WHITE PAPER

Come funzionano i sistemi di cyber difesa

Il nuovo modello di cyber difesa per la resilienza nell'era dell'IA agentica.

SOPHOS

Riepilogo

A una prima analisi, la protezione della maggior parte delle organizzazioni sembra efficace. Negli anni queste aziende hanno accumulato decine di prodotti di sicurezza. Tuttavia, secondo Gartner: "In media, le organizzazioni hanno 45 strumenti di sicurezza che spesso funzionano in modo isolato, creando complessità, punti ciechi ed esposizioni non identificate che vengono prese di mira dagli avversari"[1]. Pertanto, se da un lato non mancano gli strumenti, dall'altro la connettività tra di essi è carente.

Gli autori degli attacchi stanno già sfruttando le lacune tra i vari strumenti, spostandosi tra e-mail, identità, endpoint e rete nel giro di pochi minuti. L'IA sta aumentando la velocità, la portata e l'ambito di azione delle minacce informatiche a un ritmo senza precedenti, consentendo l'esecuzione diffusa di attacchi sofisticati a livelli multipli.

Auditor, autorità di regolamentazione e compagnie di cyberassicurazioni si aspettano ora una serie complessa di prove quasi impossibili da fornire con prodotti frammentati. La maggior parte delle organizzazioni stenta ancora a rispondere a tre domande fondamentali: siamo protetti, qual è il nostro rischio maggiore e i nostri investimenti stanno portando i risultati sperati?

Un nuovo modello di cyber difesa sta prendendo forma per garantire protezione nell'era dell'IA. La piattaforma di sicurezza si sta evolvendo verso un sistema di cyber difesa. Questi sono i suoi tratti distintivi:

- **Una vista unica e in tempo reale dell'ambiente**, alimentata da ogni punto di controllo di qualsiasi vendor.
- **Risposte coordinate automaticamente** tra i vari punti di controllo: e-mail, identità, endpoint, rete e altro.
- **IA agentica per rispondere alla velocità e al volume degli attacchi moderni**, mentre gli esperti umani stabiliscono i limiti e mantengono la responsabilità dei risultati.
- **Apprendimento continuo** a ogni nuova informazione e a ogni minaccia bloccata nell'intera base utenti, per rafforzare automaticamente le difese ovunque.
- **Spostamento del fulcro della difesa dai singoli prodotti a un'architettura che li connette**, includendo sia l'architettura tecnologica che una rete di competenze umane.

Un sistema di cyber difesa è...

Un'architettura di sicurezza unificata in cui ogni punto di controllo condivide una visibilità in tempo reale, risponde come una sola entità, apprende continuamente e opera alla velocità della macchina sotto la responsabilità umana.

Le minacce dell'era dell'IA agentica sono già una realtà

Alla fine del 2025, i ricercatori hanno documentato la prima campagna di spionaggio informatico nota, condotta prevalentemente dall'IA, anziché da operatori umani. Si stima che l'IA abbia eseguito in totale autonomia tra l'80% e il 90% dell'operazione, con una velocità e un'estensione inarrivabili per qualsiasi team umano.

Fonte: Anthropic, novembre 2025

1. *Gartner, "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*

SOPHOS

Le tue sfide di sicurezza nell'era dell'IA

Anni di decisioni di acquisto ragionevoli, valutate minaccia per minaccia, hanno portato a un ambiente talmente complesso che la complessità stessa è diventata una vulnerabilità. Oggi, questo insieme di prodotti non coordinati si trova ad affrontare autori degli attacchi che agiscono alla velocità dell'IA, senza riuscire a tenerne il passo. Come siamo arrivati a questo punto?

Le lacune dell'approccio basato sulle piattaforme

Quasi tutti i principali vendor di cybersecurity sostengono che la loro piattaforma sia in grado di soddisfare ogni esigenza. Vendono soluzioni ad hoc per acquirenti focalizzati sulle singole minacce, con l'obiettivo di farle funzionare insieme come un'unica piattaforma.

