SOPHOS

Guida All'Acquisto Di Soluzioni Di Sicurezza Endpoint

In un panorama informatico caratterizzato da minacce sempre più complesse, la responsabilità di trovare la giusta soluzione Endpoint è diventata ancora più gravosa. Tuttavia, quello dell'Endpoint Security è un mercato ormai talmente saturo di soluzioni diverse e dichiarazioni di validità infondate, che prendere una decisione informata per la tua organizzazione sta diventando praticamente impossibile.

Questa guida è stata compilata per fare luce sulla situazione e analizzare in modo dettagliato le principali funzionalità da esigere in una soluzione di protezione endpoint, indicando i componenti fondamentali di cui hai bisogno per difenderti dalle minacce avanzate attualmente in circolazione. Con queste informazioni, avrai un'ottima preparazione per scegliere il prodotto giusto per la tua organizzazione.

Whitepaper Sophos. Giugno 2024

L'attuale panorama delle minacce

Dal nostro sondaggio indipendente, a cui hanno partecipato 3.000 IT/Cybersecurity Manager dislocati in 14 paesi del mondo, è emerso che la realtà attuale del panorama della cybersecurity è caratterizzata da un sistema a due velocità, con cybercriminali e team di IT security che sviluppano le proprie strategie a velocità diverse. Rallentati da varie difficoltà, i team di IT security stanno rimanendo indietro, mentre i criminali vanno avanti a tutta velocità.

L'evoluzione dell'economia cybercriminale

Uno dei cambiamenti più significativi subiti dal panorama delle minacce negli ultimi anni è stata la trasformazione dell'economia cybercriminale, che è ormai diventata una vera e propria industria, con una rete di servizi di assistenza ben sviluppata e un approccio professionale e collaudato.

Recentemente, le aziende informatiche hanno cominciato a offrire linee di soluzioni "as-a-service" e sono state seguite a ruota dall'ecosistema del cybercrimine. Questa evoluzione ha reso l'intero sistema molto più accessibile per gli aspiranti cybercriminali e ha permesso agli antagonisti informatici di incrementare rapidamente il volume, la velocità e l'impatto dei propri attacchi.

Di conseguenza, gli hacker sono ora in grado di sferrare un'ampia selezione di attacchi molto sofisticati su vasta scala. L'anno scorso, il 94% delle organizzazioni ha subito un attacco informatico. Sebbene il ransomware sia stato il tipo di attacco maggiormente segnalato, le organizzazioni sono state colpite da molti altri tipi di minacce, tra le quali[1]:

27%	**27%**	**26%**
E-mail pericolose	Phishing (incluso spearphishing)	Esfiltrazione dei dati (da parte di un cybercriminale)
24%	**24%**	**21%**
Cyber-estorsione	Business Email Compromise	Malware dei dispositivi mobili
18%	**24%**	**14%**
Cryptominer	Denial of Service (DDoS)	Wiper

Leggi il nostro report, Il Panorama Della Cybersecurity 2023: L'Impatto Commerciale Degli Avversari Informatici, per scoprire di più.

Il ransomware continua ad affliggere le organizzazioni

Il 59% delle organizzazioni sostiene di avere subito un attacco ransomware durante l'anno scorso.

2020	2021	2022	2023	2024
51%	37%	66%	66%	59%

La tua organizzazione è stata colpita dal ransomware l'anno scorso?
Sì. n=5.000 (2024), 3.000 (2023), 5.600 (2022), 5.400 (2021), 5.000 (2020).

Sebbene la percentuale di attacchi registrata nel 2024 sia diminuita rispetto a quella del 2023, la crittografia non autorizzata dei dati per mano del ransomware rimane alta, con hacker che riescono a crittografare i dati nel 70% degli attacchi.

Come se non bastasse, anche le spese causate dal ransomware hanno raggiunto un picco record, con organizzazioni che dichiarano costi medi di riparazione dei danni pari a 2,73 milioni di $, in aumento rispetto agli 1,82 milioni di $ registrati nel 2023[2].

Leggi il nostro report annuale, La Vera Storia Del Ransomware 2024, per scoprire quali sono le realtà affrontate dalle organizzazioni nel 2024, tra cui la frequenza, i costi e le cause alla base degli attacchi.

1 Il Panorama Della Cybersecurity 2023: L'Impatto Commerciale Degli Avversari Informatici, Sophos, uno studio indipendente condotto a gennaio e febbraio 2023, a cui hanno partecipato 3.000 IT/Cybersecurity Manager in 14 paesi.

2 La Vera Storia Del Ransomware 2024, Sophos, uno studio indipendente e agnostico rispetto ai vendor condotto da gennaio a febbraio 2024 tra 5.000 IT/Cybersecurity Manager in 14 paesi del mondo.

Gli approcci obsoleti portano a risultati di sicurezza insoddisfacenti

Per molte organizzazioni, l'ambiente aziendale è cambiato molto negli ultimi anni. Gli utenti finali possono trovarsi in ufficio, lavorare da remoto o essere costantemente in movimento tra le sedi di vari clienti o partner. I dati aziendali non vengono memorizzati solo on-premise, bensì anche nel cloud o sui dispositivi degli utenti finali; in più, devono essere disponibili non solo per l'accesso sui computer locali, ma anche su quelli remoti, per venire incontro alle esigenze di dipendenti distribuiti su una superficie geografica sempre più estesa. Di conseguenza, continuare a seguire approcci obsoleti alla cybersecurity spesso porta a risultati di sicurezza insoddisfacenti.

