SOPHOS

Guida Alla Cybersecurity Per L'industria Manifatturiera

Identifica e rispondi più rapidamente alle minacce avanzate a qualsiasi ora del giorno e della notte, con l'aiuto del team di analisti Sophos specializzati in threat hunting e con il più completo database di intelligence sulle minacce disponibile a livello mondiale.

L'industria 4.0 e le "smart factory" stanno trasformando il volto dell'industria manifatturiera. I sistemi di controllo industriali (ICS) come lo SCADA, i dispositivi IoT industriali (IIoT), la robotica e le analisi avanzate stanno rivoluzionando il modo in cui operano le fabbriche moderne. Tuttavia, a causa dell'estesa trasformazione digitale, unita alla convergenza tra IT e OT e alla limitatissima tolleranza dei tempi di inattività operativa che caratterizza questo settore, la superficie di attacco nell'industria manifatturiera continua a espandersi, aumentando i rischi a cui sono esposte le aziende, tra i quali ci sono: exploit delle vulnerabilità, fuga di dati, tentativi di sabotaggio della produzione e così via.

Sophos difende le organizzazioni dell'industria manifatturiera da un'ampia selezione di attacchi informatici, inclusi quelli coordinati da menti umane che le tecnologie, da sole, non sono in grado di prevenire. Da Managed Detection and Response (MDR) a protezione endpoint e della rete, Sophos permette alle aziende manifatturiere di potenziare le difese e regala tempo prezioso ai loro team informatici, che possono così dedicarsi alle questioni strategiche dell'attività commerciale.

Whitepaper Sophos. Aprile 2023

Le Sfide Di Cybersecurity Nell'Industria Manifatturiera

Le sfide di cybersecurity per il settore dell'industria manifatturiera continuano ad aumentare: la rapida digitalizzazione e l'assenza di standard di sicurezza sufficientemente sofisticati hanno colto di sorpresa i responsabili IT e OT, che si trovano impreparati a rispondere alle nuove minacce informatiche. Come se non bastasse, le cyberminacce in questo settore continuano a crescere sia in termini di volume che di complessità.

Da un sondaggio commissionato nel 2022 da Sophos a cui hanno partecipato 419 professionisti dell'IT che lavorano nel settore dell'industria manifatturiera e della produzione, è emerso che il 55% delle organizzazioni è stato colpito dal ransomware nel 2021: un aumento pari al 52% in più rispetto al volume degli attacchi ransomware dell'anno precedente.

Per le aziende manifatturiere, il costo medio necessario per rimediare ai danni causati da un attacco ransomware è stato 1,23 milioni di USD. Inoltre, una quantità notevole di intervistati (77%) sostiene che l'attacco ha avuto ripercussioni sullo svolgimento delle loro attività, mentre il 71% afferma che l'attacco ha causato perdite commerciali e di fatturato.

Non si tratta solo di ransomware. Complessivamente, l'ambiente IT nell'ambito dell'industria manifatturiera è diventato molto più difficile da gestire: nel corso dell'anno, il 61% delle organizzazioni ha notato un aumento nel volume degli attacchi, il 66% ha segnalato un incremento nella complessità degli attacchi e il 55% ha osservato un impatto superiore per tali attacchi.

55%
Percentuale di organizzazioni manifatturiere colpite dal ransomware nel 2021

$ 1,23 Mio
Costo medio per la riparazione dei danni di un attacco

>1 mese
Il 10% delle organizzazioni manifatturiere ha avuto bisogno di più di un mese per riprendersi da un attacco

77%
Percentuale di organizzazioni manifatturiere colpite dal ransomware che sostengono che l'attacco ha avuto ripercussioni sulla capacità di svolgere le proprie attività

66%
Percentuale di professionisti dell'IT nell'industria manifatturiera che hanno notato un aumento della complessità degli attacchi

59%
Percentuale di dati recuperati dalle organizzazioni manifatturiere dopo aver pagato il riscatto

57%
Percentuale di attacchi nell'industria manifatturiera nei quali sono stati cifrati i dati

7%
Percentuale di organizzazioni manifatturiere che hanno recuperato TUTTI i dati dopo aver pagato il riscatto

Fonte: sondaggio globale Sophos La Vera Storia Del Ransomware 2022

Dietro a queste statistiche si nascondono molti cambiamenti nel panorama delle minacce:

La Professionalizzazione Del Cybercrimine

Uno dei maggiori sviluppi dell'anno scorso sono state l'evoluzione e la professionalizzazione dell'economia delle cyberminacce. Le gang di criminali tendono sempre più frequentemente a specializzarsi in una parte specifica dell'attacco, ad esempio l'accesso iniziale, il ransomware, il malware infostealer o altro. Una volta diventati esperti, offrono la propria specializzazione in modalità "as-a-service" ad altri criminali. I modelli as-a-service diminuiscono le competenze necessarie per sferrare un attacco, aumentando così la quantità di minacce e cybercriminali.

