

Sophos Managed Detection and Response



Threat Detection e Response 24/7

Sophos MDR è un servizio completamente gestito, disponibile 24/7, a cura di esperti che rilevano e rispondono agli attacchi informatici che colpiscono computer, server, reti, workload del cloud, account di posta elettronica e altro.

Servizi Di Prevenzione Di Attacchi Ransomware E Dei Tentativi Di Violazione

L'esigenza di avere una tipo di cybersecurity attiva a ogni ora del giorno e della notte è diventata essenziale. Tuttavia, la complessità dei moderni ambienti operativi e la rapida evoluzione delle minacce informatiche costituiscono un ostacolo sempre più insormontabile per la maggior parte delle organizzazioni, che fanno fatica a gestire autonomamente le attività di rilevamento e risposta.

Con Sophos MDR, il nostro team di esperti blocca gli attacchi più avanzati, coordinati da menti umane. Entriamo in azione per neutralizzare le minacce prima che possano compromettere i tuoi dati di natura sensibile o interferire in altro modo con le tue attività lavorative. Sophos MDR è personalizzabile con diversi livelli di servizio, e può essere utilizzato con le tecnologie Sophos oppure con quelle di altri prodotti di cybersecurity già presenti nei sistemi.

Cybersecurity as a Service

Grazie a capacità di Extended Detection and Response (XDR) che garantiscono protezione completa dei dati, indipendentemente da dove si trovano, Sophos MDR è in grado di:

- **Rilevare più minacce informatiche rispetto a quelle individuate dall'uso dei soli strumenti di sicurezza**

I nostri strumenti bloccano automaticamente il 99,98% delle minacce e questo permette ai nostri analisti di focalizzarsi sull'individuazione proattiva degli hacker più sofisticati, che possono essere intercettati e bloccati solo da personale con competenze tecniche molto elevate.

- **Intraprendere azioni per conto tuo, per impedire alle minacce di interferire con la tua attività commerciale**

I nostri analisti intercettano i problemi, conducono indagini e rispondono alle minacce entro pochi minuti, sia che tu desideri un servizio completo di risposta agli incidenti, o che abbia semplicemente bisogno di un valido aiuto per prendere decisioni informate.

- **Identificare la causa originaria delle minacce, per prevenire incidenti futuri**

Intraprendiamo azioni proattivamente, fornendo raccomandazioni su come ridurre il livello di rischio per la tua organizzazione. Dover affrontare meno incidenti significa avere meno interferenze con il lavoro dei tuoi team IT e di sicurezza, nonché con le attività dei tuoi dipendenti e clienti.

Compatibilità Con Gli Strumenti Di Cybersecurity Che Già Usi

Puoi scegliere di affidarti alle nostre soluzioni di sicurezza pluripremiate, oppure di adoperarne altre, già presenti nei tuoi sistemi: i nostri analisti possono utilizzare varie tecnologie di cybersecurity per rilevare le minacce e avviare una risposta appropriata.

Sophos MDR è compatibile con le opzioni di telemetria di vendor quali Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace e molti altri. I dati di telemetria vengono automaticamente unificati, correlati e presentati in ordine di priorità, grazie alle analisi approfondite del [Sophos Adaptive Cybersecurity Ecosystem \(ACE\)](#) e dell'unità organizzativa di intelligence sulle minacce [Sophos X-Ops](#).

Funzionalità principali

- Blocco del ransomware e di altri attacchi coordinati da menti umane, a cura di un team di esperti di risposta alle minacce che agiscono 24/7
- Ottimizzazione del ritorno sull'investimento nelle tue attuali tecnologie di cybersecurity
- L'incident response può essere gestita completamente da Sophos MDR o in collaborazione con il tuo team interno; è anche possibile ricevere solamente notifiche dettagliate della presenza di minacce e consulenza in merito
- Maggiore idoneità alle coperture cyberassicurative, grazie alle opzioni di monitoraggio ed Endpoint Detection and Response (EDR) disponibili 24/7
- Possibilità di liberare il personale IT e di sicurezza interno, che può quindi focalizzarsi sullo sviluppo commerciale dell'azienda