Ecco alcuni dei problemi più comuni riscontrati dai team di IT security:

- **Mancanza di competenze tecniche**: continua a essere difficile assumere dipendenti IT dotati di competenze tecniche adeguate. La mancanza di esperienza implica il fatto che il personale potrebbe non essere in grado di stabilire se un avviso di sicurezza sia pericoloso o innocuo.
- **Sovraccarico di informazioni non pertinenti**: una quantità eccessiva di avvisi provenienti da sistemi diversi è impossibile da gestire per gli operatori, che spesso non riescono ad attribuire la giusta priorità ai segnali o agli avvisi su cui occorre indagare, rischiando così di ignorare importanti indicatori di attacco.
- **Dati isolati**: segnali o avvisi consultabili solo con certe tecnologie specifiche, che impediscono ai team informatici di ottenere il quadro completo della situazione e di risolvere tempestivamente avvisi o incidenti pericolosi.
- **Mancanza di integrazione**: gli strumenti di sicurezza non si integrano né gli uni con gli altri, né con l'infrastruttura informatica, incrementando così il livello di complessità.
- **Processi manuali**: i team IT investono molte ore nel mettere in correlazione eventi, log e informazioni, per cercare di capire cosa sta succedendo. Tutto ciò causa ritardi nel processo di identificazione e risposta agli incidenti.
- **Risposta reattiva**: per via di quanto indicato sopra, molti team IT devono adottare un approccio difensivo, rispondendo alle minacce solo dopo che hanno cominciato a causare danni, invece di bloccarle in fasi precedenti della catena di attacco.
- **Tempo dedicato agli interventi di emergenza**: doversi costantemente focalizzare sul blocco di minacce immediate impedisce di introdurre miglioramenti a lungo termine. Quando i team informatici sono occupati a risolvere le emergenze, spesso non hanno la possibilità di identificare la root cause dell'incidente o di documentare l'attacco e le azioni intraprese. Questo ostacola l'implementazione di una strategia volta a risolvere i problemi strutturali.
- **Dati distribuiti**: utenti e dispositivi si trovano ovunque. Di conseguenza, i dati sono dappertutto: on-premise, nel cloud o sui dispositivi, e l'accesso avviene localmente o tramite soluzioni di accesso remoto.

Un modo per risolvere molte di queste sfide è installare una soluzione di protezione Endpoint di primissima classe.

Principi di base della protezione Endpoint

Le soluzioni di Endpoint Security devono lavorare per te e con te, adattando dinamicamente i sistemi di difesa per rispondere a un attacco. Una soluzione di protezione Endpoint all'avanguardia deve come minimo adottare un approccio incentrato sulla prevenzione che offra:

Minore esposizione alle minacce: blocco di contenuti dannosi e minacce basate sul web, con controllo dell'accesso ad applicazioni, siti web, periferiche e altro.

Blocco delle attività dannose: prevenzione degli exploit e delle tecniche utilizzate da codec e ransomware per raggiungere i loro obiettivi, con identificazione di queste attività specifiche e blocco degli attacchi prima che si trasformino in un problema grave.

Risposte automatiche e adattive: i tuoi sistemi di difesa devono rispondere automaticamente alle minacce e adattarsi a eventuali cambiamenti di comportamento da parte degli hacker. Questa funzionalità non serve solo a fermare i cybercriminali, ma anche a segnalarne la presenza al tuo team, per regalargli tempo prezioso durante il quale possono avviare un'azione di risposta.

Opzioni di threat hunting (a cura di un team interno o fornite come servizio gestito): i segnali di alta qualità, arricchiti da analisi di sicurezza, possono accelerare rapidamente le attività di rilevamento e risposta alle minacce. Più è alta la qualità dei dati ottenuti, maggiore sarà la velocità con cui viene risolto un incidente.

Risultati di sicurezza ottimali

Ora che abbiamo definito le capacità che deve avere una protezione Endpoint a livello funzionale, è fondamentale valutare una prospettiva più ampia, per scoprire quali potenziali vantaggi può offrire alla tua azienda. Per essere efficace, un sistema di protezione Endpoint deve garantire risultati di sicurezza ottimali.

Riduzione del rischio informatico

Una protezione Endpoint efficace riduce il rischio informatico e difende i sistemi da un ampio spettro di minacce.

Approccio incentrato sulla prevenzione

Prima viene bloccato un attacco, meno problemi bisognerà risolvere dopo. A volte, è persino possibile che non ce ne sia alcuno. Una protezione Endpoint superiore agisce applicando più livelli di sicurezza, per difendere i sistemi dalle minacce e dagli attacchi informatici che prendono di mira computer, laptop, dispositivi mobili e server. La protezione Endpoint mette in sicurezza questi dispositivi e i dati in essi contenuti contro malware, virus, ransomware e altre attività dannose.

Identificazione di deviazioni nel profilo di sicurezza

Nel tempo, il profilo di sicurezza può presentare delle deviazioni, che sono dovute a vari motivi. Da un recente sondaggio vendor-agnostic è emerso che nel 2023 gli errori di configurazione negli strumenti di sicurezza sono stati il principale rischio di sicurezza percepito.[2]

Il nostro consiglio è optare per soluzioni di protezione in grado di valutare continuamente il profilo di sicurezza e di ottimizzare la configurazione dei sistemi in base al risultato della valutazione. Questo approccio automatizzato è fondamentale per ottenere un profilo di sicurezza robusto, che ti aiuterà a ridurre il tuo rischio informatico e ad alleviare lo stress di dover svolgere manualmente le operazioni necessarie.

Gestione semplificata

L'uso di una console di gestione centralizzata permette agli amministratori IT di monitorare e gestire da un'unica interfaccia le impostazioni di sicurezza, i criteri, le esclusioni e gli avvisi sulle minacce per tutti gli endpoint. Questo approccio semplifica la gestione della sicurezza, riduce gli errori di configurazione e garantisce una protezione omogenea. Alcune console di gestione centralizzata vanno persino oltre, verificando automaticamente l'integrità del tuo profilo di sicurezza e segnalando eventuali attività o modifiche dei criteri che potrebbero mettere a repentaglio i sistemi informatici.

