Trend Micro™

DEEP DISCOVERY ANALYZER

Boost your protection against targeted attacks with custom sandboxing

Targeted attacks and advanced threats are customized to infiltrate your unique IT infrastructure, evade conventional defenses, and remain hidden while stealing your corporate data. The advanced malware and evasive techniques used in these attacks is typically invisible to standard security solutions. Only virtual analysis, also known as sandboxing, can reliably detect and analyze this malware by executing and observing suspicious files in a secure, isolated environment. By integrating sandboxing analysis into your standard security products you can enhance their protection value and create a unified defense against targeted attacks.

Trend Micro™ Deep Discovery Analyzer™ is a scalable sandbox analysis server that provides on-demand, on-premise sandboxing services. Analyzer lets you define multiple, custom sandboxes—virtual environments that precisely match your desktop software configurations. It supports out-of-the-box integration with Trend Micro email and web security products as well as other products of the Deep Discovery platform. An open Web Services API allows any product or authorized individual to submit samples and obtain detailed analysis.

Key Benefits

Enhanced Attack Protection
Integrates malware sandboxing to improve the protection value of any security product

An Open, Scalable Platform
Provides a high performance, on-premise resource for advanced malware detection and analysis

In-Depth Malware Analysis
Enables deep malware investigation and consolidated reporting of malware detections

NSS LABS RECOMMENDED
Trend Micro™ Deep Discovery
TOP SCORE
in breach detection
NSS Labs 2014 Breach Detection Tests

KEY FEATURES

Scalable Sandboxing Services
Ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any source of samples

Custom Sandboxing
Performs sandbox simulation and analysis in environments that precisely match your desktop software configurations, ensuring optimal detection and low false-positive rates

Broad File Analysis Range
Examines a wide range of Windows Executable, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing

Document Exploit Detection
Discovers malware and exploits delivered in common office documents, using specialized detection and sandboxing

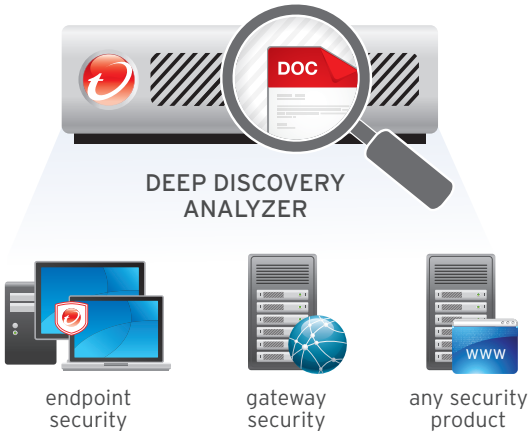
URL Analysis
Performs page scanning and sandbox analysis of URLs that are manually submitted

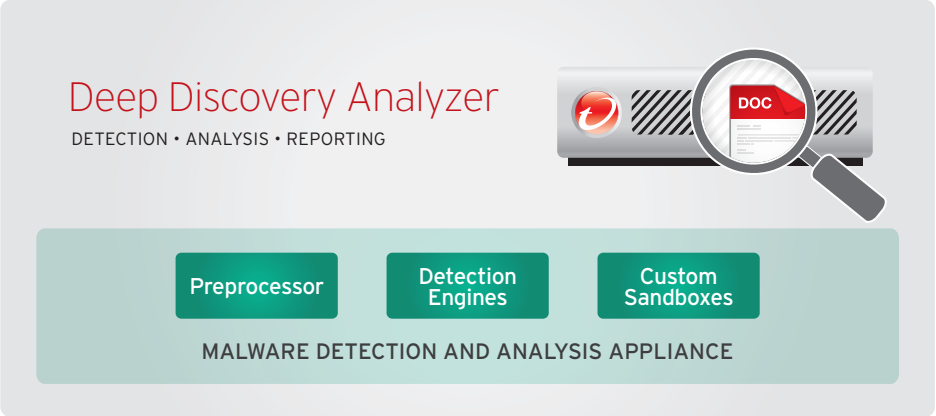
Detailed Reporting
Delivers full analysis results including detailed sample activities and command-and-control (C&C) communications via central dashboards and reports

Trend Micro Integration
Enables out-of-the-box integration with most Trend Micro email and web security products

Web Services API and Manual Submission
Allows any product or authorized threat researcher to submit samples

Custom Defense Integration
Shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products





WHY CUSTOM SANDBOXING IS ESSENTIAL

Cybercriminals are creating custom malware to target your specific environment—your desktop and laptop OS, apps, and browsers. Since the malware is designed to take advantage of your configurations, it is less likely to execute in a generic sandbox. Only a custom sandbox that precisely matches your IT configurations can accurately detect custom attacks.

Custom sandboxing simulates your real IT environment, so you can:

- 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 because it targets system or application versions that you don't use

HOW DEEP DISCOVERY ANALYZER WORKS

Preprocessor
As a first layer of detection, the preprocessor thwarts evasion techniques by extracting, unpacking, and decompressing sample files, then identifying the true file type regardless of extension used.

Detection Engines
Multiple detection engines analyze and verify files using signature and heuristics scanning, Trend Micro™ Smart Protection Network™ reputation checks, and white- and blacklists that you define.

Custom Sandboxes
Analyzer sends unknown and suspicious files to your best-fit custom sandbox, where it can safely execute and analyze potentially malicious code. A risk score and detailed summary are then delivered to the submitter. Results are also available for further analysis using the Analyzer management console.

Management, Analysis, and Reporting
The Analyzer console enables you to conduct in-depth analysis and create reports of both summary data and individual sample results. Within the management interface, you can create custom sandbox images, black- and whitelists, and sandboxing policies based on file type, for example to sandbox all PDFs automatically.

Deep Discovery Platform

Deep Discovery Analyzer 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

SPECIFICATIONS

	Deep Discovery Analyzer Model 1000
Capacity	20,000 samples/day
Supported File Types	exe, dll, swf, lnk, doc, docx, ppt, pptx, xls, pdf, hwp, cell, jtd, rtf, gul, jar, chm
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 x 1
Data Ports	10/100/1000 Base-T RJ45 x 3
AC Input Voltage	100 to 240 VAC
AC Input Current	5A to 10A
Hard Drives	8 x 300GB 3.5-in SAS
RAID Configuration	RAID 5
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

TREND MICRO™

Securing Your Journey to the Cloud