Un Servizio Di Managed Detection and Response (MDR) Che Va Incontro Alle Tue Esigenze

Sophos MDR è personalizzabile con vari livelli di servizio e ha una scelta di opzioni di risposta agli incidenti. Affida l'intera strategia di incident response al team operativo di Sophos MDR, che può agire collaborando con te per gestire le minacce informatiche. A seconda delle tue esigenze, Sophos MDR può anche essere utilizzato solo per l'invio di notifiche al tuo team SecOps interno ogni volta che vengono individuati elementi pericolosi. I nostri esperti identificano rapidamente gli autori di un attacco, le loro modalità di azione, le tempistiche e gli elementi colpiti. Siamo in grado di rispondere alle minacce entro pochissimi minuti.

Caratteristiche principali

Monitoraggio e risposta alle minacce 24/7

Rileviamo e rispondiamo alle minacce prima che possano violare i dati o causare l'interruzione delle tue attività. Grazie al supporto di sei Security Operations Center (SOC) internazionali, Sophos MDR garantisce monitoraggio e sicurezza a ogni ora del giorno e della notte.

Compatibilità con strumenti di sicurezza non Sophos

Sophos MDR è in grado di integrare i dati di telemetria di tecnologie di terze parti per endpoint, firewall, gestione delle identità, e-mail e altro, all'interno del [Sophos ACE](#).

Incident Response a 360 gradi

Quando identifichiamo una minaccia attiva, il team operativo di Sophos MDR può intraprendere un'ampia selezione di azioni di risposta per conto tuo, per interrompere l'attacco da remoto, isolare il problema e rimuovere completamente gli hacker.

Report settimanali e mensili

Sophos Central è la tua dashboard unificata per gestire gli avvisi in tempo reale, i report e il management delle attività. I report settimanali e mensili offrono analisi approfondite sulle indagini di sicurezza, sulle minacce informatiche e sul tuo profilo di protezione.

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE previene automaticamente le attività dannose e ci permette di cercare gli indizi meno evidenti della presenza di minacce sofisticate, che richiedono un intervento umano per essere rilevate, analizzate ed eliminate.

Threat hunting con la supervisione dei nostri esperti

Affidando l'individuazione proattiva delle minacce ai nostri analisti altamente qualificati, invece di utilizzare solo i prodotti di sicurezza, è possibile scoprire ed eliminare rapidamente un maggior numero di minacce. Il team operativo di Sophos MDR è anche in grado di sfruttare dati di telemetria di altri vendor per condurre attività di threat hunting e identificare i comportamenti dei cybercriminali che sono sfuggiti al rilevamento degli strumenti in uso.

Supporto diretto e dedicato

Il tuo team può usufruire di accesso diretto e dedicato al nostro Security Operations Center (SOC), che può essere coinvolto per verificare la presenza di potenziali minacce e incidenti attivi. Il team operativo di Sophos MDR è disponibile 24/7, grazie ai nostri tecnici situati in 26 località in tutto il mondo.

Contatto dedicato per la risposta agli incidenti

Ti assegneremo un contatto dedicato per la risposta agli incidenti, che collaborerà con il tuo team interno e i Partner esterni non appena viene identificato un incidente. Sarà a tua disposizione fino alla completa risoluzione dell'incidente.

Root Cause Analysis

Oltre a fornire consigli proattivi per migliorare il tuo profilo di sicurezza, svolgiamo analisi volte a identificare la causa originaria dell'attacco e tutti i problemi di fondo che hanno portato all'incidente. Offriamo una consulenza prescrittiva per risolvere le vulnerabilità di sicurezza, in modo che non possano essere sfruttate in futuro.

Sophos Account Health Check

Valutiamo e ottimizziamo continuamente impostazioni e configurazioni degli endpoint gestiti con Sophos XDR, per assicurarci che si eseguano ai massimi livelli di performance.

