

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.



Lösung

Security & Identity

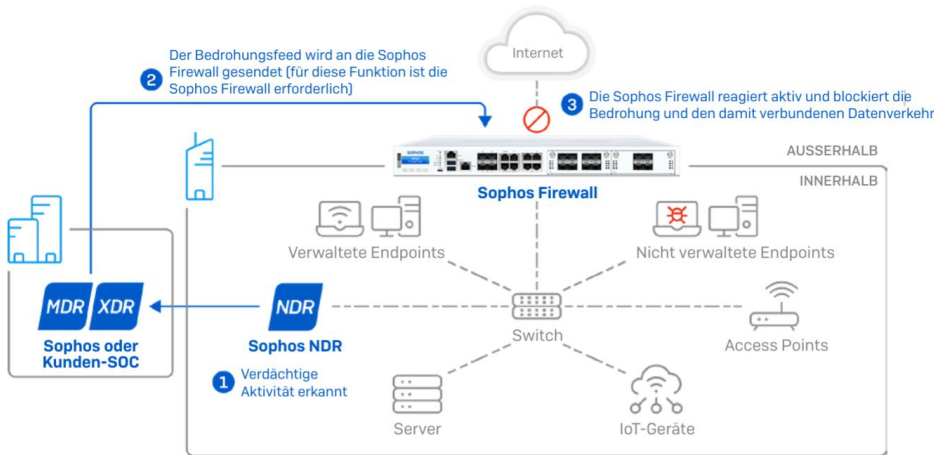
Produkt

Network Detection
Response

Vorteile im Überblick

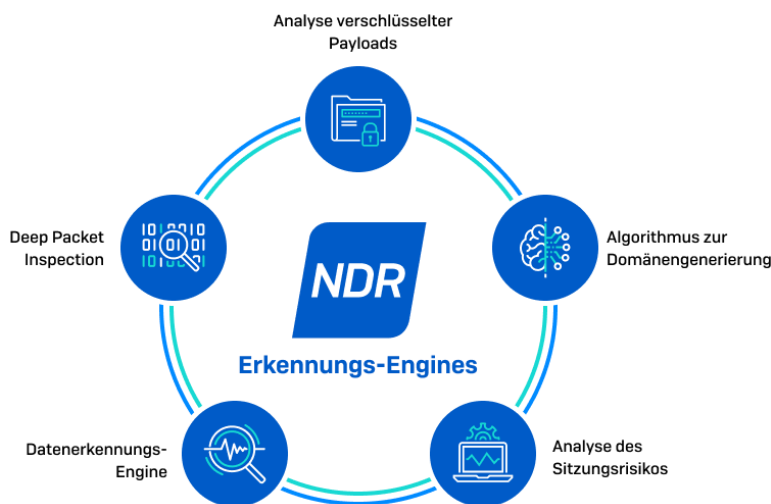
- Die perfekte Ergänzung zu Sophos XDR und Sophos MDR, erkennt Gefahren tief im Netzwerk.
- Erkennt in Zusammenarbeit mit Ihrer Firewall Netzwerkaktivitäten und Bedrohungen.
- Identifiziert verdächtige Netzwerkaktivitäten von unbekanntem und nicht verwalteten Geräten, nicht autorisierten Assets und ZeroDay-C2-Servern.
- Prüft verschlüsselte Datenflüsse, ohne personenbezogene Daten zu gefährden.
- Praktische Bereitstellung, Konfiguration und Verwaltung über Sophos Central.
- Bietet über die Untersuchungskonsole Einblick in verdächtige Netzwerkaktivitäten und die Möglichkeit, Traffic-Anomalien zu analysieren und zu untersuchen.

Sophos NDR erkennt Angriffe, die sich tief im Netzwerk verbergen



- Überwacht den Datenverkehr tief im Netzwerk mithilfe von fünf Echtzeit-Engines.
- Erkennt Aktivitäten aller Netzwerk-Assets, einschließlich nicht verwalteter Systeme, IoT-Geräte und nicht autorisierter Assets, und identifiziert den Hersteller und das Betriebssystem sowie verdächtige Datenverkehrsmuster, die von diesen Geräten ausgehen.
- Leitet Daten und Warnmeldungen weiter: an den Sophos Central Data Lake und das Sophos MDR-Team oder an Ihr XDR-Team.
- Bietet über eine benutzerfreundliche Untersuchungskonsole Transparenz und Einblick in Netzwerk- und Anwendungsaktivitäten, riskante Abläufe und verdächtigen Datenverkehr.
- 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 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.



Lösung

Security & Identity

Produkt

Network Detection Response

Vorteile im Überblick

- 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 unbekanntem und nicht verwalteten Geräten, nicht autorisierten Assets und ZeroDay-C2-Servern.
- Prüft verschlüsselte Datenflüsse, ohne personenbezogene Daten zu gefährden.
- Praktische Bereitstellung, Konfiguration und Verwaltung über Sophos Central.
- Bietet über die Untersuchungskonsole Einblick in verdächtige Netzwerkaktivitäten und die Möglichkeit, Traffic-Anomalien zu analysieren und zu untersuchen.

Sophos NDR Detection Engines und Anwendungsfälle

Detection Engines	Beschreibung
Verschlüsselte Nutzdatenanalyse (EPA)	Erkennung von Zero-Day Command-and-Control (C2)-Servern und neuen Varianten von Malware-Familien auf der Grundlage von Mustern in Bezug auf Sitzungsgröße, -richtung und Intervallzeiten.
Bereichserzeugungsalgorithmen (DGA)	Identifiziert das Vorhandensein einer dynamischen Domain-Generierungstechnologie, die von Malware verwendet wird, um eine Erkennung zu vermeiden.
Deep Packet Inspection (DPI)	Überwacht sowohl verschlüsselten als auch unverschlüsselten Datenverkehr mithilfe bekannter IoCs, um Bedrohungsakteure und TTPs schnell zu identifizieren.
Sitzungsrisiko-Analyse (SRA)	Leistungsstarke Logik-Engine, die Regeln verwendet, die bei einer Vielzahl von sitzungsbasierten Risikofaktoren Alarm schlagen.
Geräteerkennungsmodul (DDE)	Erweiterbare Abfrage-Engine, analysiert verschlüsselten Datenverkehr mithilfe eines DeepLearning-Prognosemodells über nicht zusammenhängende Netzwerkflüsse hinweg auf Muster und erkennt Port Scanning und SSH-Brute-Force-Aktivitäten.



Lösung

Security & Identity

Produkt

Network Detection Response

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 Verbindung / 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
Del R560	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

Vorteile im Überblick

- 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 unbekanntem und nicht verwalteten Geräten, nicht autorisierten Assets und ZeroDay-C2-Servern.
- Prüft verschlüsselte Datenflüsse, ohne personenbezogene Daten zu gefährden.
- Praktische Bereitstellung, Konfiguration und Verwaltung über Sophos Central.
- Bietet über die Untersuchungskonsole Einblick in verdächtige Netzwerkaktivitäten und die Möglichkeit, Traffic-Anomalien zu analysieren und zu untersuchen.