihren IT-Experten. Es zeigt sich, dass IT-Teams mit der Schnelligkeit der Cyberkriminellen nicht mehr mithalten können.

Die Evolution der Cyberkriminalität

In den letzten Jahren hat sich die Cyberkriminalität zu einem regelrechten Wirtschaftszweig entwickelt: Bedrohungsakteure gehen zunehmend professionell vor, sind gut vernetzt und bieten sogar unterstützende Dienstleistungen an.

Genau wie seriöse Technologieunternehmen setzen auch Cyberkriminelle vermehrt auf ein „As-a-Service"-Modell. Dies erleichtert den Einstieg in die Cyberkriminalität und ermöglicht es Bedrohungsakteuren, immer schneller immer mehr Angriffe mit zunehmend schwerwiegenden Folgen auszuführen.

Angreifer sind daher in der Lage, im großen Stil verschiedenste Arten von Angriffen auszuführen. 94 % der Unternehmen waren im vergangenen Jahr von Cyberangriffen betroffen. Ransomware-Angriffe wurden zwar am häufigsten gemeldet, doch verzeichneten Unternehmen auch eine Vielzahl anderer Bedrohungen, wie etwa:[1]

27 %	**27 %**	**26 %**
Schad-E-Mails	Phishing (inkl. Spear-Phishing)	Datenexfiltration (nach Angreifer)
24 %	**24 %**	**21 %**
Cyber-Erpressung	Business Email Compromise	Mobilgeräte-Malware
18 %	**24 %**	**14 %**
CryptoMining	Denial of Service (DDoS)	Wiper

Lesen Sie unseren Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, um mehr zu erfahren.

Ransomware plagt Unternehmen weiterhin

59 % der Unternehmen und Organisationen gaben an, dass sie im letzten Jahr Opfer eines Ransomware-Angriffs waren.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

Wurde Ihr Unternehmen im letzten Jahr von Ransomware getroffen?
Ja. Anzahl=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Im Vergleich zu 2023 wurden 2024 zwar weniger Angriffe gemeldet. Die Gefahr durch Ransomware-Angriffe mit Datenverschlüsselung ist jedoch keinesfalls gebannt; denn in ganzen 70 % dieser Angriffsfälle gelingt es den Cyberkriminellen, Daten erfolgreich zu verschlüsseln.

Zudem werden Ransomware-Angriffe für Unternehmen und Organisationen immer kostspieliger. Die durchschnittlichen Bereinigungskosten beliefen sich auf 2,73 Mio. US$ und fielen damit höher aus als im Vorjahr (1,82 Mio. US$).[2]

Lesen Sie unsere jährliche Ransomware-Studie, den Ransomware-Report 2024, um mehr über die Erfahrungen von Unternehmen im Jahr 2024 sowie über die Häufigkeit, Kosten und Ursachen von Angriffen zu erfahren.

1 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos – Ergebnisse einer unabhängigen Befragungvon 3.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern im Januar und Februar 2023.

2 Ransomware-Report 2024, Sophos – eine unabhängige, anbieterneutrale Befragung von 5.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern. Durchgeführt im Zeitraum Januar bis Februar 2024.

Veraltete Verfahren führen zu schlechten Sicherheitsergebnissen

Das Arbeitsumfeld hat sich in den letzten Jahren für viele Unternehmen verändert. Endbenutzer arbeiten im Büro, mobil oder an Kunden- oder Partnerstandorten. Unternehmensdaten werden nicht mehr ausschließlich lokal, sondern auch in der Cloud und auf Endbenutzer-Geräten gespeichert. Dabei erfolgt der Zugriff auf diese Daten lokal oder remote von verteilten Standorten. Infolgedessen führt das Festhalten an veralteten Cybersecurity-Konzepten häufig zu schlechten Sicherheitsergebnissen.

Am häufigsten haben IT-Security-Teams unter anderem mit den folgenden Problemen zu kämpfen:

- **Fachkräftemangel –** qualifizierte IT-Mitarbeiter sind nach wie vor Mangelware. Ohne die nötige Expertise können Mitarbeiter möglicherweise nicht feststellen, ob eine Sicherheitswarnung schädlich oder harmlos ist.
- **Flut von Fehlalarmen –** Zu viele Warnmeldungen von unterschiedlichen Systemen überfordern Benutzer, die die zu untersuchenden Signale/Warnmeldungen oft nicht priorisieren können und so Indikatoren für einen Angriff möglicherweise nicht erkennen.
- **Nicht korrelierte Daten –** Bedrohungssignale/Warnmeldungen beschränken sich auf bestimmte Technologien. IT-Teams verfügen daher nicht über die nötige Transparenz, um schnell auf Warnmeldungen oder Vorfälle reagieren zu können.
- **Mangelnde Integration –** Sicherheitstools lassen sich nicht miteinander verbinden oder in die IT-Infrastruktur eines Unternehmens integrieren, was die Komplexität erhöht.
- **Manuelle Prozesse –** IT-Teams verbringen viele Stunden damit, Ereignisse, Protokolle und Informationen miteinander zu korrelieren, um Geschehnisse nachzuvollziehen. Dadurch werden Angriffe nicht schnell genug erkannt und die Reaktion verzögert sich.
- **Reaktive Maßnahmen –** aufgrund der oben genannten Punkte geraten viele IT-Teams ins Hintertreffen und reagieren auf Bedrohungen erst, nachdem bereits Schaden entstanden ist, statt sie früher in der Angriffskette zu stoppen.
- **Fokus auf Akutmaßnahmen –** IT-Teams sind mit den täglichen Aufgaben zur Bedrohungsbekämpfung ausgelastet und können sich nicht auf langfristige Verbesserungen konzentrieren. Zudem fehlt es oft an der Zeit, die Ursache eines Vorfalls zu ermitteln und die ergriffenen Maßnahmen zu dokumentieren. So lassen sich strukturelle Probleme nicht einfach angehen.
- **Verteilte Daten –** Benutzer und Geräte sind überall. Daten werden lokal, in der Cloud und auf Geräten gespeichert. Der Zugriff auf diese Daten erfolgt lokal und über Remote-Access-Lösungen.

