SOPHOS NDR

Individua e blocca le minacce nella rete dell'era dell'intelligenza artificiale.

Una soluzione per individuare e difendersi dalle minacce note e sconosciute.

Sophos NDR combina analisi comportamentali basate su IA e machine learning, analisi del traffico crittografato, analisi di rete e threat hunting con Deep Packet Inspection e funzionalità IDS/IPS. Opzioni di distribuzione flessibili, risposta attiva in linea e difesa connessa tramite Sophos Fusion aiutano le aziende a estendere la visibilità sulle reti ibride e a monitorare le risorse non gestite e senza agente per bloccare le minacce più rapidamente e rafforzare la difesa coordinata.

77%

dei team IT non ha piena visibilità sugli ambienti ibridi[1]

3,4 ore

tempo mediano impiegato dagli aggressori per prendere di mira Active Directory dopo aver ottenuto l'accesso[2]

3 giorni

tempo mediano prima che un aggressore venga rilevato all'interno di un ambiente[2]

COSA OFFRE SOPHOS NDR

Quattro risultati per una difesa di rete più efficace.

Ottieni maggiore visibilità su tutta la rete.

Ottieni visibilità a livello di rete sulle comunicazioni che coinvolgono risorse gestite, non gestite e senza agente. Identifica comportamenti sospetti e attività di attacco che potrebbero non essere visibili ai singoli controlli.

- Analisi comportamentale per identificare comportamenti sospetti in tutta la rete
- Visibilità sulle risorse non gestite, IoT, OT e senza agente
- Rilevamento del movimento laterale e del comando e controllo

Blocca più rapidamente le minacce.

Riduci il tempo che intercorre tra il rilevamento e la risposta. Su un'appliance Sophos NDR dotata del componente aggiuntivo IDS/IPS, la modalità Active Inline può bloccare automaticamente i pacchetti dannosi noti nel percorso di rete.

- Blocca i pacchetti dannosi noti in tempo reale
- Passa dal monitoraggio passivo alla prevenzione attiva in linea
- Applica la Deep Packet Inspection e le funzionalità IDS/IPS direttamente nel percorso del traffico

Distribuiscila come preferisci.

Distribuisci la soluzione come appliance virtuale, su hardware Sophos NDR dedicato o su hardware di terze parti compatibile. Adatta le attività di monitoraggio e controllo all'architettura, ai requisiti e alla tolleranza al rischio della tua azienda.

- Distribuzioni virtuali illimitate
- Opzioni hardware adatte al tuo ambiente
- Modalità di distribuzione SPAN/TAP e in linea per soddisfare i requisiti operativi

Semplifica le operazioni con Sophos Fusion.

Integra in Sophos Fusion la telemetria di rete, i rilevamenti e il contesto di rete, insieme alle informazioni provenienti da endpoint, firewall, identità, e-mail e cloud, per le indagini e una risposta coordinata.

- Unifica il contesto di rete con le informazioni provenienti da Sophos Fusion
- Arricchisci le indagini Sophos MDR e XDR con la telemetria NDR
- Coordina il rilevamento e la risposta nell'ambito del sistema di difesa Sophos Fusion

SOPHOS NDR IN SINTESI

- L'analisi comportamentale basata su IA e apprendimento automatico scopre minacce sconosciute ed elusive
- Le comprovate capacità di Deep Packet Inspection e di IDS/IPS consentono di identificare le minacce note
- Blocco attivo in linea del traffico malevolo noto
- Opzioni di distribuzione come appliance virtuale, su hardware Sophos dedicato e su hardware di terze parti compatibile

A CHI È DESTINATO SOPHOS NDR?

- Aziende che desiderano colmare le lacune di visibilità della rete
- Team di sicurezza che cercano visibilità sulle risorse non gestite e senza agente
- Aziende che necessitano di opzioni di distribuzione NDR flessibili su reti diverse e distribuite
- MSP e MSSP che ampliano il monitoraggio della rete, il threat hunting e i servizi di sicurezza gestita

IL TUO VANTAGGIO CONTRO LE MINACCE DI RETE

Rilevamento basato sul comportamento e prevenzione attiva, insieme in un'unica soluzione.

Copertura del rilevamento più ampia

Gli aggressori possono sfruttare le lacune di visibilità nelle reti ibride, nei dispositivi non gestiti e nelle risorse senza agente. Sophos NDR combina analisi comportamentale, analisi del traffico crittografato, threat hunting, Deep Packet Inspection e IDS/IPS per rilevare minacce note e sconosciute.

Blocca direttamente le minacce nel percorso di rete

Il solo rilevamento può costringere i team di sicurezza a intervenire dopo che il traffico malevolo ha già raggiunto la sua destinazione. Su un'appliance Sophos NDR con il componente aggiuntivo IDS/IPS, la modalità Active Inline ispeziona il traffico in tempo reale e blocca automaticamente i pacchetti malevoli noti nel percorso di rete.

Difesa connessa tramite Sophos Fusion

Le minacce di rete raramente si presentano in isolamento. Sophos NDR contribuisce a Sophos Fusion con dati di telemetria di rete, rilevamenti e contesto di rete, aiutando i team ad accelerare le indagini e a coordinare la risposta nell'intero sistema di difesa.

COSA DICONO I CLIENTI

"Nel complesso, la mia esperienza con Sophos NDR è stata piuttosto positiva. Aiuta notevolmente ad acquisire visibilità sul comportamento anomalo della rete e a rilevare modelli che normalmente passerebbero inosservati nel monitoraggio tradizionale. Una cosa che apprezzo molto è che gli avvisi sono chiari e facili da interpretare, il che accelera l'analisi e il processo decisionale."[3]

Sicurezza informatica e gestione del rischio, settore bancario — Gartner® Peer Insights™

SOPHOS FUSION

Un unico sistema. Tutti i punti di controllo. Che proteggono come una singola entità.

Sophos NDR fa parte di Sophos Fusion, il più completo sistema di cyber difesa al mondo. Protegge le organizzazioni da minacce guidate dall'IA che agiscono con una rapidità superiore ai tempi di reazione dei team di sicurezza.

sophos.com/NDR →

[1] SolarWinds, Rapporto sullo stato del monitoraggio e dell'osservabilità 2026

[2] Sophos, Active Adversary Report 2026

[3] https://www.gartner.com/reviews/market/network-detection-and-response/vendor/sophos/product/sophos-ndr/review/view/6513218

I contenuti di Gartner Peer Insights sono una raccolta delle opinioni di utenti finali individuali, basate sulle relative esperienze; non devono essere interpretati come affermazioni di fatto, né come rappresentazione delle opinioni di Gartner o dei suoi affiliati. Gartner non appoggia alcun fornitore, produttore o servizio citato nei suoi contenuti, né fornisce alcuna garanzia, espressa o implicita, in riferimento a tali contenuti, alla loro accuratezza o completezza, inclusa qualsivoglia garanzia sulla commerciabilità o sull'idoneità a un particolare scopo.

Gartner® e Peer Insights™ sono marchi registrati di Gartner, Inc. e/o dei suoi affiliati. Tutti i diritti riservati.

© Copyright 2026. Sophos Ltd. Tutti i diritti riservati. Registrata in Inghilterra e Galles con Nº 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito. Sophos è marchio registrato di Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

2026-10-23 SB-IT (TA)

SOPHOS