SOPHOS
Cybersecurity evolved.

Proteggere l'organizzazione distribuita

In qualsiasi luogo. Su qualsiasi dispositivo. Per qualsiasi risorsa.

White paper Sophos febbraio 2021

Lo smart working fa ormai parte della normalità: secondo Gartner, il 74% delle organizzazioni prevede che alcuni dei propri dipendenti continueranno a lavorare da remoto anche dopo la fine della pandemia[1]. Allo stesso tempo, anche le risorse di cui hanno bisogno i dipendenti per svolgere le proprie mansioni sono distribuite in luoghi diversi: sui server in ufficio, in applicazioni cloud come Office 365 o Salesforce, e in ambienti cloud pubblici su Amazon Web Services (AWS) e Microsoft Azure.

Al personale IT spetta l'arduo compito di proteggere tutti gli utenti e tutte le risorse, indipendentemente da dove si trovino. Nel frattempo, i malintenzionati continuano a escogitare metodi costantemente più sofisticati e rivoluzionari per infiltrarsi nei sistemi di organizzazioni sempre più virtualizzate, approfittando di qualsiasi opportunità.

Per proteggere le organizzazioni decentralizzate, con dipendenti e risorse che possono essere situati ovunque, occorre:

- Proteggere la connettività, in modo che gli utenti possano accedere alle risorse da qualsiasi luogo: a casa, in loco o in ufficio
- Mettere in sicurezza i dispositivi utilizzati per stabilire queste connessioni: desktop, laptop, dispositivi mobili e tablet
- Garantire la protezione dei dati e dei workload a cui devono accedere gli utenti, sia che si trovino nel cloud o nella rete locale
- Offrire la massima semplicità di gestione, in modo che il personale tecnico sia in grado di gestire la propria organizzazione distribuita da qualsiasi luogo, senza ulteriori carichi di lavoro

Fortunatamente, Sophos aiuta le organizzazioni in tutti questi ambiti. Offriamo una gamma completa di prodotti di sicurezza next-gen, ricchi di avanzatissime funzionalità di protezione. L'intero sistema è controllato da un'unica piattaforma di sicurezza basata sul web, che aiuta a dare un taglio netto ai costi di amministrazione quotidiana, permettendo però al personale informatico di gestire la protezione della propria organizzazione da qualsiasi luogo.

Questo briefing della soluzione descrive come Sophos può soddisfare ciascuno di questi requisiti. Inoltre, esplora i vantaggi in termini di produttività e protezione di cui possono usufruire i clienti quando scelgono di utilizzare un sistema di cybersecurity Sophos per difendere la propria organizzazione.

Protezione delle connessioni

Non si può negare che la pandemia da COVID sia stata un fattore determinante per la rapida diffusione dello smart working. Nel mese di maggio del 2020, il 62% dei dipendenti statunitensi lavorava da casa. Tuttavia, lo smart working era una tendenza in aumento ancor prima del COVID e molti dipendenti in ufficio si trovavano già in fase di transizione verso una modalità di lavoro che prevedeva il telelavoro alcuni giorni alla settimana. Nel Regno Unito lo smart working ha subito un incremento pari al 74% nell'ultimo decennio, mentre in Australia circa un terzo del personale lavora regolarmente da casa.

Lo smart working è vantaggioso sia per le aziende che per i dipendenti: questi ultimi possono risparmiare sul tempo e sui costi di viaggio, con un incremento sia della flessibilità che della produttività. Nel frattempo, le organizzazioni possono risparmiare sulle spese e sul turnover del personale. Tuttavia, per i team informatici l'adozione a lungo termine dello smart working implica maggiori sfide di sicurezza. Sia che i dipendenti si connettano dalla loro abitazione, dall'ufficio di un cliente o da un hotspot Wi-Fi mentre sorseggiano una bevanda a migliaia di chilometri di distanza, la rete e i dati aziendali devono rimanere protetti in qualsiasi momento.

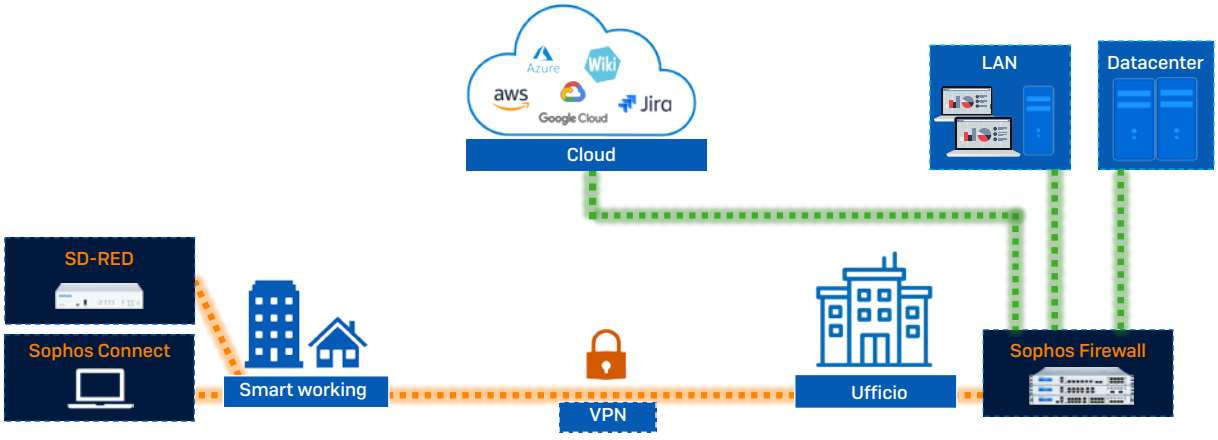
Con Sophos, i dipendenti possono connettersi e lavorare da qualsiasi luogo in maniera rapida, efficiente e soprattutto sicura. Inoltre, offriamo sia la tradizionale opzione di accesso tramite VPN che Zero Trust Network Access (ZTNA).

