SOPHOS

Sophos MDR aumenta le difese di Microsoft Defender

Riduci il rischio informatico, aumenta l'efficienza e l'impatto dei tuoi investimenti in ambito di cybersecurity e migliora la tua posizione assicurativa aumentando le potenzialità di Microsoft Defender con Sophos MDR: il servizio MDR più affidabile in assoluto, che offre rilevamento e risposta alle minacce 24/7, con monitoraggio a cura di esperti.

Whitepaper Sophos. Luglio 2023

Introduzione

La protezione endpoint è uno dei livelli di sicurezza più importanti, ma non è in grado di bloccare tutte le minacce. Oggi gli avversari informatici sono molto abili e sfruttano sempre più frequentemente tattiche, tecniche e procedure (TTP) difficili da smascherare, con le quali cercano di eludere il rilevamento e il blocco delle tecnologie di protezione. Alcuni esempi di TTP sono gli exploit di vulnerabilità a cui non sono state applicate patch, l'uso di credenziali rubate e l'utilizzo improprio di strumenti informatici legittimi.

Per bloccare gli attacchi ransomware avanzati e per prevenire le violazioni, è essenziale incrementare le potenzialità di Microsoft Defender con un servizio di Detection and Response, guidato da esperti e operativo 24/7. Tuttavia, le enormi quantità di avvisi generati dalle tecnologie di sicurezza Microsoft, unite alla complessità dell'ambiente delle minacce, hanno trasformato le operazioni di cybersecurity in attività estremamente difficoltose da gestire, che prosciugano le risorse interne della maggior parte delle aziende.

Questo ha indotto un numero sempre maggiore di organizzazioni a cercare di aumentare le potenzialità di Microsoft Defender con l'aiuto di Sophos: il fornitore di servizi MDR (Managed Detection and Response) che gode di maggiore fiducia tra i clienti a livello globale, come dimostrano le altissime valutazioni ricevute. Gli analisti Sophos monitorano, assegnano priorità e rispondono agli avvisi di sicurezza Microsoft a ogni ora del giorno e della notte, intraprendendo azioni correttive per bloccare le minacce confermate come tali. Inoltre, sfruttano risorse Sophos quali i rilevamenti, i dati di intelligence sulle minacce e le attività di threat hunting con supervisione umana per bloccare le minacce che sfuggono a Microsoft Defender.

Sophos MDR è un servizio progettato per venire incontro alle tue esigenze, in quanto utilizza le soluzioni informatiche che già usi e collabora con le tue risorse interne. Sia che tu desideri estendere le potenzialità del tuo team con l'aiuto di consulenti esperti, o voglia ampliare la difese informatiche per sentirti al sicuro anche "fuori orario ufficio", oppure cerchi un modo per affidare l'intera gestione delle tue attività di rilevamento e risposta a un servizio esterno, Sophos MDR può aiutarti a ottenere risultati di cybersecurity superiori.

Aumenta Le Potenzialità Di Microsoft Defender Con Sophos MDR

✓ Riduzione del rischio informatico

- Blocca gli attacchi ransomware avanzati e le violazioni, incluse le minacce diffuse tramite attacchi coordinati da menti umane, in grado di eludere il rilevamento di Microsoft Defender

✓ Aumenta l'efficienza e l'impatto dei tuoi investimenti in ambito di cybersecurity

- Libera più risorse IT da dedicare alla realizzazione di progetti di maggiore importanza strategica
- Riduci la probabilità di dover affrontare costi di riparazione dei danni estremamente elevati
- Ottieni un migliore ritorno sugli investimenti, grazie all'integrazione con le soluzioni di sicurezza che già usi

✓ Migliora la tua assicurabilità

- Ottieni accesso a opzioni assicurative più vantaggiose, che riconoscono e premiano il tuo impegno a ridurre il rischio informatico

Gli Active Adversary Non Usano Metodi Indiretti, Ma Accedono Con Credenziali Legittime

La realtà è che le tecnologie, da sole, non sono in grado di prevenire tutti gli attacchi informatici. E questo vale anche per Microsoft Defender. Gli active adversary sono cybercriminali che adattano le proprie tattiche, tecniche e procedure (TTP) alla situazione in cui si trovano, grazie a operazioni hands-on-keyboard eseguite in tempo reale per rispondere alle attività di difesa dei team di IT security e delle tecnologie di protezione. È inoltre una strategia che permette di eludere il rilevamento.

