SOPHOS
Cybersecurity delivered.

Best Practice Per Proteggere La Rete Dal Ransomware

Potenzia la tua strategia di difesa contro il ransomware e altri attacchi alla rete

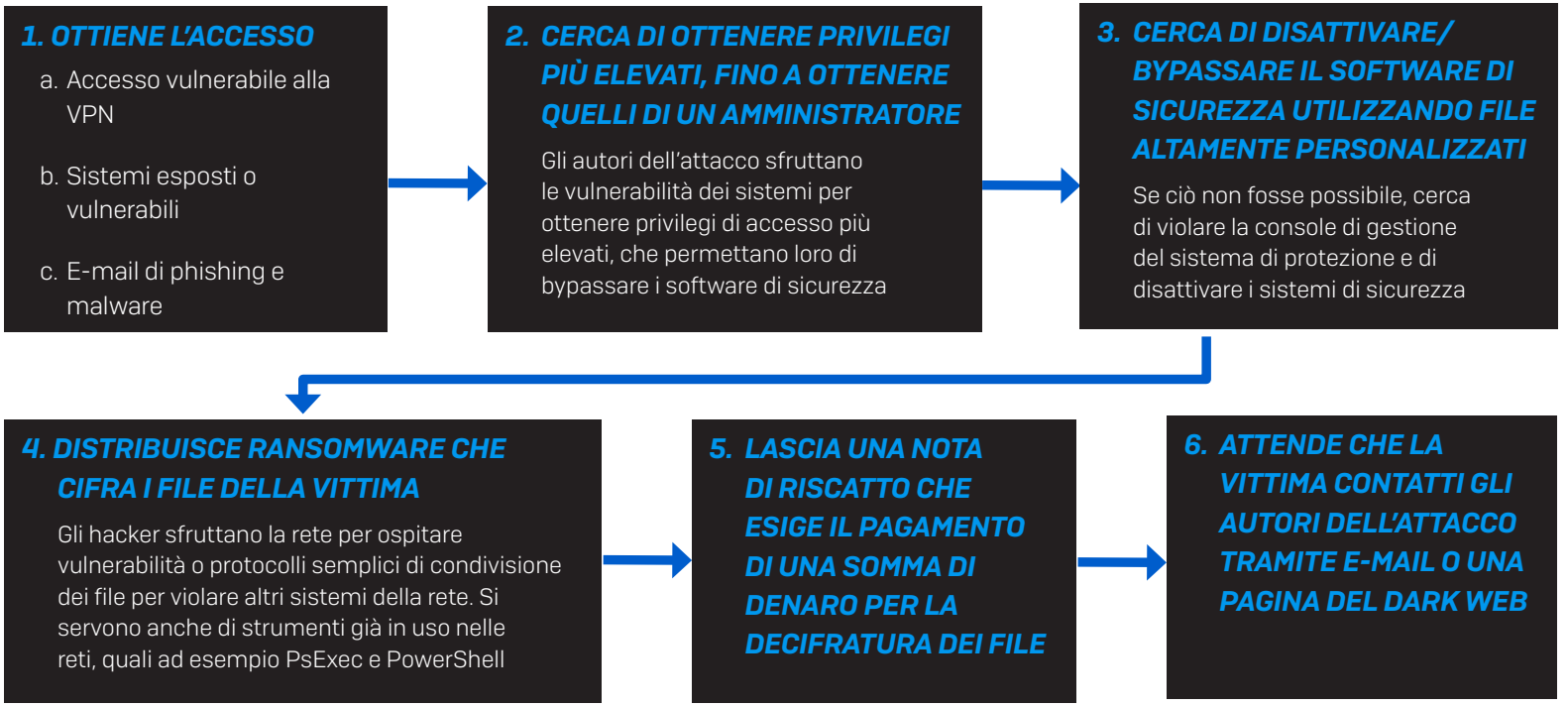
Whitepaper Sophos. Settembre 2022

Gli Attacchi Ransomware Crescono In Volume E Gravità

Negli ultimi 12 mesi, il 66% delle organizzazioni è stato colpito dal ransomware, una percentuale molto più alta rispetto al 37% del 2020[1]. Si tratta di un incremento annuo del 78%, che dimostra che, ora più che mai, gli hacker sono diventati ancora più abili nello sferrare attacchi su vasta scala. Il rapido aumento degli attacchi ransomware riflette anche l'enorme successo del modello del "Ransomware-as-a-Service", che estende il raggio di azione del ransomware, diminuendo il livello di competenze necessario per lanciare un attacco.

