WHITEPAPER

Cyber-Abwehrsysteme auf einen Blick

Wie das neue Modell der Cyberabwehr im Zeitalter der agentischen KI optimale Resilienz gewährleistet

SOPHOS

Kurzfassung

Auf dem Papier sieht die Sicherheitslage in den meisten Unternehmen und Organisationen solide aus. Sie haben im Laufe der Jahre eine Vielzahl von Sicherheitsprodukten angeschafft. Gartner zufolge „verfügen Unternehmen und Organisationen im Durchschnitt über 45 Sicherheitstools, die oft isoliert voneinander arbeiten, was zu Komplexität, blinden Flecken und unerkannten Sicherheitslücken führt, auf die Angreifer abzielen.“[1] Es mangelt also nicht an Tools, sondern an der Vernetzung dazwischen.

Angreifer nutzen die Lücken zwischen den Tools bereits aus und bewegen sich innerhalb von Minuten zwischen E-Mail-, Identitäts-, Endpoint- und Netzwerk-Ebene. KI erhöht die Geschwindigkeit, das Ausmaß und den Umfang von Cyberbedrohungen in einem beispiellosen Tempo und ermöglicht die breitflächige Ausführung komplexer, mehrschichtiger Angriffe.

Auditoren, Regulierungsbehörden und Cyber-Versicherer erwarten mittlerweile eine Vielzahl von Nachweisen, die von fragmentierten Cyber-Produkten nur schwer erbracht werden können. Die meisten Unternehmen und Organisationen haben immer noch Schwierigkeiten, drei grundlegende Fragen zu beantworten: Sind wir geschützt, wo liegt unser größtes Risiko und funktionieren unsere Investitionen?

Ein neues Modell für die Cyberabwehr nimmt Gestalt an, um das Zeitalter der KI abzusichern: Security-Plattformen entwickeln sich zu Cyber-Abwehrsystemen weiter. Cyber-Abwehrsysteme zeichnen sich durch die folgenden Merkmale aus:

- **Eine zentrale Echtzeit-Ansicht der Umgebung**, in die Daten von jedem Kontrollpunkt jedes Anbieters einfließen.
- **Reaktionsmaßnahmen werden automatisch koordiniert** – für alle Kontrollpunkte: E-Mail, Identität, Endpoint, Netzwerk und mehr.
- **Agentische KI reagiert auf die Geschwindigkeit und das Volumen moderner Angriffe**, während menschliche Experten die Grenzen festlegen und für die Ergebnisse verantwortlich bleiben.
- **Kontinuierliches Lernen** – mit jeder in der gesamten Nutzerbasis gewonnenen neuen Erkenntnis und jeder dort abgewehrten Bedrohung wird die Abwehr für alle Nutzer automatisch verstärkt.
- **Der Schwerpunkt bei der Abwehr verlagert sich von Einzelprodukten hin zu einer Architektur, die diese miteinander verbindet** – einschließlich der Technologiearchitektur und eines Netzwerks menschlicher Expertise.

Ein Cyber-Abwehrsystem ist …

Eine einheitliche Sicherheitsarchitektur, in der alle Kontrollpunkte in einer Echtzeit-Übersicht abgebildet werden, als Einheit reagieren, kontinuierlich dazulernen und unter menschlicher Verantwortung in maschineller Geschwindigkeit agieren.

1. *Gartner, „Tech FutureSight: Schützen Sie die globale Angriffsfläche mit einem autonomen Cyber-Abwehrsystem“, Neil MacDonald, 12. Dezember 2025.*

Bedrohungen des agentischen KI-Zeitalters sind bereits Realität

Ende 2025 dokumentierten Forscher die erste bekannte Cyber-Spionagekampagne, die hauptsächlich von KI und nicht von Menschen durchgeführt wurde. Die KI führte schätzungsweise 80 bis 90 % des Vorgangs eigenständig durch – und zwar in einer Geschwindigkeit und einem Ausmaß, mit denen kein menschliches Team mithalten könnte.

Quelle: Anthropic, November 2025

Ihre Sicherheitsherausforderungen im KI-Zeitalter

Jahrelange „vernünftige“, auf einzelne Bedrohungen konzentrierte Kaufentscheidungen haben zu einer Umgebung geführt, die so komplex ist, dass die Komplexität selbst zum Risiko geworden ist. Nun steht diese relativ wahllose Zusammenstellung unkoordinierter Produkte Angreifern mit KI-Geschwindigkeit gegenüber und hält nicht mehr Schritt. Wie sind wir an diesen Punkt geraten?

Defizite des Plattform-Ansatzes

Fast alle großen Cybersecurity-Anbieter behaupten, ihre Plattform könne alles leisten, was Sie benötigen. Es werden Einzellösungen für den bedrohungsorientierten Käufer angeboten, die darauf abzielen, als eine einzige Plattformeinheit zusammenzuarbeiten.