La filosofia di creare un sistema di sicurezza unificato era sulla strada giusta, ma ciò che spesso viene venduto è un insieme disorganico di strumenti sviluppati o acquisiti frettolosamente, concepiti per inseguire le mode del momento o far salire il valore delle azioni. Le promesse non vengono mantenute:

- **Promettono una "singola interfaccia di gestione"**, ma alla prova dei fatti i team di difesa devono comunque passare da una console all'altra.
- **Promettono dati condivisi**, ma i prodotti della piattaforma non sono in grado di analizzare tali dati in modo integrato per rilevare un attacco che coinvolge identità, cloud ed endpoint.
- **Promettono integrazione**, ma ogni prodotto mantiene il proprio modello di dati e le azioni di risposta restano isolate nei singoli domini.

Tutto il lavoro di gestione della piattaforma (configurazione, personalizzazione e creazione di un flusso di lavoro che colleghi tutti i componenti) viene lasciato al cliente.

Secondo Gartner®, "La semplice aggiunta di ulteriori strumenti allo stack non garantirà la struttura di cyber difesa intelligente di cui hanno bisogno le organizzazioni per mitigare gli attacchi orchestrati dall'IA come quello identificato di recente da Anthropic".

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

Gartner, 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 commerciale di Gartner, Inc. e/o delle sue affiliate

Gli attacchi su più domini superano le difese frammentate

La frammentazione dei modelli di dati e delle analisi nei prodotti della piattaforma offre un vantaggio all'autore di un attacco. Il seguente scenario di attacco dimostra perché:

- **Fase 1:** un'e-mail persuasiva riesce a infiltrarsi in una casella di posta.
- **Fase 2:** il destinatario inserisce la propria password in una pagina di accesso contraffatta.
- **Fase 3:** l'autore dell'attacco si connette da una posizione insolita.
- **Fase 4:** l'autore dell'attacco aggiunge con discrezione una regola alla casella di posta per monitorare il traffico.
- **Fase 5:** l'autore dell'attacco sfrutta l'accesso per raggiungere una condivisione di file ed esfiltrare dati.

Cinque fasi, ognuna delle quali coinvolge un dominio diverso.

- **La protezione delle e-mail** vede il messaggio.
- **La soluzione di identità** vede l'accesso insolito.
- **La protezione endpoint** nota una piccola anomalia.
- **Il firewall** registra nei log la connessione in uscita.

Ogni prodotto gestisce la propria parte, e dal punto di vista tecnico ciascuno svolge il proprio compito. Eppure, **nessuno di essi ha la visione d'insieme**, poiché nessuno condivide le informazioni acquisite con gli altri mentre l'attacco è in corso. Il tutto si presenta come semplice rumore di fondo, non come la dinamica di un attacco. La catena diventa evidente solo in un secondo momento, quando è ormai troppo tardi.

Questo tipo di movimento laterale è molto comune negli attacchi moderni e viene spesso ignorato. Il report Sophos "La vera storia del ransomware 2026" mostra che il 55% dei cybercriminali è riuscito a crittografare i dati anche quando il firewall aveva rilevato l'attacco.

Attacchi alla velocità della macchina, risposte a ritmo umano

Ora prendiamo quell'attacco su più domini e comprimiamo la tempistica dell'attacco da giorni a minuti. È esattamente ciò che ha fatto l'IA. Una difesa che aspetta che qualcuno noti un avviso in un prodotto e lo confronti con un altro è già in ritardo. Il problema non è la lentezza dei team di difesa, ma la lentezza di risposte gestite uno strumento alla volta. I flussi di lavoro altamente manuali non sono in grado di tenere il passo con un attacco automatizzato. Nel momento in cui un operatore formula una risposta, l'autore dell'attacco è già passato alla fase successiva.

Le competenze tecniche sono rare. Le informazioni superflue no.

Aggiungere personale per risolvere il problema non è un'opzione fattibile, semplicemente perché le risorse umane sono insufficienti. La mancanza di personale dotato di competenze di cybersecurity elevate è un problema reale, che non accenna a diminuire. Nello studio di ISC2 sulla forza lavoro nel 2025, il 95% dei team di sicurezza ha segnalato almeno una lacuna nelle competenze; il 59% l'ha definita critica o significativa, in aumento rispetto al 44% dell'anno precedente.

