

WHITEPAPER

Erläuterung zu Synchronized Security™

SOPHOS

Synchronized Security

Synchronized Security™ ist das Herzstück von Sophos Fusion, dem branchenführenden KI-basierten Cyberabwehrsystem von Sophos. Es ist das verbindende Element, das die Erkenntnisse über Bedrohungen an allen angeschlossenen Kontrollpunkten – Sophos und Drittanbietern – in eine koordinierte Reaktion auf Bedrohungen umwandelt.

In ihrem Tech FutureSight: Schützen Sie die globale Angriffsfläche mit einem autonomen Cyberabwehrsystem.[1] Gartner stellte fest: „Organisationen benötigen eine intelligente Überlagerung, die die verschiedenen Elemente ihrer Cybersicherheitsinstrumente miteinander verbindet, um proaktiv und reaktiv auf Risiken und Bedrohungen in Maschinengeschwindigkeit reagieren zu können.“ Synchronized Security ist ein Schlüsselelement der Umsetzung in Sophos Fusion.

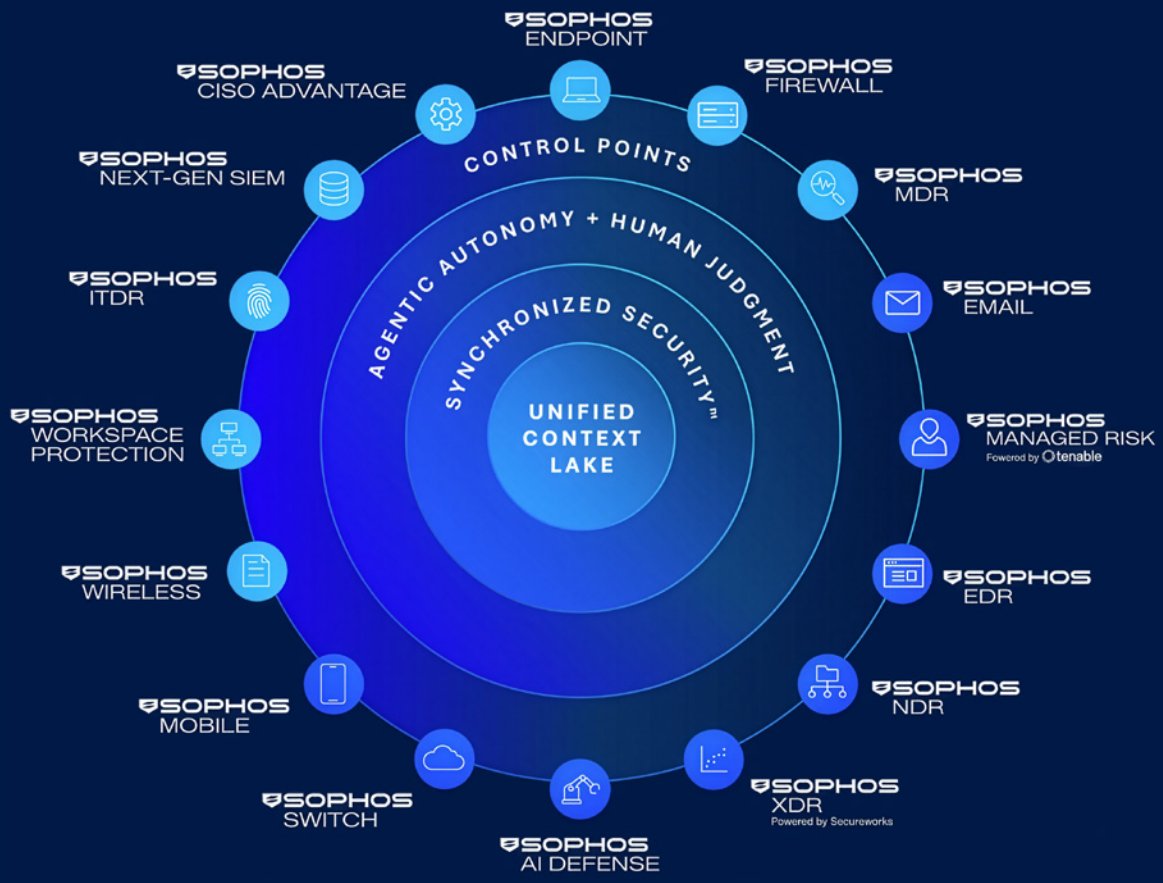
Dieser Leitfaden erklärt die Funktionsweise von Synchronized Security, die damit verbundenen Vorteile und wie Unternehmen diese nutzen können.

1 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.



Kurzzusammenfassung

- Synchronized Security ist ein Kernelement des Sophos Fusion-Sicherheitssystems und ist automatisch enthalten – es ist nicht nötig, ein zusätzliches Modul zu kaufen oder zusätzliche Komponenten zu lizenzieren.
- Es ermöglicht eine koordinierte Reaktion auf Bedrohungen über alle miteinander verbundenen Kontrollpunkte hinweg. Für den Einstieg sind zwei oder mehr Kontrollpunkte erforderlich, die innerhalb von Sophos Fusion zusammenarbeiten.
- Synchronized Security funktioniert sowohl mit Sophos als auch mit Nicht-Sophos-Kontrollpunkten. Die Reaktionsmaßnahmen in den einzelnen Kundenumgebungen hängen davon ab, welche Kontrollpunkte mit Sophos Fusion verbunden sind und welchen Grad an autonomer Handlungsfähigkeit der Kunde für jeden einzelnen Kontrollpunkt einräumt.
- Sophos XDR ist das Herzstück von Synchronized Security. Es korreliert Signale aus der gesamten Kundenumgebung zu einer einzigen Angriffskette und ermöglicht so automatisierte oder manuell gesteuerte Reaktionsmaßnahmen im gesamten Verteidigungssystem.
- Die Sophos-Lösungen können auch ohne Sophos XDR zusammenarbeiten und erhöhen damit die Synchronized Security-Tiefe.
- Synchronized Security baut auf den bewährten Basisfunktionen auf, die Sophos im Jahr 2015 eingeführt hat.



