BROCHURE ILLUSTRATIVA DELLA SOLUZIONE

Sophos Endpoint

con tecnologia Intercept X

La più sofisticata soluzione di protezione Endpoint basata sull'IA nel settore della cybersecurity

Sophos Endpoint con tecnologia Intercept X offre una protezione che non ha rivali, poiché blocca gli attacchi più avanzati prima che possano avere un impatto negativo sui tuoi sistemi. Include potenti strumenti di Endpoint Detection and Response ed Extended Detection and Response (EDR/XDR), che permettono alla tua azienda di individuare proattivamente attività sospette e indicatori di attacco e di svolgere indagini, avviando una risposta tempestiva.

Un approccio alla sicurezza incentrato sulla prevenzione

Sophos Endpoint adotta un approccio alla sicurezza a 360 gradi e incentrato sulla prevenzione, per bloccare le minacce senza fare affidamento su un'unica tecnica. I diversi modelli di deep learning basati sull'IA proteggono i sistemi sia contro attacchi noti che contro minacce mai osservate prima. I controlli del web, delle applicazioni e delle periferiche riducono la superficie esposta alle minacce e bloccano i più comuni vettori di attacco. Le capacità di analisi anti-ransomware, anti-exploit e del comportamento, nonché altre tecnologie avanzate, bloccano rapidamente le minacce, prima che possano aggravarsi. In questo modo, i team informatici, solitamente oberati di lavoro, avranno meno incidenti su cui indagare e intervenire.

Protezione anti-ransomware impenetrabile

Sophos Endpoint offre i più potenti sistemi di difesa endpoint zero-touch in assoluto, per contrastare anche i ransomware più sofisticati. La tecnologia CryptoGuard blocca in tempo reale la crittografia non autorizzata e ripristina automaticamente allo stato pre-attacco i file crittografati in maniera illecita, riducendo al minimo l'impatto commerciale dell'incidente.

Difese adattive

Le nostre difese dinamiche sono pioniere nel settore e si adattano rapidamente per rispondere in maniera tempestiva agli active adversary e agli attacchi coordinati da menti umane. Gli autori degli attacchi vengono così privati della capacità di agire, poiché l'attacco viene bloccato e isolato, facendo guadagnare al team IT tempo prezioso per avviare una risposta.

Facile da configurare e da gestire

Sophos Central è una potente piattaforma di gestione unificata e basata sul cloud per tutte le soluzioni di cybersecurity Next-Gen di Sophos. Le tecnologie e le funzionalità di sicurezza consigliate sono abilitate di default, per cui avrai immediatamente il massimo livello di protezione, senza dover ottimizzare le impostazioni.

Leader con un'ottima reputazione nel settore dell'endpoint security

Sophos Endpoint riceve continuamente i massimi riconoscimenti da parte di clienti, analisti e organizzazioni che svolgono test indipendenti. Sophos è stata collocata 16 volte tra i Leader nel Gartner® Magic Quadrant™ for Endpoint Protection Platforms (Piattaforme di protezione endpoint), e si è aggiudicata il 1° posto come migliore suite di Endpoint Detection and Response negli Spring 2025 G2 Grid® Reports.

Caratteristiche principali

- I diversi modelli di deep learning basati sull'IA proteggono i sistemi sia contro attacchi noti che contro minacce mai osservate prima.
- Riduci la superficie esposta e blocca i più comuni vettori di attacco grazie a controlli del web, delle applicazioni e delle periferiche.
- Blocca rapidamente le minacce prima che possano aggravarsi, utilizzando l'analisi del comportamento, le funzionalità anti-ransomware e anti-exploit, e altre tecnologie avanzate.
- Difendi i dati dagli attacchi ransomware locali e remoti, grazie alla migliore protezione disponibile nel settore.
- Approfitta delle nostre difese dinamiche innovative ed esclusive, che si adattano automaticamente per rispondere agli active adversary e agli attacchi hands-on-keyboard
- Individua proattivamente le attività sospette, svolgi indagini e avvia azioni di risposta con i potenti strumenti EDR e XDR.

Un approccio incentrato sulla prevenzione che riduce la superficie di attacco

Il blocco tempestivo delle minacce richiede meno risorse rispetto al monitoraggio e agli interventi correttivi nelle fasi più avanzate della catena di attacco. Sophos Endpoint include tecnologie di protezione sofisticate, in grado di fermare un'ampia gamma di attacchi. I controlli del web, delle applicazioni e delle periferiche riducono la superficie di attacco e bloccano i vettori più comunemente sfruttati dalle minacce. Queste funzionalità limitano le opportunità di attacco per gli hacker che cercano di infiltrarsi nel tuo ambiente.

Protezione web

Blocca il traffico del browser verso siti web pericolosi, bloccando le minacce in fase di distribuzione e impedendo l'accesso a siti di phishing o contenenti malware.

Controllo web

Blocca l'accesso a contenuti indesiderati e inappropriati. Implementa le norme di utilizzo accettabile del web nell'intera organizzazione e la protegge dalla perdita di dati.

Reputazione dei download

Analizza i file scaricati utilizzando i dati globali di intelligence sulle minacce dei SophosLabs per emettere un verdetto in base a fattori quali prevalenza, durata e origine, consigliando agli utenti di bloccare i file con reputazione pessima o sconosciuta.

Controllo delle applicazioni

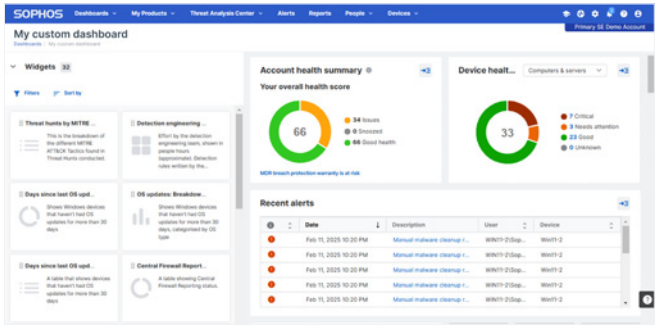
Blocca applicazioni vulnerabili o inadeguate grazie all'uso di categorie preimpostate, eliminando la necessità di bloccare le app una per una in base all'hash.

Controllo delle periferiche (Controllo dei dispositivi)

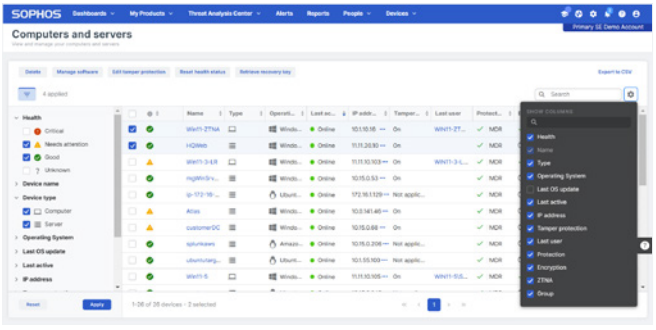
Monitora e blocca l'accesso a dispositivi rimovibili, Bluetooth e device mobili, per impedire ove lo si ritenga opportuno l'accesso alla rete aziendale.

Prevenzione della perdita di dati (Data Loss Prevention, DLP)

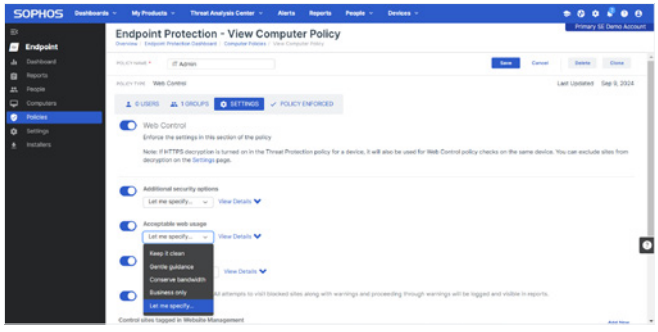
Monitora e impone restrizioni sul trasferimento di file contenenti dati di natura sensibile. Serve, ad esempio, a impedire che un utente invii un file di natura riservata alla propria webmail



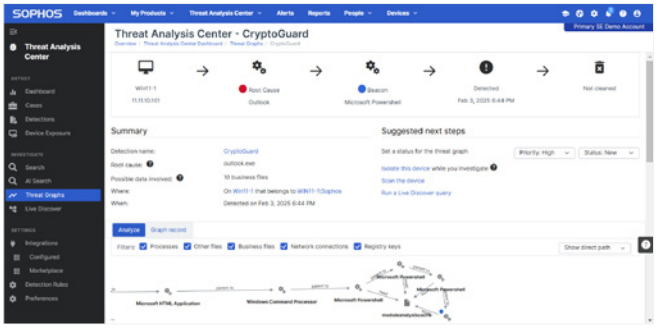
Crea dashboard personalizzate in base alle tue esigenze.



Endpoint security facile da configurare e da gestire.



Criteri configurabili, con le impostazioni consigliate abilitate di default.



Analizza le minacce per determinarne la causa originaria.

Un approccio incentrato sulla prevenzione che blocca rapidamente le minacce

Rilevare e correggere tempestivamente le minacce riduce i rischi. Sophos Endpoint blocca le minacce rapidamente e prima che possano aggravarsi. In questo modo i team informatici, solitamente oberati di lavoro, hanno meno incidenti su cui dover indagare e intervenire. Sophos offre potentissime opzioni di prevenzione delle minacce, con un'efficacia confermata dagli altissimi punteggi ottenuti ripetutamente in test indipendenti sulla sicurezza.

Protezione anti-ransomware impenetrabile

Secondo l'edizione 2024 del Report sulla difesa digitale Microsoft, la crittografia remota viene utilizzata nel 70% degli attacchi che vanno a segno, il 92% dei quali proviene da dispositivi non gestiti collegati alla rete. Sophos Endpoint offre la più potente protezione endpoint zero-touch contro i ransomware locali e remoti, grazie alla tecnologia avanzata CryptoGuard, che rileva i tentativi di crittografia, indipendentemente dalla loro origine.

- Blocca le nuove varianti di ransomware che sfruttano tecniche moderne.
- Ispeziona le modifiche dei file in tempo reale per individuare le attività di crittografia non autorizzate.
- Impedisce ai remote ransomware di crittografare i file da remoto, attraverso la rete.
- Ripristina automaticamente i file crittografati al loro stato pre-attacco, grazie alle nostre tecnologie proprietarie che non si basano sul Servizio Copia Shadow di Windows.
- Protegge file di tutti i tipi e tutte le dimensioni, con impatto minimo sulla performance.
- Tutela l'integrità del record di avvio principale (MBR), difendendolo dagli attacchi più avanzati che colpiscono l'hard disk.

IA con deep learning integrata nel rilevamento anti-malware

Rileva e blocca sia i malware noti che quelli mai osservati prima, analizzando gli attributi dei file e utilizzando logiche predittive per identificare le minacce.

Anti-exploit

Protegge l'integrità dei processi incrementando la sicurezza della memoria e offrendo più di 60 tecniche anti-exploit. Non richiede alcuna configurazione e supera nettamente le funzionalità native di Windows e di altre soluzioni di sicurezza.

Protezione basata sull'analisi comportamentale

Monitora processi, file ed eventi di registro per rilevare e bloccare le attività pericolose. Analizza la memoria, ispeziona i processi in esecuzione per identificare eventuali minacce nascoste e individua gli autori degli attacchi che utilizzano codice malevolo per eludere il rilevamento.

Synchronized Security

Sophos Endpoint condivide informazioni sullo stato di sicurezza e sull'integrità dei sistemi con Sophos Firewall, Sophos Zero Trust Network Access (ZTNA) e altri prodotti Sophos, per fornire maggiore visibilità sulle minacce e sull'uso delle applicazioni; inoltre, isola automaticamente i dispositivi compromessi.

Live Protection

Estende ulteriormente la potente protezione disponibile sui dispositivi, integrando ricerche in tempo reale nei database globali di intelligence sulle minacce dei SophosLabs. Potrai così ottenere maggiori informazioni di contesto relative ai file, prendere decisioni sulla loro natura, verificarli, eliminare i falsi positivi e determinarne la reputazione.

Lockdown delle applicazioni

Previene l'utilizzo improprio del browser e delle applicazioni, poiché impedisce di svolgere le azioni che non sono normalmente associate a questi processi.

