SOPHOS
Cybersecurity made simple.

I segreti dei firewall di rete

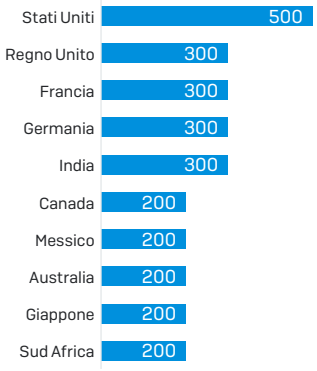
I risultati di un sondaggio indipendente, sponsorizzato da Sophos, a cui hanno partecipato 2.700 responsabili IT nelle organizzazioni di medie dimensioni.

Introduzione

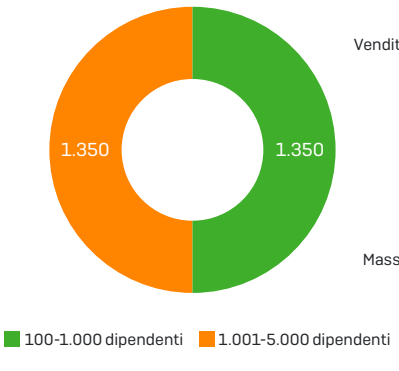
Verso la fine del 2017, Sophos ha sponsorizzato uno studio di ricerca indipendente sullo stato attuale della sicurezza della rete nelle organizzazioni di medie dimensioni in varie parti del mondo. Il programma di ricerca ha esplorato le esperienze, le preoccupazioni e le esigenze future dei responsabili IT, in particolar modo per quanto riguarda i sistemi di protezione firewall e le difese della rete.

Condotto dall'azienda britannica Vanson Bourne, leader nell'ambito della ricerca, il sondaggio ha coinvolto 2.700 responsabili IT nelle organizzazioni da 100 a5.000 utenti, situate in 10 paesi e 5 continenti.

Paese del partecipante



Dimensione dell'organizzazione



Settore dell'organizzazione

Il documento compilato con i dati ottenuti rivela gli attuali segreti dei firewall di rete, mettendo in luce i punti deboli delle organizzazioni negli ambiti principali di protezione, visibilità e risposta alle minacce, nonché l'impatto di queste mancanze sui responsabili IT in tutto il mondo.

SEGRETO 1

I FIREWALL NON SONO IN GRADO DI GARANTIRE LA PROTEZIONE DI CUI HANNO BISOGNO LE ORGANIZZAZIONI

Riepilogo

- Nelle organizzazioni, in media 16 computer al mese vengono colpiti da un'infezione.
  - Una media di 13 al mese per le organizzazioni con 100-1.000 utenti.
  - Una media di 20 al mese per le organizzazioni con 1.001-5.000 utenti.
- Il 79% dei responsabili IT vuole una protezione migliore dal proprio firewall.
- Una protezione più efficace è il miglioramento più desiderato da quasi la metà dei responsabili IT (il 48%).

Ormai è normale che ogni mese si verifichino infezioni diverse

Il firewall è il gateway situato tra rete aziendale e internet. Spesso funge anche da gateway tra aree diverse dell'ambiente informatico di un'azienda: ad es. reti perimetrali e server, segmenti diversi della LAN, reti wireless e zone attendibili e non attendibili. Insieme alla protezione endpoint, è uno dei pilastri dell'infrastruttura di sicurezza.

Grazie a questa funzione essenziale, è anche una prima e indispensabile linea di difesa contro le minacce. malwareBlocca queste minacce prima che riescano a intrufolarsi nella rete, impedendo loro di spostarsi lateralmente o di diffondersi nell'intero ambiente, come ad es. quando si trovano in un dispositivo USB infetto.

