Sophos Network Detection and Response

Un Potente Componente Aggiuntivo Per Sophos XDR e Sophos MDR

Sophos NDR agisce in perfetta sinergia con i tuoi firewall ed endpoint gestiti per monitorare l'attività della rete alla ricerca di pattern sospetti e pericolosi che altrimenti non verrebbero rilevati dalle altre soluzioni. Sophos NDR analizza le parti più nascoste della rete per rilevare i flussi di traffico anomali che vengono generati da sistemi e dispositivi IoT non gestiti, da risorse non autorizzate, da minacce interne, da attacchi zero-day mai visti prima e da comportamenti sospetti.

Sophos NDR Offre Livelli Critici Di Visibilità Sull'Attività Di Rete Che Risulta Invisibile Agli Altri Prodotti

Gli hacker sono molto abili a eludere il rilevamento, ma tutti gli attacchi sono caratterizzati dalla necessità di spostarsi all'interno della rete. Sophos NDR rileva i pattern di traffico sospetti, che non vengono rilevati dai firewall e dagli endpoint gestiti, inclusi quelli generati da:

- **Dispositivi di rete sconosciuti o non protetti**, inclusi dispositivi IoT oppure OT legittimi che non possono essere gestiti completamente con un sensore endpoint, nonché sistemi sconosciuti o non identificati che si trovano nella rete. Questi dispositivi potrebbero essere o diventare compromessi nel corso di un attacco. Sophos NDR identifica e monitora tali dispositivi per identificare comportamenti sospetti o malevoli che potrebbero indicare la presenza di un attacco.
- **Risorse non autorizzate o illegittime** che vengono introdotte nella rete, che potrebbero essere già compromesse o che rischiano di essere utilizzate per sferrare un attacco. Con Sophos NDR, queste risorse diventano facilmente identificabili e monitorabili.
- **Attività di comando e controllo (C2) nuova e mai osservata prima**. Molti attacchi o violazioni vengono orchestrati da remoto, utilizzando comunicazioni dall'apparenza legittima tra un cybercriminale e il suo processo remoto all'interno della rete della vittima. Sophos NDR è in grado di rilevare l'attività C2 zero-day, per identificare quello che potrebbe essere un attacco personalizzato e mirato nelle fasi iniziali.
- **Flussi e pattern di traffico sospetti o pericolosi**, che possono essere segnali importanti per identificare i primi stadi di un attacco informatico. Tra questi, vi possono essere: attività di rete o accessi remoti insoliti e fuori orario di lavoro, esfiltrazioni o caricamenti sospetti di dati, pattern di traffico anomali e traffico dannoso generato da malware noto.

NDR Agisce In Sinergia Con Il Tuo Firewall

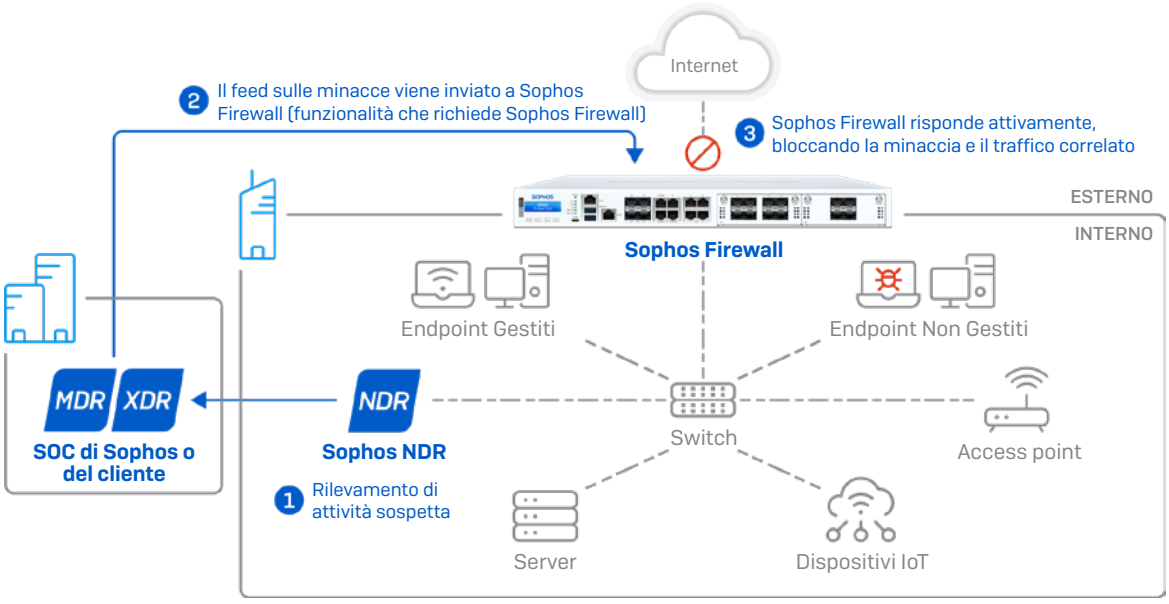
I firewall svolgono un ruolo fondamentale nella protezione del perimetro di rete e nel controllare gli elementi in entrata e in uscita. Sophos NDR è il componente complementare perfetto per la tua soluzione firewall, in quanto questi due prodotti agiscono in perfetta armonia per fornire analisi approfondite e informazioni sulle parti più nascoste della rete, dove il firewall non ha visibilità. Inoltre, include tecnologie in grado di identificare in maniera univoca le attività sospette e malevole nella rete interna, che altrimenti passerebbero inosservate agli occhi di qualsiasi firewall o prodotto di protezione endpoint.

