SOPHOS

SOPHOS NDR

Behavioral detection and active prevention, converged

See and stop threats across the AI-era network.

Modern environments span distributed users, cloud services, applications, unmanaged devices, and IoT and OT systems. At the same time, attackers are using AI to accelerate exploitation, often leveraging legitimate credentials and trusted access to move laterally across the network. Sophos Network Detection and Response (NDR) gives security teams the extensive network-level visibility, detection, and response needed to uncover suspicious activity, lateral movement, and threats that may otherwise go unnoticed.

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

3.4 hours
Median time for attackers to go after Active Directory after gaining access[2]

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

Sophos NDR combines AI- and ML-powered behavioral analytics, encrypted traffic analysis, network analytics, and threat hunting with proven deep packet inspection and Intrusion Detection and Prevention System (IDS/IPS) capabilities. The result is broader coverage across known and unknown threats, direct packet blocking in Active Inline mode, flexible deployment, and centralized management through Sophos Fusion.

OUTCOMES THAT MATTER

See more
Gain greater visibility into activity within your network from managed, unmanaged, and agentless assets. Identify suspicious behavior, lateral movement, command-and-control traffic, and other indicators that may not be visible to individual controls.

Stop threats faster
Reduce the time between detection and response. Active Inline mode can automatically block identified malicious packets directly in the path of your network before they reach their destination.

Deploy your way
Choose virtual, compatible third-party hardware, or dedicated Sophos NDR hardware to match your network's needs. Depending on deployment choice, select from Active Inline, Passive Inline, or SPAN/TAP inspection modes to fit your architecture and risk tolerance.

Simplify operations
Converge behavioral analytics and proven IDS/IPS capabilities in one Sophos solution, with centralized management, threat hunting, shared context, and coordinated workflows through Sophos Fusion.

THE CHALLENGE

Threats are getting faster and networks are expanding



Faster attacks



Expanding attack surface



Network visibility gaps



Unmanaged and agentless assets



Evasive threats



Fragmented tools

Preventive security controls remain essential, but no single control sees every part of an attack.

- **Networks are more distributed.** Cloud infrastructure, SaaS applications, remote users, connected devices, and AI-enabled workloads exacerbate visibility gaps.
- **Attackers move faster.** AI accelerates reconnaissance and exploitation, while valid credentials and trusted tools help adversaries blend into normal activity.
- **Response expectations are rising.** Security teams need more than alerts; they need context, direct response options, and coordinated workflows.
- **Complexity slows adoption.** Fragmented tools, disconnected investigations, and limited resources increase operational overhead.

THE SOLUTION

Sophos NDR

Network traffic provides a powerful vantage point across communications involving managed, unmanaged, and agentless assets, revealing how users, systems, applications, and workloads interact. Sophos NDR uses this network-level visibility to identify suspicious behavior, lateral movement, command-and-control activity, and other indicators of potential threats.

Detection and prevention in one solution

AI- and ML-powered behavioral detection

Behavioral analytics, machine learning, encrypted traffic analysis, network analytics, and threat intelligence help identify suspicious activity and unknown threats that signatures alone may miss.

Proven IDS/IPS inspection

Deep packet inspection and signature-based detection identify known attack techniques, indicators of compromise, and malicious traffic patterns.

Response built in

When deployed in Active Inline mode, Sophos NDR sits directly in your network's traffic path, inspects traffic in real time, and can automatically block identified malicious packets. With a Sophos NDR appliance and the IDS/IPS Add-on, organizations can begin with monitoring only modes and move to Active Inline mode as requirements evolve.

Investigation and threat hunting

Investigate suspicious network activity with context from Sophos Fusion, then drill deeper with the Sophos NDR Investigation Console. Rich graphical tools help security teams analyze network and application activity, detections, and suspicious patterns to support forensic investigation and threat hunting.

Flexible by design

Choose your deployment option

- **Virtual appliance:** Deploy across virtualized, cloud, and distributed environments.
- **Dedicated Sophos NDR appliance:** Deploy purpose-built Sophos hardware designed for Sophos NDR workloads.
- **Compatible third-party hardware:** Use compatible hardware that fits existing infrastructure and requirements.

Choose the deployment mode

Choose from different deployment modes (mode availability depends on your deployment option and add-ons):

- **Active Inline:** Inspect traffic in the network path and actively block identified malicious traffic.*
- **Passive Inline:** Inspect traffic inline without actively blocking it.*
- **SPAN/TAP:** Monitor mirrored traffic without requiring inline deployment.

