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.

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 100% detection rate and a recommended breach detection system four years in a row by NSS Labs.

Key Benefits

Better Detection

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

Tangible ROI

- Enhance existing investments
- Flexible deployment options
- Automation of manual tasks

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 kill chain.

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.

Greater visibility into attacks. Capture full network activity via packet capture (PCAP), simplifying the process for investigators to find clues during and after the time of attack.

Faster and higher ROI through a flexible architecture deploys as a single hardware or virtual appliance based on network throughput. Enhance existing investments in NGFW/IPS, SIEM, and gateways through sharing of threat intelligence.

Discovers ransomware anywhere in the network. Deep Discovery Inspector can detect script emulation, zero-day exploits, and targeted and password-protected malware commonly associated with ransomware. It also uses information on known threats to discover ransomware through pattern and reputation-based analysis. The custom sandbox can detect mass file modifications, encryption behavior, and modifications to backup restore.

A KEY PART OF TREND MICRO CONNECTED THREAT DEFENSE

To adequately protect against the current threat landscape, you need a multi-layered protection platform that delivers the full lifecycle 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:** Detect 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 is part of the Trend Micro Network Defense solution, powered by XGen™ security.

DEEP DISCOVERY INSPECTOR HARDWARE APPLIANCE SPECIFICATIONS

	500/1000 Series	4000 Series
Hardware Model	510/1100	4100
Throughput	500 Mbps / 1 Gbps	4 Gbps
Sandboxes Supported	2 (500), 4 (1000)	20
Form Factor	1U Rack-Mount, 48.26 cm (19")	2U Rack-Mount, 48.26 cm (19")
Weight	19.9 kg (43.87 lb)	31.5 kg (69.45 lb)
Dimensions (WxDxH)	43.4 (17.09") x 64.2 (25.28") x 4.28 (1.69") cm	48.2 cm (18.98") x 75.58 cm (29.75") x 8.73 cm (3.44")
Management Ports	10/100/1000 BASE-T RJ45 Port x 1 iDrac Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 Port x 1 iDrac Enterprise RD45 x 1
Data Ports	10/100/1000 BASE-T RJ45 Port x 5	10Gb SFP+ SR transceiver x 4 10/100/1000 Base-T RJ45 x 5
AC Input Voltage	100 to 240 VAC	100 to 240 VAC
AC Input Current	7.4A to 3.7A	10A to 5A
Hard Drives	2 x 1 TB 3.5" SATA	4 x 1TB 3.5" NLSAS
RAID Configuration	RAID 1	RAID 1+0
Power Supply	550W Redundant	750W Redundant
Power Consumption (Max.)	604W	847W (Max.)
Heat	2133 BTU/hr (Max.)	2891 BTU/hr (Max.)
Frequency	50/60 Hz	50/60 Hz
Operating Temp.	10-35 °C (50-95 °F)	10-35 °C (50-95 °F)
Hardware Warranty	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.

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

OTHER DEEP DISCOVERY PRODUCTS

Deep Discovery Inspector delivers advanced threat protection where it matters most to your organization—network, email, endpoint, or existing security solutions.

- **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 Windows and Mac O/S systems.
- **Deep Discovery Email Inspector** provides advanced malware detection, including sandboxing for email. Email Inspector can be configured to block delivery of advanced malware through email. This malware is often the first stage of a ransomware attack.

TREND MICRO™

Securing Your Journey to the Cloud