Warum eine koordinierte Reaktion wichtig ist

Historisch gesehen wurden Sicherheitstools so entwickelt, dass sie eine einzige Aufgabe gut erfüllen konnten. Ein Endpoint-Agent sichert das Gerät, auf dem er ausgeführt wird (z. B. Desktop-PC, Laptop oder Server). Eine Firewall überwacht den gesamten Datenverkehr im Netzwerk. Ein E-Mail-Dienst steuert, was im Posteingang landet. Jeder ist gut in seinem Bereich und blind für alles außerhalb davon.

Die Angreifer haben das schon vor langer Zeit verstanden. Ein moderner Einbruch ist kein einzelnes Ereignis an einem einzigen Ort. Es überschreitet bewusst die Grenzen von Identität, E-Mail, Endpunkt und Netzwerk, denn genau dort, wo die Schwachstellen liegen, nutzen Angreifer sie aus.

Die Konsequenz ist jedem bekannt, der schon einmal ein Sicherheitsteam geleitet hat. Einzellösungen betrachten nur ihren eigenen Bereich und identifizieren scheinbar unzusammenhängende Anomalien. Jeder einzelne scheint für sich genommen überlebbar zu sein. Niemand hat die Zeit oder den Kontext, um die Anomalien als ein und denselben Angriff zu erkennen, bis der Schaden bereits angerichtet ist.

Die KI hat die Lücken vergrößert. Die Angriffe erfolgen mittlerweile in Maschinengeschwindigkeit und in einem Ausmaß, wie es die Branche noch nie zuvor erlebt hat. Die meisten Verteidigungssysteme arbeiten jedoch immer noch in menschlicher Geschwindigkeit, wobei ein Analyst zwischen Konsolen hin und her wechselt und die Daten manuell korreliert.

Das Hinzufügen eines weiteren Produkts zur Umgebung schließt diese Lücke nicht. Stattdessen sollten Organisationen darauf achten, die Produkte miteinander zu verbinden, in die sie bereits investiert haben. Genau das leistet Synchronized Security innerhalb von Sophos Fusion.



Was Synchronized Security bietet

Durch Koordination werden Geschwindigkeit, Umfang und Reichweite der Bedrohungsreaktion verändert, was wiederum den Ausgang eines Angriffs beeinflusst. Wenn Endpunkte, Netzwerk und andere Kontrollpunkte zusammenwirken, erfolgt die Eindämmung in Sekundenschnelle – nicht erst, nachdem jemand es bemerkt und reagiert hat. Ein kompromittierter Endpoint wird sofort isoliert, bevor ein Angreifer lateral bewegen kann, sensible Daten erreicht oder Persistenz etabliert. Da die Reaktion automatisiert ist, funktioniert sie auch nachts und an Wochenenden, wenn die menschliche Präsenz oft eingeschränkt ist.

Durch Koordination werden auch die Lücken geschlossen, auf die Angreifer angewiesen sind. Drittanbieter-Kontrollpunkte, die zuvor lediglich Warnmeldungen auslösten, tragen nun aktiv zur Verteidigung bei. Bestehende Sicherheitsinvestitionen verbleiben nicht länger in Isolierung, sondern werden Teil der koordinierten Reaktion.

Die Auswirkungen auf den operativen Betrieb eines Sicherheitsteams sind unmittelbar. Die routinemäßige Eindämmung erfolgt ohne Eingreifen von Analysten. Wenn eine Analyse durch einen Menschen erforderlich ist, kann der Analyst auf einen bereits zusammengestellten, schichtübergreifenden Kontext zurückgreifen, anstatt ihn mühsam über mehrere Konsolen hinweg zusammenzutragen.

Durch die gleiche Koordination lässt sich der Schutz leichter nachweisen. Der schichtübergreifende Kontext bleibt erhalten, und eine koordinierte Reaktion hinterlässt eine konsistente Aufzeichnung darüber, was gefunden und was dagegen unternommen wurde. Das ist die Kontrollstrategie, die Wirtschaftsprüfer, Aufsichtsbehörden und Versicherer erwarten. Eine Architektur, die den Schutz verbessert, verbessert auch die Fähigkeit des Kunden, diesen Schutz nachzuweisen.

Die Verteidigung wird mit dem Wachstum ebenfalls stärker. Jeder neue Kontrollpunkt, der mit Sophos Fusion verbunden ist, sendet ein zusätzliches Signal in den einheitlichen Context Lake und eröffnet einen weiteren Reaktionspunkt – ohne dass der operative Aufwand entsprechend steigt. Mehr Abdeckung bedeutet nicht mehr Arbeit.

Für Managed Service Provider läuft die gleiche Koordination einheitlich in jeder Kundenumgebung ab, auch in solchen, die Sophos und Drittanbieter-Kontrollpunkte kombinieren. Die automatisierte Eindämmung reduziert den Aufwand für manuelle Triage und Bereinigung.