Die Plattformphilosophie, ein einheitliches System aufzubauen, ist im Grunde genommen der richtige Ansatz. Doch was oft verkauft wird, ist ein Flickenteppich aus hastig entwickelten oder erworbenen Tools, die darauf abzielen, vergangene Hype-Zyklen zu bedienen oder den Aktienkurs in die Höhe zu treiben. Die Versprechen greifen zu kurz:

- **Die Anbieter versprechen eine „einheitliche Oberfläche“**, aber bei Praxistests stellt sich heraus, dass Responder immer noch zwischen mehreren Konsolen hin- und herwechseln müssen.
- **Sie versprechen gemeinsame Daten**, aber die Plattformprodukte können diese Daten nicht gemeinsam analysieren, um Angriffe zu erkennen, die sich auf Identitäts-, Cloud- und Endpoint-Ebene erstrecken.
- **Sie versprechen Integration**, aber jedes Produkt behält sein eigenes Datenmodell bei und Reaktionsmaßnahmen bleiben über Domänen hinweg isoliert.

Die gesamte Arbeit an der Plattform – Konfiguration, Anpassung und die Erstellung eines Workflows, der alle Komponenten miteinander verbindet – bleibt dem Kunden überlassen.

Laut Gartner® „wird das einfache Hinzufügen weiterer Tools zum Stack nicht die intelligente Cyber-Abwehrstruktur bieten, die Unternehmen und Organisationen benötigen, um KI-gesteuerte Angriffe wie den kürzlich von Anthropic identifizierten abzuwehren.“

Neil MacDonald
Gartner | VP, Distinguished Analyst und Gartner Fellow Emeritus

Gartner, Tech FutureSight: Schützen Sie die globale Angriffsfläche mit einem autonomen Cyber-Abwehrsystem, Neil MacDonald, 12. Dezember 2025. GARTNER ist eine Marke von Gartner, Inc. und/oder seinen verbundenen Unternehmen.

Domänenübergreifende Angriffe überlisten fragmentierte Abwehrmechanismen

Fragmentierte Datenmodelle und Analysen in Plattformprodukten sind für Angreifer ein gefundenes Fressen. Das folgende Angriffsszenario zeigt, warum:

- **Schritt 1:** Eine überzeugende E-Mail gelangt in einen Posteingang.
- **Schritt 2:** Der Empfänger gibt sein Passwort auf einer gefälschten Anmeldeseite ein.
- **Schritt 3:** Der Angreifer meldet sich von einem unbekannten Standort aus an.
- **Schritt 4:** Der Angreifer fügt unbemerkt eine Postfachregel hinzu, um den Traffic zu überwachen.
- **Schritt 5:** Der Angreifer nutzt seinen Zugriff, um eine Dateifreigabe zu erreichen und Daten zu exfiltrieren.

Fünf Schritte, von denen jeder auf einer anderen Domäne landet.

- **Die E-Mail -Security**-Lösung registriert die Nachricht.
- **Die Identitätslösung** bemerkt die ungewöhnliche Anmeldung.
- **Der Endpoint-Schutz** bemerkt eine kleine Anomalie.
- **Die Firewall** protokolliert die ausgehende Verbindung.

Jedes Produkt registriert seinen Teil des Puzzles und jedes Produkt erledigt technisch gesehen seine Arbeit. Doch **keines der Produkte sieht das Gesamtbild**, da kein Produkt sein Wissen an die anderen weitergibt, während der Angriff noch im Gange ist. Stattdessen erscheinen die von den einzelnen Produkten registrierten Informationen irrelevant und nichts deutet auf ein zusammenhängendes Angriffsgeschehen hin. Die Kette wird erst später offensichtlich, wenn es zu spät ist.

Diese Art der lateralen Bewegung ist bei modernen Angriffen üblich und wird auch häufig übersehen. Der Sophos Ransomware-Report 2026 zeigte, dass 55 % der Cyberkriminellen erfolgreich Daten verschlüsselten, selbst wenn die Firewall den Angriff erkannte.

Angriffe in maschineller Geschwindigkeit – Reaktion in menschlicher Geschwindigkeit

Nehmen Sie nun diesen domänenübergreifenden Angriff und komprimieren Sie den zeitlichen Ablauf von Tagen auf Minuten. Genau das hat KI bewirkt. Eine Abwehr, die darauf wartet, dass eine Person einen Alert in einem Produkt bemerkt und diesen mit einem anderen Produkt abgleicht, ist zum Scheitern verurteilt. Das Problem sind nicht langsame Verteidiger, sondern langsame Reaktionen, bei denen immer nur eine Maßnahme nach der anderen ergriffen wird. Überwiegend manuelle Workflows können mit einem automatisierten Angriff nicht Schritt halten. Bis ein Betreiber eine Reaktion formuliert hat, ist der Angreifer bereits zur nächsten Stufe übergegangen.

Expertise ist Mangelware. Die Flut irrelevanter Daten ist endlos.