Allo stesso tempo, il carico di lavoro continua a crescere. Un team composto da poche persone può finire per doversi occupare di più prodotti, avvisi e dashboard di quanti ne possa ragionevolmente monitorare. La maggior parte di questi avvisi si riduce a semplice rumore di fondo, ma qualcuno deve pur trovare il segnale nascosto al suo interno.

L'IA avrebbe dovuto alleggerire questa pressione, ma in alcuni ambienti ha ottenuto l'effetto opposto.

L'aggiunta dell'IA come ennesimo prodotto aggiunto a posteriori crea gli stessi problemi: più informazioni superflue e avvisi, poiché non è stata progettata per interagire nativamente con gli altri prodotti della piattaforma. Ora il team informatico non deve solo passare al setaccio i falsi positivi, ma deve anche fare i conti con le allucinazioni dell'IA.

La soglia di povertà della cybersecurity è un problema reale

La “soglia di povertà” della cybersecurity è il limite al di sotto del quale un’organizzazione non può essere protetta in modo efficace. Non è definita dalle dimensioni di un’azienda, dal suo budget o dalla presenza di un CISO. In realtà, molte organizzazioni con ampie disponibilità economiche si trovano al di sotto di questa soglia.

La soglia di povertà della cybersecurity è un livello di capacità strategica.

La tua organizzazione si limita a possedere tecnologie di sicurezza, o è in grado di gestirle come un sistema integrato? I team di grandi dimensioni possono investire cifre ingenti in strumenti che nessuno possiede le competenze per far funzionare, mentre un’azienda manifatturiera con soli 200 dipendenti ma ben organizzata può utilizzare un sistema di difesa con livelli di performance superiori rispetto a quelli di realtà molto più grandi. Molte organizzazioni si trovano al di sotto della soglia di povertà senza saperlo, perché danno per scontato che la capacità di gestire la sicurezza come un unico sistema sia già presente internamente.

Per queste organizzazioni, la lacuna principale non è la mancanza di uno strumento, bensì l’assenza di una strategia chiara e dell’orchestrazione necessaria per far collaborare i controlli esistenti contro le minacce accelerate dall’IA. Continuano a investire, ma fanno ancora fatica a rispondere a tre domande fondamentali:

- Siamo protetti?
- Dove si concentrano i nostri rischi maggiori?
- I nostri investimenti stanno portando i risultati sperati?

Le autorità di regolamentazione richiedono maggiori prove di resilienza

Alle autorità di regolamentazione e alle cyberassicurazioni non interessa se hai i prodotti giusti. Al contrario, impongono sempre più spesso alle organizzazioni di dimostrare:

- Un controllo coordinato su tutti i domini.
- Prove conservate e verificabili in sede di audit.
- Segnalazioni coerenti e tempestive.
- Una resilienza testata sul campo.

Queste nuove normative rappresentano un pesante onere per le organizzazioni che hanno ancora un ambiente di sicurezza distribuito su decine di prodotti, ognuno con il proprio modello di dati e periodo di conservazione. Produrre le prove richieste da un auditor o da una compagnia di assicurazioni può diventare un lavoro a tempo pieno: esportare log da sistemi diversi, ricucirli insieme manualmente e sperare che il risultato fornisca comunque un quadro coerente. Ai fini della conformità, un controllo che non può essere dimostrato è un controllo che non conta.

Il filo conduttore

Nessuno di questi problemi si risolve aggiungendo un altro prodotto o un nuovo pulsante a una console. Condividono tutti un'unica causa originaria: le difese che operano in modo isolato vengono meno quando le minacce che le attaccano agiscono in modo orchestrato. Colmare questo divario richiede un approccio diverso, non l'ennesimo nuovo prodotto.

Sistemi di cyber difesa: un approccio moderno alla sicurezza

Se il problema è la frammentazione, la soluzione non è il consolidamento fine a se stesso. Acquistare un prodotto che cerca di fare di tutto senza riuscirci non è meglio che avere più prodotti validi che non si coordinano tra di loro.

