SOPHOS
Cybersecurity evolved.

Guida Alla Cybersecurity Per Il Settore Sanitario

Una cybersecurity per il settore sanitario in grado di bloccare gli attacchi sul nascere, senza interferire con la cura dei pazienti

Briefing Sulla Soluzione Sophos. Aprile 2021

Cybersecurity e cura dei pazienti

Basta dire "cura dei pazienti" e subito si pensa a dottori, infermieri e altri professionisti sanitari che prestano cure mediche. Tuttavia, per la sanità, le tecnologie – dall'Intelligenza Artificiale e Cloud Computing fino ai dispositivi connessi alla rete – stanno diventando sempre più indispensabili e gli hacker che prendono di mira questo settore stanno evolvendo le loro tecniche di attacco. Di conseguenza, la cybersecurity svolge ora un ruolo ancora più importante nell'erogazione delle cure mediche ai pazienti.

"Una cybersecurity inefficace è un pericolo evidente e tangibile per la sicurezza dei pazienti. Gli incidenti informatici possono causare seri disagi per le strutture medico-sanitarie e indirettamente possono persino contribuire al deterioramento della salute dei pazienti."

Institute of Global Health Innovation, Imperial College London

La pandemia da COVID-19 ha accelerato il processo di adozione di tecnologie digitali per la sanità, come ad esempio soluzioni di monitoraggio remoto dei pazienti, visite online e dispositivi medici a uso domestico. Inoltre, ha portato a un incremento del personale in Smart Working. Se da un lato i risultati di questi cambiamenti hanno portato a miglioramenti significativi ed a lungo termine, dall'altro hanno anche aumentato i rischi alla sicurezza informatica affrontati dai team tecnici che operano in questo settore.

"(I criminali informatici) cercano di approfittare del fatto che la digitalizzazione della sanità diventerà sempre più importante in futuro."

John Noble, Chair, Information Assurance and Cyber Security Committee, NHS Digital

Le sfide alla cybersecurity per il settore sanitario

Da un sondaggio condotto da Sophos nel 2021 a cui hanno partecipato 328 IT Manager operanti nel settore sanitario, è emerso che, occuparsi della cybersecurity sta diventando un compito sempre più arduo. Il 63% degli intervistati sostiene che il numero di attacchi informatici che hanno subito è salito, almeno in parte, a causa di cybercriminali senza scrupoli che hanno approfittato della pandemia per sferrare i loro attacchi. Di conseguenza, probabilmente non sorprende che, il 70% dei partecipanti al sondaggio abbia dichiarato che il carico di lavoro è molto aumentato nel corso del 2020.

Non è solo il volume degli attacchi ad aumentare, ma anche la loro complessità. Il 60% degli intervistati ammette che gli attacchi informatici sono ora troppo avanzati per essere affrontati dalla propria squadra tecnica, senza un aiuto esterno.

63%
Percentuale che ha notato un aumento degli attacchi informatici nel 2020

60%
Percentuale secondo cui gli attacchi informatici sono troppo avanzati per essere affrontati dal proprio team tecnico, senza un aiuto esterno

70%
Percentuale che ha osservato un aumento del carico di lavoro nel 2020

La complessità è acerrima nemica della sicurezza

Nelle organizzazioni che operano nel settore sanitario, la proporzione tra utenti e personale IT è più alta rispetto alla media. Più un'infrastruttura è complessa, più è difficile da tenere aggiornata, soprattutto quando i responsabili tecnici sono oberati di lavoro. Inoltre, è anche molto più complicato utilizzare tutte le opzioni di protezione disponibili.

Sophos: protezione per il settore sanitario

Sophos collabora con organizzazioni operanti nel settore sanitario in tutto il mondo, per aiutarle a superare le loro sfide di sicurezza e per garantire che siano in grado di erogare cure mediche ai pazienti senza alcuna interruzione. Di fronte a questi attacchi sempre più frequenti e sofisticati, le nostre soluzioni aiutano a mantenere protetti sia la vostra organizzazione che i vostri dati. Allo stesso tempo, riducono il carico di lavoro per il personale IT, liberandolo da diverse mansioni di cybersecurity. Proseguite con la lettura per scoprire in maniera dettagliata come possiamo risolvere le più comuni sfide di cybersecurity affrontate dalle organizzazioni del settore sanitario.