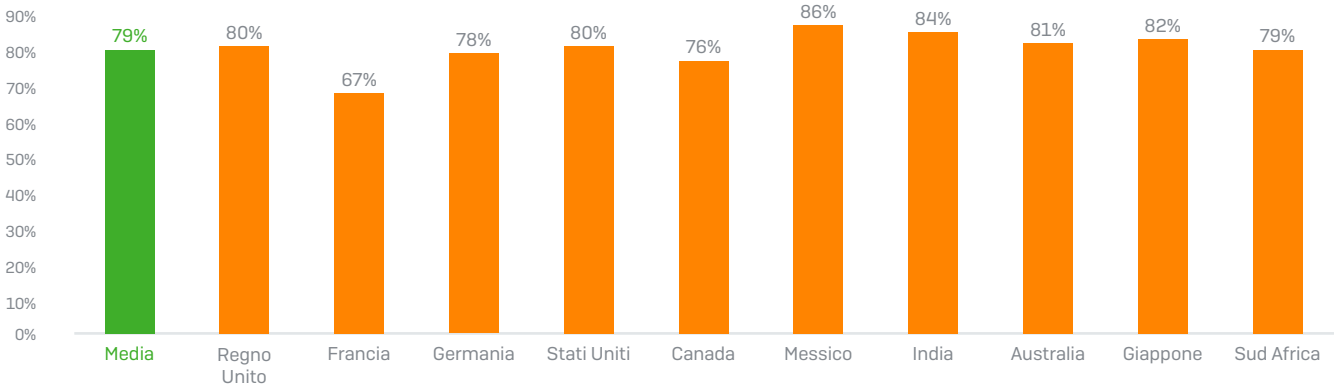
Nonostante l'importanza del suo ruolo all'interno dei sistemi di difesa contro le minacce, dal sondaggio è emerso che i firewall non sono in grado di fornire alle organizzazioni la protezione necessaria. Nelle organizzazioni, in media 16 computer al mese
vengono colpiti da un'infezione. Le organizzazioni più piccole (100-1.000 utenti) si trovano ad affrontare 13 computer infetti al mese, mentre le aziende più grandi(1.001-5.000 utenti) 20.

> **16** computer infettati al mese

Alla luce di queste infezioni continue, non sorprende che quasi quattro responsabili IT su cinque (il 79%) vogliano una protezione migliore dai propri firewall. Infatti, una protezione più efficace è il miglioramento più desiderato per quasi la metà dei responsabili IT (il 48%). Questo desiderio di una sicurezza migliore include sia la sicurezza del perimetro di rete,per tenere lontane le minacce, sia la protezione interna, per impedire a queste minacce di diffondersi, qualora dovessero riuscire a infiltrarsi.

L'inadeguatezza della protezione è, purtroppo, un problema a livello internazionale, in quanto almeno due terzi dei responsabili IT desiderano una protezione migliore in quasi tutti i paesi presi in esame.

% DI INTERVISTATI CHE DESIDERA UNA PROTEZIONE PIÙ EFFICACE DAL PROPRIO FIREWALL



SEGRETO 2

I RESPONSABILI IT NON SANNO COME VIENE UTILIZZATO IL 45% DELLA LARGHEZZA DI BANDA

Riepilogo

- In media, il traffico di rete non identificato ammonta al 45%. Di conseguenza, non può essere controllato.
- Quasi un responsabile IT su quattro (il 23%) non è in grado di identificare il 70% del traffico di rete.
- La mancanza di visibilità sul traffico di rete porta a preoccupazioni di vario genere:
  - L'84% nutre preoccupazioni sulla sicurezza.
  - Il 52% nutre preoccupazioni sulla produttività.
  - 4 su 10 nutrono preoccupazioni relative al non poter rendere conto di come viene utilizzata la larghezza di banda.
  - Il 42% nutre preoccupazioni sulla responsabilità legale o sulla conformità, per via deiproblemi che potrebbero sorgere da contenuti potenzialmente illegali o inappropriati.
  - Il 50% ha investito in app personalizzate a cui non si riesce ad attribuire la giusta priorità.
- Il settore della sanità è quello che riscontra il maggior numero di problemi relativi alle applicazioni personalizzate, in quanto due terzi (il 67%) dispongono di app personalizzate che non sono in grado di identificare.
- L'85% dei responsabili IT vuole dal firewall una migliore visibilità.