VPN

Il nostro **client VPN Sophos Connect** è disponibile gratuitamente e facile da distribuire; utilizzato insieme a **Sophos Firewall**, connette i dipendenti in smart working alla sede principale e alle risorse basate sul cloud. Con più di 1,4 milioni di utenti in tutto il mondo, Sophos Connect offre accesso sicuro alle risorse situate nella rete aziendale o nel cloud pubblico per gli utenti che lavorano da remoto su dispositivi Windows e macOS.

Per una connettività remota che non ha rivali, il dispositivo plug-and-play **Sophos SD-RED** (Remote Ethernet Device) è semplice da usare insieme a **Sophos Firewall**: connette filiali, sedi remote e singoli dipendenti alla rete principale, sia essa fisica o basata sul cloud.

Include una VPN dedicata sempre attiva o split-tunnel che è facile da installare e gestire e offre opzioni flessibili. Inoltre, è anche piccolo e portatile, una caratteristica che lo rende ideale per i senior manager o per altri dipendenti che hanno bisogno di accedere a una connessione sicura in qualsiasi momento e da qualsiasi luogo.



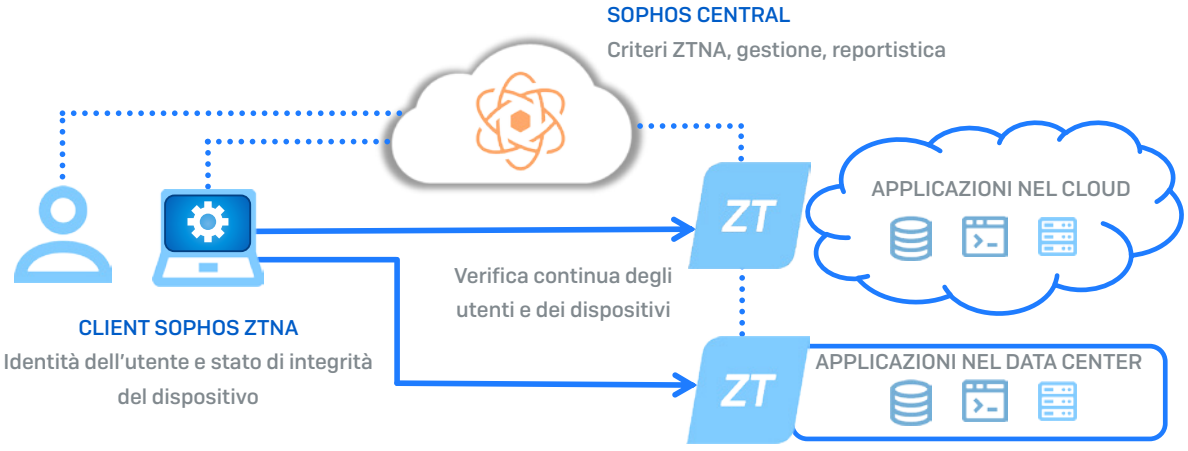
Protezione delle connessioni remote con Sophos Firewall e Sophos Connect VPN e SD-RED

ZTNA

Da diversi anni, la tecnologia VPN aiuta i dipendenti aziendali a connettersi da remoto. E all'inizio della pandemia è stata veramente un salvavita, in quanto ha permesso alle organizzazioni di cambiare rapidamente strategia e passare allo smart working nel giro di appena pochi giorni. Tuttavia, molte organizzazioni cominciano ad avere esigenze che superano di gran lunga le capacità per cui la VPN era stata originariamente progettata.

Sophos Zero Trust Network Access (ZTNA) è un'ottima alternativa alla VPN di accesso remoto, in quanto permette agli utenti di connettersi alle risorse aziendali da qualsiasi luogo e in maniera semplice e trasparente. Allo stesso tempo, ottimizza la sicurezza, in quanto verifica continuamente l'utente (solitamente tramite autenticazione a fattori multipli e un provider di identità) e convalida lo stato di integrità e conformità del dispositivo.