Funktionen

Synchronized Security beginnt mit Telemetrie. Jeder verbundene Kontrollpunkt meldet seine Beobachtungen in Echtzeit in den einheitlichen Context Lake. Endpoint-, Firewall-, E-Mail-, Cloud-, Netzwerk-, Identitäts- und Produktivitätstools speisen alle denselben Context Lake. Zusätzlich zu den Sophos-Kontrollpunkten speisen auch Kontrollpunkte von Drittanbietern den Context Lake. Es gibt keine Warteschlange zur Aggregation und keinen sekundären Datenspeicher, der später abgeglichen werden müsste.

Sophos XDR interpretiert das gemeinsame Bild und erledigt die Arbeit, die ein Analyst sonst manuell erledigen müsste. Es verknüpft zusammengehörige Ereignisse und löst sie zu einer einzigen Angriffskette auf, anstatt zu einer Reihe separater Warnmeldungen. Die Korrelation ist der entscheidende Aspekt, denn ein einzelner Kontrollpunkt erfasst immer nur einen Ausschnitt.

Die Reaktionsmaßnahmen werden dann wieder an die Kontrollpunkte zurückgeleitet. Sophos XDR liefert die Maschinen: SOAR-Automatisierung, Playbooks, Fall-Management und ein breites Spektrum an Reaktionsmaßnahmen. Die meisten laufen automatisch ohne menschliches Eingreifen. Wenn eine Beurteilung erforderlich ist, kann ein interner Analyst die gleiche Aktion manuell mit Sophos XDR auslösen, ebenso wie ein Sophos MDR Analyst.

Die bidirektionale Integration mit Kontrollpunkten von Drittanbietern ermöglicht es Sophos Fusion, Daten über die Integration abzurufen und zu senden. Beispielsweise:

- Es kann Telemetriedaten von einer Nicht-Sophos-Firewall abrufen und eine IP-Adresse zurücksenden, die von der Firewall blockiert werden soll.
- Die ServiceNow-Integration öffnet, aktualisiert und schließt Fälle.
- Die Active Threat Response-Funktion der Sophos Firewall nutzt API-gesteuerte Reaktionen auf Bedrohungsmeldungen von Drittanbietern, um kompromittierte oder nicht autorisierte Geräte aus dem Netzwerk zu entfernen.

Einzigartig ist auch, dass die Sophos-Kontrollpunkte direkt aufeinander einwirken, ohne dass Sophos XDR involviert ist. Der integrierte Security Heartbeat übermittelt den Gerätestatus eines Geräts von Sophos Endpoint an die anderen Sophos-Kontrollpunkte – ein grüner Status zeigt an, dass das Gerät gesund ist, ein gelber Status, dass es potenziell kompromittiert ist, und ein roter Status, dass es kompromittiert ist.

Die anderen Sophos-Kontrollpunkte sind darauf ausgelegt, auf den Gerätestatus zu reagieren. Sobald die Kontrollpunkte mit demselben Sophos Fusion-Konto verbunden sind, erfordern die Kernreaktionen keine zusätzliche Einrichtung. Funktionen, die den Gerätestatus nutzen, wie beispielsweise eine Firewall-Regel, die den Internetzugang beschränkt, oder eine Sophos Workspace Protection-Richtlinie, werden vom Kunden konfiguriert, bevor sie in Kraft treten.

Datenerfassung

Korrelieren

Reaktion

Sophos Fusion sammelt Telemetriedaten, Sophos XDR erstellt Kontext, und automatisierte Reaktionsmaßnahmen lenken die Durchsetzung an die Kontrollpunkte zurück.

Eine Funktion, mehrere Dimensionen der Koordination

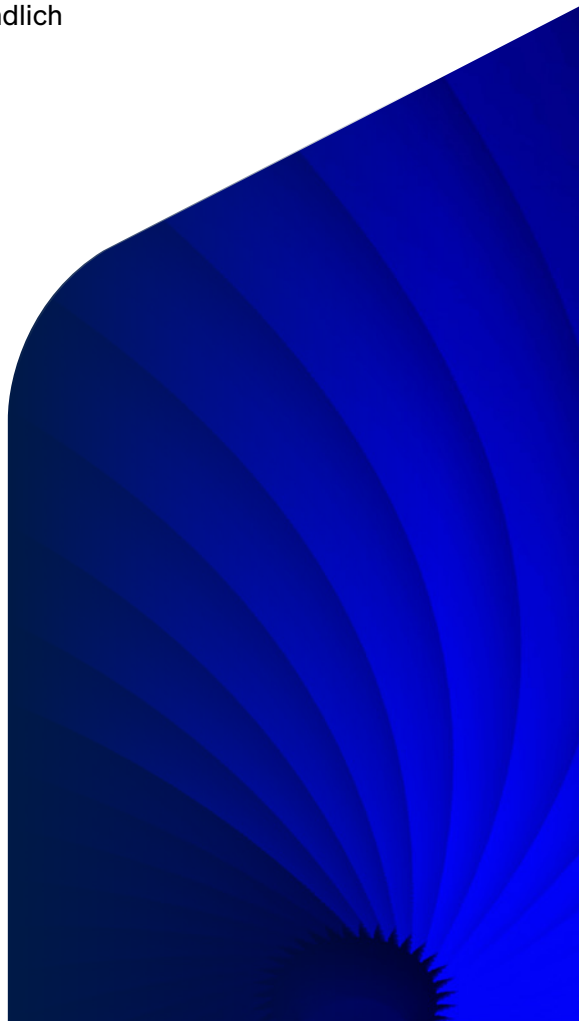
Synchronized Security wurde ursprünglich 2015 veröffentlicht und war damals eine Weltneuheit. In den mehr als einem Jahrzehnt seither hat sich der Funktionsumfang stetig erweitert. Der Grad der Koordination zwischen den Kontrollpunkten variiert von Kunde zu Kunde und hängt von der exakten Zusammensetzung der vorhandenen Kontrollpunkte ab.

