SOPHOS

CYBERSECURITY EVOLVED: L'IMPATTO DI SOPHOS SUL BUSINESS

Una quantificazione dei vantaggi tangibili del sistema di cybersecurity Sophos in termini di protezione ed efficienza, mediante l'analisi dei case study di cinque clienti

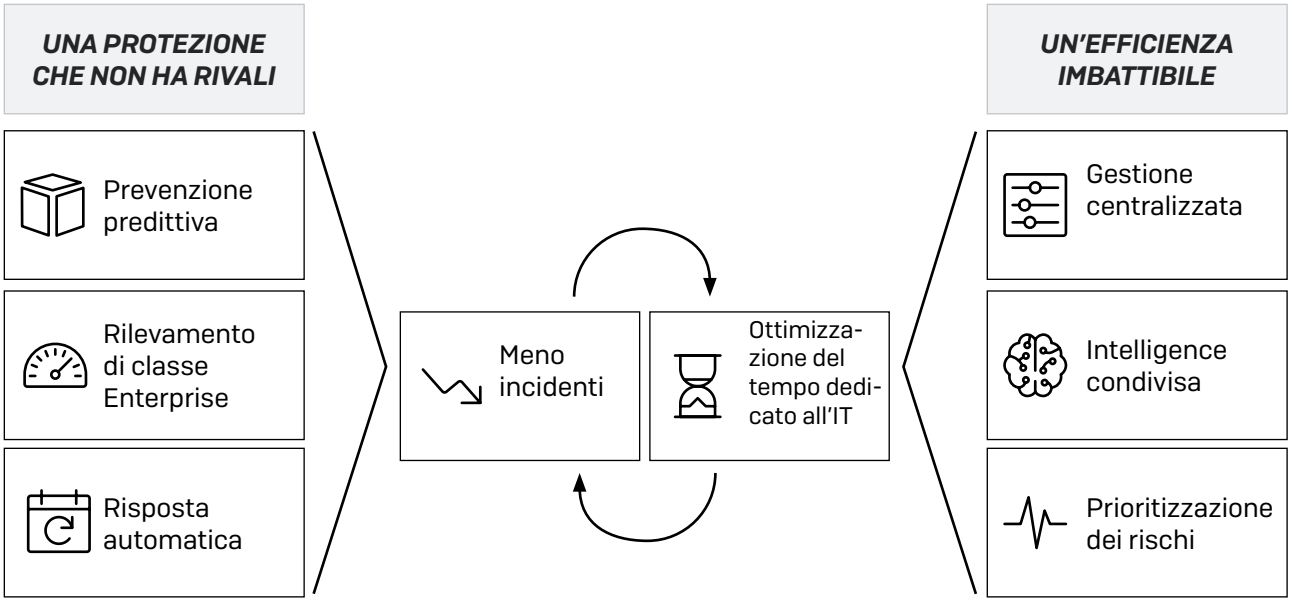
Whitepaper Sophos giugno 2020

Introduzione

Scegliere Sophos per la protezione contro le minacce significa poter usufruire del primo sistema di cybersecurity in assoluto, nonché del migliore:

- **Una gamma completa di prodotti e servizi next-gen.** Offriamo assistenza in tutti gli ambiti della cybersecurity: protezione endpoint, dispositivi mobili e server, EDR, firewall next-gen, e-mail, Unified Endpoint Management e molto altro ancora. Sia che si tratti di distribuzioni solo cloud, ibride oppure on-premise, le nostre soluzioni garantiscono massima sicurezza su tutti i fronti.
- **Protezione imbattibile.** Tutti i vantaggi delle tecnologie più all'avanguardia, insieme alle competenze di fama internazionale dei nostri team di esperti di data science e threat hunting, e dei SophosLabs. Il rilevamento di classe Enterprise blocca i moderni attacchi avanzati, mentre le reti neurali di deep learning basate su intelligenza artificiale bloccano predittivamente anche le minacce mai osservate prima. Inoltre, i prodotti Sophos interagiscono reciprocamente in tempo reale per incrementare ulteriormente la protezione. Condividono informazioni sulle minacce e sullo stato di integrità e sicurezza del sistema, rispondendo automaticamente agli incidenti.
- **Piattaforma di gestione unica.** Tutte le soluzioni di protezione Sophos vengono gestite da Sophos Central, la nostra piattaforma di gestione basata sul cloud, che sfrutta dati di intelligence condivisi per formulare informazioni sui rischi, organizzate in ordine di priorità; allo stesso tempo, le indagini guidate offrono consigli utili sulle azioni da intraprendere in qualsiasi situazione.