Questi attacchi, che spesso causano incidenti ransomware e violazioni dei dati devastanti, sono tra i più difficili da bloccare. Sono diventati molto diffusi, come dimostra il fatto che il 23% delle organizzazioni di piccole e medie dimensioni dichiara di avere subito un attacco sferrato da un active adversary nell'ultimo anno. A conferma del potenziale devastante di questi attacchi, il 30% degli IT/Cybersecurity Manager afferma che gli active adversary sono una delle loro principali preoccupazioni di cybersecurity per il 2023[1].

Bloccare gli active adversary con le tecnologie di sicurezza standard non basta per sventarne i piani. Questi avversari informatici sono abili e ostinati e sfruttano un gran numero di approcci innovativi per raggiungere i loro obiettivi, con strategie che includono:

- L'exploit delle vulnerabilità di sicurezza per infiltrarsi nei sistemi delle organizzazioni, per poi spostarsi lateralmente una volta all'interno della rete. I criminali sfruttano credenziali rubate, vulnerabilità per le quali non sono state applicate patch, errori di configurazione negli strumenti di sicurezza e altro
- L'uso improprio di strumenti informatici legittimi che vengono normalmente utilizzati dai team di IT security per evitare di attivare il rilevamento, inclusi PowerShell, PsExec e RDP
- La modifica della propria strategia di attacco in tempo reale per rispondere ai controlli di sicurezza. Gli active adversary continuano a cambiare tecnica fino a quando non raggiungono gli obiettivi che si sono prefissati.

Esempio della strategia di attacco di un active adversary

Emulando gli utenti autorizzati e approfittando delle debolezze nei sistemi di difesa delle organizzazioni, gli avversari informatici possono evitare di farsi notare dalle tecnologie di rilevamento automatico, che fanno fatica a distinguere tra utenti legittimi e malintenzionati.

A inasprire il problema per i team di sicurezza, c'è anche il fatto che i moderni active adversary possono contare su enormi risorse finanziarie; pertanto, continuano a introdurre innovazioni e a evolvere il proprio business model. La recente crescita esponenziale del modello Cybercrime-as-a-Service, che include Ransomware-as-a-Service e Phishing-as-a-Service, ha reso l'intero sistema molto più accessibile per gli aspiranti cybercriminali. Inoltre, ha semplificato l'esecuzione di attacchi su vasta scala e ha contribuito a incrementarne la qualità.

Una conseguenza di questi sviluppi nel panorama delle minacce è l'impennata del tasso di cifratura non autorizzata dei dati dovuta al ransomware, che ha raggiunto un picco assoluto: i cybercriminali riescono infatti a cifrare i dati in più di tre quarti (76%) degli attacchi[2].

La Realtà Del Ransomware

- Il 66% delle organizzazioni è stato colpito dal ransomware negli ultimi 12 mesi
- Nel 76% degli attacchi ransomware sono stati cifrati i dati
- Il 30% degli attacchi in cui sono state cifrate informazioni è stato caratterizzato anche dal furto di dati
- Causa N°1 all'origine degli attacchi: vulnerabilità soggette a exploit (36%)
- Causa N°2 all'origine degli attacchi: credenziali compromesse (29%)

1 Il Panorama Della Cybersecurity 2023: L'Impatto Commerciale Degli Avversari Informatici, Sophos.

2 La Vera Storia Del Ransomware 2023, Sophos.

Rilevamento E Risposta Alle Minacce 24/7: Un Must Per La Cybersecurity Moderna

La buona notizia è che bloccare gli attacchi avanzati e coordinati da menti umane è possibile: per farlo, occorre la sinergia tra tecnologie all'avanguardia ed esperti dotati di elevate competenze tecniche. Ogni volta che un avversario informatico svolge un'azione, genera un segnale. Grazie alla combinazione tra elevate competenze umane e modelli di machine learning basati sull'intelligenza artificiale, più ottimi strumenti di rilevamento e risposta estesi (XDR), gli analisti di sicurezza possono sfruttare i segnali generati dalle tecnologie informatiche e di cybersecurity per rilevare, svolgere indagini e neutralizzare gli attacchi coordinati da menti umane, prevenendo così il ransomware e le violazioni dei dati.