Die Koordination ist zwischen den Sophos-Kontrollpunkten am stärksten ausgeprägt, da diese von Grund auf so konzipiert wurden, dass sie zusammenarbeiten. Die Kontrollpunkte von Drittanbietern werden über die Integrationen in Sophos Fusion eingebunden, und die Reaktionsmaßnahmen variieren, je nachdem, was der andere Anbieter bereitstellt.

Die Koordinationstiefe hängt auch davon ab, inwieweit ein Kunde Sophos Fusion die Kontrolle über jeden einzelnen Kontrollpunkt überträgt. Diese Wahlmöglichkeit liegt beim Kunden, und die Tatsache, dass sie besteht, ist der springende Punkt und kein Mangel. Fragt man die meisten Unternehmen und Organisationen, ob ein infizierter Endpoint ohne Genehmigung aus dem Netzwerk entfernt werden sollte, lautet die Antwort: Ja. Fragt man, ob ein System seine Firewall-Richtlinie selbstständig überarbeiten sollte, um die Gefährdung zu reduzieren, so fallen die Antworten unterschiedlich aus.

Firewalls sind ein Beispiel, das die Spannungen deutlich macht. Letztendlich ist das Blockieren eines kompromittierten Endpunkts eine Änderung der Firewall-Regeln. Viele Organisationen stehen automatisierten Änderungen an der Firewall-Konfiguration skeptisch gegenüber, und ihre Änderungskontrollprozesse existieren aus gutem Grund.

Kunden können ihre eigenen Automatisierungen und Playbooks schreiben und diese neben den von Sophos bereitgestellten ausführen. Ein Kunde, der Sophos Endpoint einsetzt, legt selbst fest, was ein kompromittiertes Gerät für seine Fortinet-Firewall bedeutet, und legt dabei fest, wie sich die Firewall verhält und wie sie konfiguriert ist. Sobald diese Automatisierungen festgelegt sind, laufen sie innerhalb von Sophos Fusion wie jede andere koordinierte Reaktion ab.



Synchronized Security in Aktion

Koordination lässt sich anhand von Beispielen leichter erkennen. Die folgenden Anwendungsfälle zeigen dieselbe Funktionalität in unterschiedlichen Tiefen und stellen keine Liste einzelner Funktionen dar.

Koordination zwischen Sophos -Produkten

Wenn Sophos Endpoint eine Bedrohung auf einem Endpunkt oder Server erkennt, wird der Security Heartbeat Integritätsstatus dieses Geräts auf Rot gesetzt. Der neue Status wird automatisch über den Security Heartbeat mit den anderen verbundenen Sophos Kontrollpunkten geteilt. Es folgen automatisch mehrere Antworten:

- Sophos Endpoint versucht, die Bedrohung zu beheben. Dies kann das Blockieren und Zurücksetzen der Verschlüsselung durch Ransomware oder den Einsatz einer höheren Kontrollstufe umfassen, um einen aktiver Angreifer in Schach zu halten.
- Die Sophos Firewall beschränkt den Internetzugang des Geräts, unterbricht jegliche Verbindung zu einem Command-and-Control-Server und verhindert, dass es auf gesunde Geräte zugreifen kann.
- Sophos Wireless, Sophos Switches und Sophos Workspace Protection beschränken den Zugriff des Geräts auf Netzwerkressourcen und begrenzen so die Auswirkungen der Kompromittierung weiter.
- Gesunde Endpoints werden über den roten Integritätsstatus informiert und weisen Netzwerkverbindungsanfragen des betroffenen Geräts zurück.

Derselbe Mechanismus erfasst auch Probleme, die sich niemals als Infektion bemerkbar machen. Ein Endpoint oder Server, der große Mengen an Spam- oder Phishing-E-Mails versendet, wird auf den roten Integritätsstatus gesetzt. Sophos Endpoint sucht dann nach bisher nicht identifizierten bösartigen Benutzern oder Anwendungen, und Sophos Email blockiert die Nachrichten, bevor sie den Posteingang erreichen.

Ein Endpoint oder Server kann je nach erforderlicher Bereinigung Sekunden oder sogar Tage im roten Integritätsstatus verbleiben. Nach der Reinigung wird der Integritätsstatus des Geräts wieder auf Grün gesetzt und der Zugriff im gesamten System automatisch wiederhergestellt.

Sein Wert zeigt sich am deutlichsten, wenn niemand zusieht. Ein Server, der spät am Freitagabend kompromittiert wird, wird innerhalb von Sekunden vom Netzwerk getrennt, statt einem Angreifer das ganze Wochenende Zeit zu geben, sich im Netzwerk auszubreiten.

SZENARIO

Sophos Endpoint erkennt eine Bedrohung und setzt den Security Heartbeat Integritätsstatus auf Rot. Der neue Status wird automatisch mit allen verbundenen Sophos Kontrollpunkten geteilt. Wenn die Bedrohung am Endpoint entfernt wurde, wird derselbe Zyklus befolgt, um den Zugriff wiederherzustellen.

SIGNAL

SOPHOS ENDPOINT

Erkennt eine Bedrohung

KOORDINIERTE REAKTION

SOPHOS FIREWALL

Unterbricht die Netzwerkverbindung und schränkt den Netzwerkzugriff ein.