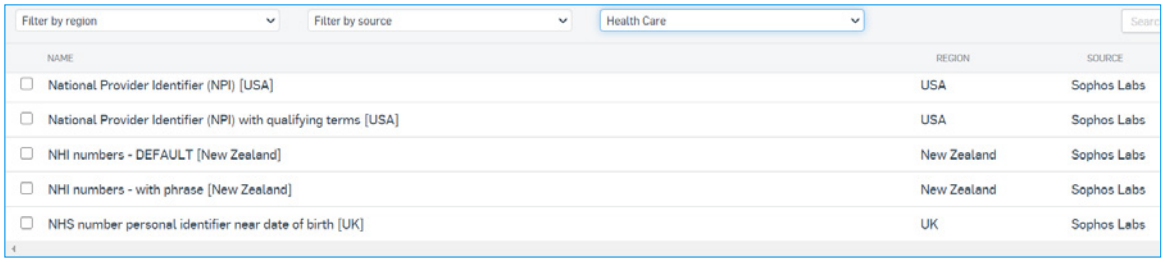
Protezione dei dati sensibili, ovunque si trovino

Le organizzazioni del settore sanitario custodiscono diversi tipi di dati di natura sensibile, da cartelle cliniche e tessere sanitarie, fino a informazioni che possono portare all'identificazione personale (PII). A causa della natura diversificata dei dati sensibili trattati da un'organizzazione del settore della sanità e dalle multiple modalità di conservazione e utilizzo di tali dati, proteggerli può essere un compito arduo.

Gli strumenti di protezione preventiva e proattiva di Sophos garantiscono la massima sicurezza per l'intera rete della struttura sanitaria, incluso ogni singolo dispositivo.

Protezione del dispositivo o del workload su cui sono memorizzati i dati

Sophos Intercept X, una soluzione di protezione per endpoint e server, implementa livelli di sicurezza multipli per proteggere i dati sui computer Windows, Mac, Linux e sulle virtual machine. Le regole di protezione contro la perdita dei dati appositamente sviluppate per il settore della sanità utilizzano termini e tipi di dati medico-sanitari per elevare la protezione.



Sophos Device Encryption offre un modo rapido e semplicissimo per garantire la cifratura dei dispositivi Windows e macOS, proteggendo i dati (e dimostrando la conformità alle normative) in caso di furto o smarrimento.

Protezione della rete utilizzata per trasmettere e ricevere dati

Sophos Firewall sfrutta tecnologie di rilevamento delle minacce basate sull'Intelligenza Artificiale per impedire che gli attacchi colpiscano i dati sanitari di natura sensibile, i sistemi medici essenziali per l'organizzazione e altri componenti dell'ecosistema informatico.

Blocco della fuga accidentale o deliberata dei dati tramite e-mail

Sophos Email cifra le informazioni che possono portare all'identificazione personale, le cartelle cliniche dei pazienti, le immagini mediche e altri dati di natura sensibile, prevenendo sia le violazioni accidentali dei dati, sia quelle intenzionali.

Controllo dell'accesso ai dati

Sophos Zero Trust Network Access (ZTNA) garantisce controllo assoluto sui dati presenti nella rete e su chi può accedervi. I controlli granulari bloccano i movimenti laterali e fanno in modo che i dati di natura sensibile possano essere visualizzati solamente dal personale autorizzato.

Affrontare in maniera diretta il ransomware che colpisce il settore sanitario

Il ransomware diventa sempre più intelligente e problematico, e il settore sanitario è un bersaglio che offre grandi opportunità di lucro. Nel settore dell'Healthcare, il costo effettivo che comporta un attacco ransomware non è solo quello del riscatto. Il prezzo da pagare per la perdita dei dati dei pazienti, per i ritardi o per la cancellazione delle procedure mediche può essere enorme e semplicemente devastante. Gli strumenti proattivi di Threat Hunting e prevenzione delle minacce di Sophos evolvono continuamente per essere sempre un passo avanti rispetto ai ransomware e per proteggere dati e reti da questi attacchi.

Impedire al ransomware di tenere in ostaggio l'organizzazione

Sophos è fiera di essere leader mondiale per la protezione anti-ransomware per le organizzazioni.

Sophos Intercept X è il migliore sistema di protezione antiransomware per Endpoint e Server disponibile sul mercato. Include livelli di sicurezza multipli, per riconoscere e bloccare il ransomware in qualsiasi fase di attacco. Eccone alcuni:

- CryptoGuard, che ripristina automaticamente i file a uno stato sicuro se vengono cifrati da utenti non autorizzati
- Tecnologie di Deep Learning basate su Intelligenza Artificiale, per bloccare ransomware noti e sconosciuti
- Protezione antiexploit, che blocca le tecniche utilizzate dagli hacker per scaricare e installare ransomware
- Protezione essenziale basata sulle firme digitali, a cura dei SophosLabs

Sophos Managed Threat Response (MTR) è il nostro prodotto che offre il maggiore livello di protezione antiransomware, include opzioni proattive di threat hunting, rilevamento e risposta, fornite come servizio gestito e operativo 24/7, a cura di un team di esperti. Vegliamo sui vostri sistemi, anche quando dormite.

