SOPHOS
Cybersecurity evolved.

Sophos Adaptive Cybersecurity Ecosystem

Das Sophos Adaptive Cybersecurity Ecosystem (ACE) ist ein breit angelegtes System zur Abwehr, Erkennung und Reaktion. Es bietet Schutz für moderne vernetzte Geschäftssysteme und wehrt die Flut immer neuer Cyberangriffe ab, bei denen verstärkt auf eine Kombination aus Automatisierung und manuellem Live-Hacking gesetzt wird.

Dank Kombination von Automatisierung und Analysten-Expertise sowie dem kollektiven Datenpool von Sophos-Produkten, -Partnern, -Kunden und -Entwicklern bietet Sophos ACE leistungsstarken Schutz. Denn dieses dynamische Cybersecurity-System lernt kontinuierlich dazu, verbessert sich und wächst mit. Beginnen Sie mit der Endpoint- oder Firewall-Technologie von Sophos, und bauen Sie nach Bedarf schrittweise auf dieser Grundlage auf.

Sophos-Whitepaper. Mai 2021

Eine Landschaft im Wandel

Das Cybersecurity-Umfeld verändert sich stetig. So haben sich sowohl Geschäftsumgebungen als auch Angriffsmethoden in den letzten Jahren erheblich gewandelt.

Geschäflicher Wandel: Interkonnektivität

Auf der ständigen Suche nach Möglichkeiten zur Produktivitäts- und Effizienzsteigerung haben Unternehmen eine sehr vernetzte Lieferkette sowie Infrastrukturen und Technologien zu deren Unterstützung geschaffen. Die Migration von Daten und Anwendungen in die Cloud hat zu vielen positiven Veränderungen geführt: Mitarbeiter können praktisch von überall arbeiten, die Betriebskosten werden gesenkt, die Performance und Skalierbarkeit gesteigert und gleichzeitig wird das Wachstum der globalen, digitalen Lieferkette vorangetrieben.

Parallel dazu hat COVID-19 die Umstellung auf Homeoffice/Remote Work rasant beschleunigt und damit jeden verbleibenden Mythos von traditionellen Netzwerkgrenzen zunichte gemacht. Heutzutage sollte einfach davon ausgegangen werden, dass Personen, Anwendungen, Geräte und Daten sich überall befinden können.

Diese miteinander verbundenen und verteilten Systeme eröffnen uns zwar ganz neue Möglichkeiten, stellen uns aber auch vor komplett neue Herausforderungen in puncto Sicherheit. Für viele Unternehmen ist es schwierig, die Reichweite ihres Netzwerks abzubilden, geschweige denn alle damit verbundenen Systeme zu schützen.

Intelligente Angreifer, die sich schnell an die neuen Gegebenheiten anpassen, zielen unablässig auf diese Systeme ab. Dabei werden sie insbesondere vom hohen Skalierungspotenzial angelockt. Nur eines von vielen aktuellen Beispielen ist der SolarWinds-Angriff vom Dezember 2020, dem neben führenden Technologieanbietern und kleineren Unternehmen auch hochrangige Behörden zum Opfer fielen.

Wandel von automatisierten zu manuellen Angriffen

Fakt ist: Es sind die Verteidiger, die im Kampf um kritische Systeme und Daten gewinnen. Doch wenn man im Bereich Cybersecurity tätig ist, kann man leicht diesen wichtigen, aber häufig unterschätzten Aspekt aus den Augen verlieren.

Die täglichen Schlagzeilen, in denen immer neue Sicherheitsverstöße gemeldet werden, dienen einem wichtigen Zweck: Sie sind Warnungen, die uns daran erinnern, präventiv zu handeln und wachsam zu bleiben. Dennoch sind diese Vorfälle die Ausnahme von der Regel. Es gibt keine Schlagzeilen über die Unternehmen, die täglich erfolgreich Tausende von Angriffsversuchen abwehren.

