INFONALIGY
Security Today for Tomorrow's Threats

MANAGED SECURITY SERVICES

SANDBLAST NETWORK

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
- 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
- Convert reconstructed 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™

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 106 new forms of malware hitting every hour, how do you protect against what you don't know?[1] 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 – 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.

EVASION RESISTANT DETECTION

Unlike other solutions, Check Point SandBlast Zero-Day Protection uses a unique technology that does inspection at the CPU-level 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. The Check Point SandBlast Threat Emulation engine monitors CPU-based instruction flow for exploits attempting to bypass operating system and hardware security controls.

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

IDENTIFY MORE MALWARE

Check Point SandBlast Zero-Day Protection conducts further investigation with OS-level threat emulation by intercepting and filtering inbound files and inspecting URLs linked to files within emails by 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.

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 AND EASY TO DEPLOY

Check Point SandBlast Threat Emulation supports multiple deployment options, providing a cost-effective solution for virtually any size organization. Files can be sent from existing gateways to either the SandBlast cloud-based service or to an on-premise appliance available with a range of throughput capacities.

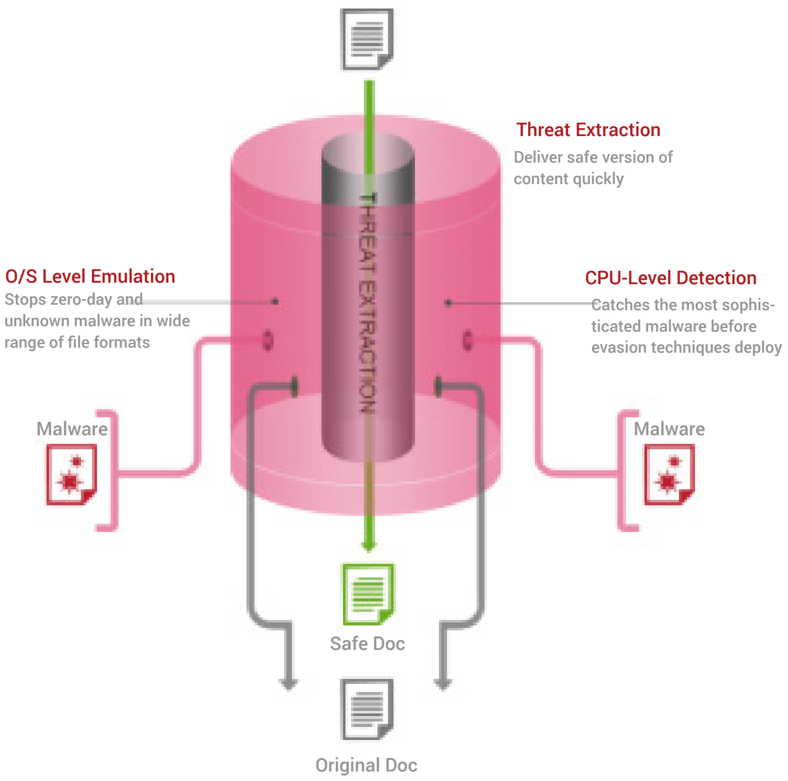
Installed as an additional software blade on the gateway, Check Point SandBlast Threat Extraction can be applied across the entire organization, or implemented only for specific individuals, domains, or departments. Administrators can configure included users and groups based upon their needs, easily facilitating gradual deployment to the organization.

PROACTIVE PREVENTION WITH PROMPT DELIVERY OF SAFE CONTENT

When it comes to threat protection, it doesn't have to be a trade-off between speed, coverage and accuracy. Unlike other solutions, Check Point SandBlast Zero-Day Protection can be deployed in detect and prevent mode, while still maintaining uninterrupted business flow.

Our Threat Extraction component within Check Point SandBlast eliminates threats by removing risky content such as macros or embedded links and then reconstructs the document using only known safe elements.

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


Threat Extraction
Deliver safe version of content quickly
THREAT EXTRACTION
O/S Level Emulation
Stops zero-day and unknown malware in wide range of file formats
CPU-Level Detection
Catches the most sophisticated malware before evasion techniques deploy
Malware
Malware
Safe Doc
Original Doc

PROTECTS MOST COMMON FILE TYPES

Check Point SandBlast Zero-Day Protection secures a wide range of the most common document types used in organizations today, from Microsoft Office Word, Excel, Power Point, and Adobe PDFs to Archive files.

COMPLETE, INTEGRATED SOLUTION

Check Point SandBlast Zero-Day Protection is fully integrated with Check Point Security Management, allowing creation of security policies and profiles, and configuration from a unified platform. Check Point SmartEvent provides visibility and reporting across your organization's threat horizon, enabling rapid investigation and resolution of security events.

BUNDLED FOR THE BEST PROTECTION

With the Next Generation Threat Extraction (NGTX) bundle, organizations are able to leverage the protections delivered by Check Point SandBlast Zero-Day Protection, and gain the added protections provided by IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, and Anti-Spam on any Check Point gateway. This comprehensive protection keeps users from downloading malicious files, accessing risky websites, and stops bot communications before damage occurs.

SANDBLAST FAMILY OF SOLUTIONS

The SandBlast Zero-Day Protection solution suite also includes additional products that provide advanced threat protection for web browsers, endpoints and cloud applications.

For more details about how Infonaligy products, technologies, consulting, deployment and security services can help you implement a cyber security strategy, please contact us at **800-985-1365** or email **info@infonaligy.com**

SANDBLAST – NETWORK SECURITY SPECIFICATIONS

Threat Emulation

Feature	Description
Supported File Types	Over 40 file types, including: Adobe PDF, Microsoft Office, EXE, files in archives, Flash, Java Applets, and PIF
Supported Emulation Environments	Microsoft Windows XP, 7, 8 Microsoft Office; Adobe Reader
Operating Environment	SecurePlatform or GAiA

Threat Extraction

Feature	Description
Supported File Types	Microsoft Office 2003-2013, Adobe PDF
Performance	~1% of throughput decrease for 8000 people 1 GB of memory required
Version and OS	From R77.30 using SecurePlatform or GAiA

Sandblast - Network Security: Deployment Options

Distributed deployment – Check Point security gateways, deployed across the network and acting as sensors, send files and objects to be inspected by one or more SandBlast appliances.

SandBlast Service – Files can be sent to the cloud-based service for emulation and analysis from an existing security gateway or from an agent for Exchange server. No infrastructure changes are required at the organization. The cloud-based service enables centralized management and visibility of both threat and service usage information.

Inline or span-port deployment – connect the SandBlast appliance inline – files and objects are examined inline by the SandBlast appliance

MTA – Acting as a Mail Transfer Agent, the Check Point security gateway receives incoming mails, and scans or cleans their content before forwarding it to the next hop mail server – MTA supports both Threat Emulation and Threat Extraction

Threat Prevention API – Open API allows sending files to the SandBlast appliance for inspection by Threat Emulation and Threat Extraction