CHECK POINT THREAT EMULATION

Product Benefits

- Turns zero-day attacks into known and preventable attacks
- Fastest at detecting and blocking unknown malware
- Best catch rate of unknown malware
- Makes it virtually impossible for hackers to evade detection
- Implement, configure, and use with no disruption to existing deployments

Product Features

- Combines OS-level and CPU-level emulation for the fastest and most accurate sandbox solution
- Protects the broadest range of common file-types, including archive files, and web objects like Flash
- Zero false-positives means you can secure the network without stopping the flow of business
- OS agnostic CPU-level detection
- Works with your existing infrastructure, no need to install new equipment
- Increase security with automatic sharing of new attack information with ThreatCloud™

INSIGHTS

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. These attacks include new malware, or even variants of known malware unleashed almost daily with no existing signatures and therefore no standard solutions to detect those variants. Malware complexity is also increasing as cybercriminals get better at combining techniques, masking their malware signatures and varying their attack methods.

It has become critical for organizations to implement protections against malware attacks hidden in executables, as well as regular documents and web pages. A new and complete approach of threat detection and prevention is needed to protect organizations against unknown malware, zero-day, and targeted attacks.

SOLUTION

Check Point Threat Emulation combines the power of both CPU-level and OS-level protection to detect and block malware, and prevent infections from undiscovered exploits, and zero-day and targeted attacks.

CPU-level sandboxing detects the use of exploit methods by carefully examining the CPU activity and the execution flow at the assembly code level while the exploit occurs. Not only is this OS-agnostic detection, but it makes it virtually impossible for hackers to evade detection. Check Point Threat Emulation is the only true zero-day solution, as detection occurs before the malware executes and before attackers have a chance to employ any evasion tactic.

To further investigate files, OS-level sandboxing quickly inspects files and runs them in a virtual sandbox to discover malicious behavior and provide additional data on the nature of the attempted attacks. In addition, it uncovers attacks using executables or macros, or those exploiting logical flaws. Discovered malware is prevented from entering the network.

The speed and accuracy of the combination of OS-level and CPU-level threat emulation delivers the best possible catch rate, and most comprehensive technology in inspecting, detecting and protecting against unknown malware, zero-day and targeted attacks.

A unique added benefit of Check Point Threat Emulation is that it reports newly discovered threat information into our ThreatCloud™ intelligence database and automatically shares the newly identified threat information with other Check Point customers to enable them to protect themselves from newly identified threats.

DETECT EXPLOITS AT THE CPU LEVEL

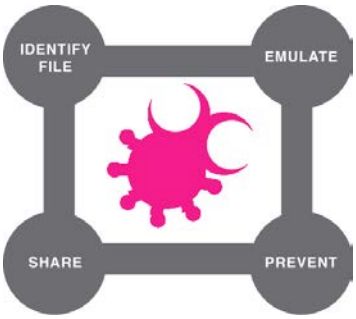
Check Point is the only zero-day solution using CPU-level sandboxing to stop attacks before they have a chance to launch. There are thousands of vulnerabilities and millions of malware implementations, but there are very few methods that cyber criminals utilize to exploit vulnerabilities. CPU-level sandboxing detects the use of these methods. Check Point's Threat Emulation engine monitors CPU-based instruction flow for exploits attempting to bypass OS security controls.

By detecting exploit attempts during the pre-infection stage, Check Point Threat Emulation CPU-level sandboxing stops attacks before they have a chance to evade detection by the sandbox.

IDENTIFY MALICOUS FILES

Check Point Threat Emulation conducts further investigation at the OS-level by intercepting and filtering inbound files, and running them in a virtual environment. File behavior is inspected simultaneously across multiple operating systems and versions. Files engaging in suspicious activity commonly associated with malware, such as modifying the registry, network connections, and new file creation are flagged and further analyzed.

Malicious files are prevented from entering your network.
A detailed report is provided for every malicious file. Information regarding newly detected malware is immediately sent to the ThreatCloud database to turn the new malware into a known and documented threat that can be prevented.



DETAILED REPORTS

A detailed report is generated for each file emulated and found to be malicious. The easy to understand report includes file details and information about any abnormal activity or 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.

THREATCLOUD™ ECOSYSTEM

Newly discovered threats are sent to the ThreatCloud intelligence database. Each newly discovered threat signature is distributed across the ThreatCloud ecosystem to protect other Check Point connected gateways. This enables connected gateways to block the new threat before it has a chance to become widespread. Constant collaboration makes ThreatCloud the most advanced and up-to-date threat Intelligence network available.

FLEXIBLE DEPLOYMENT OPTIONS

Check Point Threat Emulation works with existing networks. Multiple deployment options provide a cost-effective solution for virtually any size organization. Files can be sent to the ThreatCloud Emulation Service or to a Private Cloud Emulation Appliance.

THREATCLOUD EMULATION SERVICE

ThreatCloud Emulation Service is a cost-effective cloud-based solution that leverages the existing organizational infrastructure. Files can be sent for emulation from an existing R77 or newer security gateway, or from an agent for Exchange server. ThreatCloud Emulation Service allows centralized management and visibility of both threat and service usage information. This cloud-based service offers the flexibility to address the file emulation needs of any organization.

PRIVATE CLOUD EMULATION APPLIANCES[1]

Due to regulatory requirements, privacy concerns, or organization policy, some organizations may not want to utilize a cloud-based service. For those organizations, Check Point offers a private cloud appliance to handle their OS-level threat emulation needs.

SPECIFICATIONS

ThreatCloud Emulation Service Specifications	
Supported Files for Inspection	Adobe PDF, Microsoft Office, EXE, files in archives , Flash, and Java Applets
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

[1]Does not include CPU-Level Threat Emulation at this time

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