Sebbene il rilevamento e la risposta alle minacce 24/7 siano ormai parte integrante di qualsiasi stack di sicurezza, molte organizzazioni fanno fatica a gestirli in maniera efficace, il che le espone a un elevato rischio di attacco. I due ostacoli più comuni che impediscono di raggiungere un livello ottimale di cybersecurity sono l'assenza di personale con adeguate competenze tecniche e la mancanza di risorse.

Problema N°1: Assenza Di Personale Dotato Di Adeguate Competenze Tecniche

Il rilevamento, l'indagine e la risposta alle minacce sono attività che richiedono personale altamente specializzato, con una profonda conoscenza delle tecniche di attacco e delle strategie di indagine, oltre a una certa dimestichezza con gli strumenti di difesa. È molto raro avere a disposizione un team interno che soddisfi questo complesso (e costoso) set di caratteristiche. Il 93% delle organizzazioni ritiene infatti che lo svolgimento di attività di sicurezza essenziali è estremamente problematico:

- Il 71% sostiene che l'identificazione dei segnali pertinenti tra tutte le informazioni non rilevanti (ovvero capire quali segnali/avvisi devono essere analizzati) è un compito arduo
- Il 71% fa fatica a raccogliere una quantità sufficiente di dati per stabilire se un segnale indica un elemento pericoloso o innocuo
- Il 75% ritiene difficoltosa l'identificazione della root cause dell'incidente (ovvero il modo in cui l'avversario informatico è riuscito a infiltrarsi nell'organizzazione)

La gravità del problema diventa evidente quando si osservano i dati che i team di sicurezza ricevono dai loro strumenti di cybersecurity. La tabella riportata di seguito contiene un elenco non esaustivo di eventi di Microsoft Defender, con la categoria di evento.

Capire gli avvisi è solo una parte del processo di rilevamento e risposta alle minacce: i team di sicurezza devono applicare informazioni contestuali e dati di intelligence sulle minacce per poter capire bene la minaccia e per identificare il modo migliore per procedere.

TITOLO DELL'EVENTO	TIPO DI EVENTO
URL sospetto cliccato	Accesso iniziale
File o connessioni di rete dannose, associate al processo 3CXDesktopApp.exe	Malware
Creazione di un nuovo account utente	Persistenza
Log eventi TS_BL_Suspicious cancellato o configurazione che usa Wevtutil	Elusione dei tentativi di difesa
Privilege escalation dei processi	Privilege escalation
Tentativo di disattivare la protezione dell'Antivirus Microsoft Defender	Elusione dei tentativi di difesa
È stato rilevato un file o una connessione di rete correlata all'attore di minacce Storm-0867	Accesso con credenziali
Motori TS_BL_Script che si connettono a Internet	Comando e controllo
Potenziale attività dannosa coordinata da menti umane	Attività sospetta
Download del payload TS_BL_Malicious tramite file binari di Office	Esecuzione
Rilevato gruppo di attività della minaccia emergente DEV-0867	Accesso con credenziali
Rilevato gruppo di attività della minaccia emergente Citrine Sleet	Malware

Esempio di rilevamenti per la creazione di un caso da Microsoft Defender

Problema N°2: Mancanza Di Risorse

Rilevare, indagare e rispondere alle minacce sono attività che richiedono molto tempo. A dimostrazione di questo, il tempo medio necessario per rilevare, indagare e rispondere a un avviso varia dalle 9 ore, per le organizzazioni con 100-3.000 dipendenti, alle 15 ore se il numero di dipendenti è compreso tra 3.001 e 5.000.

La gestione degli avvisi di sicurezza richiede una quantità enorme di ore del personale IT. Allo stesso tempo, la natura urgente di questa attività può impedire ai team di focalizzarsi su questioni di importanza più strategica. Inoltre, visto che gli avversari informatici sferrano attacchi a qualsiasi ora del giorno e della notte, il rilevamento e la risposta alle minacce devono essere eseguiti 24/7, per incrementarne l'efficacia. Molte organizzazioni, se non tutte, fanno fatica a procurarsi le risorse necessarie.