*Requires Sophos NDR appliance with IDS/IPS Add-on

Simple licensing

The required software license is based on your total protected user and server count, and supports unlimited virtual deployments. You can then optionally add a dedicated Sophos NDR appliance or compatible third-party hardware. For Sophos NDR appliances, the optional per-appliance IDS/IPS Add-on adds IDS/IPS capabilities, including Active Inline mode.

Stronger together through Sophos Fusion

Sophos NDR is available as a standalone solution, but its value grows as part of Sophos Fusion, the AI-Native Cybersecurity Defense System that connects security controls through centralized management, shared context, and coordinated response.

Sophos Firewall

PREVENT AND CONTROL

Prevents and controls traffic at key enforcement points, including policy, access control, segmentation, and perimeter protection.

Sophos NDR

DETECT AND BLOCK

Detects known and unknown threats across network activity and can block known malicious packets with Active Inline mode.

Sophos MDR and XDR

INVESTIGATE AND RESPOND

Correlate NDR telemetry with endpoint, firewall, identity, email, cloud, and other signals to accelerate investigation and response.

Sophos Fusion

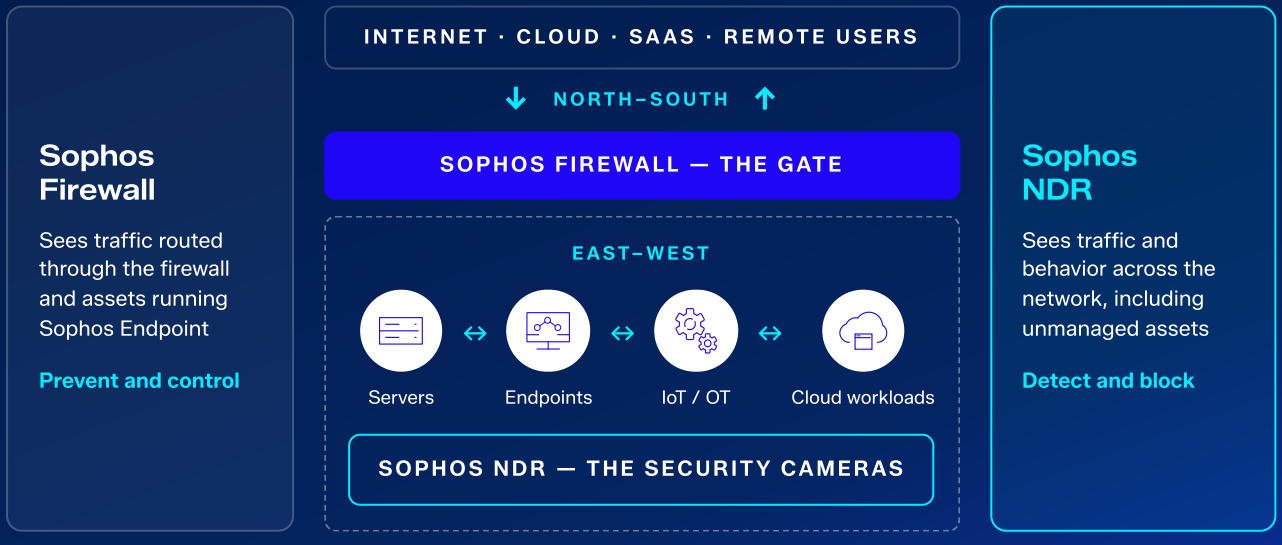
CONNECT AND COORDINATE

Connects and coordinates these capabilities through one operational experience and shared security context.

Sophos Firewall and NDR provide two complementary perspectives. Sophos Firewall inspects and controls traffic routed through it and endpoints running Sophos Endpoint. Sophos NDR extends visibility across network traffic and behavior, including activity involving unmanaged or agentless assets and traffic not routed through Sophos Firewall.

FIREWALL + NDR: WHY BOTH

Two complementary perspectives, one coordinated defense.



No single control sees every part of an attack. Through Sophos Fusion, both respond as one.

WHY SOPHOS NDR

Why choose Sophos NDR



Broader threat coverage

Behavioral analytics and proven IDS/IPS inspection address known and unknown threats in one solution.



Direct response

Active Inline mode can stop identified malicious traffic in the network path rather than only report it after the fact.



Deployment freedom

Multiple deployment options and modes support diverse network architectures and operational requirements.



Coordinated defense

Sophos Fusion brings together management, network context, investigation, and coordinated response.

WHAT CUSTOMERS ARE SAYING

> “It [Sophos NDR] 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. Source: Gartner® Peer Insights™

Licensing options

All Sophos NDR deployments start with the purchase of Sophos NDR software that is priced by total user and server count.