Le organizzazioni dovrebbero invece orientarsi verso un sistema di cyber difesa: un insieme di prodotti e servizi di sicurezza progettati per funzionare come un'unica entità. Ogni punto di controllo deve contribuire a una comprensione condivisa dell'ambiente e reagire come parte di un insieme coordinato. Il sistema deve essere ben interconnesso, sincronizzato, automatizzato, intelligente e adattivo. Cinque principi ne descrivono il funzionamento pratico.

1 Punti di controllo sincronizzati e autonomi

Un sistema di cyber difesa efficace comincia dai punti di controllo. Si tratta delle tecnologie e dei servizi in cui la telemetria di sicurezza viene monitorata e le regole di sicurezza vengono applicate. I punti di controllo possono sia osservare che intervenire su ciò che accade al loro interno. Endpoint, firewall, e-mail, gestione delle identità, strumenti di produttività e altro sono tutti punti di controllo.

2 Un'unica vista condivisa in tempo reale

Un sistema di cyber difesa si differenzia da una piattaforma poiché possiede una comprensione unificata di ciò che accade nell'intero ambiente. Ciascun punto di controllo alimenta un livello di dati comune in tempo reale, senza ritardi di duplicazione o riconciliazione. Questo permette all'intero sistema di visualizzare in tempo reale gli eventi in maniera unificata e condivisa. Nessun punto cieco, nessuna lacuna nella risposta.

3 Risposta coordinata su tutti i livelli

Una risposta coordinata comincia con un rilevamento in un livello in grado di attivare automaticamente un'azione sugli altri, senza che un analista debba inoltrare il segnale da una console a un'altra.

Un accesso sospetto può attivare controlli più approfonditi sia a livello di endpoint che di e-mail. Un file malevolo su un dispositivo può spingere il firewall o la rete a bloccare la connessione che tenta di stabilire. Il sistema risponde come un'unica entità, perché percepisce già l'attacco come un tutt'uno. E quando un attacco si muove rapidamente, questo tipo di coordinamento è importante.

4 IA agentica con responsabilità umana

La velocità è il fattore determinante. Gli attacchi che si sviluppano in pochi minuti non possono essere fermati da difese che attendono l'intervento di un essere umano. Ed è per questo motivo che l'IA deve trovarsi al centro del sistema, non ai suoi margini.

In un sistema di cyber difesa, l'IA ne costituisce l'architettura: è integrata, non aggiunta a posteriori. L'IA mette in correlazione i segnali provenienti da tutti i livelli, identifica la struttura di un attacco al suo insorgere e genera rilevamento, indagine e risposta alla velocità della macchina. Questo sistema AI-native si distingue nettamente dalle soluzioni in cui l'IA viene aggiunta in un secondo momento su un singolo prodotto e può visualizzare solo i dati di quel prodotto.

L'IA integrata in un sistema di difesa può elaborare informazioni trasversalmente su tutto ciò che il sistema rileva. Tuttavia, una risposta alla velocità della macchina priva di responsabilità umana rappresenta un rischio, non un vantaggio. I sistemi di cyber difesa non escludono il fattore umano dalla sicurezza. Al contrario, lo indirizzano dove il giudizio umano è più determinante: stabilire i limiti, gestire decisioni nuove o ad alto rischio, analizzare gli incidenti e mantenere la responsabilità dei risultati.

L'IA gestisce la velocità e il volume. Le attività di triage di routine e le azioni rapide ad elevata affidabilità.

Gli esperti umani definiscono il perimetro di fiducia: cosa può decidere l'IA in autonomia e quando invece ha bisogno di aiuto. Intervengono in caso di contesto sconosciuto o quando la posta in gioco è alta.

Man mano che il sistema acquisisce fiducia, tale perimetro può espandersi. Ma la responsabilità rimane sempre a carico di esperti umani.

L'IA gestisce la velocità e il volume.

Gli esperti umani definiscono il perimetro di fiducia.