Sophos Rapid Response offre assistenza immediata in caso di attacco ransomware. Il servizio è disponibile anche per chi non è cliente Sophos. Il nostro team vi aiuta ad assumere rapidamente il controllo della situazione durante un attacco, per proteggere reti, applicazioni e dati, nonché per attenuare i danni e il disagio causato.

Accesso sicuro per gli utenti, ovunque essi si trovino

I professionisti sanitari (sia che si tratti di personale che lavora in ospedale, nelle comunità o da casa) hanno bisogno di poter accedere in qualsiasi momento ai dati di natura sensibile dei pazienti e ai sistemi informatici sanitari essenziali. Gli strumenti Sophos permettono agli utenti del settore sanitario di connettersi in maniera sicura da qualsiasi luogo, senza incidere negativamente sulle loro mansioni di vitale importanza.

Permettere agli utenti di connettersi in maniera sicura da qualsiasi luogo

Sophos Firewall offre connessioni sicure per Windows e macOS con Sophos Connect VPN, che è disponibile gratuitamente. È facile da implementare e da configurare e garantisce accesso sicuro alle risorse situate nella rete o nel cloud pubblico per gli utenti che lavorano da remoto su dispositivi Windows e macOS. Conta oltre 1,4 milioni di client attivi, per cui avete la certezza di essere in buona compagnia.

La realtà del ransomware nel settore della sanità

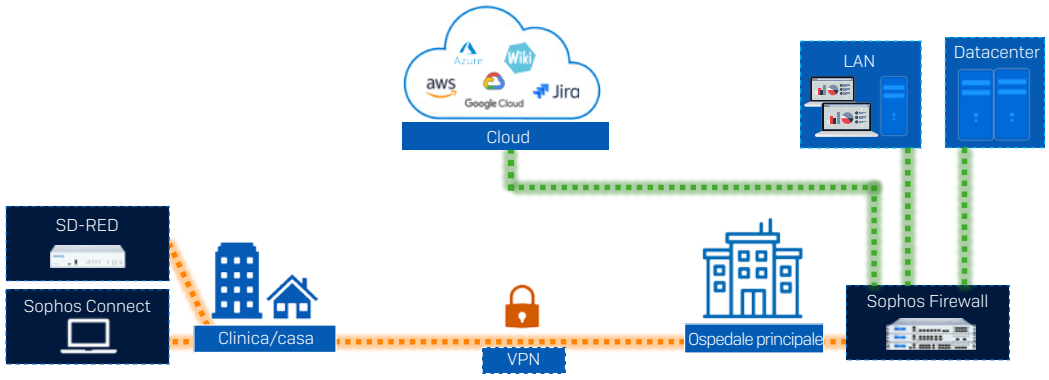
Il 34% delle organizzazioni è stato colpito dal ransomware l'anno scorso

Il 65% degli attacchi è risultato nella cifratura dei dati

Il 34% delle organizzazioni ha pagato il riscatto

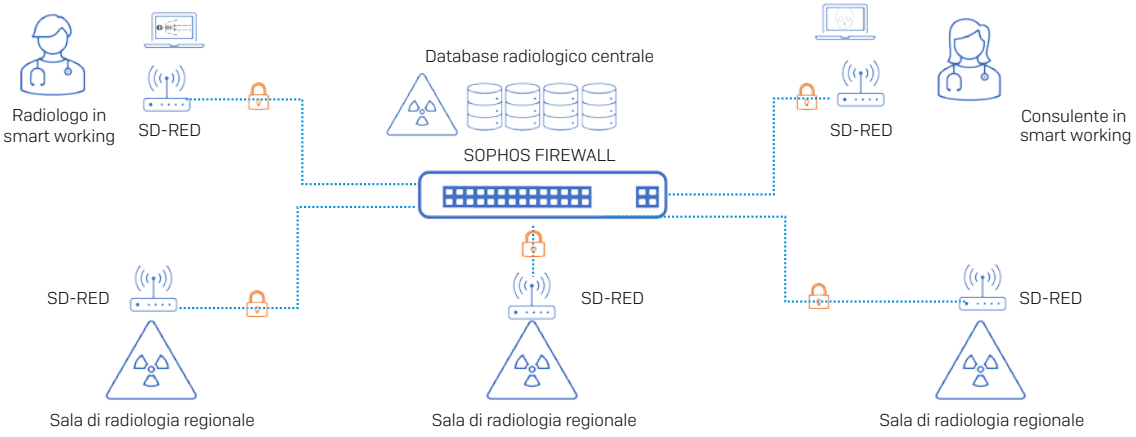
1,27 Milioni $: costo medio di riparazione dei danni