Doch nicht nur die Effektivität der Cybersecurity hat sich drastisch verbessert – auch die neuesten Tools und Managed Security Services sind zugänglicher und kostengünstiger als je zuvor. Technologien wie Anti-Ransomware, Exploit Prevention, Verhaltenserkennung und Anti-Phishing stehen allen zur Verfügung.

Diese Sicherheitsverfahren werden durch künstliche Intelligenz und Machine Learning unterstützt, optimiert und beschleunigt. Neben den bekannten im MITRE ATT&CK Framework dokumentierten Angriffstaktiken, -techniken und -prozessen wehren sie neue und sogar vollkommen neuartige Angriffe ab. Das Schließen von Schlupflöchern und Pfaden sowie das Blockieren von Techniken haben dazu geführt, dass diese Angriffe so kostspielig wurden, dass auch die Angreifer umdenken mussten. Die sicherheitstechnischen Verbesserungen sind mittlerweile so weitreichend, dass die Aussage „der Angreifer muss nur einmal richtig liegen" nicht mehr zutreffend ist. Um Geld zu verdienen, müssen Angreifer während eines Angriffs nun viele Male die richtigen Entscheidungen treffen.
Statt auf automatisierte Malware zu setzen, verfolgen Angreifer daher nun einen umfassenderen Ansatz, bei dem Automatisierung und manuelles Hacking miteinander kombiniert werden. Das Hauptziel der Angreifer ist es, unentdeckt zu bleiben. Am besten erreichen sie dies, indem sie sich wie Mitarbeiter verhalten – also lokale Tools und lokale Geräte nutzen und typische Datenverkehrsmuster produzieren.
Diese ausgeklügelten Angriffe erfordern erhebliche Investitionen in menschliche Ressourcen und sind für die Opfer umso kostspieliger. Die Angreifer sind in der Lage, ihr detailliertes Wissen über die Umgebung des Opfers auszunutzen, um maximalen Schaden anzurichten – und den größtmöglichen Ertrag für sich zu erzielen.

Wandel der IT-Sicherheit zu Security Operations

Solche geschäftlichen Veränderungen und neuen Angriffsmethoden machen eine Weiterentwicklung der IT-Sicherheit unausweichlich. Unternehmen sehen sich intelligenten Angreifern gegenüber, die ihre Angriffsziele immer wieder neu ausrichten. Um hier als Sieger die Arena zu verlassen, müssen IT-Security-Teams daher neue Gegenmaßnahmen entwickeln.

Zunächst ist ein grundlegender Wandel vom **Security Management hin zu Security Operations erforderlich**. Vorbei sind die Zeiten von Sicherheitsrichtlinien, die Sie einmal einrichten und anschließend vergessen konnten. Die Zunahme von manuellem Hacking bedeutet auch, dass Sicherheitsfunkionen aktiver gesteuert werden müssen, um verdächtige Verhaltensweisen und Ereignisse rechtzeitig zu erkennen.

IT-Security-Teams müssen so früh wie möglich nach verdächtigen Aktivitäten in der Angriffskette suchen, damit Abwehrmaßnahmen getroffen werden können, bevor Schaden entsteht. Selbst besonders versteckt agierende Angreifer hinterlassen Spuren, denen IT-Security-Teams nachgehen müssen, um den Angriff frühzeitig zu stoppen. Es geht nicht mehr nur darum, relevante Signale herauszufiltern, sondern auch kritische schwache Signale zu erkennen, bevor sie zur konkreten Bedrohung werden.Je stärker das Signal, desto näher sind Sie einem Sicherheitsvorfall. Mit geeigneten Tools können IT-Probleme proaktiv erkannt und behoben werden, bevor Angreifer diese erkennen und für Angriffe ausnutzen können.