Dem Problem mit mehr Personal zu begegnen, ist keine wirkliche Option, da das Personal dafür fehlt. Der Cybersecurity-Fachkräftemangel ist real und lässt nicht nach. In der ISC2-Studie zur Arbeitskräftesituation 2025 berichteten 95 % der Sicherheitsteams von mindestens einer Kompetenzlücke und 59 % stuften diese als kritisch oder erheblich ein – ein Anstieg gegenüber 44 % im Vorjahr.

Gleichzeitig nimmt das Arbeitsaufkommen immer weiter zu. Ein kleines Team kann am Ende für mehr Produkte, Alerts und Dashboards verantwortlich sein, als es realistischerweise überwachen könnte. Die meisten dieser Alerts sind irrelevant, aber jemand muss sie sichten, um das eine darin verborgene Signal zu finden.

KI sollte diesen Druck eigentlich verringern, aber in einigen Umgebungen hat sie das Gegenteil bewirkt.

Wird KI als ein weiteres, nachträglich aufgesetztes Produkt ergänzt, führt sie zu den bereits beschriebenen Problemen: mehr Störsignale und Alerts, da sie nicht dafür konzipiert wurde, nativ mit den übrigen Produkten der Plattform zu interagieren. Mit dem Ergebnis, dass Cyberteams nicht mehr nur False Positives aussortieren, sondern sich auch mit KI-„Halluzinationen“ auseinandersetzen müssen.

Die Cybersecurity-„Armutsgrenze“ ist real

Die Cybersecurity-„Armutsgrenze“ ist die Grenze, unterhalb der ein Unternehmen oder eine Organisation nicht effektiv geschützt werden kann. Sie wird nicht durch die Größe, das Budget oder das Vorhandensein eines CISO definiert. Tatsächlich gibt es viele finanziell gut aufgestellte Unternehmen und Organisationen, die unterhalb dieser Grenze liegen.

Die Cybersecurity-„Armutsgrenze“ ist eine strategische Fähigkeitsschwelle.

Besitzt Ihr Unternehmen oder Ihre Organisation lediglich isoliert agierende Sicherheitstechnologien oder können diese als System betrieben werden? Große Teams geben unter Umständen viel Geld für Tools aus, für deren Bedienung niemand über die nötige Expertise verfügt, während ein diszipliniertes Produktionsunternehmen mit 200 Mitarbeitenden ein Abwehrsystem betreiben kann, das weitaus größere Organisationen in puncto Leistung übertrifft. Viele Unternehmen und Organisationen liegen unwissentlich unter der Cybersecurity-„Armutsgrenze“, weil sie davon ausgehen, dass die Fähigkeit, Sicherheit als System zu betreiben, intern bereits vorhanden ist

Für diese Unternehmen und Organisationen ist die größte Lücke kein fehlendes Tool. Es ist das Fehlen einer klaren Strategie und der Orchestrierung, die erforderlich ist, damit bestehende Kontrollen gegen KI-beschleunigte Bedrohungen zusammenarbeiten. Sie investieren weiter, haben aber immer noch Schwierigkeiten, drei grundlegende Fragen zu beantworten:

- Sind wir geschützt?
- Wo liegen unsere größten Risiken?
- Funktionieren unsere Investitionen tatsächlich?

Regulierungsbehörden fordern mehr Resilienznachweise

Regulierungsbehörden und Cyber-Versicherer interessieren sich nicht dafür, ob Sie die richtigen Produkte implementiert haben. Stattdessen fordern Sie immer häufiger Nachweise für Folgendes:

- Koordinierte, domänenübergreifende Kontrollmaßnahmen
- Gespeicherte, prüfbare Beweismittel
- Konsistente, zeitnahe Offenlegungen
- Getestete, praxiserprobte Resilienz

Diese neuen Vorschriften stellen eine erhebliche Belastung für Unternehmen und Organisationen dar, deren Sicherheitsinfrastruktur nach wie vor auf eine Vielzahl von Produkten verteilt ist, von denen jedes sein eigenes Datenmodell und seine eigene Aufbewahrungsfrist hat. Die Bereitstellung der von einem Auditor oder Versicherer geforderten Nachweise kann zu einer Vollzeitbeschäftigung werden: Protokolle aus verschiedenen Systemen exportieren, sie von Hand zusammenfügen und hoffen, dass das Ergebnis dennoch ein schlüssiges Bild ergibt. Eine Kontrollmaßnahme, die nicht nachgewiesen werden kann, zählt für Compliance-Zwecke nicht.

Viele Probleme – eine gemeinsame Ursache

Keines dieser Probleme wird durch das Hinzufügen eines weiteren Produkts oder einer weiteren Schaltfläche zu einer Konsole gelöst. Sie haben eine gemeinsame Ursache: Abwehrmaßnahmen, die in Isolation arbeiten, versagen, wenn Bedrohungen koordiniert gegen sie vorgehen. Diese Schutzlücke lässt sich nicht durch den Kauf eines weiteren neuen Produkts schließen. Stattdessen ist ein komplett neuer Sicherheitsansatz erforderlich.

