

WHITE PAPER

Spiegazione di Synchronized Security™

SOPHOS

Synchronized Security

Synchronized Security™ è il cuore pulsante di Sophos Fusion, il sistema di difesa AI-native leader di settore di Sophos. È il tessuto connettivo che trasforma le informazioni sulle minacce su tutti i punti di controllo connessi (Sophos e di terze parti) in una risposta coordinata alle minacce.

Nel loro FutureSight tecnologico: Proteggi la superficie di attacco globale con un sistema di cyber difesa autonomo[1], Gartner ha identificato che "le aziende hanno bisogno di una copertura intelligente che colleghi i diversi elementi del loro set di strumenti di cybersecurity per rispondere proattivamente e reattivamente ai rischi e alle minacce alla velocità della macchina". Synchronized Security è un elemento chiave per l'implementazione di questa funzionalità in Sophos Fusion.

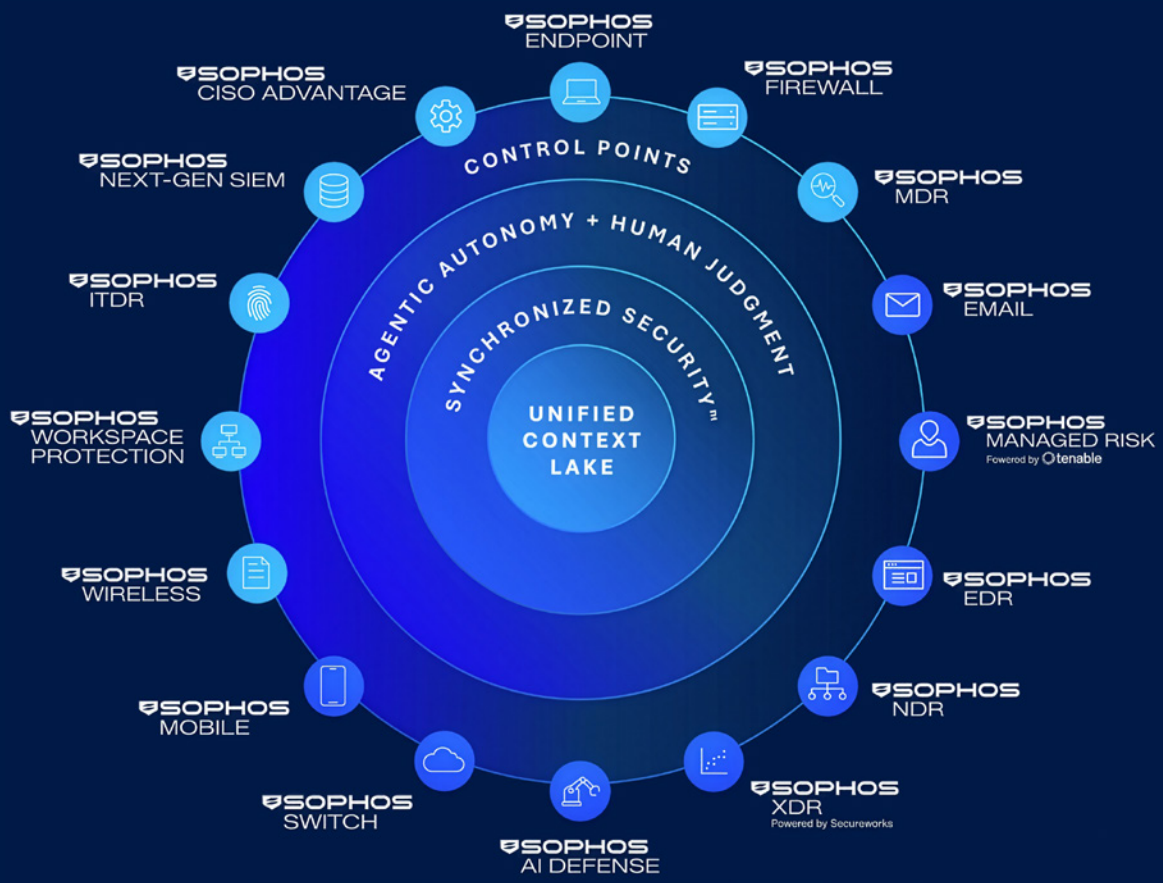
Questa guida descrive come funziona Synchronized Security, i vantaggi che offre e come può essere sfruttata dalle aziende.

1 Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System (Proteggere la superficie di attacco globale con un sistema di cyber difesa autonomo), Neil MacDonald, 12 dicembre 2025. GARTNER è un marchio di Gartner, Inc. e/o delle sue affiliate.