Accelerazione delle attività di rilevamento e risposta

Quando un hacker si infiltra nel tuo ambiente, ogni secondo è importante. Una protezione Endpoint che comincia da un approccio incentrato sulla prevenzione riduce la quantità di avvisi non pertinenti, fornendo ai responsabili IT solo quelli ad alta affidabilità. Per indagare su questi avvisi, è possibile utilizzare tecnologie di Endpoint Detection and Response (EDR) ed Extended Detection and Response (XDR).

Alcune soluzioni offrono ancora di più, sfruttando dati di intelligenza artificiale (IA) e intelligence sulle minacce per assegnare automaticamente priorità ai rilevamenti. Con queste soluzioni, il tuo team saprà esattamente dove concentrare l'attenzione, accelerando così la risposta alle minacce con intervento umano.

Maggiore efficienza per il reparto IT

Il 64% delle aziende preferirebbe che il personale IT dedicasse più tempo ad attività di importanza strategica e meno tempo a risolvere incidenti di sicurezza urgenti[3]. Una protezione Endpoint automatizzata e semplice da usare aiuta il team IT a raggiungere questo obiettivo.

Le soluzioni Endpoint di alta qualità bloccano e rimuovono automaticamente la maggior parte delle minacce. Questo approccio aiuta a risparmiare tempo e capacità in termini di risorse IT, permettendo al personale tecnico di concentrarsi su iniziative volte a promuovere la crescita dell'azienda. Tecnologie come l'XDR agiscono alleviando il problema dell'"affaticamento da allarme", causato da una quantità eccessiva di segnali. In questo modo, il team avrà più tempo da dedicare ai progetti di maggiore importanza strategica.

L'aumento dell'efficienza derivato da questi accorgimenti consente al personale IT di passare da una protezione reattiva a una cybersecurity proattiva, poiché offre il tempo necessario per individuare le minacce prima che possano causare danni irreparabili. Questo a sua volta porta a una riduzione del rischio informatico.

2 La Vera Storia Del Ransomware 2024, Sophos, uno studio indipendente e agnostico rispetto ai vendor condotto da gennaio a febbraio 2024 tra 5.000 IT/Cybersecurity Manager in 14 paesi del mondo.

3 Il Panorama Della Cybersecurity 2023: L'Impatto Commerciale Degli Avversari Informatici, Sophos, uno studio indipendente condotto a gennaio e febbraio 2023, a cui hanno partecipato 3.000 IT/Cybersecurity Manager in 14 paesi.

Maggiore ritorno sugli investimenti nella cybersecurity

Una cybersecurity di qualità deve proteggere le organizzazioni dalle conseguenze finanziarie e operative di un incidente di sicurezza grave.

Il segreto è investire in una protezione Endpoint di qualità superiore. Una buona strategia di prevenzione costa molto meno del dover affrontare le conseguenze di un incidente. Una protezione Endpoint efficace blocca anticipatamente la maggior parte delle minacce, diminuendo il rischio di subire un attacco e di dover affrontare i costi associati.

Inoltre, le migliori soluzioni di protezione Endpoint sono in grado di integrarsi e di comunicare con i prodotti di sicurezza che già usi, per estendere la tua protezione, ridurre la complessità e fare in modo che i sistemi di sicurezza che hai già (ad es. e-mail, firewall, rete, gestione delle identità e cloud) agiscano in maniera più intelligente ed efficace.

Tutti questi accorgimenti incrementano il ritorno sui tuoi investimenti nella cybersecurity, riducendo contemporaneamente il costo totale di proprietà.

Migliore posizione cyberassicurativa

Negli ultimi anni si è osservato un aumento significativo dei premi cyberassicurativi; allo stesso tempo, i requisiti necessari per richiedere una polizza assicurativa sono diventati molto più complessi e impegnativi. Le compagnie di assicurazione esigono ora controlli informatici più potenti: il 95% delle organizzazioni che hanno acquistato un'assicurazione l'anno scorso sostiene infatti che la qualità dei sistemi di difesa ha avuto un impatto diretto sulla loro posizione assicurativa[4].

Il fattore fondamentale per migliorare la tua posizione assicurativa è ridurre al minimo il rischio informatico. Investire in sistemi di protezione efficaci, inclusi servizi di sicurezza operativi 24/7 e strumenti di rilevamento e risposta leader di settore, garantisce molti vantaggi in termini assicurativi:

1. Aiuta a ottenere più facilmente una copertura cyberassicurativa (ad es. migliorando l'assicurabilità)
2. Contribuisce a ridurre i premi assicurativi e ad avere condizioni migliori
3. Diminuisce la probabilità di dover chiedere un indennizzo, e di conseguenza anche il rischio di aumento dei premi assicurativi
4. Riduce il rischio di mancato pagamento per le richieste di indennizzo

Utilizzando tecnologie di protezione Endpoint di primissima classe, puoi aumentare le capacità di rilevamento e risposta alle minacce; ti consigliamo quindi di accertarti che siano incluse nei prodotti dei vendor che stai prendendo in considerazione. L'Endpoint Detection and Response (EDR) è ora un prerequisito obbligatorio per la maggior parte delle compagnie di cyberassicurazione; di conseguenza, le organizzazioni che non hanno questa capacità fanno fatica a stipulare una polizza.

I servizi in grado di ottimizzare il rilevamento e la risposta (e di conseguenza di minimizzare il rischio di attacco informatico) sono ormai considerati lo "standard di riferimento" per le cyberassicurazioni. Nello specifico, le organizzazioni che utilizzano servizi di Managed Detection and Response (MDR) sono ritenute clienti di "livello 1" dalle compagnie di assicurazione, poiché presentano un rischio minore.

Sulla base di queste premesse, consigliamo pertanto di optare per vendor che offrono un percorso di upgrade fluido da una soluzione di protezione Endpoint a un servizio MDR completamente gestito. Il servizio fornito deve includere threat hunting, rilevamento e/o incident response 24/7 e deve integrarsi con prodotti e controlli di sicurezza di terze parti.

5 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos.