Il sistema di cybersecurity Sophos **eleva la protezione**, pur **riducendo il costo totale di proprietà (Total Cost of Ownership, TCO)**. Raggiunge questo obiettivo creando un circolo virtuoso, costituito da una protezione che non ha rivali e da un'efficienza imbattibile: due elementi che continuano a potenziarsi a vicenda.



Questo circolo virtuoso permette di incrementare significativamente l'efficienza del personale tecnico e di ridurre il rischio di esposizione alle minacce, tutto senza dover assumere altro personale.

L'impatto sui clienti

Per quantificare l'impatto del sistema di cybersecurity Sophos negli ambienti live dei clienti, abbiamo intervistato cinque clienti Sophos in Nord America, Europa e Asia. I clienti presentano scenari diversi, caratterizzati da strutture organizzative, sfide e requisiti aziendali eterogenei. Tuttavia, è emerso che avevano tutti un aspetto comune molto importante:

*I clienti hanno dichiarato che, senza un sistema di cybersecurity Sophos next-gen, avrebbero bisogno del **doppio** del personale di sicurezza attuale per mantenere gli stessi livelli di protezione.*

Hanno anche aggiunto che, grazie alle nostre soluzioni, hanno riscontrato meno incidenti di sicurezza e che sono in grado di identificare e rispondere più rapidamente ad eventuali problemi. I risultati derivati dall'utilizzo delle soluzioni Sophos includono:

- Una riduzione del 50% dei costi legati all'assunzione di personale di IT security
- Una riduzione di più del 90% del tempo trascorso a svolgere normali mansioni amministrative quotidiane di cybersecurity
- Una riduzione di più del 90% del tempo necessario per identificare i problemi
- Una riduzione dell'85% del numero di incidenti di sicurezza
- Un calo significativo dei tempi di inattività all'interno dell'intera organizzazione

Cliente A: settore sanitario, Stati Uniti

- 4.500 dipendenti
- 80 tecnici informatici, 3 dei quali addetti alla cybersecurity
- Prodotti Sophos: Intercept X Advanced with EDR, XG Firewall, Intercept X for Server Protection (Windows, Linux e virtual machine)

Il Cliente A opera nel settore della sanità a livello locale e offre servizi che includono assistenza di pazienti ospedalizzati e ambulatoriali, studi medici, RSA e un'ampia gamma di servizi specialistici.

Impatto sul business

- **Una riduzione del 50% delle risorse umane necessarie per gestire l'IT security**
  Il cliente ha già alle proprie dipendenze tre responsabili di cybersecurity. Ha calcolato che, se non utilizzasse soluzioni Sophos, avrebbe bisogno di assumere altre tre analisti di sicurezza a tempo pieno, dedicati esclusivamente alla risposta agli incidenti.

  Prima di Sophos, il team doveva svolgere un'enorme quantità di operazioni manuali per scoprire quello che accadeva nelle reti e trascorreva gran parte del tempo a identificare gli incidenti. Grazie a Sophos, ora i problemi vengono identificati proattivamente e risolti automaticamente nel 95% dei casi. Di conseguenza, il team si può dedicare al rimanente 5% dei casi che richiedono intervento manuale.

- **Una riduzione di più del 90% delle normali mansioni amministrative quotidiane di cybersecurity**
  I responsabili di IT security dedicano 30 minuti al giorno all'analisi dei log e all'indagine di eventuali elementi sospetti. Prima di Sophos, dovevano investire un'intera giornata per ottenere le stesse informazioni e lo stesso livello di accuratezza. Con Sophos, tutti i dati vengono consolidati in un'unica piattaforma di gestione e presentati in un formato coerente, per semplificare l'identificazione e la risposta ai problemi. In questo modo viene eliminato il laborioso compito di correlare i dati ottenuti da fonti diverse per contraddistinguere gli elementi innocui da quelli sospetti e da quelli malevoli.

