SOPHOS

Le novità di

Sophos Firewall

Nuove funzionalità importanti in Sophos Firewall OS v21.5

Maggiore protezione e livelli superiori di performance

Integrazione di Sophos NDR Essentials con Sophos Firewall

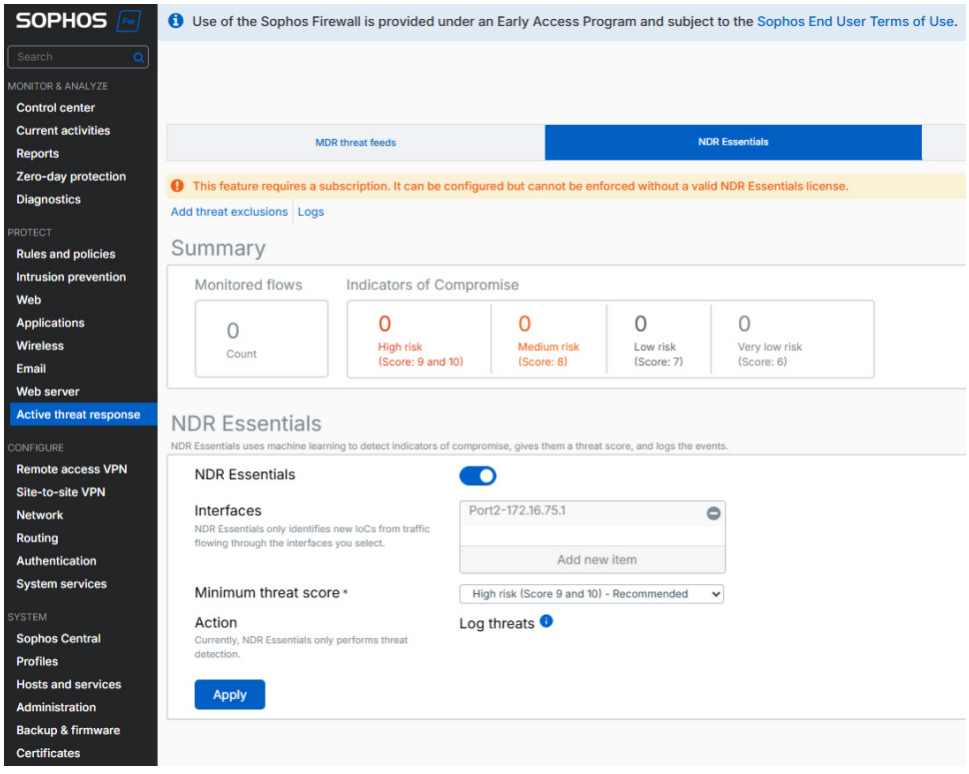
Network Detection and Response (NDR) è una categoria di prodotti di sicurezza della rete progettati per rilevare comportamenti anomali nel traffico, contribuendo così all'identificazione di active adversary attivi nella rete. Gli hacker più esperti sono molto abili a eludere il rilevamento, ma prima o poi dovranno spostarsi all'interno della rete o comunicare all'esterno della rete per sferrare un attacco. Tipicamente, una soluzione NDR viene implementata nella rete, dove utilizza sensori che monitorano e analizzano il traffico di rete per identificare questo tipo di attività sospetta.

I prodotti NDR esistono da diversi anni e Sophos NDR è stata inclusa nella nostra linea di prodotti MDR/XDR all'inizio del 2023. Tuttavia ora, con SFOS v21.5, NDR è integrata in Sophos Firewall: una novità assoluta nel settore, che significa anche che i clienti Sophos Firewall con Xstream Protection potranno usufruirne liberamente, senza alcun costo aggiuntivo.

L'integrazione di NDR con un firewall next-gen potrebbe sembrare una scelta ovvia, ma la vera sfida è fare in modo che non incida sulla performance del firewall. L'analisi del traffico di NDR richiede un'elevata capacità di elaborazione. Di conseguenza, abbiamo adottato un approccio innovativo, che prevede la distribuzione di una soluzione NDR nel cloud di Sophos per alleggerire il carico di lavoro del firewall.

Con Sophos Firewall v21.5 viene introdotta la nostra nuova piattaforma di Network Detection and Response implementata nel cloud: NDR Essentials. Questa piattaforma utilizza rilevamenti basati sulle più moderne tecnologie di IA per identificare gli active adversary e condividere le informazioni con l'API Feed sulle minacce di Sophos Firewall nell'ambito della risposta alle minacce attive, tenendoti al corrente sui rilevamenti e sul loro rischio relativo.