Riepilogo rapido

- Synchronized Security è un elemento fondamentale del sistema di difesa Sophos Fusion ed è incluso automaticamente, senza bisogno di acquistare moduli aggiuntivi o componenti aggiuntivi per le licenze.
- Consente una risposta coordinata alle minacce su tutti i punti di controllo connessi. Per cominciare, occorrono due o più punti di controllo che interagiscono all'interno di Sophos Fusion.
- Synchronized Security è compatibile sia con i punti di controllo Sophos che con quelli non Sophos. Le azioni di risposta nei singoli ambienti dei clienti dipendono dai controlli connessi a Sophos Fusion e dal livello di azione autonoma che il cliente concede su ciascun punto di controllo.
- Sophos XDR è il cuore pulsante della Synchronized Security, in quanto mette in correlazione i segnali provenienti dall'intero ambiente del cliente in un'unica catena di attacco e consente azioni di risposta automatizzate o coordinate da menti umane nell'intero sistema di cyber difesa.
- Le soluzioni Sophos possono anche funzionare insieme senza Sophos XDR, aggiungendo una profondità aggiuntiva di Synchronized Security.
- Synchronized Security si basa sulle funzionalità di base dall'efficacia comprovata che Sophos ha introdotto nel 2015.



Perché una risposta coordinata è importante

Storicamente, gli strumenti di sicurezza sono stati progettati per svolgere bene un solo lavoro. Un agente endpoint protegge il dispositivo su cui viene eseguito (ad es. desktop, laptop o server). Un firewall monitora ciò che attraversa la rete. Un servizio e-mail controlla ciò che arriva nella casella di posta. Ciascuno è bravo nel suo lavoro e cieco rispetto a tutto ciò che è al di fuori.

Gli attaccanti lo hanno capito molto tempo fa. Un'intrusione moderna non è un singolo evento in un unico luogo. Attraversa identità, e-mail, endpoint e rete per progettazione, perché lo spazio tra di essi è esattamente dove si trovano le lacune e gli attaccanti le sfruttano.

La conseguenza è nota a chiunque abbia gestito un team di sicurezza. Le singole soluzioni vedono solo il proprio dominio, identificando anomalie apparentemente disparate. Ognuna sembra in grado di sopravvivere da sola. Nessuno ha il tempo o il contesto per riconoscere le anomalie come lo stesso attacco finché il danno non è già stato fatto.

L'IA ha ampliato le lacune. Gli attacchi ora si svolgono a velocità della macchina e a volumi mai osservati prima. Tuttavia, nella maggior parte dei casi le difese continuano a funzionare a velocità umana, con un analista che si sposta da una console all'altra e correla a mano.

L'aggiunta di un altro prodotto all'ambiente non colma questa lacuna. Le aziende dovrebbero invece cercare di connettere i prodotti in cui hanno già investito. Questo è esattamente ciò che Synchronized Security fa in Sophos Fusion.



Cosa offre Synchronized Security

Il coordinamento trasforma la velocità, la portata e l'ambito della risposta alle minacce, cambiando l'esito di un attacco. Quando endpoint, rete e altri controlli agiscono insieme, il contenimento avviene nel giro di pochi secondi, non dopo che qualcuno se ne accorge e reagisce. Un endpoint compromesso viene isolato immediatamente prima che un attaccante possa spostarsi lateralmente, raggiungere dati sensibili o stabilire la persistenza. Inoltre, poiché la risposta è automatizzata, funziona di notte e nel fine settimana, quando la copertura umana è spesso ridotta.

Il coordinamento colma anche le lacune su cui si basano gli attaccanti. I punti di controllo di terze parti che prima generavano solo avvisi cominciano invece a contribuire attivamente alla difesa. Gli attuali investimenti nella sicurezza smettono di rimanere isolati e diventano parte della risposta coordinata.

L'impatto operativo su un team di sicurezza è immediato. Il contenimento di routine avviene senza l'intervento di analisti. Quando è richiesta un'indagine umana, l'analista comincia con un contesto a livelli multipli già assemblato, invece di metterlo insieme a mano su più console.

Lo stesso coordinamento semplifica la dimostrazione della protezione. Viene conservato il contesto a livelli multipli e una risposta coordinata lascia un resoconto coerente di ciò che è stato trovato e di ciò che è stato fatto al riguardo. Questo è il controllo narrativo che revisori, enti normativi e compagnie di assicurazioni si aspettano. L'architettura che migliora la protezione migliora anche la capacità del cliente di dimostrarlo.