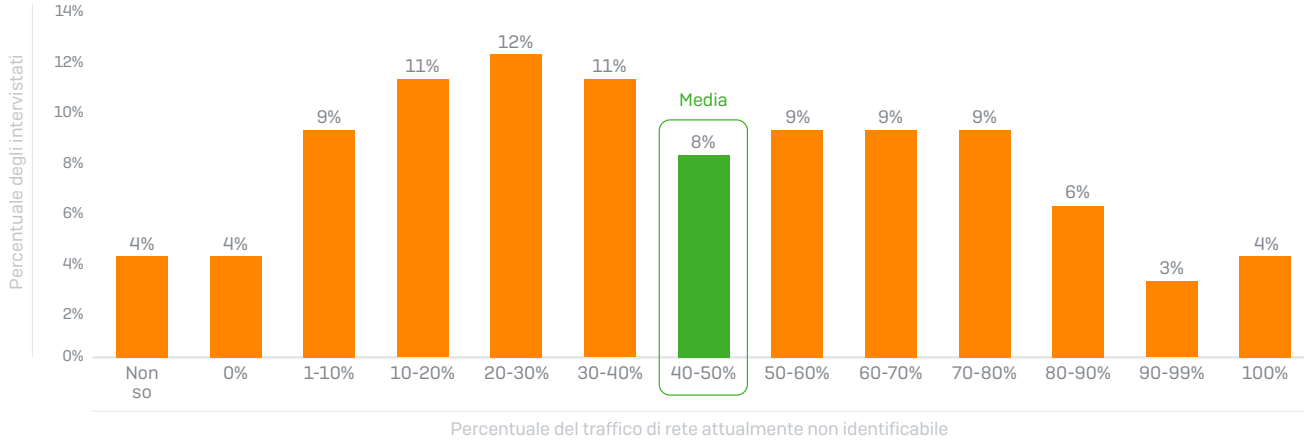
I problemi che non si notano sono impossibili da risolvere

Controllare il traffico di rete è una delle funzioni principali di qualsiasi firewall. Occorre attribuire priorità alle app essenziali, limitare le app che non rientrano nell'ambito di lavoro e bloccare app malevole come i client di BitTorrent.

Il problema è che non è possibile controllare ciò che si esegue di nascosto all'interno della rete.

Dal sondaggio è emerso che attualmente il 45% del traffico di rete non è identificabile, per cui non può essere controllato.

A quasi la metà del traffico non è possibile applicare il sistema definito come "controllo delle applicazioni". Inoltre, quasi un responsabile IT su quattro (il 23%) si trova ad affrontare un compito molto più arduo, con una percentuale del traffico di rete non identificabile pari o superiore al 70%.



QUALE PERCENTUALE DEL VOSTRO TRAFFICO DI RETE NON È ATTUALMENTE IDENTIFICABILE?

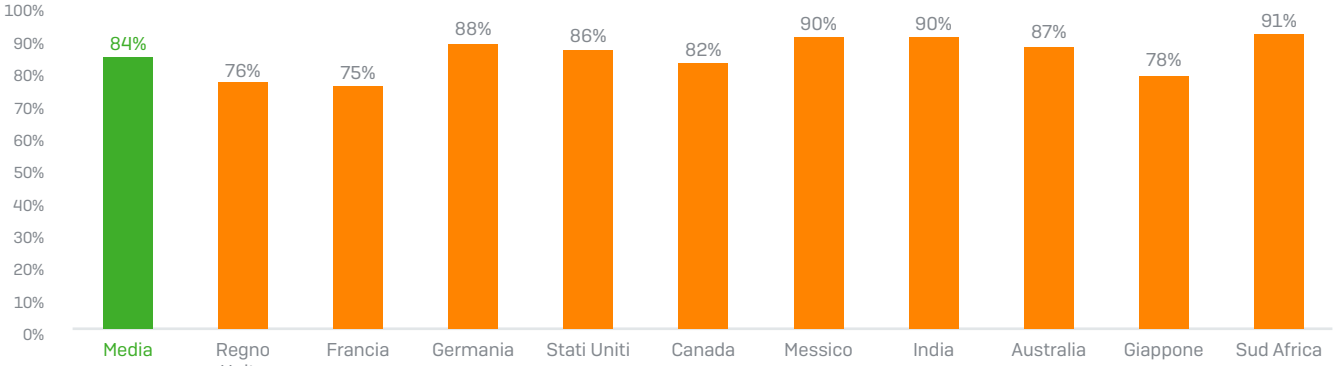
Ciò è dovuto al fatto che la maggior parte dei firewall convenzionali identifica le applicazioni affidandosi al rilevamento basato sulle firme, con lo stesso sistema utilizzato dai software antivirus tradizionali. Pertanto, le conseguenze sono le stesse dei sistemi AV tradizionali: in questo caso le applicazioni precedentemente inedite e non catalogate passano inosservate e, anche se hanno una firma, molte applicazioni fanno di tutto per modificare i propri pattern di rete per eludere il rilevamento. Inoltre, esistono molte applicazioni che si camuffano da browser web per evitare i controlli, in quanto quasi tutti i firewall autorizzano l'accesso a internet per la navigazione.