La Vera Storia Del Ransomware 2021, Sophos



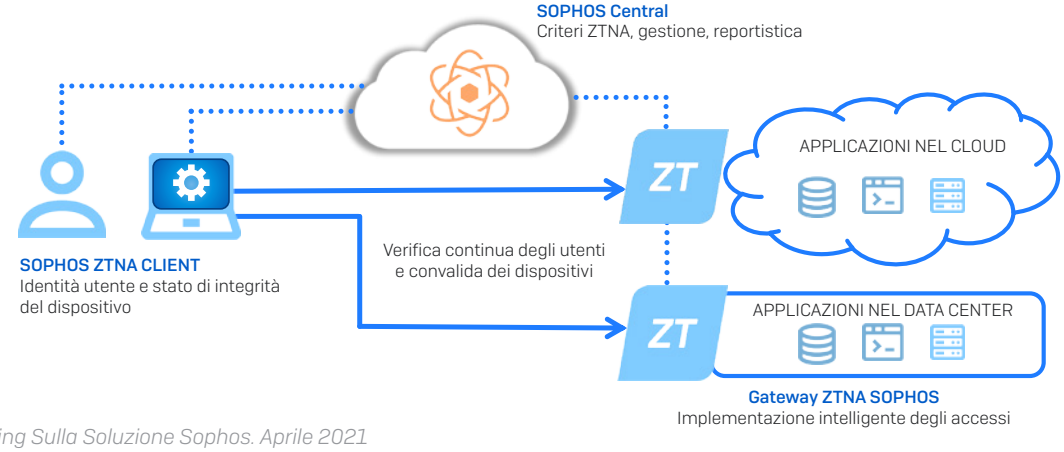
Sophos Firewall abilita l'accesso remoto sicuro con Sophos Connect Client e i dispositivi SD-RED

Per la protezione definitiva della connettività remota, **SD-RED** (Remote Ethernet Device) è un dispositivo plug-and-play di piccole dimensioni, che agisce insieme a **Sophos Firewall** per connettere sedi remote e singoli dipendenti alla rete principale. È la soluzione ideale per le cliniche locali e le sale mediche, nonché per le persone che hanno accesso a dati di natura estremamente sensibile.



Esempio di utilizzo di Sophos Firewall ed SD-RED per la radiologia

Per un accesso sicuro di ultima generazione, **Sophos Zero Trust Network Access** incentra la strategia di difesa sull'identità, convalidando continuamente utenti e dispositivi e verificando la conformità ai criteri. Offre agli utenti un'esperienza priva di complicazioni e allo stesso tempo permette al personale tecnico di concedere rapidamente l'accesso alle risorse ai nuovi utenti.



Aumentare la capacità di azione del personale IT

Nel 2020 abbiamo condotto un sondaggio a cui hanno partecipato 5.000 IT Manager che operano in settori diversi, incluso quello sanitario. L'81% degli intervistati sostiene che trovare e mantenere alle dipendenze professionisti IT qualificati è una delle sfide principali per la protezione informatica della propria organizzazione.

Sia che desideriate aggiungere competenze tecniche o ampliare le risorse a vostra disposizione, i professionisti Sophos possono agire come un'estensione del vostro team, per garantire la protezione 24/7 dei sistemi informatici sanitari e dei dati dei pazienti.

Un team dedicato di esperti di cybersecurity, per aumentare la capacità di azione del personale IT

Sophos Managed Threat Response (MTR) è un team di esperti di Threat Hunting e risposta alle minacce che agisce come una vera e propria estensione del vostro team. Il personale IT operante nel settore sanitario è oberato di lavoro, ma il nostro servizio è in grado di offrire loro le capacità e le competenze tecniche aggiuntive di cui hanno bisogno per affrontare qualsiasi minaccia.

Il team Sophos MTR monitora il vostro ambiente 24/7, individuando proattivamente potenziali minacce e incidenti e confermandone la presenza. Se Sophos MTR nota elementi sospetti, contatta gli esperti in materia di malware dei SophosLabs per analizzare gli indicatori rilevati e dissipare ogni dubbio.

