Sophos Network Detection and Response

Das leistungsstarke Add-on zu Sophos XDR und Sophos MDR

Sophos NDR überwacht in Zusammenarbeit mit Ihren verwalteten Endpoints und Firewalls Netzwerkaktivitäten und erkennt verdächtige und schädliche Muster, die Lösungen nicht sehen können. Sophos NDR erkennt ungewöhnliche Datenverkehrsflüsse von nicht verwalteten Systemen und IoT-Geräten, nicht autorisierte Assets, interne Bedrohungen, bisher unbekannte Zero-Day-Angriffe und ungewöhnliche Muster tief im Netzwerk.

Sophos NDR bietet wichtige Einblicke in Netzwerkaktivitäten, die andere Produkte übersehen

Raffinierte Angreifer wissen, wie sie Erkennungsmechanismen überlisten. Aber um ihre Angriffe auszuführen, müssen sie sich im Netzwerk bewegen. Sophos NDR erkennt verdächtige Netzwerkverkehrsmuster, die Ihre verwalteten Endpoints und Ihre Firewalls übersehen, darunter:

- **Unbekannte oder ungeschützte Netzwerkgeräte** – einschließlich legitimer IoT- oder OT-Geräte, die nicht vollständig mit einem Endpoint-Sensor verwaltet werden können, sowie unbekannte oder nicht identifizierte Systeme im Netzwerk. Diese Geräte können im Rahmen eines Angriffs kompromittiert werden. Sophos NDR identifiziert und überwacht solche Geräte auf verdächtige oder böswillige Verhaltensweisen, die auf einen Angriff hindeuten könnten.
- **Nicht autorisierte Assets** – Werden diese ins Netzwerk eingebracht und sind vielleicht bereits kompromittiert oder werden zum Starten eines Angriffs verwendet, können sie von Sophos NDR leicht erkannt und überwacht werden.
- **Neue und zuvor noch nicht beobachtete Command-and-Control(C2)-Aktivitäten** – Viele Angriffe und Sicherheitsverletzungen werden remote gesteuert und wirken wie legitime Kommunikationen im Netzwerk. Sophos NDR kann neue Zero-Day-C2-Aktivitäten erkennen und gezielte, hoch spezialisierte Angriffe somit bereits im Anfangsstadium aufdecken.
- **Verdächtige oder schädliche Netzwerkverkehrsflüsse und -muster** – Diese können wichtige Signale bei der Früherkennung eines Cyberangriffs sein. Beispiele: ungewöhnliche Netzwerk-Aktivitäten oder Remote-Zugriff außerhalb der Geschäftszeiten, verdächtige Daten-Uploads oder Exfiltration, ungewöhnliche Datenverkehrsmuster sowie schädlicher Datenverkehr, der von bekannter Malware generiert wird.

NDR arbeitet mit Ihrer Firewall

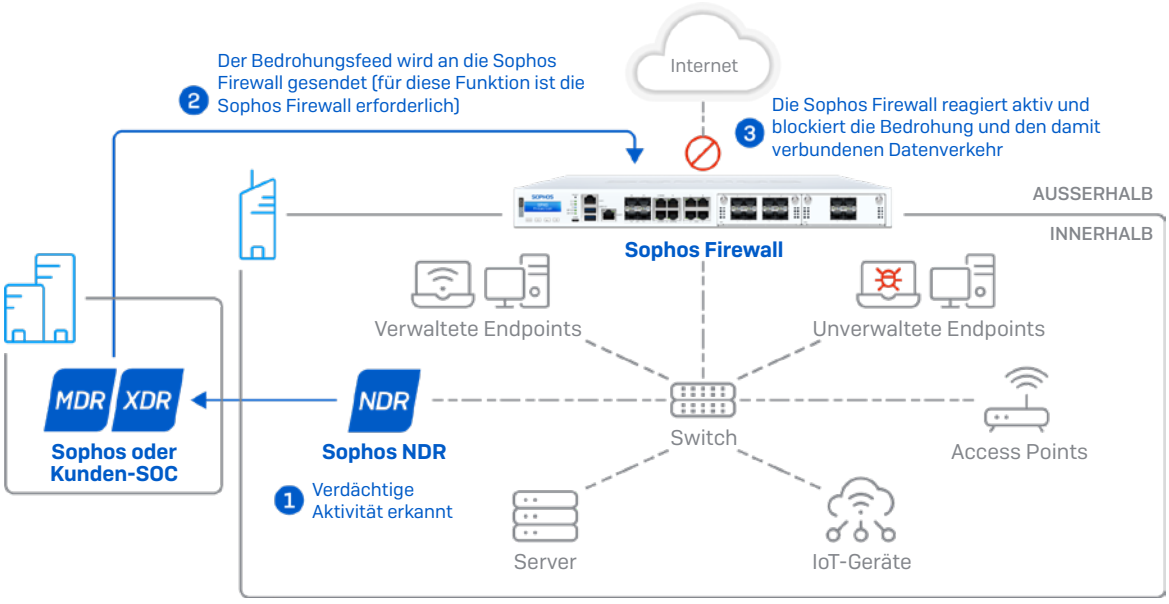
Firewalls spielen eine wichtige Rolle bei der Sicherung Ihrer Netzwerkgrenze und kontrollieren ein- und ausgehende Datenbewegungen. Sophos NDR ist die perfekte Ergänzung zu Ihrer Firewall-Lösung, denn NDR liefert wichtige Erkenntnisse aus tiefen Bereichen des Netzwerks, die für Ihre Firewall nicht sichtbar sind. NDR umfasst auch Technologien zur eindeutigen Identifizierung verdächtiger und böswilliger Aktivitäten, die Ihr internes Netzwerk passieren und sonst von Firewall- oder Endpoint-Produkten nicht erkannt werden können.