Analogamente alla mancanza di protezione, anche la scarsa visibilità è un problema diffuso in tutto il mondo: l'India è il paese maggiormente colpito, con una percentuale di traffico di rete non identificabile pari al 57%. Il Giappone invece è il paese che ne risente di meno, con un terzo del traffico di rete che non è identificabile. Questo risultato è dovuto a controlli dei criteri più severi, una propensione limitata a utilizzare applicazioni SaaS/cloud (che sono spesso cifrate) e una minore tendenza a utilizzare applicazioni non autorizzate.

La mancanza di visibilità porta a preoccupazioni di vario genere:

Sicurezza. Se non si conoscono gli elementi che si trovano all'interno della rete, com'è possibile sapere se siano malevoli, sospetti o ad alto rischio? E come si può capire se siano presenti utenti non autorizzati il cui comportamento mette a repentaglio l'organizzazione, esponendola a minacce di malware o a tentativi di violazione? Ecco perché la sicurezza è una preoccupazione per l'84% degli intervistati.

% DI INTERVISTATI CHE CONCORDA SUL FATTO CHE LA MANCANZA DI APPLICAZIONI EFFICACI È UNA SERIA PREOCCUPAZIONE PER LA SICUREZZA



Produttività. Se non si conoscono le attività che consumano la larghezza di banda, non sarà possibile attribuire la giusta priorità alle applicazioni mission-critical di produttività e non si sarà in grado di assegnare una priorità minore alle applicazioni che non sono necessarie per le operazioni lavorative. Inoltre, non si avranno informazioni dettagliate sulle app adoperate dagli utenti: la perdita di produttività dovuta ad app indesiderate o non essenziali rappresenta una preoccupazione per poco più della metà (il 52%) delle organizzazioni che hanno partecipato al sondaggio.

Responsabilità. Nell'era odierna, caratterizzata dall'onnipresenza di internet e dalla prevalenza di app basate sul cloud, la larghezza di banda è diventata sia una risorsa critica per le aziende sia una spesa notevole. Le organizzazioni esigono dal personale tecnico la prova di dove venga utilizzata questa risorsa preziosa, ma la mancanza di visibilità sul traffico di rete rende il tutto pressoché impossibile. Di conseguenza, in media, 4 responsabili IT su 10 nutrono preoccupazioni dovute al non essere in grado di giustificare il consumo della larghezza di banda.