SOPHOS WIRELESS

SOPHOS SWITCH

SOPHOS WORKSPACE PROTECTION

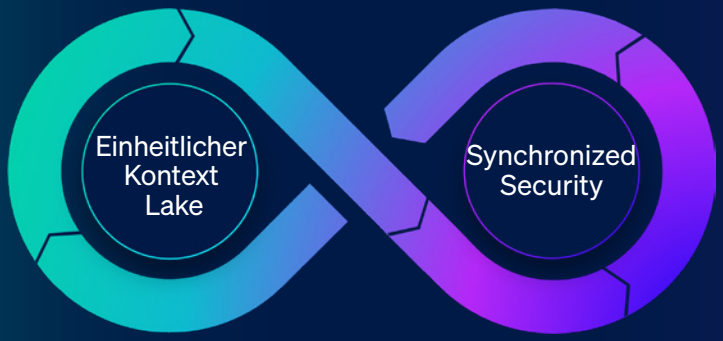
Den Zugriff des Geräts auf Netzwerkressourcen einschränken.

SOPHOS ENDPOINT

Gesunde Endpoints weisen die Netzwerkkommunikation zurück.

SOPHOS FUSION

AI-Native Cybersecurity Defense System



Sophos Endpoint und eine Firewall eines Drittanbieters

Die Koordination beschränkt sich nicht auf die Sophos Kontrollpunkte. Bei einem Kunden, der Sophos Endpoint zusammen mit einer Fortinet-Firewall betreibt, kann ein kompromittiertes Gerät eine Reaktion der Fortinet-Firewall auslösen. Der Kunde definiert, wie diese Reaktion aussieht und wie weit sie geht, wodurch die Automatisierung innerhalb seiner eigenen Änderungskontrollgrenzen bleibt. Die Automatisierungs- und Playbook-Funktionen (SOAR) von Sophos XDR machen dies möglich, indem sie mit der Fortinet-Integration in Sophos Fusion zusammenarbeiten.



Microsoft-Technologie und Telemetrie

Nahezu jede Organisation nutzt Microsoft-Technologie, und Identität ist der führende Angriffsvektor für Ransomware-Angriffe. Ein gestohlenes Session-Token oder ein kompromittiertes Konto bietet einem Angreifer einen legitimen Zugang, und selbst die beste Endpoint-Eindämmung hilft nichts, wenn das Konto selbst kompromittiert bleibt. Die Reaktion muss bis in die Microsoft-Umgebung hineinreichen, um die Bereinigung abzuschließen.

Das Sperren des Kontos ist das deutlichste Beispiel: Sophos Fusion kann ein kompromittiertes Microsoft-Konto sperren, um den Angreifer auszusperren, und es dann wieder entsperren, sobald das Konto wieder sicher verwendet werden kann. Das Konto wird wie jeder andere Kontrollpunkt behandelt – etwas, das das System sehen und auf das es reagieren kann, und nicht etwas, das ein Administrator im Nachhinein separat handhabt.

Die Integration ist bidirektional. Telemetriedaten aus einer Reihe von Microsoft-Quellen fließen in denselben einheitlichen Context Lake ein wie Sophos-Kontrollpunkte, Microsoft Entra ID und Microsoft Graph Security. Ein Microsoft-Signal kann also genauso gut eine Reaktion an einem Sophos Kontrollpunkt auslösen wie umgekehrt. Ein von Microsoft aufgedeckter verdächtiger Anmeldevorgang kann einen durch Sophos geschützten Endpunkt isolieren, ohne dass eine der beiden Seiten so konfiguriert ist, dass sie die andere überwacht.

Netzwerkrand, kabelgebunden und drahtlos

Switches und Access Points werden selten als Teil einer Verteidigung betrachtet. Es handelt sich um Infrastruktur, die angeschafft wurde, um den Datenverkehr zu lenken und die Menschen miteinander zu verbinden, und die meisten Unternehmen und Organisationen behandeln sie dementsprechend. Sie befinden sich jedoch an dem Punkt, an dem jedes Gerät auf das Netzwerk trifft, was sie zu einem der ersten Orte macht, an denen ein kompromittiertes oder nicht autorisiertes Gerät gestoppt werden kann.

In Sophos Fusion fungieren Sophos Switches und Sophos Wireless Access Points als Kontrollpunkte: Sie tragen dazu bei, was sie über verbundene Geräte sehen, und können auf die Erkenntnisse des Gesamtsystems reagieren. Administratoren können neue oder nicht autorisierte Geräte, Clients mit einer unerwarteten SSID oder ein Gerät, das an den falschen Switch-Port angeschlossen ist, identifizieren.

Active Threat Response, eine Funktion von Synchronized Security in der Sophos Firewall, setzt diesen Kontext in konkrete Maßnahmen um. Mithilfe der Telemetriedaten im einheitlichen Context Lake kann ein Gerät auf der kabelgebundenen oder drahtlosen Zugriffsschicht blockiert werden, bevor es sich weiter im Netzwerk ausbreitet. Die Kunden entscheiden selbst, ob sie Active Threat Response aktivieren, und behalten somit die Entscheidung, ob eine automatische Blockierung auf der Zugriffsebene zugelassen wird.

Bei Netzwerkgeräten von Drittanbietern gilt das gleiche Muster wie im obigen Beispiel der Firewall eines Drittanbieters.



