CHECK POINT SANDBLAST NETWORK

NETWORK THREAT PREVENTION

CHECK POINT SANDBLAST NETWORK

Detects and blocks previously undiscovered malware, taking network security to the next level

Product Benefits

- Best catch rate of unknown malware, including today's most sophisticated evasive attacks, ransomware, spyware and file-less malware.
- Identifies and blocks URL-based and attachment-based threats in their infancy
- Rapid reconstruction of files and delivery of safe content
- Reduces risk of expensive breaches or downtime
- Integrated protection maximizes operational value and minimizes TCO

Product Features

- Deep malware inspection at the CPU level, where exploits cannot hide
- Inspects broad range of documents and common file-types, as well as URLs linked to files within emails
- Works with existing infrastructure, no need to install new equipment
- Removes active content and other exploitable content from documents
- Clean and reconstruct files to PDF for best security, or keep original format
- Integrated threat prevention and security management for complete security and threat visibility
- Automatic sharing of new attack information with ThreatCloud^{TM}

INSIGHTS

The cyber war rages on, and hackers constantly modify their strategies and techniques to remain elusive and achieve their goals. Today's hacker ecosystem makes it easy for cybercriminals to share exploit code, newly identified vulnerabilities, and even talent with their co-conspirators. Even novice hackers can leverage these resources to identify vulnerabilities and susceptible organizations, and easily create new zero-day or unknown attacks using custom variants of already existing malware.

Anti-virus, Next Generation Firewalls, and other core security solutions focus only on known threats, those with existing signatures or profiles. With an ever-growing number of new forms of malware hitting every hour, how do you protect against what you do not know? Traditional sandbox solutions identify "new" and unknown malware, but take time, risking potential exposure to network infection before detection and blocking occurs. Unfortunately, they are also vulnerable to evasion techniques capable of bypassing traditional sandbox detection technology.

SOLUTION

Check Point SandBlast Zero-Day Protection employs Threat Emulation and Threat Extraction capabilities to elevate network security to the next level with evasion resistant malware detection, and comprehensive protection from the most dangerous attacks such as ransomware, spyware, Trojans and file-less malware – and at the same time ensures quick delivery of safe content to your users.

Threat Emulation performs deep CPU-level inspection, stopping even the most dangerous attacks before malware has an opportunity to deploy and evade detection. SandBlast Threat Emulation uses OS-level inspection to examine a broad range of file types, including executables and data files. With its unique inspection capabilities, SandBlast Threat Emulation delivers the best possible catch rate for threats, and is virtually immune to attackers' evasion techniques.

SandBlast Threat Extraction complements this solution by promptly delivering safe content, or clean and reconstructed versions of potentially malicious files, maintaining uninterrupted business flow. By eliminating unacceptable delays created by traditional sandboxes, Threat Extraction makes real-world deployment in prevent mode possible, not just issuing alerts, but blocking malicious content from reaching users at all.

Check Point SandBlast Zero-Day Protection provides complete detection, inspection, and protection against the most dangerous zero-day and targeted attacks at the network.

SANDBLAST NETWORK - SPECIFICATIONS

Threat Emulation	
Emulation environments	• Windows XP • Windows 7 • Windows 8.1 • Windows 10
Detection Engines	SandBlast implements a multi-layer defense architecture that filters possible threats by using sophisticated analysis, to optimize efficiency and ensure rapid response to any type of attack (incl. worms, ransomware, file-less malware, spyware, and more) without compromising network performance or security policies. SandBlast Zero Day Threat Detection integrates static analysis, dynamic analysis, AI and behavioral based Machine Learning algorithms implemented in over 40 detection engines to ensure maximum detection and catch rates. Additionally, SandBlast utilized CPU level detection engines in order to detect exploit attempts during the pre-infection stage and stop the attacks before they have a chance to evade detection by the sandbox
File types	Over 70 file types, including: Microsoft Office documents and templates, EXE, DLL, Archives (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts and more.
Archive files	• Scan files contained in archives • Open password protected archives

Threat Extraction	
File types	• Microsoft Word • Microsoft PowerPoint • Microsoft Excel • Adobe PDF • Image files
Extraction modes	• Clean and keep original file type • Convert to PDF
Extractable components	Over 15 extractable component types (configurable) including: • Macros and Code • Embedded Objects • Linked Objects • PDF JavaScript Actions • PDF Launch Actions
Self-catered access to original files	Yes Access to original depend on Threat Emulation benign verdict (configurable)

Additional Protections (included with NGTX package)	
IPS	Protects from network-based intrusions and exploitations
Anti-Virus	Protects from malware in files downloads and mail attachments (signature-based)
Anti-Bot	Identify and contain infections by blocking C&C traffic
URL Filtering & App Control	Optimized web security through full integration in the gateway to prevent bypass through external proxies and control of social networks, applications and application features.
General	
SSL Inspection	Included
Identity Awareness	Included
Management	Check Point SmartCenter, R77 and above
Supported protocols	
Threat Emulation	HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, FTP
Threat Extraction	SMTP, SMTPS – MTA deployment