SOPHOS

SOPHOS NDR

# See and stop threats across the AI-era network.

## One solution to detect and defend against known and unknown threats.

Sophos NDR combines AI- and ML-powered behavioral analytics, encrypted traffic analysis, network analytics, and threat hunting with deep packet inspection and IDS/IPS capabilities. Flexible deployment options, active inline response, and connected defense through Sophos Fusion help organizations extend visibility across hybrid networks and monitor unmanaged and agentless assets to stop threats faster and strengthen coordinated defense.

**77%**
of IT teams lack full visibility across hybrid environments[1]

**3.4 hours**
median time for attackers to target Active Directory after gaining access[2]

**3 days**
median time before an attacker is detected within an environment[2]

WHAT SOPHOS NDR DELIVERS

## Four outcomes for stronger network defense.

### See more across the network.

Gain network-level visibility into communications involving managed, unmanaged, and agentless assets. Identify suspicious behavior and attack activity that may not be visible to individual controls.

- Behavioral analytics to identify suspicious behavior across the network
- Visibility into unmanaged, IoT, OT, and agentless assets
- Lateral movement and command-and-control detection

### Stop threats faster.

Reduce the time between detection and response. On a Sophos NDR appliance with the IDS/IPS add-on, Active Inline mode can automatically block known malicious packets in the network path.

- Block known malicious packets in real time
- Move from passive monitoring to active inline prevention
- Apply deep packet inspection and IDS/IPS directly in the traffic path

### Deploy your way.

Deploy as a virtual appliance, on dedicated Sophos NDR hardware, or compatible third-party hardware. Match monitoring and enforcement to your architecture, requirements, and risk tolerance.

- Unlimited virtual deployments
- Hardware options to match your environment
- SPAN/TAP and inline deployment modes to match operational requirements

### Simplify operations through Sophos Fusion.

Bring network telemetry, detections, and context into Sophos Fusion alongside endpoint, firewall, identity, email, and cloud insights for investigation and coordinated response.

- Unify network context with insights from across Sophos Fusion
- Enrich Sophos MDR and XDR investigations with NDR telemetry
- Coordinate detection and response across the Sophos Fusion defense system

## SOPHOS NDR AT A GLANCE

- AI- and ML-powered behavioral analytics uncover unknown and evasive threats
- Proven deep packet inspection and IDS/IPS capabilities identify known threats
- Active inline blocking of known malicious traffic
- Virtual, dedicated Sophos hardware, and compatible third-party hardware deployment options

## WHO SOPHOS NDR IS FOR

- Organizations looking to close network visibility gaps
- Security teams seeking visibility into unmanaged and agentless assets
- Organizations requiring flexible NDR deployment across diverse and distributed networks
- MSPs and MSSPs expanding network monitoring, threat hunting, and managed security services

YOUR EDGE AGAINST NETWORK THREATS

# Behavioral detection and active prevention, converged.

### Broader detection coverage

Attackers can exploit visibility gaps across hybrid networks, unmanaged devices, and agentless assets. Sophos NDR combines behavioral analytics, encrypted traffic analysis, threat hunting, deep packet inspection, and IDS/IPS to detect known and unknown threats.

### Directly block threats in the network path

Detection alone can leave security teams responding after malicious traffic has already reached its destination. On a Sophos NDR appliance with the IDS/IPS add-on, Active Inline mode inspects traffic in real time and automatically blocks known malicious packets in the network path.

### Connected defense through Sophos Fusion

Network threats rarely exist in isolation. Sophos NDR contributes network telemetry, detections, and context to Sophos Fusion, helping teams accelerate investigations and coordinate response across the defense system.

WHAT CUSTOMERS ARE SAYING

"Overall, my experience with Sophos NDR has been quite good. It greatly helps in gaining visibility into abnormal network behavior and detecting patterns that would normally go unnoticed in traditional monitoring. Something I really appreciate is that the alerts are clear and easy to interpret, which speeds up analysis and decision-making."[3]

IT Security & Risk Management, Banking Industry — Gartner® Peer Insights™

SOPHOS FUSION

## One system. Every control point. Defending as one.

Sophos NDR is part of Sophos Fusion, the world's most complete cyber defense system. It protects organizations from AI-enabled threats that move faster than defenders can respond.

**sophos.com/NDR →**

[1] SolarWinds, 2026 State of Monitoring & Observability Report
[2] Sophos, Active Adversary Report 2026
[3] https://www.gartner.com/reviews/market/network-detection-and-response/vendor/sophos/product/sophos-ndr/review/view/6513218

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved.

© Copyright 2026. Sophos Ltd. All rights reserved. Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK. Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-10-23 SB (TA)

SOPHOS