Sophos AI Defense deckt Schatten-KI-Nutzung auf

Koordination beschränkt sich nicht nur auf Malware und Eindringversuche. Sophos AI Defense ist ein Kontrollpunkt in Sophos Fusion, der regelt, wie KI innerhalb einer Organisation eingesetzt wird. Es interpretiert KI-Aktivitätstelemetriedaten aus einer Vielzahl von Sophos-Produkten im einheitlichen Context Lake, zusammen mit allen anderen Signalen, die für Sophos EDR, Sophos XDR und Sophos MDR sichtbar sind. Sophos AI Defense ist darauf ausgelegt, die detaillierten Informationen zur KI-Nutzung aufzudecken, und sobald diese Informationen im einheitlichen Kontextsee vorliegen, durchlaufen sie dieselbe Synchronized Security-Funktionalität wie alles andere.

Schatten-KI zeigt, warum dies notwendig ist. Ein Mitarbeiter beginnt, ein KI-Tool zu nutzen, von dem niemand etwas weiß, und fügt Quellcode und Kundendatensätze hinein. Der Browser sieht die eingefügten Daten, der Endpoint sieht die Anwendung, und die Firewall sieht Traffic zu einem KI-Dienst von einem Gerät, das möglicherweise gar nicht verwaltet wird. Da kein Kontrollpunkt das Gesamtbild erfasst, bleibt das Werkzeug unentdeckt.

Sophos AI Defense sammelt diese Signale und wertet sie im Kontext aus, wodurch ein Security-Analyst die Beweise erhält, die er benötigt, um zu verstehen, was passiert ist. Es kombiniert Telemetriedaten wie Identität, Berechtigungen, Verhalten, Datenexposition und den Standort sowohl des Benutzers als auch des KI-Modells, wodurch die zulässige Nutzung von nicht verwalteten, übermäßig privilegierten oder gegen die Richtlinie verstoßenden Aktivitäten getrennt wird.

Die Durchsetzung erfolgt dann an den Kontrollpunkten:

- Sophos Workspace Protection kontrolliert den Browser, einschließlich Kopieren und Einfügen, Hochladen, Herunterladen und Erstellen von Screenshots.
- Sophos Endpoint beschränkt den Zugriff auf KI-Anwendungen und Websites über verschiedene Benutzergruppen und Gerätetypen hinweg.
- Die Sophos Firewall steuert den Traffic von KI-Diensten auf der Netzwerkschicht, einschließlich nicht verwalteter Geräte und Aktivitäten außerhalb des Browsers.
- Sophos Produkte können Eingabeaufforderungen, Uploads und KI-Interaktionen in Echtzeit überprüfen und dabei Quellcode, Kundendatensätze und Finanzdaten innerhalb des Unternehmens belassen.
- Ein Administrator kann über Sophos Fusion ein bestimmtes KI-Tool in der gesamten Umgebung blockieren.

Die Richtlinie ist nicht das Ende. Ein Verstoß oder unautorisiertes Agentenverhalten wird in denselben Sophos EDR, Sophos XDR- und Sophos MDR Workflows angezeigt wie jede andere Erkennung und mit den Automatisierungen und Playbooks behandelt, die bereits für Identitäts-, Endpunkt- und Netzwerkbedrohungen verwendet werden. Wie weit die Koordination reicht, hängt davon ab, welche Kontrollpunkte mit Sophos Fusion verbunden sind.

82 %

82 % der Unternehmen und Organisationen haben unbekannte KI-Tools oder Workflows in ihrer Umgebung entdeckt.[2]

2 Cloud Security Alliance, Das Problem des Schatten-KI-Agenten in Unternehmensumgebungen, 2025

Koordination über die Bedrohungsreaktion hinaus.

Die Koordination zwischen den Sophos-Kontrollpunkten geht über die bloße Übermittlung einer Bedrohungsbewertung hinaus. Ein Kontrollpunkt kann einem anderen eine direkte Frage stellen und entsprechend der Antwort handeln. Ein durch Sophos Endpoint geschützter Endpunkt oder Server weiß bereits das meiste über den Traffic, was eine Sophos Firewall Ihnen nicht mitteilen kann. Drei Beispiele verdeutlichen, was dadurch möglich wird: die Identifizierung der Anwendung hinter dem Traffic auf einem Port, die Identifizierung des Benutzers hinter einer Sitzung und die Entscheidung, ob ein Gerät überhaupt für den Zugriff geeignet ist.

Synchronized Application Control

Nehmen Sie eine nicht klassifizierte Verbindung über einen ungewöhnlichen Port auf. Eine Firewall, die dies isoliert betrachtet, sieht lediglich einen Datenstrom und sonst kaum etwas. Die Sophos Firewall kann den Sophos Endpoint fragen, welche Anwendung auf diesem Port sendet und empfängt, und erhält eine Antwort darüber, welche Anwendung dafür verantwortlich ist. Auf dieser Grundlage können Kunden die Anwendung dann zulassen oder blockieren. Mit der Zeit entsteht so auch ein genaues Bild davon, was im Netzwerk läuft, und das ist in der Regel vielfältiger, als man erwartet.

Identitäten, nicht IP-Adressen

Die Benutzeridentität funktioniert auf die gleiche Weise. Sophos Endpoint leitet authentifizierte Benutzerinformationen an Sophos Firewall weiter, sodass Richtlinien um Personen und deren Identität herum geschrieben werden können, anstatt um Benutzer- oder IP-Adressen, die sich ändern. Dadurch entfällt eine Kartierungsübung, die Administratoren sonst manuell durchführen müssten und die dazu neigt, zu veralten.

Nur Geräte mit Integritätsstatus verbinden sich.