Soluzione: Utilizzare Managed Detection and Response (MDR) Come Soluzione Complementare Per Le Difese Esistenti

Il 52% degli IT/Cybersecurity Manager sostiene che le cyberminacce sono ora troppo avanzate per essere affrontate dal team tecnico della propria organizzazione senza alcun aiuto esterno. Il risultato è una maggiore tendenza a rivolgersi a fornitori specializzati in servizi di Managed Detection and Response (MDR) come Sophos, per potenziare le capacità del proprio team interno.

Definire L'MDR

Managed Detection and Response (MDR) è un servizio operativo 24/7 e completamente gestito, a cura di esperti specializzati nel rilevamento e nella risposta agli attacchi informatici, che previene incidenti che sarebbero impossibili da fermare con l'uso delle sole tecnologie.

Extended Detection and Response (XDR) è una piattaforma che unisce i dati di protezione provenienti da origini diverse, per automatizzare e accelerare il rilevamento, le indagini e la risposta alle minacce in modi che sarebbero impensabili per le singole soluzioni autonome.

Gli analisti di Sophos MDR sfruttano la piattaforma Sophos XDR per individuare proattivamente le minacce, svolgere indagini e neutralizzare gli attacchi per conto tuo. Si servono dei segnali raccolti dall'intero stack informatico, incluse le soluzioni per firewall, e-mail, cloud e protezione dei dispositivi mobili, per accelerare il rilevamento e la risposta alle minacce.

Aumenta Le Potenzialità Di Microsoft Defender Con Sophos MDR

Sophos MDR offre un servizio di rilevamento e risposta alle minacce dall'efficacia comprovata e operativo 24/7 per gli ambienti Microsoft Defender. Gli analisti Sophos monitorano, assegnano priorità e rispondono agli avvisi di sicurezza Microsoft a ogni ora del giorno e della notte, intraprendendo azioni correttive per bloccare le minacce confermate come tali. Inoltre, sfruttano risorse Sophos quali i rilevamenti, i dati di intelligence sulle minacce e le attività di threat hunting con supervisione umana per bloccare le minacce coordinate da menti umane che sfuggono a Microsoft Defender.

Più vediamo, più velocemente agiamo. Sophos MDR sfrutta le origini degli eventi aggiuntive di Microsoft Security, incluse nelle licenze E3 ed E5, oltre a segnali raccolti da firewall e prodotti di terze parti per cloud, e-mail, gestione delle identità e Network Detection and Response (NDR), per accelerare il rilevamento e la risposta alle minacce.

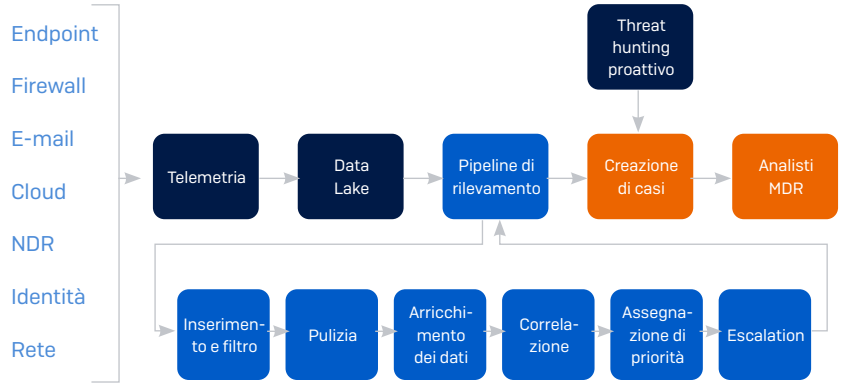
Gli utenti di Microsoft Defender possono usufruire dell'accesso telefonico immediato agli esperti Sophos, disponibili 24/7, nonché di una reportistica dettagliata sulle attività delle minacce nella piattaforma Sophos Central.

