SOPHOS
Cybersecurity evolved.

Sophos Adaptive Cybersecurity Ecosystem

Sophos Adaptive Cybersecurity Ecosystem (ACE) è una struttura estesa realizzata per ottimizzare la prevenzione, il rilevamento e la risposta alle minacce. Protegge la nuova realtà dei sistemi aziendali interconnessi e li difende dagli attacchi informatici sempre più complessi ed in continua evoluzione, frutto di un mix tra automazione e manualità.

Sophos ACE sfrutta l'automazione e le competenze tecniche dei nostri analisti, oltre ai dati raccolti da prodotti, partner e clienti Sophos e dagli sviluppatori, per creare una protezione che continua a migliorarsi: un circolo virtuoso che ne permette il costante apprendimento e miglioramento. E il bello è che si può cominciare con poco, per poi crescere. È possibile iniziare con le tecnologie Sophos Endpoint o Firewall e aggiungere componenti a questa base.

Whitepaper Sophos. Maggio 2021

Un panorama in continuo cambiamento

Il panorama della cybersecurity continua a evolversi e negli ultimi anni si sono osservati cambiamenti significativi sia negli ambienti aziendali che nella natura degli attacchi.

Il cambiamento negli ambienti aziendali: Interconnettività

Nella costante ricerca di nuovi modi per incrementare la produttività e l'efficienza, le organizzazioni hanno creato una supply chain interconnessa, accompagnata da un'infrastruttura e da tecnologie in grado di supportarla. La migrazione dei dati e delle applicazioni verso il cloud ha comportato diversi vantaggi, come ad esempio: la possibilità di lavorare da qualsiasi luogo, la riduzione dei costi operativi e un miglioramento in termini di performance e scalabilità. Inoltre, questa tendenza ha anche svolto la funzione di catalizzatore per la crescita della supply chain digitale a livello globale.

Parallelamente, il COVID-19 ha accelerato la diffusione dello smart working, sfatando definitivamente il mito del perimetro di rete delle organizzazioni. Ormai bisogna dare per scontato che persone, applicazioni, dispositivi e dati possono trovarsi ovunque.

Sebbene da un lato questi sistemi interconnessi e decentralizzati siano molto pratici, dall'altro generano nuove sfide alla sicurezza. Molte organizzazioni fanno fatica a mappare l'estensione della propria rete e trovano ancora più difficile proteggere tutti i sistemi connessi a tale rete.

Questi sistemi sono uno tra i bersagli principali di hacker intelligenti ed estremamente adattabili, attratti dalle maggiori opportunità che offrono. Una recente dimostrazione (che non rappresenta un caso isolato) di questo problema è stato l'attacco SolarWinds a dicembre 2020, che ha fatto vittime di vario genere, da importanti vendor di soluzioni tecnologiche e piccole imprese, fino a enti del settore pubblico di altissimo livello.

Il cambiamento negli attacchi: da automatizzati a operativi

Quando si lavora nell'ambito della cybersecurity, è facile perdere di vista una questione molto importante ma purtroppo sottovalutata: nella battaglia per proteggere i sistemi e i dati critici, sta vincendo chi li difende.

Le notizie che segnalano ogni giorno nuovi casi di violazione dei dati svolgono un compito importante: sono un avvertimento che ci ricorda di adottare misure preventive e di non abbassare mai la guardia. Tuttavia, queste storie sono l'eccezione alla regola. Nessun articolo di rilievo documenta le organizzazioni che ogni giorno riescono a proteggersi contro migliaia di tentativi di violazione.

L'efficacia della cybersecurity non è solo migliorata drasticamente, ma è diventata anche più conveniente, con nuovi strumenti e servizi gestiti di sicurezza, disponibili a prezzi più accessibili che mai. Tecnologie come antiransomware, prevenzione degli exploit, rilevamento di comportamenti sospetti e antiphishing sono alla portata di tutti.