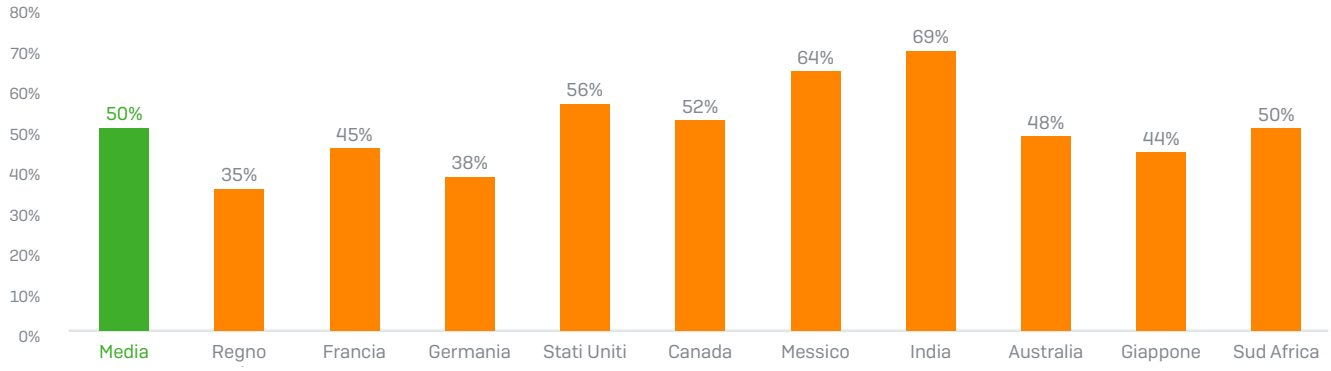
Il sondaggio ha rivelato variazioni regionali significative in termini di responsabilità. I responsabili IT in India (61%) e Sudafrica (55%) sono quelli che nutrono maggiori preoccupazioni a questo riguardo, mentre in Giappone (28%) e Germania (30%) si tende a preoccuparsi di meno. Probabilmente questi risultati riflettono le diverse pratiche commerciali in tutto il mondo, oltre alla divergenze di aspettativa in termini di aderenza alle politiche aziendali.

Responsabilità legale e conformità. Se da un lato i responsabili IT che hanno partecipato al sondaggio si trovano ad affrontare obblighi legali e requisiti di conformità diversi, dall'altro nutrono una preoccupazione comune: il rischio che gli utenti scarichino, ospitino o inviino contenuti illegali o inappropriati. In media, questa preoccupazione è comune al 42% degli intervistati, con India (52%) e Regno Unito (47%) in cima all'elenco. Se non riescono a visualizzare i programmi in esecuzione nella rete, i responsabili IT non possono garantire che tutte le attività siano legittime, il che espone le organizzazioni al rischio di una potenziale violazione della conformità.

Ritorno sull'investimento. Le applicazioni personalizzate aziendali o destinate al mercato verticale sono sempre più comuni e rappresentano un investimento notevole per qualsiasi azienda. Variano da programmi ottimizzati per soddisfare esigenze aziendali specifiche ad applicazioni realizzate su misura al 100% per una singola azienda. Dal sondaggio è emerso che il 50% delle organizzazioni utilizza applicazioni di rete personalizzate che il firewall non è in grado di identificare. Di conseguenza, è impossibile attribuirvi un grado di priorità, limitando così le possibilità di sfruttare il massimo potenziale dell'applicazione in termini di ritorno sull'investimento e di garantire che gli utenti possano lavorare al massimo dell'efficienza.

Il ritorno sull'investimento è un altro ambito in cui si notano oscillazioni di regione in regione. India, Messico e Stati Uniti hanno un numero di app personalizzate non identificabili superiore alla media, mentre il Regno Unito è in fondo all'elenco con appena il 35%. È probabile che questa variazione rifletta le diverse tendenze a investire in app personalizzate, piuttosto che in quelle preconfezionate, oltre ai problemi di visibilità.

% DI INTERVISTATI CHE HA APP PERSONALIZZATE CHE IL FIREWALL NON È IN GRADO DI IDENTIFICARE



Tutti i settori segnalano problemi relativi ad applicazioni aziendali personalizzate non identificabili, ma il settore sanitario è quello che ne risente di più. Due terzi delle organizzazioni che operano nel settore sanitario hanno applicazioni che i loro firewall non sono in grado di identificare e che quindi non possono essere controllate. Probabilmente ciò deriva dal fatto che le organizzazioni del settore sanitario hanno una maggiore tendenza a utilizzare applicazioni di rete personalizzate per soddisfare esigenze particolari. Un altro fattore potrebbero essere le infrastrutture obsolete.