Questi servizi specializzati offrono ai propri "clienti" risorse e consulenza sull'uso, potenziando l'efficacia dei loro attacchi. A dimostrazione di questo, a marzo 2022 un hacker associato alla gang di ransomware-as-a-service Conti ha pubblicato un archivio che conteneva una vera e propria miniera d'oro di documenti e istruzioni per gli "affiliati"; i documenti descrivevano in maniera dettagliata come sferrare un attacco ransomware.

Oltretutto, i criminali stanno adottando molti comportamenti tipici dei fornitori di servizi IT legittimi, inclusa la richiesta di "feedback sul servizio" alle vittime del ransomware, una volta pagato il riscatto e decifrati i file.

L'Evoluzione Delle Tattiche, Tecniche E Procedure Dei Cybercriminali

Spesso gli avversari informatici sfruttano le vulnerabilità nel profilo di sicurezza delle organizzazioni, nel tentativo di eludere il rilevamento delle soluzioni di sicurezza. Includono:

- **Exploit delle vulnerabilità prive di patch**: l'anno scorso, questo è stato il principale metodo di infiltrazione utilizzato dai criminali negli attacchi per cui è stato richiesto l'intervento degli esperti di incident response di Sophos. Questo exploit è stato infatti riscontrato nel 47% degli incidenti.
- **Exploit di strumenti informatici legittimi**: esistono numerosi strumenti regolarmente utilizzati dai professionisti dell'IT, come PowerShell e PsExec, che vengono sfruttati in modo improprio dagli avversari informatici per appropriarsi illecitamente di dati di accesso e credenziali. Spacciandosi per utenti legittimi, questi hacker cercano con l'inganno di ottenere l'accesso a un ambiente.

Le sfide di cybersecurity affrontate da questo settore non sono solo queste. Le organizzazioni manifatturiere si trovano alle prese anche con altri problemi, tra i quali: minacce interne (incidenti sia intenzionali che non), requisiti di conformità alle normative molto rigidi e rischi introdotti da vendor di terze parti.

Sicurezza Sophos Per Il Settore Dell'Industria Manifatturiera

Sophos offre soluzioni di cybersecurity all'avanguardia, che permettono alle organizzazioni manifatturiere di gestire e ridurre il rischio informatico. Il nostro Adaptive Cybersecurity Ecosystem include una gamma completa di servizi e prodotti leader di settore, in grado di elevare le difese dei nostri clienti, proteggendoli contro tutte le minacce, anche quelle più avanzate. Il sistema si basa su tecnologie esclusive di threat hunting e intelligenza artificiale, e può contare sulle competenze in ambito SecOps del team Sophos X-Ops.



Sophos garantisce risultati di sicurezza leader di mercato a più di **530.000 clienti** in tutto il mondo.