Die gute Nachricht ist, dass sich viele dieser Probleme mit einer leistungsstarken Endpoint-Protection-Lösung beheben lassen.

Was muss Endpoint Protection leisten?

Endpoint-Security-Lösungen müssen für Sie und mit Ihnen arbeiten und Abwehrmechanismen als Reaktion auf Angriffe anpassen. Eine moderne Endpoint-Security-Lösung muss daher auf jeden Fall folgende präventive Cybersecurity-Funktionen bieten:

Reduzieren der Angriffsfläche – Blockieren schädlicher inhalts- und webbasierter Bedrohungen sowie Zugriffssteuerung für Anwendungen, Websites, Peripherie-Geräte und mehr.

Blockieren schädlicher Aktivitäten – Schutz vor Exploits und Techniken von Cyberkriminellen und Ransomware: Spezifische Aktivitäten werden erkannt und gestoppt, bevor Schaden entsteht.

Adaptive, automatisierte Reaktion – Ihre Abwehrmechanismen sollten automatisch auf Bedrohungen reagieren und sich an Veränderungen im Angreiferverhalten anpassen. Dies stört Angreifer. Zudem kann Ihr Team über den Angriff informiert werden und Sie gewinnen wertvolle Zeit für die Reaktion.

Basis für die Bedrohungssuche (intern oder verwaltet) – Aussagekräftige Signale und Sicherheitsinformationen können die Bedrohungserkennung und -reaktion erheblich beschleunigen. Je mehr Einblicke IT-Teams haben, desto schneller können sie reagieren.

Optimaler Cyberschutz

Nachdem wir uns jetzt angeschaut haben, was eine Endpoint-Protection-Lösung auf funktionaler Ebene leisten sollte, möchten wir Ihnen einen umfassenden Überblick darüber verschaffen, wie Ihr Unternehmen von Endpoint Protection profitieren kann. Eine starke Endpoint Protection sollte für optimale Sicherheitsergebnisse sorgen.

Cyberrisiko senken

Eine effektive Endpoint Protection reduziert Ihr Cyberrisiko und schützt Sie vor einer Vielzahl an Cyberbedrohungen.

Präventive Cybersecurity

Je eher Sie einen Angriff stoppen, desto weniger Arbeit fällt im Nachgang an. Starke Endpoint Protection umfasst mehrere Schutzebenen und wehrt so Cyberbedrohungen und Angriffe ab, die auf Computer, Laptops, Mobilgeräte und Server abzielen. Endpoint Protection schützt diese Geräte und ihre Daten vor Malware, Viren, Ransomware und anderen schädlichen Aktivitäten.

Änderungen am Sicherheitsstatus erkennen

Im Laufe der Zeit kann sich der Sicherheitsstatus aus diversen Gründen ändern. Laut einer aktuellen, unabhängigen Befragung wird die Fehlkonfiguration von Sicherheitstools im Jahr 2023 als das größte Sicherheitsrisiko wahrgenommen.[2]

Suchen Sie nach einer Endpoint-Security-Lösung, die Ihren Sicherheitsstatus kontinuierlich bewertet und Ihre Konfiguration optimiert. Automatisierung ist hier entscheidend, um lückenlose IT-Security zu gewährleisten, Ihr Cyberrisiko zu reduzieren und aufwändige, manuelle Aufgaben zu minimieren.

2 Ransomware-Report 2024, Sophos – eine unabhängige, anbieterneutrale Befragung von 5.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern. Durchgeführt im Zeitraum Januar bis Februar 2024.

Schlanke Verwaltung

Mit einer zentralen Management-Konsole können IT-Administratoren Sicherheitseinstellungen, Richtlinien, Ausschlüsse und Bedrohungswarnungen über alle Endpoints hinweg überwachen und verwalten. Dies vereinfacht das Sicherheitsmanagement, verringert das Risiko von Fehlkonfigurationen und gewährleistet einen konsistenten Schutz. Einige zentrale Management-Konsolen gehen noch einen Schritt weiter: Sie überprüfen Ihre Sicherheitslage automatisch und melden potenziell riskante Aktivitäten oder Richtlinienänderungen.

Erkennung und Reaktion beschleunigen

Wenn ein Angreifer in Ihre Umgebung gelangt ist, zählt jede Sekunde. Hochwertige Endpoint Protection umfasst präventive Security-Funktionen, filtert Unnötiges heraus und liefert so relevante Warnmeldungen. Mit Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) können diese Warnmeldungen analysiert werden.

Einige Lösungen gehen einen Schritt weiter und priorisieren Erkennungen automatisch mit Hilfe von künstlicher Intelligenz (KI) und Bedrohungsinformationen. Mit solchen Lösungen können IT-Teams schnell feststellen, worauf sie sich konzentrieren sollten, und die Reaktion auf Bedrohungen durch Experten wird beschleunigt.

IT-Effizienz steigern

64 % der Unternehmen möchten, dass ihre IT-Abteilungen mehr Zeit für strategische Projekte statt für fieberhafte Akutmaßnahmen gegen Cyberangriffe aufwenden.[3] Automatisierter, benutzerfreundlicher Endpoint-Schutz hilft IT-Teams, dieses Ziel zu erreichen.

Erstklassige Endpoint-Lösungen blockieren und bereinigen die meisten Bedrohungen automatisch im Vorfeld. Dadurch werden IT-Kapazitäten freigesetzt, sodass IT-Teams geschäftskritische Aufgaben priorisieren können. Technologien wie XDR reduzieren die Flut irrelevanter Daten und setzen so Kapazitäten für wichtige Projekte frei.