CAMBIAMENTO NEGLI AMBIENTI AZIENDALI

Supply chain interconnessa

Migrazione di app e dati verso il cloud

Ambienti di smart working

CAMBIAMENTO NEGLI ATTACCHI

Vince chi difende i sistemi

Automazione + operazione degli hacker

Incremento dei costi delle violazioni

Queste opzioni (rese possibili, migliori e più veloci grazie all'utilizzo dell'intelligenza artificiale e dal machine learning) sono realizzate per affrontare le tattiche, le tecniche e le procedure dei cybercriminali documentate nel framework MITRE ATT&CK. Inoltre, sono predisposte per identificare e rispondere ad attacchi nuovi e innovativi che non sono mai stati visti prima. Colmando le lacune, bloccando i punti di ingresso e intercettando le varie tecniche, questi miglioramenti hanno reso alcuni attacchi molto più difficili da azionare, per cui gli hacker si sono dovuti adattare. Questi miglioramenti della sicurezza sono talmente importanti che oramai il vecchio detto "a un hacker basta colpire nel segno una sola volta" non riflette più la realtà. Per ottenere un guadagno, gli hacker hanno bisogno di colpire nel segno diverse volte.

Si è pertanto notato un cambiamento nel loro approccio: sono passati dall'utilizzo di malware automatico a una strategia più completa, che combina automazione e manualità. L'obiettivo principale degli autori degli attacchi è continuare a sfuggire al rilevamento e il migliore modo per farlo è agire come farebbe un dipendente, utilizzando strumenti e dispositivi locali e sfruttando i più comuni modelli di traffico.

Questi attacchi estremamente sofisticati, che comportano un impegno significativo in termini di risorse umane, implicano costi molto più elevati per le vittime. Gli hacker acquisiscono una conoscenza approfondita dell'ambiente della vittima e la possono sfruttare per causare più danni possibili e per ottenere la massima resa.

Il passaggio dell'IT security alle security operations

Questi cambiamenti negli ambienti aziendali e nelle modalità di attacco richiedono un'evoluzione dell'IT security. Le organizzazioni affrontano ora hacker che modificano costantemente il proprio obiettivo mentre procedono con l'attacco, per cui i team di IT security devono sviluppare contromisure in grado di migliorare la probabilità di successo dei sistemi di difesa.

In primo luogo, occorre un cambiamento graduale da **gestione della sicurezza a security operations**. Sono ormai lontani i tempi in cui era possibile impostare una policy di sicurezza e non dovere più intervenire; gli hacker sono sempre più attivamente coinvolti negli attacchi, per cui l'IT security non può essere da meno: deve rilevare proattivamente comportamenti ed eventi sospetti prima che diventino una vera e propria violazione.

I team di sicurezza devono cercare e individuare le attività sospette il prima possibile nella catena di attacco, per poter dare ai sistemi di difesa la possibilità di rispondere prima che sia troppo tardi. Anche gli hacker più elusivi lasciano tracce, e i team di sicurezza devono identificare e seguire gli indizi per stroncare l'attacco sul nascere. Non si tratta più di distinguere gli elementi pertinenti da quelli non rilevanti, bensì di identificare i segnali deboli prima che diventino forti. Più chiaro è il segnale, più si è vicini a una violazione. Utilizzando strumenti adeguati, i problemi informatici possono essere rilevati e corretti proattivamente, prima che un hacker possa identificarli e sfruttarli in un attacco.

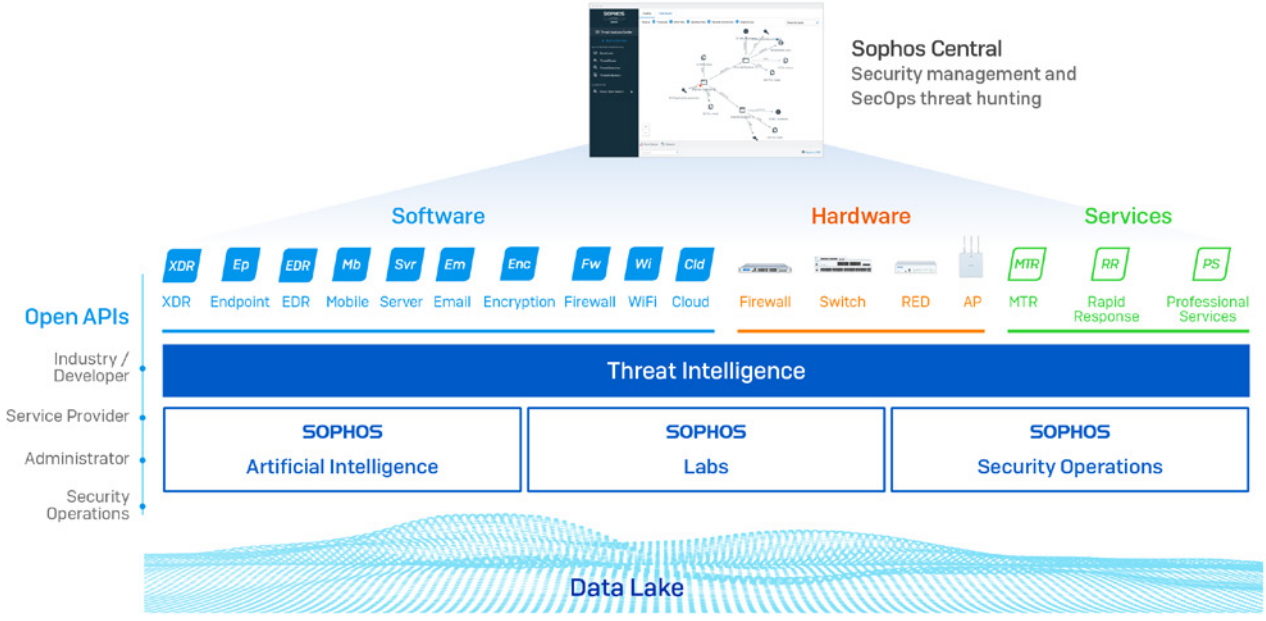
Ora che le organizzazioni sono estremamente interconnesse, la sicurezza non può essere da meno. I team di IT security devono passare da prodotti individuali e non integrati a un **sistema di sicurezza adattiva** in grado di applicare il più possibile una prevenzione automatica, aiutando allo stesso tempo gli operatori a individuare proattivamente i segnali deboli (ad es. comportamenti ed eventi sospetti), per impedire che diventino vere e proprie violazioni.