5 Un'intelligence che continua a migliorarsi

I sistemi di cyber difesa apprendono. Una minaccia individuata in un punto qualsiasi diventa conoscenza condivisa ovunque. L'endpoint vede quello che ha visto il firewall. Il gateway e-mail comunica al livello di gestione delle identità cosa ha intercettato. Ogni strumento impara insieme agli altri e si basa sulle esperienze precedenti. Tutto questo avviene senza alcuna configurazione manuale. L'intelligence del sistema di difesa cresce in modo cumulativo con l'aumentare degli utenti e dei pattern osservati, consentendo al sistema di evolversi alla stessa velocità degli attacchi basati sull'IA.

SOPHOS

Dalle piattaforme ai sistemi di cyber difesa

Nel loro insieme, questi cinque principi definiscono una categoria a sé stante. I sistemi di cyber difesa rappresentano l'evoluzione della piattaforma, ottimizzati per l'era dell'IA. Di solito una piattaforma è solo un insieme di prodotti raccolti sotto un'unica console, legati tra loro da un accesso e un contratto di licenza, piuttosto che da un'effettiva progettazione integrata.

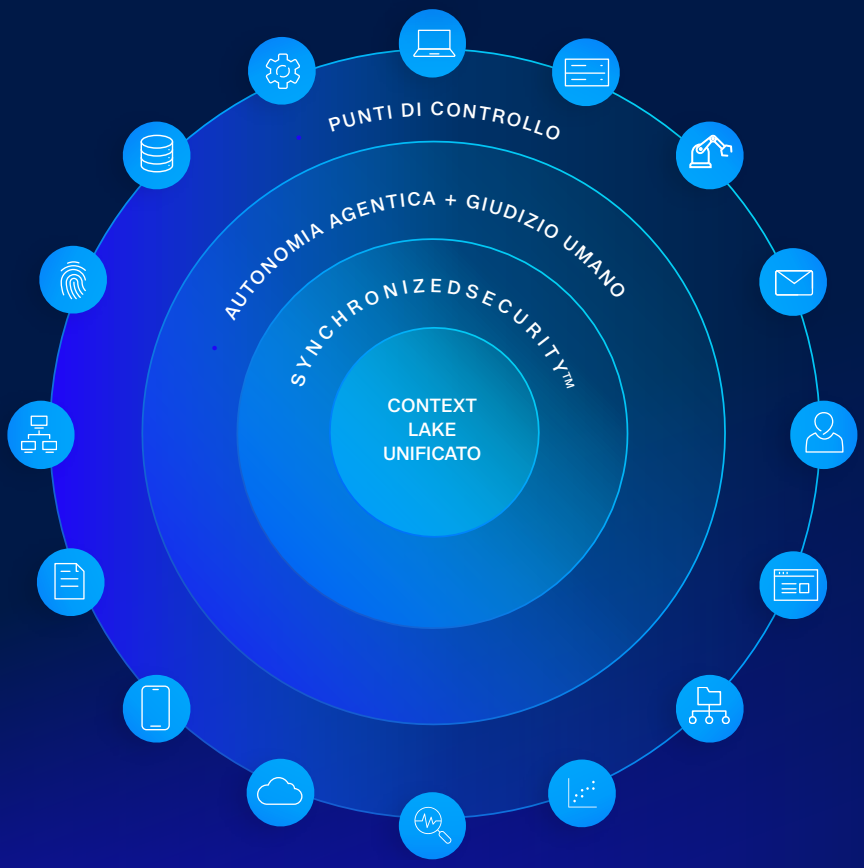
Un sistema di cyber difesa è diverso. I suoi dati sono condivisi, l'IA è integrata, la risposta è coordinata e gli esperti umani mantengono il controllo. È un'architettura progettata per funzionare come un unico prodotto, anziché un insieme di prodotti assemblati in modo da sembrare uno solo.

Sophos Fusion: il sistema di cyber difesa di Sophos

Sophos Fusion è il sistema di difesa informatica più completo del settore. È progettato per un mondo in cui le minacce si muovono alla velocità dell'IA. Basato sull'architettura Sophos AI-Native Cybersecurity Defense System e su oltre 500 integrazioni Sophos e di terze parti, vede tutto, connette tutto e consente ai tuoi sistemi di difesa di rispondere come un'unica entità.

