Trend Micro™

DEEP DISCOVERY™ EMAIL INSPECTOR

Stop targeted email attacks that can lead to data breaches or ransomware

Targeted attacks and advanced threats have proven their ability to evade conventional security defenses and exfiltrate sensitive data, or encrypt critical data until ransom demands are met. Trend Micro Research shows 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 that are often used to deliver advanced malware and ransomware to unsuspecting employees. Email Inspector can be deployed in MTA (blocking), BCC mode (monitor only), or SPAN/TAP mode.

KEY CAPABILITIES

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

Extensive detection techniques
Detects zero-day exploits, advanced threats, ransomware, and attacker behavior. It uses techniques such pre-execution machine learning, real-time URL analysis, and custom sandbox analysis to detect known and unknown threats. Supports Mitre ATT&CK framework to help you detect and respond to threats more effectively.

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 rates of advanced threats that are 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
In addition to customer sandbox analysis of URLs, which follows URL redirects and file downloads, time-of-click protection is included. When a user clicks on a link, a real-time website analysis is performed via the Trend Micro™ Smart Protection Network™.

Password Extraction

In order to scan encrypted attachments, Email Inspector guesses the password of protected archives and documents using customizable dictionaries and keywords found in the message.

Fraud/Business Email Compromise (BEC) Prevention

A combination of expert rules and machine learning identify fraud emails by looking for attack indicators and email intention. More stringent protection can be applied to executives and other important users in your organization.

Gateway Filtering

The optional gateway module enables Email Inspector to filter inbound messages based on senders, spam and phishing filters, and content, while providing outbound Trend Micro™ Data Loss Prevention™ and email encryption to fulfill compliance requirements. Gateway filerting also includes end-user quarantine for spam messages, and content disarm and reconstruction (CDR) to remove executable objects from Microsoft files for file sanitation.

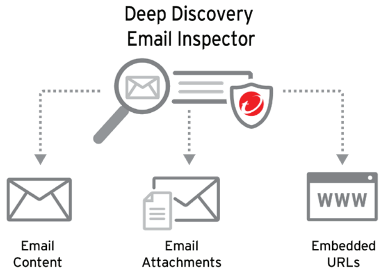
Key Benefits

Better Protection

- Stops spear phishing emails that are responsible for most targeted attacks
- Detects ransomware before damage is done
- Finds the threats invisible to standard email security by using custom sandboxing

Tangible ROI

- Stops targeted spear phishing and ransomware, which means costly damage cleanup is avoided
- Works seamlessly with existing email security solutions
- Shares indicators of compromise (IoCs) with network and endpoint security layers



Email Inspector can detect and block attempts to infiltrate ransomware against unsuspecting employees by finding:

- Unknown ransomware: machine learning analysis, communication fingerprinting, script emulation, zero-day exploits, targeted and password-protected malware
- Mass file modifications, encryption behavior, and modifications to backup through custom sandboxing

Once ransomware is detected, it can be blocked from being delivered to a recipient and prevented from encrypting any data. IOCs can be shared automatically with network and endpoint controls to stop subsequent attacks.

DEEP DISCOVERY EMAIL INSPECTOR APPLIANCE HARDWARE SPECIFICATIONS

Hardware Specifications	Model 7200	Model 9200
Deployment Options	MTA, BCC, SPAN/TAP modes	MTA, BCC, SPAN/TAP modes
Capacity	Up to 400,000 emails/day	Up to 800,000 emails/day
Form Factor	1U rack-mount, 48.26 cm (19")	2U rack-mount, 48.26 cm (19")
Dimensions	43.4 (17.09") x 64.2 (25.28") x 4.28 (1.69") cm	43.4 (17.08") x 75.13 (29.58") x 8.68 (3.42") cm
Weight	17.5 kg (38.58 lb)	31.5 kg (69.45 lb)
Management Ports	10/100/1000 BASE-T RJ45 port x 1 iDRAC Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 port x 1 iDRAC Enterprise RD45 x 1
Data Ports	10/100/1000 BASE-T RJ45 x 3	10/100/1000 BASE-T RJ45 x 3
AC Input Voltage	100 to 240 VAC	100 to 240 VAC
AC Input Current	7.4A to 3.7A	10A to 5A
Hard Drives	2 x 1 TB 3.5-inch SATA	2 x 4 TB 3.5-inch SATA
Internet Protocol Support	IPv4 / IPv6	IPv4 / IPv6
RAID Configuration	RAID 1	RAID 1
Power Supply	550W redundant	750W redundant
Power Consumption (Max)	604W	847W
Heat	2133 BTU/hr. (max.)	2891 BTU/hr. (max.)
Operating Temperature	10 to 35°C (50-95°F)	10 to 35°C (50-95°F)
Hardware Warranty	3 years	3 years
Optional Fiber 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 on your own environment when connected to Deep Discovery Analyzer hardware appliances. In this deployment scenario, the virtual appliance will provide all functions except for sandbox analysis, which is done on Analyzer appliances.

Virtual Appliance Requirements:

- Supports VMware ESXi 6.0 or 6.5, Microsoft Hyper-V on Windows Server 2016 or 2019
- Nested virtual machines are not supported
- Analyzer hardware appliance(s) are required for sandbox analysis

MOVING TO THE CLOUD?

Trend Micro™ Email Security Advanced offers similar protection as cloud email gateway and Trend Micro™ Cloud App Security provides API-integrated protection for Microsoft 365 and Google Workspace™ email and file sharing. Combine both layers with Trend Micro™ Smart Protection for Office 365.

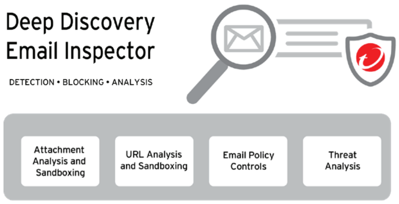
Deep Discovery Email Inspector is part of the Trend Micro Network Defense solution, powered by XGen™ security.

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

Securing Your Connected World

[DS11_Deep_Discovery_Email_Inspector_Datasheet_210329US]