Come Funzionano Gli Attacchi Ransomware

Per capire come difenderci dagli attacchi ransomware, dobbiamo prima analizzare come funzionano. Un tipico attacco ransomware mirato agisce come segue:



Spesso i moderni attacchi ransomware sfruttano strumenti informatici legittimi e destinati agli utenti finali, come VPN o Remote Desktop Protocol (RDP), per ottenere l'accesso iniziale. Questi strumenti vengono comunemente utilizzati anche da personale autorizzato per svolgere il proprio lavoro, ed è questo a rendere difficile il rilevamento iniziale dei moderni attacchi ransomware. La radice del problema è l'eccessiva fiducia implicita riposta nell'uso di questi strumenti: si presume infatti che chiunque abbia accesso a una VPN o a un RDP possa essere ritenuto attendibile. Questo approccio si è dimostrato più volte estremamente pericoloso.

1 La Vera Storia Del Ransomware 2022, Sophos - Un sondaggio indipendente che ha coinvolto 5.600 professionisti dell'IT in 31 paesi.

Come Prevenire Gli Attacchi Ransomware

Esistono tre misure di protezione della rete che possono aiutare a mitigare il rischio di un attacco ransomware.

1. Eliminare l'esposizione ai rischi derivati dall'accesso remoto

Molti ritengono che una VPN (Virtual Private Network) offra protezione contro gli attacchi ransomware. In realtà, questo è un falso mito, in quanto la VPN è un vettore facile da sfruttare per i cybercriminali. Ultimamente, questo vettore di attacco è diventato ancora più invitante per gli hacker, grazie all'ampia proliferazione dell'uso di VPN di accesso remoto, poiché negli ultimi due anni milioni di dipendenti hanno cambiato modalità di lavoro, passando allo smart working I cybercriminali sono consci del fatto che queste reti domestiche non hanno una protezione adeguata e di conseguenza sono vulnerabili, il che le rende bersagli estremamente facili.

Uno degli attacchi ransomware di più alto profilo del 2021 ha coinvolto un'azienda di oleodotti statunitense, che ha riscontrato problemi nella consegna di combustibile a gran parte dei propri clienti nelle parti orientali e meridionali degli USA. Durante gli attacchi, i cybercriminali hanno utilizzato una VPN di accesso remoto.

Anche la maggior parte dei client VPN obsoleti contengono vulnerabilità soggette a exploit, e questo contribuisce a inasprire il problema, rendendo più difficile l'applicazione di una protezione adeguata della rete contro le minacce esterne. Tutto questo ha indotto le forze dell'ordine statunitensi, tra cui l'FBI, il Dipartimento della sicurezza interna (Department of Homeland Security) e la Cybersecurity and Infrastructure Security Agency (CISA), a emettere avvisi sul rischio di attacchi rivolti all'infrastruttura VPN di accesso remoto.

Best Practice: sostituire la VPN di accesso remoto con ZTNA

Zero Trust Network Access (ZTNA) è la più recente soluzione sostitutiva per le VPN di accesso remoto. Elimina l'attendibilità implicita e l'ampio accesso alla rete che caratterizzano le VPN, applicando invece i principi dell'approccio Zero Trust: non fidarti mai, verifica tutto. ZTNA offre maggiore sicurezza e semplicità di gestione, con una visibilità superiore e una migliore esperienza utente rispetto alle VPN di accesso remoto.

ZTNA elimina il bisogno di utilizzare client VPN vulnerabili, sfrutta l'autenticazione a più fattori (MFA) e lo stato di integrità del dispositivo per controllare l'accesso e concederlo solo ad applicazioni di rete specifiche, micro-segmentando la tua rete in maniera efficace. È talmente importante che la Casa Bianca ha emesso un mandato per l'architettura Zero Trust a cui devono conformarsi tutti gli enti federali entro il 2024.