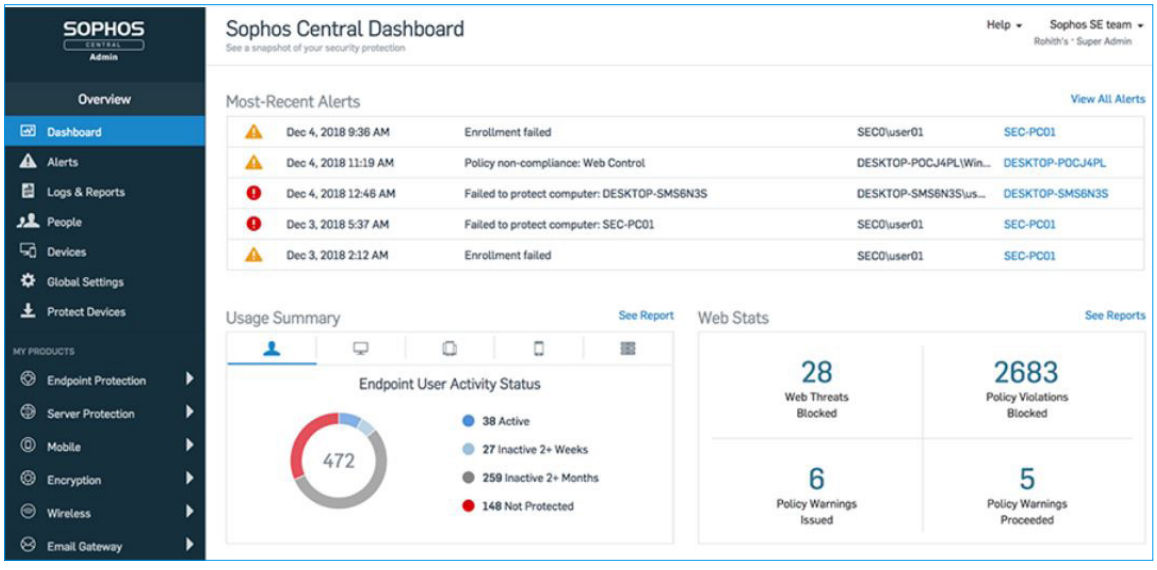
Inoltre, se desiderate, il team Sophos MTR può anche intraprendere un'azione di risposta per conto vostro. A differenza di altri servizi di rilevamento e risposta gestiti, i nostri esperti non si limitano a segnalare il problema, ma possono anche neutralizzare la minaccia per conto vostro. Sostanzialmente, siete voi a decidere il livello di intervento che desiderate da parte nostra e il modo in cui dobbiamo collaborare con il vostro team.

Meno tempo da investire nella gestione della cybersecurity

Quando le risorse IT sono limitate, diventa difficile passare al setaccio tutti gli avvisi di sicurezza per distinguere quelli più urgenti. Sophos aiuta a eliminare le informazioni superflue, grazie alla visualizzazione dell'intera infrastruttura di sicurezza da un'unica console e grazie a un livello di automazione che permette alle nostre soluzioni di risolvere i problemi prima che diventino causa di preoccupazione. In questo modo avrete più tempo per elaborare una strategia di massima efficacia.

Gestire la cybersecurity diventa più semplice

Sophos Central è la nostra piattaforma unificata e basata sul web per la gestione di tutti i prodotti di sicurezza Sophos. Ora non sarete più costretti a passare da una console a un'altra per proteggere la vostra organizzazione: Sophos Central semplifica l'implementazione e la gestione della sicurezza e permette di svolgere indagini su prodotti multipli, mettendo in correlazione le informazioni provenienti da tutti i servizi e visualizzandole in un'unica schermata.



L'intero sistema di cybersecurity viene gestito dalla piattaforma Sophos Central

Automazione della sicurezza

Sophos Central permette ai prodotti Sophos di condividere le informazioni in maniera proattiva e di interagire in tempo reale per abilitare la risposta automatica agli incidenti. Questo livello di integrazione e automazione eleva la sicurezza e allo stesso tempo riduce il carico di lavoro dei team IT.

Esempio 1: risposta automatica agli incidenti

- Se Sophos Intercept X identifica una minaccia su un endpoint, lo comunica immediatamente a Sophos Firewall.
- Sophos Firewall isola automaticamente l'endpoint infetto dalla rete e dagli altri dispositivi sulla stessa LAN.
- Intercept X rimuove la minaccia e segnala a Sophos Firewall quando ha terminato il processo.
- Sophos Firewall ripristina immediatamente l'accesso alla rete.