L'85% concorda: la visibilità è una delle priorità principali

Come abbiamo già detto, i problemi che non si notano sono impossibili da risolvere. Ed è per questo motivo che l'85% dei responsabili IT esprime il desiderio comune di poter utilizzare firewall che garantiscano maggiore visibilità. Questa caratteristica permetterebbe loro di:

- **Ridurre i rischi di sicurezza**, grazie all'identificazione degli utenti e delle applicazioni a rischio.
- **Aumentare la produttività**, controllando il traffico delle applicazioni che non vengono utilizzate per lavoro.
- **Ottimizzare la larghezza di banda** per le attività dell'azienda.
- **Ridurre al minimo le preoccupazioni relative a responsabilità legali e rispetto della conformità**, bloccando i contenuti illegali o inappropriati.
- **Ottenere il massimo ritorno sull'investimento** per le applicazioni aziendali personalizzate.
- **Rendere conto** del traffico di rete.

> **L'85%** vuole dal firewall una migliore visibilità

SEGRETO 3

I FIREWALL INEFFICACI COSTANO TEMPO E DENARO

Riepilogo

- Occorrono in media 3,3 ore per identificare, isolare e applicare azioni correttive per i computer infetti.
- In media, le organizzazioni impiegano sette giorni lavorativi al mese a svolgere azioni correttive per i computer infetti.
  - Le organizzazioni di piccole dimensioni (100-1.000 utenti) trascorrono in media 5 giorni lavorativi a svolgere azioni correttive.
  - Le organizzazioni più grandi (1.001-5.000 utenti) trascorrono in media 10 giorni lavorativi a svolgere azioni correttive.
- Il 99% concorda che sarebbe utile avere un firewall in grado di isolare automaticamente i computer infetti.
- Il 97% dichiara che probabilmente acquisterebbe soluzioni di sicurezza per endpoint e firewall dallo stesso vendor, se ciò garantisse tassi di rilevamento più elevati e una migliore risposta automatica agli incidenti.

Più di una settimana al mese viene sprecata applicando azioni correttive per i computer infetti

Come abbiamo già visto, i firewall non sono in grado di garantire la protezione di cui hanno bisogno le organizzazioni.

Di conseguenza, i responsabili IT investono molto tempo e impegno in attività di correzione per i computer infetti.

Per determinare l'entità del problema, il sondaggio ha rivolto ai partecipanti due domande principali:

1. **Quanto tempo** vi occorre, in media, per identificare, isolare e applicare azioni correttive per i computer infetti?
2. In media, **con quanti** computer infetti ha a che fare la vostra organizzazione ogni mese?

I risultati sono stati sorprendenti.

In media occorrono 3,3 ore, ovvero quasi mezza giornata lavorativa, per identificare, isolare e applicare azioni correttive su un computer infetto. È interessante osservare che per le organizzazioni di piccole dimensioni i tempi sono stati minori rispetto alle aziende più grandi, con una media di 2,9 ore per le organizzazioni con 100-1.000 utenti, e 3,9 ore per le organizzazioni con 1.001-5.000 utenti.

> **7 giorni al mese** trascorsi a svolgere azioni correttive per i computer infettati (in base a una giornata lavorativa di 7,5 ore)

Nelle organizzazioni, in media 16 computer al mese vengono colpiti da un'infezione. Se si considera una giornata lavorativa di 7,5 ore, ciò significa trascorrere 7 giorni lavorativi al mese a svolgere azioni correttive per le infezioni.

Dimensioni dell'organizzazione	Nº di computer infettati al mese	Ore richieste per la disinfezione di un computer	Totale ore richieste per la disinfezione al mese	Nº di giorni al mese (7,5 ore = 1 giorno)
100 - 1.000	13	2,8	36,4	4,9
1.001 - 5.000	20	3,9	78	10,4
Media	16	3,3	52,8	7,04

Considerando cosa comporta rimediare ad un'infezione , occorre tenere in considerazione sia il tempo materiale e i costi in termini di risorse,sia le conseguenze finanziarie dovute alla perdita di opportunità: quali altre attività avrebbe potuto svolgere il personale tecnico, invece di queste? Il personale tecnico è sempre più oberato di lavoro, sia a causa delle necessità sempre maggiori in termini di tempo, sia per quanto riguarda la grave carenza di competenze tecniche nell'ambito della sicurezza informatica. Il 70% dei professionisti della sicurezza IT sostiene che nella propria azienda manchino competenze tecniche di cybersecurity[i]. Nella maggior parte dei casi, non ci si può permettere di trascorrere sette giorni al mese a risolvere i problemi dei computer infetti.