Diese gesteigerte Effizienz ermöglicht es IT-Abteilungen letztendlich, von reaktiver zu proaktiver Cybersicherheit zu wechseln. Dies verschafft IT-Teams Zeit, Bedrohungen aufzuspüren, bevor sie langfristigen Schaden verursachen. Dadurch verringert sich wiederum das Cyberrisiko.

3 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos – Ergebnisse einer unabhängigen Befragung von 3.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern im Januar und Februar 2023.

Cybersecurity ROI maximieren

Leistungsstarke Cybersicherheit sollte Unternehmen vor den finanziellen und betrieblichen Folgen von Sicherheitsvorfällen schützen.

In erstklassige Endpoint Protection zu investieren, ist ein wesentlicher Faktor. Denn gezielte Prävention kostet erheblich weniger als die Bereinigung von Vorfällen. Starke Endpoint Protection blockiert die meisten Bedrohungen im Vorfeld und reduziert die Wahrscheinlichkeit von potenziell kostspieligen Angriffen.

Darüber hinaus lassen sich branchenführende Endpoint-Protection-Lösungen in Ihre bestehenden Sicherheitssysteme integrieren und können mit diesen kommunizieren. Dies sorgt für mehr Schutz und reduziert die Komplexität. Ihre vorhandenen Schutztechnologien (wie E-Mail-, Firewall-, Netzwerk-, Identity- und Cloud-Produkte) arbeiten so smarter und besser zusammen.

All diese Faktoren steigern den Cybersecurity ROI und senken gleichzeitig die Gesamtbetriebskosten.

Cyber-Versicherungsschutz optimieren

Cyber-Versicherungsprämien sind in den letzten Jahren deutlich gestiegen und die Anwendung von Policen ist komplexer und zeitaufwändiger geworden. Versicherer fordern striktere Cyber-Kontrollmechanismen. So bestätigten 95 % der Unternehmen, die im letzten Jahr eine Versicherung abgeschlossen hatten, dass die Qualität ihrer Abwehrmaßnahmen direkten Einfluss auf ihren Versicherungsstatus hatte[4].

Die besten Versicherungskonditionen erzielen Sie, indem Sie Cyberrisiken minimieren. Durch die Investition in starke Abwehrmaßnahmen, einschließlich 24/7 Sicherheitsservices und führender Detection and Response Tools, erhalten Sie bessere Konditionen bei Cyber-Versicherungen:

1. Erleichtert den Abschluss von Cyber-Versicherungen
2. Kann Prämien reduzieren und die Konditionen verbessern
3. Verringert die Wahrscheinlichkeit von Schadenfällen – und die daraus resultierenden höheren Prämien
4. Reduziert das Risiko, dass die Versicherung nicht zahlt

Branchenführende Endpoint-Protection-Technologien schaffen die Basis für Erkennungs- und Reaktionsfunktionen. Achten Sie darauf, dass die Lösung Ihrer Wahl diese Funktionen bietet. Die meisten Cyber-Versicherer setzen heutzutage Endpoint Detection and Response (EDR) voraus. Ohne EDR können Unternehmen in der Regel nur schwer eine Cyber-Versicherung abschließen.

Services, die die Erkennung und Reaktion optimieren und somit das Risiko eines Cybervorfalls minimieren, stehen bei Cyber-Versicherern besonders hoch im Kurs. Insbesondere Unternehmen, die Managed Detection and Response (MDR) Services in Anspruch nehmen, gelten bei Versicherern häufig als Premium-Kunden, da sie das geringste Risiko darstellen.

Suchen Sie nach Anbietern, die einen nahtlosen Upgrade-Pfad von einer Endpoint-Protection-Lösung zu einem rund um die Uhr verfügbaren, vollständig verwalteten Service bieten. Dieser sollte Threat Hunting, Detection und/oder Incident Response umfassen und mit vorhandenen Lösungen und Sicherheits-Tools von anderen Herstellern genutzt werden können.

5 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.

Endpoint Security bewerten: 10 Fragen, die Sie stellen sollten

Nachdem Sie jetzt eine klarere Vorstellung davon haben, welche Funktionen eine leistungsstarke Endpoint-Security-Lösung umfassen sollte, geben wir Ihnen im Folgenden Fragen an die Hand, die Sie den Anbietern auf Ihrer Auswahlliste stellen können.