Anche la difesa si rafforza man mano che cresce. Ogni nuovo punto di controllo connesso a Sophos Fusion invia un segnale aggiuntivo all'unified Context Lake e apre un altro punto di risposta, senza un aumento dell'impegno operativo. Più copertura non significa più lavoro.

Per i Managed Service Provider, lo stesso coordinamento viene applicato in maniera coerente a tutti gli ambienti dei clienti, inclusi quelli che utilizzano la combinazione di punti di controllo Sophos e di terze parti. Il contenimento automatico riduce il carico di lavoro legato al triage e alla remediation manuale.

Come funziona

Synchronized Security comincia con la telemetria. Ciascun punto di controllo connesso segnala ciò che vede nel Context Lake in tempo reale. Endpoint, firewall, e-mail, cloud, rete, identità e strumenti di produttività alimentano tutti lo stesso Context Lake. I punti di controllo di terze parti lo alimentano insieme a quelli Sophos. In una coda non c'è niente in attesa di essere aggregato e non c'è un archivio dati secondario da riconciliare in un secondo momento.

Sophos XDR interpreta il quadro condiviso e svolge il lavoro che un analista farebbe altrimenti a mano. Mette in correlazione gli eventi correlati e li risolve in un'unica catena di attacco, invece di una serie di avvisi separati. La correlazione è la parte che conta, perché un punto di controllo vede sempre e solo un frammento.

Le azioni di risposta vengono quindi inviate ai punti di controllo. Sophos XDR fornisce i macchinari: Automazione SOAR, playbook, gestione dei casi e un ampio set di azioni di risposta. La maggior parte si esegue automaticamente senza intervento umano. Laddove sia necessario il giudizio, un analista interno può attivare la stessa azione manualmente utilizzando Sophos XDR, così come può farlo un analista di Sophos MDR.

Grazie all'integrazione bidirezionale con punti di controllo di terze parti, Sophos Fusion è in grado di estrarre e inviare dati attraverso l'integrazione. Alcuni esempi:

- Può recuperare dati di telemetria da un firewall non Sophos e inviare un indirizzo IP affinché il firewall lo blocchi.
- L'integrazione ServiceNow apre, aggiorna e chiude i casi.
- Risposta alle minacce attive in Sophos Firewall utilizza risposte attivate tramite API a feed sulle minacce di terze parti per escludere dalla rete un dispositivo compromesso o non autorizzato.

Esclusivamente, i punti di controllo Sophos agiscono anche uno sull'altro in maniera diretta, senza alcun coinvolgimento da parte di Sophos XDR. Il Security Heartbeat integrato trasmette lo stato di integrità di un dispositivo da Sophos Endpoint agli altri punti di controllo Sophos: uno stato verde indica un dispositivo sano, uno stato giallo segnala una potenziale compromissione e uno stato rosso indica una compromissione.

Gli altri punti di controllo Sophos sono progettati per agire sullo stato di integrità del dispositivo. Una volta connessi i punti di controllo allo stesso account Sophos Fusion, le risposte principali non richiedono alcuna configurazione aggiuntiva. Le funzionalità che sfruttano lo stato di integrità, come una regola firewall che blocca l'accesso a Internet o un criterio Sophos Workspace Protection, vengono configurate dal cliente prima di essere implementate.

Raccolta

Correlazione

Risposta

Sophos Fusion raccoglie dati di telemetria, Sophos XDR crea il contesto e le azioni di risposta automatizzate applicano le misure ai punti di controllo.

Una funzionalità, molteplici dimensioni di coordinamento.

Synchronized Security è stata rilasciata inizialmente nel 2015, una novità assoluta per l'epoca, e da allora ha subito un'espansione della sua portata negli oltre dieci anni. La profondità del coordinamento tra i punti di controllo Sophos varia da un ambiente all'altro, in funzione del mix esatto di punti di controllo implementati.

La coordinazione è più profonda tra i punti di controllo Sophos, in quanto sono progettati per interagire fin dalle basi. I punti di controllo di terze parti si uniscono attraverso le integrazioni in Sophos Fusion e le azioni di risposta variano a seconda di ciò che l'altro vendor espone.

La profondità di coordinamento dipende anche dal livello di controllo che un cliente concede a Sophos Fusion su ciascun punto di controllo. Questa scelta spetta al cliente e il fatto che essa esista rappresenta il vero punto, anziché essere una carenza. Chiedi alla maggior parte delle organizzazioni se un endpoint infetto debba essere rimosso dalla rete senza che nessuno lo approvi, e la risposta è sì. Chiedi se un sistema debba riscrivere un criterio Sophos Firewall per ridurre l'esposizione ai rischi in maniera autonoma e la risposta è diversa.