Valutazione delle soluzioni di sicurezza endpoint: le 10 domande essenziali

Ora che abbiamo un'idea più chiara delle caratteristiche di una soluzione di sicurezza Endpoint di primissima classe, ecco un elenco di domande consigliate da rivolgere a un potenziale vendor.

1. Il prodotto adotta un approccio a livelli multipli e incentrato sulla prevenzione? Oppure è impostato su una strategia basata principalmente sul rilevamento? Quali sono le funzionalità specifiche alla base della sua tecnologia?
2. Il prodotto offre funzionalità di rilevamento e correzione automatica di eventuali deviazioni nel profilo di sicurezza? È in grado di segnalare le modifiche delle impostazioni dei criteri che aumentano il livello di rischio?
3. Il prodotto risponde automaticamente alle minacce? È in grado di rimuovere automaticamente una minaccia e di rispondere a un incidente senza interazione?
4. Il prodotto ha opzioni di difesa che rilevano gli attacchi coordinati da menti umane e adattano automaticamente le azioni di risposta?
5. Il prodotto offre potenti funzionalità antiransomware e antiexploit, che includono protezione in tempo reale contro gli attacchi basati sui ransomware che cifrano i dati da remoto? Queste funzionalità sono abilitate per impostazione predefinita? Oppure devono essere attivate e addestrate, prima che possano essere utilizzate nel tuo ambiente?
6. Quante console servono per gestire il prodotto? Questa o queste console sono ospitate nel cloud o richiedono l'installazione locale on-premise?
7. Il prodotto offre una transizione fluida a EDR/XDR con la stessa console di gestione e lo stesso agent per Endpoint e server?
8. La funzionalità XDR integra e incorpora gli avvisi provenienti da strumenti di sicurezza nativi e di terze parti, per offrire completa visibilità sull'ambiente?
9. Il prodotto offre un percorso di upgrade fluido a un servizio completamente gestito che include threat hunting, rilevamento e incident response 24/7? È predisposto per l'integrazione con i sistemi e i controlli di sicurezza di terze parti che già uso?
10. L'efficacia delle soluzioni di questo vendor è stata verificata da test indipendenti, analisti e testimonianze dei clienti, che confermano la validità del suo approccio alla protezione endpoint?

L'approccio di Sophos

Analizziamo ora l'approccio di Sophos all'Endpoint Security. Sophos Endpoint offre difese imbattibili contro gli attacchi informatici più avanzati. Con la sua protezione impenetrabile e il suo approccio di difesa in profondità a 360 gradi, blocca un'ampia gamma di minacce diverse, prima che possano compromettere i tuoi sistemi. Inoltre, offre potenti strumenti EDR e XDR che consentono al tuo team di individuare proattivamente gli attacchi, svolgere indagini e rispondere alle minacce con estrema rapidità e precisione.

Approccio incentrato sulla prevenzione

Sophos Endpoint adotta un approccio alla protezione Endpoint a 360 gradi, evitando di affidarsi a una singola tecnica di sicurezza principale. Grazie al blocco anticipato di un maggior numero di minacce, i tuoi team IT, spesso oberati di lavoro, avranno una quantità minore di incidenti da analizzare e risolvere.

Riduzione dell'esposizione alle minacce

Sophos Endpoint riduce l'esposizione alle minacce e le opportunità di attacco degli hacker. Blocca i contenuti web dannosi e le minacce on-line, permettendoti di controllare l'accesso ad applicazioni, siti web e periferiche.

Blocco delle minacce on-line e controllo dell'accesso al web

Esistono moltissime minacce on-line. Spesso le organizzazioni si affidano a firewall next-gen per proteggere gli utenti che lavorano in ufficio contro phishing, siti web dannosi e altre minacce on-line. Anche se questa strategia difende gli Endpoint all'interno del perimetro di rete aziendale, i computer possono essere utilizzati anche a casa, in viaggio, in bar e altri luoghi dove il firewall non può proteggerli.

Sophos Endpoint blocca l'accesso a siti web di phishing o contenenti altre minacce, analizzando file, pagine web e indirizzi IP. Offre una protezione ininterrotta degli endpoint, che li difende dalle minacce ovunque si trovino.

Inoltre, i SophosLabs e il team Sophos MDR forniscono dati di intelligence sulle minacce aggiornati in tempo reale, per proteggere i clienti Sophos anche dalle minacce emergenti.

Controlli per web, periferiche e applicazioni

Sophos ti consente di limitare le attività degli endpoint. Generalmente, questi controlli vengono utilizzati in combinazione con la policy di utilizzo accettabile dell'organizzazione.

Il primo controllo prevede il monitoraggio e/o il blocco dell'accesso a categorie specifiche di siti web (gioco d'azzardo, social media ecc.). Sophos Endpoint permette di monitorare e bloccare certe categorie specifiche di siti web, con criteri implementati sia all'interno che all'esterno del perimetro di rete aziendale.

Anche il controllo dell'accesso a supporti rimovibili o altre periferiche può contribuire a ridurre la superficie di attacco. Pensa a tutte le volte che un utente connette una stampante o un dispositivo di archiviazione USB, o a quando carica il suo cellulare da una porta USB... Si tratta di azioni che al momento sono autorizzate? Questo tipo di controllo non impedisce solo l'installazione di codice dannoso per mezzo di un vettore di attacco, ma è anche in grado di bloccare l'esfiltrazione dei dati aziendali.

Le applicazioni sono un'altra categoria da considerare. Il controllo delle applicazioni può impedire l'esecuzione di applicazioni o plug-in del browser sui dispositivi di lavoro. Rimanendo in tema di esfiltrazione dei dati, pensa ad esempio ad applicazioni di archiviazione nel cloud come OneDrive o Google Drive. In alternativa, considera programmi torrent, browser TOR ecc., e valuta se autorizzarne o meno l'uso sui tuoi endpoint. Esiste un'ampia selezione di plug-in del browser, alcuni hanno usi legittimi e utili, altri invece no.