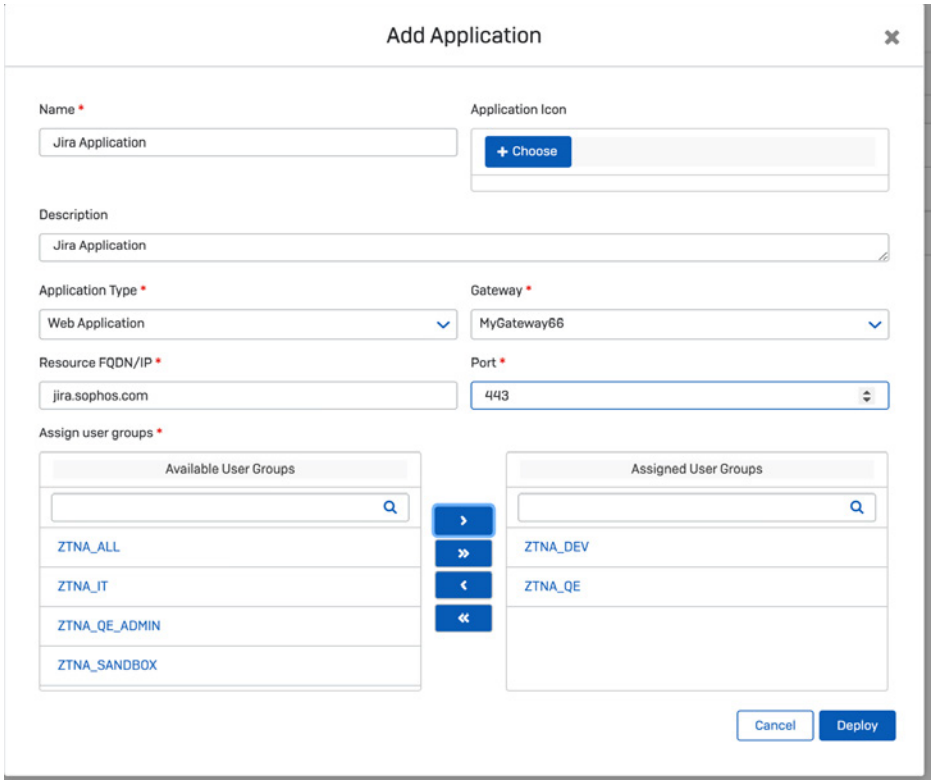
Sophos ZTNA si accerta che il dispositivo sia registrato al sistema di sicurezza e ne controlla lo stato di aggiornamento, protezione e cifratura. Utilizzando le informazioni raccolte, prende quindi decisioni basate su criteri personalizzabili che stabiliscono i privilegi e i diritti di accesso di un utente alle applicazioni di rete business critical.



L'approccio Sophos ZTNA

Con Sophos ZTNA, è possibile:

- Potenziare le difese informatiche. Sophos ZTNA offre controlli estremamente granulari: qualsiasi utente, dispositivo o applicazione può essere controllato individualmente in base a criteri aziendali personalizzati e al livello di rischio ritenuto più idoneo. Inoltre, elimina il concetto di attendibilità implicita di un utente che si trova all'interno della rete. Agisce invece valutando continuamente l'identità e lo stato di integrità del dispositivo prima di concedere l'accesso, elevando così il livello di protezione e riducendo al minimo il rischio di movimenti laterali all'interno della rete.
- Incrementare l'efficienza. Poiché Sophos ZTNA è gestito dalla piattaforma Sophos Central, semplifica la registrazione di nuovi dispositivi e il passaggio a un ambiente di lavoro in costante evoluzione. Inoltre, è più trasparente per gli utenti finali e garantisce un'esperienza di connessione priva di problemi, che risulta molto più semplice rispetto alla VPN.



Aggiunta semplice delle applicazioni con Sophos ZTNA

Qualsiasi sia il metodo selezionato, i pluripremiati prodotti di sicurezza Sophos aiutano le organizzazioni a proteggere i dipendenti in qualsiasi luogo e su qualsiasi dispositivo.

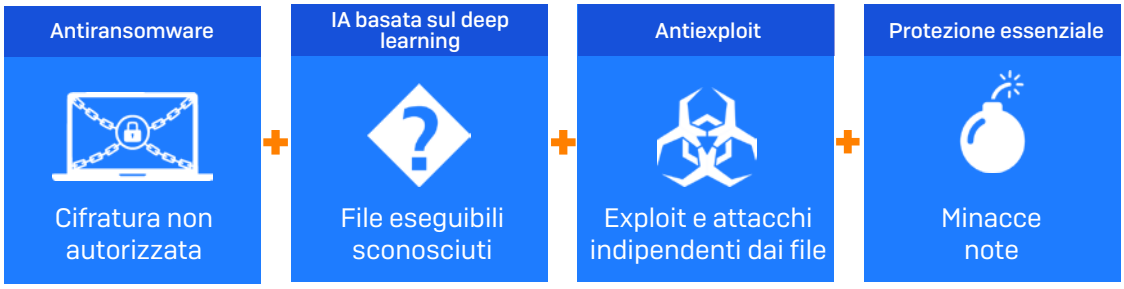
Protezione dei dispositivi

Il 51% delle organizzazioni è stato colpito dal ransomware negli ultimi dodici mesi e i cybercriminali sono riusciti a cifrare i dati nel 73% di questi attacchi[2].

Aggiungendo a queste statistiche già allarmanti l'esigenza di proteggere attrezzature di vario tipo (desktop, laptop, dispositivi aziendali e personali) e una miriade di sistemi operativi (da Windows, macOS e Linux, fino ad Android, Chromebook e iOS), il risultato è la ricetta perfetta per un bel grattacapo di sicurezza.