Caratteristiche Principali

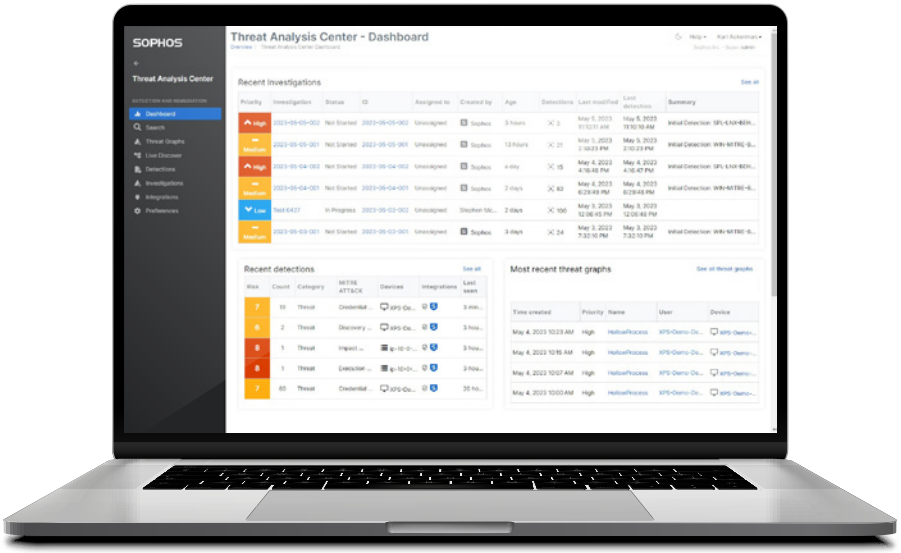
- Il componente aggiuntivo ideale per Sophos XDR e MDR: offre rilevamento nelle parti più nascoste della rete.
- Agisce in perfetta sinergia con il tuo firewall, per rilevare attività di rete sospette e minacce.
- Rileva le attività di rete sospette che provengono da dispositivi sconosciuti o non gestiti, da risorse non autorizzate e da server C2 zero-day.
- Ispeziona i flussi di traffico crittografo, senza compromettere le informazioni sull'identità.
- Distribuzione, configurazione e gestione da Sophos Central.
- Approfitta della Console di indagine per ottenere informazioni approfondite sulle attività di rete sospette e per analizzare o indagare su pattern anomali.

