CHECK POINT
TE250X APPLIANCE

CHECK POINT
TE250X APPLIANCE

Stop new and unknown threats

Product Benefits

- Prevent new and unknown attacks in business documents and executable files
- Reduces costs by leveraging existing security infrastructure
- Maximize protection through unified management, monitoring, and reporting
- Secure the network with a zero false-positive sandbox solution
- Increase security with automatic sharing of new attack information with ThreatCloud™

Product Features

- Identify new malware hidden in Adobe PDF, Microsoft Office, Java, Flash, executables, and archives
- Protection against attacks targeting multiple Windows OS environments
- Recommended for 250,000 file-scans per month (performance varies)
- Threat Extraction removes exploitable content to deliver malware free documents

INSIGHTS

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments.

These threats include new exploits, or even variants of known exploits unleashed almost daily with no existing signatures and therefore no standard solutions to detect those variants. New and undiscovered threats require new solutions that go beyond signatures of known threats.

SOLUTION

Threat Emulation prevents infections from undiscovered exploits, zero-day, and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior, preventing it from entering the network. Our Threat Emulation reports to the ThreatCloud™ service and automatically shares the newly identified threat information with all our other customers.

Traditional solutions have focused on detection, providing notifications after a threat has breached the network. Check Point Threat Emulation blocks new threats before infection can even occur.

Emulation Specifications	
Supported files for emulation	Adobe PDF, Microsoft Office, Executables, Java, Flash, files in archives
Supported Emulation Environments	Microsoft Windows XP, 7; Office; Adobe Reader

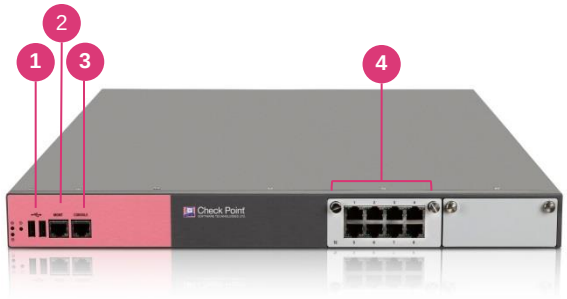
PRIVATE CLOUD EMULATION APPLIANCES

We offer a wide range of appliances to support your security, including the ThreatCloud™ Emulation Service. However, if regulatory or privacy concerns lead you to prefer not to use cloud applications, we offer the TE250X, an on-site appliance option.

TE250X Appliance	
Recommended files/month	250,000
Recommended users	3,000
Throughput (Mbps)	700

TE250X Appliance

1. 2 x USB ports
2. 10/100/1000Base-T Management port
3. Console port
4. 8 x 10/100/1000Base-T ports



DEPLOYMENT OPTIONS

Emulate threats in one of two deployment options:

1. Private cloud: Check Point security gateways send files to a TE250X appliance for emulation
2. Inline: This is a stand-alone option that deploys a TE250X inline or on a SPAN port, and uses all of the Threat Prevention Blades

KNOWN AND UNKNOWN THREAT DETECTION

Threat Emulation Private Cloud Appliances protect you from both known and unknown threats with Antivirus, Anti-Bot, Threat Emulation, and Threat Extraction technologies.

KNOWN THREAT DETECTION

The Antivirus Software Blade uses real-time virus signatures from ThreatCloud™ to detect and block known malware at the gateway before users are affected. The Anti-Bot Software Blade detects bot-infected machines, preventing damages by blocking bot Command & Control communications.

UNKNOWN THREAT DETECTION

Threat Emulation employs the fastest and most accurate sandboxing tools available to pre-screen files, protecting your organization from attackers before they enter your network.

CPU-LEVEL SANDBOX READY

Threat Emulation Private Cloud Appliances include the hardware needed to take sandbox detection of unknown threats to the next level. Threat Emulation with a CPU-level sandbox engine will monitor the instruction flow at the CPU-level to detect exploits attempting to bypass OS security controls, effectively stopping attacks before they have a chance to launch.

MALWARE FREE DOCUMENTS

Documents that we use on a daily basis can contain exploitable content, including macros or embedded links, which can infect your computers and networks. Threat Extraction eliminates threats by removing exploitable content and reconstructing the document using known safe elements, delivering a malware-free document to its intended destination.

Threat Extraction delivers documents with zero malware in zero seconds. Analyzing the original document in an isolated sandbox, it immediately identifies unknown threats. Configure Threat Extraction in one of two ways: Quickly provide a reconstructed document to the user, or await response from Threat Emulation before determining whether or not to reconstruct the document.

INSPECT ENCRYPTED COMMUNICATIONS

Files delivered into the organization over SSL and TLS represent a secure attack vector that bypasses many industry standard implementations. Our Threat Prevention looks inside these protected SSL and TLS tunnels to extract and launch files to discover hidden threats.

THREAT EMULATION DETAILED REPORT

Every file emulation generates a detailed report. Simple to understand, the report includes detailed information about any malicious attempts originated by running this file. The report provides actual screenshots of the simulated environment(s) while running the file.

THREATCLOUD ECOSYSTEM

Newly discovered threats are sent to ThreatCloud, which can then protect other Check Point connected gateways. This allows all other Check Point connected gateways to block the threat before it has a chance to become widespread. This constant collaboration makes the ThreatCloud™ ecosystem the most advanced and up-to-date threat network available.

TECHNICAL SPECIFICATIONS

	TE250X
Performance	
Recommended users	Up to 3,000
Throughput (Mbps)	700
Number of virtual machines	8
Hardware	
Storage	1 TB HDD
Memory	16 GB DDR4
LOM	Not included
Slide Rails (22” to 32”)	Included
Network	
10/100/1000Base-T RJ45 interfaces	8
1000Base-F SFP interfaces	-
Expansion slot	Not used
Dimensions	
Enclosure	1U
Metric (W x D x H)	438 x 621 x 44 mm
Standard (W x D x H)	17.25 x 24.45 x 1.73 in.
Weight	9.8 kg (21.6 lbs.)
Environment	
Operating	32º ~ 104ºF / 0º ~ 40ºC (20~90%, non-condensing)
Storage	-14° to 158°F / -10° to 70° (20% - 90% non-condensing)
Power	
Dual, hot swappable	optional
AC input	100-240V
Frequency	47-63 Hz
Single Power Supply Rating	400W
Power Consumption Maximum	104W
Maximum Thermal Output	355.7 BTU/h
Certifications	
Safety	CB, UL, Multiple Listing, LVD, TUV
Emissions	FCC, CE, VCCI, RCM
Environment	RoHS

APPLIANCE PACKAGES

BASE CONFIGURATION[1]	
TE250X Private Cloud Appliance with 1 year Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service (includes Microsoft Windows and Office license for 8 Virtual Machines)	CPAP-TE250X-8VM
SOFTWARE BLADE PACKAGE[1]	
Threat Emulation, Threat Extraction, Antivirus and Anti-Bot annual service for the TE250 Appliance	CPSB-TE-250-1Y

[1] SKUs for 2 and 3 years are available, see the online Product Catalog

ACCESSORIES

SPARES AND MISCELLANEOUS	
AC Power Supply for TE250X	CPAC-PSU-TE250X

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com