Sophos Intercept X garantisce la migliore protezione in assoluto per tutti questi dispositivi e piattaforme. Fornisce livelli multipli di tecnologie in grado di bloccare i cybercriminali in vari punti della catena di attacco. Queste tecnologie includono:

- Protezione antiransomware, per bloccare la cifratura non autorizzata di file, hard disk e record di avvio, ripristinando gli elementi attaccati a uno stato sicuro
- Intelligenza artificiale basata sul deep learning, che sfrutta milioni di attributi dei file per analizzare le minacce e prevenire sia il malware noto che quello mai osservato prima, bloccandolo ancor prima che riesca a eseguirsi
- Tecnologie antiexploit per bloccare gli exploit, le tecniche degli active adversary e gli attacchi indipendenti dai file basati su script
- Protezione essenziale basata sulle firme, per bloccare le minacce conosciute



Inoltre, Sophos Intercept X protegge tutti i dispositivi su tutte le piattaforme, per cui i dipendenti potranno lavorare in completa sicurezza su qualsiasi dispositivo preferiscano:

- Desktop e laptop con Windows e macOS
- Server Windows e Linux
- Ambienti desktop virtuali ospitati su provider di servizi cloud
- Dispositivi mobili con Android, iOS o Chromebook

Endpoint Detection and Response (EDR)

Le minacce informatiche più distruttive sono generalmente coordinate da menti umane e sovente si servono di strumenti legittimi, come PowerShell. Le attività di hacking svolte in tempo reale permettono ai cybercriminali di bypassare i prodotti e i protocolli di sicurezza modificando le proprie tattiche, tecniche e procedure (TTP). Una volta infiltratisi nella rete, gli autori degli attacchi si possono muovere lateralmente per esfiltrare dati, distribuire ransomware e installare malware e backdoor per attacchi futuri.

Per bloccare questi attacchi coordinati da una mente umana, occorre un threat hunting con supervisione umana. **Intercept X with EDR** (Endpoint Detection and Response) fornisce gli strumenti necessari per svolgere il threat hunting dalla stessa console utilizzata per gestire la protezione endpoint di Intercept X.

È Il primo sistema di EDR progettato per gli analisti di sicurezza e gli amministratori IT. A differenza di altri strumenti di EDR che richiedono personale appositamente dedicato o un Security Operations Center (SOC) interno, Sophos EDR è semplice da utilizzare e non implica limitazioni in termini di efficacia delle capacità di analisi.

Intercept X with EDR permette di indagare sui segnali sospetti e sulle minacce (migliorando così lo stato di integrità informatica), grazie alle potenti query SQL subito pronte per l'uso e personalizzabili. I più comuni casi di utilizzo includono:

- Rallentamento di Chrome. Identificazione di eventuali estensioni di Chrome installate senza autorizzazione
- Controllo dell'attività di rete. Individuazione di eventuali tentativi di accesso non riusciti e comunicazione attiva da PowerShell
- Query sui software. Verifica della rimozione dei file di natura sensibile dai dispositivi e/o controlli relativi alle licenze software, per garantire che non vengano superati i limiti massimi di utilizzo
- Indagini sul phishing. Identificazione degli utenti che hanno cliccato su un link sospetto e rilevamento di eventuali file scaricati in queste circostanze

Inoltre, è possibile accedere ai dispositivi da remoto con uno strumento da riga di comando per correggere eventuali problemi e svolgere operazioni quali: riavvio dei dispositivi, terminazione di processi attivi, esecuzione di script o programmi, modifica dei file di configurazione, esecuzione di strumenti di analisi approfondita e installazione/disinstallazione di software.

Managed Detection and Response (MDR)

Chi non dovesse avere il tempo, la capacità o le competenze necessari per svolgere indipendentemente attività di indagine e threat hunting può affidarsi al servizio **Sophos Managed Threat Response** (MTR).

Sophos MTR è un team di esperti di threat hunting e risposta strategica che offre un servizio completamente gestito e disponibile 24/7 di monitoraggio, rilevamento e risposta alle minacce. Il team agisce individuando proattivamente potenziali minacce e incidenti, ne conferma la gravità e li blocca prima che possano arrecare danni.

Inoltre, raccoglie e mette in correlazione i feed di dati forniti dalle soluzioni di protezione Sophos, per identificare gli indicatori di compromissione. A differenza di altri servizi di rilevamento e risposta gestiti, Sophos non si limita semplicemente a segnalare i problemi: il nostro servizio determina e applica le azioni più appropriate per neutralizzare la minaccia.

Dispositivi mobili

Quando i dipendenti utilizzano i dispositivi personali per lavoro, i team tecnici devono affrontare il problema di tutelare i dati aziendali senza compromettere la privacy degli utenti. La nostra soluzione di Unified Endpoint Management **Sophos Mobile** protegge i dispositivi iOS, Android, Chrome OS, Windows 10 e macOS. Permette di proteggere qualsiasi combinazione di utilizzo di dispositivi personali e forniti in dotazione dall'azienda, non richiede un impegno eccessivo ed è la soluzione ideale per gli scenari BYOD (Bring Your Own Device).

Sophos Mobile consente di:

- Bloccare le minacce sui dispositivi mobili. Offre un sistema di difesa leader di settore e in grado di proteggere i sistemi dal malware dei dispositivi mobili, dal phishing, dagli attacchi man-in-the-middle e altro, tutto grazie alla tecnologia Intercept X
- Proteggere i dati aziendali. È possibile scegliere di gestire l'intero dispositivo o solamente il container, a seconda delle esigenze
- Ridurre il carico amministrativo. Il flessibilissimo portale self-service permette agli utenti di registrare i propri dispositivi (macOS, Windows 10 o dispositivi mobili), reimpostare le password e richiedere assistenza, tutto senza coinvolgere il reparto IT

