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 80 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 FEATURES**

**Comprehensive Threat Detection**
Monitors all ports and more than 80 protocols to identify attacks anywhere on your network

**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 Sandboxing**
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

**Custom Defense Solution**
Shares indicators of compromise (IOC) intelligence, automatically updating Trend Micro and other security products to protect you from further attack

**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

**Cornerstone of a Custom Defense**
Shares IOC intelligence with other security solutions, creating an integrated, real-time custom defense against targeted attacks

---

**NSS Labs 2014 Breach Detection Tests**

**TOP SCORE**
Trend Micro Deep Discovery

**NSSRECOMMENDED**

NSSLabs

---

**Deep Discovery Inspector**

**Corporate network**

**Critical resources**

**Mobile devices**
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.

**Virtual Analyzer**
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.

**Real-Time Threat Console**
The Deep Discovery Inspector console puts real-time threat visibility and deep analysis capabilities at your fingertips. It features quick-access widgets for critical information, geo-tracking of threat origins, Watch List monitoring of critical resources, and Threat Connect intelligence to assess attack characteristics.

**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 Smart Protection Network to provide you with the full breadth of available data relevant to your 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 independently or via the Trend Micro Control Manager. In addition, it integrates fully with leading SIEM platforms, including HP ArcSight, IBM QRadar, and Splunk.

**Dets 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

**IOC Information Sharing**
Deep Discovery Inspector shares IOC information on new sandbox detections with other Deep Discovery, Trend Micro, and third-party products, creating a real-time custom defense against attackers.

**Flexible, High-Capacity Deployment**
Meets diverse deployment and capacity requirements with a range of hardware and virtual appliances from 100 Mbps to 4 Gbps.
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

HOW DEEP DISCOVERY DETECTION WORKS

Monitoring 80+ protocols and applications across all network ports

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

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 integrated. 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 sandboxing capacity and flexibility of Inspector or to centralize the sandboxing analysis across multiple Inspector units. The Analyzer can also be used to augment the protection capabilities of other Trend Micro solutions as well as third-party security products.

Deep Discovery Endpoint Sensor is a context-aware endpoint security monitor that records and reports detailed system-level activities on target endpoints. It is especially useful to aid in the investigation and remediation of targeted attacks identified by Inspector.

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.

Trend Micro Custom Defense

The Deep Discovery platform is the foundation of the Trend Micro Custom Defense—enabling you to rapidly detect, analyze, and respond to your attackers. Deep Discovery detection and IOC intelligence integrates with a host of Trend Micro and third-party products to unite your security infrastructure into a real-time defense tailored to protect your organization against targeted attacks.
## Deep Discovery Inspector Hardware Appliance Specifications

<table>
<thead>
<tr>
<th></th>
<th>Inspector Model 250</th>
<th>Inspector Model 500</th>
<th>Inspector Model 1000</th>
<th>Inspector Model 4000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity</strong></td>
<td>250 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>4 Gbps</td>
</tr>
<tr>
<td><strong>Form Factor</strong></td>
<td>1U Rack-Mount, 48.26 cm (19&quot;)</td>
<td>1U Rack-Mount, 48.26 cm (19&quot;)</td>
<td>1U Rack-Mount, 48.26 cm (19&quot;)</td>
<td>2U Rack-Mount, 48.26 cm (19&quot;)</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>19.9 Kg (43.87lbs)</td>
<td>19.9 Kg (43.87lbs)</td>
<td>19.9 Kg (43.87lbs)</td>
<td>32.5kg (71.65lbs)</td>
</tr>
<tr>
<td><strong>Dimensions (WxDxH)</strong></td>
<td>43.4 (17.09&quot;) x 64.2 (25.28&quot;) x 4.28 (1.69&quot;) cm</td>
<td>43.4 (17.09&quot;) x 64.2 (25.28&quot;) x 4.28 (1.69&quot;) cm</td>
<td>43.4 (17.09&quot;) x 64.2 (25.28&quot;) x 4.28 (1.69&quot;) cm</td>
<td>48.2cm (18.98&quot;) x 75.58cm (29.75&quot;) x 8.73cm (3.44&quot;)</td>
</tr>
<tr>
<td><strong>Management Ports</strong></td>
<td>10/100/1000 BASE-T RJ45 Port x 1</td>
<td>10/100/1000 BASE-T RJ45 Port x 1</td>
<td>10/100/1000 BASE-T RJ45 Port x 1</td>
<td>10/100/1000 BASE-T RJ45 Port x 1</td>
</tr>
<tr>
<td><strong>Data Ports</strong></td>
<td>10/100/1000 BASE-T RJ45 Port x 2</td>
<td>10/100/1000 BASE-T RJ45 Port x 4</td>
<td>10/100/1000 BASE-T RJ45 Port x 4</td>
<td>10Gb SFP+ Direct Attach Copper x 2, 10/100/1000 Base-T RJ45 x 2</td>
</tr>
<tr>
<td><strong>AC Input Voltage</strong></td>
<td>100 to 240 VAC</td>
<td>100 to 240 VAC</td>
<td>100 to 240 VAC</td>
<td>100 to 240 VAC</td>
</tr>
<tr>
<td><strong>AC Input Current</strong></td>
<td>7.4A to 3.7A</td>
<td>7.4A to 3.7A</td>
<td>7.4A to 3.7A</td>
<td>10A to 5A</td>
</tr>
<tr>
<td><strong>Hard Drives</strong></td>
<td>2 x 500GB 3.5 inch SATA</td>
<td>2 x 500GB 3.5 inch SATA</td>
<td>2 x 500GB 3.5 inch SATA</td>
<td>8 x 600GB 3.5 inch SAS</td>
</tr>
<tr>
<td><strong>RAID Configuration</strong></td>
<td>RAID 1</td>
<td>RAID 1</td>
<td>RAID 1</td>
<td>RAID 5</td>
</tr>
<tr>
<td><strong>Power Supply</strong></td>
<td>350W Redundant</td>
<td>550W Redundant</td>
<td>550W Redundant</td>
<td>750W Redundant</td>
</tr>
<tr>
<td><strong>Power Consumption (Max)</strong></td>
<td>385W</td>
<td>604W</td>
<td>604W</td>
<td>847W (Max.)</td>
</tr>
<tr>
<td><strong>Heat</strong></td>
<td>1356 BTU/hr maximum</td>
<td>2133 BTU/hr (Max.)</td>
<td>2133 BTU/hr (Max.)</td>
<td>2891 BTU/hr (Max.)</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>50/60 Hz</td>
<td>50/60 Hz</td>
<td>50/60 Hz</td>
<td>50/60 Hz</td>
</tr>
<tr>
<td><strong>Operating Temp.</strong></td>
<td>10 to 35 °C (50-95 °F)</td>
<td>10 to 35 °C (50-95 °F)</td>
<td>10 to 35 °C (50-95 °F)</td>
<td>10 to 35 °C (50-95 °F)</td>
</tr>
<tr>
<td><strong>Hardware Warranty</strong></td>
<td>3 Years</td>
<td>3 Years</td>
<td>3 Years</td>
<td>3 Years</td>
</tr>
</tbody>
</table>

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.

### Custom Defense

The Deep Discovery platform is at the heart of the Trend Micro Custom Defense, weaving your security infrastructure into a comprehensive defense tailored to protect your organization against targeted attacks.

Deep Discovery’s custom detection, intelligence, and controls enable you to:

- Detect and analyze your attackers
- Immediately adapt protection against attack
- Rapidly respond before sensitive data is lost