Date le implicazioni in termini di tempo e denaro derivate dalla disinfezione annuale dei computer, non sorprende che il 99% dei responsabili IT desideri firewall che siano in grado di isolare automaticamente i sistemi compromessi; il 90% concorda che una tale possibilità sarebbe "estremamente" o "molto" utile. Una percentuale simile (il 97%) sostiene che probabilmente acquisterebbe i sistemi di sicurezza per endpoint e firewall dallo stesso vendor, se ciò garantisse tassi di rilevamento più elevati e una migliore risposta automatica agli incidenti.

Conclusione

I segreti degli attuali firewall di rete sono allo scoperto: non sono in grado di offrire le funzionalità essenziali di cui le organizzazioni hanno bisogno. Dalla protezione della rete, alla visibilità, alla risposta agli incidenti; le esperienze attuali dei responsabili IT sono deludenti alla luce delle loro aspettative ed esigenze reali, in termini di ciò che occorra per proteggere un'organizzazione. Pertanto è ora che le organizzazioni adottino un approccio innovativo alla protezione della rete, implementando soluzioni che siano in grado di soddisfare le loro esigenze.

[i] *The Life and Times of Cybersecurity Professionals. The Enterprise Strategy Group, 2017*

Approfondimenti

- Documento: "**Il firewall e le migliori pratiche per bloccare il ransomware**" –Come si sono verificati alcuni dei recenti attacchi di ransomware come WannaCry e Petya e delle funzionalità che i firewall devono avere per poter bloccare questi tipi di attacco.
- Documento: "**Perché gli amministratori di rete hanno bisogno di avere visibilità completa sulle applicazioni**" – Un'analisi approfondita dei problemi relativi alla visibilità sul traffico di rete e di cosa si possa fare per risolverli.
- **Guida all'acquisto di una soluzione Firewall** – Le principali tecnologie e funzionalità da richiedere quando si sceglie un firewall, con le domande da rivolgere ai vendor.

Sophos XG Firewall: Come risolvere i problemi che affliggono i firewall di rete

Sophos XG Firewall è realizzato per soddisfare le esigenze in costante evoluzione dei responsabili IT. Offre una soluzione per risolvere i principali problemi dei firewall di rete attuali.

- **Protezione.** XG Firewall blocca le minacce sconosciute, mediante l'uso di una suite completa di soluzioni di protezione avanzata che include: Deep Learning, sistema di prevenzione delle intrusioni, protezione avanzata contro le minacce, sandboxing e AV a doppio motore di scansione.
- **Visibilità.** XG Firewall espone i rischi nascosti grazie alle sue opzioni di visibilità su tutte le app, sugli utenti maggiormente a rischio, sulle minacce avanzate, sui payload sospetti e molto altro ancora.
- **Risposta.** XG Firewall risponde automaticamente agli incidenti, grazie all'identificazione e all'isolamento immediato dei sistemi colpiti, fino a quando non sia possibile eliminare le infezioni.

Ecco i riconoscimenti in situazioni pratiche ricevuti da XG Firewall:

- **NSS Labs**: "Top rated" (punteggio massimo)
- **SC Media**: "Una convergenza molto creativa di diverse funzionalità estremamente efficaci"
- **PC Pro**: "Un'appliance UTM molto versatile, che offre la combinazione ideale tra alti livelli di performance e un ottimo rapporto qualità-prezzo"

Per maggiori informazioni e per avviare una prova gratuita, visitare: www.sophos.it/xgfirewall.

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

04/04/18 IT (TN)

SOPHOS