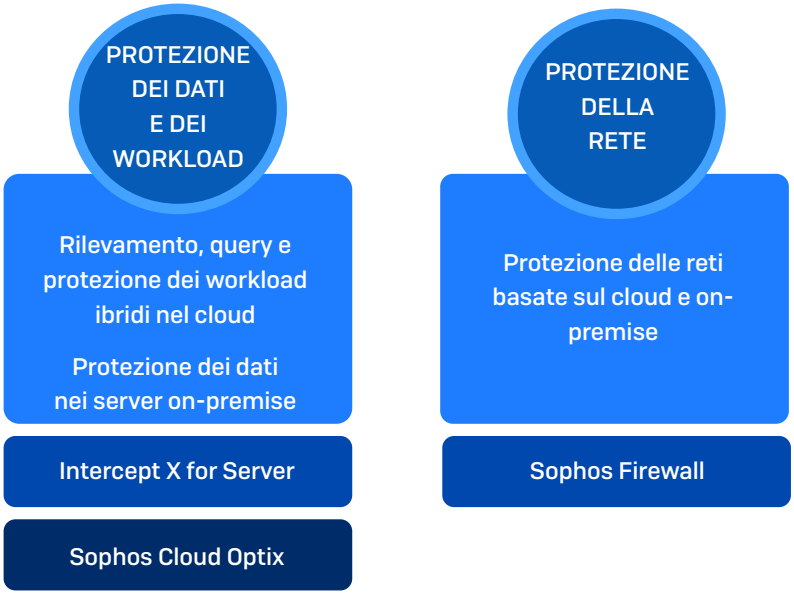
Protezione delle risorse

A seconda delle proprie esigenze, un'organizzazione può eseguire server on-premise, utilizzare applicazioni basate sul cloud oppure ospitare risorse in ambienti cloud privati e pubblici su AWS, Azure o GCP. Gli scenari più comuni implicano una combinazione di tutte queste possibilità.

Il cloud sta diventando sempre più essenziale per lo svolgimento delle normali operazioni quotidiane della maggior parte delle organizzazioni. Di conseguenza, le potenziali opportunità del cloud sono oggetto di grande interesse da parte dei cybercriminali: lo dimostra il fatto che il 70% delle aziende che utilizza il cloud pubblico è stata vittima di un incidente di sicurezza negli ultimi 12 mesi[3].

Per tutelare le proprie risorse (indipendentemente da dove si trovino), occorrono due elementi strategici fondamentali:

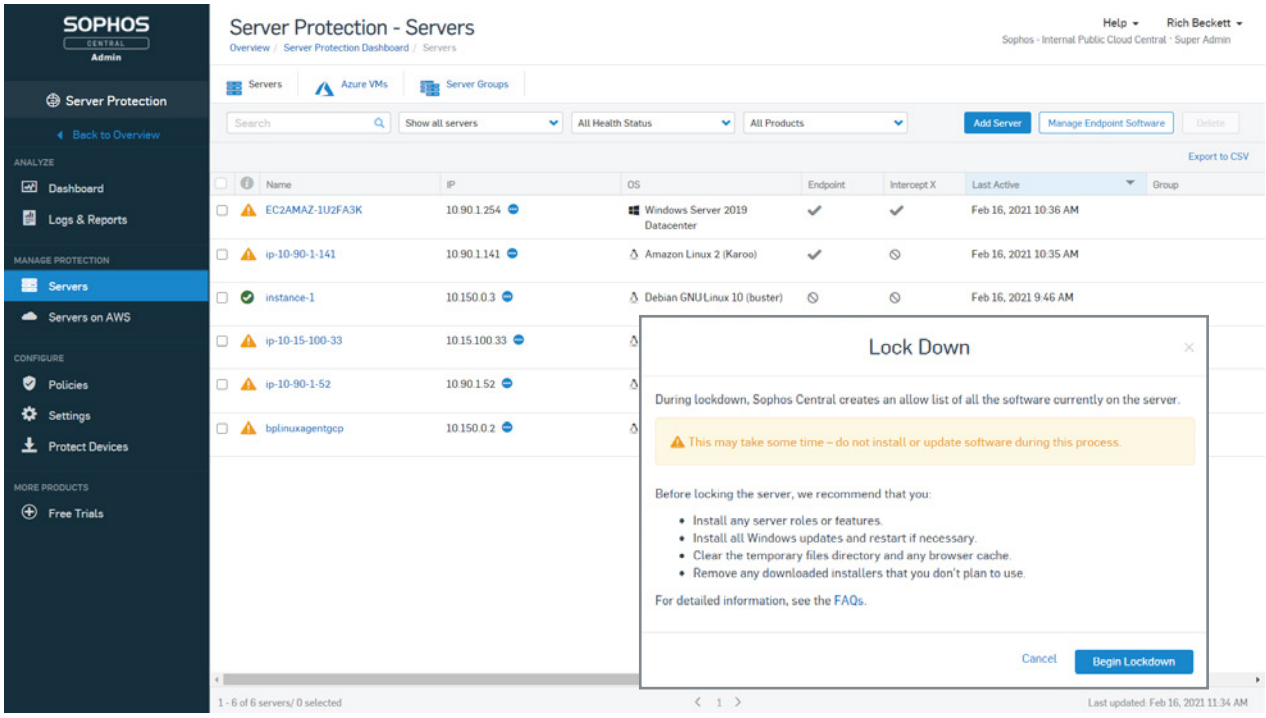
1. La protezione dei dati e degli stessi workload
2. La protezione della rete su cui sono situati, per tenere lontani gli intrusi



Protezione dei dati e dei workload

I dati e i workload sono le risorse più importanti di un'organizzazione. **Sophos Intercept X for Server** protegge gli ambienti di workload sul cloud, on-premise e ibridi. Garantisce la sicurezza delle virtual machine Windows e Linux e dei desktop virtuali, difendendoli dalle minacce più recenti.