Vorteile auf einen Blick

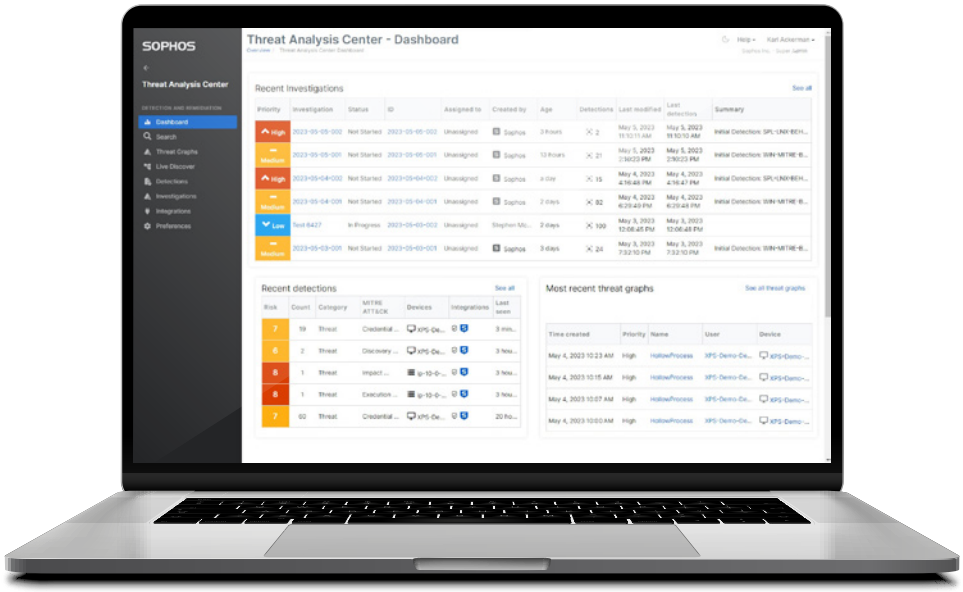
- Die perfekte Ergänzung zu Sophos XDR und Sophos MDR, erkennt Gefahren tief im Netzwerk
- Erkennt in Zusammenarbeit mit Ihrer Firewall Netzwerkaktivitäten und Bedrohungen
- Identifiziert verdächtige Netzwerkaktivitäten von unbekannten und nicht verwalteten Geräten, nicht autorisierten Assets und Zero-Day-C2-Servern
- Prüft verschlüsselte Datenflüsse, ohne personenbezogene Daten zu gefährden
- Praktische Bereitstellung, Konfiguration und Verwaltung über Sophos Central