I firewall sono l'esempio che rende evidente la tensione. Alla fine, il blocco di un endpoint compromesso è una modifica delle regole firewall. Molte organizzazioni sono caute delle modifiche automatiche alla configurazione del firewall e i loro processi di controllo delle modifiche esistono per una buona ragione.

I clienti possono scrivere le proprie automazioni e playbook ed eseguirli insieme a quelli forniti da Sophos. Un cliente che esegue Sophos Endpoint decide autonomamente cosa significa un dispositivo compromesso per il proprio firewall Fortinet, descrivendo come si comporta e come viene configurato il firewall. Una volta scritte, queste automazioni vengono eseguite all'interno di Sophos Fusion come qualsiasi altra risposta coordinata.



La Synchronized Security in azione

Il coordinamento è più facile da riconoscere con esempi. I casi di utilizzo riportati di seguito mostrano la stessa funzionalità che opera a profondità diverse, piuttosto che un elenco di funzionalità separate.

Coordinamento tra i prodotti Sophos

Quando Sophos Endpoint rileva una minaccia su un endpoint o su un server, imposta, tramite il Security Heartbeat, lo stato di integrità del dispositivo su Rosso. Il nuovo stato viene automaticamente condiviso con gli altri punti di controllo Sophos connessi tramite Security Heartbeat. Seguono automaticamente diverse risposte:

- Sophos Endpoint effettua tentativi di correzione della minaccia, che possono includere il blocco e il ripristino della crittografia tramite ransomware, oppure l'implementazione di un livello di controllo più elevato per bloccare un active adversary.
- Sophos Firewall limita l'accesso a Internet del dispositivo, interrompendo qualsiasi connessione a un server di comando e controllo e impedendo che raggiunga dispositivi integri.
- Sophos Wireless, Sophos Switch e Sophos Workspace Protection limitano l'accesso del dispositivo alle risorse di rete, limitando ulteriormente l'impatto della compromissione.
- Gli endpoint integri vengono informati dello stato di integrità Rosso e rifiuteranno le richieste di connessione di rete provenienti dal dispositivo interessato.

Lo stesso meccanismo individua i problemi che non si annunciano mai come infezioni. Un endpoint o server che invia grandi volumi di e-mail di spam o phishing è impostato su uno stato di integrità Rosso. Sophos Endpoint cerca quindi utenti o applicazioni malevole precedentemente non identificati e Sophos Email blocca i messaggi prima che raggiungano una casella di posta.

Un endpoint o server può rimanere in stato di integrità Rosso per secondi o persino giorni, a seconda della correzione richiesta. Una volta che il dispositivo risulta pulito, il suo stato di integrità torna Verde e l'accesso viene ripristinato automaticamente in tutto il sistema.

Il valore emerge più chiaramente quando nessuno osserva. Un server compromesso a tarda notte di venerdì sera viene bloccato nel giro di pochi secondi, invece di concedere all'avversario l'intero fine settimana per muoversi all'interno della rete.

SCENARIO

Sophos Endpoint rileva una minaccia e imposta lo stato di integrità di Security Heartbeat su Rosso. Il nuovo stato viene condiviso automaticamente con tutti i punti di controllo Sophos connessi. Quando la minaccia sull'endpoint viene rimossa, viene seguito lo stesso ciclo per ripristinare l'accesso.

SIGNAL

SOPHOS ENDPOINT

Rileva una minaccia

RISPOSTA COORDINATA

SOPHOS FIREWALL

Rimuove la connettività di rete e limita l'accesso alla rete.

SOPHOS WIRELESS

SOPHOS SWITCH

SOPHOS WORKSPACE PROTECTION

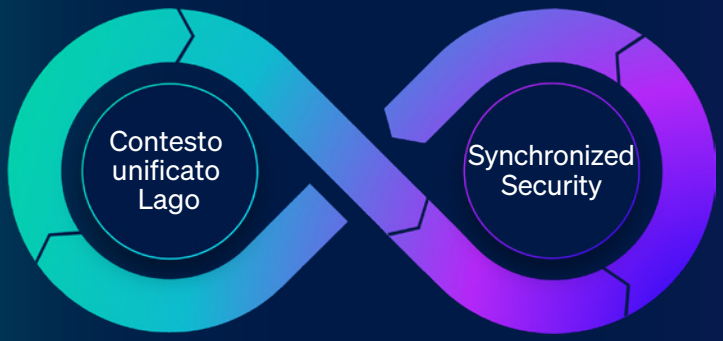
Limitare l'accesso del dispositivo alle risorse di rete.