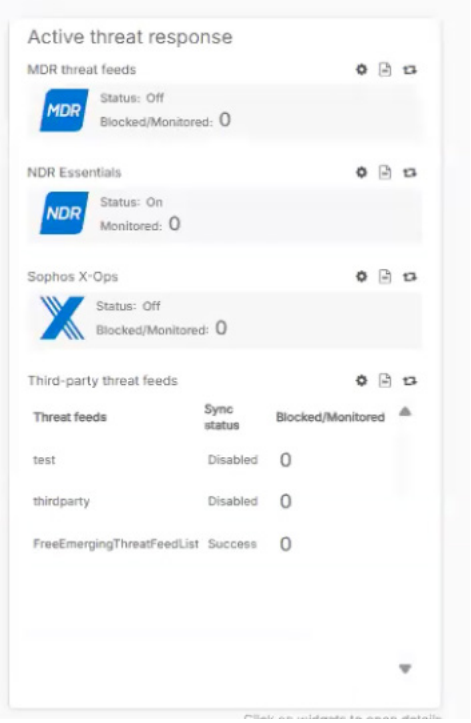
Come funziona: Sophos Firewall acquisisce metadati dal traffico crittografato con TLS e dalle query DNS, per poi inviare tutti i dati a NDR Essentials nel Sophos Cloud, dove queste informazioni vengono analizzate con più motori di IA. È in grado di rilevare payload crittografati dannosi senza eseguire la decrittografia TLS; inoltre, individua domini nuovi e insoliti generati mediante algoritmi, che spesso costituiscono un importante indicatore di compromissione. L'estrazione dei metadati viene svolta da un nuovo motore a basso impatto nel FastPath di Xstream e di conseguenza è disponibile solo sui firewall hardware XGS Series. L'integrazione di NDR nei firewall virtuali, software e cloud potrebbe essere disponibile in futuro, ma non nella v21.5.



Configura e monitora il tuo feed di NDR Essentials sotto "Active Threat Response", insieme ai tuoi altri feed sulle minacce.

Il nuovo feed sulle minacce di NDR Essentials viene gestito insieme ai tuoi altri feed sulle minacce (Sophos X-Ops, MDR e feed di terze parti) nell'area "Risposta alle minacce attive" del firewall, come mostrato nello screenshot qui sopra. La configurazione è semplice: attiva la funzionalità con l'interruttore, seleziona le interfacce interne che desideri monitorare, imposta una soglia minima per il rischio di rilevamento... ed è tutto!

I rilevamenti di NDR Essentials ricevono un punteggio compreso tra 1 (basso rischio) e 10 (alto rischio). Sei tu a decidere quale punteggio di rischio usare come soglia per gli avvisi generati nel tuo ambiente. L'impostazione consigliata è alto rischio (9-10). Tutti i rilevamenti con un punteggio pari o superiore a 6 vengono registrati nei log, ma solo quelli che raggiungono o superano la soglia da te impostata attiveranno notifiche e verranno visualizzati come avvisi nella dashboard, all'interno del nuovo widget Control Center. I rilevamenti con punteggio inferiore a 6 potrebbero essere falsi positivi e non vengono inseriti nei log. Al momento nessun rilevamento di NDR Essentials viene bloccato, ma questa opzione potrebbe essere introdotta in futuro. Tutti i rilevamenti vengono indicati nel report Risposta alle minacce attive, che è disponibile sia nell'appliance, sia in Sophos Central Firewall Reporting.



Tutti i rilevamenti di NDR Essentials che raggiungono o superano la soglia di rischio da te impostata vengono visualizzati nella nuova versione del widget Control Center.

Se desideri dati di rilevamento più approfonditi e maggiori opzioni di threat hunting, ti consigliamo vivamente di dare un'occhiata a Sophos Extended Detection and Response (XDR) con l'implementazione completa di Sophos NDR che include la nuova Console di indagine di NDR. Potrebbe interessarti anche il nostro servizio completo Managed Detection and Response, che è operativo 24/7. Tutti questi prodotti e servizi agiscono in maniera ottimale in sinergia con i tuoi Sophos Firewall.

SSO per la VPN di accesso remoto

Single Sign-On di Entra ID (Azure AD) per Sophos Connect Client e il portale VPN

Una delle opzioni più richieste è la possibilità di utilizzare le credenziali della rete aziendale con il Sophos Connect Client e il portale VPN del firewall, per semplificare l'uso della VPN di accesso remoto per gli utenti finali. SFOS v21.5 include ora l'integrazione del Single Sign-On di Entra ID (Azure AD) con Sophos Connect e il portale VPN. Offre integrazione nativa del cloud sui protocolli standard di settore OAuth 2.0 e OpenID Connect, per un'esperienza semplice e fluida. Questa funzionalità è supportata per Sophos Connect Client 2.4 e versioni successive su Microsoft Windows.

Altri miglioramenti della VPN e della scalabilità

Miglioramenti dell'interfaccia utente e dell'usabilità: i tipi di connessione hanno cambiato nome da "site-to-site" a "in base al criterio" e le interfacce del tunnel sono state rinominate come "in base alla route", per renderle più intuitive.