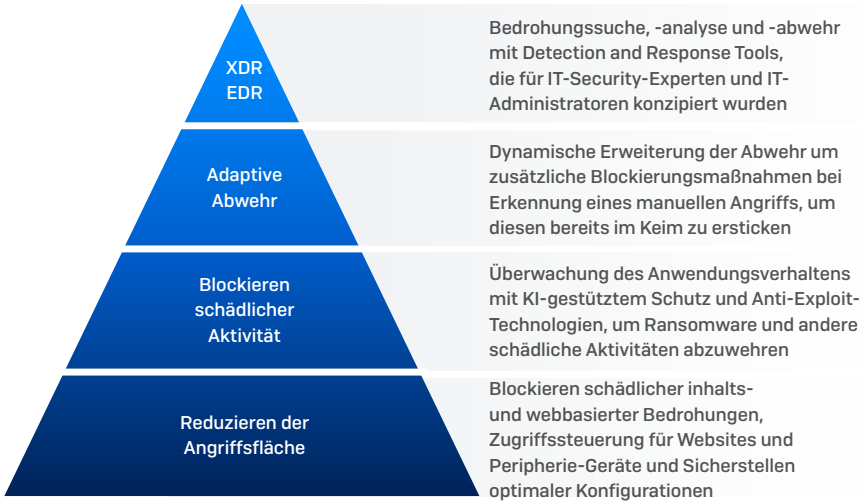
1. Basiert das Produkt auf einem mehrschichtigen, präventiven Ansatz? Oder konzentriert es sich auf Erkennungen? Welche speziellen Funktionen stehen im Mittelpunkt der Technologie?
2. Kann das Produkt Änderungen am Sicherheitsstatus erkennen und automatisch darauf reagieren? Kann es Änderungen an Richtlinien-Einstellungen hervorheben, die das Risiko erhöhen?
3. Reagiert das Produkt automatisch auf eine Bedrohung? Kann es Bedrohungen automatisch entfernen und auf Vorfälle reagieren?
4. Verfügt das Produkt über Abwehrmechanismen, die sich automatisch anpassen, wenn ein manueller Angriff erkannt wird?
5. Verfügt das Produkt über moderne Anti-Ransomware- und Anti-Exploit-Funktionen, einschließlich Echtzeitschutz vor Remote-Ransomware-Angriffen? Sind diese Funktionen standardmäßig aktiviert? Müssen diese Funktionen aktiviert und trainiert werden, bevor sie in Ihrer Umgebung eingesetzt werden?
6. Wie viele Konsolen werden zur Verwaltung des Produkts benötigt? Werden die Konsolen in der Cloud gehostet oder ist eine lokale Installation erforderlich?
7. Ermöglicht das Produkt einen nahtlosen Wechsel zu EDR/XDR und nutzt es eine zentrale Management-Konsole und einen einzigen Agenten auf dem Endpoint/Server?
8. Integriert die XDR-Funktion Warnungen von nativen und Drittanbieter-Sicherheitskontrollen und liefert es Ihnen so ein vollständiges Bild Ihrer Umgebung?
9. Bietet das Produkt einen nahtlosen Upgrade-Pfad zu einem rund um die Uhr verfügbaren, vollständig verwalteten Threat Hunting, Detection und Incident Response Service, der mit vorhandenen Lösungen und Sicherheits-Tools von anderen Herstellern genutzt werden kann?
10. Wurde die Endpoint-Security-Strategie des Anbieters von unabhängigen Testinstituten, Analysten und Kunden validiert?

Der Ansatz von Sophos

Sophos nutzt einen umfassenden Ansatz zum Schutz Ihrer Endpoints. Sophos Endpoint bietet einzigartigen Schutz vor komplexen Cyberangriffen. Mit lückenlosem Ransomware-Schutz und umfassenden Abwehrmaßnahmen stoppen Sie die meisten Bedrohungen bereits, bevor sie Ihre Systeme beeinträchtigen. Leistungsstarke EDR- und XDR-Tools ermöglichen Ihrem Team, Bedrohungen schnell und präzise zu suchen, zu analysieren und darauf zu reagieren.

Präventive Cybersecurity

Sophos Endpoint nutzt einen umfassenden Ansatz zum Schutz Ihrer Endpoints und verlässt sich nicht auf eine einzelne Sicherheitstechnologie. Da mehr Bedrohungen im Vorfeld gestoppt werden, müssen IT-Teams mit begrenzten Ressourcen weniger Vorfälle untersuchen und beheben.



Reduzieren der Angriffsfläche

Sophos Endpoint reduziert die Angriffsfläche. So haben Angreifer keine Chance, in Ihre Umgebung vorzudringen. Die Lösung blockiert schädliche inhalts- und webbasierte Bedrohungen. Zudem können Sie den Zugriff auf Anwendungen, Websites und Peripherie-Geräte steuern.

Blockieren webbasierter Bedrohungen und Webzugriffs-Kontrolle

Es gibt eine Vielzahl webbasierter Bedrohungen. Unternehmen setzen häufig auf Next-Generation Firewalls, um ihre Benutzer, die im Büro arbeiten, vor Phishing, schädlichen Websites und anderen webbasierten Bedrohungen zu schützen. Dies umfasst die Endgeräte in Büronetzwerken. Endpoints können jedoch auch zu Hause, unterwegs, in Cafés usw. genutzt werden – eine Firewall bietet hier keinen Schutz.

Sophos Endpoint blockiert den Zugriff auf Phishing- und schädliche Websites durch die Analyse von Dateien, Webseiten und IP-Adressen. Unsere Technologie schützt Endpoints kontinuierlich, unabhängig vom Standort.

Darüber hinaus liefern die SophosLabs und das Sophos MDR-Team Echtzeit-Bedrohungsdaten zum Schutz vor neuen Bedrohungen.

Zugriffssteuerung für Websites, Peripherie-Geräte und Anwendungen

Mit Sophos-Lösungen können Sie Aktivitäten auf Endpoints einschränken. Diese Kontrollmechanismen werden in der Regel auf die Nutzungsrichtlinien eines Unternehmens abgestimmt.

Der erste Kontrollmechanismus ist die Überwachung und/oder Sperrung des Zugriffs auf Website-Kategorien (Glücksspiele, soziale Medien usw.). Mit Sophos Endpoint können Sie Website-Kategorien überwachen und blockieren, und zwar sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks.

Die Kontrolle des Zugriffs auf Wechselmedien und Peripheriegeräte kann die Angriffsfläche weiter reduzieren. Ein Beispiel: Ein Benutzer schließt einen Drucker oder ein USB-Speichergerät an oder lädt sein Smartphone über einen USB-Anschluss auf. Sind diese Aktionen zulässig? Diese Funktion verhindert nicht nur, dass ein Angriffsvektor schädlichen Code auf einen Endpoint überträgt, sondern kann auch die Exfiltration von Unternehmensdaten blockieren.