SOPHOS

Sophos NDR Rileva Gli Attacchi Nelle Parti Più Nascoste Della Rete

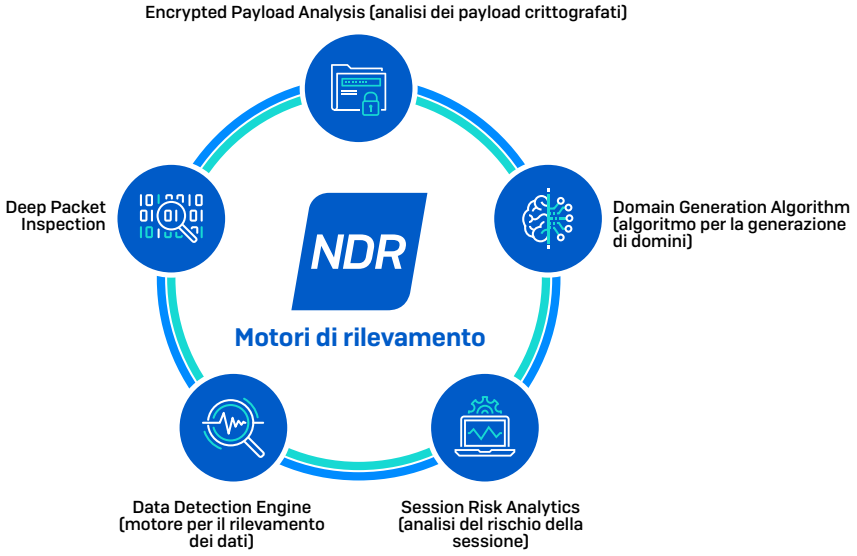


- Monitora il traffico nelle parti più nascoste di una rete, grazie a cinque motori che agiscono in tempo reale.
- Rileva le attività provenienti da tutte le risorse di rete, inclusi i sistemi non gestiti, i dispositivi IoT e le risorse non autorizzate, identificandone l'azienda produttrice e il sistema operativo, nonché eventuali pattern di traffico sospetti provenienti da questi dispositivi.
- Invia dati e avvisi al Data Lake di Sophos Central e al team SOC di MDR, oppure al tuo team XDR.
- Ottieni visibilità e analisi approfondite per tutte le attività della rete e delle applicazioni, nonché per i flussi rischiosi e il traffico sospetto, tutto grazie a una Console di indagine estremamente semplice da usare.
- Se usi Sophos Firewall, puoi usufruire della risposta automatica alle minacce, che blocca immediatamente le minacce e ne impedisce i movimenti laterali.
- Si esegue come appliance virtuale sulle piattaforme hypervisor più utilizzate, come VMware e Hyper-V.
- Si connette direttamente al tuo switch tramite mirroring delle porte SPAN, per monitorare tutto il traffico.
- Ispeziona i dati dei pacchetti crittografati, senza compromettere le informazioni sull'identità.



Motori Di Rilevamento Di Sophos NDR

Sophos NDR include cinque motori di rilevamento che analizzano ininterrottamente i flussi di traffico e applicano le analisi di machine learning basate sull'intelligenza artificiale per identificare attività sospette e dannose nelle parti più nascoste della rete.



Motori di rilevamento	Descrizione
Encrypted Payload Analytics (EPA, analisi dei payload crittografati)	Rileva i server di comando e controllo (C2) zero-day e le nuove varianti di famiglie di malware, basandosi su pattern individuati nelle dimensioni della sessione, nella direzione del traffico e nei tempi di interarrivo.
Domain Generation Algorithms (DGA, algoritmi di generazione del dominio)	Identifica la presenza di tecnologie di generazione dinamica di domini, che vengono sfruttate dal malware per eludere il rilevamento.
Deep Packet Inspection (DPI, ispezione profonda dei pacchetti)	Monitora sia il traffico crittografato che quello non crittografato, utilizzando gli indicatori di compromissione conosciuti, per identificare i cybercriminali e le rispettive TTP (tattiche, tecniche e procedure).
Session Risk Analytics (SRA, analisi del rischio della sessione)	Un potente motore logico che utilizza regole specifiche per segnalare un ampio spettro di fattori di rischio in base alla sessione.
Device Detection Engine (DDE, motore di rilevamento dei dispositivi)	Un motore di query con funzionalità estese, che utilizza un modello predittivo basato sul deep learning per analizzare il traffico crittografato, identificare pattern in flussi di rete non correlati e individuare attività di scansione delle porte e attacchi brute force SSH.

Licenze Sophos NDR

Sophos NDR è il componente complementare perfetto per Sophos XDR e Sophos MDR ed è disponibile come pacchetto di integrazione. I prezzi di Sophos NDR vengono calcolati in base al numero totale di utenti e server di un'organizzazione. L'appliance software virtuale è inclusa nel costo della licenza e puoi distribuire tutti gli NDR Sensor di cui hai bisogno: questa opzione è molto più flessibile e finanziariamente sostenibile delle soluzioni della concorrenza, che prevedono un costo per ogni istanza.

Specifiche Tecniche Di Sophos NDR

Piattaforme supportate

- VMware ESXi6.7 o versione successiva
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) o versioni successive
- Amazon AWS c5n.2xlarge
- Hardware certificati

Hardware	Throughput max	Connessioni/ secondo max	CPU	Memoria
Dell R660 (2 socket)	40Gbps	120.000	64	128 GB
Dell R660 (1 socket)	40Gbps	80.000	32	64 GB
Dell R650	20Gbps	40.000	24	64 GB
Dell R450	10Gbps	20K	16	32 GB
Dell R350	4Gbps	8.000	8	32 GB
Intel NUC 13ª Gen	2.5Gbps	4.000	12	32 GB

Requisiti di sistema per la virtual machine

Le VM Sophos NDR supportano fino a 1 Gbps per sensore:

- Per volumi di traffico medi, ti consigliamo di utilizzare le impostazioni predefinite per la VM:
  - Fino a 500 Mbps
  - Fino a 70.000 pacchetti al secondo
  - Fino a 1.200 flussi al secondo
- Per volumi di traffico più elevati, ridimensiona la VM per 8 vCPU:
  - Fino a 1 Gbps
  - Fino a 300.000 pacchetti al secondo
  - Fino a 4.500 flussi al secondo

Altre risorse:

- Risorse della Community per Sophos NDR
- Come Migliorare L'Efficienza Delle Security Operations Con Sophos Network Detection And Response (NDR)
- Specifiche per gli hardware certificati

Per scoprire di più, visita

sophos.it/ndr

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

24-12-19 DS-IT (MP)

SOPHOS