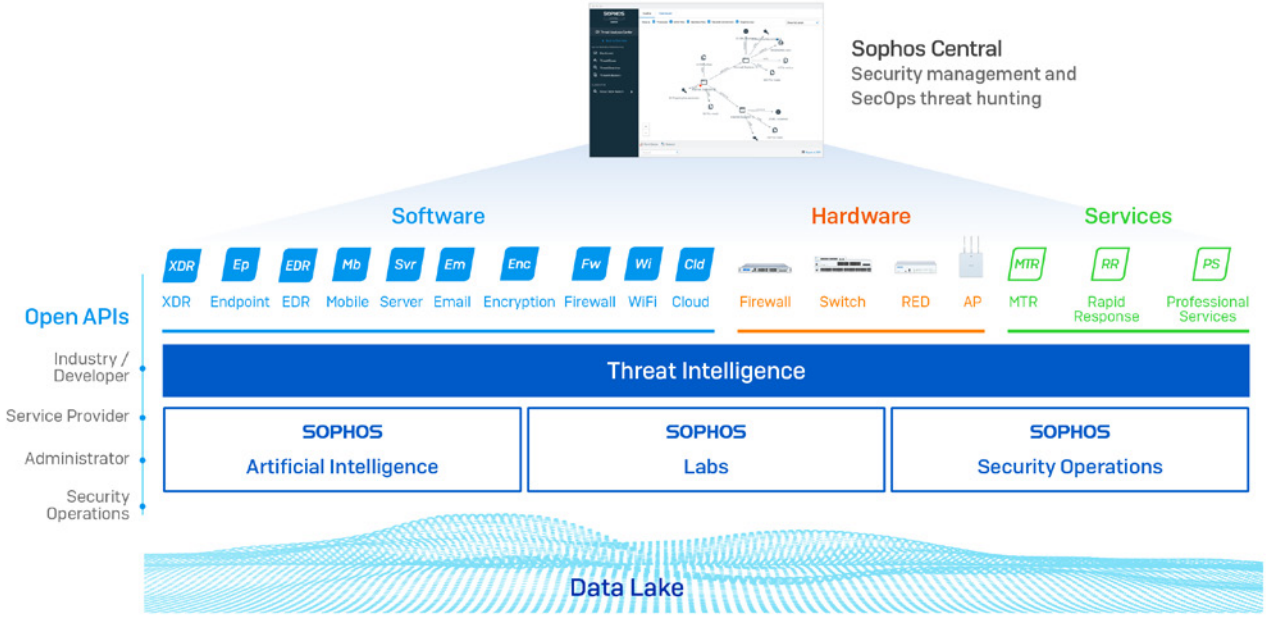
Angesichts einer zunehmend vernetzten Geschäftswelt muss die Sicherheit nachziehen. Für IT-Security-Teams ist es daher notwendig, von nicht integrierten Insellösungen auf ein **adaptives Sicherheitssystem umzusteigen**, das automatisch so viele Abwehrmaßnahmen wie möglich ergreift und Security-Experten gleichzeitig ermöglicht, auch nach schwächeren Signalen – wie verdächtige Verhaltensweisen und Ereignisse – zu suchen und diese rechtzeitig zu erkennen.

Geschäftsumgebungen und Angriffe entwickeln sich stetig weiter. Die Zukunft der IT-Sicherheit ist ein System, das dank einer einzigartigen Feedback-Schleife **fortlaufend dazulernt und sich verbessert.** Neue Informationen und Ereignisse, die vom Operations Team erkannt werden, können automatisiert verarbeitet werden. Das Ergebnis: bessere Prävention und weniger neue Angriffe, die ins System gelangen. Gleichzeitig können Experten bei verbesserter Automatisierung der Software verdächtige Verhaltensweisen und Ereignisse schneller finden und so Vorfälle weiter reduzieren. Durch diesen Erfolgszyklus wird die übergreifende Sicherheit von Unternehmen und ihren vernetzten Strukturen kontinuierlich verbessert.