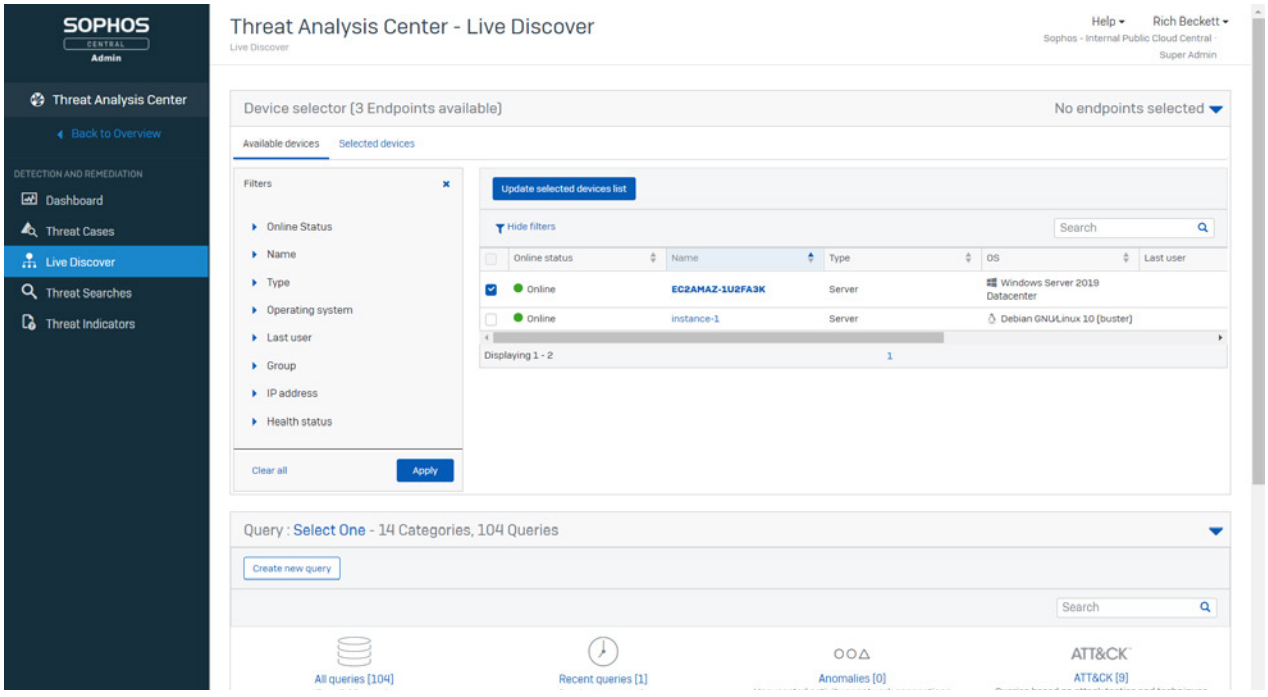
- Blocca gli attacchi più avanzati, inclusi quelli di ransomware, basati sugli exploit e persino malware mai osservato prima
- Isola i workload dei server. Offre controllo assoluto sugli elementi autorizzati a eseguirsi e su quelli bloccati, inviando notifiche per tutti i tentativi di modifica non autorizzata
- Aiuta a gestire tutti i componenti in maniera centralizzata. Permette di distribuire e gestire l'intero ambiente da un'unica console, anche in scenari misti, caratterizzati dalla presenza sia di workload nel cloud che di server on-premise



Intercept X for Server

Le indagini di EDR possono essere estese anche ai server (sia on-premise che nel cloud), con **Intercept X for Server with EDR**. In questo modo è possibile:

- Svolgere attività essenziali per la gestione operativa dei sistemi informatici e il threat hunting: identificazione di eventuali problemi di performance, visualizzazione degli elementi installati e della loro posizione, individuazione proattiva di eventuali attività sospette
- Rilevare automaticamente i workload nel cloud: monitoraggio dei servizi cloud business critical, inclusi i bucket S3, i database e le funzioni indipendenti dai server
- Individuare le distribuzioni non sicure, grazie al monitoraggio costante basato su tecnologie di intelligenza artificiale degli ambienti cloud e alla segnalazione di eventuali irregolarità