Threat Containment

Per le organizzazioni che non desiderano una gestione completa dell'incident response con Sophos MDR, il team operativo di Sophos MDR può eseguire attività di contenimento, bloccando così le minacce e impedendone la diffusione. Questa opzione contribuisce a ridurre il carico di lavoro dei responsabili delle SecOps dell'azienda, che possono così concentrarsi sull'esecuzione tempestiva di azioni correttive.

Briefing di intelligence sulle minacce – “Sophos MDR ThreatCast”

“Sophos MDR ThreatCast” è un briefing mensile a cura del team operativo di Sophos MDR ed è riservato esclusivamente ai clienti Sophos MDR. Offre analisi approfondite sui più recenti dati di intelligence sulle minacce e sulle best practice di sicurezza.

Breach Protection Warranty










Inclusa in tutte le licenze annuali (da 1 a 5 anni) e mensili di Sophos MDR Complete, la garanzia offre fino a 1 milione di \$ per coprire le spese correlate alla risposta agli incidenti. Non ci sono livelli di garanzia, termini contrattuali minimi o ulteriori requisiti di acquisto.

Livelli di servizio Sophos

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
Monitoraggio e risposta 24/7 alle minacce, a cura di un team di esperti	✓	✓	✓
Compatibilità con strumenti di sicurezza non Sophos	✓	✓	✓
Report settimanali e mensili	✓	✓	✓
Briefing di intelligence sulle minacce: "Sophos MDR ThreatCast"	✓	✓	✓
Sophos Account Health Check		✓	✓
Threat hunting con supervisione dei nostri esperti		✓	✓
Contenimento delle minacce: interruzione degli attacchi e prevenzione della diffusione <small>Utilizza la versione completa dell'agente Sophos XDR (protezione, rilevamento e risposta) oppure Sophos XDR Sensor (rilevamento e risposta)</small>		✓	✓
Supporto diretto e dedicato durante gli incidenti attivi		✓	✓
Incident Response a 360 gradi: le minacce vengono eliminate completamente <small>Richiede la versione completa dell'agente XDR (protezione, rilevamento e risposta)</small>			✓
Root Cause Analysis			✓
Contatto dedicato per la risposta agli incidenti			✓
Breach Protection Warranty <small>Fino a 1 milione di \$ di copertura totale per le spese correlate alla risposta agli incidenti</small>			✓








Integrazioni incluse in Sophos MDR

I dati di sicurezza provenienti dalle seguenti origini possono essere integrati e utilizzati dal team operativo di Sophos MDR, senza costi aggiuntivi. 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.

 <p>Sophos XDR</p> <p>L'unica piattaforma XDR che unisce le integrazioni native di endpoint, server, firewall, cloud, e-mail, dispositivi mobili e Microsoft</p> <p><small>Integrazione inclusa nel costo di Sophos MDR e Sophos MDR Complete</small></p>	 <p>Sophos Firewall</p> <p>Monitoraggio e filtro del traffico di rete in entrata, per bloccare le minacce avanzate prima che abbiano l'opportunità di infliggere danni</p> <p><small>Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo</small></p>	 <p>Microsoft Graph Security</p> <ul style="list-style-type: none"> • Microsoft Defender for Endpoint • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Endpoint • Identity Protection (Azure AD) • Microsoft Azure Sentinel • Office 365 Security and Compliance Center • Azure Information Protection
 <p>Sophos Endpoint</p> <p>Blocco delle minacce avanzate e rilevamento dei comportamenti dannosi, inclusi quelli di cybercriminali che imitano utenti legittimi</p> <p><small>Integrazione inclusa nel costo di Sophos MDR e Sophos MDR Complete</small></p>	 <p>Sophos Email</p> <p>Protezione antimalware per la tua casella di posta, grazie a opzioni avanzate di intelligenza artificiale, in grado di bloccare gli attacchi mirati di imitazione e phishing</p> <p><small>Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo</small></p>	 <p>Office 365 Management Activity</p> <p>Fornisce informazioni sulle azioni e sugli eventi relativi a utenti, amministratori, sistema e criteri, secondo i dati ottenuti dai log attività di Office 365 e Azure Active Directory</p>
 <p>Sophos Cloud</p> <p>Blocco delle violazioni nel cloud e visibilità su tutti i servizi cloud critici, inclusi AWS, Azure e Google Cloud Platform</p> <p><small>Prodotto venduto separatamente, integrato senza alcun costo aggiuntivo</small></p>	 <p>90 giorni di conservazione dei dati</p> <p>Conserva nel Sophos Data Lake i dati raccolti da tutti i prodotti Sophos e da quelli di terze parti (non Sophos)</p>	 <p>Protezione endpoint di terze parti</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • Microsoft • CrowdStrike • SentinelOne • Trend Micro • Trellix • BlackBerry (Cylance) • Symantec (Broadcom) • Malwarebytes