Blocco delle attività dannose

Il livello di protezione successivo prevede l'uso di intelligenza artificiale, analisi del comportamento, antiransomware, antiexploit e altre tecnologie, per bloccare le minacce prima che diventino un serio pericolo.

Sophos applica una protezione con approccio AI-first, che comincia con la classificazione basata sull'intelligenza artificiale dei file eseguibili. Sfrutta un modello addestrato con milioni di file eseguibili dannosi e innocui. Questo modello è in grado di identificare rapidamente i file eseguibili pericolosi in base alle loro proprietà, ed è completamente indipendente dalle firme.

Protezione impenetrabile contro i remote ransomware

Sophos Endpoint è la strategia di sicurezza endpoint zero-touch più efficace contro gli attacchi ransomware, sia che agiscano localmente o da remoto. Include la tecnologia avanzata CryptoGuard, che rileva gli indicatori di crittografia non autorizzata, indipendentemente da quale origine abbiano. Questo approccio universale blocca le nuove varianti del ransomware, proteggendoti anche da quelle che crittografano i sistemi da remoto. Si basa sull'ispezione delle modifiche dei contenuti dei file in tempo reale, per rilevare i tentativi di crittografia non autorizzata, fermando i remote ransomware che si eseguono su un dispositivo diverso e che cercano di crittografare i file sfruttando la rete. I file crittografati dal ransomware vengono automaticamente ripristinati allo stato pre-attacco, indipendentemente dalle dimensioni o dal tipo di file. Questo riduce al minimo l'impatto sulla produttività aziendale. Inoltre, protegge il Master Boot Record (MBR) dai tipi di crittografia utilizzati in alcuni tipi di attacchi ransomware.

Antiexploit

Le tecnologie antiexploit bloccano i comportamenti e le tecniche che gli hacker sfruttano per compromettere i dispositivi, prelevare illecitamente le credenziali e distribuire malware. Per prevenire gli exploit, Sophos adotta approcci innovativi basati sui singoli dispositivi e completamente scalabili per tutte le applicazioni. Le soluzioni Sophos sono subito pronte per l'uso: si basano sulla protezione di Microsoft Windows e la utilizzano come base, aggiungendo un minimo di 60 attenuazioni degli exploit esclusive, preconfigurate e già ottimizzate. Sophos è quindi in grado di proteggere la tua organizzazione dagli attacchi fileless e dagli exploit zero-day, bloccando le tecniche utilizzate in tutte le fasi della catena di attacco.

Difese Adattive

Queste ulteriori funzionalità di difesa dinamiche sono innovazioni esclusive nel settore della cybersecurity: offrono infatti una protezione automatica più evoluta, che si adatta al contesto di un attacco. Sophos Endpoint blocca le azioni che non sono di per sé dannose in un contesto quotidiano, ma che sono pericolose nell'ambito di un attacco. Questa funzionalità risponde in maniera dinamica e interrompe gli attacchi attivi, nei quali i cybercriminali potrebbero aver ottenuto l'accesso ai sistemi senza destare sospetti e senza servirsi di codice dannoso.

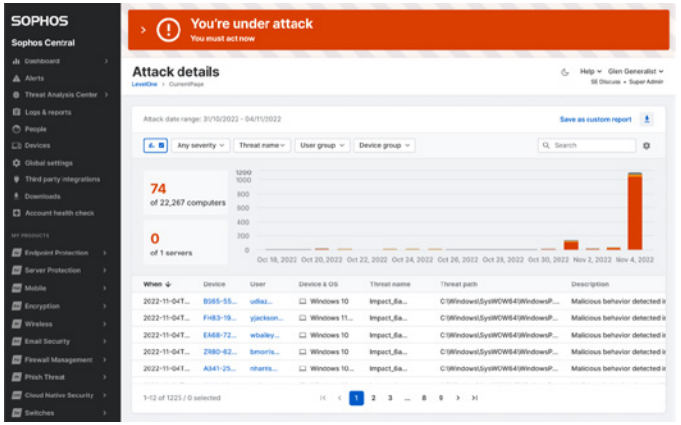
	PROTEZIONE BASATA SUL COMPORTAMENTO	PROTEZIONE ADATTIVA CONTRO GLI ATTACCHI	AVVISO DI ATTACCO CRITICO
AMBITO	DISPOSITIVO INDIVIDUALE	DISPOSITIVO INDIVIDUALE	DISPOSITIVO INDIVIDUALE
VANTAGGI	Il motore di rilevamento dei comportamenti blocca le fasi iniziali degli attacchi degli antagonisti attivi	Eleva la sensibilità della protezione, per prevenire i danni	Segnala al cliente la presenza di un attacco che richiede un'incident response immediata
DETONAZIONE	Regole di comportamento	Rilevamento di strumenti di hacking	Indicatori ad alto impatto di presenza di antagonisti attivi, che includono correlazioni a livello dell'intera organizzazione e soglie specifiche
ANALOGIA	"PROTEZIONE ATTIVA!"	"PROTEZIONE RAFFORZATA!"	"ALLARME ROSSO!"

Adaptive Attack Protection

L'Adaptive Attack Protection attiva dinamicamente livelli più alti di protezione sugli endpoint, non appena viene rilevato un attacco coordinato da menti umane. Questa strategia nega ai cybercriminali la capacità di intraprendere altre azioni, riducendo la superficie di attacco, bloccando e isolando l'attacco in corso e regalando tempo prezioso ai team di sicurezza, che possono quindi avviare una risposta adeguata.

Critical Attack Warning

Un Critical Attack Warning segnala la presenza di un attacco grave che riguarda l'intero ambiente informatico: si verifica quando viene rilevata attività criminale su più Endpoint o server all'interno della tua infrastruttura, con ulteriori indicatori ad alto impatto. È una situazione di allarme rosso e sei sotto attacco! Le tecnologie automatiche ti informano della situazione, fornendoti il contesto e i dettagli dell'attacco. Puoi rispondere utilizzando Sophos XDR, puoi richiedere assistenza al tuo Partner, oppure puoi rivolgerti al team Sophos Incident Response per contrastare la minaccia.