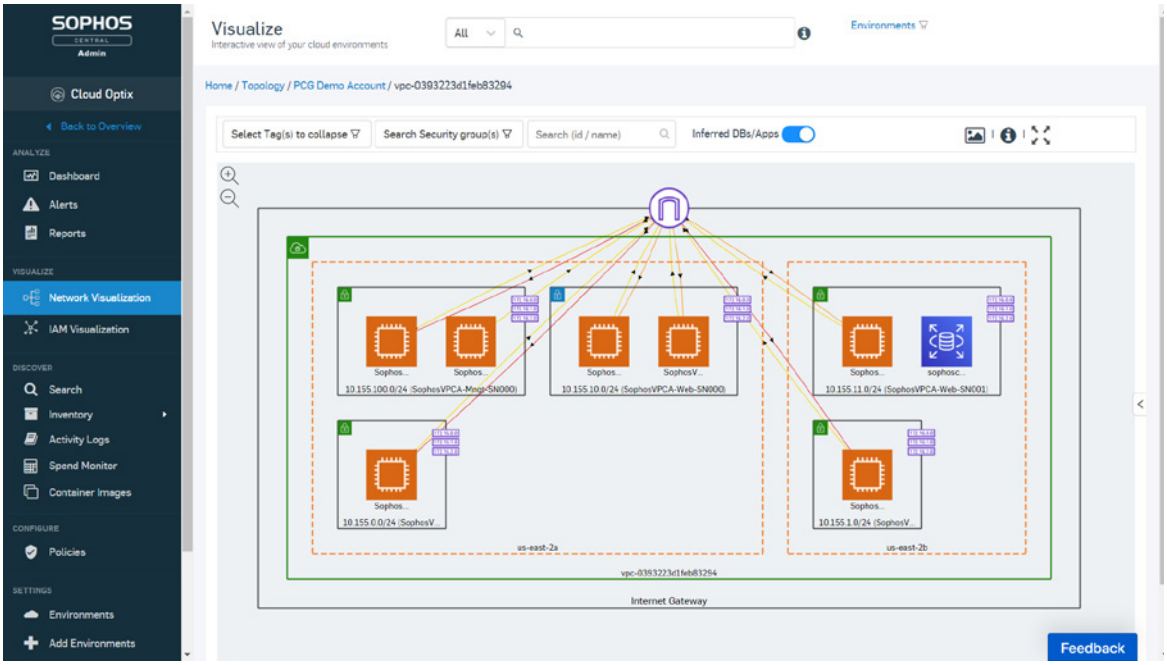
Le indagini EDR possono essere estese anche ai server

La protezione rappresenta solo un lato della medaglia della messa in sicurezza di dati e workload. L'altro lato è la visibilità.

Occorre una chiara linea di visibilità sugli elementi in esecuzione ed è necessario anche avere la capacità di configurare le opzioni dei fornitori dei servizi cloud, per prevenire le violazioni di sicurezza.

Sophos Cloud Optix, la nostra soluzione di gestione dello stato di sicurezza generale sul cloud, offre la visibilità necessaria per proteggere l'organizzazione, con vantaggi che includono:

- Visibilità multicloud. Un inventario dettagliato delle risorse cloud, inclusi server, container, archiviazione, rete e IAM per AWS, Azure e GCP
- Attribuzione di priorità stabilite in base al rischio. Analisi continua delle configurazioni, per individuare i rischi di sicurezza e gli accessi IAM con privilegi eccessivi
- Gestione della conformità. Monitoraggio costante della conformità, con modelli subito pronti per l'uso, criteri personalizzati e strumenti di collaborazione
- Sicurezza integrata. Identificazione dei Sophos Firewall e protezione dei workload su AWS
- Ottimizzazione dei costi correlati al cloud. Gestione delle spese di AWS e Azure da un'unica schermata



Sophos Cloud Optix

Sebbene gli avvisi di sicurezza per gli ambienti cloud siano molto utili, grazie anche a servizi che offrono un ottimo rapporto qualità-prezzo come Amazon GuardDuty, l'enorme quantità di notifiche può essere difficile da gestire. Pertanto, può diventare praticamente impossibile riconoscere quali sono le notifiche su cui occorre veramente indagare.

Sophos utilizza Sophos Cloud Optix per proteggere gli ambienti Amazon Web Services su cui è ospitata Sophos Central, la nostra piattaforma di cybersecurity. Uno dei principali vantaggi di Cloud Optix per il nostro team interno di sicurezza è poter focalizzare l'attenzione sugli elementi importanti.

"Con Sophos Cloud Optix, siamo riusciti a ridurre in maniera significativa lo stress dovuto all'eccesso di informazioni. Le potenti tecnologie di intelligenza artificiale integrate in Sophos Cloud Optix mettono in correlazione i dati, mostrandoci solamente informazioni pratiche e significative."

Ross McKerchar, VP e CISO, Sophos

Protezione della rete

Per difendere le risorse occorre mettere in sicurezza le reti su cui vengono eseguite. **Sophos Firewall** garantisce livelli di protezione e visibilità che non hanno rivali, sia per gli ambienti on-premise che per quelli AWS o Azure.

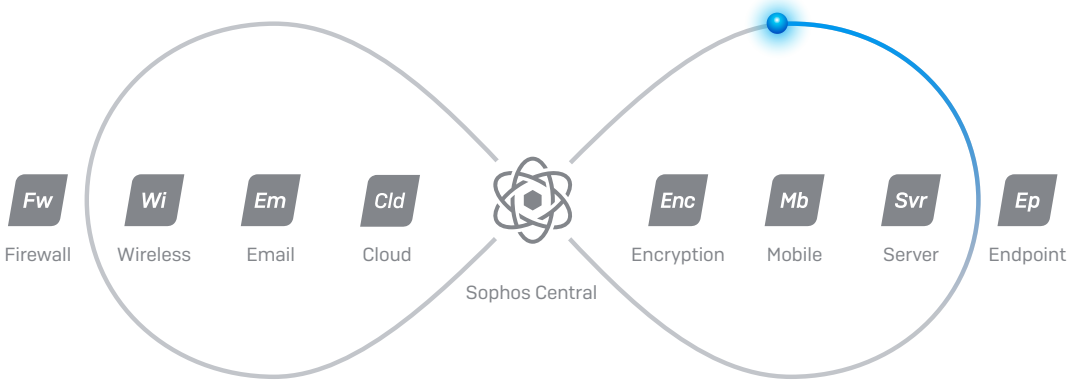
- Protezione integrata e a livelli multipli, per bloccare anche le minacce più avanzate
- Potente soluzione all-in-one con WAF (Web Application Firewall), IPS (Intrusion Prevention System), ATP (Advanced Threat Protection), filtro degli URL, routing basato sul percorso e blocco a livello del paese, nonché vaste opzioni di reportistica, inclusi dati approfonditi sugli utenti e sulle attività di rete
- Visibilità sulle applicazioni cloud, rilevamento dello shadow IT e risposta automatica alle minacce
- Protezione avanzata per i workload nel cloud contro tentativi di hacking quali SQL injection e cross-site scripting, pur garantendo accesso sicuro agli utenti con l'autenticazione tramite reverse proxy
- Flessibilità di esecuzione in modalità standalone o come soluzione di disponibilità elevata

Inoltre, per semplificare la distribuzione nel cloud, tutti i componenti sono disponibili in un'unica immagine di virtual machine preconfigurata.