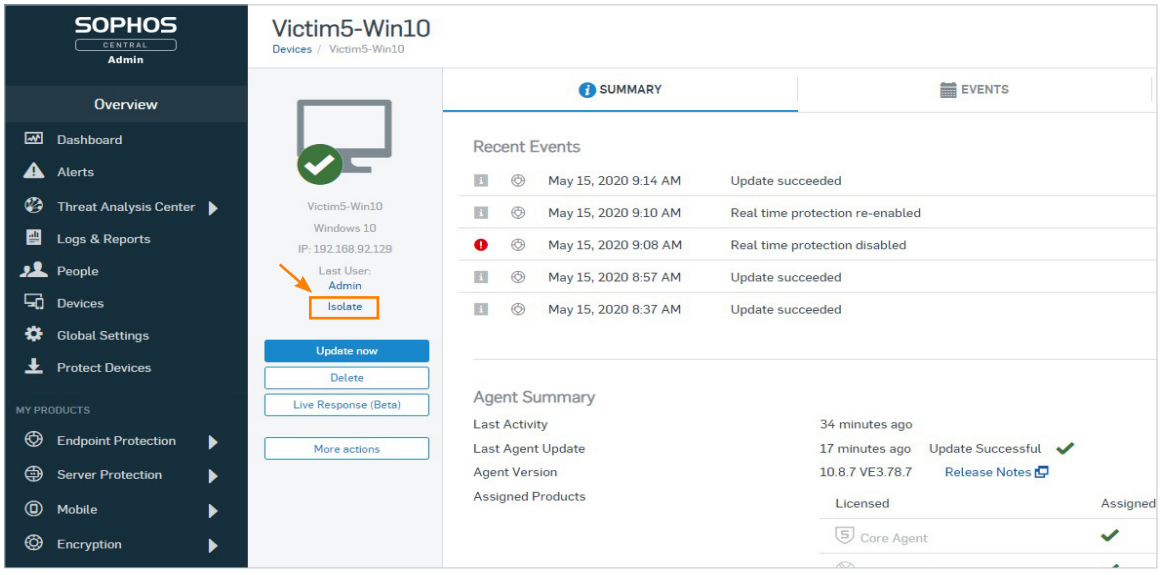
- **Una riduzione dell'85% del numero di incidenti di sicurezza**
  Come tutti gli ospedali, questo cliente conserva elevate quantità di informazioni personali (Personally Identifiable Information, PII) e coordinate di pagamento. Questa caratteristica lo rende un bersaglio molto desiderabile per i cybercriminali. Prima di Sophos, il cliente registrava una media di tre incidenti al giorno, su cui era necessario svolgere ulteriori indagini. Con Sophos, questa statistica è diminuita a un incidente ogni tre giorni.

- **Una riduzione di più del 90% del tempo necessario per identificare i problemi**
  Prima di Sophos, svolgere un'indagine su un incidente richiedeva circa tre ore, incluso il tempo necessario per ottenere accesso locale al computer colpito. Ora occorrono al massimo 15 minuti e tutte le operazioni possono essere effettuate da remoto grazie alla piattaforma Sophos Central.

  In passato, il team doveva disattivare la scheda di rete e recarsi fisicamente nel luogo dove era situato il dispositivo per indagare sul problema, risolverlo e infine riconnettere manualmente il computer. Inoltre, doveva anche adattarsi al flusso di lavoro degli utenti. Doveva, ad esempio, attendere la fine del trattamento di un paziente prima di poter accedere al sistema interessato per svolgere azioni di correzione. La possibilità di isolare il dispositivo dalla console di Sophos Central permette al team di indagare sul problema da remoto, senza ripercussioni sugli utenti e sulla disponibilità del sistema.

  La riduzione dei tempi di indagine e la capacità di gestire l'intero sistema da remoto limita le interruzioni del servizio anche per altri utenti che si trovano all'interno dell'ospedale.

- **Protezione ininterrotta durante le indagini**
  In passato, per svolgere indagini sui dispositivi occorreva rimuoverli dalla rete, impedendo così che ricevessero aggiornamenti della protezione mentre si trovavano off-line. Con Sophos, i dispositivi che vengono isolati dal team IT a scopo di indagine rimangono on-line e continuano a ricevere aggiornamenti della protezione.



Cliente B: settore dell'istruzione, India

- 700 dipendenti
- Sede principale a Bangalore, con responsabili locali situati su tutto il territorio dell'India e nella regione del Sud Est Asiatico
- Prodotti Sophos: Intercept X Advanced with EDR, Intercept X Advanced for Server, XG Firewall

Il Cliente B fornisce servizi formativi a istituti di formazione superiore e università situati su tutto il territorio dell'India e nella regione del Sud Est Asiatico. Questo cliente protegge decine di migliaia di studenti grazie a un team centralizzato di tecnici informatici nella sede principale di Bangalore e un team di responsabili IT locali presso gli uffici dei clienti.