SOPHOS

Sophos NDR erkennt Angriffe, die sich tief im Netzwerk verbergen

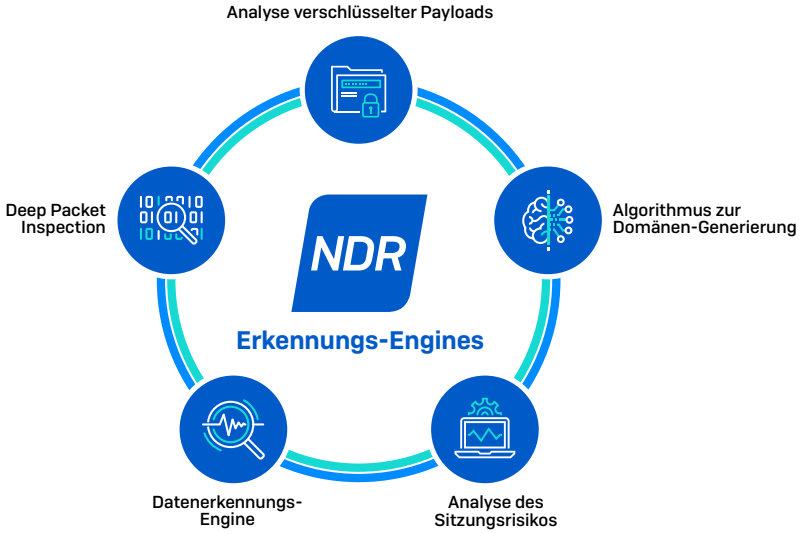


- Überwacht den Datenverkehr tief im Netzwerk mithilfe von fünf Echtzeit-Engines.
- Erkennt Aktivitäten von nicht verwalteten Systemen, IoT-Geräten, nicht autorisierten Benutzern oder Assets und allen anderen Quellen des Netzwerkverkehrs.
- Leitet Daten und Warnmeldungen weiter: an den Sophos Central Data Lake und das Sophos MDR-Team oder an Ihr XDR-Team.
- Wenn Sie eine Sophos Firewall haben, steht eine automatisierte Bedrohungsreaktion zur Verfügung, um eine Bedrohung sofort zu blockieren und laterale Bewegungen zu unterbinden.
- Wird als virtuelle Appliance auf gängigen Hypervisor-Plattformen wie VMware und Hyper-V ausgeführt.
- Verbindet sich per SPAN Port Mirroring direkt mit Ihrem Switch und überwacht den gesamten Datenverkehr.
- Prüft verschlüsselte Paketdaten, ohne personenbezogene Daten zu gefährden.



Sophos NDR Detection Engines

Sophos NDR arbeitet mit fünf Erkennungs-Engines, die den Netzwerkverkehr kontinuierlich analysieren und mittels KI-Machine-Learning-Analysen verdächtige und schädliche Aktivitäten tief in Ihrem Netzwerk erkennen.



Erkennungs-Engines	Beschreibung
Encrypted Payload Analytics (EPA)	Erkennt Zero-Day-C2-Server und neue Varianten von Malware-Familien auf Basis von Mustern in der Sitzungsgröße, -richtung und in Interarrival-Zeiten.
Domain Generation Algorithms (DGA)	Erkennt Technologien zur dynamischen Domänen-Generierung, die Malware nutzt, um unerkannt zu bleiben.
Deep Packet Inspection (DPI)	Überwacht sowohl verschlüsselten als auch unverschlüsselten Datenverkehr mithilfe bekannter IOCs, um Angreifer und TTPs schnell zu erkennen.
Session Risk Analytics (SRA)	Leistungsstarke Logik-Engine, sendet mittels Regeln Warnmeldungen über eine Vielzahl sitzungsbasierter Risikofaktoren.
Device Detection Engine (DDE)	Erweiterbare Abfrage-Engine, analysiert verschlüsselten Datenverkehr mithilfe eines Deep-Learning-Prognosemodells über nicht zusammenhängende Netzwerkflüsse hinweg auf Muster.

Sophos NDR-Lizenzierung

Sophos NDR ist die perfekte Ergänzung zu Sophos XDR und Sophos MDR und als Integrationspaket erhältlich. Die Preise für Sophos NDR basieren auf der Gesamtzahl der Benutzer und Server eines Unternehmens. Die Software für die virtuelle Appliance ist in der Lizenz enthalten und Sie können so viele NDR-Sensoren wie gewünscht bereitstellen. Damit ist NDR bei uns günstiger und flexibler als bei anderen Anbietern, die NDR pro Instanz in Rechnung stellen.

Technische Spezifikationen von Sophos NDR

Unterstützte Plattformen

- VMware ESXi6.7 und höher
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) oder höher
- Amazon AWS c5n.2xlarge
- Zertifizierte Hardware

Hardware	Max. Durchsatz	Max. Verbindungen/ Sek.	CPUs	Speicher
Dell R660 (2 Sockel)	40 GBit/s	120.000	64	128 GB
Dell R660 (1 Sockel)	40 GBit/s	80.000	32	64 GB
Dell R650	20 GBit/s	40.000	24	64 GB
Dell R450	10 GBit/s	20.000	16	32 GB
Dell R350	4 GBit/s	8.000	8	32 GB
Intel Nuc, 13. Gen.	2,5 GBit/s	4.000	12	32 GB

VM-Systemanforderungen

Sophos NDR VMs unterstützen bis zu 1 GBit/s pro Sensor:

- Verwenden Sie für mittlere Datenverkehrsvolumen die VM-Standardeinstellungen:
  - Bis zu 500 MBit/s
  - Bis zu 70.000 Pakete/Sek.
  - Bis zu 1.200 Datenflüsse/Sek.
- Erweitern Sie die VM bei hohen Datenverkehrsvolumen auf 8 vCPUs:
  - Bis zu 1 GBit/s
  - Bis zu 300.000 Pakete/Sek.
  - Bis zu 4.500 Datenflüsse/Sek.

Weiterführende Informationen

- Sophos NDR – Community-Ressourcen
- Optimierte Security Operations mit Sophos Network Detection and Response (NDR)
- Zertifizierte Hardware – Spezifikationen

Weitere Informationen unter

sophos.de/ndr

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

24-05-23 DS-DE (PC)

SOPHOS