Sophos MDR Per Microsoft Defender È Compatibile Con Le Origini Degli Eventi Di Microsoft Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centro sicurezza e conformità di MS O365
- Microsoft Azure Sentinel
- Office 365 Management Activity (log di controllo unificato)

Flusso Degli Eventi Di Sicurezza Di Sophos MDR

Il nostro Flusso degli eventi di sicurezza è un elemento chiave del servizio Sophos MDR. I dati di telemetria raccolti dall'intero ambiente di sicurezza, incluso Microsoft Defender, vengono inseriti nel Sophos Data Lake, per poi essere elaborati nella nostra pipeline di rilevamento: qui l'enorme quantità di avvisi provenienti da prodotti Microsoft e di terze parti vengono convertiti in approfondimenti pratici da consultare e classificati in base alla priorità, che ci permettono di svolgere indagini e rispondere in maniera tempestiva ed efficace.



Il Flusso degli eventi di sicurezza di Sophos MDR

Inserimento e filtro: inserimento dei dati di telemetria e filtro delle informazioni non rilevanti

Pulizia: trasformazione dei dati in uno schema normalizzato, con mappatura a MITRE ATT&CK®

Arricchimento dei dati: aggiunta di dati di intelligence sulle minacce di terze parti e di informazioni sul contesto aziendale

Correlazione: raggruppamento degli avvisi in base alle entità, alla classificazione MITRE ATT&CK e all'orario

Assegnazione di priorità: assegnazione di punteggi e raggruppamento degli eventi, per semplificarne la classificazione in ordine di priorità

Escalation: applicazione di ragionamenti logici per eseguire l'escalation dei gruppi di eventi, trasformandoli in casi pronti per le indagini

Protezione 24/7, Grazie A Sette Security Operations Center (SOC) Globali

Le minacce vengono sottoposte ad analisi e risolte da un team di esperti di rilevamento e risposta alle minacce situati in sette Security Operations Center (SOC) globali: America del Nord (Indiana, Utah, Hawaii), Europa (Regno Unito/Irlanda, Germania) e Asia-Pacifico (India, Australia). Con più di 500 tecnici specializzati (inclusi esperti in materia di malware, automazione, intelligenza artificiale e correzione degli incidenti) che vegliano instancabilmente sull'intero ambiente delle minacce, Sophos MDR offre competenze vaste e approfondite che sono praticamente impossibili da riprodurre nelle strutture interne delle singole organizzazioni.

Tempi Di Rilevamento E Risposta Imbattibili A Livello Globale

La combinazione esclusiva di tecnologie, interazione umana ed elevate competenze in materia di minacce permettono a Sophos MDR di offrire tempi di incident response di soli 38 minuti. Queste tempistiche, a loro volta, generano risultati di cybersecurity superiori:

- Tempo medio di rilevamento: 1 minuto
- Tempo medio di indagine: 25 minuti
- Tempo medio di risposta: 12 minuti

Chi Utilizza Sophos MDR?

Il servizio Sophos MDR viene utilizzato da migliaia di organizzazioni di qualsiasi dimensione e settore: da aziende con pochi dipendenti e risorse IT limitate, fino a grandi imprese con un SOC interno. I tre più comuni modelli di risposta per Sophos MDR sono:

- Sophos MDR gestisce ogni aspetto della risposta alle minacce per conto del cliente
- Sophos MDR interagisce con il team interno del cliente, con una gestione collaborativa della risposta alle minacce
- Sophos MDR espande il team interno del cliente e offre il supporto necessario, inviando comunicazioni relative agli incidenti che richiedono attenzione e fornendo analisi approfondite sulle minacce, più consulenza sulle azioni di correzione necessarie

Caso Di Minaccia: Utilizzo Di Microsoft Defender Per Rilevare Un Caso Di Comando E Controllo

SETTORE
Servizi professionali

SEDE CENTRALE
Stati Uniti

DIPENDENTI
750

LIVELLO DI SERVIZIO
Sophos MDR per Microsoft Defender

ORIGINI DI TELEMETRIA INTEGRATE IN SOPHOS MDR

- ✓ Endpoint
- X Identità
- ✓ Firewall
- X Cloud
- X E-mail
- ✓ Rete

Che Cos'È Un Attacco Di Comando E Controllo?