Riduci il costo totale di proprietà delle soluzioni di cybersecurity

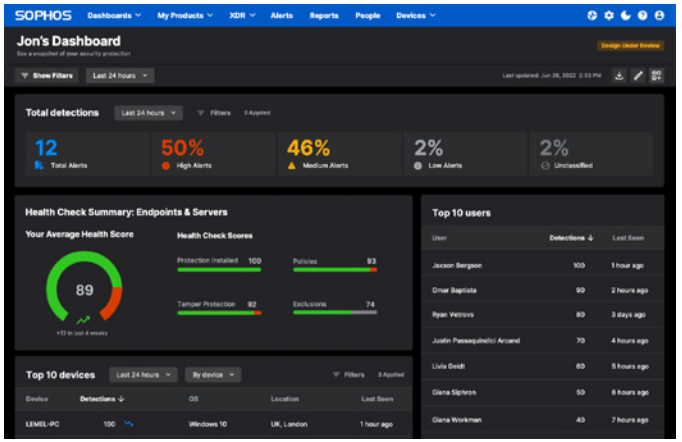
Nella maggior parte dei casi, i team IT e il personale di cybersecurity sono oberati di lavoro. Automazione e strategie volte a risparmiare tempo e fatica sono il leitmotiv di Sophos Endpoint. Qualsiasi azione che possa essere automatizzata, ridotta o rimossa dal carico di lavoro del reparto IT e del personale di cybersecurity permette a questi team di concentrare la loro attenzione su altre iniziative di importanza strategica per l'azienda.

Sophos Central offre una piattaforma di management basata sul cloud, con la quale puoi gestire tutti i tuoi prodotti Sophos (soluzioni per endpoint, server, dispositivi mobili, firewall, switch, access point, e-mail e cloud), incluso Sophos Endpoint. Con una singola interfaccia, puoi creare e gestire criteri, visualizzare rilevamenti e avvisi, indagare su potenziali minacce, correggerle, e svolgere altre azioni sui tuoi prodotti Sophos.

Le tecnologie di sicurezza consigliate da Sophos sono tutte abilitate per default; di conseguenza, sono semplici da configurare e offrono immediatamente il massimo livello di protezione, senza bisogno di complicate modifiche delle impostazioni.
Se richiesto, è anche disponibile un controllo più granulare.

Identificazione di deviazioni nel profilo di sicurezza

Nel tempo, il profilo di sicurezza di un'organizzazione può presentare deviazioni dagli standard di conformità o dalle configurazioni ottimali. Se non vengono configurate correttamente, le impostazioni dei criteri, le esclusioni e altre opzioni possono presentare un rischio di sicurezza per il tuo profilo di protezione. Il Sophos Account Health Check valuta il tuo profilo di sicurezza, identificando deviazioni dagli standard di settore ed eventuali errori di configurazione: potrai così risolvere i problemi con un semplice clic.