Software license (required)	
Software license*	Unlimited virtual deployments, behavioral detection capabilities, IDS capabilities**

*Sophos NDR is available for Term customers only; MSP Flex availability is to be confirmed.
**IDS capabilities available on supported platforms; see page 9

Deploy Sophos NDR using virtual appliances, Sophos NDR hardware, or on your own compatible third-party hardware.

Hardware (optional)	
Sophos NDR appliance*	Purpose-built Sophos appliance
Compatible third-party appliance	Bring your own compatible third-party hardware to match existing infrastructure

*Sophos NDR hardware is not currently sold in India.

One of two bypass module options must be selected for each Sophos NDR appliance.

Flexi Port bypass modules (required selection for each Sophos NDR 5500)	
Bypass modules	Choose from one of two options: 2 × 4-port 1 GE copper (8 ports total) OR 2 × 2-port 10 GE fiber (4 ports total)

An optional add-on can be added to your Sophos NDR hardware.

Add-ons (optional for each Sophos NDR appliance)	
IDS/IPS Add-on	Per-appliance add-on that adds IDS/IPS capabilities, including active inline blocking, to a Sophos NDR appliance

Two tiers of premium Support are available as optional add-ons.

Premium Support (optional for each Sophos NDR appliance)	
Enhanced Support	24/7 multi-channel support, software updates and maintenance, advanced hardware replacement for appliances, and remote assistance
Enhanced Plus Support	All Enhanced Support benefits, plus remote consulting (2-8 hours depending on device), VIP access to senior technical resources, priority case and sample handling, and proactive device health alert support with device health event cases

Deployment options



Sophos NDR appliance

Purpose-built Sophos hardware.



Virtual appliance

Deploy Sophos NDR on VMware ESXi, Microsoft Hyper-V, AWS, or Nutanix.



Compatible third-party hardware

Deploy Sophos NDR on your own compatible hardware to match existing infrastructure.

Sophos NDR hardware lineup

The Sophos NDR appliance offers a purpose-built hardware option for Sophos NDR workloads.

Product matrix

Model		Tech specs		Performance		
Model	**Form factor**	**Bypass ports**	**Components**	**Inspection throughput (Gbps)**	**Connections (per second)**	**Packet latency (µs)**
NDR 5500 Fiber*	1U Long	4	Built in: redundant power, SSDs, fans	TBC	TBC	TBC
NDR 5500 Copper*	1U Long	8	Built in: redundant power, SSDs, fans	TBC	TBC	TBC

*Not currently sold in India. Availability in Brazil is pending certification in Jan-2027.

Performance test methodology TBC



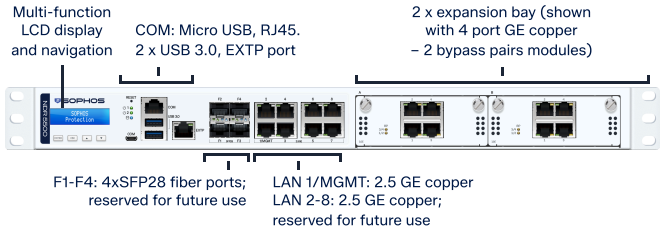
Need sizing help?

Sophos offers free sizing assistance and an NDR sizing tool for partners via the Partner Portal.

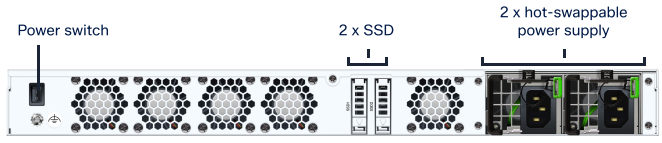
Sophos NDR 5500

Technical specifications

Front view



Back view



Physical specifications	
Mounting	1 U rackmount (slide rail kit / ear mounts included)
Dimensions: Width x depth x height	438 × 510 × 44 mm
Storage	2 × 2 TB removable NVMe M.2 SSDs 1 32 GB eMMC
Weight	15.1 kg / 33.29 lb (packaged) 9.4 kg / 20.72 lb (unpackaged)

Environment	
Power supply	2 x hot-swappable power supplies
Power consumption	135 W / 460.64 BTU/hr idle (typical) 270.20 W / 921.96 BTU/hr loaded (typical)
Operating temperature	0°C to 40°C operating –20°C to 70°C storage
Humidity	10% to 90% RH, non-condensing (operating and storage)

Performance	
NDR 5500 Fiber*	
Inspection throughput (Gbps)	TBC
Connections (per second)	TBC
Packet latency (µs)	TBC
NDR 5500 Copper*	
Inspection throughput (Gbps)	TBC
Connections (per second)	TBC
Packet latency (µs)	TBC

*Not currently sold in India. Availability in Brazil is pending certification in Jan-2027.