SOPHOS ENDPOINT

Endpoint integri rifiutano le comunicazioni di rete.

SOPHOS FUSION

AI-Native Cybersecurity Defense System



Sophos Endpoint e un firewall di terze parti.

Il coordinamento non è limitato ai punti di controllo Sophos. Un cliente che utilizza Sophos Endpoint insieme a un firewall Fortinet può far sì che un dispositivo compromesso attivi una risposta sul firewall Fortinet. Il cliente definisce quale sia quella risposta e fino a che punto si estende, mantenendo così l'automazione entro i limiti del proprio controllo delle modifiche. Le capacità di automazione e playbook (SOAR) di Sophos XDR rendono tutto ciò possibile, in collaborazione con l'integrazione Fortinet in Sophos Fusion.

Tecnologia e telemetria Microsoft.

Quasi tutte le aziende utilizzano tecnologia Microsoft e l'identità è il vettore principale per gli attacchi ransomware. Un token di sessione rubato o un account compromesso danno all'attaccante un modo legittimo per accedere, e nessun contenimento dell'endpoint aiuta se l'account stesso rimane compromesso. La risposta deve estendersi anche all'ambiente Microsoft per completare la correzione.

Bloccare l'account è l'esempio più chiaro: Sophos Fusion è in grado di bloccare un account Microsoft compromesso per impedire l'accesso all'attaccante e sbloccarlo una volta che l'account può essere nuovamente utilizzato in sicurezza. L'account viene trattato come un punto di controllo come qualsiasi altro – qualcosa che il sistema può monitorare e gestire, e non qualcosa che un amministratore deve trattare separatamente in seguito.

L'integrazione è bidirezionale. I dati di telemetria provenienti da varie fonti Microsoft alimentano lo stesso Context Lake unificato dei punti di controllo Sophos, tra cui Microsoft Entra ID e Microsoft Graph Security. Pertanto, un segnale Microsoft può innescare una risposta in un punto di controllo Sophos tanto facilmente quanto avviene il contrario. Un accesso sospetto rilevato da Microsoft può isolare un endpoint protetto da Sophos, senza che nessuna delle due parti sia configurata per monitorare l'altra.



Il perimetro di rete, cablato e wireless.

Gli switch e gli access point sono raramente considerati parte della difesa. Sono considerate infrastrutture acquistate per spostare il traffico e mantenere connesse le persone, e la maggior parte delle aziende le gestisce di conseguenza. Tuttavia, essi si trovano nel punto in cui ogni dispositivo si connette alla rete, il che li rende uno dei primi luoghi in cui un dispositivo compromesso o non autorizzato può essere fermato.

In Sophos Fusion, gli switch Sophos e gli access point wireless Sophos Wireless svolgono la funzione di punti di controllo: contribuiscono con ciò che vedono sui dispositivi connessi e possono agire in base a ciò che viene rilevato dal sistema in generale. Gli amministratori possono identificare dispositivi nuovi o non autorizzati, client su uno SSID inatteso o un dispositivo connesso alla porta sbagliata dello switch.

Risposta alle minacce attive, una funzionalità di Synchronized Security in Sophos Firewall, trasforma questo contesto in azione. Utilizzando i dati di telemetria del Context Lake unificato, un dispositivo può essere bloccato a livello di accesso cablato o wireless prima di spostarsi ulteriormente all'interno della rete. I clienti possono scegliere se attivare la Risposta alle minacce attive, mantenendo nelle proprie mani la decisione di autorizzare il blocco automatico a livello di accesso.

I dispositivi di rete di terze parti seguono lo stesso schema dell'esempio di firewall di terze parti riportato sopra.



Sophos AI Defense svela l'utilizzo della shadow AI

Il coordinamento non riguarda solo malware e intrusioni. Sophos AI Defense è un punto di controllo in Sophos Fusion che regola l'uso dell'AI in un'organizzazione. Interpreta la telemetria dell'attività basata sull'AI di un'ampia gamma di prodotti Sophos nel Context Lake unificato, insieme a qualsiasi altro segnale visibile a Sophos EDR, Sophos XDR e Sophos MDR. Sophos AI Defense è progettata per mettere in evidenza i dettagli granulari dell'utilizzo dell'AI e, una volta inserite nel Context Lake unificato, queste informazioni vengono elaborate con la stessa funzionalità Synchronized Security di qualsiasi altro componente.