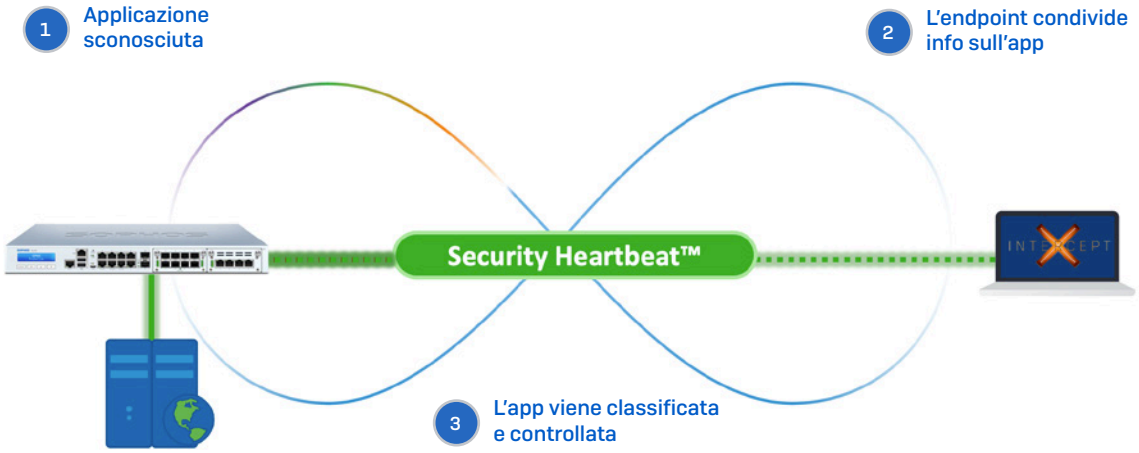
L'intero processo, che manualmente richiederebbe circa tre ore e mezzo, viene completato in meno di otto secondi.

Automazione della risposta agli incidenti

Esempio 2: identificazione di tutte le app indesiderate presenti nella rete

In media, il traffico di rete non identificato ammonta al 43%. A volte si tratta di applicazioni personalizzate che non hanno una firma standard. Altre volte si tratta di app che vogliono mascherare la propria identità dal firewall perché hanno intenzione di svolgere attività illecite.

- Se Sophos Firewall rileva un'applicazione che non trova corrispondenza con una firma nota, anziché assegnarla a un gruppo di traffico generico come "HTTPS", procede contattando Sophos Intercept X.
- Intercept X fornisce a Sophos Firewall il nome dell'applicazione, la patch e la categoria, per permetterne la classificazione. L'applicazione viene quindi assegnata automaticamente al giusto gruppo.
- Se per il gruppo sono previste misure di controllo (come ad esempio un blocco), verranno applicate le stesse regole. All'occorrenza, ad esempio nel caso delle app personalizzate, l'amministratore può impostare manualmente una categoria e un criterio da applicare.



Identificazione di tutte le app e tutti i processi presenti nella rete

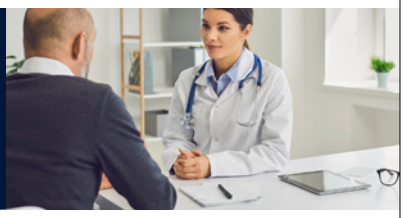
Ridurre il costo totale di proprietà negli ambienti reali

I vantaggi di un sistema di cybersecurity Sophos sono molteplici. La combinazione tra tecnologie di ultima generazione, funzionalità di risposta automatica agli incidenti, capacità di condividere informazioni in tempo reale e una piattaforma di gestione unificata ha un impatto enorme sia sulla protezione che sul costo totale di proprietà.

*I clienti che utilizzano Sophos Intercept X per gli Endpoint e Sophos Firewall sostengono che avrebbero bisogno del **doppio del personale per garantire gli stessi livelli di protezione**, se non avessero un sistema di cybersecurity Sophos. Inoltre, segnalano una diminuzione fino all'85% degli incidenti di sicurezza.*

CUSTOMER CASE STUDY **HEALTHCARE PROVIDER, U.S.**

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements
The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload
Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident
Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users
4,500 employees

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY **CLINICAL TRIALS PROVIDER, U.S.**

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.

Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements
Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue
Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification
Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior
As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users
150 employees across four locations

IT team
Two IT staff, covering all areas including cybersecurity

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

La certezza di una protezione efficace per professionisti sanitari che non si fermano un attimo

In un ambiente come quello della sanità, dove le pressioni sono molteplici, i rischi di errore umano sono e saranno sempre difficili da eliminare e da controllare. Sophos offre una rete di sicurezza indispensabile, per permettere ai professionisti sanitari di svolgere rapidamente il proprio lavoro senza doversi preoccupare della cybersecurity.

