

TrendAI Vision One™ Network Detection and Response (NDR)

Network-wide detection of targeted attacks, advanced threats, and ransomware

Strengthen network security through non-disruptive monitoring of out-of-band traffic

Delivered as a physical or virtual sensor, TrendAI Vision One™ Network Detection and Response (NDR) brings network visibility into TrendAI Vision One™, where network telemetry is correlated with endpoint, email, cloud, and identity signals for full-lifecycle detection and response. NDR delivers deep visibility into network activity to detect hidden threats and analyze suspicious behavior in real time, including advanced encrypted traffic analysis without requiring full decryption, enhancing security while maintaining privacy. This non-intrusive approach allows you to identify and respond to attacks throughout the entire attack lifecycle, from infiltration to data exfiltration.

Monitor 360 degrees of your network

Available in a physical or virtual network appliance, NDR gives you complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. By utilizing specialized detection engines and custom sandbox analysis, you have the ability to identify advanced and unknown malware, ransomware, zero-day exploits, command and control (C&C) communications, and evasive attacker activities that are invisible to standard security defenses. Enhance detection by monitoring all physical, virtual, north-south, and east-west traffic.

Key capabilities

Inspect across all network content. Monitor all traffic across physical and virtual network segments, all network ports, and over 100 network protocols, and identify targeted attacks, advanced threats, and ransomware. Our agnostic approach to network traffic allows you to detect targeted attacks, advanced threats, and ransomware from both inbound and outbound traffic. This includes monitoring for lateral movement, C&C activities, and other attacker behaviors throughout all phases of the attack lifecycle.

Gain extensive detection techniques. Utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.

Customize your sandbox analysis. Use virtual images tuned to precisely match your organization's system configurations, drivers, installed applications, and language versions. This approach allows you to improve the detection rate of advanced threats and ransomware designed to evade standard virtual images.

Manage detection and response. Let TrendAI™ security experts and industry-leading AI help monitor and prioritize threats detected by NDR.

Turn unknown threats into known threats. Leverage standards-based advanced threat intelligence sharing to keep ahead of threats (STIX/TAXII and YARA). Automate the sharing of threat information across TrendAI™ solutions and third-party security products, which simultaneously strengthens multiple links in the security chain.

Leverage complete visibility with encrypted traffic analysis. Achieve comprehensive visibility into encrypted traffic using AI-driven anomaly detection, TLS fingerprinting, and threat intelligence correlation without full decryption. This capability strengthens defense against advanced threats while preserving privacy and compliance.

A key part of TrendAI Vision One™

TrendAI Vision One™ is the only industry-leading AI security platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This comprehensive approach helps you predict and prevent threats, accelerating proactive security outcomes across your entire digital estate.

NDR serves as a critical sensor for TrendAI Vision One™, extending visibility and telemetry into unmanaged systems, such as contractor and third-party systems, IoT and industrial internet of things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

Key benefits

Better detection and investigation

- Reduce breach risk with multiple detection techniques across all traffic
- Eliminate blind spots by monitoring every network segment
- Accelerate threat validation through custom sandbox analysis
- Strengthen defenses by integrating global threat intelligence
- Improve detection accuracy with machine learning-driven insights
- Expose hidden threats in encrypted traffic using encrypted traffic analysis without compromising privacy

Operational efficiency

- Maximize ROI by extending existing security investments
- Adapt quickly with flexible deployment options for diverse environments
- Free up analyst time by automating repetitive tasks
- Speed investigations with intuitive graphical attack analysis

Detect and protect

- Prevent breaches from targeted attacks and advanced threats
- Stop ransomware before it disrupts operations
- Block zero-day malware and document exploits to protect productivity
- Identify attacker behavior early to reduce dwell time and impact
- Protect users from web exploits and drive-by downloads
- Prevent phishing and email-based compromise to secure sensitive data

Proven leadership



TrendAI Vision One™ ranked #1
out of 59 Enterprise Solutions



Recognized in 2024

Voice of the Customer

for Network Detection and Response, Midsize Enterprise (\$50M–\$1B)



Named a Leader in The

Forrester Wave™: Network Analysis and Visibility, Q4 2025

	NDR hardware specifications				
	Series 500	Series 1000	Series 4000	Series 9000	Series 40G
Throughput	500 Mbps	1 Gbps	4 Gbps	10 Gbps	40 Gbps
Sandboxes supported	2	4	20	30	40
Form factor	1U rackmount, 48.26 cm (19")	1U rackmount, 48.26 cm (19")	2U rackmount, 48.26 cm (19")	2U rackmount, 48.26 cm (19")	2U rackmount, 48.26 cm (19")
Weight	18.62 kg (41.05 lbs)	18.62 kg (41.05 lbs)	25.84 kg (54.96 lbs)	25.84 kg (54.96 lbs)	36.1 kg (79.58 lbs)
Dimensions (WxDxH)	48.2 cm (18.98") x 74.9 cm (29.48") x 4.28 cm (1.68")	48.2 cm (18.98") x 74.9 cm (29.48") x 4.28 cm (1.68")	48.2 cm (18.98") x 70.78 cm (27.85") x 8.68 cm (3.42")	48.2 cm (18.98") x 70.78 cm (27.85") x 8.68 cm (3.42")	48.2 cm (18.98") x 77.21 cm (30.39") x 8.68 cm (3.42")
Management ports	10/100/1,000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1,000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1,000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1,000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1,000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1
Data ports	10/100/1,000 base-T RJ45 port x 5	10/100/1,000 base-T RJ45 port x 5	10/25 GbE SFP28 x 4 10/100/1,000 base-T RJ45 port x 5	10/25 GbE SFP28 x 4 10/100/1,000 base-T RJ45 port x 5	100 GbE QSFP28 x 2 10/25 GbE SFP28 x 4 10/100/1,000 base-T RJ45 port x 1
AC input voltage	100 – 240 VAC	100 – 240 VAC	100 – 240 VAC	100 – 240 VAC	100 – 240 VAC
AC input current	9.2A – 4.7A	9.2A – 4.7A	9.2A – 4.7A	12A – 6.3A	12A – 8A
Memory	32 GB	32 GB	128 GB	192 GB	512 GB
Hard drives	2 x 2 TB 3.5" SATA	2 x 2 TB 3.5" SATA	4 x 2 TB 3.5" SATA	4 x 2 TB 3.5" SATA	4 x 2.4 TB 3.5" SATA
RAID configuration	RAID 1	RAID 1	RAID 10	RAID 10	RAID 10
Power supply	800 W redundant	800 W redundant	800 W redundant	1,100 W redundant	1,400 W redundant
Power consumption (max.)	899 W (max.)	899 W (max.)	899 W (max.)	1,202 W (max.)	1,573 W (max.)
Heat	3,000 BTU/hr. (max.)	3,000 BTU/hr. (max.)	3,000 BTU/hr. (max.)	4,125 BTU/hr. (max.)	5,250 BTU/hr. (max.)
Frequency	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
Operating temp.	10 – 35 °C (50 – 95 °F)	10 – 35 °C (50 – 95 °F)	10 – 35 °C (50 – 95 °F)	10 – 35 °C (50 – 95 °F)	10 – 35 °C (50 – 95 °F)

**Start free trial of
TrendAI Vision One™**

Learn more at trendaisecurity.com

Copyright ©2026 Trend Micro Incorporated. All rights reserved. TrendAI and TrendAI Vision One are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS20_Network_Detection_Response_Datasheet_260901US] trendaisecurity.com

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy