Brochure

Sophos Extended Detection and Response

Proteggiti Dagli Active Adversary Con Funzionalità Complete Di EDR E XDR

Bloccare tempestivamente gli attacchi è essenziale. Sophos XDR offre potenti strumenti e dati accurati di intelligence sulle minacce, con i quali puoi rilevare, svolgere indagini e rispondere adeguatamente alle attività sospette individuate nel tuo sistema informatico.

Una Soluzione Impostata Sulle Basi Della Protezione Più Efficace

Grazie al blocco automatico di un maggior numero di minacce, anche i team IT più oberati di lavoro avranno meno incidenti su cui dover indagare. Sophos abbina l'Extended Detection and Response alla migliore protezione endpoint attualmente disponibile, bloccando le minacce prima che richiedano un intervento manuale e alleggerendo il carico di lavoro per la tua organizzazione.

Endpoint Detection And Response (EDR) Integrata

Sophos XDR include strumenti di EDR completi, caratterizzati da potenti opzioni di ricerca personalizzabili e 90 giorni di storico dei dati raccolti da endpoint e server, nonché accesso remoto sicuro ai dispositivi. Puoi così indagare su un maggior numero di problemi, installare e disinstallare software, terminare processi e molto di più, tutto senza dove essere presente fisicamente.

Estendi La Visibilità Oltre Gli Endpoint

Più vedi, più velocemente puoi agire. Sia che vengano generati dai prodotti Sophos o da quelli di altri vendor, gli eventi vengono incorporati, filtrati, messi in correlazione e ordinati in base alla priorità. Questo permette di estendere la visibilità su tutte le principali superfici di attacco e consente di rilevare e bloccare gli active adversary con maggiore tempestività.

Soluzioni A 360 Gradi, Predisposte Per Sophos XDR

Le tecnologie Sophos si integrano in maniera fluida nella piattaforma XDR per garantire i migliori risultati di sicurezza possibili. Le soluzioni con integrazione nativa includono Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email e Sophos Cloud.

Compatibilità Con Gli Strumenti E Le Tecnologie In Cui Hai Già Investito

Sfrutta i dati di telemetria di un'ampia selezione di strumenti di sicurezza non Sophos per incrementare il ritorno sull'investimento nei prodotti che hai già acquistato, potenziando e velocizzando allo stesso tempo le tue attività di SecOps. Le integrazioni includono tecnologie di gestione delle identità, rete, firewall, e-mail, cloud, produttività e protezione endpoint.

Caratteristiche Principali

- Visibilità sulle attività sospette in tutte le principali superfici di attacco
- Una piattaforma XDR unificata con una vasta gamma di soluzioni Sophos integrate
- Possibilità di sfruttare gli strumenti e le tecnologie in cui hai già investito, grazie all'ampia selezione di integrazioni con prodotti non Sophos
- Indagini e risposta tempestiva alle minacce, con rilevamenti ordinati in base alla priorità e flussi di lavoro ottimizzati da tecnologie di intelligenza artificiale
- Include protezione e funzionalità EDR leader di settore

Accelerazione Delle Attività Di Rilevamento, Risposta E Indagine

Sophos XDR include strumenti e funzionalità progettati per incrementare l'efficienza degli analisti di sicurezza e dei team informatici. Le indagini guidate dall'intelligenza artificiale consentono di comprendere rapidamente l'impatto e la causa di un incidente, riducendo al minimo i tempi di risposta.

Rilevamenti con priorità stabilite dall'IA su tutte le principali superfici di attacco

Identifica subito le attività sospette che richiedono attenzione immediata. Sophos XDR assegna automaticamente priorità ai rilevamenti in base al livello di rischio, fornendone il contesto completo.

Mapping del Framework MITRE ATT&CK

Rilevamenti e casi vengono automaticamente mappati alle Tattiche MITRE ATT&CK, per permetterti di identificare facilmente eventuali lacune di sicurezza nei tuoi sistemi di difesa e stabilire un ordine di priorità per i miglioramenti necessari.

Threat hunting e indagini rapide sulle minacce

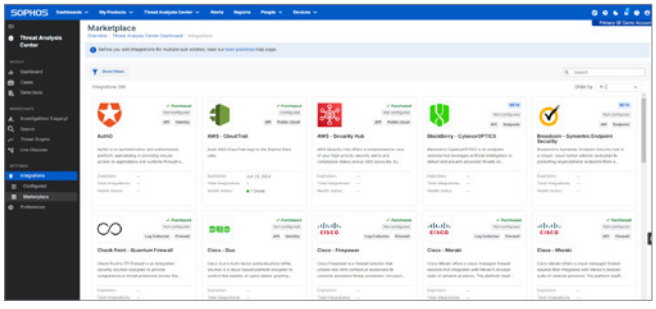
I potenti strumenti di ricerca con modelli di query preimpostati ti aiutano a trovare più velocemente i dati di cui hai bisogno, senza che tu debba conoscere SQL come le tue tasche.

Risposta automatizzata e accelerata

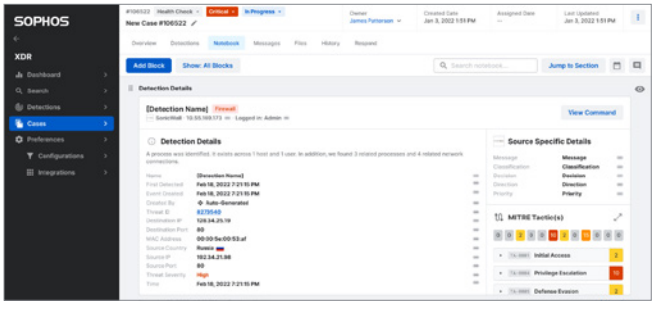
Azioni automatizzate e accelerate come l'interruzione dei processi, il ripristino dei file crittografati dal ransomware e la segregazione della rete isolano rapidamente le minacce e ti aiutano a risparmiare tempo prezioso.

Gestione collaborativa dei casi

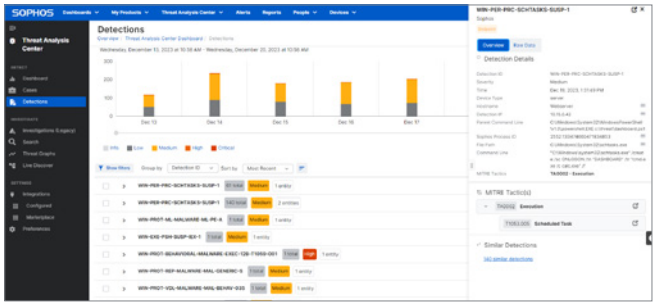
La creazione automatica dei casi consente di svolgere analisi in maniera tempestiva, con strumenti completi di gestione dei casi che facilitano la collaborazione con gli altri membri del team.



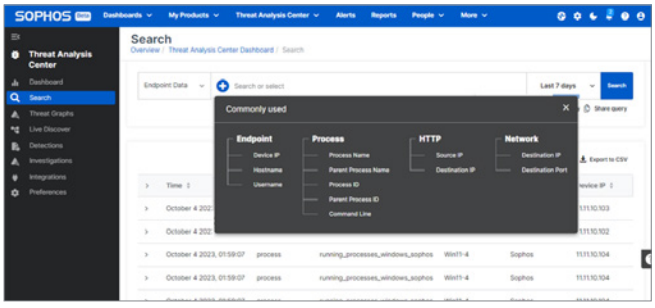
Compatibile con le soluzioni Sophos e con quelle di terze parti



Potenti strumenti di gestione dei casi e collaborazione



Rilevamenti con priorità stabilite dall'IA su tutte le principali superfici di attacco



Funzionalità di ricerca efficaci e semplici, anche per chi non conosce SQL

Integrazioni Incluse In Sophos XDR

I dati di sicurezza provenienti dalle origini indicate di seguito possono essere integrati con la piattaforma Sophos XDR senza alcun costo aggiuntivo. Le origini dei dati di telemetria aiutano a estendere la visibilità sull'intero ambiente, a generare nuovi rilevamenti e a migliorare l'attendibilità dei sistemi attuali di rilevamento delle minacce. Permettono inoltre di ottimizzare il threat hunting e di usufruire di opzioni di risposta aggiuntive.