Antimalware Scan Interface (AMSI)

L'Antimalware Scan Interface (AMSI) di Windows blocca gli attacchi fileless, nei quali il malware viene caricato direttamente dalla memoria. Sophos Endpoint include anche un'opzione proprietaria di mitigazione dei tentativi di eludere il rilevamento di AMSI.

Malicious Traffic Detection (Rilevamento del traffico malevolo)

Rileva i dispositivi che comunicano con server di Comando e Controllo (C2), intercettando e analizzando il traffico non generato dai browser, per identificare eventuali destinazioni pericolose.

Difese adattive

Sophos Endpoint si basa sulle nostre difese dinamiche, con funzionalità innovative che automatizzano la protezione adattandosi in tempo reale, per rispondere agli active adversary e agli attacchi coordinati da menti umane. Sophos Endpoint blocca le azioni che di per sé potrebbero non essere 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.

Adaptive Attack Protection

Implementa dinamicamente livelli di protezione più elevati su un endpoint quando viene identificato un attacco coordinato da menti umane, sventando così i piani degli active adversary e consentendo di recuperare tempo prezioso per adottare una risposta adeguata.

Critical Attack Warning

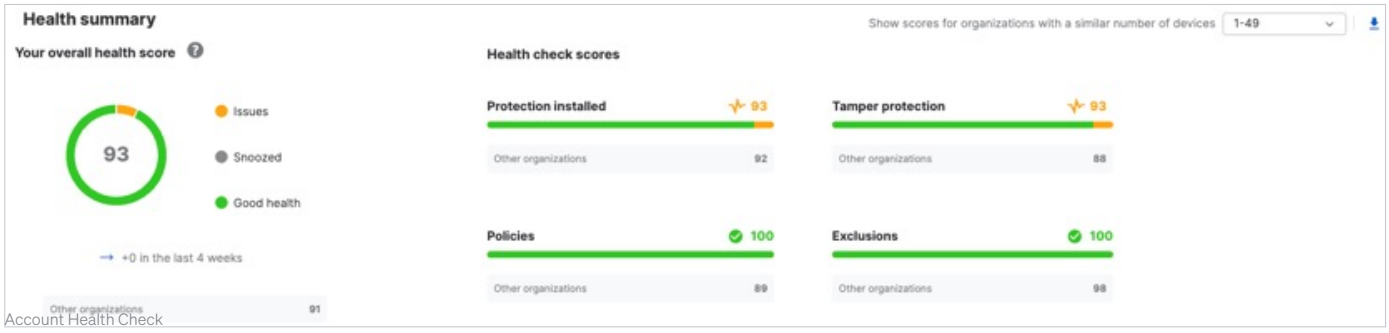
Segnala agli amministratori quando vengono rilevate attività cybercriminali gravi su più endpoint, basandosi sui dati di rilevamento delle minacce raccolti nell'intera organizzazione.

	PROTEZIONE BASATA SULL'ANALISI COMPORTAMENTALE	PROTEZIONE ADATTIVA CONTRO GLI ATTACCHI	AVVISO DI ATTACCO CRITICO
AMBITO	DISPOSITIVO INDIVIDUALE	DISPOSITIVO INDIVIDUALE	INTERO AMBIENTE
VANTAGGI	Il motore di rilevamento dei comportamenti blocca le fasi iniziali degli attacchi degli active adversary	Eleva la sensibilità della protezione, per prevenire gli attacchi	Segnala l'eventuale 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!"

Difese adattive in Sophos Endpoint

Identificazione di deviazioni nel profilo di sicurezza

Se non vengono configurate correttamente, le impostazioni dei criteri, le esclusioni e altre opzioni possono mettere in pericolo il tuo profilo di sicurezza. La funzionalità Account Health Check valuta il tuo profilo di sicurezza, identificando le deviazioni dagli standard di settore ed eventuali errori di configurazione. Potrai così risolvere i problemi con un semplice clic.



Account Health Check

Livelli di protezione aggiuntivi (add-on)

Sophos ZTNA

Connetti in modo sicuro i tuoi utenti alle tue applicazioni, con l'opzione definitiva per sostituire la VPN. Sophos ZTNA è l'unica soluzione Zero Trust Network Access profondamente integrata nei prodotti di protezione endpoint next-gen.