Gli ambienti aziendali e gli attacchi si evolvono costantemente. Il futuro dell'IT security è un sistema che utilizza un ciclo continuo di feedback, per **apprendere e migliorarsi continuamente**. Le nuove informazioni e i nuovi eventi rilevati dal team di IT operations possono essere automatizzati, migliorando il rilevamento e riducendo il numero di nuovi attacchi che riescono a infiltrarsi nei sistemi. Analogamente, man mano che viene ottimizzata l'automazione dei software, gli operatori possono individuare comportamenti ed eventi sospetti in maniera più rapida, limitando ulteriormente il numero di incidenti. Questo circolo virtuoso migliora costantemente la sicurezza complessiva di un'organizzazione e delle aziende connesse.

Sophos Adaptive Cybersecurity Ecosystem

La buona notizia è che un sistema di sicurezza di questo tipo esiste già. Sophos Adaptive Cybersecurity Ecosystem (ACE) è progettato per la nuova realtà in cui viviamo. Sfrutta la potenza dell'automazione e le competenze dei nostri analisti per rendere possibile il passaggio dalla gestione della sicurezza alle security operations. L'automazione analizza e reagisce più rapidamente a comportamenti ed eventi sospetti, mentre gli analisti umani riescono a correlare con maggiore efficacia i vari segnali, interpretandone correttamente il significato.

Sophos ACE è realizzato per proteggere l'interconnettività delle nostre aziende e del nostro mondo on-line. Protegge sistemi e dati ovunque si trovino e apprende costantemente, migliorandosi per difendere i sistemi dai cambiamenti futuri delle tecnologie e degli attacchi.



Sophos ACE comincia dall'**intelligence collettiva sulle minacce** dei team SophosLabs, Sophos Security Operations (composto da analisti umani che svolgono threat hunting avanzato su migliaia di ambienti dei clienti, mediante il nostro servizio Managed Threat Response) e Sophos Artificial Intelligence. Queste capacità di intelligence in tempo reale migliorano continuamente le tecnologie next-gen della nostra linea di soluzioni **software** e **hardware** leader di settore a livello globale.

Un singolo **data lake** integrato raccoglie informazioni da tutti i nostri prodotti e dalle nostre origini di dati di intelligence sulle minacce. I team di sicurezza delle organizzazioni possono così utilizzare le analisi in tempo reale per prevenire le violazioni e individuare proattivamente i segnali sospetti, distinguendoli da tutte le informazioni non pertinenti. Parallelamente, le **API aperte** permettono a clienti, partner e sviluppatori di realizzare strumenti e soluzioni in grado di interagire con il sistema. L'intera struttura è gestita dalla **piattaforma di gestione Sophos Central**. Tutta la sicurezza si trova in un posto solo, per garantire un'efficienza di livelli imbattibili.