Cyber-Abwehrsysteme: ein moderner Sicherheitsansatz

Wenn das Problem in der Fragmentierung liegt, ist die Lösung nicht die Konsolidierung um ihrer selbst willen. Ein Produkt zu kaufen, das alles können will und dabei versagt, ist nicht besser, als mehrere gute Produkte zu haben, die schlecht miteinander harmonieren.

Stattdessen sollten Unternehmen und Organisationen auf ein Cyber-Abwehrsystem setzen: Eine Reihe von Security-Produkten und -Services, die darauf ausgelegt sind, als einheitliches System zu agieren. Jeder Kontrollpunkt sollte zu einem gemeinsamen Verständnis der Umgebung beitragen und als Teil eines koordinierten Ganzen reagieren. Das System sollte gut vernetzt, synchronisiert, automatisiert, intelligent und anpassungsfähig sein. Fünf Grundsätze beschreiben, wie das in der Praxis aussieht.

1 Synchronisierte, autonome Kontrollpunkte

Ein Cyber-Abwehrsystem beginnt mit Kontrollpunkten. Dies sind die Technologien und Services, bei denen Sicherheitstelemetrie erfasst und Sicherheitsregeln durchgesetzt werden. Kontrollpunkte können sowohl wahrnehmen, was mit ihnen geschieht, als auch darauf reagieren. Endpoints, Firewalls, E-Mails, Identitätsmanagement, Produktivitätstools und vieles mehr sind allesamt Kontrollpunkte.

2 Ein gemeinsamer Überblick in Echtzeit

Ein Abwehrsystem unterscheidet sich dadurch von einer Plattform, dass es ein gemeinsames Verständnis davon hat, was in der gesamten Umgebung geschieht. Jeder Kontrollpunkt speist seine Erkenntnisse in Echtzeit in einen gemeinsamen Data Layer ein – ohne verzögerte Kopiervorgänge oder Abgleiche. Dadurch erhält das gesamte System einen einheitlichen, gemeinsamen Überblick über die Ereignisse in Echtzeit. Keine blinden Flecken, keine Reaktionslücken.

3 Koordinierte Reaktionsmaßnahmen auf allen Ebenen

Eine koordinierte Reaktion beginnt mit einer Erkennung auf einer Ebene, die automatisch eine Aktion auf den anderen Ebenen auslösen kann, ohne dass ein Analyst das Signal von einer Konsole zur nächsten weiterleiten muss.

Eine verdächtige Anmeldung kann eine genauere Überprüfung sowohl auf der Endpoint- als auch auf der E-Mail-Ebene veranlassen. Eine schädliche Datei auf einem Gerät kann dazu führen, dass die Firewall oder das Netzwerk die Verbindung blockiert, die das Gerät herstellen möchte. Das System reagiert als Einheit, weil es einen Angriff bereits als Einheit sieht. Und wenn ein Angriff schnell abläuft, ist diese Art der Koordination wichtig.

SOPHOS

4 Agentische KI mit menschlicher Verantwortlichkeit

Geschwindigkeit ist der entscheidende Faktor. Angriffe, die sich in Minutenschnelle entfalten, lassen sich nicht durch Abwehrmaßnahmen stoppen, die darauf warten, dass ein Mensch eingreift. Deshalb muss KI im Zentrum des Systems stehen und darf keine zweitrangige Position einnehmen.

In einem Cyber-Abwehrsystem ist KI in die Architektur integriert und wurde nicht nachträglich hinzugefügt. KI korreliert Signale auf allen Ebenen, erkennt das Muster eines Angriffs bereits in der Entstehungsphase und treibt die Erkennung, Analyse und Reaktion mit maschineller Geschwindigkeit voran. Dieses KI-native System unterscheidet sich von KI, die nachträglich in ein einzelnes Produkt integriert wurde und nur die Daten dieses Produkts sehen kann.

Eine in ein Abwehrsystem integrierte KI kann alles, was das System wahrnimmt, logisch verarbeiten. Reaktionsmaßnahmen in maschineller Geschwindigkeit ohne menschliche Verantwortlichkeit sind jedoch ein Risiko, kein Vorteil. Cyber-Abwehrsysteme schließen Menschen nicht aus Sicherheitsprozessen aus. Stattdessen setzen sie sie dort ein, wo menschliches Urteilsvermögen am wichtigsten ist: beim Festlegen von Grenzen, beim Umgang mit neuartigen oder risikoreichen Entscheidungen, bei der Aufarbeitung von Vorfällen und bei der Übernahme von Verantwortung für die Ergebnisse.

KI bearbeitet Fälle schnell und im richtigen Maßstab. Sie übernimmt die routinemäßige Triage und Aktionen mit hoher Konfidenz.

Menschliche Experten definieren die Vertrauensgrenze: worüber die KI selbst entscheiden kann und wann sie Hilfe benötigt. Sie greifen ein, wenn der Kontext unbekannt ist oder viel auf dem Spiel steht.