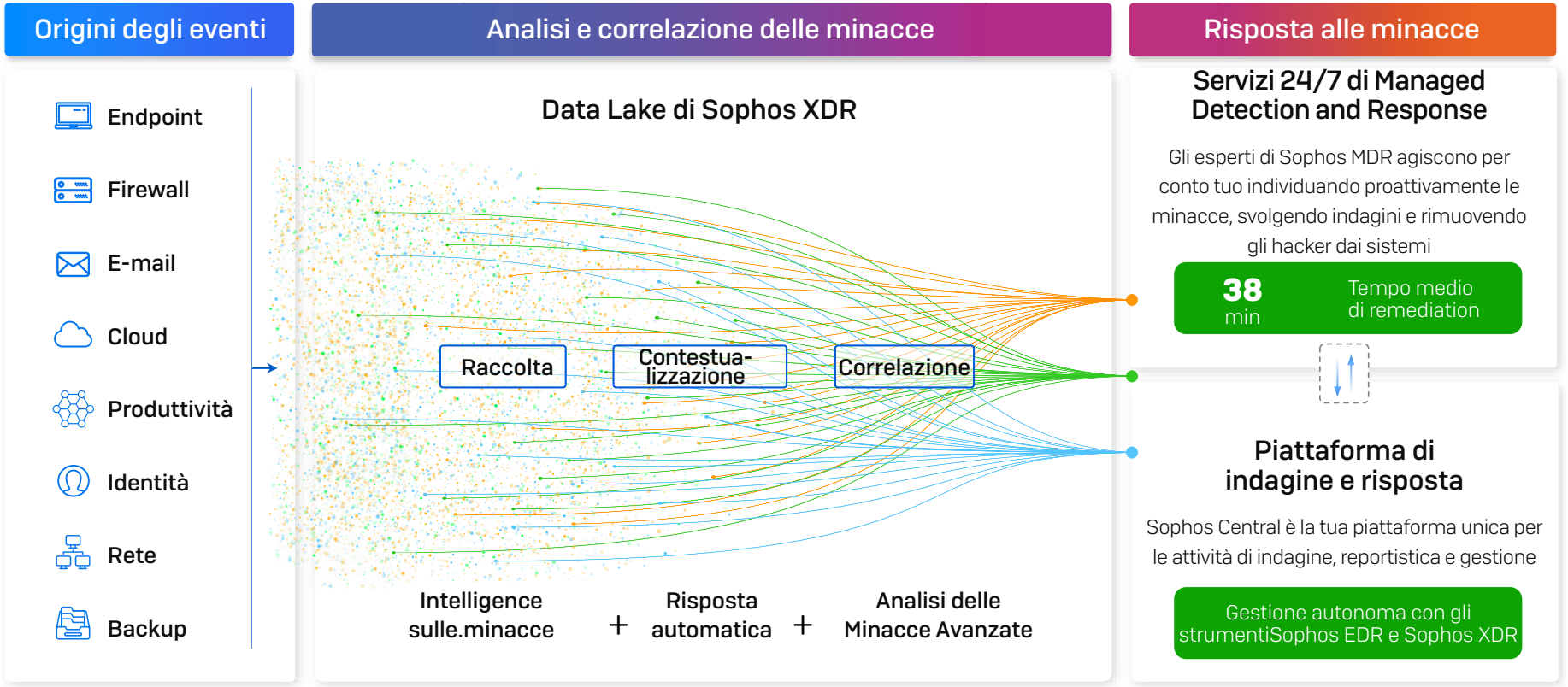


Synchronized Security

Le soluzioni Sophos danno il meglio di sé quando vengono utilizzate insieme. Sophos Endpoint condivide informazioni sullo stato di sicurezza e sull'integrità dei sistemi con Sophos Firewall, Sophos ZTNA e altri prodotti, per fornire maggiore visibilità sulle minacce e sull'uso delle applicazioni. Synchronized Security isola automaticamente i dispositivi compromessi fino a quando non ne viene completata la disinfezione, concedendo di nuovo l'accesso alla rete solo dopo la neutralizzazione della minaccia. L'intero processo è automatico e non richiede alcun intervento manuale da parte degli amministratori.

Accelerazione del rilevamento e della risposta: EDR, XDR e MDR

L'approccio incentrato sulla prevenzione di Sophos blocca e rimuove automaticamente tutte le minacce possibili; di conseguenza, i team IT e il personale di cybersecurity avranno una quantità minore di rilevamenti da analizzare, e questi rilevamenti saranno di alta qualità.



L'approccio di Sophos alla prevenzione, al rilevamento e alla risposta.

Sophos Endpoint Detection and Response (EDR)

Sophos integra potenti capacità di rilevamento e risposta alle minacce nell'approccio incentrato sulla prevenzione di Sophos Endpoint, permettendoti così di individuare proattivamente le minacce, di svolgere indagini e di rispondere in maniera tempestiva alle attività sospette rilevate su Endpoint e server. I rilevamenti ricevono una priorità, grazie alle analisi basate sull'IA. Questa strategia ti fa risparmiare tempo prezioso, poiché ti aiuta a capire dove devi concentrare la tua attenzione. Il personale tecnico può accedere ai dispositivi da remoto per indagare sui problemi, installare e disinstallare software o svolgere altre attività di troubleshooting.

Sophos Extended Detection and Response (XDR)

Per le organizzazioni che cercano una soluzione più completa, che va oltre le funzionalità di rilevamento e risposta, Sophos XDR consente di individuare proattivamente le minacce, condurre indagini e rispondere alle attività sospette e agli attacchi a più fasi che vengono rilevati nell'intero ambiente informatico. Progettata dagli analisti di sicurezza per offrire la soluzione ideale ad altri esperti, Sophos XDR è l'unico strumento SecOps nell'intero settore della cybersecurity che unisce i dati di telemetria nativi di Sophos a quelli generati dai controlli di sicurezza di terze parti, accelerando così le attività di rilevamento e risposta. Sophos XDR offre integrazioni subito pronte per l'uso con un ampio ecosistema di soluzioni per endpoint, firewall, rete, e-mail, identità, produttività, cloud e backup. Questo ti permette di ottenere un maggiore ritorno sull'investimento per gli strumenti di sicurezza già in tuo possesso.

Sophos Managed Detection and Response (MDR)

Alle organizzazioni che non hanno le risorse necessarie per gestire internamente il rilevamento e la risposta alle minacce, Sophos MDR offre un servizio operativo 24/7, a cura di un team selezionato di esperti di threat hunting e incident response. Sophos MDR sfrutta i dati di telemetria dei prodotti Sophos e dei controlli di sicurezza di terze parti per rilevare e neutralizzare anche le minacce più complesse e sofisticate.

Sia Sophos XDR che Sophos MDR sono soluzioni realizzate per venire incontro alle tue esigenze: si integrano con le tecnologie che già usi (inclusi prodotti per e-mail, firewall, rete, gestione delle identità e cloud), per permetterti di ottenere un maggiore ritorno sui tuoi investimenti informatici.

Sophos Incident Response Service Retainer

Sophos Incident Response Services Retainer è una subscription annuale che offre ai clienti Endpoint, EDR e XDR accesso rapido e "on-demand" al nostro team di esperti di incident response, subito pronti a entrare in azione nel tuo ambiente IT per sventare e isolare l'attacco, rimuovendo completamente la presenza dei cybercriminali. I nostri esperti sono capaci di ristabilire la normale operatività, evitando lunghi tempi di attesa e molta burocrazia, grazie ai termini di servizio concordati in anticipo.

Perché Sophos

Sophos è un'azienda leader mondiale e innovatrice nell'ambito delle soluzioni avanzate di cybersecurity. Aiuta le organizzazioni a debellare gli attacchi informatici, offrendo servizi che includono MDR e incident response, oltre a una vasta gamma di tecnologie di protezione per endpoint, rete, e-mail e cloud. In quanto uno dei principali provider di cybersecurity, Sophos protegge oltre 550.000 realtà e più di 100 milioni di utenti a livello globale da potenziali minacce, ransomware, phishing, malware e altro. Questa visibilità imbattibile sul panorama delle minacce offre dati di intelligence sulle minacce che non hanno eguali e che vengono utilizzati per potenziare le capacità di difesa dei prodotti e dei servizi Sophos per tutti i clienti.

Test indipendenti

I test indipendenti condotti da aziende che godono di un'ottima reputazione nel mondo della cybersecurity sono uno strumento utilissimo, perché aiutano le organizzazioni a prendere decisioni informate, nonché a scegliere meglio i prodotti di sicurezza da acquistare e inserire nel loro stack tecnologico. Tuttavia, con il costante aumento del volume e della complessità degli attacchi, è possibile ottenere risultati significativi solo quando i test riflettono le capacità effettive delle organizzazioni nel mondo reale.

