SOPHOS NDR

Erkennen und stoppen Sie Bedrohungen im Netzwerk des KI-Zeitalters.

Eine Lösung zur Erkennung und Abwehr bekannter und unbekannter Bedrohungen.

Sophos NDR kombiniert KI- und ML-gestützte Verhaltensanalysen, die Analyse verschlüsselten Datenverkehrs, Netzwerkanalysen und Threat Hunting mit Deep Packet Inspection sowie IDS/IPS-Funktionen. Flexible Bereitstellungsoptionen, aktive Inline-Reaktion und vernetzte Abwehr durch Sophos Fusion helfen Unternehmen und Organisationen, die Transparenz über hybride Netzwerke hinweg zu erweitern und nicht verwaltete sowie agentenlose Assets zu überwachen, um Bedrohungen schneller zu stoppen und die koordinierte Abwehr zu stärken.

77 %

der IT-Teams verfügen nicht über vollständige Transparenz in hybriden Umgebungen[1]

3,4 Stunden

Mediane Zeit, bis Angreifer nach Erlangen des Zugriffs Active Directory ins Visier nehmen[2]

3 Tage

Mediane Zeit, bis ein Angreifer innerhalb einer Umgebung erkannt wird[2]

LEISTUNGEN VON SOPHOS NDR

Vier Ergebnisse für eine stärkere Netzwerkabwehr.

Mehr Transparenz im gesamten Netzwerk.

Erhalten Sie Transparenz auf Netzwerkebene für die Kommunikation mit verwalteten, nicht verwalteten und agentenlosen Assets. Identifizieren Sie verdächtiges Verhalten und Angriffsaktivitäten, die für einzelne Kontrollen möglicherweise nicht sichtbar sind.

- Verhaltensanalyse zur Identifizierung verdächtigen Verhaltens im gesamten Netzwerk
- Transparenz bei nicht verwalteten, IoT-, OT- und agentenlosen Assets
- Erkennung von lateralen Bewegungen und Command-and-Control

Schnelleres Stoppen von Bedrohungen.

Verkürzen Sie die Zeit zwischen Erkennung und Reaktion. Auf einer Sophos NDR-Appliance mit dem IDS/IPS-Add-on kann der Active Inline-Modus bekannte schädliche Pakete im Netzwerkpfad automatisch blockieren.

- Blockieren Sie bekannte schädliche Pakete in Echtzeit
- Wechseln Sie von passiver Überwachung zu aktiver Inline-Prävention
- Wenden Sie Deep Packet Inspection und IDS/IPS direkt im Pfad des Datenverkehrs an

Bereitstellung nach Ihren Wünschen.

Stellen Sie die Lösung als virtuelle Appliance, auf dedizierter Sophos NDR-Hardware oder auf kompatibler Hardware von Drittanbietern bereit. Passen Sie Überwachung und Durchsetzung an Ihre Architektur, Anforderungen und Risikotoleranz an.

- Unbegrenzte virtuelle Bereitstellungen
- Hardware-Optionen passend für Ihre Umgebung
- SPAN/TAP- und Inline-Bereitstellungsmodi passend zu den betrieblichen Anforderungen

Vereinfachen Sie den Betrieb mit Sophos Fusion.

Führen Sie Netzwerk-Telemetrie, Erkennungen und Kontext mit Erkenntnissen zu Endpoint, Firewall, Identität, E-Mail und Cloud in Sophos Fusion zusammen, um Analysen und koordinierte Reaktionen zu ermöglichen.