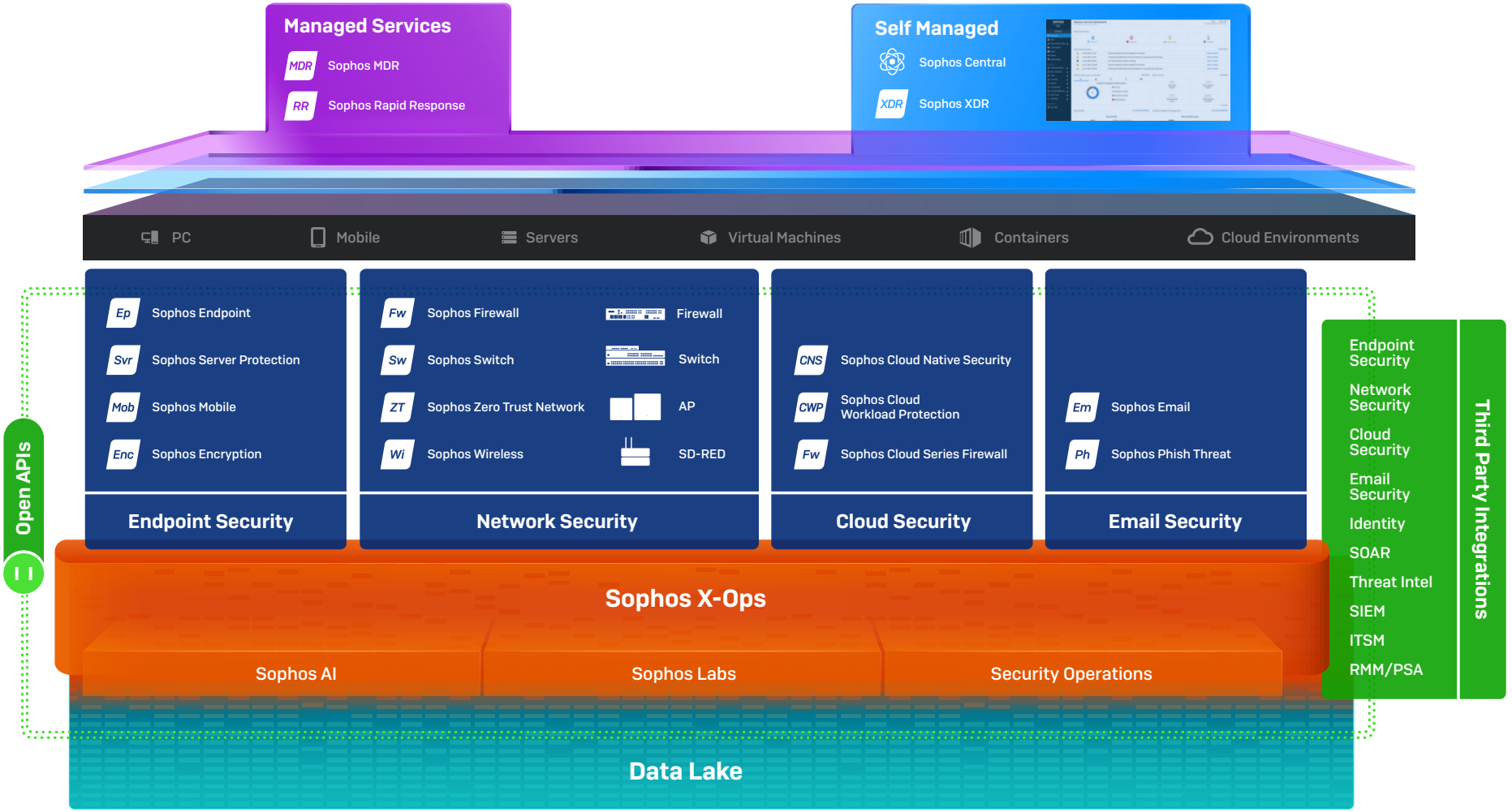
Nessun altro vendor è mai stato **nominato da Gartner leader** nella categoria endpoint security tante volte quanto Sophos.



Il servizio MDR, la soluzione Endpoint e il Firewall **con le valutazioni più alte** e **con il maggior numero di recensioni** su Gartner Peer Insights.

Secondo i dati disponibili al 1° agosto 2022,

Sophos Adaptive Cybersecurity Ecosystem



Casi di utilizzo

Sophos aiuta le organizzazioni manifatturiere a superare le più comuni sfide di cybersecurity che si trovano ad affrontare.

Blocco Degli Attacchi Avanzati E Coordinati Da Menti Umane, Ransomware Incluso

Sophos MDR è un servizio operativo 24/7 e completamente gestito, a cura di esperti specializzati nel rilevamento e nella risposta agli attacchi informatici; previene gli incidenti che sarebbero impossibili da fermare con l'uso delle sole tecnologie. Il nostro team di professionisti di cybersecurity blocca gli attacchi più avanzati e coordinati da menti umane, neutralizzando le minacce prima che possano interferire con le attività commerciali dei clienti o comprometterne i dati di natura sensibile.

"Con Sophos MDR abbiamo abbreviato drasticamente i nostri tempi di risposta."

Tata BlueScope Steel

"Sophos MDR è in grado di correggere i problemi o rimuovere le minacce rapidamente, segnalandoci la loro presenza. Questa capacità ci permette di dedicare un maggior numero di risorse ad attività più critiche."

Tomago Aluminium

"Sophos libera i team IT dal peso di dover gestire i problemi di cybersecurity, permettendogli di dedicarsi ad attività più proattive."

AG Barr

Con Sophos MDR, le minacce vengono rilevate e risolte dai nostri esperti (utilizzando la tecnologia che preferisci) in pochi minuti, sia che tu cerchi un servizio di incident response a 360 gradi o che abbia semplicemente bisogno di assistenza per prendere decisioni di sicurezza più informate.

Utilizziamo:

- Le pluripremiate soluzioni Sophos, inclusi i nostri prodotti per endpoint, firewall, cloud e protezione delle e-mail
- Prodotti di altri vendor quali Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace e molti altri
- Qualsiasi combinazione tra le nostre tecnologie e quelle di altri vendor

Sophos MDR difende la tua organizzazione dagli attacchi più avanzati che le tecnologie, da sole, non sono in grado di prevenire. Allo stesso tempo, ti permette di potenziare il ritorno sull'investimento nelle soluzioni che già usi. Siamo il fornitore di servizi MDR che gode del maggiore livello di fiducia a livello globale. Ci siamo guadagnati questa reputazione perché vantiamo competenze di un'ampiezza e una profondità imbattibili in tema di minacce che colpiscono l'industria manifatturiera. Sfruttando questa telemetria estremamente ricca, siamo in grado di raggiungere l'"immunità della comunità", poiché possiamo applicare tutto ciò che impariamo da un'organizzazione manifatturiera a qualsiasi altro cliente che opera nello stesso settore. Il risultato è un sistema di difesa più elevato per tutti.

