Sophos Network Detection and Response

A Powerful Addition to Sophos XDR and Sophos MDR

Sophos NDR works together with your managed endpoints and firewalls to monitor network activity for suspicious and malicious patterns solutions cannot see. Sophos NDR detects abnormal traffic flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.

Sophos NDR Provides Critical Visibility Into Network Activity That Other Products Miss

Attackers are skilled at evading detection, but every attack needs to move around a network. Sophos NDR detects suspicious network traffic patterns that go unseen by your managed endpoints and firewalls, including:

- **Unknown or Unprotected Network Devices** – including legitimate IoT or OT devices that cannot be fully managed with an endpoint sensor, as well as unknown or unidentified systems on the network. These devices may be compromised or become compromised as part of an attack. Sophos NDR identifies and monitors these devices for suspicious or malicious behavior that might signal an attack.
- **Unauthorized or Rogue Assets** – that are brought onto the network that may already be compromised or used to launch an attack can be readily identified and monitored by Sophos NDR.
- **New and Previously Unseen Command and Control (C2) Activity** – many attacks or breaches are orchestrated remotely using what looks like legitimate communications between a bad actor and their remote processes inside the network. Sophos NDR can detect new zero-day C2 activity to identify a bespoke, targeted attack that may be just getting started.
- **Suspicious or Malicious Network Traffic Flows and Patterns** – can be important signals in the early identification of a cyberattack. Indications can include unusual off-hours network activity or remote access, suspicious data uploads or exfiltration, abnormal traffic patterns, and malicious traffic generated by known malware.

NDR Works With Your Firewall

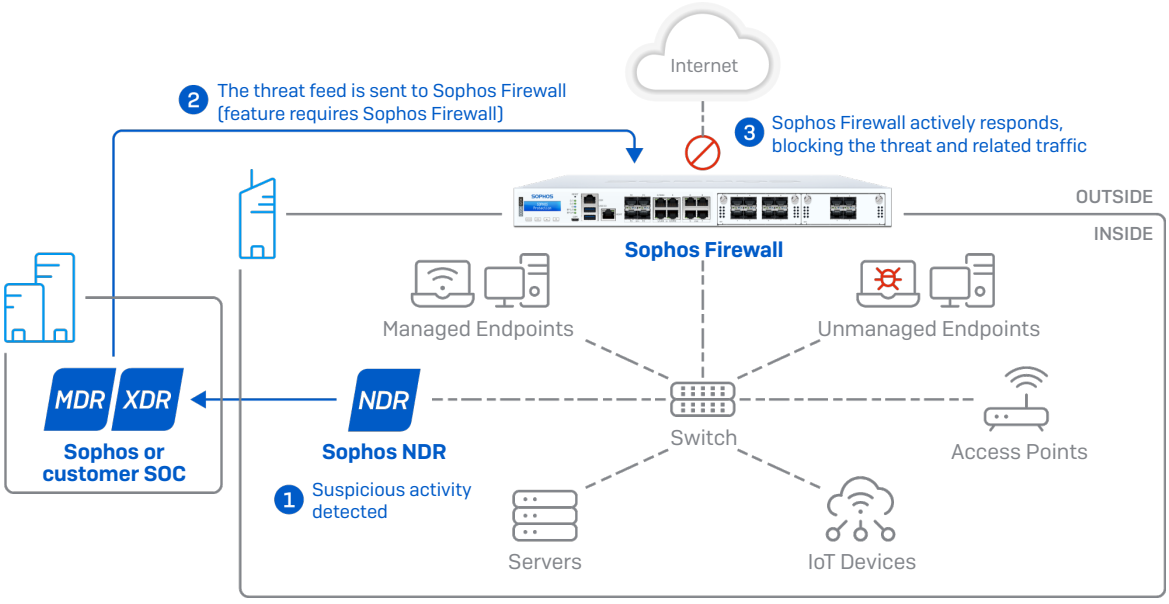
Firewalls play a critical role in securing your network perimeter and controlling what comes and goes. Sophos NDR is the perfect complement to your firewall solution, as they work together to provide insights and coverage deep inside the network where your firewall lacks visibility. It also includes technologies that uniquely identify suspicious and malicious activity traversing your internal network that can't otherwise be detected by any firewall or endpoint protection product.

Highlights

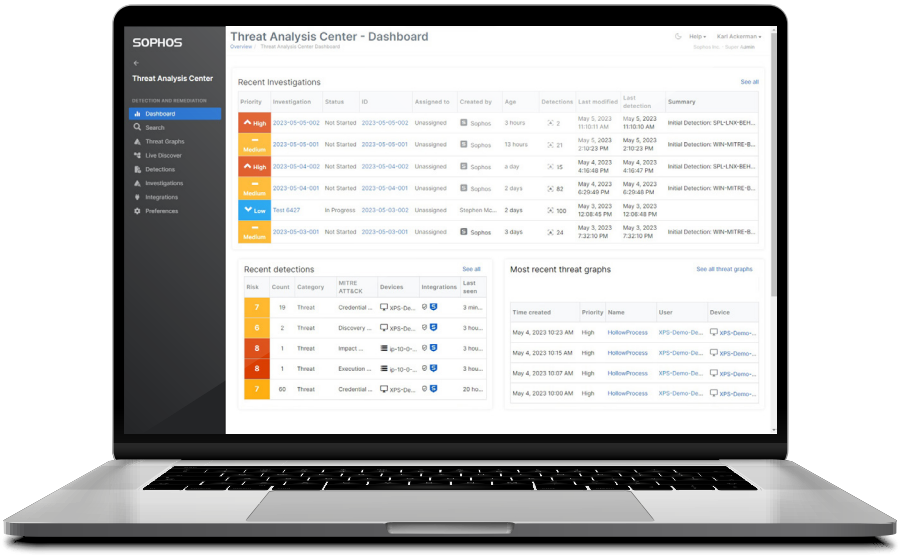
- The perfect addition to Sophos XDR and MDR, providing detections deep within a network.
- Works with your firewall to detect network activity and threats.
- Detects suspicious network activity originating from unknown or unmanaged devices, rogue assets, and zero-day C2 servers.
- Inspects encrypted traffic flows without compromising PII.
- Deploy, configure, and manage from Sophos Central.
- Utilize the Investigation Console to gain insights into suspicious network activity and analyze or investigate anomalous patterns.

