Datasheet

Trend Micro™ Deep Discovery™ Email Inspector

Stop targeted email attacks that can cause data breaches and ransomware

Targeted attacks and advanced threats have proven their ability to evade conventional security defenses, exfiltrating sensitive data and/or encrypting critical data until ransom demands are met. Trend™ Research findings show **that more than 90% of these attacks** begin with a spear phishing email containing a malicious URL or attachment that is undetectable by standard email or endpoint security.

By working in tandem with your existing secure email gateway or by replacing it completely, Trend Micro Deep Discovery Email Inspector uses advanced detection techniques to identify and block purpose-built spear phishing emails often used to deliver advanced malware and ransomware to unsuspecting employees.

Email Inspector can be deployed in three different modes:

- Message transfer agent (MTA), for blocking
- Blind carbon copy (BCC), monitor-only
- Switched port analyzer (SPAN) or test access point (TAP)

Key capabilities

Transparency: Interface seamlessly with an existing spam filter or secure email gateway to detect advanced phishing attacks.

Extensive detection techniques: Detect zero-day exploits, advanced threats, ransomware, and attacker behavior. Use powerful techniques including pre-execution machine learning, real-time URL analysis, and custom sandbox analysis to detect known and unknown threats. In addition, Email Inspector supports MITRE ATT&CK™ framework to help you detect and respond to threats more effectively.

Custom sandbox analysis: Use virtual images tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rates of advanced threats designed to evade standard virtual images. The custom sandbox environment includes safe external "live mode access" to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more.

URL protection: Utilize time-of-click protection in addition to customer sandbox analysis of URLs, the latter of which follows URL redirects and file downloads. When a user clicks on a link, a real-time website analysis is performed.

Password extraction: Use Email Inspector to enable scanning of encrypted attachments. Determine the passwords of protected archives and documents using customizable dictionaries and keywords found within the message.

Business email compromise (BEC) and fraud prevention: Harness a combination of expert rules and machine learning to identify fraud emails by looking for indicators of attack (IoA) and email intention. More stringent protection can be applied to executives and other important users in your organization.

Gateway filtering: Utilize this optional gateway module for Email Inspector to filter inbound messages based on senders, spam and phishing filters, and content, all while providing outbound Trend Micro Data Loss Prevention™ and email encryption to fulfill compliance requirements. Gateway filtering also includes end-user quarantine for spam messages, and content disarm and reconstruction (CDR) to remove potentially malicious code.

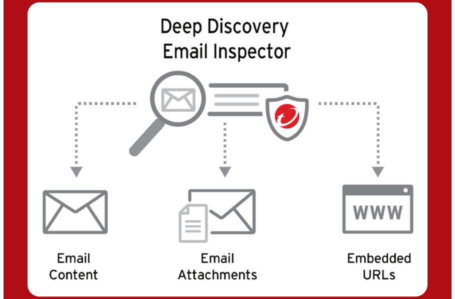
Key Benefits

Better protection

- Stops spear phishing emails, which are responsible for most targeted attacks
- Detects ransomware before systems are compromised
- Finds threats invisible to standard email security by using custom sandboxing

Tangible ROI

- Stops targeted spear phishing and ransomware, avoiding costly damage clean-up
- Works seamlessly with existing email security solutions
- Shares indicators of compromise (IoCs) with network and endpoint security layers



Email Inspector appliance hardware specifications

Hardware specifications	Model 7300	Model 9200
Deployment options	MTA, BCC, SPAN/TAP modes	MTA, BCC, SPAN/TAP modes
Capacity	Up to 400,000 emails per day	Up to 800,000 emails per day
Form factor	1U, rack-mounted, 48.26 cm (19")	2U, rack-mounted, 48.26 cm (19")
Dimensions	43.4 cm (17.08") x 73.5 cm (28.94") x 4.28 cm (1.69")	43.4 cm (17.08") x 75.13 cm (29.58") x 8.68 cm (3.42")
Weight	18.6 kg (41.05 lb)	31.5 kg (69.45 lb)
Management ports	10/100/1000 BASE-T RJ45 port x 1 Integrated Dell Remote Access Controller (iDRAC) Enterprise RJ45 x 1	10/100/1000 BASE-T RJ45 port x 1 iDRAC Enterprise J45 x 1
Data ports	10/100/1000 BASE-T RJ45 port x 5	10/100/1000 BASE-T RJ45 port x 3
AC input voltage	100 to 240 VAC	100 to 240 VAC
AC input current	9.2 A to 4.7 A	10 A to 5 A
Hard drives	2 x 2-TB SATA	2 x 4-TB 3.5-inch SATA
Internet protocol (IP) support	IPv4/IPv6	IPv4/IPv6
RAID configuration	RAID 1	RAID 1
Power supply	800 W redundant	750 W redundant
Max. power consumption	899 W	847 W
Heat	3000 BTU/hr (max.)	2891 BTU/hr. (max.)
Operating temperature	10-35°C (50-95°F)	10-35°C (50-95°F)
Hardware warranty	Three years	Three years
Optional fiber network interface card (NIC)	Dual-port fiber gigabit (SX/LX) or 10-gigabit	Dual-port fiber gigabit (SX/LX) or 10-gigabit

Virtual appliance deployment when connected with Trend Micro™ Deep Discovery™ Analyzer

For additional flexibility, Email Inspector can be deployed as a virtual server within your own environment when connected to Deep Discovery Analyzer hardware. In this deployment scenario, the virtual appliance will provide all functions except for sandbox analysis, which is completed on Deep Discovery Analyzer appliances.

Virtual appliance deployment supports VMware ESXi 6.0 or 6.5 as well as Microsoft Hyper-V on Windows Server (2016 or 2019). Nested virtual machines are not supported. Please note that a Deep Discovery Analyzer hardware appliance is required for sandbox analysis.

Moving to the cloud?

Trend Micro™ Email Security Advanced offers a level of protection similar to that of a cloud email gateway. Meanwhile, Trend Micro™ Cloud App Security provides API-integrated protection for Microsoft 365 and Google Workspace™ email and file sharing. Both cloud solutions can now update to **Trend Vision One™ – Email and Collaboration Security**.

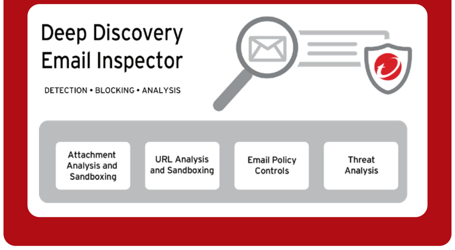
ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Detect and protect against

- Targeted attacks and advanced threats
- Phishing, spear phishing, and other email threats
- Zero-day malware and document exploits
- Ransomware attacks

Optional gateway module

- Top-rated spam prevention
- Sender reputation and content filtering
- End-user-quarantine for spam messages
- Data loss prevention and email encryption for compliance
- CDR to remove executable objects for file sanitation


Deep Discovery
Email Inspector
DETECTION • BLOCKING • ANALYSIS
Attachment Analysis and Sandboxing
URL Analysis and Sandboxing
Email Policy Controls
Threat Analysis

For details about what personal information we collect and why, please see our Privacy Notice at **trendmicro.com/privacy**