Datasheet

Trend Micro™ Deep Discovery™ Inspector

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

Targeted attacks and advanced threats are customized to evade your conventional security defenses, and remain hidden while stealing your corporate data, intellectual property, and communications, or encrypting critical data until ransom demands are met. To detect targeted attacks and advanced threats, analysts and security experts agree that organizations should utilize advanced detection technology as part of an expanded strategy.

Trend Micro™ Deep Discovery™ Inspector is a physical or virtual network appliance that monitors 360 degrees of your network to create complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. By using specialized detection engines and custom sandbox analysis, Deep Discovery Inspector identifies 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. Detection is enhanced by monitoring all physical, virtual, north-south, and east-west traffic.

Key Capabilities

Inspects all network content. Deep Discovery Inspector monitors all traffic across physical and virtual network segments, all network ports, and over 100 network protocols to identify targeted attacks, advanced threats, and ransomware. Our agnostic approach to network traffic enables Deep Discovery Inspector to detect targeted attacks, advanced threats, and ransomware from inbound and outbound network traffic as well as lateral movement, C&C, and other attacker behavior across 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 uses virtual images that are tuned to precisely match an organization's system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats and ransomware that are designed to evade standard virtual images.

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

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

Network Analytics. Security professionals are flooded with threat data from numerous sources. Network analytics help prioritize threats and provide visibility into an attack. By looking back at months of historical data, you will be able to see what the first point of entry was, who else in the organization is impacted, and with whom the threat is communicating (for example, C&C).

Key Benefits

Better Detection

- Multiple detection techniques
- Monitors all network traffic
- Custom sandbox analysis
- Standards-based threat intelligence sharing
- Increased detection with machine learning

Tangible ROI

- Enhance existing investments
- Flexible deployment options
- Automation of manual tasks
- Graphical analysis of attacks

FORRESTER®
WAVE LEADER 2023
Network Analysis And Visibility

A Key Part of Trend Vision One™

The XDR capabilities in Trend Vision One break down the silos between email, endpoints, servers, cloud workloads, and networks. It offers broader visibility and expert security analytics, leading to fewer alerts and more higher-confidence detections for an earlier, faster response. With XDR, you can identify and respond more effectively and efficiently to threats, minimizing the severity and scope of an attack on the organization. Deep Discovery Inspector and Trend Vision One™ – XDR for Network are valuable parts of the XDR solution, providing critical logs and visibility into unmanaged systems, such as contractor/third-party systems, internet of things (IoT) and industrial internet of things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

Detect and Protect Against

- Targeted attacks and advanced threats
- Targeted and known ransomware attacks
- 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, keyloggers
- Disruptive applications

DEEP DISCOVERY INSPECTOR HARDWARE SPECIFICATIONS			
	Series 500/1000	Series 4000	Series 9000
Throughput	500 Mbps / 1 Gbps	4 Gbps	10 Gbps
Sandboxes Supported	2 / 4	20	30
Form Factor	1U rack-mount, 48.26 cm (19")	2U rack-mount, 48.26 cm (19")	2U rack-Mount, 48.26 cm (19")
Weight	18.62kg (41.05 lbs)	28.6 kg (63.05 lbs)	28.6 kg (63.05 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 71.55 cm (28.17") x 8.68 cm (3.42")	48.2 cm (18.98") x 71.55 cm (28.17") x 8.68 cm (3.42")
Management Ports	10/100/1000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1	10/100/1000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1
Data Ports	10/100/1000 base-T RJ45 port x 5	10 Gb SFP+ SR transceiver x 4 10/100/1000 base-T RJ45 port x 5	10 Gb SFP+ SR transceiver x 4 10/100/1000 Base-T RJ45 port x 5
AC Input Voltage	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
AC Input Current	9.2A to 4.7A	10A to 5A	12A to 6.5A
Hard Drives	2 x 2 TB 3.5" SATA	4 x 1 TB 3.5" SATA	4 x 1 TB 3.5" SATA
RAID Configuration	RAID 1	RAID 10	RAID 10
Power Supply	800W redundant	750W redundant	1,100W redundant
Power Consumption (Max.)	899W (max.)	847W (max.)	1,202W (max.)
Heat	3,000 BTU/hr. (max.)	2,891 BTU/hr. (max.)	4,100 BTU/hr. (max.)
Frequency	50/60 Hz	50/60HZ	50/60HZ
Operating Temp.	10 to 35 °C (50-95 °F)	10 to 35 °C (50-95 °F)	10-35 °C (50-95 °F)
Hardware Warranty	3 years	3 years	3 years

Deep Discovery Inspector virtual appliances are available at 100/250/500/1000 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™ Deep Discovery™ Analyzer as a Service add-on.

Other network security products

Trend network security solutions provide a layered security solution to protect you from known, unknown, and undisclosed threats.

- **Deep Discovery Analyzer** provides advanced sandbox analysis to extend the value of security products such as endpoint protection, web and email gateways, network security, and other Trend Micro™ Deep Discovery™ solutions. Deep Discovery Analyzer can detect ransomware, advanced malware, zero-day exploits, command and control, and multi-stage downloads resulting from malicious payloads or URLs on Microsoft Windows and Mac operating systems.
- **Trend Micro™ TippingPoint™** provides high-speed, inline intrusion prevention system (IPS) inspection, offering comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy and low latency.
- **Trend Micro™ Deep Discovery™ Director.** In addition to providing central management, data deduplication, log aggregation, and more for the Deep Discovery family, it provides advanced threat sharing via an indicators of compromise (IoC) exchange. It uses standards-based formats and transfers like YARA, STIX, and TAXII to share advanced threat intelligence across your security ecosystem.

For more information, please visit
trendmicro.com