Impatto sul business

- **Riduzione del 50% delle risorse umane necessarie per svolgere le normali mansioni di sicurezza quotidiana**
  In passato, il cliente aveva alle dipendenze quattro tecnici per le mansioni di sicurezza quotidiana. Dopo essere passato a Sophos, i tecnici necessari per gestire la sicurezza dell'intera azienda sono scesi a due.
- **Riduzione del 94% del tempo necessario per identificare gli elementi ad alto rischio che richiedono ulteriore indagine**
  Prima di Sophos, al cliente occorrevano dalle tre alle quattro ore per identificare i problemi critici sui quali indagare ulteriormente. Ora con Sophos Central bastano 10-15 minuti per individuare le priorità nell'intera organizzazione.
- **Riduzione del 98% del tempo necessario per identificare l'origine di eventuale traffico malevolo rilevato sulla rete**
  Con la precedente implementazione di rete, ci volevano due giorni (e talvolta anche di più) per individuare i dispositivi connessi alla rete che erano causa di problemi di sicurezza o di performance. Ora in soli 15 minuti è possibile identificare con estrema precisione il problema e avviare azioni di risoluzione.
- **Riduzione del 95% dei tempi di gestione degli aggiornamenti del firmware**
  La precedente implementazione di rete generava anche rischi e problemi di disponibilità, in quanto ogni aggiornamento del software aveva una durata di 3-4 ore. Ora con Sophos gli aggiornamenti non richiedono che una decina di minuti ciascuno. Considerando una media di 20-25 aggiornamenti all'anno, il tempo risparmiato corrisponde a circa 75 ore per gli aggiornamenti (l'equivalente di quattro settimane di lavoro).

Cliente C: settore degli studi clinici, Stati Uniti

- 150 dipendenti in 4 sedi
- 2 tecnici informatici che gestiscono tutti gli aspetti, cybersecurity inclusa
- Prodotti Sophos: Intercept X Advanced with EDR, XG Firewall, Central Device Encryption

Il Cliente C è un'organizzazione del settore privato che fornisce dati sugli studi clinici essenziali per ottenere l'approvazione normativa per nuovi farmaci. A causa della natura della sua attività, questo cliente conserva elevate quantità di informazioni personali di natura sensibile.

Impatto sul business

- **Riduzione del 50% delle risorse umane necessarie per gestire la struttura informatica**Questo cliente affida la gestione di tutti gli aspetti informatici a un team composto da sole due persone. Attualmente questo team dedica un'ora al giorno al controllo dei log e all'indagine di eventuali cause di preoccupazione. Il cliente ci informa che, se dovesse passare a un'altra soluzione, avrebbe bisogno di assumere uno o due altri tecnici di sicurezza per gestire i log.

- **Riduzione del 33% del tempo necessario per risolvere un potenziale problema**
  In passato, quando un dispositivo presentava problemi di sicurezza, la soluzione era ricrearne l'immagine, con un processo che poteva richiedere da 90 minuti a due ore. Ora può semplicemente svolgere un'indagine approfondita sul sistema isolato, sfruttando il threat hunting per effettuare una scansione di sicurezza completa e correggere i problemi in circa un'ora, senza bisogno di ricreare l'immagine del dispositivo. Uno dei principali vantaggi dell'approccio Sophos per questo cliente è il livello di produttività che può raggiungere un utente appena terminate le attività di indagine, mentre in passato ricreare l'immagine del dispositivo richiedeva un notevole investimento di tempo anche per la riconfigurazione e la personalizzazione del computer.
- **Riduzione dell'88% del rischio di minacce, grazie alla maggiore rapidità di individuazione**
  Con il sistema di cybersecurity Sophos, il team dei responsabili tecnici è in grado di individuare i nuovi problemi e svolgere indagini entro pochi minuti dalla comparsa di un evento sospetto. Prima di Sophos, l'analisi dei log per identificare i problemi su cui indagare richiedeva un giorno intero. La riduzione dei tempi di risposta implica anche una notevole diminuzione dell'esposizione ai rischi.
- **Miglioramento nel comportamento degli utenti**
  Con Sophos, gli utenti sanno che il personale tecnico è in grado di risolvere problemi e incidenti con rapidità, senza tempi di inattività o lavoro extra. I responsabili IT dichiarano che, di conseguenza, gli utenti sono più propensi a segnalare problemi o preoccupazioni (ad es. se cliccano su un link malevolo in un'e-mail).