Questi cinque elementi (intelligence sulle minacce, tecnologie next-gen, data lake, API e gestione centralizzata) interagiscono reciprocamente per creare un ecosistema di cybersecurity adattiva che apprende e migliora costantemente. Inoltre, anche se la potenza di questo ecosistema completo è estesa, è possibile usufruirne nella quantità desiderata. Molti clienti cominciano con la nostra protezione endpoint o il nostro firewall, per poi estendere il sistema a un ritmo che segue le loro esigenze.

Negli ultimi 12 mesi, molti Security Operations Center si sono trasformati in SOC virtuali. Sophos ACE può essere gestito da esperti di sicurezza situati in qualsiasi parte del mondo, garantendo alle organizzazioni la flessibilità di trovare i migliori talenti di sicurezza a livello internazionale. In alternativa, è possibile usufruire del nostro servizio di rilevamento e risposta alle minacce.

L'evoluzione della Synchronized Security

Synchronized Security, la capacità dei prodotti Sophos di condividere informazioni in tempo reale tramite Security Heartbeat™ e di automatizzare la risposta agli incidenti, è stata per molti anni uno dei capisaldi della nostra protezione. Al momento del lancio nel 2015, Synchronized Security era una soluzione esclusiva nel mercato e tutt'oggi continuiamo a offrire un'analisi approfondita di dati provenienti da prodotti diversi, con livelli di integrazione semplicemente irraggiungibili per gli altri vendor di soluzioni di sicurezza.

"Sophos conferma il suo ruolo di leader di mercato con le opzioni XDR tra firewall e prodotti di sicurezza endpoint".

Gartner
Gartner Magic Quadrant for Enterprise Network Firewalls,
analisti: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 novembre 2020

Sophos Adaptive Cybersecurity Ecosystem si basa sull'automazione e sull'integrazione di Synchronized Security, estendendo ulteriormente la struttura di cybersecurity Sophos.

Più visibilità

Nessuno può prevedere da dove arriverà il prossimo attacco, ed è semplicemente impossibile per gli operatori umani riuscire a monitorare tutto. Quello che occorre è invece un sistema in grado di monitorare ogni elemento, che consenta di rispondere rapidamente alle minacce emergenti. Ed è per questo motivo che abbiamo esteso l'ecosistema in modo da includere una gamma ancora più ampia di tecnologie, incluse la nostra nuova Sophos Extended Detection and Response (XDR) e le nostre API. I prodotti Sophos individuano e registrano tutti gli eventi, i comportamenti e i rilevamenti sospetti all'interno dell'ambiente, per fornire le informazioni necessarie in maniera pratica.

Più dati

Il data lake unisce e mette in correlazione le informazioni provenienti da questi sensori, per fornire approfondimenti più dettagliati su prodotti multipli. Gli operatori possono eseguire query direttamente nel data lake con Sophos Intercept X with EDR e Sophos XDR, per identificare comportamenti ed eventi sospetti nell'intero ambiente e per impedire che i problemi diventino violazioni a tutti gli effetti.

Più intelligence

Grazie alla rapida crescita del nostro servizio Managed Threat Response (MTR), siamo in grado di aggiungere informazioni in tempo reale, curate dai nostri esperti di threat hunting, per completare i dati di rilevamento. Parallelamente, continuiamo a migliorare i nostri modelli di intelligenza artificiale (AI) e gli input dei dati di rilevamento delle minacce provenienti dai SophosLabs.

Più integrazione

I team SophosLabs, Sophos AI e Sophos Security Operations lavorano insieme, integrando nel sistema le proprie competenze affinché ne possano usufruire tutti i clienti, creando così un circolo virtuoso. Ad esempio, PowerShell è uno strumento legittimo e molto utile, ma è anche frequentemente utilizzato in maniera impropria dagli hacker. Gli operatori di MTR sfruttano l'esperienza maturata nel mondo reale per addestrare i nostri modelli di intelligenza artificiale in modo che riescano a distinguere tra utilizzo "lecito" e "illecito" di PowerShell. L'intero sistema viene quindi aggiornato con le informazioni apprese dall'intelligenza artificiale, elevando il livello di protezione dei clienti.

Sophos Adaptive Cybersecurity Ecosystem in azione

Sophos ACE è un sistema che agisce in tempo reale e che sta già elevando ed estendendo la protezione in situazioni reali. A marzo 2021, una gang di cybercriminali chiamata Hafnium ha sfruttato una vulnerabilità di ProxyLogon in Microsoft Exchange. Si trattava di una vulnerabilità zero-day, per cui gli hacker hanno approfittato di una debolezza intrinseca della progettazione di Exchange per eludere il rilevamento.