Gli attacchi di tipo Comando e Controllo (detti anche C&C o C2) sono composti da varie tecniche, che gli avversari informatici sfruttano per comunicare con i sistemi e per inviare comandi ai sistemi che controllano all'interno della rete di una vittima.

I canali di Comando e Controllo stabiliti tra l'ambiente della vittima e l'infrastruttura del cybercriminale possono essere creati in molti modi, incluso tramite e-mail di phishing, social engineering, malware, vulnerabilità nei plugin del browser e altro. Spesso gli avversari informatici utilizzano risorse pubblicamente disponibili, emulando il traffico di rete atteso per eludere il rilevamento e non destare sospetti.

RILEVAMENTO

Microsoft Defender genera un avviso relativo al rilevamento di una comunicazione verso un indirizzo IP dannoso.

L'avviso di Microsoft viene automaticamente correlato agli eventi registrati nel Data Lake di Sophos XDR, per stabilire se l'attacco è stato bloccato dal firewall del cliente e se sono coinvolti anche altri endpoint.

INDAGINE

Gli analisti del team Sophos MDR confermano che la connessione dannosa associata all'avviso di Microsoft Defender è stata bloccata e che la minaccia immediata è stata isolata.

Viene utilizzata SophosLabs Intelix per identificare la famiglia dell'attacco, i relativi indicatori di compromissione (IoC) e gli IP e domini noti utilizzati dall'avversario informatico.

L'avviso originario di Microsoft viene arricchito con dati di intelligence su questa minaccia, in modo che possa essere utilizzato per la Root Cause Analysis.

RISPOSTA

Il dispositivo compromesso viene isolato e l'attacco viene contenuto.

Sophos MDR conferma che l'accesso iniziale è avvenuto a causa di un'e-mail di phishing. Viene svolta un'indagine per identificare come era strutturata l'e-mail di phishing e per verificare che non siano stati compromessi altri account utente.

Sophos fornisce consigli pratici per ridurre la probabilità di subire ulteriori attacchi di phishing in futuro.

I vantaggi per i clienti

Sia che tu stia cercando un modo per espandere e offrire il supporto necessario al tuo team IT interno, o che preferisca usufruire di tutti i vantaggi di un servizio operativo 24/7 gestito da esperti, senza il peso di dover strutturare il tuo SOC interno: Sophos MDR ti può aiutare. Le organizzazioni che sfruttano al meglio le potenzialità di Microsoft Defender grazie all'integrazione con Sophos MDR ottengono risultati superiori in termini di sicurezza informatica, inclusi un minore rischio, maggiore efficienza e impatto degli investimenti, nonché una migliore posizione assicurativa.

Blocca Le Minacce Avanzate Con Microsoft + Sophos MDR

Monitoraggio E Risposta 24/7, A Cura Di Un Team Di Esperti
Gli analisti del team Sophos MDR monitorano, assegnano priorità e rispondono agli avvisi di Microsoft Defender a ogni ora del giorno e della notte, intraprendendo azioni correttive per bloccare le minacce confermate come tali

Rilevamento e Blocco Delle Minacce Che Riescono A Eludere Microsoft Defender
Rilevamenti proprietari di Sophos, più dati di intelligence sulle minacce, threat hunting con supervisione umana e livelli aggiuntivi di protezione

Maggiore Visibilità E Contestualizzazione Degli Avvisi Di Microsoft Defender
Integrazione delle origini degli eventi aggiuntive di Microsoft Security, incluse nelle licenze E3 ed E5

Accesso Immediato Ai Nostri Esperti Di Sicurezza
Gli analisti di Sophos MDR sono raggiungibili telefonicamente 24/7; inoltre, una reportistica dettagliata sulle attività delle minacce è disponibile nella piattaforma Sophos Central

Riduzione del rischio informatico

Uno dei principali vantaggi dell'aumentare le potenzialità di Microsoft Defender con Sophos MDR è l'elevato livello di protezione dal ransomware e da altre minacce informatiche avanzate.