Eine weitere Kategorie, die Sie berücksichtigen sollten, sind Anwendungen. Mit Application Control können Sie die Ausführung von Anwendungen oder Browser-Plug-ins auf Unternehmensgeräten blockieren. Denken Sie in Sachen Datenexfiltration etwa an Anwendungen wie OneDrive oder Google Drive für die Cloud-Speicherung. Oder an Torrent-Programme, Tor-Browser usw. Sollte deren Nutzung auf Ihren Endgeräten erlaubt werden? Es gibt eine Vielzahl von Webbrowser-Plug-ins. Viele dieser Plug-ins sind seriös und nützlich, jedoch nicht alle.

Blockieren schädlicher Aktivitäten

Die nächste Verteidigungsebene umfasst künstliche Intelligenz, Verhaltensanalysen, Anti-Ransomware, Anti-Exploit und weitere Technologien, die Bedrohungen schnell stoppen, bevor diese sich ausweiten.

Sophos setzt auf KI-gestützten Schutz, wobei ausführbare Dateien zunächst von der KI klassifiziert werden. Unser KI-Modell wurde mit Millionen bekanntermaßen unbedenklichen und schädlichen ausführbaren Dateien trainiert. Die künstliche Intelligenz erkennt schädliche ausführbare Dateien schnell und effektiv anhand ihrer Eigenschaften – ganz ohne Signaturen.

Lückenloser Ransomware-Schutz

Sophos Endpoint bietet die zuverlässigste Zero-Touch-Endpoint-Abwehr gegen lokale und Remote-Ransomware. Die integrierte Technologie CryptoGuard erkennt Anzeichen einer Verschlüsselung, unabhängig von der Quelle. Dieser universelle Ansatz stoppt neue Varianten und sowohl lokale als auch Remote-Ransomware. Änderungen an Datei-Inhalten werden in Echtzeit überprüft, um schädliche Verschlüsselungen zu erkennen. Außerdem wird auf einem anderen Gerät ausgeführte Remote-Ransomware blockiert, die versucht, Dateien über das Netzwerk zu verschlüsseln. Mit Ransomware verschlüsselte Dateien werden automatisch wieder in ihren unverschlüsselten Zustand versetzt – unabhängig von Größe oder Dateityp. So werden Betriebsstörungen auf ein Minimum reduziert. Außerdem schützt die Lösung den Master Boot Record (MBR) vor Verschlüsselung im Rahmen von Ransomware-Angriffen.

Anti-Exploit

Anti-Exploit-Technologie stoppt die Verhaltensweisen und Techniken, mit denen Angreifer Geräte kompromittieren, Zugangsdaten stehlen und Malware in Umlauf bringen. Sophos setzt neuartige Anti-Exploit-Funktionen auf Geräte-Ebene in großem Maßstab für alle Anwendungen ein. Sophos baut mit seiner direkt einsatzbereiten Cybersecurity auf dem Basisschutz von Microsoft Windows auf und bietet darüber hinaus mindestens 60 zusätzliche vorkonfigurierte und abgestimmte Exploit-Abwehrfunktionen. Sophos schützt Ihr Unternehmen vor dateilosen Angriffen und Zero-Day-Exploits, indem die verwendeten Techniken entlang der gesamten Angriffskette gestoppt werden.

Adaptive Abwehr

Diese zusätzlichen dynamischen Abwehrmaßnahmen sind bislang branchenweit einmalig. Sie bieten automatisierten Schutz, der sich an den Kontext eines Angriffs anpasst. 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.

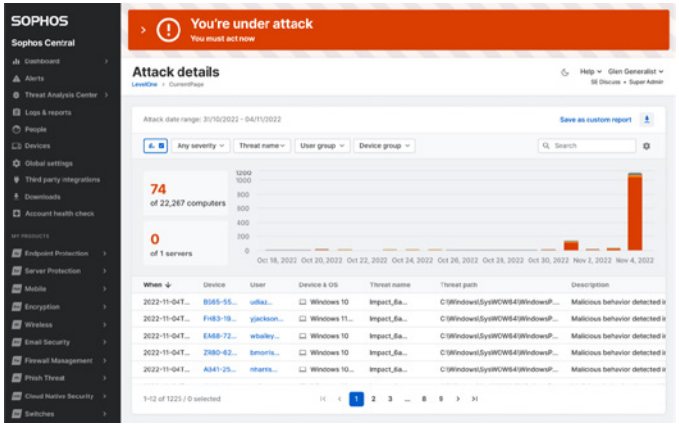
	VERHALTENSERKENNUNG	ADAPTIVE ATTACK PROTECTION	WARNUNG VOR KRITISCHEM ANGRIFF
UMFANG	EINZELGERÄT	EINZELGERÄT	EINZELGERÄT
LEISTUNGEN	Die verhaltensbasierte Engine blockiert die frühen Phasen aktiver Angriffe	Verstärkt die Schutzfunktion, um Schaden zu vermeiden	Warnt Kunden bei Angriffen, auf die sofort reagiert werden muss
AUSLÖSER	Verhaltensregeln	Hacking-Toolsets erkannt	Relevante Indikatoren aktiver Angreifer, einschließlich Korrelationen und Schwellenwerte auf Organisationsebene
ANALOGIE	„SCHILDE AN!“	„Schilde hoch!“	„Alarmstufe Rot!“

Adaptive Attack Protection

So verstärkt die Adaptive Attack Protection die Sicherheit dynamisch, wenn ein manueller Angriff auf einem Endpoint erkannt wird. Dadurch wird verhindert, dass ein Angreifer weitere Maßnahmen ergreifen kann, da die Angriffsfläche minimiert und der Angriff unterbrochen und eingedämmt wird. So gewinnen Sie wertvolle Zeit, um Reaktionsmaßnahmen zu ergreifen.

