CHECK POINT THREAT EXTRACTION

CHECK POINT THREAT EXTRACTION

Zero Malware in Zero Seconds

Product Benefits

- Preemptive protection against known and unknown threats contained in emailed and web-downloaded documents
- Zero second delivery of malware-free documents
- Flexible protection addresses the unique needs of any organization

Product Features

- Protects Microsoft Office and PDF documents
- Removes active content and other exploitable content from documents
- Convert reconstructed files to PDF format for best security, or keep in original format depending upon policy
- Reconstructs files in approximately one second
- Configurable protection options
- Easy access to original files as necessary

[1] Check Point Security Report 2014

INSIGHTS

Documents still pose one of the greatest risks to organizations today. Last year, 84% of companies downloaded a malicious document.1 However, in business functions from human resources to purchasing and beyond, employees must routinely open documents from job applicants, customers, and vendors as part of their job responsibilities. While researching markets, competitors, and new technologies, employees regularly open documents downloaded from the web. Most employees open these documents without considering the implications, and risk exposing their companies to threats, Trojans, and other malware embedded inside them.

Organizations need to implement protections against the risks posed by malicious content in documents. The traditional approach of protecting against infected documents by looking for malware and blocking it does not provide complete protection. Antivirus is fast, but it can only catch known or “old” malware, and does not prevent zero-day malware infections. Zero-day solutions identify “new”, unknown malware and Advanced Persistent Threats (APTs). However, this approach takes time and risks potential exposure to network infection before detection and blocking occurs. A new approach is needed to address these threats and eliminate all malware, before it ever has the opportunity to reach employees.

SOLUTION

Check Point Threat Extraction provides a new approach to eliminate malware contained in emailed documents and web downloaded documents. Providing complete protection from threats by removing potentially exploitable content, Threat Extraction delivers malware-free documents to your employees with zero delay.

Threat Extraction eliminates threats from Microsoft Office and PDF documents by removing exploitable content, such as macros, embedded objects and files, and external links. Employees receive documents reconstructed with known safe elements.

With Threat Extraction, organizations can provide documents with zero malware in zero seconds.

MALWARE-FREE DOCUMENTS

Documents used on a daily basis can contain risky content, including macros or embedded links that can be exploited to infect your computers and networks. With Check Point Threat Extraction, threats are eliminated by removing this content and reconstructing it using known safe elements, delivering a malware-free document to its intended destination.

July 2, 2015

ZERO SECOND DELIVERY

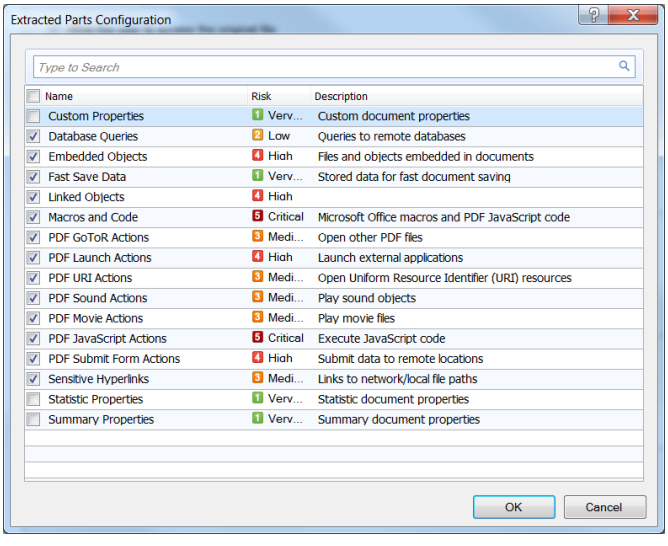
Unlike detection technologies that require time to search for and identify threats before blocking them, Threat Extraction preemptively eliminates risk, ensuring zero second delivery of safe documents.

PROTECTS MOST COMMON FILE TYPES

Check Point Threat Extraction supports the most common document types used in organizations today, including Microsoft Office Word, Excel, Power Point, and Adobe PDF documents. Administrators can select which of these document types will undergo Threat Extraction when entering the network via email or web download.

FLEXIBLE PROTECTION OPTIONS

Threat Extraction provides flexibility for organizations to select the document protection options that best suit their operational needs. For the best protection, we recommend reconstructing and converting documents into a PDF format. Alternatively, organizations can choose to maintain the original document format, and remove content that may pose a threat. This option allows administrators to determine the types of content to remove, from high risk macros to embedded files and external links.



EASY TO DEPLOY

Installed as an additional software blade on the gateway, Threat Extraction integrates in Mail Transfer Agent-Mode to the email network. Apply Threat Extraction across the organization, or implement only for specific individuals, domains, or departments. Administrators can configure included users and groups based upon their needs, easily facilitating gradual deployment to the organization.

SYNCHRONIZED WITH THREAT EMULATION

Threat Extraction and Threat Emulation work together to bring you even better protection. Threat Extraction delivers documents with zero malware in zero seconds. Threat Emulation analyzes the original document in an isolated sandbox, identifying unknown threats. It executes this analysis and provides attack visibility to the organization.

Configure Threat Extraction in one of two ways. Quickly provide a reconstructed document to the user, or configure Threat Extraction to await response from Threat Emulation before determining whether or not to reconstruct the document. In addition, access to original files is only permitted when the document is determined to be non-malicious by Threat Emulation.

BUNDLE FOR THE BEST PROTECTION

With the Next Generation Threat Extraction (NGTX) bundle, organizations are able to leverage the protections delivered by Threat Extraction, and gain the added protections provided by IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, Anti-Spam, and Threat Emulation. This comprehensive protection keeps users from downloading malicious files, accessing risky websites, and it stops bot communications before damage occurs. Organizations already leveraging the Next Generation Threat Prevention (NGTP) appliance can add this capability via the TX bundle.

SPECIFICATIONS

Feature	Description
Supported File Types	Microsoft Office 2003-2013, Adobe PDF
Document Language Support	Latin languages: full support Non-Latin languages – partial support
Deployment Options	• MTA – gateway receives all incoming email, and forwards it to the next hop after inspection • WebAPI - sends files to the machine for reconstruction • Web Browser Extension - supports reconstruction for downloaded files
Performance	~1% of throughput decrease for 8000 people 1 GB of memory required
Version and OS	From R77.30 using SecurePlatform or GAiA

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

July 2, 2015