L'esperienza estesa e approfondita maturata dagli analisti Sophos, unita alla loro grande dimestichezza nell'uso di strumenti di telemetria e threat hunting è praticamente impossibile da riprodurre internamente. Di conseguenza, gli esperti Sophos sono in grado di avviare un'azione di risposta con estrema rapidità e precisione in tutte le fasi dell'attacco, dall'identificazione dei segnali pertinenti, alle indagini sui potenziali incidenti per neutralizzare le attività pericolose.

Sophos MDR protegge più organizzazioni di qualsiasi altro vendor, una caratteristica che ci permette di offrire un'"immunità della comunità" che non ha rivali. I dati di intelligence ottenuti quando proteggiamo un cliente vengono automaticamente applicati a tutti gli altri profili analoghi: questo ci permette di prevenire proattivamente gli attacchi simili nella nostra comunità.

★★★★★

"I penetration tester sono rimasti sorpresi di non trovare una via di accesso: è questo che ci ha convinti che potevamo riporre completa fiducia nel servizio Sophos."
University of South Queensland, Australia

★★★★★

"Con Sophos MDR, abbiamo abbreviato drasticamente i nostri tempi di risposta."
Tata BlueScope Steel, India

★★★★★

"Riceviamo notifiche in tempo reale per qualsiasi tipo di minaccia."
Bardiani Valvole, Italy

Aumenta L'Efficienza E L'Impatto Dei Tuoi Investimenti In Ambito Di Cybersecurity

Sophos MDR permette di incrementare l'efficienza e l'impatto del tuo team e dei tuoi strumenti di sicurezza.

Le attività di rilevamento e risposta alle minacce richiedono un'enorme quantità di risorse IT. Sophos MDR ti solleva da questo peso, liberando preziosissime risorse IT da dedicare alla realizzazione di progetti di maggiore importanza strategica. Allo stesso tempo, l'accesso telefonico 24/7 agli esperti Sophos e la reportistica dettagliata sulle attività delle minacce nella piattaforma Sophos Central accelerano le tempistiche per i tuoi team interni, che possono così rispondere agli avvisi in maniera più rapida e accurata.

Sophos MDR sfrutta i dati di telemetria raccolti dai tuoi strumenti di sicurezza Microsoft e di terze parti per accelerare il processo di rilevamento e risposta alle minacce. Parallelamente, eleva le tue difese e aumenta il tuo ritorno sull'investimento nelle soluzioni che già usi.

In più, considerando che il costo medio necessario per rimediare ai danni causati da un attacco ransomware ammonta a 1,85 milioni di $ e che l'84% delle vittime del ransomware sostiene che l'attacco ha provocato perdite commerciali/di fatturato[2], investire in un servizio quale Sophos MDR riduce il costo totale di proprietà della cybersecurity.

★★★★★

"Da quando abbiamo implementato Sophos, siamo riusciti a liberare ore di lavoro preziose per i nostri team, che a loro volta si sono così potuti focalizzare su iniziative volte a incrementare il tasso di soddisfazione dei nostri studenti."

London South Bank University, Regno Unito

Migliora La Tua Assicurabilità

Sophos MDR permette alle organizzazioni di ottenere molti dei controlli informatici che sono fondamentali per migliorare l'assicurabilità e ottenere condizioni più vantaggiose nella propria polizza. Tra queste vi sono: rilevamento e risposta alle minacce 24/7, pianificazione dell'incident response informatica, compilazione di log e monitoraggio, e molto di più.

I nostri clienti sostengono di avere incrementato la propria idoneità a stipulare un'assicurazione, nonché di avere ottenuto una polizza che riconosce e premia il loro impegno a ridurre il rischio informatico.

★★★★★

"La nostra decisione di entrare in partnership con Sophos per l'XDR e l'MDR è stata un fattore cruciale nell'ottenere premi cyberassicurativi più bassi, rispetto a quelli praticamente doppi che altrimenti saremmo stati costretti ad accettare. È stata pertanto una scelta vincente, che comporta un vantaggio tangibile … Mi è anche arrivato un messaggio del CFO che ringrazia il nostro team per i risultati ottenuti. E MDR è stato un fattore importante durante l'intero processo."

Bob Pellerin, CISO, The Fresh Market, U.S.