Integrazioni add-on

I dati di sicurezza provenienti dalle seguenti origini di terze parti possono essere integrati e utilizzati gratuitamente dal team operativo di Sophos MDR. 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.

 <p>Sophos Network Detection and Response</p> <p>Monitoraggio ininterrotto delle attività all'interno della rete, per rilevare interazioni sospette tra i dispositivi, che altrimenti passerebbero inosservate</p> <p>Compatibile con qualsiasi rete, attraverso il mirroring delle porte SPAN</p>	 <p>Firewall</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • Palo Alto Networks • Fortinet • Check Point • Cisco • SonicWall 	 <p>Identità</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • Okta • Duo • ManageEngine
 <p>Cloud pubblico</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • AWS Security Hub • AWS CloudTrail • Orca Security • Google Cloud Platform Security 	 <p>Email</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • Proofpoint • Mimecast 	 <p>Rete</p> <p>Compatibilità con...</p> <ul style="list-style-type: none"> • Darktrace • Tinkst Canary • Skyhigh Security
 <p>Pacchetto di conservazione dei dati di 1 anno</p>		

Attivazione guidata di Sophos MDR

Con un costo aggiuntivo, è possibile usufruire dell'attivazione guidata di Sophos MDR per ricevere assistenza remota in fase di attivazione. Il servizio offre supporto diretto, con una distribuzione semplice ed efficiente, che garantisce l'implementazione delle best practice e offre formazione per ottimizzare il valore del tuo investimento nel servizio MDR. Ti verrà assegnato un contatto dedicato all'interno dei Sophos Professional Services, che ti assisterà durante i tuoi primi 90 giorni, per assicurarti il massimo successo per l'implementazione. L'Attivazione guidata di Sophos MDR include:

Giorno 1 – Implementazione

- Inizio del progetto
- Configurazione di Sophos Central e rassegna delle funzionalità
- Strutturazione e test del processo di implementazione
- Configurazione delle integrazioni MDR
- Configurazione del/dei Sophos NDR Sensor
- Distribuzione nell'intera azienda

Giorno 30 – Formazione su XDR

- Impara a pensare e agire come un SOC
- Scopri come individuare proattivamente gli indicatori di compromissione
- Approfondisci l'uso della nostra piattaforma XDR per le attività di amministrazione
- Impara a compilare query per indagini future

Giorno 90 – Valutazione del Profilo di Sicurezza

- Analisi dei criteri attuali, con raccomandazioni basate sulle best practice
- Discussione delle funzionalità al momento non utilizzate, che potrebbero incrementare il livello di protezione
- Valutazione della sicurezza, secondo il framework NIST
- Report con un riepilogo delle raccomandazioni, in base alla nostra valutazione

Per scoprire di più, visita

sophos.it/mdr

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

© Copyright 2022. Sophos Ltd. Tutti i diritti riservati.
Registrazione 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.

22-11-29 DS-IT [DD]

SOPHOS