Auch die Zugriffsentscheidungen profitieren davon; ein herkömmliches VPN hat keine Möglichkeit zu wissen, ob ein Gerät einen guten Integritätsstatus aufweist oder nicht, und lässt den Endpoint nur auf der Grundlage seiner Zugangsdaten zu. Allerdings überprüft Sophos Workspace Protection den Integritätsstatus des Geräts mit Sophos Endpoint, bevor der Zugriff gewährt wird, sodass ein kompromittierter Endpoint niemals Netzwerkanwendungen oder Daten erreichen kann.

Solche Austausche sind nicht fest definiert. Jeder Austausch existiert, weil er von Sophos entwickelt wurde, und Sophos hat die Funktionalitäten im Laufe der Zeit stetig erweitert. Der Datenaustausch zwischen den Sophos-Kontrollpunkten ist heute wesentlich umfangreicher als vor zehn Jahren.

Nichts davon beginnt als Bedrohungsreaktion, aber es bleibt selten davon getrennt. Eine Anwendung, für die niemand verantwortlich ist, oder ein Benutzer, der sich an einem Ort anmeldet, an dem er nichts zu suchen hat, ist bis zu dem Moment, in dem es das nicht mehr ist, ein normales Betriebsdetail. Eine Transparenz, die den Betrieb eines Netzwerks erleichtert, macht es auch einfacher, aufkommende Bedrohungen zu erkennen.

Eine koordinierte Reaktion in einem hybriden Umfeld

Dieses Praxisbeispiel von Sophos MDR zeigt Synchronized Security in Aktion. Bei der betroffenen Organisation handelte es sich um einen Sophos MDR-Kunden, der Sophos Endpoint und Sophos Email sowie Microsoft Entra ID, Microsoft Graph Security und eine Fortinet-Firewall einsetzte. Sie betrieben außerdem eine Sophos Firewall in einem separaten Netzwerk. Jeder dieser Kontrollpunkte speiste denselben einheitlichen Kontextsee.

- Der Angreifer begann mit einem KI-gestützten Köder, indem er eine Phishing-Seite verwendete, die auf einer legitimen Website gehostet wurde. Der Benutzer klickte und gab sein Passwort ein.
- Das Kit hat das Live-Session-Token anstatt der Zugangsdaten gestohlen. Dadurch gelang es dem Angreifer, die Multi-Faktor-Authentifizierung zu umgehen, wodurch ein Zurücksetzen des Passworts wirkungslos wurde.
- Der Angreifer meldete sich über eine bekannte Angreiferinfrastruktur an und erstellte eine Regel für einen stillen Posteingang, die alle E-Mails eines bestimmten Lieferanten ausblendete. Dies ist die Grundlage für Drahtbetrug.
- Vier Kontrollpunkte registrierten etwas Verdächtiges – Sophos Endpoint, zwei Microsoft-Lösungen und die Fortinet-Firewall. Kein einzelnes Signal war laut genug, um eine Reaktion auszulösen.
- Eine speziell entwickelte Sophos-Erkennung wurde ausgelöst und die einzelnen Signale wurden zu einer einzigen Angriffskette zusammengeführt.
- Der Anmeldevorgang wurde blockiert, die Sitzungen wurden widerrufen, und der Endpoint wurde erfolgreich isoliert. Bösartige IP-Adressen wurden an der Sophos Firewall mithilfe von Telemetriedaten, die von der Fortinet Firewall erfasst wurden, blockiert.

Ein Mensch schloss daraufhin den Fall ab. Ein Analyst bestätigte, dass die Posteingangsregel einen bestimmten Lieferanten nannte, was darauf hindeutete, dass es sich um eine Vorbereitung für Drahtbetrug handelte.



Wie Kunden Synchronized Security aktivieren

Synchronized Security ist kein Produkt, keine SKU und kein Add-on, und es fallen keine zusätzlichen Lizenzgebühren an. Kunden erhalten diese Funktion automatisch, wenn zwei oder mehr Kontrollpunkte innerhalb von Sophos Fusion zusammenarbeiten, unabhängig davon, ob es sich bei den Kontrollpunkten um Sophos oder Nicht-Sophos-Produkte handelt.

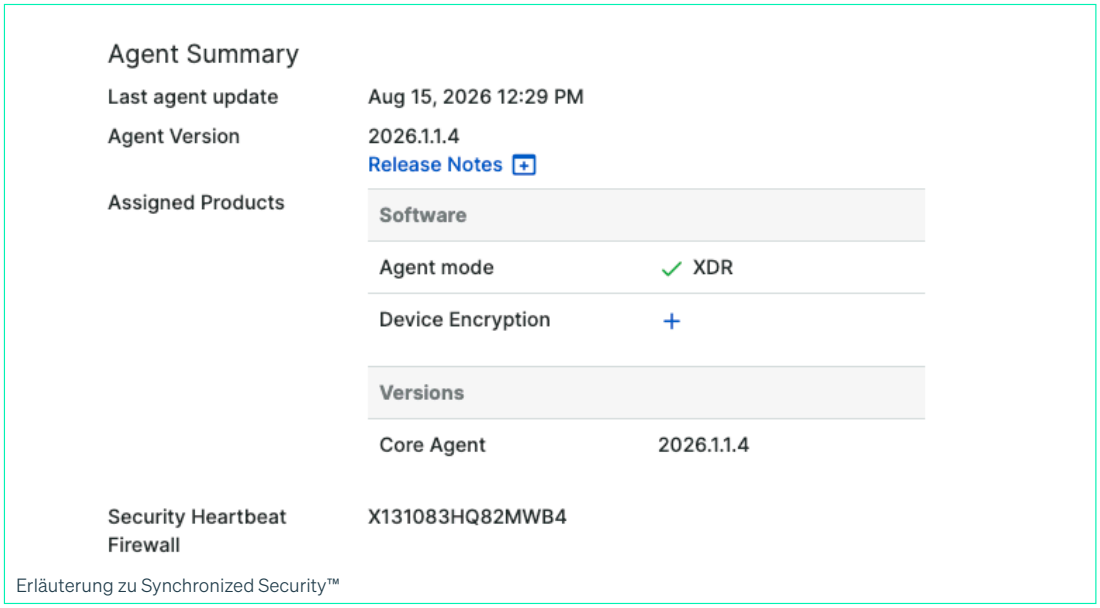
Die Verwaltung von Sophos Endpoint und Sophos Firewall über dasselbe Sophos Fusion-Konto ist ein häufiger Ausgangspunkt. Die Koordination zwischen ihnen ist aktiv, sobald beide mit diesem Konto verbunden sind; es ist keine weitere Konfiguration erforderlich. Anwendungsfälle, die auf dem Integritätsstatus aufbauen, wie z. B. die Verwendung des Integritätsstatus als Teil von Firewall-Regeln oder Sophos Workspace Protection Richtlinien, werden vom Kunden eingerichtet.