Sophos Adaptive Cybersecurity Ecosystem

Die gute Nachricht: Es gibt bereits das passende System. Denn das Adaptive Cybersecurity Ecosystem (ACE) von Sophos ist auf genau diese neuen Gegebenheiten eingestellt. Es nutzt das Potenzial von Automatisierung und Analysten und ermöglicht damit die Verlagerung von Security Management auf Security Operations. Mittels Automatisierung können Verhaltensweisen und Ereignisse schneller analysiert und bearbeitet werden, während menschliche Experten mehrere verdächtige Signale besser korrelieren und ihre Bedeutung interpretieren können.

Sophos ACE wurde speziell zum Schutz der hochvernetzten Geschäfts- und Online-Welt entwickelt. Es schützt Systeme und Daten unabhängig vom Standort, lernt ständig dazu und verbessert sich. So passt es sich kontinuierlich an technologische Weiterentwicklungen und neue Angriffsmethoden an.



Sophos ACE umfasst die kollektive **Threat Intelligence** der SophosLabs, Sophos Security Operations (Security-Experten, die über unseren Managed Threat Response Service erweitertes Threat Hunting in Tausenden von Kundenumgebungen durchführen) und die Sophos Artificial Intelligence Group. Diese Echtzeit-Intelligence-Funktionen verbessern kontinuierlich die Next-Gen-Technologien in unseren weltweit führenden **Software-** und **Hardware**-Lösungen.

Ein einziger, integrierter **Data Lake** kombiniert Informationen von allen Sophos-Produkten und Threat-Intelligence-Quellen mit Echtzeit-Analysen. So sind IT-Experten in der Lage, relevante Warnsignale proaktiv herauszufiltern und Sicherheitspannen bereits im Vorfeld zu verhindern. Parallel dazu ermöglichen **offene APIs** Kunden, Partnern und Entwicklern, Tools und Lösungen zu entwickeln, die mit dem System interagieren. Sämtliche Vorgänge werden über **Management-Plattform Sophos Central** verwaltet. Das heißt: maximale Effizienz – denn Ihre gesamte IT-Sicherheit befindet sich an einem zentralen Ort.

Diese fünf Elemente – Threat Intelligence, Next-Gen-Technologien, Data Lake, APIs und zentrale Verwaltung – arbeiten zusammen und schaffen so ein adaptives Cybersecurity-Ökosystem, das kontinuierlich dazulernt und sich verbessert. Je umfangreicher das Ökosystem, desto stärker ist die Cybersecurity. Trotzdem können Sie „klein" anfangen und das System ganz nach Bedarf ausbauen. Viele Kunden beginnen beispielsweise mit unserem Endpoint-Schutz oder unserer Firewall und erweitern ihre Sicherheit dann im eigenen Tempo.

Im vergangenen Jahr wurden viele Security Operations Center zu virtuellen SOCs. Sophos ACE kann von jedem Ort aus verwaltet werden. Unternehmen können bei der Suche nach Security-Experten also aus einem weit größeren Kandidaten-Pool wählen. Alternativ können unsere Experten die Bedrohungserkennung und -reaktion auch als Service für Sie verwalten.

Die Evolution der Synchronized Security

Synchronized Security, die Fähigkeit von Sophos-Produkten, über einen Security Heartbeat™ Echtzeit-Informationen auszutauschen und die Reaktion auf Vorfälle zu automatisieren, ist seit vielen Jahren eine Schlüsselkomponente unseres Sophos-Schutzportfolios. Bei der Markteinführung im Jahr 2015 war Synchronized Security branchenweit einmalig und die Integration unserer Produkte ist bis heute konkurrenzlos und jedem anderen Anbieter überlegen.

„Sophos ist mit seinen XDR-Funktionen zwischen Firewall- und Endpoint-Sicherheitsprodukten weiterhin marktführend."

Gartner
Gartner Magic Quadrant for Enterprise Network Firewalls,
Analysten: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 09. November 2020

Das Sophos Adaptive Cybersecurity Ecosystem nutzt die Automatisierung und Integration von Synchronized Security und baut das Sophos-Cybersecurity-System weiter aus.