Blocco delle minacce, prima che possano raggiungere gli utenti

Possiamo aiutarvi ad alleggerire la pressione che grava sui vostri utenti (e di conseguenza anche sul personale IT) sia bloccando le minacce, sia impedendo che raggiungano gli utenti:

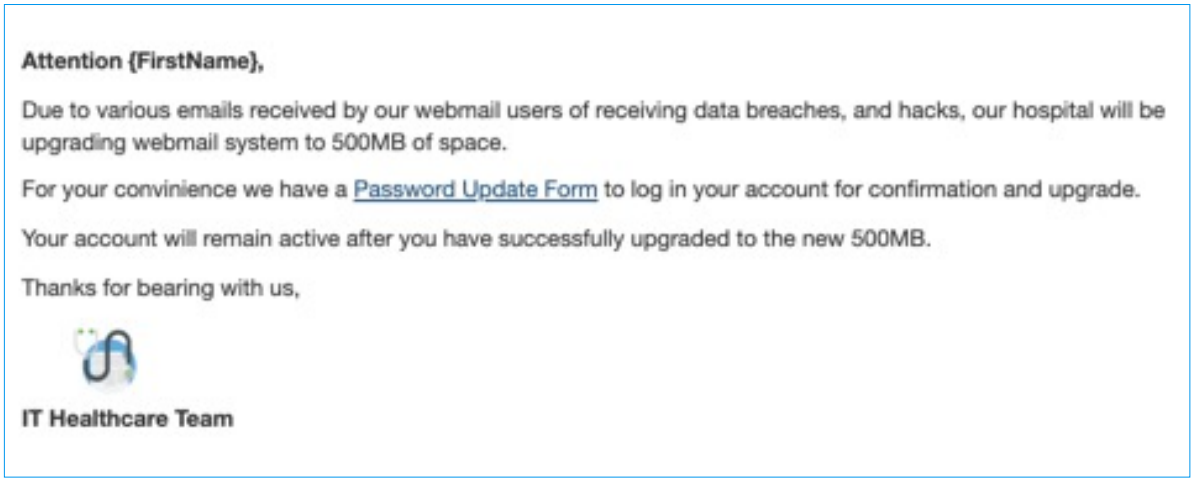
Intercept X with EDR offre la combinazione tra antiransomware, prevenzione degli exploit e rilevamento basato su Intelligenza Artificiale, per bloccare le minacce in vari punti della catena di attacco. Gli utenti possono lavorare con tranquillità, nella consapevolezza di essere protetti dal migliore sistema di sicurezza endpoint in assoluto.

Sophos Email abilita la sicurezza predittiva e basata su Intelligenza Artificiale direttamente nella casella di posta in arrivo degli utenti. Identifica le e-mail pericolose e le rimuove automaticamente prima ancora che gli utenti possano cliccare su un link sospetto.

L'ecosistema di cybersecurity Sophos permette ai prodotti Sophos di interagire reciprocamente per rispondere in maniera automatica alle minacce, bloccandole e rimuovendole in pochi secondi.

Formazione per gli utenti, per educarli a riconoscere le minacce

Sophos Phish Threat aiuta gli utenti a identificare le e-mail pericolose, con messaggi di posta che simulano un attacco di phishing e con corsi di formazione on-line. Potete inviare i corsi di formazione agli utenti che ne hanno maggiormente bisogno, in base alla natura del ruolo che svolgono nell'organizzazione o secondo il risultato che ottengono durante le simulazioni di attacco.



Attention {FirstName},

Due to various emails received by our webmail users of receiving data breaches, and hacks, our hospital will be upgrading webmail system to 500MB of space.

For your convinience we have a Password Update Form to log in your account for confirmation and upgrade.

Your account will remain active after you have successfully upgraded to the new 500MB.

Thanks for bearing with us,

IT Healthcare Team

Esempio di e-mail di simulazione di phishing in Sophos Phish Threat

L'importanza di scegliere una sicurezza che non rallenta le strutture sanitarie

Se il funzionamento e la rapidità dei sistemi è importante per qualsiasi settore, in quello sanitario è di vitale importanza. Per questo motivo molti utenti del settore della sanità installano app che non sono approvate, nel tentativo di semplificare le proprie mansioni lavorative. Questa consuetudine espone la rete e i dati a rischi molto pericolosi. Sophos aiuta a risolvere il problema dello shadow IT senza interferire con le normali attività lavorative di ogni giorno.

Una protezione avanzata che garantisce il funzionamento dei sistemi

Intercept X with EDR protegge gli endpoint e i server, impedendo alle minacce di interferire con il lavoro degli utenti. Le funzionalità EDR consentono di eseguire query da remoto sui dispositivi degli utenti e all'occorrenza di intraprendere azioni correttive.

Sophos Firewall mantiene la rete al sicuro dalle minacce e semplifica l'assegnazione della giusta priorità al traffico di rete attendibile, per garantire l'esecuzione ininterrotta dei processi critici. Inoltre, offre visibilità e controllo sullo shadow IT, poiché consente di identificare e bloccare le attività che potrebbero mettere a repentaglio l'organizzazione.

