Datasheet

Trend Micro™ Deep Discovery™ Inspector

Enable network-wide detection of targeted attacks, advanced threats, and ransomware

As part of our Trend Vision One™ platform, Trend Micro™ – Deep Discovery™ enhances your out-of-band network security by enabling you to passively monitor traffic without disrupting operations. Integrated with our powerful network detection and response (NDR) capabilities, it empowers your security teams with deeper visibility into network activity, enabling you to better detect hidden threats and analyze suspicious behavior in real time. This non-intrusive approach allows you to identify and respond to attacks throughout the entire attack lifecycle, from infiltration to data exfiltration.

Our Trend Micro™ Deep Discovery™ Inspector solution comprises a physical or virtual network appliance that allows you to monitor 360 degrees of your network. This provides you with complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. Using specialized detection engines and custom sandbox analysis, Deep Discovery Inspector lets you 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 all network content. Monitor all traffic across physical and virtual network segments, all network ports, and over 100 network protocols. 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.

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.

Custom 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.

Managed detection and response. Let Trend Micro security experts and industry-leading AI help monitor and prioritize threats detected by Deep Discovery Inspector.

Turn unknown threats into known threats. Leverage standards-based advanced threat intelligence sharing to stay ahead of the latest structured threat information expression (STIX), trusted automated exchange of indicator information (TAXII), and yet another-recursive-acronym (YARA) insights. Automate threat information sharing across Trend and third-party security solutions while simultaneously strengthening multiple links in the security chain.

Key benefits

- Utilize multiple detection techniques
- Monitor all network traffic
- Gain custom sandbox analysis
- Allow for standards-based threat intelligence sharing
- Leverage increased detection with machine learning
- Enhance existing investments
- Choose from flexible deployment options
- Automate manual tasks
- Obtain a graphical analysis of attacks

Proven leadership

Recognized in 2024 Gartner® Peer Insights™ Voice of the Customer for Network Detection and Response, Midsize Enterprise ($50M - $1B)

Recognized as a Representative Vendor in the 2024 Gartner® Market Guide for Network Detection and Response (NDR)

Named a Leader in the Forrester Wave™, Network Analysis and Visibility (NAV), Q2 2023

A key part of Trend Vision One

Trend Vision One enables you to break down your organizational silos that exist between email, endpoints, servers, cloud workloads, and networks. Broader visibility and expert security analytics lead to fewer alerts and higher-confidence detection for an earlier, faster response.

Deep Discovery Inspector and Trend Vision One™ – XDR for Networks are valuable solutions, unified within our AI-powered Trend Vision One platform. They provide critical logs and visibility into unmanaged systems, such as contractor/third-party systems, IoT and industrial internet of things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

Detect and protect against:

- Targeted and known attacks (including ransomware) and advanced threats
- Zero-day malware and document exploits
- Attacker behavior and other network activity
- Web threats, including exploits and drive-by downloads
- Phishing, spear phishing, and other email threats
- Data exfiltration
- Bots, Trojans, worms, and keyloggers
- Disruptive applications

Deep Discovery Inspector 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 rack-mount, 48.26 cm (19")	1U rack-mount, 48.26 cm (19")	2U rack-mount, 48.26 cm (19")	2U rack-mount, 48.26 cm (19")	2U rack-mount, 48.2 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	100GbE QSFP28 x 2 10/25GbE SFP28 x 4 10/100/1,000 base-T RJ45 port x 2
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	12 A - 6.3 A	12 A - 8 A
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	4x 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)

Deep Discovery Inspector virtual appliances are available at 100/250/500/1,000 Mbps capacities and are deployable on VMware vSphere 5 and above, as well as KVM. Cloud sandboxing can be added to the virtual Deep Discovery Inspector through the Trend Micro™ Sandbox as a Service add-on.

For more information, please visit TrendMicro.com

TrendMicro.com