Warnung vor kritischem Angriff

Ein Critical Attack Warning erfolgt, wenn Angriffsaktivitäten auf mehreren Endpoints oder Servern in der gesamten Umgebung sowie relevante Indikatoren beobachtet werden. Es handelt sich um Alarmstufe Rot: Sie werden angegriffen! In diesem Fall werden Sie automatisch benachrichtigt und erhalten genaue Angaben zur Bedrohungslage und zum Kontext. Sie können mit Sophos XDR selbst Reaktionsmaßnahmen ergreifen oder sich an Ihren Partner oder unser Incident-Response-Team wenden, wenn Sie Unterstützung bei der Reaktion auf einen Vorfall benötigen.



Total Cost of Ownership senken

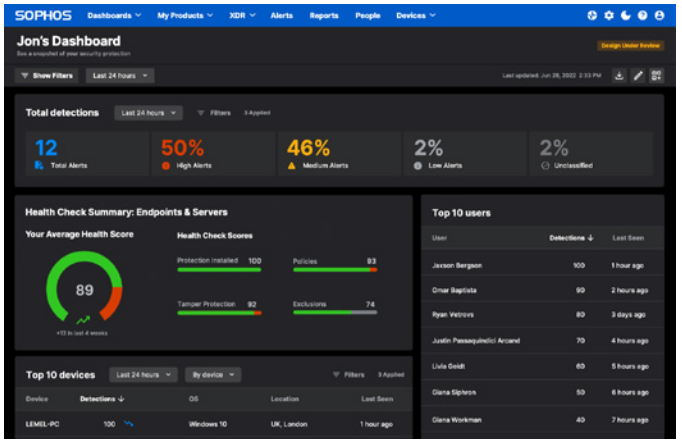
IT- und Sicherheitsteams sind nicht selten überlastet. Automatisierung, Zeitersparnis und Aufwandsminimierung spielen bei Sophos Endpoint eine zentrale Rolle. Dank der Automatisierung oder Minimierung manueller Workflows können sich IT- und Sicherheitsteams auf andere geschäftskritische Aufgaben konzentrieren.

Sophos Central ist eine cloudbasierte Management-Plattform zur Verwaltung Ihrer Sophos-Produkte (Endpoints, Server, Mobilgeräte, Firewalls, Switches, Access Points, E-Mail und Cloud), einschließlich Sophos Endpoint. Über eine einzige, zentrale Konsole können Sie Richtlinien erstellen und verwalten, Erkennungen und Warnmeldungen anzeigen, potenzielle Bedrohungen analysieren und beseitigen und andere Aktionen in Ihren Sophos-Produkten durchführen.

Unsere empfohlenen Schutztechnologien sind standardmäßig aktiviert, was die Einrichtung enorm erleichtert. So verfügen Sie sofort über die stärksten Schutzeinstellungen, ohne eine Feinabstimmung vornehmen zu müssen. Bei Bedarf ist eine granulare Kontrolle verfügbar.

Änderungen am Sicherheitsstatus erkennen

Im Laufe der Zeit kann sich der Sicherheitsstatus im Unternehmen ändern, beispielsweise wenn es zu Abweichungen von der optimalen Konfiguration oder Compliance kommt. Schlecht konfigurierte Richtlinien-Einstellungen, Ausschlüsse und andere Faktoren können Ihre Sicherheit beeinträchtigen. Der Sophos Account Health Check erkennt Security-Posture-Abweichungen und risikoreiche Fehlkonfigurationen, die sich mit einem Klick beheben lassen.

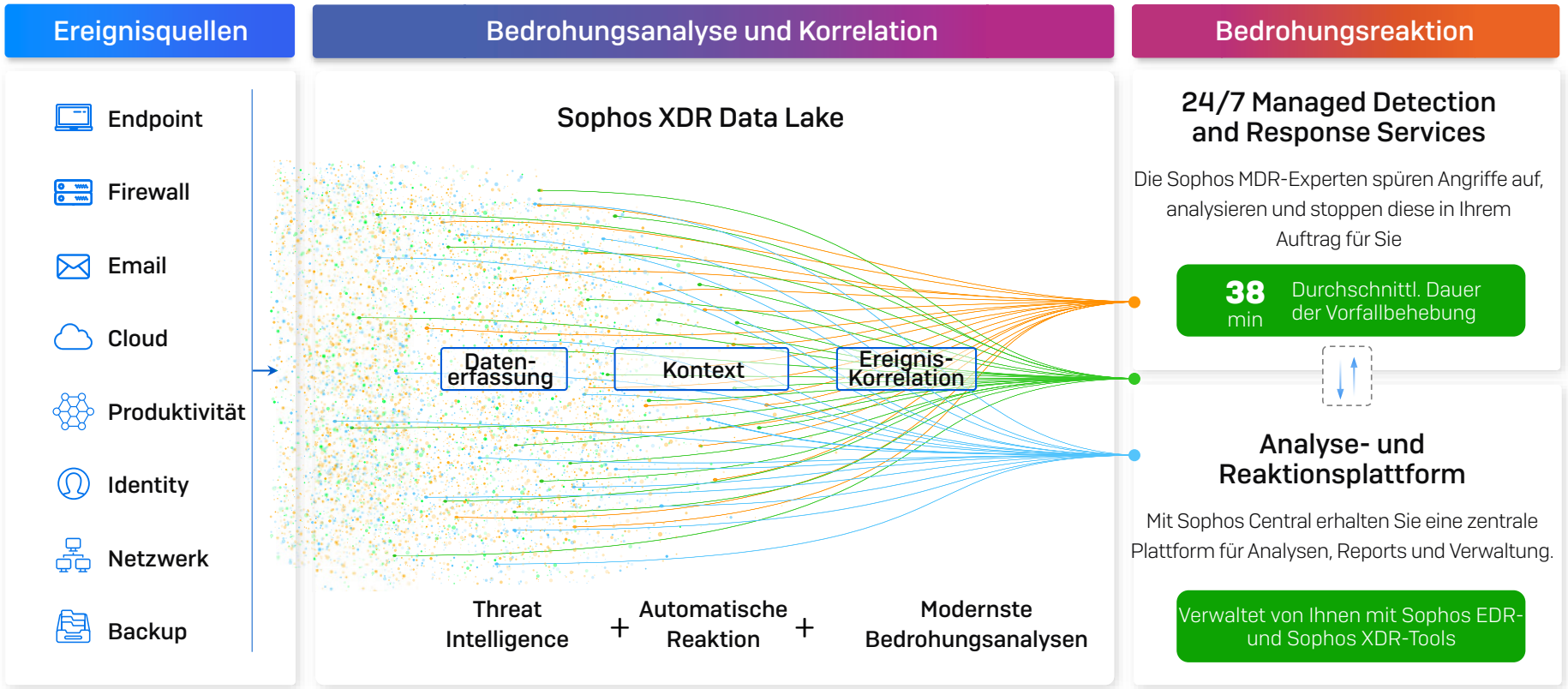


Synchronized Security

Sophos-Lösungen arbeiten perfekt zusammen. Sophos Endpoint tauscht Status- und Integritätsinformationen mit der Sophos Firewall, Sophos ZTNA und anderen Produkten aus, um die Transparenz über Bedrohungen und die Anwendungsnutzung zu erhöhen. Synchronized Security isoliert kompromittierte Geräte während der Bereinigung automatisch und gibt den Netzwerkzugriff wieder frei, sobald die Bedrohung beseitigt wurde – ganz ohne Eingreifen des Administrators.

Erkennung und Reaktion beschleunigen: EDR, XDR und MDR

Die präventive Cybersecurity von Sophos stoppt zahlreiche Bedrohungen bereits im Vorfeld. So können sich IT- und Sicherheitsteams auf die Analyse relevanter Erkennungen konzentrieren.



Der Ansatz von Sophos zur Prävention, Erkennung und Reaktion

Sophos Endpoint Detection and Response (EDR)

Sophos kombiniert leistungsstarke Erkennungs- und Reaktionsfunktionen mit der robusten, präventiven Cybersecurity von Sophos Endpoint. So können Sie nach verdächtigen Aktivitäten auf Endpoints und Servern suchen, diese analysieren und darauf reagieren. Erkennungen werden mit KI-basierten Analysen priorisiert, damit Sie sehen, wo Sie Ihre wertvolle Zeit und Ressourcen am besten einsetzen sollten. Benutzer können per Remote-Zugriff auf Geräten Analysen vornehmen, Software (de)installieren oder Probleme beheben.

Sophos Extended Detection and Response (XDR)

Unternehmen, die umfassendere Erkennungs- und Reaktionsfunktionen wünschen, können mit Sophos XDR nach verdächtigen Aktivitäten und mehrphasigen Angriffen in der gesamten Umgebung suchen, diese analysieren und darauf reagieren. Die Lösung wurde von Sicherheitsexperten für Sicherheitsexperten entwickelt und nutzt als branchenweit einziges Security-Operations-Tool Telemetriedaten von anderen Herstellern und Sophos-Lösungen zur Beschleunigung der Bedrohungserkennung und -reaktion. 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 erheblich steigern können.

Sophos Managed Detection and Response (MDR)

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

Sophos XDR und MDR lassen sich individuell auf Ihre Bedürfnisse zuschneiden und in Ihre vorhandenen Technologien (einschließlich E-Mail-, Firewall-, Netzwerk-, Identity- und Cloud-Produkte) integrieren. So steigern Sie den ROI aus Ihren Cybersecurity-Investitionen.

Sophos Incident Response Service Retainer

Als jährliche Subscription bietet der Sophos Incident Response Services Retainer Kunden mit Sophos Endpoint, EDR und XDR im Bedarfsfall schnellen Zugang zu Incident-Response-Experten. Diese werden auf Basis vorab vereinbarter Service-Konditionen umgehend in Ihrer Umgebung aktiv, um akute Angriffe schnellstmöglich zu stoppen und den Normalbetrieb wiederherzustellen.

Warum Sophos?

Sophos ist ein weltweit führender Anbieter von modernsten Cybersecurity-Lösungen, einschließlich MDR, Incident Response sowie Endpoint-, Netzwerk-, E-Mail- und Cloud-Security-Technologien, die Unternehmen bei der Abwehr von Cyberangriffen unterstützen. Als einer der größten ausschließlich auf Cybersicherheit spezialisierten Anbieter schützt Sophos weltweit mehr als 550.000 Unternehmen und Einrichtungen und mehr als 100 Mio. Benutzer vor aktiven Angreifern, Ransomware, Phishing, Malware und mehr. Maximale Transparenz über die Bedrohungslandschaft sorgt für aussagekräftige Bedrohungsinformationen, die die Schutzfunktionen unserer Produkte und Services für unsere Kunden optimieren.

Unabhängige Tests

Seriöse Tests von unabhängigen Testinstituten können Sie dabei unterstützten, eine fundierte Entscheidung über Ihre Technologie- und Sicherheitsinvestitionen zu treffen. Da die Anzahl und Komplexität von Angriffen stetig zunimmt, können nur dann aussagekräftige Ergebnisse erzielt werden, wenn Tests die realen Gegebenheiten des Unternehmens widerspiegeln.

SE Labs

SE Labs zählt zu den wenigen Sicherheitstestern in der Branche, die moderne Angriffstools und -taktiken, -techniken und -verfahren (TTPs) von Cyberkriminellen und Penetrationstestern simulieren.