LA SCELTA FIDATA	IL PUNTEGGIO PIÙ ALTO	LA MIGLIORE PROTEZIONE
N°1 tra tutti i provider	**4,8/5** Gartner Peer Insights	**38 min** Per rilevamento, indagine, risposta
Le organizzazioni preferiscono Sophos MDR a qualsiasi altro vendor	La soluzione MDR con le valutazioni più alte e con il maggior numero di recensioni (al 1° agosto 2022)	I nostri analisti sono 5 volte più rapidi dei più veloci team SOC interni

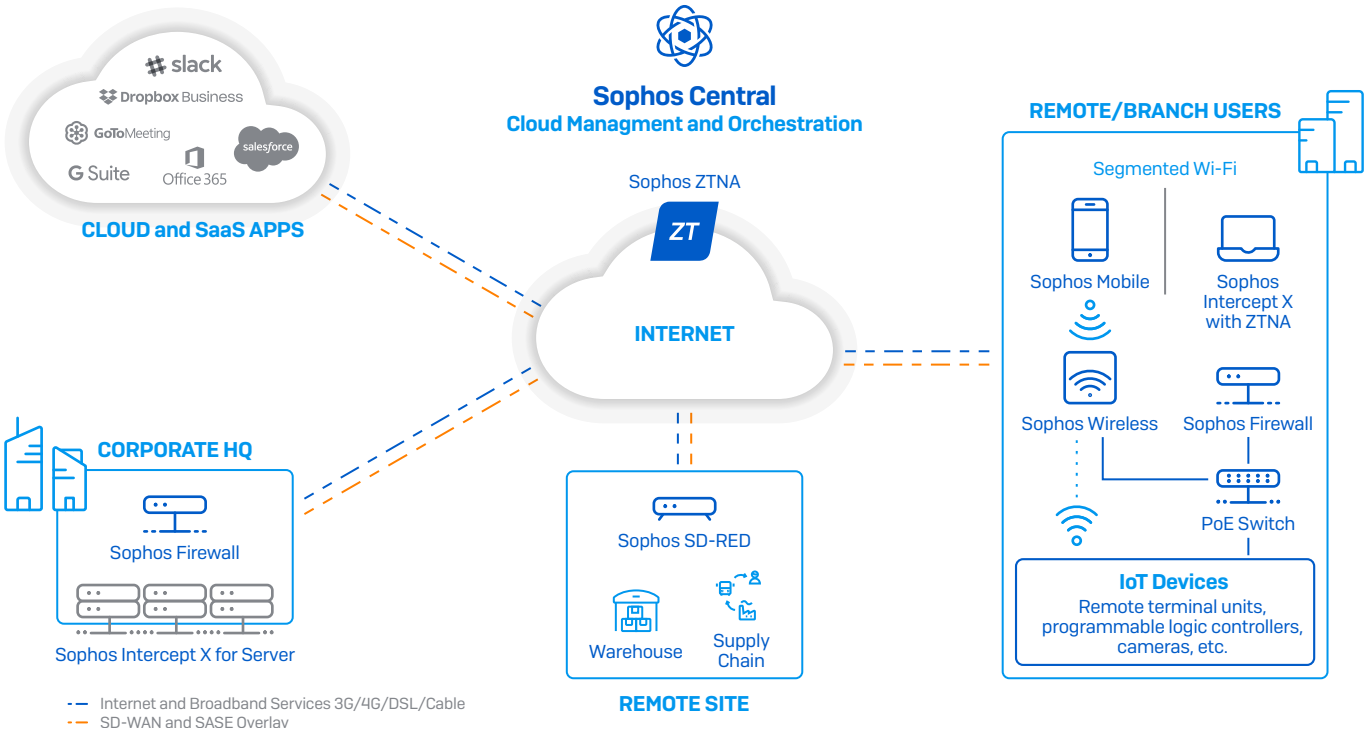
Secondo i dati disponibili a settembre 2022

Protezione Dell'Accesso Ai Sistemi Di Controllo Industriale E Ai Dati Critici

Per proteggere l'accesso alla propria infrastruttura critica e alle informazioni vitali, le aziende manifatturiere devono adottare un approccio zero-trust, che si basa sul principio "mai fidarsi di niente, meglio controllare tutto". Prima di garantire accesso ad applicazioni e dati, la soluzione Sophos Zero Trust Network Access convalida continuamente l'identità dell'utente, lo stato di integrità del dispositivo e la conformità alle policy.