Die Koordination mit Kontrollpunkten von Drittanbietern beginnt mit der Integration des Kontrollpunkts in Sophos Fusion, das native Sophos Integrationen und über 500 Drittanbieterintegrationen unterstützt. Der Umfang der verfügbaren automatisierten Reaktionen variiert jedoch von Kontrollpunkt zu Kontrollpunkt. Active Threat Response in Sophos-Kontrollpunkten ist ein Beispiel dafür; sie wird vom Kunden aktiviert und ist nicht standardmäßig aktiviert.

Sophos bietet Automatisierungen und Playbooks, die über Synchronized Security automatisch ausgeführt werden und ein breites Spektrum an Anwendungsfällen abdecken. Wie oben beschrieben, können Kunden ihre eigenen Automatisierungen hinzufügen, wenn eine Standardautomatisierung nicht zu ihrer Umgebung passt.

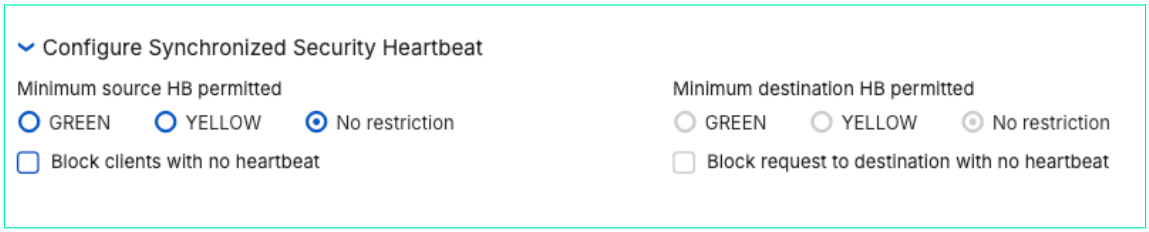
Sophos Endpoint koordiniert mit der Sophos Firewall

Um zu überprüfen, ob Sophos Endpoint mit einer Firewall kommuniziert, öffnen Sie die Computerübersicht in Sophos Fusion. Hier wird die Seriennummer der Sophos Firewall angezeigt, die den Security Heartbeat dieses Endpoints empfängt.



Sophos Firewall Richtlinien mit Synchronized Security

Eine Firewall-Regel kann optional einen grünen Integritätsstatus vorschreiben, bevor ein Gerät auf das Internet zugreifen darf. Ungeschützte Geräte (d. h. solche, auf denen Sophos Endpoint nicht läuft) könnten dann keine Verbindung herstellen, ebenso wenig wie Geräte mit einem fragwürdigen Integritätsstatus.



Zusammenführung

Das Problem war nie ein Mangel an Sicherheitswerkzeugen. Das Problem liegt darin, dass die Werkzeuge, die ein Unternehmen bereits besitzt, dazu neigen, isoliert zu arbeiten, und Angreifer haben ihre Methoden so entwickelt, dass sie die Lücken zwischen ihnen ausnutzen. Synchronized Security ermöglicht es Ihren Sicherheitswerkzeugen, als einheitliche und koordinierte Verteidigung zusammenzuarbeiten.

Wenn Sie zwei oder mehr Kontrollpunkte in Sophos Fusion verwenden, arbeitet Synchronized Security bereits in Ihrem Auftrag. Wenn Sie weitere Kontrollpunkte verbinden, wird die Reichweite noch größer. Die Nicht-Sophos-Werkzeuge, in die Sie bereits investiert haben, werden in die Reaktionsmaßnahmen einbezogen, anstatt nur von der Seitenlinie aus zu berichten.

Wie viel automatisch ausgeführt wird, bleibt Ihre Entscheidung. Eine Koordination, die Ihre Änderungskontrollprozesse ignoriert, wäre nicht sinnvoll. Daher bestimmen Sie die Tiefe der Automatisierung selbst, Kontrollpunkt für Kontrollpunkt.

Das ist der praktische Nutzen des Sophos Cyber Defense System. Nicht eine längere Liste von Produkten, sondern die, die Sie bereits einsetzen, reagieren gemeinsam mit Maschinengeschwindigkeit – schneller, als ein KI-beschleunigter Angriff sich zwischen ihnen bewegen kann.

Um mehr zu erfahren, besuchen Sie www.sophos.com/synchronizedsecurity

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

© Copyright 2026. 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 erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.