Elimina i rischi causati da Remote Desktop Protocol (RDP) e altri sistemi

Gli strumenti di gestione remota come RDP, Virtual Network Computing (VNC) e altre soluzioni simili permettono al personale in smart working di accedere e gestire i sistemi. Purtroppo, senza adeguati sistemi di protezione, questi strumenti possono anche offrire agli hacker opportunità per loro estremamente pratiche per accedere ai sistemi e sferrare attacchi ransomware.

La mancata protezione di RDP e di altre soluzioni di gestione remota può lasciare spazio ad attacchi ransomware. Spesso i cybercriminali eseguono scansioni generali e si servono di strumenti di hacking di tipo brute force, che sono in grado di effettuare centinaia di migliaia di tentativi per dedurre combinazioni di nome utente e password, finché non ne trovano una valida. A volte le credenziali ottenute in questo modo vengono utilizzate per sferrare immediatamente un attacco. Tuttavia, possono anche essere vendute ad altre gang di cybercriminali.

"Abbiamo trovato una vecchia vulnerabilità critica Log4j non risolta su Horizon, grazie alla quale siamo riusciti a ottenere l'accesso iniziale. Abbiamo eseguito una scansione generale, non abbiamo mai avuto intenzione di sferrare un attacco mirato. Una volta entrati nella VM Horizon, abbiamo effettuato il dump delle credenziali, ottenuto accesso come amministratori di dominio, craccato l'hash e siamo stati in grado di spostarci lateralmente".

Citazione di una gang di hacker di ransomware, che descrive come è stato ottenuto l'accesso

La citazione riportata sopra è di una gang di cybercriminali che è riuscita a estorcere denaro a un'organizzazione dopo aver ottenuto accesso ai suoi sistemi grazie a una vulnerabilità priva di patch in VMware Horizon, scoperta durante una scansione generale. Questo mette in rilievo l'importanza di mantenere firmware e software sempre aggiornati, applicando le dovute patch.

Best Practice: eliminare l'accesso diretto dall'esterno

Proteggi i sistemi remoti bloccando ogni accesso tramite firewall e autorizzando solo l'accesso tramite ZTNA. Procedendo in questo modo, rimuoverai la possibilità di accedere direttamente dall'esterno del perimetro di rete.

Verifica tutte le regole firewall per accertarti che non ci siano sistemi RDP o di gestione remota esposti a rischi, implementando il port-forwarding o regole NAT. Oltre a questo, assicurati che l'accesso protetto sia scrupolosamente controllato tramite ZTNA: così facendo, avrai la certezza che ad accedere ai tuoi sistemi saranno solo gli utenti e i dispositivi autorizzati, che hanno superato i controlli dell'identità (tramite MFA) e dello stato di integrità.

Inoltre, potresti considerare l'uso di nuove tecnologie di autenticazione protetta, come Windows Hello for Business. E naturalmente, è essenziale mantenere l'infrastruttura aggiornata, applicando ogni patch appena viene rilasciata, per impedire di diventare bersagli facili a causa di vulnerabilità facilmente risolvibili.

2. Impedire a malware e ransomware di infiltrarsi nei sistemi attraverso attacchi di phishing e download dannosi

Un altro problema annoso è l'uso di tattiche che inducono gli utenti a rispondere alle e-mail di phishing e/o ad aprire messaggi pericolosi. Oggi come oggi, occorrono firewall, e sistemi di protezione per endpoint ed e-mail all'avanguardia, utilizzati insieme alle più recenti tecnologie di machine learning e sandboxing: questa sinergia di soluzioni permette di identificare minacce mirate in continua evoluzione, che cercano di accedere alla rete. Preferibilmente, queste minacce vanno bloccate prima che riescano a infiltrarsi nella rete, oppure devono essere isolate per impedirne l'avanzamento qualora dovessero essere già entrate nei sistemi.

Best practice: usare protezione contro le minacce zero-day

Assicurati di avere implementato la protezione più aggiornata contro attacchi di phishing ed e-mail dannose, per tenere queste minacce lontane dalle caselle di posta degli utenti. È anche consigliabile aggiungere al firewall la Deep-Packet Inspection (DPI), con decifratura TLS 1.3 inclusa, per ispezionare i payload cifrati; altre funzionalità desiderabili sono le analisi di machine learning per individuare le minacce zero-day e il sandboxing, che aiuta a valutare i file ricevuti mentre si eseguono. Insegna ai tuoi utenti come identificare le potenziali minacce di phishing e assicurati di installare sugli endpoint la migliore protezione disponibile contro i tentativi di furto di credenziali, gli exploit e il ransomware.