Sophos ZTNA protegge dagli attacchi i tuoi sistemi RDP (Remote Desktop Protocol): uno strumento utilizzato molto frequentemente da dipendenti remoti e amministratori, ma anche uno dei vettori di attacco preferiti dai cybercriminali. ZTNA garantisce accesso sicuro solo a utenti e dispositivi autorizzati, e include nuove opzioni di autenticazione senza password con Microsoft Windows Hello for Business, per proteggere ulteriormente le credenziali più importanti da potenziali tentativi di violazione.

Con la linea di soluzioni di accesso sicuro Sophos, le organizzazioni manifatturiere possono abilitare la connessione con dispositivi remoti e filiali da qualsiasi luogo, implementare applicazioni cloud e SaaS essenziali e condividere dati in maniera sicura. Sfrutta tutti i vantaggi di Sophos ZTNA per garantire accesso sicuro alle tue applicazioni; utilizza i dispositivi Ethernet remoti Sophos SD-RED per estendere la tua rete in maniera sicura a sedi remote e filiali; installa Sophos Wireless Access Point per proteggere la rete wireless; e approfitta degli switch di accesso Sophos Switch per garantire accesso sicuro sulla LAN. L'intero sistema è gestito da Sophos Central: la nostra piattaforma di sicurezza unica e basata sul cloud.



Protezione Della Rete

Sophos Firewall offre una protezione estremamente efficace contro le minacce più recenti, velocizzando il traffico delle applicazioni SaaS, SD-WAN e cloud essenziali. Riconosciuto nel 2022 come Gartner Customers' Choice for Network Firewalls (Scelta dei clienti Gartner per i firewall di rete), Sophos Firewall offre una suite integrata di tecnologie di protezione in grado di contrastare le minacce moderne, con opzioni facili da configurare e da gestire.

La segmentazione della rete è una strategia molto efficace, che le organizzazioni manifatturiere possono adottare per ridurre l'esposizione ai rischi informatici e per riprendere più rapidamente le normali attività commerciali in seguito a una violazione. Ad esempio, la rete IT di un'organizzazione manifatturiera può essere segmentata dalla rete OT per prevenire movimenti e tentativi laterali di infezione. Sophos Firewall offre potenti opzioni di segmentazione flessibile attraverso aree e VLAN. In questo modo, avrai a disposizione più opzioni diverse per separare i livelli di attendibilità all'interno della rete; inoltre, potrai contare su un livello aggiuntivo di protezione contro i movimenti laterali tra le varie parti della rete stessa.

Puoi anche segregare il traffico a livello di switch con Sophos Switch, che consente di configurare le VLAN per segmentare il traffico interno, riducendo così la superficie di attacco in caso di violazione di sicurezza o infezione dei sistemi.

Protezione Contro Gli Attacchi Di Phishing

Le truffe di phishing, in particolare gli attacchi di spearphishing, sono uno dei modi preferiti dai cybercriminali per ottenere l'accesso ai tuoi sistemi e ai tuoi dati più importanti.

Una delle strategie migliori per bloccare gli attacchi di phishing è sensibilizzare i tuoi dipendenti, insegnandogli come riconoscere una truffa di phishing. Sophos Phish Threat offre un catalogo di più di 30 moduli di formazione sulla sicurezza, per educare e mettere alla prova i tuoi utenti finali. Le risorse includono simulazioni di attacco automatiche, ottimi corsi di formazione e sensibilizzazione sulla sicurezza e pratici dati di reportistica.

Autorizza le caselle di posta dei tuoi dipendenti a ricevere solo i messaggi provenienti da mittenti attendibili, con Sophos Email: questa soluzione esegue la scansione in tempo reale di tutti i messaggi in entrata, alla ricerca dei principali indicatori di phishing (ad es. lo spoofing di un brand e i tentativi di imitazione), grazie a tecniche di autenticazione SPF, DKIM e DMARC e all'analisi delle anomalie nell'intestazione. Queste opzioni aiutano a individuare e bloccare le e-mail di phishing prima ancora che riescano a raggiungere i tuoi utenti. Puoi prevenire ulteriormente la perdita dei dati creando policy DLP che includono regole multiple per gruppi e singoli utenti, garantendo la sicurezza dei dati di natura sensibile, grazie alla segnalazione della presenza di informazioni vitali e altri contenuti riservati nelle e-mail e negli allegati.

Nella maggior parte dei casi, gli attacchi di phishing colpiscono i punti di accesso alla rete, cercando di indurre i destinatari delle e-mail a cliccare su un link dannoso, che scarica malware sul dispositivo o che concede agli hacker accesso a dati di natura sensibile. Per incrementare le difese della tua rete contro gli attacchi di phishing, devi potenziare la tua endpoint security. Ottieni protezione completa per tutti i tuoi endpoint (Windows, Mac, Linux e virtual machine) con Sophos Intercept X Endpoint, la nostra soluzione EDR leader di mercato.

