Sophos Network Detection and Response

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

Speak with an Expert

Get a Quote

Detect Suspicious Behaviors That Extend Beyond Your Firewalls and Endpoints

Sophos NDR works together with your managed endpoints and firewalls activity for suspicious and malicious patterns they cannot see. It detect

flows from unmanaged systems and IoT devices, rogue assets, insider threats, previously unseen zero-day attacks, and unusual patterns deep within the network.

Download Solution Brief

Sophos NDR detects a range of network behaviors, making it an effective solution for identifying:

Unprotected Devices

Identify legitimate devices that aren't protected and could be used as entry points, including IoT and OT assets.

Rogue Assets

Pinpoint unauthorized and potentially malicious devices communicating across a network.

Insider Threats

Gain visibility to network traffic flows and "normal" data movement from inside an organization.

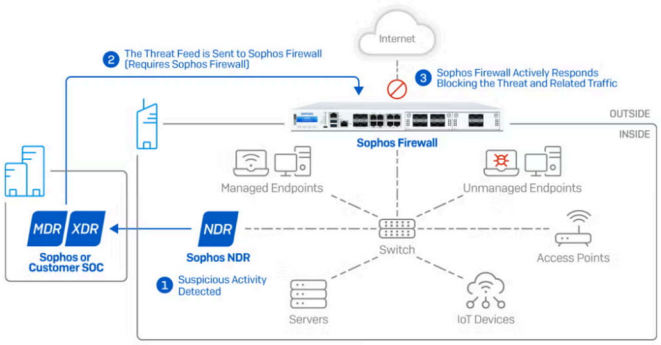
Zero-Day Attacks

Detect server command-and-control (C2) attempts based on patterns found in session packets.

Download Datasheet

Early Detection and Automatic Response

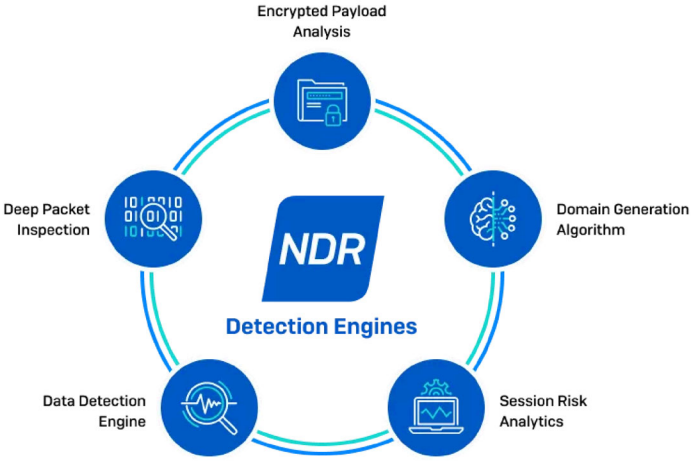
Sophos cross-product automation between NDR, XDR, MDR, and Firewall provides immediate response to stop active threats dead in their tracks.



How it works: Sophos NDR monitors traffic deep within the network, sending suspicious activity to Sophos Central's data lake for further analysis. In the event an active threat or adversary is identified, analysts can immediately push a threat feed to Sophos Firewall that can coordinate an Active Threat Response to isolate and block malicious activity automatically in real-time.

Learn More About Sophos MDR

5 Independent Detection Engines That Work in Real-Time



Data Detection Engine

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.

Domain Generation Algorithm

Identifies dynamic domain generation technology used by malware to avoid detection.

Deep Packet Inspection

Uses known indicators of compromise to identify threat actors and malicious tactics, techniques, and procedures across encrypted and unencrypted network traffic.

Session Risk Analytics

Powerful logic engine utilizes rules that send alerts based on session-based risk factors.

Encrypted Payload Analysis

Detects zero-day C2 servers and new variants of malware families based on patterns found in the session size, direction, and interarrival times.

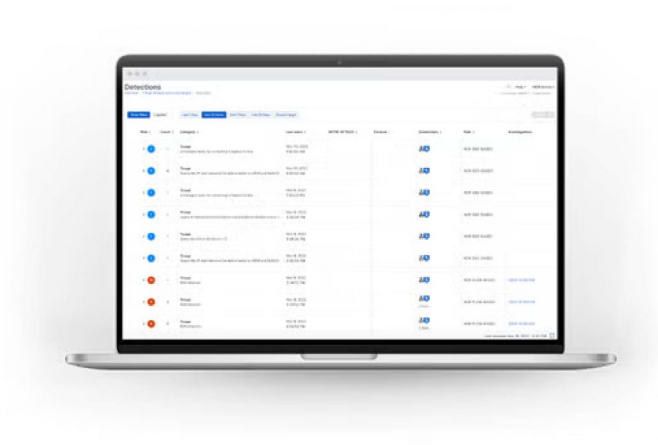
Get valuable insights and perform deep investigations

Sophos Central and the Sophos NDR Investigation Console provides all the tools you need to easily:

Get instant insights into into network and application activity, risky flows, and suspicious traffic detections in Sophos Central

Drill-down and perform deep forensic investigations with the Investigation Console

Identify all unmanaged, IoT, and potential rogue assets on your network inc



DOWNLOADS

Sophos NDR Datasheet

Sophos NDR Solution Brief

VIDEOS

Sophos Network Detection and Response (NDR)

Sophos NDR Demo Video

SOPHOS NEWS

Faster, safer, stronger: Sophos Firewall v22 security enhancements — 5 Nov 2025

Detecting fraudulent North Korean hires: A CISO playbook — 5 Nov 2025

5 ways to strengthen your firewall and endpoint's defenses against ransomware — 5 Nov 2025

Phake phishing: Phundamental or pholly? — 31 Oct 2025

PLATFORM

SERVICES

SOLUTIONS

WHY SOPHOS

PARTNERS

RESOURCES

SECUREWORKS

SUPPORT

GET STARTED

LEGAL

English (US)