SOPHOS

Sophos NDR Operates Deep Within Your Network to Detect an Attack

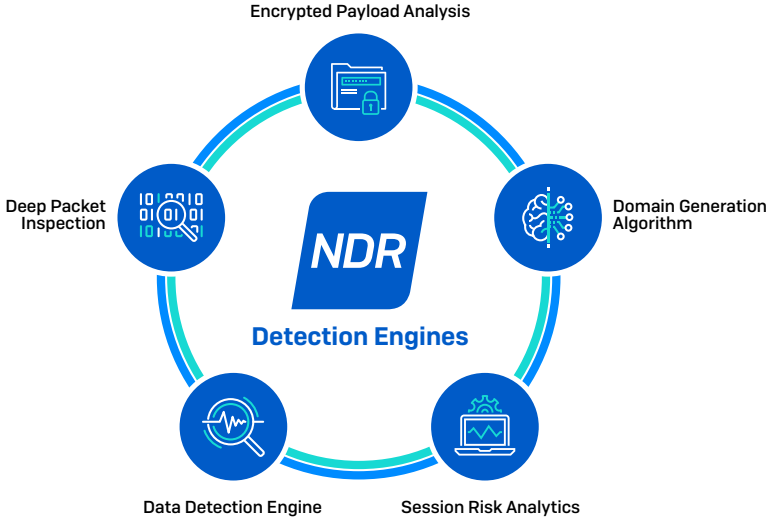


- Monitors traffic deep within a network using five real-time engines.
- Detects activity from all network assests including unmanaged systems, IoT devices, and rogue assets, identifying the manufacturer and OS and any suspicious traffic patterns originating from these devices.
- Feeds data and alerts to the Sophos Central Data Lake and Sophos' MDR SOC team or your XDR team.
- Gain visibility and insights into network and application activity, risky flows, and suspicious traffic with an easy to use Investigation Console.
- If you have Sophos Firewall, automated threat response is available to immediately block a threat and prevent lateral movement.
- Runs as a virtual appliance on popular hypervisor platforms like VMware and Hyper-V.
- Connects directly to your switch via SPAN port mirroring to monitor all traffic.
- Inspects encrypted packet data without compromising PII data.



Sophos NDR Detection Engines

Sophos NDR includes five detection engines that continuously analyze network traffic flows and applying AI machine learning analysis to identify suspicious and malicious activity deep within your network.



Detection Engines	Description
Encrypted Payload Analytics (EPA)	Detects zero-day C2 servers and new variants of malware families based on patterns found in the 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 utilizes rules that alert on a multitude of session-based risk factors.
Device Detection Engine (DDE)	Extensible query engine uses a deep learning prediction model to analyze encrypted traffic for patterns across unrelated network flows and detect port scanning and SSH brute force activity.

Sophos NDR Licensing

Sophos NDR is the perfect complement to Sophos XDR and Sophos MDR as an integration package. Sophos NDR pricing is based on an organization's total number of users and servers. The virtual appliance software is included with the license, and you can deploy as many NDR sensors as needed. This is more affordable and flexible than competing offerings that charge per-instance.

Sophos NDR Technical Specifications

Supported Platforms

- VMware ESXi6.7 and later
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) or later
- Amazon AWS c5n.2xlarge
- Certified Hardware

Hardware	Max Throughput	Max Connections/Sec	CPUs	Memory
Dell R660 (2 socket)	40Gbps	120K	64	128GB
Dell R660 (1 socket)	40Gbps	80K	32	64GB
Dell R650	20Gbps	40K	24	64GB
Dell R450	10Gbps	20K	16	32GB
Dell R350	4Gbps	8K	8	32GB
Intel Nuc 13th Gen	2.5Gbps	4K	12	32GB

VM System Requirements

Sophos NDR VMs support up to 1Gbps per sensor:

- Use Default VM settings for medium traffic volumes:
  - Up to 500Mbps
  - Up to 70,000 packets/sec
  - Up to 1,200 flows/sec
- Resize the VM for 8 vCPUs for high-traffic volumes:
  - Up to 1Gbps
  - Up to 300,000 packets/sec
  - Up to 4,500 flows/sec

Additional Resources:

- Sophos NDR Community Resources
- Enhancing Security Operations with Sophos Network Detection and Response (NDR)
- Certified Hardware Specifications

To learn more, visit

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

24-12-19 DS-EN (MP)

SOPHOS