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 encrypt 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. This capability has earned Trend Micro a "Recommended" rating for Breach Detection Systems by NSS Labs five years in a row.

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

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 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 life cycle.

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's security experts and industry leading artificial intelligence help monitor and prioritize threats detected by Deep Discover 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 automates the sharing of threat information across Trend Micro and third-party security solutions, which strengthens multiple links in the security chain at the same time.

Network Analytics. Security professionals are flooded with threat data coming 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 was the first point of entry, who else in the organization is impacted, and with whom the threat is communicating (for example, C&C)

TREND MICRO
DEEP DISCOVERY
BREACH DETECTION
SYSTEMS 2018

NSS LABS RECOMMENDED

RECOMMENDED 5 YEARS IN A ROW

ICSA labs CERTIFIED

A KEY PART OF TREND MICRO'S CONNECTED THREAT DEFENSE

To adequately protect against the current threat landscape, you'll need a multi-layered protection platform that delivers the full life cycle of threat defense. Trend Micro Connected Threat Defense is a layered approach to security that gives your organization a better way to quickly prevent, detect, and respond to new threats that are targeting you, while improving visibility and control across your network.

- **Prevent:** Assess potential vulnerabilities and proactively protect endpoints, servers, and applications.
- **Detect:** Identify advanced malware, behavior, and communications invisible to standard defenses.
- **Respond:** Enable rapid response through shared threat intelligence and delivery of real-time security updates.
- **Visibility and control:** Gain centralized visibility across the network and systems—analyze and assess the impact of threats.

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, 19" (48.26 cm)
Weight	17.5kg (38.58 lbs)	28.6 kg (63.05 lbs)	28.6 kg (63.05 lbs)
Dimensions (WxDxH)	43.4 cm (17.08") x 72.8 cm (28.68") x 4.28 cm (1.69")	43.4 cm (17.08") x 75.13 cm (29.58") x 8.68 cm (3.42")	43.4 cm (17.08") x 75.13 cm (29.58") 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	7.4A to 3.4A	10A to 5A	12A to 6.5A
Hard Drives	2 x 1 TB 3.5" SATA	4 x 1 TB 3.5" SATA	4 x 1 TB 3.5" SATA
RAID Configutation	RAID 1	RAID 10	Raid 10
Power Supply	550W redundant	750W redundant	1,100W redundant
Power Consumption (Max.)	750W (max.)	847W (max.)	1,202W (max.)
Heat	2,559 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 Micro 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 Deep Discovery products. 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™ Threat Protection System** 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 also 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.
- **Trend Micro™ Deep Discovery™ Network Analytics** can correlate threat data for up to 180 days to provide visibility into undetected threats, help prioritize your response, and provide actionable threat intelligence to mitigate the threat quickly.

Deep Discovery Inspector is part of the Trend Micro Network Defense solution, powered by XGen™ security.

POWERED BY XGen™ SECURITY

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

TREND MICRO™

Securing Your Connected World

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy
[DS11_Deep_Discovery_Inspector_200226US]