Sophos Fusion trasforma in pratica i principi del sistema di cyber difesa: un'unica architettura aperta in cui ogni punto di controllo agisce come un'unica entità, potenziata dall'IA agentica e affiancata dal discernimento umano, per proteggere le organizzazioni dalle minacce basate sull'IA che si muovono più rapidamente della capacità di risposta dei team di difesa.

Più soluzioni del portafoglio Sophos vengono attivate dal cliente, maggiore è il valore offerto da Sophos Fusion.



Punti di controllo sincronizzati e autonomi

Ogni punto di controllo che già possiedi fornisce continuamente dati di intelligence sulle minacce in tempo reale e svolge azioni di risposta. L'architettura è completamente aperta: si integra nativamente con i prodotti Sophos e con più di 500 tecnologie di terze parti, per cui gli investimenti che hai già effettuato diventano parte di un'unica difesa coordinata, anziché rimanere isolati.

Include anche la più profonda integrazione di sicurezza con Microsoft disponibile sul mercato, estesa a tutti i piani Microsoft e non solo a quelli più costosi. In questo modo anche le organizzazioni con licenze Microsoft di base possono rafforzare le proprie difese sfruttando questa telemetria.

Un'unica vista condivisa in tempo reale

Tutta la telemetria raccolta da ogni punto di controllo confluisce in tempo reale nel Context Lake unificato, un unico livello di dati condiviso. Non c'è alcun ritardo di aggregazione, né alcun archivio dati separato per i singoli punti di controllo. Si può considerare come un sistema nervoso condiviso: ogni punto di controllo rileva ciò che percepiscono tutti gli altri, nel momento esatto in cui accade. Questa comprensione condivisa è ciò che rende possibile il coordinamento.

Risposta coordinata su tutti i livelli: Synchronized Security™

Synchronized Security™ è il tessuto connettivo che trasforma la comprensione condivisa in un'azione coordinata all'interno di Sophos Fusion. Consente ai punti di controllo Sophos e non Sophos di rispondere automaticamente e in modo congiunto alle minacce.

Un rilevamento a livello di endpoint può attivare una risposta a livello di firewall. Un'identità compromessa può bloccare l'accesso all'intero ambiente. Un'e-mail sospetta può innalzare il livello di attenzione su ogni altro livello. Più soluzioni Sophos si implementano, maggiori saranno i vantaggi offerti da Synchronized Security™.

Pensa al sistema antincendio di un edificio moderno: un sensore in una stanza non si limita a far scattare un allarme, ma chiude le porte tagliafuoco, reindirizza la ventilazione e attiva gli sprinkler nei piani adiacenti. Sophos Fusion funziona allo stesso modo, come un'unica entità coordinata. È in grado di farlo perché i dati sono già unificati. Non richiede alcuna configurazione o azione aggiuntiva.

IA agentica con responsabilità umana

Sophos Fusion rileva le minacce, svolge indagini e risponde alla velocità della macchina, ma non agisce mai senza la supervisione umana. Ogni azione rimane all'interno di limiti ben definiti e continuamente affinati da esperti umani. Ed è proprio questo a renderla un'IA agentica: un'IA in grado di valutare situazioni nuove, e non soltanto di seguire strategie predefinite.

Un'analogia efficace è il pilota automatico nell'aviazione. Il sistema può pilotare l'aereo, ma spetta al pilota impostare i parametri, monitorare la strumentazione e assumere il controllo quando la situazione è sconosciuta o ad alto rischio.

In Sophos Fusion, questa capacità agentica viene fornita da Fusion AI, l'IA agentica nativa di Sophos. Sophos integra nelle proprie difese oltre 50 modelli di IA, tutti continuamente perfezionati con dati di intelligence sulle minacce in tempo reale. Ad esempio, Sophos Email utilizza oltre 20 modelli, inclusi modelli proprietari di elaborazione del linguaggio naturale (NLP) che analizzano testo, tono, contesto e struttura delle e-mail, per identificare attacchi di phishing e Business Email Compromise.