SE Labs

Gli SE Labs sono una delle poche aziende specializzate in test di sicurezza che utilizzano simulazioni realistiche con le tattiche, tecniche e procedure (TTP) di attacco sfruttate attualmente da cybercriminali e penetration tester.

Nell'ultimo report sull'Endpoint Security degli SE Labs (gennaio-marzo 2024), Sophos si è classificata ancora una volta come la migliore protezione nell'intero settore, aggiudicandosi valutazioni AAA in tutti i test, sia nella categoria Enterprise che SMB. Il report degli SE Labs per il primo trimestre del 2024 è disponibile su questo link:

Endpoint Security: Enterprise | Endpoint Security: SMB

Valutazioni MITRE Engenuity ATT&CK

Sophos ha spiazzato la concorrenza nelle valutazioni MITRE Engenuity ATT&CK 2023 per la categoria Enterprise (Turla). In questa valutazione, Sophos XDR ha rilevato il 99% dei comportamenti dannosi, segnalando 141 su 143 fasi di attacco malware. Inoltre, a dimostrazione della sua capacità di offrire ai team di sicurezza un contesto estremamente dettagliato sul cosa, come e perché dei comportamenti dei cybercriminali, Sophos XDR ha registrato un'ottima copertura analitica, rilevando il 98% delle fasi di attacco nella valutazione.

Le valutazioni MITRE Engenuity ATT&CK sono fra i test di sicurezza indipendenti più autorevoli a livello internazionale. Questo è in parte dovuto all'accurata ricostruzione ed emulazione di scenari di attacco realistici, alla trasparenza dei risultati e alla grande quantità di informazioni fornite sui vendor analizzati.

Premi e report degli analisti

Gartner

- ✓ Leader nel Gartner Magic Quadrant for Endpoint Protection Platforms (piattaforme di protezione endpoint) per 14 report consecutivi
- ✓ Customers' Choice nei report Gartner® Peer Insights™ "Voice of the Customer for Endpoint Protection Platforms" (EPP) per il 2022, il 2023 e il 2024

IDC

- ✓ Leader nel report IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses 2024

G2

- ✓ Leader complessivo | Categoria suite di protezione endpoint: report Grid primavera 2023 e autunno 2023
- ✓ Leader complessivo | Categoria EDR: report Grid primavera 2023 e autunno 2023
- ✓ Leader complessivo | XDR: report Grid autunno 2023
- ✓ Leader complessivo e soluzione n°1 | XDR: report Grid primavera 2023

Omdia

- ✓ Leader Complessivo | Novembre 2022, piattaforme complete di Extended Detection and Response (XDR)

CRN Tech Innovators Awards 2023

- ✓ Sophos Intercept X viene nominata migliore protezione endpoint

Readers' Choice Awards di ChannelPro

- ✓ Sophos Intercept X si aggiudica il titolo di Gold Winner nella categoria Best Endpoint Security Vendor

Testimonianze dei clienti

★★★★★

"La funzionalità più potente di Sophos Endpoint Protection è la sua protezione avanzata contro le minacce, poiché Sophos utilizza una combinazione di tecnologie avanzate quali machine learning, analisi del comportamento e rilevamento basato sulle firme, per rilevare e bloccare le minacce più pericolose."

Software Developer | Finance (settore non bancario)| Leggi la recensione completa su Gartner Peer Insights

★★★★★

"Una soluzione con un'interfaccia unica, per rispondere alle minacce di cybersecurity più avanzate."

Network Administrator | Education | Leggi la recensione completa su Gartner Peer Insights

★★★★★

"La mia esperienza è stata appagante dal punto di vista industriale: riduce la superficie di attacco e impedisce all'attacco di diffondersi nella rete della nostra organizzazione. Con le sue capacità antiransomware e le tecnologie di IA basate sul deep learning, blocca gli attacchi prima che possano avere ripercussioni sul sistema, il che è un vantaggio enorme."

ICT Security Officer | Mezzi di comunicazione radiotelevisivi | Leggi il commento intero nelle recensioni di G2

★★★★★

"Sophos è una soluzione semplice da usare, ma potente."

IT Operations Manager | Organizzazione di medie dimensioni | Leggi il commento intero nelle recensioni di G2

★★★★★

"Sophos Endpoint aiuta a ridurre la nostra vulnerabilità agli attacchi e ci garantisce la tranquillità di una protezione costante contro gli hacker per i sistemi dei nostri clienti."

Responsabile di gestione, backup e ripristino dei sistemi | Impresa di grande dimensioni | Leggi il commento intero nelle recensioni di G2

Conclusione

La cybersecurity è caratterizzata da una quantità estremamente elevata di cybercriminali. Come se non bastasse, si evolve in maniera estremamente rapida. Gli hacker sfruttano tecniche sempre più complicate per eludere le difese delle aziende, e i vendor e le organizzazioni devono necessariamente adattarsi.

Per farlo, è fondamentale impiegare strumenti che adottano un approccio incentrato sulla prevenzione. Questi strumenti offrono una strategia di difesa automatizzata e adattiva, che blocca o rallenta gli autori degli attacchi e aiuta a guadagnare tempo prezioso per avviare un'azione di risposta.

Allo stesso tempo, una buona conoscenza delle caratteristiche da esigere in una soluzione di protezione endpoint, unita a un'ottima comprensione di quali debbano essere i risultati di sicurezza ottimali, può aiutarti a prendere una decisione informata. La tua organizzazione potrà così ottenere la protezione più efficace contro gli attacchi moderni.

Sophos difende le organizzazioni dalle minacce attuali e da quelle in continua evoluzione: le nostre soluzioni aiutano le organizzazioni a raggiungere i migliori risultati di sicurezza possibili. Per saperne di più, contattaci oggi stesso.

Per scoprire di più su Sophos Endpoint e su come agisce per garantire una protezione imbattibile anche contro gli attacchi più avanzati, visita **Sophos.it/endpoint**

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

2024-06-18 IT-WP (PS)

SOPHOS