Shadow AI mostra perché è necessaria. Un dipendente inizia a utilizzare uno strumento di AI sconosciuto, incollandovi codice sorgente e record dei clienti. Il browser vede i dati incollati, l'endpoint vede l'applicazione e il firewall vede il traffico verso un servizio di AI proveniente da un dispositivo che potrebbe non essere gestito affatto. Nessun punto di controllo vede l'intero quadro, quindi lo strumento passa inosservato.

Sophos AI Defense raccoglie questi segnali e li valuta nel loro contesto, fornendo all'analista di sicurezza le prove di cui ha bisogno per capire cosa è successo. Combina dati di telemetria quali identità, autorizzazioni, comportamento, esposizione dei dati e posizione sia dell'utente sia del modello di AI, separando l'uso accettabile da attività non gestite, con privilegi eccessivi o contrarie ai criteri.

L'applicazione viene quindi eseguita ai punti di controllo:

- Sophos Workspace Protection controlla il browser, inclusi copia e incolla, upload, download e screenshot.
- Sophos Endpoint limita l'accesso ad applicazioni e siti web di IA in base a gruppi di utenti e tipi di dispositivi.
- Sophos Firewall controlla il traffico dei servizi di IA a livello di rete, inclusi i dispositivi non gestiti e le attività non svolte dal browser.
- I prodotti Sophos possono ispezionare prompt, caricamenti e interazioni con l'IA in tempo reale, conservando codice sorgente, record dei clienti e dati finanziari all'interno dell'azienda.
- Un amministratore può bloccare uno strumento di IA specifico nell'intero ambiente direttamente da Sophos Fusion.

I criteri non sono tutto. Una violazione o un comportamento da agente non autorizzato emergono negli stessi flussi di lavoro di Sophos EDR, Sophos XDR e Sophos MDR di qualsiasi altro rilevamento, gestiti con l'automazione e i playbook già utilizzati per le minacce di identità, endpoint e rete. L'estensione della coordinazione dipende dai punti di controllo connessi a Sophos Fusion.

82%

L'82% delle aziende ha scoperto strumenti o flussi di lavoro di IA sconosciuti nel proprio ambiente.[2]

2 Cloud Security Alliance, Il problema dell'agente shadow AI negli ambienti aziendali, 2025

Coordinamento oltre la risposta alle minacce

Tra i punti di controllo Sophos, il coordinamento va oltre la condivisione di un verdetto sulla minaccia. Un punto di controllo può rivolgere a un altro una domanda diretta e agire in base alla risposta. Un endpoint o server protetto da Sophos Endpoint sa già la maggior parte delle cose che un Sophos Firewall non può dirti sul traffico di rete. Tre scambi mostrano cosa rende possibile questo processo: identificare l'applicazione dietro al traffico su una porta, identificare l'utente dietro una sessione e decidere se un dispositivo è idoneo a ricevere accesso.

Synchronized Application Control

Prendere una connessione non classificata su una porta insolita. Un firewall che lo ispeziona in isolamento rileva un flusso di pacchetti e poco altro. Sophos Firewall può chiedere a Sophos Endpoint quale applicazione invia e riceve su quella porta e ottenere una risposta su quale applicazione è responsabile. I clienti possono quindi autorizzare o bloccare l'applicazione su questa base. Con il passare del tempo, questo permette anche di ottenere un quadro preciso di ciò che viene eseguito sulla rete, che di solito è più vario di quanto ci si possa aspettare.

Identità, non indirizzi IP

L'identità utente funziona allo stesso modo. Sophos Endpoint inoltra le informazioni degli utenti autenticati a Sophos Firewall, in modo che i criteri possano essere scritti in base alle persone e alla loro identità, piuttosto che in base agli utenti o agli indirizzi IP che cambiano. Rimuove un esercizio di mapping che altrimenti gli amministratori manterrebbero a mano e che tende a diventare obsoleto.

Solo i dispositivi con integrità si connettono

Anche le decisioni di accesso ne traggono vantaggio: una VPN tradizionale non ha modo di sapere se un dispositivo si presenta con uno stato di integrità adeguato e ammette l'endpoint solo in base alle sue credenziali. Tuttavia, Sophos Workspace Protection verifica lo stato di integrità del dispositivo con Sophos Endpoint prima di concedere qualsiasi autorizzazione, in modo che un endpoint compromesso non raggiunga mai applicazioni o dati di rete.

Scambi come questi non sono un set fisso. Ognuna di esse esiste perché è stata creata da Sophos e Sophos ha continuato a espandere le sue capacità nel tempo. Quello che viene condiviso tra i punti di controllo Sophos oggi è molto più ricco di quello che veniva condiviso tra loro dieci anni fa.