Im aktuellen Endpoint Security Report von SE Labs (Januar bis März 2024) wurde unsere Schutzlösung erneut als branchenweit führend eingestuft und erhielt in den Kategorien „Enterprise“ und „SMB“durchgehend AAA-Bewertungen. Sie finden die SE Labs-Report für das 1. Quartal 2024 hier:

Endpoint Security: Enterprise | Endpoint Security: Small Business

MITRE Engenuity ATT&CK Evaluations

Sophos erzielte bei den 2023 MITRE Engenuity ATT&CK Evaluations for Enterprise (Turla) herausragende Ergebnisse. Sophos XDR erkannte 99 % der Bedrohungsaktivitäten und meldete 141 von 143 Teilschritten des Angriffs. Außerdem konnte Sophos XDR zeigen, dass es Sicherheitsteams umfassende Details zur Angriffsursache und zur Vorgehensweise der Angreifer liefert. Die Lösung verzeichnete 98 % Erkennungen in der Kategorie umfassende „Analytic Coverage“.

Die MITRE Engenuity ATT&CK Evaluations gehören zu den weltweit angesehensten unabhängigen Sicherheitstests. Grund dafür ist insbesondere die durchdachte Gestaltung und Nachbildung realer Angriffsszenarien, die Transparenz der Ergebnisse und die Fülle der Teilnehmerinformationen.

Awards und Analyseberichte

Gartner

- ✓ Zum dreizehnten Mal in Folge als ein Leader im Gartner Magic Quadrant for Endpoint Protection Platforms eingestuft
- ✓ Customers' Choice in den Gartner® Peer Insights™ Voice of the Customer Reports for Endpoint Protection Platforms (EPP), 2022, 2023 und 2024

IDC

- ✓ Ein Leader im IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses 2024

G2

- ✓ Overall Leader | Endpoint Protection Suites: Grid-Reports vom Frühjahr und Herbst 2023
- ✓ Overall Leader | EDR: Grid-Reports vom Frühjahr und Herbst 2023
- ✓ Overall Leader | XDR: Grid-Report, Herbst 2023
- ✓ Overall Leader & beste Lösung | XDR: Grid-Report, Frühjahr 2023

Omdia

- ✓ Overall Leader | Comprehensive Extended Detection and Response (XDR) Platforms, November 2022

CRN Tech Innovators Awards 2023

- ✓ Die beste Endpoint Protection am Markt: Sophos Intercept X

ChannelPro Readers' Choice Awards

- ✓ Sophos Intercept X erhält als Best Endpoint Security Vendor „Gold Winner"-Status

Kundenmeinungen

★★★★★

„Die beste Funktion der Endpoint Protection von Sophos ist der Schutz vor komplexen Bedrohungen. Sophos setzt auf eine Kombination aus modernsten Technologien wie maschinellem Lernen, Verhaltensanalyse und signaturbasierter Erkennung, um schädliche Bedrohungen zu erkennen und zu blockieren."

Software-Entwickler | Finanzwesen (Non-Banking) | Vollständige Bewertung auf Gartner Peer Insights lesen

★★★★★

„Eine zentrale Lösung zum Schutz vor komplexen Cyberbedrohungen."

Netzwerk-Administrator | Bildungswesen | Vollständige Bewertung auf Gartner Peer Insights lesen

★★★★★

„Ich bin sehr zufrieden. Die Lösung reduziert die Angriffsfläche und verhindert, dass sich Angriffe innerhalb des Netzwerks unseres Unternehmens ausbreiten. Besonders positiv ist, dass Anti-Ransomware und Deep-Learning-KI Angriffe stoppen, bevor sich diese auf das System auswirken."

ICT Security Office | Rundfunkmedien | Vollständige Bewertung auf G2 lesen

★★★★★

„Sophos ist eine äußerst benutzerfreundliche und dennoch leistungsstarke Endpoint-Lösung."

IT Operations Manager | Mittelständisches Unternehmen | Vollständige Bewertung auf G2 lesen

★★★★★

„Sophos Endpoint reduziert unsere Anfälligkeit für Angriffe und sorgt so für die Gewissheit, dass die Systeme unserer Kunden vor Bedrohungsakteuren geschützt sind."

Manager of Systems Management and Backup & Recovery | Unternehmensorganisation | Vollständige Bewertung auf G2 lesen

Fazit

Die Cybersecurity muss stets mit der sich schnell ändernden Bedrohungslandschaft mithalten. Angreifer entwickeln ihre Techniken ständig weiter, um Abwehrmaßnahmen auszuhebeln. Dies wiederum zwingt Sicherheitsanbieter und Unternehmen dazu, ihren Schutz kontinuierlich anzupassen.

Eine wichtige Rolle kommt hier den Sicherheitstools zu, die präventive Cybersecurity bieten. Diese Tools umfassen automatisierte und adaptive Abwehrmechanismen, um Angreifer zu blockieren oder auszubremsen. Dies verschafft Ihnen zusätzliche Zeit für die Reaktion auf Cyberangriffe.

Wichtig ist: Sie müssen wissen, worauf es bei einer Endpoint-Security-Lösung ankommt und wie optimale Sicherheitsergebnisse aussehen. Mit diesem Wissen können Sie fundierte Entscheidungen in Bezug auf den besten Schutz für Ihr Unternehmen treffen.

Sophos-Lösungen schützen Unternehmen selbst vor völlig neuen Bedrohungen. Unsere Lösungen unterstützen Sie dabei, die bestmöglichen Sicherheitsergebnisse zu erzielen. Wenn Sie mehr erfahren möchten, kontaktieren Sie uns noch heute.

Weitere Informationen über Sophos Endpoint und den einzigartigen Schutz vor komplexen Bedrohungen der Lösung erhalten Sie unter **www.sophos.de/endpoint**

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.

© Copyright 2024. 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.

2024-06-18 DE-WP (PS)

SOPHOS