Trend Micro™

DEEP DISCOVERY™ ANALYZER

Enhanced protection against targeted attacks

Targeted attacks and advanced threats are customized to evade your conventional security defenses and remain hidden, while stealing your sensitive data 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 to address today's evasive threats.

Deep Discovery Analyzer extends the value of existing security investments from Trend Micro and third-parties (through a web services API) by providing custom sandboxing and advanced analysis. It can also provide expanded sandboxing capabilities to other Trend Micro products. Suspicious objects can be sent to the Analyzer sandbox for advanced analysis using multiple detection methods. If a threat is discovered, security solutions can be updated automatically.

KEY CAPABILITIES

Custom Sandbox Analysis uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Flexible Deployment Analyzer can be deployed as a standalone sandbox or alongside a larger Deep Discovery deployment to add additional sandbox capacity. It is scalable to support up to 60 sandboxes in a single appliance, and multiple appliances can be clustered for high availability or configured for a hot or cold backup.

Advanced Detection Methods such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.

- **Broad file analysis range** Examines a wide range of Windows executables, Microsoft® Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. Custom policies can be defined by file type.
- **Document exploit detection** Discovers malware and exploits delivered in common document formats by using specialized detection and sandboxing.
- **URL analysis** Performs sandbox analysis of URLs contained in emails or manually submitted samples.
- **Web services API and manual submission** Enables any product or malware analyst to submit suspicious samples. Shares new IOC detection intelligence automatically with Trend Micro and third-party products.
- Support for Windows, Mac, and Android operating systems.

Detect ransomware Detects script emulation, zero-day exploits, 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 and restore.

Key Benefits

Better Detection

- Superior detection versus generic virtual environments
- Superior evasion resistance

Tangible ROI

- Enhance existing investments through integration and sharing of threat intelligence and additional processing capacity for high traffic environments
- Remove time consuming manual analysis of suspicious files
- Protect against expensive ransomware remediation
- Flexible deployment options for centralized or decentralized analysis

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery

100%

Breach Detection Rate

- 2017 -

RECOMMENDED 4 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 multi-layered protection platform that delivers the full life cycle of threat defense. Trend Micro Connected Threat Defense is a new cyber security model that can give organizations a better way to quickly protect, detect, and respond to new threats that are targeting them, while simultaneously improving visibility and control across their network.

- **Protect**: 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 to Trend Micro security layers and to/from third-party security using YARA and STIX.
- **Visibility and Control**: Gain centralized visibility across the network and systems; analyze and assess the impact of threats.

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

DEEP DISCOVERY ANALYZER APPLIANCE SPECIFICATIONS

	Hardware Model 1100
Capacity	45,000 samples/day
Supported File Types	cell, chm, class, dll, doc, docx, exe, gul, hwp, hwpx, jar, js, jse, jtd, lnk, mov, pdf, ppt, pptx, ps1, rtf, swf, vbs, vbe, xls, xlsx, xml
Supported Operating Systems	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, Mac OS
Form Factor	2U Rack-Mount, 48.26 cm (19")
Weight	32.5kg (71.65lbs)
Dimensions	Width 48.2cm (18.98") x Depth 75.58cm (29.75") x Height 8.73cm (3.44")
Management Ports	10/100/1000 Base-T RJ45 Port x 1
Data Ports	10/100/1000 Base-T RJ45 x 3
AC Input Voltage	100 to 240 VAC
AC Input Current	10A to 5A
Hard Drives	2 x 4 TB 3.5 inch SATA
RAID Configuration	RAID 1
Power Supply	750W Redundant
Power Consumption (Max)	847W (Max.)
Heat	2891 BTU/hr (Max.)
Frequency	50/60HZ
Operating Temp.	50-95 °F (10 to 35 °C)
Hardware Warranty	3 Years

Securing Your Journey to the Cloud

OTHER DEEP DISCOVERY PRODUCTS

Deep Discovery Analyzer 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.

- **Deep Discovery Inspector** is a virtual or hardware appliance which enables 360-degree detection of network-based targeted attacks and advanced threats. By using specialized detection engines and custom sandbox analysis, Inspector identifies advanced and unknown malware, ransomware, zero-day exploits, command and control (C&C) communications, lateral movement, and evasive attacker activities that are invisible to standard security defenses.
- **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 before it is delivered.