Per isolare le minacce che riescono nonostante tutto a infiltrarsi nella rete e per limitarne la capacità di movimento, puoi seguire diverse best practice, che verranno discusse nella prossima sezione.

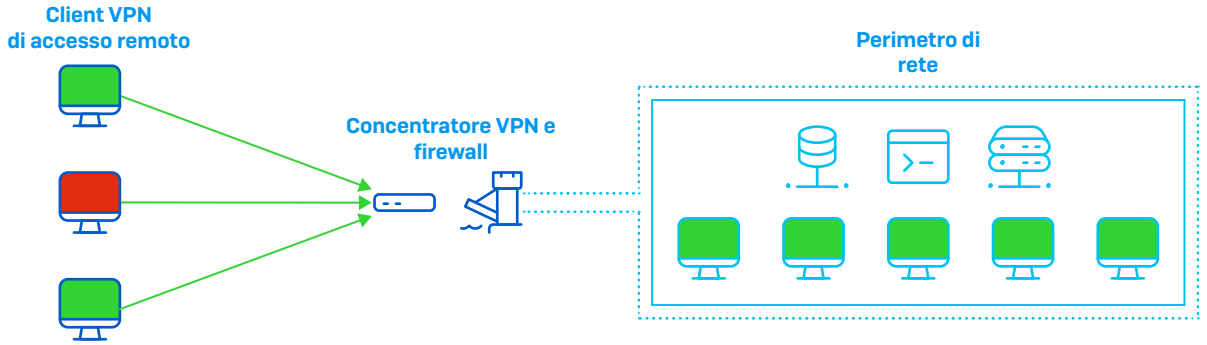
5 Active Adversary Playbook 2022 - Sophos

3. Limitare i movimenti laterali

Durante un attacco, è fondamentale che la tua soluzione di protezione della rete sia in grado di limitare la capacità di movimento verticale o laterale degli hacker all'interno dei tuoi sistemi.

Purtroppo, la struttura della maggior parte delle reti è simile a quella di una fortificazione medievale, con un castello al centro e un fossato intorno, che rappresenta il perimetro sicuro che difende le risorse. Le VPN offrono l'equivalente di una porta cittadina, che consente agli utenti autorizzati di entrare nel perimetro sicuro. Tuttavia, se un cybercriminale dovesse riuscire ad accedere a una rete, ha poi accesso completo a tutto quello che si trova al suo interno. Ad approfittare di questa stessa libertà di movimento in una rete possono essere anche minacce come il ransomware.

I cybercriminali sfruttano RDP e altri sistemi di gestione, più eventuali dispositivi non gestiti, come punti di ingresso. Se ne servono anche per spostarsi lateralmente all'interno di una rete.



Best practice: micro-segmentare la rete

Insieme a Zero Trust, questa pratica è fondamentale per le reti moderne. Per progettare la rete, consigliamo di seguire queste tre best practice:

1. **Segmentare la rete.** Crea piccole aree o VLAN e connettile utilizzando switch gestiti e un firewall, per garantire protezione antimalware e IPS tra i vari segmenti. In questo modo, sarai in grado di identificare e bloccare in maniera efficace le minacce che effettuano tentativi di movimento laterale all'interno della tua rete.
2. **Usare ZTNA.** Effettua la micro-segmentazione delle tue applicazioni di rete e concedi l'accesso solo agli utenti autorizzati e solo alle risorse di cui hanno bisogno. In questo modo, se un dispositivo dovesse essere compromesso e un elemento dannoso dovesse sfuggire al rilevamento, la minaccia potrà essere eliminata rapidamente. Sophos ZTNA va oltre, rimuovendo completamente l'accesso in caso di compromissione del dispositivo.
3. **Implementare tecnologie come Sophos Synchronized Security.** Synchronized Security avvia una risposta automatica alle minacce attive individuate nella rete, isolandole e impedendone i movimenti laterali. È in grado di identificare una minaccia e segnalarla immediatamente ai dispositivi integri, in modo che possano ignorare tutto il traffico di un host compromesso; allo stesso tempo, i Sophos Switch scartano i pacchetti provenienti da un dispositivo infettato, mentre Sophos Firewall limita l'accesso dell'host compromesso ad altre aree della rete.