- Vereinheitlichen Sie den Netzwerkkontext mit Erkenntnissen aus Sophos Fusion
- Reichern Sie Sophos MDR- und XDR-Analysen mit NDR-Telemetrie an
- Koordinieren Sie Erkennung und Reaktion im gesamten Sophos Fusion-Abwehrsystem

SOPHOS NDR AUF EINEN BLICK

- KI- und ML-gestützte Verhaltensanalysen decken unbekannte und schwer erkennbare Bedrohungen auf
- Bewährte Funktionen für Deep Packet Inspection und IDS/IPS identifizieren bekannte Bedrohungen
- Aktives Inline-Blockieren von bekanntem schädlichem Datenverkehr
- Bereitstellungsoptionen als virtuelle Appliance, auf dedizierter Sophos-Hardware und auf kompatibler Hardware von Drittanbietern

SOPHOS NDR IST IDEAL GEEIGNET FÜR

- Unternehmen, die Sichtbarkeitslücken im Netzwerk schließen möchten
- Sicherheitsteams, die Transparenz über nicht verwaltete und agentenlose Assets gewinnen möchten
- Unternehmen, die eine flexible NDR-Bereitstellung in diversen und verteilten Netzwerken benötigen
- MSPs und MSSPs, die ihre Netzwerküberwachung, ihr Threat Hunting und ihre Managed Security Services erweitern möchten

IHR VORTEIL GEGENÜBER NETZWERKBEDROHUNGEN

Verhaltenserkennung und aktive Prävention vereint.

Umfassendere Erkennungsabdeckung

Angreifer können Sichtbarkeitslücken in hybriden Netzwerken, nicht verwalteten Geräten und agentenlosen Assets ausnutzen. Sophos NDR kombiniert Verhaltensanalysen, Analyse von verschlüsseltem Datenverkehr, Threat Hunting, Deep Packet Inspection und IDS/IPS, um bekannte und unbekannte Bedrohungen zu erkennen.

Bedrohungen direkt im Netzwerkpfad blockieren

Die Erkennung allein kann dazu führen, dass Sicherheitsteams erst reagieren, wenn schädlicher Datenverkehr bereits sein Ziel erreicht hat. Auf einer Sophos NDR-Appliance mit dem IDS/IPS-Add-on untersucht der Active Inline-Modus den Traffic in Echtzeit und blockiert automatisch bekannte schädliche Pakete im Netzwerkpfad.

Vernetzte Verteidigung durch Sophos Fusion

Netzwerkbedrohungen treten selten isoliert auf. Sophos NDR liefert Netzwerk-Telemetrie, Erkennungen und Kontext an Sophos Fusion und hilft Teams dabei, Analysen zu beschleunigen und die Reaktion im gesamten Abwehrsystem zu koordinieren.

DAS SAGEN UNSERE KUNDEN

„Insgesamt sind meine Erfahrungen mit Sophos NDR sehr gut. Die Lösung trägt wesentlich dazu bei, Einblicke in ungewöhnliches Netzwerkverhalten zu gewinnen und Muster zu erkennen, die bei herkömmlicher Überwachung normalerweise unentdeckt bleiben würden. Was ich sehr schätze, ist, dass die Warnmeldungen klar und leicht zu interpretieren sind, was die Analyse und Entscheidungsfindung beschleunigt.“[3]

IT-Sicherheit und Risikomanagement, Bankwesen — Gartner® Peer Insights™

SOPHOS FUSION

Ein System. Verschiedenste Kontrollpunkte. Eine zentrale Abwehr.

Sophos NDR ist Teil von Sophos Fusion, dem weltweit umfassendsten Cyberabwehrsystem. Es schützt Unternehmen und Organisationen vor KI-gestützten Bedrohungen, die sich schneller bewegen, als die Cyberabwehr reagieren kann.

sophos.com/NDR →

[1] SolarWinds, 2026 State of Monitoring & Observability Report

[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

Gartner Peer Insights geben die subjektiven Meinungen einzelner Enduser wieder, die auf deren eigenen Erfahrungen basieren. Sie sind in keinem Fall als Tatsachenfeststellung zu werten und repräsentieren nicht die Ansichten von Gartner oder seinen verbundenen Unternehmen. Gartner befürwortet in dieser Publikation keine bestimmten Hersteller, Produkte oder Dienstleistungen und übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

Gartner® und Peer Insights™ sind eingetragene Marken von Gartner, Inc. und/oder seiner verbundenen Unternehmen. Alle Rechte vorbehalten.

© Copyright 2026. Sophos Ltd. Alle Rechte vorbehalten. Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB. Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

2026-10-23 SB-DE (TA)

SOPHOS