Mehr Transparenz

Niemand weiß, woher der nächste Angriff kommt, und es ist einfach unmöglich für menschliche Experten, alles im Blick zu behalten. Stattdessen benötigen Sie ein System, das alles überwacht und Ihnen eine schnelle Reaktion auf neue Bedrohungen ermöglicht. Deshalb haben wir das Ökosystem um noch mehr Sicherheitstechnologien erweitert, darunter die neuen Sophos Extended Detection and Response (XDR) und unsere APIs. Sophos-Produkte sehen und zeichnen alle verdächtigen Ereignisse, Verhaltensweisen und Erkennungen in Ihrer Umgebung auf, sodass Sie die benötigten Informationen jederzeit zur Hand haben.

Mehr Daten

Der Data Lake kombiniert und korreliert die Informationen all dieser Sensoren und bietet somit tiefere produktübergreifende Einblicke. Experten können den Data Lake mit Sophos Intercept X with EDR und Sophos XDR direkt abfragen. So können sie verdächtige Verhaltensweisen und Ereignisse in ihrer gesamten Umgebung erkennen und rechtzeitig reagieren.

Mehr Intelligenz

Dank des rasanten Wachstums unseres Managed Threat Response (MTR) Service sind wir in der Lage, die Erkennungsdaten mit Echtzeitdaten unserer Threat-Hunting-Experten zu ergänzen. Parallel dazu entwickeln wir unsere KI-Modelle und Bedrohungserkennungsdaten aus den SophosLabs weiter.

Mehr Integration

SophosLabs, Sophos AI und Sophos Security Operations arbeiten zusammen. Ihre gebündelte Expertise fließt zum Nutzen aller Kunden in einen virtuellen Zyklus ein. PowerShell ist beispielsweise ein seriöses Tool mit vielen guten Einsatzmöglichkeiten, wird jedoch von Angreifern häufig zweckentfremdet. Die MTR-Experten trainieren unsere KI-Modelle, damit basierend auf ihren realen Erfahrungen zwischen „unbedenklicher" und „schädlicher" PowerShell-Nutzung unterschieden werden kann. Anschließend wird das gesamte System entsprechend aktualisiert, wodurch sich der Schutz von Kunden erhöht.

Das Sophos Adaptive Cybersecurity Ecosystem in Aktion

Sophos ACE ist ein Live-System, das den Schutz unter Realbedingungen bereits erhöht und erweitert. Im März 2021 gelang der Hacker-Gruppe Hafnium ein weltweiter Angriff aufgrund einer ProxyLogon-Schwachstelle in Microsoft Exchange. Es handelte sich um eine Zero-Day-Sicherheitsanfälligkeit, und die Angreifer nutzten die entwicklungsbedingten Schwachpunkte von Exchange gezielt aus, um keine unmittelbaren Erkennungen auszulösen.

Gleich nach Bekanntwerden der Sicherheitsanfälligkeit aktualisierte der Sophos Managed Threat Response (MTR) Service das Sensor Monitoring und berücksichtigte das mit ProxyLogon verbundene Verhalten. Da sich die Informationen bereits im Data Lake befanden, hatte Sophos MTR sofortigen Zugriff auf alle Informationen, die zum Erkennen und Beheben schädlicher Aktivitäten im Zusammenhang mit dieser Sicherheitsanfälligkeit erforderlich waren.

