Trend Micro™

DEEP DISCOVERY INSPECTOR

Network-Wide Targeted Attack Detection

Targeted attacks and advanced threats are customized to infiltrate your unique IT infrastructure, evade conventional defenses, and remain hidden while stealing your corporate data. To detect these criminal intrusions, analysts and security experts agree that organizations should deploy advanced threat protection as part of an expanded security monitoring strategy.

Trend Micro Deep Discovery Inspector is an advanced threat protection appliance that provides network-wide visibility and intelligence to detect and respond to targeted attacks and advanced threats. The Inspector monitors all ports and more than 100 protocols to analyze virtually all network traffic, giving you the broadest protection available. Specialized detection engines and custom sandboxing identify and analyze malware, command-and-control (C&C) communications, and evasive attacker activities invisible to standard security. In-depth detection intelligence aids your rapid response, and is automatically shared with your other security products to create a real-time custom defense against your attackers.

Key Benefits

Targeted attack protection
Discovers threats that are invisible to standard security products

360-degree visibility and detection
Monitors virtually all traffic to detect attacks and reveal your true security posture

Rapid analysis and response
Fully characterizes threat and risk factors to drive a rapid response

Lower cost of ownership
Simplifies protection and management with a single appliance that lowers TCO

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery
MOST EFFECTIVE
Recommended Breach Detection System

2015 Breach Detection Tests

KEY FEATURES

Comprehensive threat detection
Monitors all ports and more than 80 protocols to identify attacks anywhere on your network

Detect malware, C&C, attacker activity
Uses specialized detection engines, correlation rules, and custom sandboxing to detect all aspects of a targeted attack, not just malware

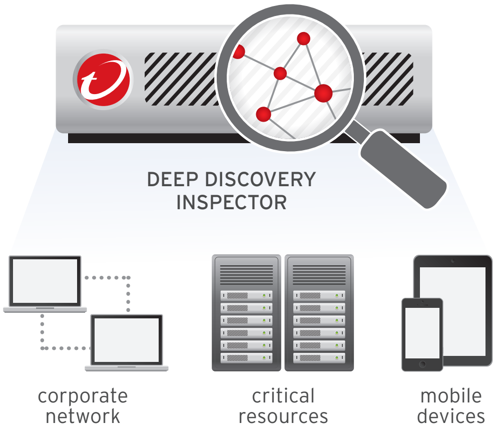
Custom sandboxes
Uses images that precisely match your system configurations to detect the threats that target your organization

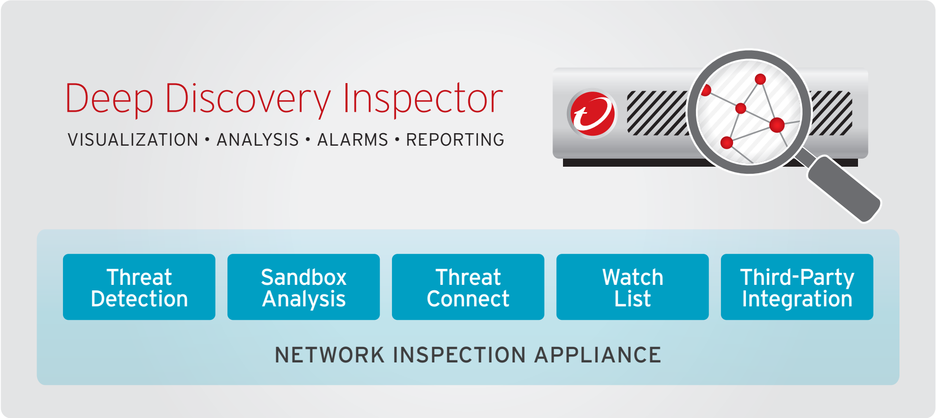
Smart Protection Network intelligence
Global threat intelligence powers detection and the Threat Connect portal for attack investigation

Broad system protection
Detects attacks against Windows, Mac OS X, Android, Linux, and any system

Single appliance simplicity and flexibility
Simplifies security with a single appliance available in a range of capacities, deployable in hardware or virtual configurations

