CHECK POINT ADVANCED THREAT PREVENTION

CHECK POINT ADVACED THREAT PREVENTION: ENABLING NEXT GENERATION ZERO-DAY PROTECTION

The Best Protection at Every Level

Threat Emulation

- 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
- Supports the broadest range of common file-types, including archive files, and web objects like Flash
- Leverages OS-level and CPU-level emulation for complete protection

Threat Extraction

- Zero second delivery of malware-free documents
- Preemptive protection against threats in email attachments and web documents
- Protects Microsoft Office and PDF documents
- Removes active content and other exploitable content from documents

INSIGHTS

Documents, executables, and other files still pose great risk to organizations today. According to the website Internet Live Stats, more than 2.3 million emails are sent every second, and about 67% of those are spam. In functions from human resources to accounts receivable and beyond, employees routinely open documents emailed from job applicants and customers. Marketing receives content from vendors in archive files and executables. And, many employees open Flash files downloaded from the web while researching markets, competitors, and new technologies. Most employees assume that once a file has reached them, it is safe to open. They often fail to consider the implications and possible risk of malware attack.

Modern malware has become much more complex. A good anti-virus is no longer sufficient for total protection. It has become extremely critical for organizations to implement protections against malware attacks hidden in executables and regular documents and web pages. A new and radical approach of threat prevention is needed to protect organizations against known malware, unknown malware and zero-day attacks, and deliver safe documents while maintaining the flow of business.

SOLUTION

Check Point Advanced Threat Prevention combines innovative technologies to deliver a radical approach to eliminate threats. Deep CPU-level and OS-level sandbox capabilities detect and block malware, while threat extraction reconstructs incoming documents to deliver zero malware documents in zero seconds.

Deep CPU-level sandboxing detects infections in data files at the exploit phase, while OS-level sandboxing accompanies it to detect attacks in both executable and data files. Together, they create a next generation technology that delivers the best possible catch rate for threats, virtually immune to attackers' evasion techniques. Threat extraction complements these technologies by delivering malware-free documents, and providing advanced protection against any zero-day attack. Next Generation Zero-Day Protection is the only solution that provides complete detection, inspection and protection.

April 15, 2015

ADVANCED THREAT PREVENTION: THREAT EMULATION
Discover Exploits and Stop Unknown Malware

Stopping attackers from accessing your system is critical to preventing malware infection. But end users unwittingly open malicious files and executables in your network, enabling attackers to gain full access to your system and exploit vulnerabilities. Check Point Threat Emulation employs the fastest and most accurate sandboxing tools available to pre-screen files and protects your organization from attackers before they enter your network. Files are quickly quarantined, inspected, and are run in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering your network, stopping infection from unknown malware, zero-day and targeted attacks.

To elevate defenses to the next level, Check Point uses CPU-level sandboxing to stop attacks before they have a chance to launch. Check Point's threat emulation engine monitors the instruction flow at the CPU-level and looks for exploits attempting to bypass OS security controls. By detecting exploit attempts during the pre-infection stage, Check Point Threat Emulation avoids evasion techniques and adds significantly greater protection with no additional latency.

ADVANCED THREAT PREVENTION: THREAT EXTRACTION
Zero Malware in Zero Seconds

Documents still pose one of the greatest threats to organizations. Check Point Advanced Threat Prevention employs Threat Extraction capabilities to eliminate malware contained in email attachments and web downloaded documents. It eliminates threats from Microsoft Office and PDF documents by removing exploitable content, such as macros, embedded objects and files, and external links. For the web, it delivers first pass protection against macros. Threat Extraction reconstructs documents with known safe elements, delivering malware-free documents with zero delay.

Advanced Threat Prevention
The Best Protection at Every Level

April 15, 2015