Ep Sophos Endpoint

Blocco delle minacce avanzate e rilevamento dei comportamenti dannosi su tutti gli endpoint

Prodotto incluso nel prezzo Sophos XDR

WP Workload Protection

Protezione e rilevamento avanzato delle minacce per server e container Windows e Linux

Prodotto incluso nel prezzo Sophos XDR

Mob Sophos Mobile

Protezione dei dati e dei dispositivi iOS e Android contro le nuove minacce che colpiscono i sistemi mobili

Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo

Fw Sophos Firewall

Monitoraggio e filtro del traffico di rete in entrata, per bloccare le minacce avanzate prima che abbiano l'opportunità di infliggere danni

Prodotto venduto separatamente, è richiesta la subscription Xstream Protection, integrata senza alcun costo aggiuntivo

Em Sophos Email

Protezione antimalware per la tua casella di posta, con opzioni avanzate di intelligenza artificiale in grado di bloccare gli attacchi mirati di imitazione e phishing

Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo

Cld Sophos Cloud

Blocco delle violazioni nel cloud e visibilità su tutti i servizi cloud critici, inclusi AWS, Azure e GCP

Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo

ZT Sophos ZTNA

Sostituisci le VPN di accesso remoto con un accesso con meno privilegi possibili, per connettere in maniera sicura i tuoi utenti alle applicazioni nella tua rete

Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo

Protezione endpoint di terze parti

Compatibilità con:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ compatibilità con altre soluzioni, con l'agent Sophos "XDR Sensor"

Strumenti di protezione Microsoft

- Defender for Endpoint
- Defender per Office 365
- Defender for Cloud Apps
- Defender per identità
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

90 giorni di conservazione dei dati

Conserva i dati raccolti dai prodotti Sophos e da quelli di terze parti (non Sophos) nel Sophos Data Lake

Possibilità di estensione a 1 anno come add-on facoltativo

Microsoft Office 365 Management Activity

Fornisce informazioni sulle azioni e sugli eventi relativi a utenti, amministratori, sistema e criteri, secondo i dati acquisiti tramite l'Office 365 Management Activity API

Google Workspace

Acquisisce la telemetria di sicurezza dall'API di Google Workspace Alert Center

Integrazioni Add-On

I dati di sicurezza provenienti dalle origini indicate di seguito possono essere integrati con la piattaforma Sophos XDR acquistando gli Integration Pack. Le origini dei dati di telemetria aiutano a estendere la visibilità sull'intero ambiente, a generare nuovi rilevamenti e a migliorare l'attendibilità dei sistemi attuali di rilevamento delle minacce. Permettono inoltre di ottimizzare il threat hunting e di usufruire di opzioni di risposta aggiuntive.

Sophos NDR

Monitoraggio ininterrotto delle attività all'interno della rete, per rilevare interazioni sospette tra i dispositivi, che altrimenti passerebbero inosservate

Compatibile con qualsiasi rete, attraverso il mirroring delle porte SPAN

Firewall

Compatibilità con:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- WatchGuard

Rete

Compatibilità con:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Identità

Compatibilità con:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Integrazione Microsoft inclusa senza alcun costo extra

E-mail

Compatibilità con:

- Mimecast
- Proofpoint

Integrazioni Microsoft 365 e Google Workspace incluse senza alcun costo extra

Cloud

Compatibilità con:

- Orca Security

Integrazioni con AWS, Azure e GCP incluse con il prodotto Sophos Cloud Optix, venduto separatamente.