Integrate Into Any Environment
Shares indicators of compromise (IOC) with third-party products and services such as HP Tipping Point, IBM and Palo Alto Networks firewalls, Check Point, and others





Deep Discovery Inspector

VISUALIZATION • ANALYSIS • ALARMS • REPORTING

Threat Detection

Sandbox Analysis

Threat Connect

Watch List

Third-Party Integration

NETWORK INSPECTION APPLIANCE

Detects and protects against

- Targeted attack and advanced threats
- Zero-day malware and document exploits
- Attacker 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 provides traffic inspection, advanced threat detection, and real-time analysis—all purpose-built for detecting targeted attacks. It uses a 3-level detection scheme to perform initial detection, then custom sandbox simulation, and finally, event correlation to discover evasive attacker activities.

Detection and correlation engines provide the most accurate and up-to-date protection, powered by global threat intelligence from Trend Micro™ Smart Protection Network™, and dedicated threat researchers. The results are high detection rates, low false positives, and in-depth intelligence designed to speed attack response.

HOW DEEP DISCOVERY INSPECTOR WORKS

Threat detection engines
An array of specialized detection engines and correlation rules focus on finding malware, C&C, and attacker activities across virtually all network traffic—beyond standard HTTP and SMTP. The Smart Protection Network and dedicated threat researchers continuously update these engines and rules.

Custom sandbox analysis
Custom sandbox analysis—using virtual environments that precisely match your system configurations—further analyzes suspect files and Web content. Custom sandboxing accurately detects the threats that target your organization, thwarts evasion techniques, and excludes irrelevant malware detections.

Watch list
A special display provides risk-focused monitoring of high-severity threats and high-value assets. Designated systems can be specifically tracked for suspicious activities and events, and for detailed analysis.

Threat connect
Threat Connect is a unique information portal that taps the global intelligence of the Trend Micro™ Smart Protection Network™ to provide you with the full breadth of available data relevant to a specific attack. This profile includes risk assessment; malware characteristics, origins, and variants; related C&C IPs; attacker profile; and suggested remediation procedures.

Central management and SIEM
Deep Discovery Inspector can be managed via the Trend Micro Control Manager. In addition, it integrates fully with leading SIEM platforms, including HP ArcSight, IBM QRadar, and Splunk.

IOC information sharing
Deep Discovery Inspector shares IOC information on new sandbox detections with other Deep Discovery, Trend Micro, and third-party products, including Palo Alto Networks, HP, IBM, Check Point, and others.

Flexible, high-capacity deployment
Meets diverse deployment and capacity requirements with a range of hardware and virtual appliances that can handle traffic capacity from 500 Mbps to 4 Gbps.

HOW DEEP DISCOVERY DETECTION WORKS

Monitoring 100+ protocols and applications across all network ports

	Attack Detection	Detection Methods
Advanced Malware	• Zero-day & known malware • Emails containing embedded document exploits • Drive-by downloads	• Decode & decompress embedded files • Custom sandbox simulation • Browser exploit kit detection • Malware scan (signature and heuristic)
C&C Communication	• C&C communication for all malware: bots, downloaders, data stealing, worms, blended threats, etc. • Backdoor activity by attacker	• Destination analysis (URL, IP, domain, email, IRC channel, etc.) via dynamic blacklisting, white listing • Smart Protection Network reputation of all requested and embedded URLs • Communication fingerprinting rules
Attacker Activity	• Attacker activity: scan, brute force, tool download, etc. • Data exfiltration • Malware activity: propagation, downloading, spamming, etc.	• Rule-based heuristic analysis • Extended event correlation and anomaly detection techniques • Behavior fingerprinting rules

WHY CUSTOM SANDBOXING IS ESSENTIAL

Cybercriminals are creating custom malware to target your specific environment—your desktop and laptop OS, apps, browsers, and more. Since the malware is designed to take advantage of these configurations, the malicious code may not execute in a generic sandbox. The bottom line: custom malware is more likely to go undetected in a generic sandbox that doesn't match your IT environment.