Crittografia dei dispositivi

Con l'enorme quantità di dispositivi che ogni giorno vengono rubati o smarriti, la crittografia completa del disco è indispensabile. Device Encryption integrata in Sophos Endpoint permette di gestire in maniera efficace BitLocker (Windows) e FileVault (macOS).

Accelerazione delle attività di rilevamento, indagine e risposta

Sophos Endpoint blocca automaticamente la maggior parte delle minacce nelle fasi iniziali di un attacco, riducendo la quantità di eventi da analizzare. Per le attività sospette e le minacce che richiedono un'analisi a cura di esperti umani, Sophos offre potenti soluzioni in grado di svolgere rapidamente attività di rilevamento, indagine e risposta su tutti i principali vettori di attacco.

Sophos XDR

Sophos Extended Detection and Response (XDR) ti permette 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. Progettati dai nostri analisti di sicurezza per utenti di qualsiasi livello di competenza tecnica, i nostri potenti strumenti con funzionalità GenAI permettono a chiunque (dal personale tecnico non specializzato fino agli analisti SOC esperti) di indagare rapidamente sulle minacce e neutralizzare gli active adversary.

Sophos XDR offre integrazioni pronte all'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.

Per saperne di più, visita Sophos.it/XDR

Sophos MDR

Sophos Managed Threat Detection and Response (MDR) offre alle aziende che non hanno le risorse necessarie per gestire internamente il rilevamento e la risposta alle minacce, un servizio operativo 24/7, a cura di un team selezionato di analisti di sicurezza, threat hunter ed esperti di incident response. Sophos MDR sfrutta i dati di telemetria dei prodotti Sophos e delle tecnologie di sicurezza di terze parti per rilevare e neutralizzare anche le minacce più sofisticate.

Sophos MDR viene incontro alle esigenze della tua azienda, offrendo vari livelli di servizio, modalità di risposta diverse e un'ottima compatibilità con gli strumenti e le tecnologie che già usi.

Per saperne di più, visita Sophos.it/MDR

	Sophos Endpoint	Sophos XDR	Sophos MDR
Protezione next-gen contro le minacce IA con deep learning integrata nel rilevamento antimalware, protezione web	✓	✓	✓
Blocco delle attività pericolose Anti-ransomware, anti-exploit, difese adattive	✓	✓	✓
Riduzione dell'esposizione alle minacce DLP e funzionalità di controllo del web, delle periferiche e delle applicazioni	✓	✓	✓
Rilevamento e risposta Potenti strumenti di indagine e risposta alle minacce		✓	✓
Visibilità sulle principali superfici di attacco Integrazione di tecnologie Sophos e di terze parti		✓	✓
Rilevamento e risposta gestiti Monitoraggio e incident response 24/7 a cura di un team di esperti			✓

Scopri perché i clienti scelgono Sophos Endpoint

Sophos è uno dei leader indiscussi nel mercato dell'endpoint security e i riconoscimenti ufficiali degli esperti di settore lo dimostrano.

Gartner

Sophos nominata tra i Leader nel Gartner® Magic Quadrant™ per il 2025 nella categoria Piattaforme di protezione endpoint, per 16 report consecutivi.

SE Labs

Sophos continua a ottenere le massime valutazioni nei test indipendenti sull'endpoint security, confermando la sua posizione di Leader di settore.

Leader

Sophos è l'unico vendor a essere nominato tra i Leader nei Winter 2025 Overall Grid® Reports di G2 per le categorie Endpoint Protection Suites (Suite di protezione endpoint), EDR, XDR e MDR.

IDC

Sophos si classifica tra i Leader nel report 2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses.

Gartner Peer Insights Customers' Choice 2025

Sophos è il vendor "Customers' Choice" di Gartner® Peer Insights™ nel report Voice of the Customer 2025 per le Endpoint Protection Platforms.

Effettua subito una prova gratuita

Registrati per una prova gratuita di 30 giorni su: sophos.it/endpoint

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

© Copyright 2025. 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 un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

2025-07-16 BR-IT (NP)

SOPHOS