Backup e ripristino

Compatibilità con:

- Acronis
- Veeam

Conservazione dei dati di 1 anno

Conserva i dati raccolti dai prodotti Sophos e da quelli di terze parti (non Sophos) nel Sophos Data Lake

Una Soluzione Basata Sulla Migliore Protezione Endpoint In Assoluto

Svolgi indagini mirate, bloccando sul nascere un maggior numero di tentativi di violazione. La maggior parte dei prodotti XDR disponibili sul mercato costringe gli analisti a perdere tempo prezioso indagando su incidenti che il sistema di sicurezza avrebbe dovuto bloccare. Sophos abbina l'XDR alla migliore protezione endpoint attualmente disponibile, bloccando le minacce prima che richiedano un intervento manuale e alleggerendo il tuo carico di lavoro.

Le subscription Sophos XDR includono Sophos Intercept X Endpoint, che offre funzionalità antiransomware e antiexploit avanzate, nonché protezione antimalware e difese sensibili al contesto che si basano su tecnologie di intelligenza artificiale. Questa potente combinazione aiuta ad adattare in maniera dinamica i livelli di protezione applicati.

Scopri di più alla pagina: sophos.it/endpoint

Rilevamento E Risposta Come Servizio Completamente Gestito

Puoi scegliere se svolgere il rilevamento e le indagini sulle minacce in autonomia con Sophos XDR, oppure affidarti a un servizio completamente gestito che opera 24/7 per alleggerire il carico di lavoro del tuo team interno, che potrà così dedicarsi ad altre attività. Con Sophos Managed Detection and Response (MDR), il nostro team di analisti ed esperti di threat hunting può offrirti un Security Operations Center subito a tua disposizione per garantirti capacità di incident response a 360 gradi.

Scopri di più alla pagina: sophos.it/mdr

Cosa Includono Le Subscription Sophos XDR

	Sophos XDR
Rilevamenti in ordine di priorità e indagini guidate, con tecnologie di intelligenza artificiale	✓
Gestione dei casi, collaborazione e azioni di risposta	✓
Strumenti di ricerca semplici e potenti, per svolgere threat hunting e indagini	✓
Soluzioni Sophos Endpoint e Workload Protection (Intercept X Advanced)	✓
Strumenti di Endpoint Detection and Response (EDR)	✓
Conservazione dei dati nel cloud	90 giorni (può essere estesa fino a 1 anno)
Disponibilità sul dispositivo di dati completi su endpoint e server per l'EDR	✓
Integrazioni con le soluzioni Sophos: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud	✓
Sophos Network Detection and Response (NDR)	Add-on facoltativo
Integrazioni con soluzioni di protezione endpoint non Sophos	✓
Integrazioni con soluzioni Microsoft	✓
Integrazioni con soluzioni di produttività Google Workspace	✓
Integrazioni con soluzioni non Sophos per firewall, rete, e-mail, cloud, gestione dell'identità, e backup e ripristino	Add-on facoltativi

Scopri Perché I Clienti Scelgono Sophos XDR

Sophos è leader indiscusso nel mercato del Managed Detection and Response e i riconoscimenti ufficiali degli esperti di settore lo dimostrano.

Gartner

Sophos nominata tra i Leader nel Gartner® Magic Quadrant™ per il 2023, categoria Endpoint Protection Platforms (EPP, piattaforme di protezione endpoint), per 14 report consecutivi

Sophos nominata Customers' Choice 2024 di Gartner® Peer Insights™ per le Piattaforme di Protezione Endpoint e i Firewall di Rete

Leader

Sophos nominata tra i Leader nelle categorie Endpoint Protection, EDR, XDR, Firewall e MDR nei Summer 2024 G2 Grid® Reports

OMDIA

Sophos è il vendor con le valutazioni più alte, nonché unico leader nel report Omdia Universe for Comprehensive XDR del 2023

MITRE ENGENUITY | ATT&CK® Evaluations

Ottimo performer nelle valutazioni MITRE Engenuity ATT&CK per i Servizi gestiti

SE Labs

Sophos continua a ottenere le massime valutazioni nei test indipendenti, confermandosi come leader di settore

Effettua subito una prova gratuita

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

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

© Copyright 2024. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con N° 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.

2024-07-18 DS-IT (PS)

SOPHOS