Sophos Network Detection and Response

Erkennen Sie schneller verdächtige Aktivitäten in Ihrer Umgebung

Wenn ein Angreifer in Ihre Umgebung gelangt ist, zählt jede Sekunde. Oft fehlen jedoch die nötige Transparenz und Einsicht in wichtige Daten, um schnell genug zu reagieren. Und noch komplizierter wird es, wenn Ihre Sicherheitstools nicht gut zusammenarbeiten.

Umfassende Daten für eine genaue Erkennung

Unternehmen und Einrichtungen benötigen ein ganzheitliches Konzept zum Erkennen und Bekämpfen von Bedrohungen sowie schnellere Möglichkeiten zum Korrelieren von Daten, die immer umfangreicher und vielfältiger werden. Je detaillierter die Transparenz und der Kontext, desto präziser die Analyse der Bedrohungsaktivitäten. Das bedeutet im Klartext: Wenn Sicherheits-Telemetriedaten zusammengeführt werden, ergibt sich ein genaueres Bild des gesamten Angriffspfads.

Als Add-on zu Sophos MDR überwacht die virtuelle Appliance Sophos Network Detection and Response (NDR) den Netzwerkverkehr auf verdächtige Datenflüsse. Erkennungen werden an den Sophos Data Lake gesendet, ausgewertet und mit einer Risikobewertung versehen. Dabei werden Fälle generiert, die das Sophos Threat Response Team analysiert und validiert. NDR-Erkennungen können Analysen interner Host-Verbindungen zu Netzwerk-Servern auslösen und auch zur Ergänzung von Threat Hunts nach Endpoint-Aktivitäten genutzt werden, um zu bestimmen, welche Geräte kommunizieren.

Sicherheitstools, die zusammenarbeiten

Als native Sophos MDR-Integration kann Sophos NDR problemlos und störungsfrei eingebunden werden – ohne abweichende Risikobewertungen oder langwierige Einrichtung wie bei anderen Lösungen.

Sophos NDR wird als virtuelle Appliance angeboten. Nach der Bereitstellung authentifiziert sich Sophos NDR bei der Sophos Central Management-Konsole und beginnt mit dem Senden von Daten. NDR-Status und -Erkennungen werden in Sophos Central angezeigt. In der folgenden Tabelle sind die Funktionen der einzelnen Erkennungs-Engines von Sophos NDR beschrieben.

Vorteile auf einen Blick

- Erweitert Sophos MDR um Netzwerk-Erkennungen, um verdächtige Netzwerkflüsse zu überwachen, auf die Endpoint-Software keinen Zugriff hat
- Ermöglicht Bedrohungsanalysen und Suchen nach internen Host-Verbindungen zu Netzwerkdiensten und anderen Netzwerkverbindungen
- Erkennt Malware auch im verschlüsselten Datenverkehr
- Zeigt den NDR-Sensor-Status und NDR-Erkennungen in Sophos Central an

Erkennungs-Engines und Anwendungsfälle

Erkennungs-Engines	Beschreibung
Encrypted Payload Analytics (EPA)	Erkennt Zero-Day Command-and-Control(C2)-Server und neue Varianten von Malware-Familien auf Basis von Mustern in der Session-Größe, -Richtung und Interarrival-Zeiten.
Domain Generation Algorithms (DGA)	Erkennt Technologien zur dynamischen Domänengenerierung, 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, die mittels Regeln Warnmeldungen über eine Vielzahl sitzungsbasierter Risikofaktoren sendet.
Device Detection Engine (DDE)	Erweiterbare Abfrage-Engine, die verschlüsselten Datenverkehr mithilfe eines Deep-Learning-Prognosemodells über nicht zusammenhängende Netzwerkflüsse hinweg auf Muster analysiert.

SOPHOS

Erkennen Sie verdächtiges Verhalten überall – nicht nur auf Ihren Endpoints

Sophos NDR verwendet unabhängige Engines zur Bedrohungserkennung, um ungewöhnliche und verdächtige Verhaltensweisen im Netzwerkverkehr zu erkennen, u. a.:

- Verbindungen von unbekannten Geräten
- Während einer Remote-Sitzung hochgeladene Daten
- Verstärkte Nutzung von Dateien mit proprietären Daten
- Von Malware-Familien generierte Netzwerksitzungen

Mit der Fähigkeit, potenziell schädliches Verhalten zu erkennen, identifiziert Sophos NDR:

- **Ungeschützte Geräte** – Sophos NDR erkennt legitime Geräte, die nicht geschützt sind und als Eintrittspunkte für Cyberangriffe missbraucht werden könnten.
- **Rogue Assets** – Sophos NDR überwacht nicht nur den Datenverkehr zu ungeschützten Geräten, sondern erkennt auch nicht autorisierte Geräte, die über das Netzwerk kommunizieren.
- **IoT- und OT-Sensoren** – IoT(Internet of Things)- und OT(Operational Technology)-Geräte lassen sich nur schwer auf Bedrohungen überwachen, da auf vielen dieser Geräte kein Endpoint-Protection-Agent installiert werden kann. Sophos NDR überwacht Daten von IoT- und OT-Geräten auf Angriffsaktivitäten.
- **Zero-Day-Angriffe** – Sophos NDR verfügt über ein patentiertes Verfahren zur Erkennung von Zero-Day-C2-Servern, die von Angreifern verwendet werden – auf Basis von Mustern in der Session-Größe, -Richtung und Interarrival-Zeiten.
- **Interne Bedrohungen** – Sophos NDR bietet Einblick in den Netzwerkverkehr und Datenexfiltrationen, die innerhalb der Netzwerkgrenzen auf den ersten Blick „normal“ erscheinen können.

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. Die Systemvoraussetzungen für Sophos NDR finden Sie in der folgenden Tabelle.

Systemvoraussetzungen

Netzwerk-Durchsatz	1 GBit/s	5 GBit/s	10 GBit/s
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
Speicher	160 GB	320 GB	640 GB
Geschätzte Benutzerzahl*	Bis zu 2.000	Bis zu 10.000	Bis zu 30.000

* Variiert je nach Unternehmen/Einrichtung.

Mehr erfahren unter

sophos.de/ndr

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

22-11-15 DS-DE (DD)

SOPHOS