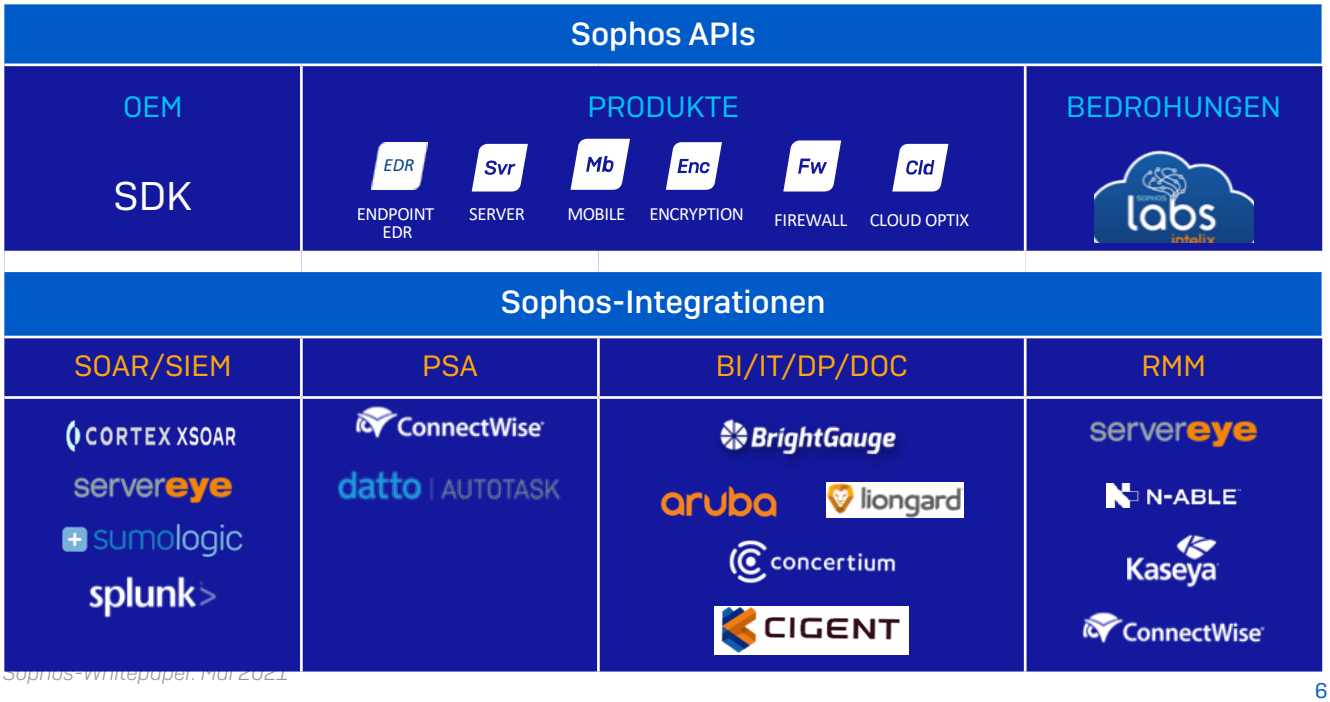
Zudem kombinierten die MTR-Spezialisten ihre Threat-Hunting-Expertise mit der Sophos-XDR-Technologie und waren so in der Lage, neue Artefakte und Indicators of Compromise (IOCs) im Zusammenhang mit dem Angriff aufzudecken. Diese Indikatoren wurden direkt an die SophosLabs weitergegeben, die diese zur Veröffentlichung weiterer IOCs im Zusammenhang mit der Sicherheitsanfälligkeit in Exchange nutzten und damit den Schutz aller Sophos-Kunden weiter verbesserten.

Offene Plattform mit leistungsstarken Integrationen und offenen APIs

In unserer vernetzten Welt ist es von entscheidender Bedeutung, dass Cybersecurity sich in das breitere Geschäftsumfeld integrieren lässt. Cybersecurity ist vielseitig, und das Sophos Adaptive Cybersecurity Ecosystem unterstützt eine Vielzahl von Sicherheitsanforderungen, darunter:

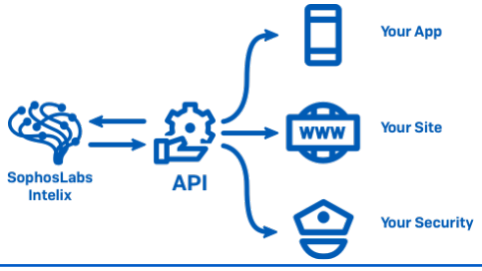
- MSSPs – Unterstützung bei der Bereitstellung modernster Cybersecurity-Lösungen
- Channel-Partner – Optimierung ihrer Geschäftsprozesse
- ISPs – Gewährleistung der Sicherheit angebotener Internet-Dienste
- Kleine und mittlere Unternehmen – Unterstützung bei der Erstellung benutzerdefinierter Tools zur Kontrolle und Realisierung der Sicherheit

Unzählige APIs und Integrationen sind bereits vorhanden – und mehr sind in Planung – Sophos ACE verarbeitet bereits über fünf Millionen API-Anfragen pro Tag.



API-Erfolgsprojekt: SophosLabs Intelix™

Intelix ist eine Suite einfacher und schnell reagierender RESTful APIs, mit denen Anwendungen Bedrohungen identifizieren, klassifizieren und abwehren können, wodurch sich ihre Sicherheit erhöht. Kunden, Partner und Entwickler, die das Sophos-Ökosystem nutzen, können diese APIs für Cloud-Bedrohungsanalysen sowie statische und dynamische Dateianalysen verwenden. Weitere Informationen zu den SophosLabs Intelix APIs finden Sie unter https://www.sophos.com/de-de/labs/intelix.aspx.



Sophos ACE: echten Business Impact generieren

Das Sophos Adaptive Cybersecurity Ecosystem bietet zahlreiche Vorteile, die sich im Zusammenspiel noch verstärken. Dabei wirkt sich die Kombination von Next-Gen-Technologien entscheidend auf den Schutz und die Effizienz aus. Threat Intelligence aus den SophosLabs, Sophos AI und Sophos Security Operations, ein integriertes, adaptives, ständig weiterlernendes System und eine zentrale Verwaltung über die Plattform Sophos Central greifen hier wirksam ineinander.

Next-Gen-Technologien	**+**	**Threat Intelligence**	**+**	**Integriertes, adaptives System**	**+**	**Zentrale Verwaltung**

Kunden, die die Sophos Firewall und Sophos Intercept X gemeinsam nutzen, berichten uns bereits, dass sie ohne Cybersecurity-Lösungen von Sophos doppelt so viele IT-Security-Mitarbeiter einstellen müssten, um ihren Schutz aufrechtzuerhalten. Zudem verzeichnen unsere Kunden weniger Sicherheitsvorfälle und können Probleme schneller ermitteln und beheben. Sophos ACE baut darauf auf und trägt zu einer fortlaufend optimierten Cybersecurity in puncto Total Cost of Ownership (TCO) und Schutz bei.

Erste Schritte

Das Sophos Cybersecurity Ecosystem ist sehr flexibel und der Einstieg ist kinderleicht: Sie müssen lediglich ein Schutzprodukt oder -service von Sophos bereitstellen. Unternehmen profitieren unmittelbar von der kombinierten Threat-Intelligence-Expertise von Sophos AI, den SophosLabs und Sophos Security Operations. Sie können Ihr Ökosystem jederzeit und ganz nach den individuellen Bedürfnissen Ihres Unternehmens erweitern. Die meisten unserer Kunden entscheiden sich beim Einstieg für:

Sophos Intercept X für Ihre Endpoints oder Server (mit der Option, XDR-Funktionalität hinzuzufügen)

Sophos Firewall – Hardware, Software oder virtuell

Sophos Managed Threat Response (MTR) Service

Weitere Informationen erhalten Sie bei Ihrem Sophos-Ansprechpartner und auf unserer Website. Oder starten Sie gleich eine kostenlose Testversion.

Gartner Magic Quadrant for Enterprise Network Firewalls,
Analysten: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 09. November 2020

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.

Erfahren Sie mehr über Ransomware und darüber, wie Sophos Sie und Ihr Unternehmen davor schützen kann

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 2021. 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.

2021-04-26 (SB-NP)

SOPHOS