Cliente D: settore dei servizi pubblici, Serbia

- 300 dipendenti
- 10 tecnici informatici, 4 dei quali addetti alla cybersecurity
- Prodotti Sophos: Intercept X Advanced, Intercept X Advanced for Server, XG Firewall, Sophos Email, Sophos Mobile

Il Cliente D è un'organizzazione che opera nel settore dei servizi pubblici ed è situata nella capitale della Serbia: Belgrado. Questo cliente che si affida ai sistemi Sophos da vari anni ha appena completato la migrazione ai nostri prodotti next-gen con gestione da Sophos Central.

Impatto sul business

- **Riduzione del 50% del tempo trascorso a svolgere normali mansioni quotidiane di gestione della sicurezza**
  Adesso questo cliente dedica 30 minuti al giorno alla gestione della sicurezza, controllando avvisi, log, utenti, dispositivi, traffico e applicazioni dalla console di gestione di Sophos Central, per assicurarsi che non ci siano problemi. In passato, queste attività di gestione quotidiane richiedevano almeno il doppio del tempo per poter determinare i problemi a priorità più elevata da risolvere immediatamente e le azioni da intraprendere.
- **Riduzione di più del 90% del tempo trascorso a svolgere normali mansioni quotidiane di gestione della sicurezza rispetto ad altri vendor**
  Secondo il cliente, in base alle proprie esperienze passate, la gestione quotidiana della sicurezza richiederebbe un giorno intero con le soluzioni di altri vendor. Con Sophos, invece, servono solo 30 minuti.
- **Zero incidenti gravi di sicurezza**
  Il cliente adopera Sophos da diverso tempo e negli ultimi 8-10 anni non ha mai riscontrato un incidente grave di sicurezza. Questo non significa che sia immune alle minacce, ma piuttosto che i prodotti Sophos che utilizza sono in grado di risolvere le minacce rapidamente e in maniera invisibile in background, senza che l'utente se ne accorga.

Cliente E: ente di regolamentazione, Slovenia

- 150 dipendenti, un terzo dei quali in smart working, mentre gli altri due terzi sono situati nella sede centrale
- Due tecnici informatici che gestiscono tutti gli aspetti, cybersecurity inclusa, più il supporto di un provider esterno per progetti più onerosi
- Prodotti Sophos: Sophos Endpoint Protection, Intercept X Advanced for Server, XG Firewall, Sophos Mobile, Sophos Device Encryption

Il Cliente E è un'organizzazione che opera nel settore pubblico e si occupa di verificare che i prodotti soddisfino gli standard richiesti. Questo cliente che si affida ai sistemi Sophos da vari anni ha appena completato la migrazione ai nostri prodotti next-gen con gestione da Sophos Central.

Impatto sul business

- **Riduzione del 50% del tempo trascorso a svolgere normali mansioni quotidiane di gestione della sicurezza**
  Il cliente dedica 15-30 minuti al giorno all'amministrazione della sicurezza: verifica del firewall, analisi degli avvisi, disinfezione delle e-mail in quarantena, ecc. In passato, le stesse attività avrebbero richiesto il doppio del tempo. Questo aumento dell'efficienza deriva dal poter gestire tutti i prodotti di sicurezza da un'unica vista, senza bisogno di dover passare da una schermata all'altra per applicazioni e server.
- **Zero incidenti gravi di sicurezza**
  Il cliente non ricorda un singolo incidente grave di sicurezza da quando utilizza Sophos.

Conclusione

Come dimostrano le testimonianze dei clienti, l'approccio di Sophos alla cybersecurity garantisce una protezione tangibile, risparmi notevoli e massima efficienza. Permette di incrementare significativamente l'efficienza del personale tecnico e di ridurre il rischio di esposizione alle minacce, tutto senza dover assumere altro personale.

Sebbene caratterizzati da ambienti aziendali, risorse e sfide molto diverse a seconda dell'organizzazione, i nostri clienti segnalano costantemente workload dimezzati per la gestione della sicurezza, e questo è dovuto all'utilizzo dei sistemi di cybersecurity Sophos. Gli altri vantaggi per i nostri clienti includono un calo di più del 90% del tempo trascorso a svolgere normali mansioni amministrative quotidiane di cybersecurity e una diminuzione dell'85% del numero di incidenti di sicurezza.

Per maggiori informazioni sulle soluzioni di cybersecurity Sophos e per avviare una prova gratuita senza obbligo di acquisto, visitare www.sophos.it, o contattare un rappresentante commerciale Sophos.

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

200612 WPIT (NP)

SOPHOS