Gestione semplificata

Con Sophos, l'intero sistema di sicurezza può essere gestito da un'unica piattaforma basata sul web: Sophos Central. Ora non c'è più bisogno di passare da una console a un'altra per proteggere la propria organizzazione, poiché tutto si trova in una singola interfaccia. Inoltre, permette di svolgere indagini su più dispositivi con estrema semplicità, in quanto mette in correlazione i dati provenienti da servizi diversi.

E in più, siccome Sophos Central è ospitata nel cloud, è la soluzione ideale per i team IT decentralizzati. Con oltre 400.000 utenti in tutto il mondo, i responsabili tecnici potranno dormire sonni tranquilli, nella consapevolezza di essere protetti dalla più efficace piattaforma di cybersecurity in assoluto.



Inoltre, Sophos Central permette ai prodotti Sophos di condividere in tempo reale informazioni relative alla sicurezza e allo stato di integrità, abilitandone la cooperazione reciproca per rispondere automaticamente alle minacce: un sistema che abbiamo denominato Synchronized Security. I vantaggi includono:

- Risposta automatica in caso di incidenti. Se un prodotto Sophos individua un elemento sospetto (ad es. un'infezione di malware o un dispositivo che non rispetta la conformità), condivide questa informazione con il resto del sistema di cybersecurity. Gli altri prodotto avviano quindi una risposta automatica all'incidente, e il tutto avviene nel giro di pochi secondi. Per esempio:
  - Sophos Firewall isola immediatamente i dispositivi infetti, impedendo alla minaccia di diffondersi e bloccando i movimenti laterali.
  - Intercept X analizza automaticamente un endpoint quando vengono rilevate caselle di posta compromesse, limitando l'impatto delle minacce provenienti dalla posta elettronica.
  - Sophos Wi-Fi limita l'accesso alla rete per i dispositivi che non rispettano la conformità, tenendo lontani dalla rete wireless i dispositivi non autorizzati e non sicuri.
- Capacità esclusive di analisi approfondita. Il personale IT può ottenere maggiori livelli di visibilità e controllo sulla rete, con la possibilità di:
  - Identificare i dispositivi infettati per nome (e non indirizzo IP), per velocizzare le indagini di sicurezza.
  - Identificare tutte le app nella rete. In media, il 43% del traffico di rete viene contrassegnato come "non classificato", per cui il personale IT non può sapere se sia innocuo, pericoloso o dannoso. Con Synchronized Security, Sophos Firewall e Intercept X agiscono in maniera coordinata per identificare e classificare automaticamente TUTTE le app presenti all'interno della rete.

Una protezione che non ha rivali. Un'efficienza imbattibile.

Eseguire un sistema di cybersecurity Sophos significa poter usufruire di: protezione next-gen, un'unica piattaforma di gestione, condivisione dei dati di intelligence sulle minacce tra i vari prodotti e risposta automatica in caso di incidenti. Insieme, queste funzionalità costituiscono un enorme vantaggio per il personale IT in termini di efficienza e produttività.

Infatti, i clienti che utilizzano Sophos Intercept X e Sophos Firewall con gestione da Sophos Central, sostengono sistematicamente di aver potuto **raddoppiare l'efficienza del personale IT** e **ridurre dell'85% gli incidenti di sicurezza**.

"Poter contare su strumenti in grado di rilevare e risolvere automaticamente la maggior parte degli eventi di sicurezza permette al nostro team IT, composto da pochi dipendenti, di gestire la sicurezza dell'azienda e prevenire la compromissione dei nostri sistemi."

Chief Technology Officer di un fornitore di servizi software

Protezione in qualsiasi luogo. Su qualsiasi dispositivo. Per qualsiasi risorsa.

Le modalità flessibili di smart working e il sempre più diffuso utilizzo del cloud sono talmente integrati nelle nostre vite che è ormai impossibile tornare sui nostri passi. Da un lato semplificano il nostro lavoro, ma dall'altro presentano nuove sfide per il personale tecnico e nuove opportunità per i malintenzionati. Per difendere questo nuovo ambiente è essenziale garantire connessioni protette, risorse protette e dispositivi protetti, indipendentemente da dove si trovino. Il tutto deve essere fatto senza incidere sul budget dedicato ai sistemi informatici.

Sophos aiuta le organizzazioni ad affrontare tutte queste sfide attuali con soluzioni potenti e dall'efficacia comprovata. Contattate il vostro rappresentante Sophos per parlare delle vostre esigenze o avviate una prova gratuita senza obbligo di acquisto per fare un giro di prova dei nostri prodotti.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2.Nota a piè di pagina: La vera storia del ransomware, Sophos

3.Nota a piè di pagina: La Cloud Security nel 2020, Sophos

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

150221 WPIT (MP)

SOPHOS