Per ottimizzare i tuoi sistemi di difesa, ti serve una protezione a livelli multipli: varie funzionalità di sicurezza estremamente sofisticate, ognuna delle quali svolge un ruolo importantissimo nella protezione contro gli attacchi più avanzati. Sophos Endpoint include diversi livelli di protezione, tra i quali:

- Protezione contro il furto di credenziali, per prevenire l'accesso non autorizzato ai sistemi.
- Protezione contro gli exploit, per bloccare le tecniche utilizzate dagli avversari informatici.
- Protezione antiransomware, che identifica e blocca i tentativi di cifratura non autorizzati.
- Blocco rimozione, che impedisce agli hacker di disattivare i sistemi di difesa per distribuire payload di malware.

Questa combinazione ottimale di tecnologie di protezione a più livelli ci permette di ottimizzare le difese dei nostri clienti. A conferma della qualità dei nostri sistemi di sicurezza (nonché della potenza della nostra protezione a livelli multipli), blocchiamo anticipatamente il 99,98% delle minacce (punteggio medio di AV-TEST) e recentemente abbiamo ottenuto le massime valutazioni nel report degli SE Labs sulla protezione endpoint.

Proteggi La Tua Proprietà Intellettuale (PI) Dai Tentativi Di Furto

Con il termine "proprietà intellettuale" (PI) viene definito qualsiasi tipo di informazione cruciale che aiuta le aziende manifatturiere a rimanere competitive sul mercato. Informazioni riservate quali i dati di progettazione di un prodotto, le formulazioni, i brevetti per i processi e altre forme esclusive di know-how appartenenti a un'organizzazione manifatturiera sono tutti bersagli molto allettanti per cybercriminali, competitor ed ex dipendenti: offrono infatti accesso immediato a informazioni critiche, senza la necessità di dover investire tempo e denaro in attività di ricerca e sviluppo. Per le aziende manifatturiere, il furto di proprietà intellettuale può significare un'enorme perdita finanziaria e a volte persino il rischio di chiusura permanente.

Proteggi la tua proprietà intellettuale educando i dipendenti a identificare le potenziali minacce e crea una cultura positivamente incentrata sulla sicurezza all'interno della tua organizzazione con Sophos Phish Threat, che offre un catalogo di simulazioni di attacco e corsi di formazione e sensibilizzazione sulla sicurezza informatica.

Ottieni pieno controllo sugli utenti che sono autorizzati ad accedere ai dati sulla tua rete, sfruttando i vantaggi di Sophos ZTNA. Puoi implementare controlli granulari per bloccare i movimenti laterali e assicurarti che solo il personale autorizzato sia in grado di accedere ai tuoi dati di natura sensibile.

Attenua le vulnerabilità note e previeni le più recenti minacce di cybersecurity (ad es. ransomware, attacchi indipendenti dai file, exploit e malware) su tutti i tuoi dispositivi endpoint, grazie alla protezione endpoint di Sophos Intercept X. Le funzionalità della nostra prevenzione della perdita dei dati (DLP) identificano i tuoi dati sensibili e impediscono la fuga di informazioni attraverso e-mail, caricamento di file e copie locali.

Previeni le violazioni dei dati con Sophos Email, che permette di creare policy DLP con regole multiple per gli utenti, al fine di garantire la protezione delle informazioni sensibili grazie al rilevamento di contenuti di natura riservata in tutte le e-mail e tutti gli allegati. Inoltre, cifra in maniera invisibile i tuoi dati sensibili, prevenendo così le violazioni.

Protezione Contro Gli Attacchi Interni

Sull'intera industria manifatturiera incombe una grave minaccia, ovvero il rischio che utenti interni con accesso autorizzato a dati vitali o a sistemi di controllo critici per l'attività manifatturiera possano utilizzare i loro privilegi in modo malevolo, oppure tradire la fiducia dell'organizzazione per cui lavorano. Il furto di segreti commerciali, il sabotaggio dei processi di produzione o il danneggiamento delle attrezzature tramite accesso remoto sono solo alcuni esempi dei rischi posti dal personale interno.

Ottieni informazioni approfondite sugli utenti e sulle applicazioni maggiormente a rischio, per garantire l'implementazione delle tue policy prima che venga messa a repentaglio la tua sicurezza, grazie ai dati di intelligence pronti per l'uso del Quoziente di minaccia dell'utente (UTQ) Sophos. Metti una marcia in più alla tua protezione con Sophos Firewall, che protegge i tuoi dati di natura sensibile dalla divulgazione accidentale o intenzionale. Garantisce pieno controllo su: policy per le varie categorie web, applicazioni, supporti rimovibili e dispositivi mobili sull'intera rete. Inoltre, offre opzioni di sensibilizzazione degli utenti per tutti gli ambiti del firewall, grazie a policy di accesso basate sui singoli utenti per lo shaping del traffico (QoS) e altre risorse di rete, indipendentemente da indirizzo IP, posizione, rete o dispositivo.