Wenn das System Vertrauen gewinnt, kann diese Grenze erweitert werden.
Die Verantwortung liegt jedoch immer bei den menschlichen Experten.

KI bearbeitet Fälle schnell und im richtigen Maßstab.

Menschliche Experten bestimmen die Vertrauensgrenze.

5 Kombinierte Intelligence

Cyber-Abwehrsysteme lernen. Informationen über jede erkannte Bedrohung fließen an alle Kontrollpunkte. Der Endpoint sieht, was die Firewall gesehen hat. Das E-Mail-Gateway teilt der Identitätsebene mit, was es abgefangen hat. Jedes Tool lernt von den anderen und baut auf dem auf, was zuvor geschah. All dies geschieht ohne manuelle Konfiguration. Die Intelligenz des Cyber-Abwehrsystems wächst mit mehr Benutzern und mehr beobachteten Mustern, wodurch das System sich mit der gleichen Geschwindigkeit weiterentwickeln kann wie KI-gesteuerte Angriffe.

Von Plattformen zu Cyber-Abwehrsystemen

Zusammengenommen definieren diese fünf Prinzipien eine eigene Kategorie. Cyber-Abwehrsysteme sind die Weiterentwicklung von Security-Plattformen – optimiert für das KI-Zeitalter. Eine Plattform ist in der Regel lediglich eine Zusammenstellung von Produkten, die über eine gemeinsame Konsole zugänglich sind und eher durch eine Anmeldung und eine Lizenzvereinbarung als durch ihr Design miteinander verbunden sind.

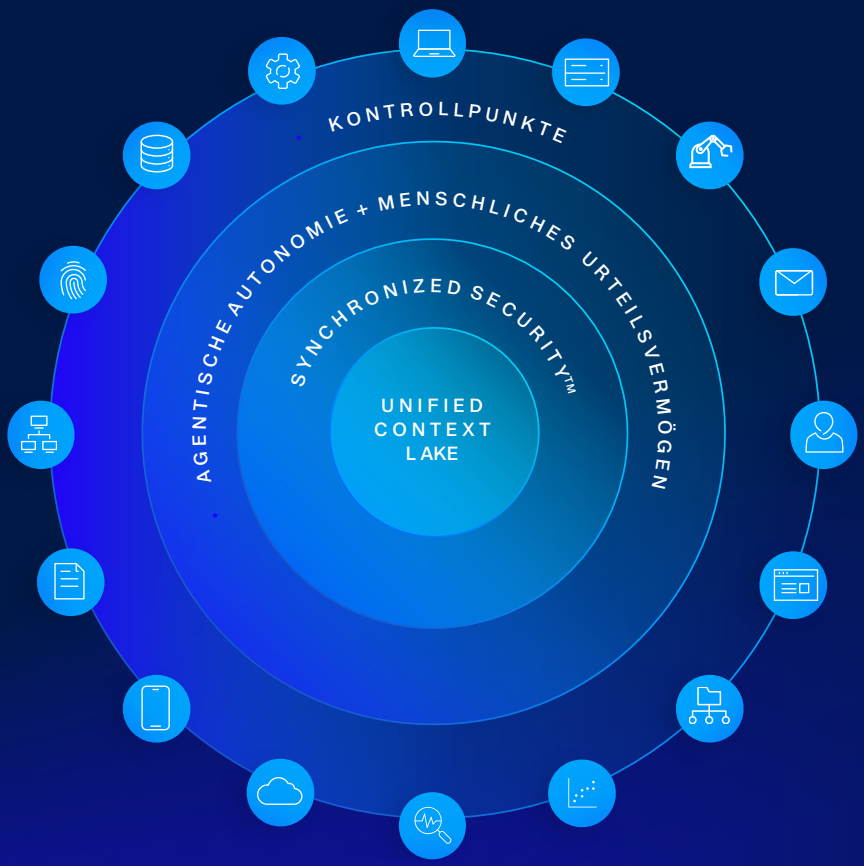
Ein Cyber-Abwehrsystem ist anders. Seine Daten werden gemeinsam genutzt, KI ist integriert, die Reaktion erfolgt koordiniert und menschliche Experten behalten die Kontrolle. Es handelt sich um eine Architektur, die so konzipiert ist, dass sie als ein einziges Produkt ausgeführt wird, und nicht um eine Ansammlung von Produkten, die so angeordnet sind, dass sie wie ein einziges Produkt wirken.

Sophos Fusion: das Sophos Cyber Defense System

Sophos Fusion ist das branchenweit umfassendste Cyber-Abwehrsystem – entwickelt für eine Welt, in der Bedrohungen mit KI-Geschwindigkeit agieren. Dank der Architektur des Sophos AI-Native Cybersecurity Defense Systems und über 500 Sophos- und Fremdanbieter-Integrationen sieht Sophos Fusion alles, vernetzt alles und ermöglicht Ihren Abwehrmaßnahmen, als Einheit zu reagieren.