Tutto questo non comincia con la risposta alle minacce, ma raramente rimane separato da essa. Un'applicazione di cui nessuno può rendere conto, o un utente che ha effettuato l'accesso dove non dovrebbe essere, è un normale dettaglio operativo fino al momento in cui non lo è. Una visibilità che semplifica l'esecuzione di una rete rende più facile l'individuazione di una minaccia emergente.

Una risposta coordinata in un ambiente ibrido

Questo esempio reale di Sophos MDR mostra Synchronized Security in azione. L'organizzazione colpita era un cliente Sophos MDR che eseguiva Sophos Endpoint e Sophos Email, insieme a Microsoft Entra ID, Microsoft Graph Security e un firewall Fortinet. Hanno anche eseguito un Sophos Firewall su una rete separata. Tutti questi punti di controllo alimentavano lo stesso Context Lake unificato.

- L'autore dell'attacco ha aperto con un'esca assistita dall'IA, utilizzando una pagina di phishing ospitata su un sito legittimo. L'utente ha cliccato su e ha inserito la propria password.
- Il kit ha rubato il token della sessione in tempo reale invece della credenziale. In questo modo, l'autore dell'attacco è riuscito a bypassare l'autenticazione multifattoriale, rendendo inefficace la reimpostazione della password.
- L'attaccante ha effettuato l'accesso dall'infrastruttura nota degli attaccanti e ha creato una regola silenziosa nella casella di posta che nascondeva eventuali e-mail provenienti da un fornitore specifico, configurando così la predisposizione per una wire fraud.
- Quattro punti di controllo hanno registrato elementi sospetti: Sophos Endpoint, due soluzioni Microsoft e il firewall Fortinet. Nessun singolo segnale era abbastanza forte da attivare una risposta.
- È stato attivato un rilevamento Sophos appositamente realizzato e i singoli segnali sono stati risolti in un'unica catena di attacco.
- L'accesso è stato bloccato, le sessioni sono state revocate e l'endpoint è stato isolato. Indirizzi IP malevoli sono stati bloccati nel Sophos Firewall, utilizzando dati di telemetria emersi dal firewall Fortinet.

Una persona ha chiuso il caso. Un analista ha confermato che la regola della casella di posta indicava un fornitore specifico, e questo ha fatto sì che venisse identificata come preparazione per una wire fraud.



Come abilitare Synchronized Security

Synchronized Security non è un prodotto, un codice SKU o un add-on, e non è necessario acquistare alcuna licenza extra. I clienti possono ottenerla automaticamente quando due o più punti di controllo interagiscono all'interno di Sophos Fusion, indipendentemente dal fatto che i punti di controllo siano o meno Sophos.

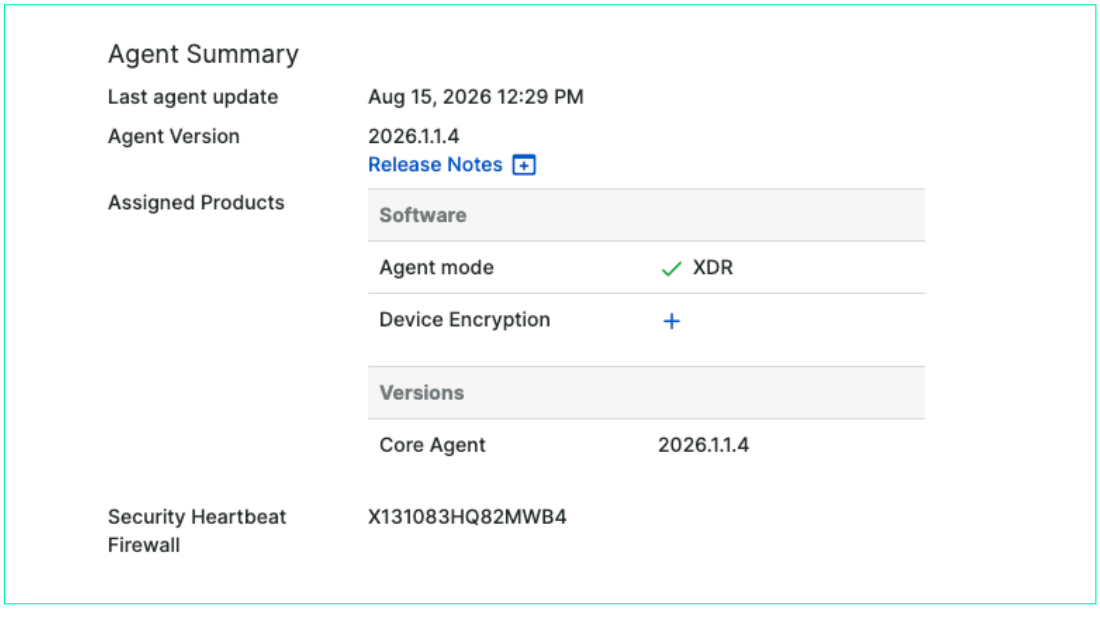
Sophos Endpoint e Sophos Firewall gestiti dallo stesso account Sophos Fusion sono un punto di partenza comune. Il coordinamento tra questi è attivo non appena entrambi sono connessi a quell'account, senza bisogno di configurare altro. I casi di utilizzo basati sullo stato di integrità, ad esempio l'utilizzo dello stato di integrità come parte delle regole firewall o dei criteri Sophos Workspace Protection, vengono impostati dal cliente.