Physical interfaces	
Management ports	1 × RJ45 MGMT 1 × COM RJ45 1 × COM Micro-USB
Flexi Port bays (for bypass modules)	2
Bypass module options*	2 × 4-port 1 GE copper (8 ports total) 2 × 2-port 10 GE fiber (4 ports total)
USB ports	2 × USB 3.0
Display	Multi-function LCD module

*Must be selected with appliance

Product certifications	
Certifications	CE, FCC, ISED, RCM, VCCI, BSMI, CB, UL, KC
Certifications (post launch) Expected early 2027	Anatel

Virtual deployment

Sophos NDR can be deployed as a virtual appliance on VMware, Hyper-V, AWS, or Nutanix infrastructure. Please see the table below for virtual deployment requirements.

Virtual deployment requirements				
Deployment platform	**Minimum / standard configuration**	**Sizing guidance**	**Behavioral analytics support**	**IDS support**
VMware ESXi	4 vCPUs; 16 GB RAM; 160 GB storage	Medium traffic: Up to 500 Mbps, 70K packets/sec, and 1,200 flows/sec using the default VM configuration. High traffic: Up to 1 Gbps, 300K packets/sec, and 4,500 flows/sec with 8 vCPUs.	✓	✓
Microsoft Hyper-V	4 vCPUs; 16 GB RAM; 160 GB storage	Medium traffic: Up to 500 Mbps, 70K packets/sec, and 1,200 flows/sec using the default VM configuration. High traffic: Up to 1 Gbps, 300K packets/sec, and 4,500 flows/sec with 8 vCPUs.	✓	✓
AWS	Supported EC2 instance types: c5n.2xlarge, c6i.4xlarge, and c7i.16xlarge*	Select a supported EC2 instance based on deployment requirements.	✓	–
Nutanix	4 vCPUs; 16 GB RAM; 160 GB storage	8 CPU cores required when using both SPAN interfaces.	✓	–

* The c7i.16xlarge instance uses Nitro virtualization.
CPU requirements: Sophos NDR requires pdpe1gb and avx2 CPU flags.

Compatible third-party hardware

Want to bring your own third-party hardware? Sophos NDR can be deployed on compatible third-party hardware based on the below requirements.

Third-party hardware requirements				
Minimum recommendation	**CPU**	**Memory**	**Storage**	**Network interfaces**
Up to 1 Gbps or 4K connections/sec	Intel Core i5, at least 4 cores / 8 threads	16 GB	1 TB high-performance NVMe or SAS	Intel i350 1 GbE network card, dual or quad port
Up to 4 Gbps or 8K connections/sec	Intel Xeon, at least 8 cores / 16 threads	32 GB	2 TB high-performance NVMe or SAS	2 onboard NICs for management and syslog + supported NIC capable of ingesting 4 Gbps
Up to 10 Gbps or 20K connections/sec	Intel Xeon, at least 16 cores / 32 threads	64 GB	3 TB high-performance NVMe or SAS	2 onboard NICs for management and syslog + supported NIC capable of ingesting 10 Gbps
Up to 20 Gbps or 40K connections/sec	Intel Xeon, at least 24 cores / 48 threads	64 GB	4 TB high-performance NVMe or SAS	2 onboard NICs for management and syslog + supported NIC capable of ingesting 20 Gbps
Up to 40 Gbps or 80K connections/sec	Intel Xeon, at least 32 cores / 64 threads	64 GB	6 TB high-performance NVMe or SAS	2 onboard NICs for management and syslog + supported NIC capable of ingesting 40 Gbps
Up to 40 Gbps or 100K connections/sec	2 × Intel Xeon, at least 32 cores / 64 threads	128 GB	6 TB high-performance NVMe or SAS	2 onboard NICs for management and syslog + supported NIC capable of ingesting 40 Gbps

General hardware requirements	
Component	**Requirement**
CPU	At least 2.5 GHz; must support pdpe1gb and avx2 CPU flags
Memory	DDR4-2400 or better
Storage	High-performance NVMe recommended; high-performance SAS supported. Single- or dual-drive configurations supported; RAID encouraged when redundancy is required
Network interfaces	At least 2 network interfaces: one for management/syslog and one for packet capture
Packet capture NIC	Must use a supported DPDK-compatible network adapter
System	UEFI BIOS boot mode and GPT partitions required

SPEAK WITH AN EXPERT

Sophos NDR: One solution to detect and defend against known and unknown threats.

Learn more or request a quote today.

sophos.com/NDR →

[1] SolarWinds 2026 State of Monitoring & Observability Report.
[2] Sophos Active Adversary Report 2026.
[3] Gartner® Peer Insights™ review.

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 is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, PEER INSIGHTS is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. 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.

2026-11-19 BR (TA)

SOPHOS