Non appena questa vulnerabilità è stata resa nota, il servizio Sophos Managed Threat Response (MTR) ha immediatamente aggiornato il monitoraggio dei sensori in modo da includere i comportamenti associati a ProxyLogon. Con le informazioni già disponibili nel data lake, Sophos MTR ha avuto subito accesso a tutti i dati di input necessari per identificare e correggere le attività dannose associate a questa vulnerabilità.

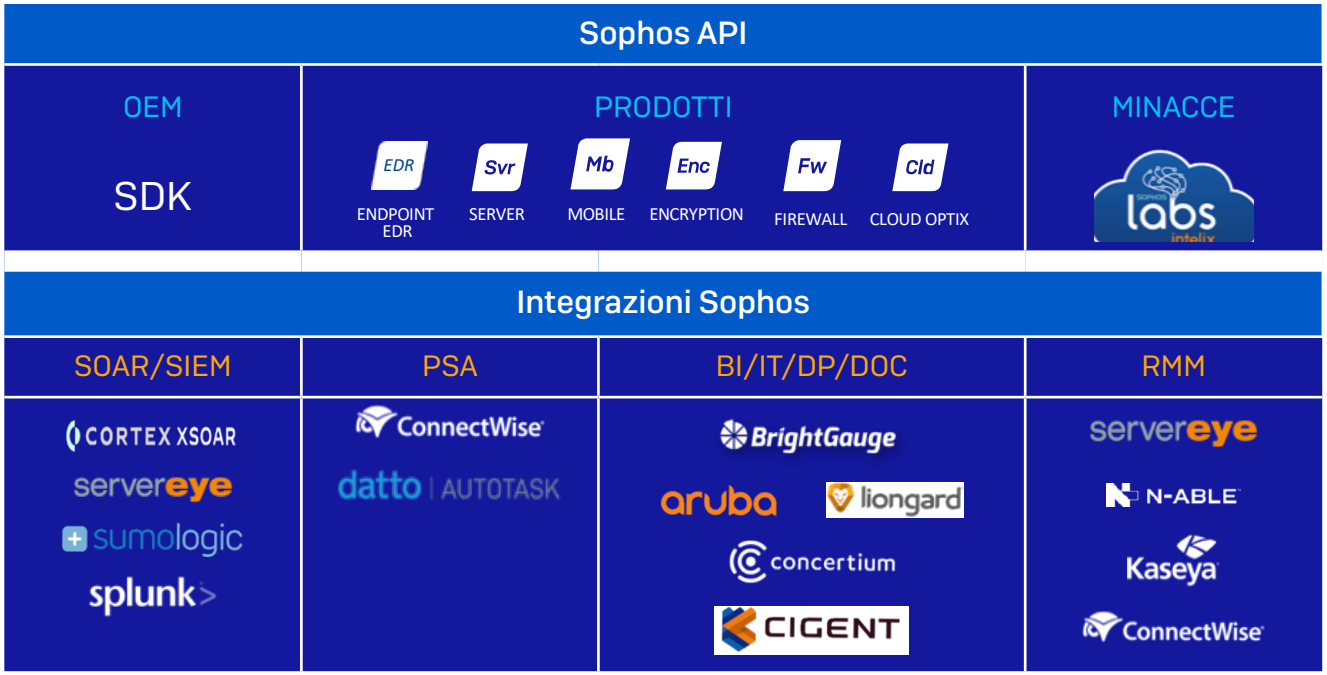
Inoltre, ha utilizzato la tecnologia Sophos EDR insieme alle proprie abilità di threat hunting, per smascherare nuovi elementi o indicatori di compromissione (IoC) correlati all'attacco. Questi indicatori sono stati quindi condivisi direttamente con i SophosLabs, che li hanno utilizzati per pubblicare ulteriori IoC associati alla vulnerabilità di Exchange e offrire maggiore protezione a tutti i clienti Sophos.