2 La vera storia del ransomware 2023, Sophos.

Il servizio MDR più affidabile al mondo

Sophos è il fornitore di servizi MDR numero 1 al mondo, in quanto protegge più organizzazioni di qualsiasi altro vendor contro ransomware, violazioni dei sistemi e altre minacce che le tecnologie, da sole, non sarebbero in grado di bloccare.

Sophos MDR difende varie migliaia di organizzazioni in tutto il mondo e in tutti i settori. Proprio per questo motivo possiamo vantare competenze di un'ampiezza e una profondità imbattibili in tema di minacce che colpiscono le varie industrie. Questa telemetria estremamente ricca ci permette di raggiungere l'"immunità della comunità", poiché ci consente di applicare tutto ciò che impariamo da un'organizzazione a qualsiasi altro cliente con un profilo simile. Il risultato è un sistema di difesa più elevato per tutti.

Naturalmente, il nostro obiettivo principale sono i risultati di cybersecurity che possiamo garantire ai nostri clienti. Sophos è la soluzione MDR con le valutazioni più alte e con il maggior numero di recensioni in Gartner® Peer Insights™, con un punteggio pari a 4,8/5 ottenuto in 300 recensioni (dati aggiornati al 14 giugno 2023) e con il 97% dei clienti che afferma che consiglierebbe Sophos.

Inoltre, Sophos anche è stata nominata Leader nei Report G2 Grid® per Managed Detection and Response ed è stata riconosciuta come Leader per l'MDR da G2 nei segmenti Overall (generale), Midmarket (medie dimensioni), ed Enterprise (grandi imprese).

La Scelta Più Affidabile

Più di 17.000 organizzazioni utilizzano Sophos MDR (2° trimestre del 2023)

Le Valutazioni Più Alte

Valutazione indipendente dei clienti pari a 4,8/5

Il Maggior Numero Di Recensioni

300 recensioni su Gartner Peer Insights negli ultimi 12 mesi

Per scoprire di più su Sophos MDR e su come aiuta gli utenti di Microsoft Defender a ridurre il rischio informatico, ad aumentare l'efficienza e l'impatto degli investimenti in ambito di cybersecurity e a migliorare la loro posizione assicurativa, visita www.sophos.it/mdr

Esplora Sophos Endpoint Protection

La protezione Sophos Intercept X Endpoint lavora per te e con te, adattando la tua strategia di difesa quando rispondi a un attacco.

È ricca di potentissime opzioni di protezione a livelli multipli, che offrono sicurezza superiore contro ransomware e minacce avanzate in tutte le fasi della catena di attacco. Queste funzionalità includono il ripristino basato sul comportamento dei file cifrati dal ransomware, più 60 attenuazioni degli exploit attivate come opzione predefinita e che non richiedono alcuna ottimizzazione per essere utilizzate.

La nostra Protezione adattiva contro gli attacchi è una funzionalità innovativa che risponde in maniera dinamica agli attacchi coordinati da menti umane, implementando automaticamente difese aggiuntive per sventare i tentativi degli avversari informatici e regalare tempo prezioso al team di sicurezza.

Gli utenti del servizio Sophos MDR che usano Microsoft Defender possono passare alla protezione Sophos Endpoint in qualsiasi momento: questo ti garantisce massima flessibilità, permettendoti allo stesso tempo di preparare la tua infrastruttura di cybersecurity ad affrontare le sfide del futuro.

✓ Leader nelle valutazioni di Gartner per 13 report consecutivi
Dal 2008, Sophos si aggiudica ogni anno il titolo di Leader nel report Gartner Magic Quadrant per le piattaforme di protezione endpoint (EPP)

✓ Punteggio più alto su Gartner Peer Insights
Valutazione indipendente dei clienti pari a 4,8/5

✓ Leader nelle valutazioni di G2 per le categorie Enterprise, Midmarket e SMB
Risultato basato esclusivamente sulle recensioni dei clienti

✓ Punteggio di protezione pari al 100% – SE Labs
Valutazione AAA sia per le soluzioni Enterprise, sia per la protezione delle piccole imprese

Per scoprire di più e per attivare una prova gratuita, visita:
www.sophos.it/endpoint

Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31 dicembre 2022

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.

2023-06-27 (WP-NP)

SOPHOS