



ThreatCloud Emulation Service

Discover and stop new, zero-day and targeted attacks

ThreatCloud Emulation Service

CHALLENGE

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

ThreatCloud 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. Discovered malware is prevented from entering the network. Check Point ThreatCloud Emulation reports to the ThreatCloud™ service and automatically shares the newly identified threat information with other Check Point customers.

Traditional solutions have focused on detection, providing notifications after a threat has breached the network. With Check Point ThreatCloud Emulation, new threats are blocked and infection does not occur.

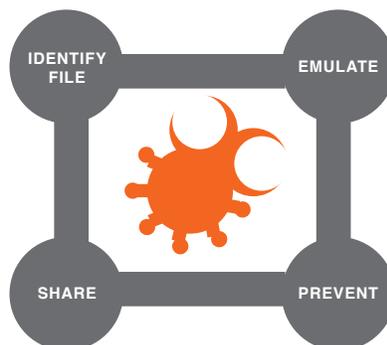
HOW IT WORKS

Identify suspicious files at the organization

- Identify files in email attachments or downloads from the web
- Suspicious files are sent to the ThreatCloud Emulation Service
- Supported without Check Point infrastructure using a unique agent for Exchange server
- Supported on existing Security Gateways running R77

File Emulation

- Launch files for emulation in a virtual sandbox environment
- Inspect file behavior in multiple operating systems and office versions
- Monitor activities: file-system, system-registry, processes and network connections
- Suspicious activities by files are flagged, and a unique algorithm further determines whether the file is engaged in malicious activities
- Generate a detailed report including file details, abnormal activity details and actual screenshots of the sandbox environment while running the file



KEY FEATURES

- Identify new malware hidden in Adobe PDF, Microsoft Office, executable and archive files
- Emulate files and documents for threats in a secure sandbox
- Protection against attacks targeting multiple Windows OS environments
- Emulate files within SSL and TLS communications
- Prevent malicious files from entering the organization

KEY BENEFITS

- Cloud based service—works with your existing infrastructure. No need to install new equipment
- Reduce operational overhead with a low monthly price for the entire organization, based on incoming file volume
- A unique exchange integration monitors email attachments offering protection from email-borne threats
- Zero false-positives means you can secure the network without stopping the flow of business
- Increase security with automatic sharing of new attack information with ThreatCloud



Datasheet: Check Point ThreatCloud Emulation Service

Prevent malicious file from entering the organization

- Malicious files are stopped inline before breaching the network

Share malicious information with ThreatCloud

- Immediate update to ThreatCloud to prevent newly detected malicious files from entering other organizations

CHECK POINT THREATCLOUD EMULATION FEATURES

ThreatCloud Emulation Service

ThreatCloud Emulation Service is a cost-effective subscription where customers pay only for the amount of incoming files to the organization. No changes are required at the organization—files can be sent for emulation from an existing security gateway or from an agent for Exchange server. A global quota for the organization allows centralized management and visibility of both threat and service usage information.



Virtual Sandboxing

Check Point ThreatCloud Emulation works by intercepting and filtering inbound files, running them in a virtual environment, and flagging those files that engage in suspicious or malicious behavior commonly associated with malware, such as modifying the registry, network connections, new file creation, and more. Once these new threats are discovered, the file signature is sent to Check Point ThreatCloud to turn the new malware into a known and documented threat that can be prevented.

Multiple Emulation OS Support

Check Point ThreatCloud Emulation provides multiple simultaneous environments for file simulation: Windows XP, 7, Microsoft Office and Adobe environments.

ThreatCloud Emulation Detailed Report

A detailed report is generated per any file emulation. The report is simple to understand and includes detailed information about any malicious attempts originated by running the file. The report provides actual screenshots of the environment while running the file for any operating system on which it was simulated.

Encrypted Communications

Files delivered into the organization over SSL and TLS represent a secure attack vector that bypasses many industry standard implementations. Check Point ThreatCloud Emulation looks inside SSL and TLS tunnels to extract and launch files to discover threats hidden in those protected streams.

Prevent Malicious Files from entering the Organization

Files returned back to the security gateway or Exchange agent with detailed information about their activity from the ThreatCloud Emulation Service. Malicious files then stopped from getting into the user and prevent infection at the organization.

ThreatCloud Ecosystem

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

Simple and Flexible Deployment at the Organization

Check Point ThreatCloud Emulation is implemented in a way that works with existing networks. Files can be sent to the ThreatCloud Emulation Service or to a Private Cloud Emulation Appliance. Any R77 Security Gateway or an agent for Exchange server can monitor incoming files and send suspicious ones to emulation.

SPECIFICATIONS

ThreatCloud Emulation Service

Organizations can choose from 5 options for global file inspections per month, starting at 10,000 files per month and up.

Private Cloud Emulation Appliances

Two appliance options are available, with overall performance supporting organizations up to 3,000 users and above 3,000 users.

Emulation Specifications

Supported Files for Inspection	Adobe PDF, Microsoft Office, EXE, files in archives
Supported Emulation Environments	Microsoft Windows XP, 7; Microsoft Office; Adobe Reader

Security Gateway Specifications

To detect and send files to ThreatCloud Emulation Service

Supported Platforms	Check Point Appliances: 2000, 4000, 12000, 13000, and 21000 using R77 or higher; other appliances and open servers with equivalent performance to the above models are supported
Operating Environment	SecurePlatform or GAiA

CONTACT CHECK POINT

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