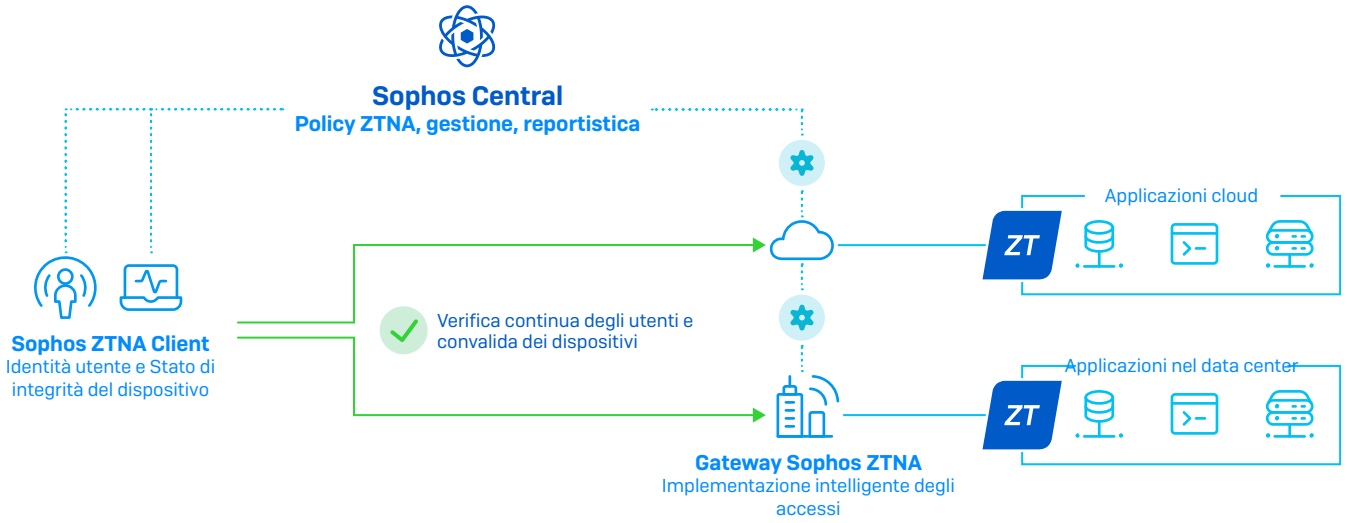
Riduzione Dei Rischi Alla Supply Chain

Le supply chain nel settore dell'industria manifatturiera sono estese e complesse. Una singola vulnerabilità in una qualsiasi delle reti di un fornitore può permettere a una minaccia di propagarsi rapidamente e infettare più fornitori e aziende.

Usa Sophos Intercept X per usufruire di capacità di prevenzione antiexploit, protezione contro i comportamenti dannosi e altre tecnologie all'avanguardia, che ti difendono dalle minacce che si infiltrano nei sistemi delle organizzazioni manifatturiere attraverso fornitori di terze parti. In più, le nostre potenti funzionalità XDR permettono di identificare automaticamente le attività sospette, di dare la giusta priorità agli indicatori di minacce e di cercare rapidamente potenziali minacce in tutti gli endpoint e i server.

Ottieni supporto 24/7 a cura di oltre 500 specialisti che lavorano a qualsiasi ora del giorno e della notte per individuare proattivamente, verificare e risolvere per conto tuo eventuali minacce e potenziali incidenti nella supply chain, con Sophos MDR.

Previeni gli attacchi alla supply chain che si basano sull'accesso dei fornitori ai tuoi sistemi, grazie ai controlli granulari degli accessi di Sophos ZTNA, che offre autenticazione per le richieste dei partner attendibili, ovunque si trovino fisicamente. Il livello esclusivo di integrazione tra Sophos Endpoint e Sophos ZTNA blocca automaticamente le connessioni alle risorse della rete da parte di host compromessi e impedisce i movimenti laterali delle minacce che cercano di fare breccia nella tua rete.



Protezione Dei Sistemi Non Aggiornati

Le aziende manifatturiere devono difendere dalle vulnerabilità note tutti i sistemi di controllo non aggiornati o privi di patch. Spesso questi dispositivi eseguono sistemi operativi o browser obsoleti, che sono impossibili da aggiornare perché non più supportati. Tuttavia, devono necessariamente restare connessi alla rete.