Sophos MDR, un servizio operativo 24/7 in cui gli esperti Sophos monitorano i sistemi e intervengono per conto tuo, gestisce il più grande SOC (Security Operations Center) agentico al mondo, utilizzando il Sophos Cyber Defense System. È la più grande operazione di rilevamento e risposta gestiti del settore, e protegge più di 40.000 organizzazioni. Risolve il 52% degli incidenti end-to-end con l'IA, con una media di 89 secondi dall'avviso alla risposta automatizzata, mentre gli esperti umani mantengono la responsabilità delle decisioni che comportano rischi per l'azienda.

Un'intelligence che continua a migliorarsi

Il Sophos Cyber Defense System impara da ogni attacco, non solo da quelli diretti alla tua organizzazione. Tutte le minacce intercettate nelle oltre 625.000 aziende protette da Sophos confluiscono in Sophos Fusion, insieme a ogni caso limite risolto da un analista e a ogni nuovo ambiente portato on-line. Sophos X-Ops arricchisce queste informazioni con le proprie competenze e dati di intelligence sulle minacce in tempo reale, che vengono poi inoltrati automaticamente a tutti i prodotti Sophos e a tutti i clienti, migliorandone le difese.

Il funzionamento è molto simile a quello di un sistema immunitario biologico. Ogni minaccia incontrata dall'organismo entra a far parte di una memoria permanente: viene catalogata, compresa e rimane pronta per la volta successiva che viene riscontrata. Sophos Fusion agisce allo stesso modo. Un nuovo cliente è protetto fin dal primo giorno contro minacce mai osservate prima, poiché il sistema le ha già affrontate.

Ecco perché il dato delle oltre 625.000 organizzazioni è così significativo. Riflette l'ampia esperienza maturata nel campo, che permette alla protezione e all'intelligence di continuare a migliorarsi. Più elementi il sistema analizza, più diventa efficace nel difendere tutti coloro che ne fanno parte.

Sophos Fusion: dove vedi il sistema di cyber difesa in azione

Il Sophos AI-Native Cybersecurity Defense System è l'architettura. Sophos Fusion è dove vedi il sistema in azione. Un unico posto per gestire i tuoi punti di controllo Sophos, avere una visione d'insieme da ogni punto di controllo connesso e intraprendere azioni.

Questo significa che non devi acquistare o attivare nient'altro, e non c'è alcun bisogno di cambiare il modo in cui lavori attualmente. Tutti i punti di controllo Sophos fanno già parte di Sophos Fusion, per cui nel momento stesso in cui ne implementi uno, ti troverai all'interno dell'architettura. E man mano che aggiungi altri punti di controllo Sophos o di terze parti, una porzione sempre più ampia del sistema prende vita, alimentando una visione condivisa più ricca e generando maggior valore da tutti gli strumenti già in esecuzione.

L'attacco osservato da Sophos Fusion

Torniamo all'attacco a più fasi di prima. Un'e-mail malevola, una credenziale rubata, un accesso insolito, una regola di inoltro della casella di posta e un movimento laterale verso dati di natura sensibile. In Sophos Fusion, la telemetria proveniente da Sophos Email e dall'ambiente Microsoft del cliente confluisce nel Context Lake unificato. Sophos XDR mette quindi in correlazione questi segnali man mano che arrivano, riconoscendo la sequenza come un unico attacco interconnesso, anziché cinque avvisi non correlati.

Da qui, Synchronized Security™ coordina la risposta tra e-mail, identità, endpoint e rete. L'IA agentica agisce alla velocità della macchina, mentre gli analisti di Sophos MDR intervengono direttamente prendendo le decisioni più critiche. L'attacco che potrebbe sfuggire ai prodotti isolati viene intercettato da un sistema che possiede una visione d'insieme.

Cosa significa Sophos Fusion per la tua organizzazione

Sophos Fusion offre resilienza informatica per l'era dell'IA agentica in quattro ambiti fondamentali per l'azienda.