I prodotti Sophos sono efficaci da soli, ma diventano ancora più potenti quando vengono utilizzati insieme. Come abbiamo visto, Sophos Intercept X e Sophos Firewall interagiscono reciprocamente per avviare una risposta automatica alle minacce e incrementare il livello di visibilità.

Protezione delle tecnologie obsolete

Una delle principali sfide segnalate dalle organizzazioni del settore sanitario è quella di dover proteggere apparecchiature non aggiornate. Spesso questi dispositivi sono dotati di sistemi operativi obsoleti che non possono essere aggiornati a causa di problemi normativi, ma che devono comunque rimanere connessi alla rete. Se un dispositivo non può ricevere patch, aggiornamenti e non utilizza una soluzione antivirus o antimalware supportata, occorre cercare una soluzione fisica.

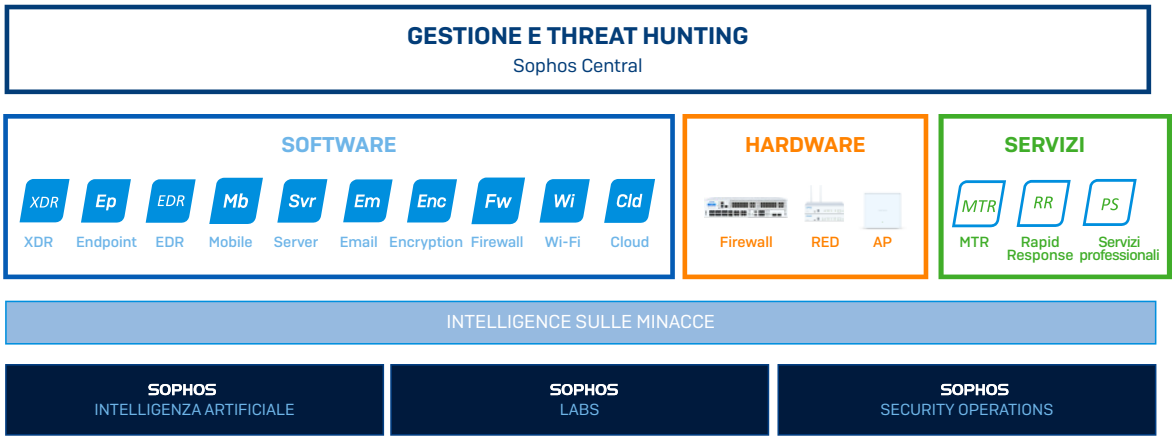
Sophos Firewall ed **SD-RED** (Remote Ethernet Device) sono le soluzioni ideali in queste situazioni. Proteggendo le connessioni del dispositivo a rischio con un SD-RED, è possibile reindirizzare l'intero traffico su un Sophos Firewall, che può effettuarne la scansione. Se la rete è semplice, saranno probabilmente necessarie alcune modifiche agli schemi di indirizzi IP e potenzialmente un cambiamento della topologia. I nostri tecnici specializzati possono discuterne con voi e offrire consulenza su come procedere.

Protezione delle apparecchiature non aggiornate

Conclusione

Per proteggere gli ambienti IT del settore sanitario e i dati di natura sensibile in essi contenuti, occorre una sicurezza a livelli multipli. Implementando una protezione intelligente in ogni punto vulnerabile (dalle reti fino ai dati), è possibile difendere i sistemi, il personale e i pazienti da rischi interni ed esterni.

Tutte le soluzioni Sophos fanno parte del nostro ecosistema di cybersecurity adattiva. Sono eccezionali quando vengono implementate da sole (molte organizzazioni cominciano con un solo prodotto) e danno risultati ancora migliori quando vengono utilizzate insieme. Con la crescita dell'infrastruttura informatica di Sophos, aumentano anche i vantaggi di un ecosistema integrato: condivisione delle informazioni, gestione centralizzata da un'unica console, risposta automatica agli incidenti, analisi approfondite. Tutte queste funzionalità interagiscono reciprocamente per elevare ulteriormente il livello di protezione, incrementando allo stesso tempo l'efficienza del team IT.



Protezione per il settore della sanità: l'ecosistema di cybersecurity Sophos

Per scoprire di più sulla protezione Sophos per le organizzazioni del settore sanitario e per discutere dei vostri requisiti, potete rivolgervi al vostro commerciale di riferimento Sophos o richiedere di essere contattati dai nostri specialisti di sicurezza.

Inviate una richiesta di contatto oggi stesso e i nostri specialisti di sicurezza contatteranno al più presto

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.

05/05/2021 (SB-NP)

SOPHOS