Sophos Firewall e Sophos SD-RED possono esserti di aiuto. Proteggi le connessioni di un dispositivo a rischio con un SD-RED, per reindirizzare l'intero traffico su un Sophos Firewall che potrà quindi effettuarne la scansione. Se la tua rete è semplice, saranno probabilmente necessarie alcune modifiche agli schemi di indirizzi IP e potenzialmente un cambiamento della topologia; i nostri tecnici specializzati possono discutere la tua situazione con te e indicarti come procedere.

Protezione Dei Dati Negli Ambienti Manifatturieri Multicloud

Le smart factory si basano sulla tecnologia cloud. L'adozione del cloud consente alle moderne organizzazioni manifatturiere di raccogliere dati in tempo reale sugli impianti installati nelle officine e di convertire grandi volumi di dati in intelligence commerciale: queste opzioni permettono di individuare eventuali pratiche inefficienti e di mettere in evidenza modi alternativi per gestire l'attività in maniera più sostenibile. Purtroppo il cloud è un bersaglio molto interessante anche per i cybercriminali che desiderano sfruttare le pratiche di cybersecurity meno consolidate di questi ambienti, visto che offrono ai malintenzionati un vantaggio rispetto ai tradizionali sistemi on-premise.

Sophos Cloud Native Security offre protezione multicloud completa per ambienti, workload e identità. Difende la tua infrastruttura cloud e i tuoi dati con una sicurezza dei workload flessibile per host e container ed è compatibile con Windows e Linux. Le difese a livelli multipli proteggono i sistemi dal ransomware e da altri attacchi avanzati, grazie a tecnologie native del cloud, ad es. il rilevamento in fase di runtime di comportamenti anomali ed exploit, che individuano minacce come le uscite dai container, gli exploit del kernel e i tentativi di privilege escalation. Inoltre, semplificano il monitoraggio e il controllo della spesa per il cloud. Puoi identificare rapidamente eventuali utilizzi impropri del tuo account, rimuovendo gli avversari informatici prima che generino costi eccessivi.

Conclusione:

Gli attacchi informatici come ransomware, exploit e phishing possono avere gravi conseguenze in termini commerciali e di reputazione per le organizzazioni manifatturiere. Per proteggere i tuoi ambienti informatici e i tuoi dati di natura sensibile, ti serve un approccio di sicurezza integrato.

Con i nostri servizi e tecnologie next-gen, Sophos protegge sistemi e dati, ovunque si trovino, permettendoti di consolidare la gestione dell'intera infrastruttura di sicurezza con un solo vendor. Tutte le soluzioni Sophos sono controllate dalla nostra console di gestione unificata e basata sul cloud, Sophos Central, che permette ai vari prodotti di condividere informazioni in tempo reale. Inoltre, Sophos Central offre gestione centralizzata, risposta automatica agli incidenti e analisi approfondite: tutti elementi che interagiscono in perfetta sinergia per elevare ulteriormente il tuo livello di protezione, incrementando anche l'efficienza del tuo team di tecnici informatici.

Per scoprire di più sulla protezione Sophos per le organizzazioni manifatturiere e per discutere dei tuoi requisiti, rivolgiti al tuo commerciale di riferimento Sophos o richiedi una telefonata dai nostri specialisti di sicurezza.

Gartner non appoggia alcun fornitore, produttore o servizio citato all'interno delle sue pubblicazioni di ricerca e non consiglia agli utenti delle tecnologie di selezionare solo i fornitori con le valutazioni più alte o altre designazioni. Le pubblicazioni di Gartner riflettono solamente le opinioni dell'organizzazione di ricerca e consulenza di Gartner e non devono pertanto essere considerate come affermazioni di fatto. Gartner rinuncia a qualsiasi garanzia, implicita o esplicita, in merito a questa ricerca, incluse le garanzie sulla commerciabilità o sull'idoneità a un particolare scopo.

GARTNER è un marchio registrato e un marchio di servizio di Gartner, Inc. e/o dei suoi affiliati negli U.S.A. e a livello internazionale, MAGIC QUADRANT e PEER INSIGHTS sono marchi registrati di Gartner Inc. e/o dei suoi affiliati e vengono qui adoperati con la dovuta autorizzazione. Tutti i diritti riservati.
I contenuti di Gartner Peer Insights sono una raccolta delle opinioni di utenti finali individuali, basate sulle relative esperienze con i vendor indicati nella piattaforma; non devono essere interpretate come affermazioni di fatto, né come rappresentazione delle opinioni di Gartner o dei suoi affiliati. Gartner non appoggia alcun fornitore, produttore o servizio citato nei suoi contenuti, né fornisce alcuna garanzia, espressa o implicita, in riferimento a tali contenuti, alla loro accuratezza o completezza, inclusa qualsivoglia garanzia sulla commerciabilità o sull'idoneità a un particolare scopo.

© Copyright 2023. 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.

2023-04-05 IT-WP (NP)

SOPHOS