Una piattaforma aperta, con integrazioni potenti e API aperte

Nel nostro mondo interconnesso è essenziale che la cybersecurity sia in grado di integrarsi con l'ambiente aziendale esteso. La cybersecurity ha varie sfaccettature e Sophos Adaptive Cybersecurity Ecosystem soddisfa una vasta gamma di esigenza di sicurezza, incluse quelle di:

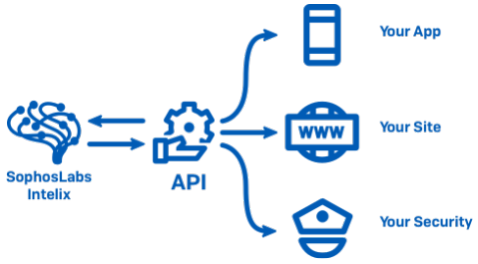
- MSSP – Supporta la distribuzione di sistemi di difesa informatica negli ambienti dei loro clienti
- Channel Partner – Snellisce i processi commerciali
- ISP – Permette loro di garantire la sicurezza dei servizi Internet che offrono
- Piccole e medie imprese – Consente di creare strumenti personalizzati per controllare e abilitare la sicurezza

Moltissime API e integrazioni sono già disponibili (e ne sono previste altre) e Sophos ACE gestisce già più di cinque milioni di richieste API al giorno.



Presentazione delle API: SophosLabs Intelix™

Intelix è una suite di RESTful API semplici e a risposta rapida che permette alle app di identificare, classificare e prevenire le minacce, incrementandone la sicurezza. I clienti, i partner e gli sviluppatori che utilizzano un ecosistema Sophos possono utilizzare queste API per svolgere ricerche nel cloud sulle minacce, nonché per effettuare analisi statiche e dinamiche dei file. Per maggiori informazioni sulle API di SophosLabs Intelix, visitare: https://www.sophos.com/it-it/labs/intelix.aspx.



Sophos ACE: un impatto estremamente positivo sul business

I vantaggi di Sophos Adaptive Cybersecurity Ecosystem sono molteplici. Offre la combinazione di tecnologie Next-Gen straordinarie: dati di intelligence sulle minacce provenienti da SophosLabs, Sophos AI e Sophos Security Operations; un sistema integrato e adattivo che apprende costantemente; una gestione centralizzata con la piattaforma Sophos Central. Tutte queste opzioni hanno un impatto molto positivo, sia in termini di protezione che di efficienza.

Tecnologie next-gen	**+**	**Intelligence sulle minacce**	**+**	**Sistema integrato e adattivo**	**+**	**Gestione centralizzata**

I clienti che già utilizzano Sophos Firewall e Sophos Intercept X contemporaneamente sostengono che avrebbero bisogno del doppio del personale nei team di sicurezza per garantire gli stessi livelli di protezione, se non avessero un sistema di cybersecurity Sophos. Inoltre, dichiarano di aver riscontrato meno incidenti di sicurezza e di essere stati in grado di identificare e rispondere più rapidamente ai problemi che sono emersi. Sophos ACE si fonda su queste basi ma va oltre, trasformando ulteriormente non solo la protezione, ma anche il costo totale di proprietà.

Per cominciare

Sophos Cybersecurity Ecosystem è estremamente flessibile e per cominciare basta semplicemente implementare uno dei prodotti o servizi di protezione Sophos. Le organizzazioni potranno quindi usufruire immediatamente della combinazione delle competenze in ambito di intelligence sulle minacce dei team Sophos AI, SophosLabs e Sophos Security Operations. L'ecosistema può essere esteso in qualsiasi momento, in linea con le esigenze dell'organizzazione. Le soluzioni più frequentemente utilizzate come punto di partenza includono:

Sophos Intercept X per endpoint o server (con l'opzione di aggiungere funzionalità EDR o XDR)

Sophos Firewall in versione hardware, software o virtuale

Sophos Managed Threat Response (MTR), fornita come servizio

Per scoprire di più, rivolgetevi al vostro rappresentante Sophos di fiducia, visitate il nostro sito web o avviate una prova gratuita.

Gartner Magic Quadrant for Enterprise Network Firewalls,

analisti: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 novembre 2020

Gartner non appoggia non sostiene alcun fornitore, produttore o servizio citato all'interno delle sue pubblicazioni di ricerca e non consiglia agli utenti delle tecnologie di selezionare solo i fornitori con le valutazioni più alte o altre designazioni. Le pubblicazioni di Gartner riflettono solamente le opinioni dell'organizzazione e non devono pertanto essere considerate come affermazioni di fatto. Gartner rinuncia a qualsiasi garanzia, implicita o esplicita, in merito a questa ricerca, incluse le garanzie sulla commerciabilità o sull'idoneità a un particolare scopo.

Scoprite di più sul ransomware e su come Sophos può essere di aiuto per la protezione della vostra organizzazione.

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.

2021-04-26 (SB-NP)

SOPHOS