- **Protezione dalle minacce accelerate dall'IA che si muovono più velocemente della capacità di risposta dei team di sicurezza.** Gli attacchi a più fasi vengono intercettati e contenuti negli stadi iniziali, anche quando l'IA ne accelera la velocità e ne estende la portata, poiché ogni punto di controllo condivide il contesto e risponde in modo sinergico, invece di agire in isolamento.

- **Maggiore impatto generato dalle risorse umane e dagli investimenti.** L'IA agentica si fa carico del lavoro di routine e della gestione del sovraccarico di notifiche per le attività di triage e risposta. In questo modo, il tuo team e i punti di controllo esistenti ottengono risultati superiori senza bisogno di altro personale e senza aggiungere complessità. Ogni strumento connesso, Sophos o di terze parti, contribuisce al risultato finale.

- **Miglioramento della conformità e del profilo assicurativo.** Copertura 24/7, conservazione del contesto su più livelli e risposta coordinata offrono le prove richieste da auditor, autorità di regolamentazione e compagnie di assicurazioni, il tutto all'interno di un unico registro consultabile, invece di log esportati manualmente. La stessa architettura che migliora la protezione ottimizza anche la tua capacità di dimostrarne l'efficacia.

- **Una strategia di cybersecurity allineata alla tua attività** Connettendo e coordinando le tue difese, Sophos Fusion ti permette di passare dalla gestione di dashboard tattiche a una certezza operativa concreta, garantendo una visibilità chiara su dove risiedono le tue lacune e rischi maggiori, e dimostrando se i tuoi investimenti stiano portando i risultati sperati. È il modo in cui le organizzazioni di qualsiasi dimensione, con o senza un CISO, possono finalmente mettere in atto la strategia che hanno sempre desiderato.

Tutti i clienti Sophos fanno già parte di Sophos Fusion, il sistema di difesa Sophos. È un upgrade automatico e trasparente, che protegge i clienti dalle minacce dell'era dell'IA.

Come iniziare con Sophos Fusion

Ogni soluzione Sophos fa parte di Sophos Fusion, rendendola un punto d'ingresso, anziché uno strumento indipendente. Iniziare è semplicissimo, basta implementare un prodotto o un servizio Sophos: Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall e Sophos Email sono punti di partenza comuni. Più soluzioni aggiungi, più potenziale dell'architettura sblocchi.

Non occorre sostituire gli altri punti di controllo di terze parti su cui fai affidamento oggi. Puoi integrarli in Sophos Fusion per fornire continuamente dati di intelligence sulle minacce in tempo reale ed eseguire azioni di risposta. Inizia dagli ambiti in cui il tuo rischio è maggiore, per poi estendere la protezione secondo i tuoi ritmi.

Ora non ti resta che cominciare. Parla con un esperto Sophos per definire il punto di partenza ideale per il tuo ambiente, oppure scopri di più visitando la pagina sophos.it/fusion.

Conclusione

Per anni, la prassi consolidata per rispondere a ogni nuova minaccia è stata quella di aggiungere un ulteriore prodotto, e questa abitudine ha alimentato la frammentazione che oggi i cybercriminali sfruttano a proprio vantaggio. L'IA non ha fatto altro che peggiorare il problema, ampliando la discrepanza tra la rapidità con cui si muove un attacco e la capacità di contenerlo gestendo la risposta console per console. Continuare ad aggiungere prodotti non colmerà questo divario. Un sistema di cyber difesa invece sì.

Un sistema di cyber difesa sposta il fulcro della difesa dai singoli prodotti all'architettura che li connette:

- Una vista condivisa
- Risposta coordinata su tutti i livelli
- IA integrata per un intervento alla velocità della macchina
- Esperti umani a cui restano affidati la capacità di giudizio e la responsabilità delle decisioni

Garantire la sicurezza nell'era dell'IA significa far collaborare in modo unificato tutte le soluzioni già in tuo possesso. Sophos Fusion, il Sophos AI-Native Cybersecurity Defense System, è il modo in cui mettere in pratica questo modello senza sostituire gli strumenti già presenti nella tua infrastruttura.

SOPHOS

Desideri valutare le tue esigenze di cyber difesa per l'era dell'IA?

Parla subito con un esperto Sophos.

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