Sophos Fusion setzt die Prinzipien eines Cyber-Abwehrsystems in die Praxis um: eine einheitliche, offene Architektur, in der alle Kontrollpunkte als Einheit agieren – gestützt auf agentische KI und ergänzt durch menschliches Urteilsvermögen –, um Unternehmen und Organisationen vor KI-gestützten Bedrohungen zu schützen, die sich schneller bewegen, als die Cyberabwehr reagieren kann.

Je mehr vom Sophos-Portfolio ein Kunde aktiviert, desto mehr Mehrwert liefert Sophos Fusion.



Synchronisierte, autonome Kontrollpunkte

Jeder Kontrollpunkt, den Sie bereits besitzen, liefert kontinuierlich Echtzeit-Threat-Intelligence und führt Reaktionsmaßnahmen durch. Die Architektur ist vollständig offen: Sie lässt sich nativ in Sophos-Produkte und mehr als 500 Drittanbieter-Technologien integrieren, sodass die Investitionen, die Sie bereits getätigt haben, Teil einer koordinierten Abwehr werden, anstatt in Isolation zu verbleiben.

Zudem bietet Sophos Fusion die marktweit tiefgreifendste Microsoft-Sicherheitsintegration – und zwar für alle Microsoft-Pläne, nicht nur für die teuersten –, sodass selbst Unternehmen und Organisationen mit Microsoft-Basislizenzen ihre Abwehr mithilfe dieser Telemetriedaten stärken können.

Ein gemeinsamer Überblick in Echtzeit

Sämtliche Telemetriedaten von jedem Kontrollpunkt fließen in Echtzeit in den zentralen Context Lake ein – einen einzigen gemeinsamen Data Layer. Es gibt keine Verzögerung durch Aggregation und keinen separaten Datenspeicher an den einzelnen Kontrollpunkten. Stellen Sie sich das Ganze wie ein gemeinsames Nervensystem vor: Jeder Kontrollpunkt nimmt wahr, was jeder andere Kontrollpunkt wahrnimmt, und zwar in dem Moment, in dem es geschieht. Dieses gemeinsame Verständnis ermöglicht die Koordination.

Koordinierte Reaktion auf allen Ebenen: Synchronized Security™

Synchronized Security™ ist das Bindeglied, das gemeinsames Verständnis innerhalb von Sophos Fusion in koordiniertes Handeln umsetzt. So können Kontrollpunkte von Sophos und anderen Anbietern automatisch gemeinsam auf Bedrohungen reagieren.

Eine Erkennung am Endpoint kann eine Reaktion an der Firewall auslösen. Bei Kompromittierung einer Identität kann der Zugriff auf die gesamte Umgebung gesperrt werden. Eine verdächtige E-Mail kann auf allen weiteren Ebenen zu einer genaueren Überprüfung führen. Je mehr Sophos-Lösungen Sie bereitstellen, desto mehr Vorteile von Synchronized Security™ erhalten Sie.

Denken Sie an das Brandschutzsystem eines modernen Gebäudes: Ein Sensor in einem Raum löst nicht nur einen Alarm aus; er schließt Brandschutztüren, leitet den Luftstrom um und startet Sprinkler auf nahegelegenen Etagen. Sophos Fusion funktioniert auf dieselbe Weise – als ein koordiniertes Ganzes. Dies ist möglich, da die Daten bereits vereinheitlicht sind. Es ist keine zusätzliche Konfiguration oder Aktion erforderlich.

Agentische KI mit menschlicher Verantwortlichkeit

Sophos Fusion erkennt, analysiert und reagiert in maschineller Geschwindigkeit, jedoch immer unter menschlicher Aufsicht. Jede Aktion bleibt innerhalb der Grenzen, die von menschlichen Experten definiert und kontinuierlich angepasst werden. Was es zu agentischer KI macht: KI, die neue Situationen durchdenken kann, anstatt nur festen Playbooks zu folgen.

Eine nützliche Analogie ist der Autopilot in der Luftfahrt. Das System kann das Flugzeug fliegen, aber der Pilot legt die Parameter fest, überwacht die Instrumente und übernimmt, wenn die Situation ungewohnt oder risikoreich ist.

In Sophos Fusion wird diese agentische Fähigkeit durch Fusion AI bereitgestellt, die native agentische KI von Sophos. Sophos verfügt über mehr als 50 KI-Modelle, die in seine Abwehrmechanismen integriert sind und kontinuierlich mit Echtzeit-Threat Intelligence optimiert werden. Sophos Email verwendet beispielsweise mehr als 20 Modelle, einschließlich proprietärer Natural Language Processing (NLP)-Modelle, die den Text, den Ton, den Kontext und die Struktur von E-Mails analysieren, um Phishing- und Business Email Compromise-Angriffe zu identifizieren.

