Datasheet

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.

Trend Micro™ 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 solutions. Suspicious objects can be sent to the Deep Discovery 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.

Flexibility Deploy Deep Discovery Analyzer as a standalone sandbox or alongside a larger Trend Micro™ 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. Deep Discovery 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 Microsoft Windows executables, Microsoft 365, 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 indicators of compromise (IoC) detection intelligence automatically with Trend and third-party products.
- Support for Windows, Mac, and Android™ operating systems.

Detect ransomware including detects script emulation, zero-day exploits, and 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.

ICSA labs CERTIFIED

FORRESTER® WAVE LEADER 2023 Network Analysis And Visibility

A Key Part of Trend Vision One™

To adequately protect against the current threat landscape, you'll need multi-layered protection platform that delivers the full lifecycle of threat defense. Trend Vision One is a cybersecurity platform 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:** Identify 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 security layers and to/from third-party security using YARA and STIX.
- **Visibility and Control:** Gain centralized visibility across the network and systems to analyze and assess the impact of threats.

Deep Discovery Analyzer Appliance Specifics

	DEEP DISCOVERY ANALYZER
Capacity	36,000 samples/day
Supported File Types	alz, bat, cmd, cell, chm, csv, class, dll, doc, docx, egg, elf, exe, gul, hta, html, hwp, hwpx, igy jar, js, jse, jtd, lnk, mht, mhtml, mov, odt, odp, ods, pdf, ppt, pptx, ps1, pub, rtf, sh, slk, svg, swf, vbe, vbs, wsf, xls, xlsx, xml, xht, xhtml, url and much more
Supported Operating Systems	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016, 2019,Mac OS, Linux
Form Factor	2U rack-mount, 48.26 cm (19")
Weight	28.6 kg (63.05 lb)
Dimensions	Width 48.2 cm (18.98") x Depth 75.13 cm (29.58") x Height 8.68 cm (3.42")
Management Ports	10/100/1000 base-T RJ45 port x 1 – optional 10G SR SFP+
Data Ports	10/100/1000 base-T RJ45 x 3 – optional 10G SR SFP+
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	50/60 HZ
Operating Temp.	50-95 °F (10 to 35 °C)
Hardware Warranty	3 years

Other Deep Discovery Solutions

Deep Discovery Analyzer is part of the Trend Micro™ Deep Discovery™ portfolio, delivering advanced threat protection where it matters most to your organization–network, email, endpoint, or 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 identifies 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. Deep Discovery Email Inspector can be configured to block delivery of advanced malware through email before it is delivered.

For more information, please visit **TrendMicro.com**