Only a custom sandbox can simulate your real IT environment and enable you to:

- Clearly identify custom malware targeting your organization—your Windows license, your language, your applications, and your mix of desktop environments
- Thwart sandbox evasion techniques based on generic Windows license, limited standard apps and versions, and English language
- Ignore malware that does not affect your organization, e.g., targeting other versions of Windows or applications

EXPAND YOUR SECURITY STRATEGY

Deep Discovery Inspector is part of the Deep Discovery platform, delivering advanced threat protection where it matters most to your organization—network, email, endpoint, or existing security solutions. You can extend the capabilities of Inspector by adding Deep Discovery Analyzer, Deep Discovery Endpoint Sensor, or Trend Micro Control Manager, and by sharing Inspector IOC detection intelligence with other products.

Deep Discovery Analyzer is an open, scalable custom sandbox analysis server. The Analyzer can be used to augment the protection capabilities of other Trend Micro solutions as well as third-party security products. The Analyzer can also be used to augment the sandboxing capacity and flexibility of Inspector or to centralize the sandboxing analysis across multiple Inspector units.

Deep Discovery Endpoint Sensor is a context-aware endpoint security monitor that records and reports detailed system-level activities on target endpoints. It can investigate based on targeted attacks discovered by Deep Security or by any third-party solution using OpenIOC or YARA files. Discovered IOC data can be used in Endpoint Sensor searches to verify infiltrations and discover the full context, timeline, and extent of the attack.

Trend Micro Control Manager provides centralized views, threat investigation, and reporting across Deep Discovery Inspector units, as well as central management functions for all Deep Discovery and Trend Micro products. Control Manager also acts as a distribution point for sharing newly discovered detection intelligence (C&C, other IOC information) across Deep Discovery units, Trend Micro, and third-party products.

DEEP DISCOVERY INSPECTOR HARDWARE APPLIANCE SPECIFICATIONS

	Inspector Model 250	Inspector Model 500 and 1000	Inspector Model 4000
Sandboxes Supported	1	2 (500) 4(1000)	20
Form Factor	1U Rack-Mount, 48.26 cm (19″)	1U Rack-Mount, 48.26 cm (19″)	2U Rack-Mount, 48.26 cm (19″)
Weight	19.9 Kg (43.87 lbs)	19.9 Kg (43.87 lbs)	31.5 kg (69.45 lb)
Dimensions (WxDxH)	43.4 (17.09″) x 64.2 (25.28″) x 4.28 (1.69″) cm	43.4 (17.09″) x 64.2 (25.28″) x 4.28 (1.69″) cm	43.4 (17.09″) x 75.58cm (29.75″) x 8.73cm (3.44″)
Management Ports	10/100/1000 BASE-T RJ45 Port x 1	10/100/1000 BASE-T RJ45 Port x 1 iDrac Enterprise RD45 X 1	10/100/1000 BASE-T RJ45 Port x 1
Data Ports	10/100/1000 BASE-T RJ45 Port x 2	10/100/1000 BASE-T RJ45 Port x 4	10Gb SFP+ Direct Attach Copper x 2 10/100/1000 Base-T RJ45 x 2
AC Input Voltage	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
AC Input Current	7.4A to 3.7A	7.4A to 3.7A	10A to 5A
Hard Drives	2 x 500GB 3.5 inch SATA	2 x 1 TB 3.5 inch SATA	4 x 1TB 3.5 inch NLSAS
RAID Configuration	RAID 1	RAID 1	RAID 1+0
Power Supply	350W Redundant	550W Redundant	750W Redundant
Power Consumption (Max)	385W	604W	847W (Max.)
Heat	1356 BTU/hr maximum	2133 BTU/hr (Max.)	2891 BTU/hr (Max.)
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
Operating Temp.	10 to 35 °C (50-95 °F)	10 to 35 °C (50-95 °F)	10 to 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.

Deep Discovery Platform

Deep Discovery Inspector is part of the Deep Discovery family of interconnected products, delivering network, email, endpoint and integrated protection—so you can deploy advanced threat protection where it matters most to your organization.

TREND MICRO™

Securing Your Journey to the Cloud