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 percent of these attacks begin with a spear phishing email containing a malicious attachment or URL that is undetectable by standard email or endpoint security.

Deep Discovery Email Inspector uses advanced detection techniques to identify and block spear phishing emails that are often used to deliver advanced malware and ransomware to unsuspecting employees. By working seamlessly, and in tandem with your existing secure email gateway, Email Inspector can detect and block purpose-built spear phishing emails–which use malicious attachments and URLs as a common delivery vehicle for targeted attacks–along with advanced threats and ransomware. Deep Discovery 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 spear phishing email attacks that use attachments and URLs to conceal advanced malware including ransomware (often buried within macros).

Extensive detection techniques
Detects zero-day exploits, advanced threats, ransomware, and attacker behavior. It uses techniques such as file, IP and web reputation, static analysis, heuristic analysis, algorithms, and custom sandbox analysis to detect known and unknown threats. Local threat intelligence is correlated with threat insight from Trend Micro.

Flexibility
Available with the following deployment options: in-line blocking/quarantine, logging, or removing a detected threat from an email and notifying the user.

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. Sandboxing capabilities are offered as part of an integrated appliance or as a scalable standalone capability.

Protection from Ransomware Attacks
From the time a spear phishing attack is launched, the first user will open a malicious email within one minute and 40 seconds.[1] Given the fact that email is the threat vector of choice for the delivery of ransomware, all the users in your organization are at risk.

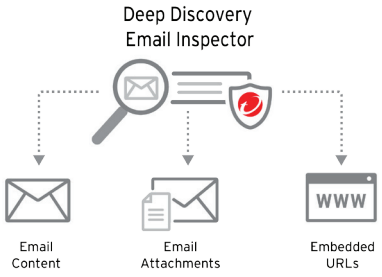
Key Benefits

Better Protection

- Stops spear phishing emails that start 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 IOCs with network and endpoint security layers



NSS LABS RECOMMENDED
RECOMMENDED
Breach Detection System
3 YEARS IN A ROW
99.8% Detection Rate

ICSA labs CERTIFIED

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

- Known ransomware: pattern and reputation-based analysis
- Unknown ransomware: communication fingerprinting, script emulation, zero-day exploits, targeted, and password protected malware
- Mass file modifications, encryption behavior, and modifications to backup restore 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 7100	Model 9100
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 (17.09") x 75.58 (29.75") x 8.73 (3.43") cm
Weight	19.9 Kg (43.87 lbs)	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 600 GB 2.5 inch SAS	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)	Dual Port Fiber Gigabit (SX/LX)

PART OF THE DEEP DISCOVERY PLATFORM

Deep Discovery Email Inspector is part of the Deep Discovery platform, delivering advanced threat protection where it matters most to your organization—network, email, endpoint or in-place security solutions.

Deep Discovery Inspector is a turnkey network appliance that monitors all ports and over 107 protocols for targeted attacks. Extensive detection techniques, including onboard sandboxing, ensuring targeted attacks are identified quickly.

Deep Discovery Analyzer provides advanced sandbox analysis to extend the value of security products such as endpoint protection, web and email gateways, network security, and other Deep Discovery products. Suspicious objects or URLs can be automatically or manually sent to Deep Discovery Analyzer for analysis. Using extensive detection and anti-evasion techniques, Deep Discovery Analyzer can detect ransomware, advanced malware, zero-day exploits, C&C, and multi-stage downloads resulting from malicious payloads or URLs on Windows, Mac, and Android operating systems.

1 2016 Verizon Data Breach Investigations Report

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

TREND MICRO™

Securing Your Journey to the Cloud