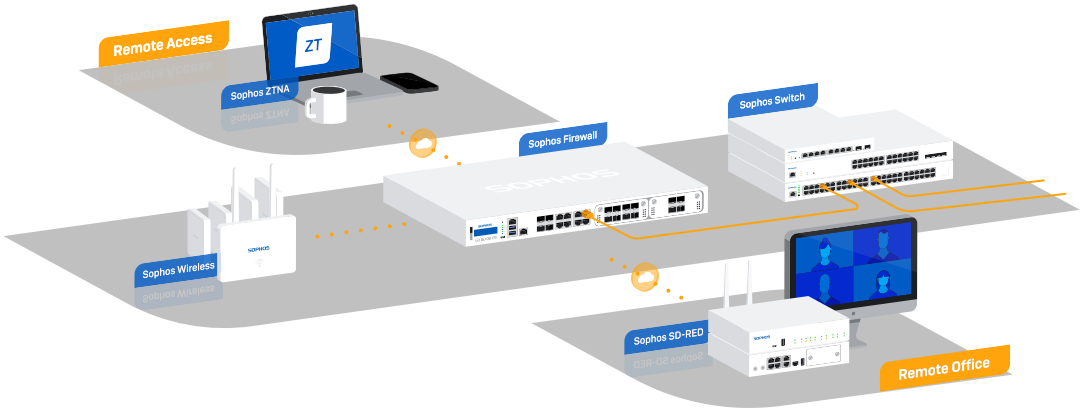
Best Practice Di Network Security Per Proteggersi Dal Ransomware

In sintesi, ecco le best practice da utilizzare per proteggere la rete dal ransomware e da altre minacce informatiche:

- **Micro-segmentare la rete.** Questa strategia ti permette di limitare i movimenti laterali delle minacce. Implementa Sophos ZTNA per micro-segmentare l'accesso alle tue applicazioni di rete. Utilizza anche Sophos Firewall e Sophos Switch per micro-segmentare le tue risorse di rete interne. Infine, usa un SD-RED per segmentare e connettere in maniera sicura i dispositivi e le sedi remote.
- **Sostituire le VPN di accesso remoto con ZTNA.** Elimina uno dei più comuni vettori di attacco, rimuovendo client VPN obsoleti e potenzialmente vulnerabili. Esegui l'upgrade a una soluzione ZTNA all'avanguardia come Sophos ZTNA, che si integra con la protezione endpoint next-gen Sophos per proteggere adeguatamente i dispositivi e l'identità dei tuoi utenti, l'accesso alle tue app e ai dati, più la rete: tutto questo viene offerto da un solo vendor, con un unico agente, in una singola console.
- **Implementare i massimi livelli di protezione possibili.** Consigliamo di applicare i massimi livelli di protezione su firewall, endpoint, server, dispositivi mobili e per l'accesso remoto.
  - Assicurati che il tuo firewall offra ispezione TLS 1.3, IPS next-gen e DPI di streaming con machine learning e sandboxing, per garantire protezione contro le minacce zero-day. Sophos Firewall include tutte queste tecnologie, integrandole in maniera ottimale per garantire una protezione potente e una performance superlativa: potrai così ottenere il migliore rapporto qualità-prezzo per il tuo investimento nel firewall.
  - Accertati anche che sui tuoi endpoint siano installate funzionalità moderne di protezione next-gen, per difendere i sistemi contro tentativi di furto di credenziali, exploit e ransomware. Sophos continua a ricevere valutazioni altissime, che la classificano tra i migliori vendor di soluzioni endpoint next-gen. Proteggiamo endpoint, dispositivi mobili e server, permettendoti di gestirli dalla stessa console basata sul cloud, proprio come tutti gli altri tuoi prodotti Sophos.
- **Ridurre la superficie di attacco.** Verifica le tue regole firewall e rimuovi tutte le autorizzazioni di accesso remoto o accesso RDP tramite VPN, NAT o port forwarding. Inoltre, assicurati che il traffico autorizzato venga protetto in maniera adeguata. Sophos Firewall semplifica il processo, grazie a una visibilità superiore, con dashboard e opzioni di reportistica e gestione delle regole.
- **Mantieni aggiornati firmware e software, applicando le patch.** Questa raccomandazione è particolarmente importante per le infrastrutture di rete come i firewall o i software/client di accesso remoto, ma è altrettanto essenziale per tutti i sistemi in generale, visto che ogni aggiornamento include importanti patch di sicurezza per vulnerabilità già identificate. Sophos ti aiuta a tenere automaticamente aggiornati tutti i tuoi prodotti di cybersecurity.
- **Utilizzare l'MFA.** Assicurati che nella tua rete venga adottato un approccio Zero Trust, in cui ogni utente e dispositivo deve continuamente guadagnarsi l'attendibilità in base a un processo di verifica dell'identità. Oltre a questo, ti consigliamo di implementare una policy per l'utilizzo di password sicure e di considerare l'uso di soluzioni di autenticazione come Windows Hello for Business. Tutti i prodotti Sophos supportano l'MFA con il provider di identità da te selezionato.