Unser Sophos MDR-Service, bei dem Sophos-Experten Ihre Umgebung rund um die Uhr für Sie überwachen und reagieren, betreibt das weltweit größte agentische SOC (Security Operations Center) und nutzt dazu das Sophos Cyber Defense System. Es handelt sich um den branchenweit größten Managed-Detection-and-Response-Betrieb, der mehr als 40.000 Unternehmen und Organisationen schützt. 52 % der Vorfälle werden von Anfang bis Ende mittels KI behoben, wobei die Zeit vom Alert bis zur automatisierten Reaktion durchschnittlich 89 Sekunden beträgt. Menschliche Experten tragen jedoch weiterhin die Verantwortung für Entscheidungen, die ein Risiko für das Unternehmen/die Organisation darstellen.

Kombinierte Intelligence

Das Sophos Cyber Defense System lernt aus jedem Angriff im gesamten Kundenstamm, nicht nur aus Angriffen auf Ihr Unternehmen oder Ihre Organisation. Informationen zu jeder Bedrohung, die in den über 625.000 von Sophos geschützten Unternehmen und Organisationen auftritt, fließen in Sophos Fusion ein – ebenso wie jeder von einem Analysten gelöste Sonderfall und jede neue Umgebung, die in Betrieb genommen wird. Sophos X-Ops ergänzt dies durch seine eigene fundierte Expertise und Echtzeit-Threat-Intelligence, die anschließend automatisch an jedes Sophos-Produkt und jeden Kunden weitergeleitet werden, wodurch deren Abwehrmaßnahmen sich stetig verbessern.

Die Funktionsweise ist mit einem biologischen Immunsystem vergleichbar. Jede Bedrohung, der der Körper begegnet, wird Teil des permanenten Gedächtnisses – sie wird katalogisiert, verstanden und es werden Maßnahmen für ein erneutes Auftreten getroffen. Sophos Fusion funktioniert auf die gleiche Weise. Ein neuer Kunde ist vom ersten Tag an vor Bedrohungen geschützt, die er noch nie zuvor gesehen hat, weil das System sie bereits kennt.

Deshalb ist die Zahl von über 625.000 so wichtig. Sie spiegelt die Bandbreite an Erfahrungen wider, die gewährleistet, dass sich Schutz und Intelligence gegenseitig verstärken. Je mehr das System wahrnimmt, desto besser kann es alle schützen, die Teil des Systems sind.

Sophos Fusion: Wo Sie ein Cyber-Abwehrsystem in Aktion erleben

Das Sophos AI-Native Cybersecurity Defense System ist die Architektur. Sophos Fusion ist der Ort, an dem Sie dieses System in Aktion erleben. Ein zentraler Ort, an dem Sie Ihre Sophos-Kontrollpunkte verwalten, sich einen umfassenden Überblick über alle verbundenen Kontrollpunkte verschaffen und Maßnahmen ergreifen können.

Das bedeutet, dass Sie nichts zusätzlich kaufen oder aktivieren müssen und Ihre derzeitige Arbeitsweise nicht ändern müssen. Jeder Sophos-Kontrollpunkt ist bereits Teil von Sophos Fusion – sobald Sie einen bereitstellen, befinden Sie sich innerhalb der Architektur. Und je mehr Kontrollpunkte von Sophos und anderen Anbietern Sie hinzufügen, desto leistungsstärker wird das System – es liefert einen umfassenderen gemeinsamen Überblick und schafft zusätzlichen Mehrwert für alle Technologien, die Sie bereits im Einsatz haben.

Der Angriff aus der Perspektive von Sophos Fusion

Kehren wir zu dem mehrstufigen Angriff von vorhin zurück. Eine infizierte E-Mail, gestohlene Zugangsdaten, eine ungewöhnliche Anmeldung, eine Postfach-Weiterleitungsregel und laterale Bewegungen in Richtung sensibler Daten. In Sophos Fusion fließen Telemetriedaten von Sophos Email und der Microsoft-Umgebung des Kunden in den zentralen Context Lake. Sophos XDR korreliert diese Signale bei ihrem Eintreffen und erkennt die Sequenz als einen zusammenhängenden Angriff und nicht als fünf unabhängige Alerts.

Von dort aus koordiniert Synchronized Security™ die Reaktion über E-Mail, Identität, Endpoint und Netzwerk hinweg. Agentische KI agiert in maschineller Geschwindigkeit, während die Sophos MDR-Analysten direkt eingreifen und Entscheidungen in Hochrisikosituationen treffen. Ein Angriff, der isoliert agierende Produkte unbemerkt passieren kann, wird von einem System abgefangen, das den Gesamtzusammenhang im Blick hat.

Was Sophos Fusion für Sie bedeutet

Sophos Fusion sorgt für Cyberresilienz im Zeitalter der agentischen KI – und zwar in vier Bereichen, die für den Geschäftsbetrieb von zentraler Bedeutung sind.

