Sophos Network Detection and Response

Monitor Network Traffic to Identify Suspicious Activity Faster

Every second counts when an adversary is in your environment. Yet all too often, defenders are slowed down by limited visibility and insights. And this becomes even more complicated when security tools don't work well together.

The Most Comprehensive Data Drives the Most Accurate Detection Strategy

Organizations can benefit from a holistic approach to threat detection and response and faster ways to correlate an ever-growing volume and variety of data. The deeper the visibility and context, the more precise the investigation into threat activity. That means when security telemetry can come together, it paints a more accurate picture of the entire attack path.

As an add-on to Sophos MDR, the Sophos Network Detection and Response (NDR) virtual appliance monitors network traffic to identify suspicious network flows. Detections are sent to the Sophos data lake, evaluated, and assigned a corresponding risk score, generating cases for the Sophos threat response team to investigate and validate. NDR detections can trigger an investigation into internal host connections to network servers and can also be used to enrich threat hunts for endpoint activity to determine which devices are communicating.

Your Security Needs Tools That Work Well Together

Sophos NDR is a native Sophos MDR integration. It readily connects, does not produce excessive noise or mismatched risk scores, and does not require time to establish a baseline like other solutions. The table below describes the functionality of Sophos NDR's detection engines.

Sophos NDR is delivered as a virtual appliance. Once deployed, it authenticates with the Sophos Central management console and starts sending data. NDR status and detections are viewable in Sophos Central.

Highlights

- Add network detections to Sophos MDR to monitor suspicious network flows that endpoint software can't access
- Enable threat investigations and hunts into internal host connections to network services and other network connections
- Detect malware within encrypted traffic where it often remains hidden
- Easily view NDR sensor status and detections in Sophos Central

Sophos NDR Detection Engines and Use Cases

Detection Engines	Description
Encrypted Payload Analytics (EPA)	Detects zero-day command-and-control (C2) servers and new variants of malware families based on patterns found in session size, direction, and interarrival times.
Domain Generation Algorithms (DGA)	Identifies the presence of dynamic domain generation technology used by malware to avoid detection.
Deep Packet Inspection (DPI)	Monitors both encrypted and unencrypted traffic using known IoCs to rapidly identify threat actors and TTPs.
Session Risk Analytics (SRA)	Powerful logic engine that utilizes rules that alert on a multitude of session-based risk factors.
Device Detection Engine (DDE)	Extensible query engine that uses a deep learning prediction model to analyze encrypted traffic for patterns across unrelated network flows.

SOPHOS

Recognize Suspicious Behavior Beyond Your Endpoints

Sophos NDR uses independent threat detection engines to detect suspicious and abnormal network traffic behaviors like:

- Connections from an unknown device
- Data uploaded during a remote session
- Increased use of proprietary data files
- Network sessions generated by malware families

With the ability to detect potentially malicious behaviors, Sophos NDR identifies:

- **Unprotected Devices** – Sophos NDR identifies legitimate devices that haven't been protected and could be used as entry points for cyberattacks.
- **Rogue Assets** – In addition to monitoring traffic to unprotected devices, Sophos NDR identifies unauthorized devices that communicate across the network.
- **IoT and OT Sensors** – Internet of Things (IoT) and operational technology (OT) devices represent challenges to threat monitoring because many of these devices cannot support an endpoint protection agent. Sophos NDR monitors data from IoT and OT devices to detect attacker activity.
- **Zero-Day Attacks** – Sophos NDR has a patented process for detecting zero-day C2 servers used by attackers based on patterns found in session packet size, direction, and interarrival times.
- **Insider Threats** – Sophos NDR provides visibility into network traffic flows and data exfiltration that may initially appear "normal" from those on the inside.

Sophos NDR pricing is based on an organization's total number of users and servers. The virtual appliance software is included with the license. The table below describes Sophos NDR system requirements.

Sophos NDR System Requirements

Network Throughput	1 Gbps	5 Gbps	10 Gbps
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
Storage	160 GB	320 GB	640 GB
Estimated User Range*	Up to 2,000	Up to 10,000	Up to 30,000

*Will vary by organization.

Learn more about Sophos NDR

sophos.com/ndr

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-11-29 DS-EN (DD)

SOPHOS