- **Rispondere immediatamente agli attacchi informatici.** Utilizza la combinazione perfetta tra tecnologie di automazione e competenze umane, per velocizzare la risposta e le attività di correzione in caso di incidente informatico.
  - Imposta un'infrastruttura di network security in grado di rispondere automaticamente agli attacchi attivi, per permetterti di isolare un eventuale host compromesso, prima che possa causare gravi danni. Solo Sophos Synchronized Security può garantirti i livelli di risposta di cui hai veramente bisogno, proprio nel momento in cui ti servono.
  - Implementa un servizio di Managed Detection and Response (MDR) come Sophos MDR: con Sophos MDR potrai contare su un team di esperti in materia di minacce che lavora ininterrottamente per te, monitorando e rispondendo agli incidenti prima ancora che diventino un problema. Avrai così piena sicurezza e tranquillità.

Proteggi la Tua Rete Con Sophos



Sophos offre tutto il necessario per la protezione completa contro gli attacchi alla rete, grazie a soluzioni come: ZTNA, switch, connettività wireless, dispositivi RED (Remote Edge Device), protezione per i messaggi, MDR, oltre alla protezione endpoint next-gen per tutti i tuoi dispositivi e server. E il bello è che l'intero sistema è gestito da un'unica console basata sul cloud (Sophos Central), con soluzioni perfettamente integrate per permetterti di usufruire della Sophos Synchronized Security e delle opzioni di rilevamento e risposta alle minacce o rilevamento e risposta estesi (XDR) su più prodotti.

La Synchronized Security fa in modo che i tuoi prodotti Sophos condividano continuamente dati relativi alla telemetria e allo stato di integrità, per aiutarti a rispondere più rapidamente agli attacchi informatici. Quando viene rilevato un host compromesso, gli endpoint integri cominciano automaticamente a ignorare il traffico, gli switch scartano i pacchetti provenienti dall'host compromesso e il firewall blocca l'accesso ad altre parti della rete fino a quando il problema non viene risolto. Nessun altro sistema di sicurezza è in grado di offrire tutto questo: con noi la cybersecurity diventa più semplice e più efficace.

Sophos XDR è l'unica soluzione XDR del settore in grado di sincronizzare la protezione nativa di firewall, endpoint, server, e-mail, cloud e Microsoft 365, per darti una panoramica olistica dell'ambiente della tua organizzazione. Offre informazioni complete e analisi profonda, fornendo opzioni di rilevamento, indagine e risposta fruibili sia dai team di un Security Operations Center dedicato, sia dagli amministratori IT.

Se per te la cybersecurity è diventata eccessivamente complessa, difficile e mutevole per poterla gestire in maniera autonoma, puoi contare su di noi. Sophos MDR protegge oltre 11.000 organizzazioni in tutto il mondo, garantendo servizi di threat hunting e neutralizzazione degli attacchi 24/7, a cura di un team globale di esperti in materia di minacce.

In pratica, Sophos offre una gamma completa di prodotti e servizi di cybersecurity che ti permettono di proteggere facilmente la rete dal ransomware.

Scopri come Sophos può proteggere
la tua rete, visita: www.sophos.com

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.

© Copyright 2022. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con No 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

2022-09-12 EN-WP (DD)

SOPHOS