Datasheet

TREND MICRO™

Deep Discovery™ Analyzer

Enhanced protection against targeted attacks

Cyberattacks and threats are customized to evade conventional security and remain hidden, stealing or encrypting sensitive data until ransom demands are met. To detect these threats, organizations need to utilize advanced detection technology as part of a proactive security strategy.

Trend Micro™ Deep Discovery™ Analyzer extends the value of existing security investments from Trend Micro and, through a web services API, third parties. Empower your security operations center (SOC) team with custom sandboxing and advanced analysis. You can expand sandboxing capabilities to other Trend solutions, and suspicious objects can be sent to your Deep Discovery Analyzer sandbox for advanced analysis using multiple detection methods. If a threat is discovered, your security solutions are updated automatically.

Integrate seamlessly and secure proactively with Trend Vision One™

Integrate Deep Discovery Analyzer with Trend Vision One™ Sandbox Analysis for even more flexibility. Suspicious samples detected by our AI-powered enterprise cybersecurity platform, Trend Vision One™, can then be submitted for analysis. This benefits SOC teams that prefer to utilize their existing Deep Discovery Analyzer deployment instead of cloud-based sandbox analysis.

Key capabilities

Customize and enhance your sandbox analysis

Leverage virtual images tuned to precisely match system configurations, drivers, installed applications, and language versions. Improve the detection rate of advanced threats designed to evade standard virtual images. Utilize a custom sandbox environment with safe, external access to identify and analyze multi-stage downloads, URLs, and command and control (C&C) activity, while supporting manual or automated file and URL submission.

Expand your flexibility

Deploy Deep Discovery Analyzer as a standalone sandbox or alongside a larger Trend Micro™ Deep Discovery™ deployment for additional sandbox capacity. Scale to support up to 60 sandboxes in a single appliance, with the option to cluster multiple appliances for high availability or configure for hot or cold backup scenarios.

Leverage advanced detection methods

Utilize static, heuristic, and behavior analysis, web reputation, and file reputation for quick threat discovery. Detect multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.

Stay ahead of ransomware threats

Protect against script emulation, zero-day exploits, and targeted and password-protected malware commonly associated with ransomware. Utilize information on known threats to discover ransomware through pattern and reputation-based analysis. The custom sandbox enables you to detect mass file modifications, encryption behavior, and adjustments to backup and restore settings.

Key benefits

- Gain superior threat detection
  - Proactively manage risk with insights from Trend Vision One
  - Go further than generic virtual environments
  - Leverage flexible deployment options for centralized or decentralized analysis
  - Get support for Windows, macOS, and Linux operating systems
- Achieve tangible ROI
  - Enhance existing investments with integrated threat intelligence and extra processing for high traffic
  - Remove time-consuming manual analysis of suspicious files
  - Protect against expensive ransomware remediation

Go further with additional Deep Discovery options

Deep Discovery Analyzer is part of our Deep Discovery portfolio, delivering advanced threat protection where it matters most to your organization including network, email, endpoint, and existing security solutions.

Trend Micro™ 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, Deep Discovery Inspector enables you to identify advanced and unknown malware, ransomware, zero-day exploits, C&C communications, lateral movement, and evasive attacker activities that are invisible to standard security defenses.

Trend Micro™ Deep Discovery™ Email Inspector provides advanced malware detection, including sandboxing for email. It can be configured to block email-based delivery of advanced malware.

Proactive security starts here

Trend Vision One empowers SOC teams with real-time risk insights, Visualize, prioritize, and mitigate threats with speed and precision. Take control of your cyber risk, and leave adversaries with no place to hide.

- **Protect:** Assess potential vulnerabilities and proactively protect endpoints, servers, and applications
- **Detect:** Identify advanced malware, behavior, and communications invisible to standard defenses
- **Respond:** Respond rapidly with shared threat intelligence and delivery of real-time updates to Trend and third-party security layers using YARA and STIX
- **Visibility and control:** Centralize visibility across your network and systems to analyze and assess the impact of threats

Utilize advanced detection methods

- **Broad file analysis:** examine a wide range of file types including Microsoft Windows executables, Microsoft 365 documents, PDFs, web content, and compressed files via multiple detection engines and sandboxing
- **Document exploit detection:** Discover malware and exploits delivered in common document formats through specialized detection and sandboxing
- **URL analysis:** Perform sandbox analysis of URLs contained in emails or manually submitted samples
- **Web services API and manual submission:** Enable any solution or malware analyst to submit suspicious samples; share new indicators of compromise (IoC) detection intelligence automatically with Trend and third-party solutions

	Hardware Model 1300
Capacity	40,000 samples per day
Supported file types	**Windows**: Bat, cell, chm, class, cmd, com, csv, dll, doc, docx, exe, gul, hta, htm, html, hwp, iqy, jar, js, jse, jtd, lnk, mht, mhtml, mov, msi, odp, ods, odt, pdf, ppt, pptx, ps1, pub, rtf, shtm, shtml, slk, svg, swf, url, vbe, vbs, wsf, xht, xhtml, xls, xlsx, xml **Linux**: elf,sh **Mac**: class,dmg,jar,macho,pkg
Supported operating systems	Windows XP, 7, 8/8.1, 10, 11 - Windows Server 2003, 2008, 2012, 2016, 2019, 2022 - macOS - CentOS 7.8, RHEL 7,9 RHEL 8.3, Ubuntu 20.04.6
Form factor	2U rackmount, 48.2 cm (18.98")
Weight	28.82 kg (63.53 lb)
Dimensions	Width 48.2 cm (18.98") x Depth 75.13 cm ((29.58") x Height 8.68 cm (3.42")
Management ports	10/100/1,000 BASE-T RJ45 port x 1
Data ports	10/100/1,000 Base-T RJ45 port x 3
AC input voltage	100 - 240 VAC
AC input current	12A - 6.3A
Hard drives	4 TB 3.5-inch SATA x 2
RAID configuration	RAID 1
Power supply	1,100W redundant
Heat	4,125 BTU/hr. (max.)
Frequency	50/60 HZ
Operating temperature	41-104 °F (5 - 40 °C)
Hardware warranty	Three years; refer to Deep Discover product family hardware warranty validity

Industry recognition

Named a Leader in the Forrester Wave™: Network Analysis and Visibility Solutions, Q4 2025

ICSA labs CERTIFIED

Start your free trial

of Trend Vision One at TrendMicro.com/trial