- **Schutz vor KI-beschleunigten Bedrohungen, die sich schneller bewegen, als die Cyberabwehr reagieren kann.** Mehrstufige Angriffe werden frühzeitig erkannt und eingedämmt, selbst wenn sie per KI beschleunigt und potenziert werden, da jeder Kontrollpunkt Kontext teilt und gemeinsam reagiert, anstatt isoliert zu agieren.

- **Effektiverer Einsatz Ihrer Mitarbeitenden und Investitionen.** Agentische KI übernimmt die mühsame Routinearbeit der Triage und Reaktion, sodass Ihr bestehendes Team und bereits vorhandene Kontrollpunkte ganz ohne zusätzliches Personal oder Komplexität mehr erreichen. Jedes vernetzte Tool von Sophos oder anderen Anbietern trägt zum Ergebnis bei.

- **Compliance- und Cyber-Versicherungsvorteile.** Rund-um-die-Uhr-Abdeckung, über alle Ebenen hinweg beibehaltener Kontext und koordinierte Reaktionsmaßnahmen liefern Ihnen die Nachweise, die Auditoren, Regulierungsbehörden und Versicherer von einem durchsuchbaren Datensatz erwarten – anstelle von Protokollen, die manuell exportiert werden müssen. Dieselbe Architektur, die den Schutz verbessert, verbessert auch Ihre Fähigkeit, diesen Schutz nachzuweisen.

- **Eine auf Ihr Unternehmen abgestimmte Cybersecurity-Strategie.** Durch die Vernetzung und Koordination Ihrer Abwehrmaßnahmen ermöglicht Ihnen Sophos Fusion den Übergang von der Verwaltung taktischer Dashboards hin zu betrieblichem Vertrauen – mit klarer Transparenz darüber, wo Ihre Schwachstellen und größten Risiken liegen und ob sich Ihre Investitionen auszahlen. So können Unternehmen und Organisationen jeder Größe, mit oder ohne CISO, endlich die Strategie umsetzen, die sie sich schon immer gewünscht haben.

Alle Sophos-Kunden sind bereits Teil von Sophos Fusion, dem Sophos-Abwehrsystem. Es ist ein automatisches, nahtloses Upgrade, das Kunden vor Bedrohungen im KI-Zeitalter schützt.

Ihre ersten Schritte mit Sophos Fusion

Jede Sophos-Lösung ist Teil von Sophos Fusion, wodurch jede einzelne zu einem Einstiegspunkt und nicht zu einem isolierten Tool wird. Der Einstieg ist so einfach wie die Bereitstellung eines Sophos-Produkts oder -Services – Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall und Sophos Email sind beliebte Einstiegspunkte. Je mehr Lösungen Sie hinzufügen, desto mehr von der Architektur schalten Sie frei.

Dabei können Sie Kontrollpunkte anderer Anbieter weiterhin nutzen. Integrieren Sie diese einfach in Sophos Fusion, um kontinuierliche Echtzeit-Threat-Intelligence bereitzustellen und Reaktionsmaßnahmen auszuführen. Beginnen Sie dort, wo Ihr Risiko am größten ist, und erweitern Sie das System dann in Ihrem eigenen Tempo.

Sind Sie bereit für den nächsten Schritt? Sprechen Sie mit einem Sophos-Experten, um den richtigen Einstiegspunkt für Ihre Umgebung zu ermitteln, oder erfahren Sie mehr unter sophos.de/fusion.

Fazit

Jahrelang bestand die Standardreaktion auf jede neue Bedrohung darin, ein weiteres Produkt hinzuzufügen, und diese Gewohnheit schuf die Fragmentierung, die Angreifer heute ausnutzen. KI hat das Problem nur noch verschärft, indem sie die Kluft zwischen der Geschwindigkeit eines Angriffs und der Reaktionsgeschwindigkeit – bei der auf jeder einzelnen Konsole individuelle Maßnahmen ergriffen werden müssen – vergrößert hat. Mehr Produkte werden diese Lücke nicht schließen. Ein Cyber-Abwehrsystem schon.

Ein Cyber-Abwehrsystem verlagert den Schwerpunkt der Abwehr von einzelnen Produkten auf die Architektur, die diese miteinander verbindet:

- Ein gemeinsamer Überblick
- Koordinierte Reaktionsmaßnahmen auf allen Ebenen
- Integrierte KI, die in maschineller Geschwindigkeit agiert.
- Menschliche Experten, die dafür sorgen, dass Urteilsvermögen und Verantwortlichkeit dort bleiben, wo sie hingehören

Ihre Cybersecurity für das KI-Zeitalter zu wappnen, bedeutet, alle bereits vorhandenen Sicherheitstechnologien in einem System zu vereinen. Mit dem Sophos AI-Native Cybersecurity Defense System „Sophos Fusion“ können Sie dieses Modell in die Praxis umsetzen, ohne Ihre derzeitigen Lösungen ersetzen zu müssen.

Bereit, Ihre Cyberabwehr-Anforderungen für die KI-Ära zu besprechen?

Sprechen Sie noch heute mit einem Sophos-Experten.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 58580
E-Mail: sales@sophos.de