Miglioramento della convalida dei pool di IP in lease: su VPN SSL, IPsec, L2TP e VPN di accesso remoto su PPTP per eliminare potenziali conflitti di indirizzi IP.

Implementazione di profili rigidi: sui profili IPsec che escludono valori predefiniti per garantire la corretta esecuzione di handshake, eliminando la potenziale frammentazione dei pacchetti e il rischio che i tunnel non vengano stabiliti correttamente.

Scalabilità della VPN in base alla route: la capacità della VPN in base alla route è raddoppiata, con il supporto di fino a 3.000 tunnel.

Scalabilità per SD-RED: i Sophos Firewall supportano ora fino a 1.000 tunnel RED site-to-site e fino a 650 dispositivi SD-RED.

Sophos DNS Protection

Sophos DNS Protection è ora più semplice

L'anno scorso abbiamo lanciato il nostro servizio DNS Protection, disponibile gratuitamente per tutti i clienti con firewall dotati di licenza Xstream Protection. Con questo rilascio, Sophos DNS Protection ottiene un'integrazione ancora più profonda con Sophos Firewall per mezzo di un nuovo widget Control Center che indica lo stato del servizio. Sono stati introdotti anche la possibilità di sfruttare log e notifiche per accedere ad analisi utili per la risoluzione dei problemi, più un nuovo tutorial guidato su come configurare facilmente Sophos DNS Protection.

Gestione semplificata e miglioramenti in termini di qualità generale

Come accade con ogni rilascio di Sophos Firewall, questa versione include diversi miglioramenti in termini di qualità generale che semplificano le attività quotidiane di gestione.

Dimensioni modificabili per le colonne della tabella: un'opzione richiesta da diverso tempo. Molte schermate di stato e configurazione del firewall offrono ora la possibilità di modificare la larghezza delle colonne e di conservare le impostazioni nella memoria del browser per le visite successive. Questa novità è disponibile in molte schermate, come SD-WAN, NAT, SSL, Host e servizi, e VPN site-to-site.

Ricerca a testo libero estesa: le route SD-WAN permettono ora di effettuare ricerche per nome della route, ID, oggetto e valore dell'oggetto, come indirizzi IP, domini o altri criteri. Le regole ACL locali supportano ora la ricerca per nome e valore dell'oggetto, inclusa la ricerca in base ai contenuti.

Configurazione predefinita: a grande richiesta, sono state rimosse le regole predefinite e i gruppi di regole precedentemente creati durante la configurazione di un nuovo firewall. Ora durante la configurazione iniziale vengono fornite solo la regola di rete predefinita e le regole dell'MTA . Il gruppo predefinito di regole firewall e i probe predefiniti del gateway per i gateway personalizzati sono entrambi configurati come "Nessuno" per impostazione predefinita.

Nuovo font: l'interfaccia utente di Sophos Firewall offre ora un font più leggero, nitido e ben definito, che migliora la leggibilità e la performance.

Altri miglioramenti

Licenze virtuali, software, cloud: Tutte le licenze Sophos Firewall virtuali, software e cloud (BYOL) non hanno più limiti di RAM. Le licenze sono ora limitate solamente dal numero di core e non presentano alcuna restrizione per la RAM.

Estensione dei limiti delle dimensioni dei file nel WAF: il Web Application Firewall (WAF) permette ora di impostare un limite configurabile delle dimensioni dei file di richiesta (caricamento), ed è ora in grado di analizzare file fino a 1 GB.

Secure by Design: continuiamo a potenziare la sicurezza di Sophos Firewall e in questo rilascio abbiamo aggiunto la raccolta di dati di telemetria in tempo reale per segnalare eventuali modifiche sospette nei file core del sistema operativo. Questa opzione permetterà ai nostri team di monitoraggio di identificare proattivamente e tempestivamente gli incidenti di sicurezza, prima che diventino un problema serio.

Allentamento delle restrizioni per la delega del prefisso DHCP: sono ora supportati i prefissi da /48 a /64, il che aiuta a ottimizzare l'interoperabilità tra ISP. Anche gli annunci router (Router Advertisement, RA) e il server DHCPv6 sono ora abilitati per impostazione predefinita.

Individuazione del percorso dell'MTU: questa opzione risolve gli errori di decrittografia TLS dovuti al supporto della versione più recente dello scambio di chiavi ML-KEM (Kyber) nei browser. Ora il motore di Deep Packet Inspection di Sophos Firewall rileva e ottimizza automaticamente l'MTU di ogni flusso, garantendo una performance ottimale, basata su condizioni di rete specifiche.

NAT64 (traffico da IPv6 a IPv4): NAT64 è supportato per il traffico da IPv6 a IPv4 in modalità proxy esplicita. In questa modalità i client solo IPv6 possono accedere ai siti web che utilizzano IPv4. Il firewall supporta anche il proxy upstream IPv4 per client solo IPv6.

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

2025-03-31 IT (DD)

SOPHOS