Il coordinamento con i punti di controllo di terze parti comincia integrando il punto di controllo in Sophos Fusion, che supporta integrazioni native di Sophos e oltre 500 integrazioni di terze parti. Tuttavia, il livello di risposta automatica disponibile varia da un punto di controllo all'altro. Risposta alle minacce attive nei punti di controllo Sophos è un esempio, abilitato dal cliente, non per impostazione predefinita.

Sophos offre automazioni e playbook che si eseguono automaticamente tramite Synchronized Security, per una vasta gamma di casi di utilizzo. I clienti possono aggiungerne di nuovi quando l'automazione predefinita non si addice al proprio ambiente, come descritto sopra.

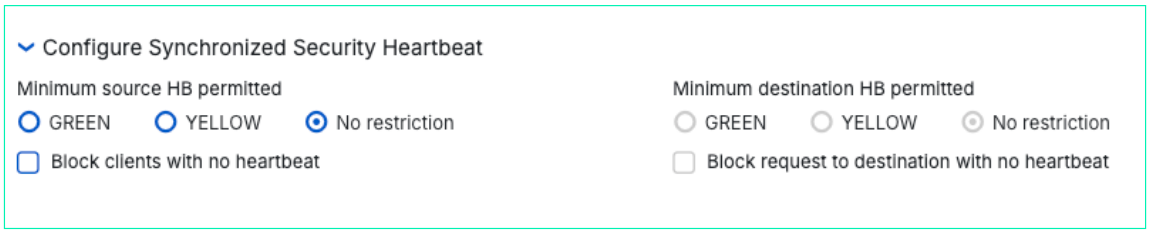
Coordinamento di Sophos Endpoint con Sophos Firewall

Per confermare che Sophos Endpoint si coordina con un firewall, aprire il Riepilogo computer in Sophos Fusion. Qui viene mostrato il numero di serie del Sophos Firewall che riceve il Security Heartbeat da quell'endpoint.



Policy Sophos Firewall con Synchronized Security

Facoltativamente, una regola firewall può richiedere uno stato di integrità verde prima che un dispositivo possa accedere a Internet. I dispositivi non protetti (ovvero quelli che non eseguono Sophos Endpoint) non saranno quindi in grado di connettersi, così come qualsiasi dispositivo con uno stato di integrità discutibile.



Mettere tutto insieme

Il problema non è mai stato la mancanza di strumenti di sicurezza. Gli strumenti di un'organizzazione tendono a lavorare in isolamento e gli autori degli attacchi hanno sviluppato i loro metodi per sfruttare le lacune tra di loro. Synchronized Security permette ai tuoi strumenti di sicurezza di agire come una difesa unificata e coordinata.

Se si eseguono due o più punti di controllo in Sophos Fusion, Synchronized Security sta già lavorando per tuo conto. Collega più punti di controllo e la portata si estende ulteriormente. Gli strumenti non Sophos su cui hai già investito vengono coinvolti nella risposta, invece di essere lasciati a margine.

Il grado di automazione rimane a tua discrezione. Un coordinamento che ignorasse i processi di controllo delle modifiche non avrebbe senso, per cui la profondità dell'automazione viene stabilita da te, punto per punto.

Questo è il valore pratico del Sophos Cyber Defense System. Non si tratta di un elenco più lungo di prodotti, ma di quelli che già utilizzi, rispondendo insieme alla velocità della macchina, più velocemente di quanto un attacco accelerato dall'IA possa spostarsi tra di loro.

Per saperne di più, visita
www.sophos.com/
synchronizedsecurity

Vendite per l'Italia
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

© Copyright 2026. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con Nº 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è marchio registrato di Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.