Check Point SOFTWARE TECHNOLOGIES LTD.
SECURE YOUR EVERYTHING™

CHECK POINT SANDBLAST APPLIANCES

CHECK POINT SANDBLAST APPLIANCES

Stop new and unknown threats

Product Benefits

- Prevent new and unknown attacks in documents and executable files
- Makes it virtually impossible for hackers to evade detection
- Reduces costs by leveraging existing security infrastructure
- Maximize protection through unified management, monitoring, and reporting
- Increase security with automatic sharing of new attack information with ThreatCloud™

Product Features

- Identify new malware hidden in over 40 files types, including: Adobe PDF, Microsoft Office, Java, Flash, executables, and archives
- Protect against attacks targeting multiple Windows OS environments
- The range of available appliances covers any performance need
- Threat Extraction removes exploitable content to deliver clean files without delay
- Unique CPU-Level technology catches malware before it has an opportunity to deploy and evade detection

INSIGHTS

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments.

These threats include new exploits, or even variants of known exploits unleashed almost daily with no existing signatures and therefore no standard solutions to detect those variants. New and undiscovered threats require new solutions that go beyond signatures of known threats.

SOLUTION

Check Point SandBlast Zero-Day Protection, with evasion-resistant malware detection, provides comprehensive protection from even the most dangerous attacks while ensuring quick delivery of safe content to your users. At the core of our solution are two unique capabilities – Threat Emulation and Threat Extraction that take threat defense to the next level.

As part of the Check Point SandBlast solution, the Threat Emulation engine picks up malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

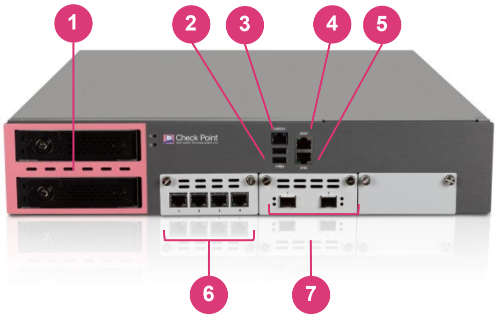
In addition, the SandBlast Threat Extraction capability immediately provides a safe version of potentially malicious content to users. Exploitable content, including active content and various forms of embedded objects, are extracted out of the reconstructed file to eliminate potential threats. Access to the original suspicious version is blocked, until it can be fully analyzed by SandBlast Zero-Day Protection. Users have immediate access to content, and can be confident they are protected from the most advanced malware and zero-day threats.

SANDBLAST APPLIANCES

We offer a wide range of SandBlast Appliances. These are perfect for customers who have regulatory or privacy concerns preventing them from using the SandBlast Threat Emulation cloud-based service.

TE1000X SandBlast Appliance Example

1. 2x 2 TB hard disks
2. 2x USB ports
3. Console port
4. 10/100/1000Base-T Management port
5. 10/100/1000Base-T Sync port
6. 4x 10/100/1000Base-T ports
7. 2x 10GBase-F SFP+ ports



DEPLOYMENT OPTIONS

Emulate threats in one of two deployment options:

1. Private cloud: Check Point security gateways send files to a SandBlast appliance for emulation
2. Inline: This is a stand-alone option that deploys a SandBlast Appliance inline as MTA or as an ICAP server or on a SPAN port, utilizing all NGTX Software Blades including IPS, Antivirus, Anti-Bot, Threat Emulation, Threat Extraction, URL Filtering and Application Control.

COMPREHENSIVE THREAT PROTECTION

SandBlast Appliances protect you from both known and unknown threats utilizing IPS, Antivirus, Anti-Bot, Threat Emulation (sandboxing), and Threat Extraction technologies.

SANDBLAST ZERO-DAY PROTECTION

The SandBlast Threat Emulation technology employs the fastest and most accurate sandboxing engine available to pre-screen files, protecting your organization from attackers before they enter your network.

KNOWN THREAT DETECTION

The Antivirus Software Blade uses real-time virus signatures from ThreatCloud™ to detect and block known malware at the gateway before users are affected. The Anti-Bot Software Blade detects bot-infected machines, preventing damages by blocking bot Command & Control communications.

EVASION RESISTANT DETECTION

Traditional sandbox solutions detect malware behavior at the OS level – after the exploitation has occurred and the hacker code is running. They are therefore susceptible to evasion.

SandBlast Threat Emulation capability utilizes a unique CPU-level inspection engine which monitors the instruction flow at the CPU-level to detect exploits attempting to bypass OS security controls, effectively stopping attacks before they have a chance to launch.

PROACTIVE PREVENTION WITH PROMPT DELIVERY OF SAFE CONTENT

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

SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

Configure Threat Extraction in one of two ways: Quickly provide a reconstructed document to the user, or await response from SandBlast Threat Emulation before determining whether or not to reconstruct the document.

INSPECT ENCRYPTED COMMUNICATIONS

Files delivered into the organization over SSL and TLS represent a secure attack vector that bypasses many industry standard implementations. Check Point Threat Prevention looks inside these protected SSL and TLS tunnels to extract and launch files to discover hidden threats.

THREAT EMULATION DETAILED REPORT

Every file emulation generates a detailed report. Simple to understand, the report includes detailed forensic information about any malicious attempts originated by running this file. The report provides actual screenshots of the simulated environments while running the file.

THREATCLOUD ECOSYSTEM

For each new threat discovered by Threat Emulation, a new signature is created and sent to Check Point ThreatCloud, where it is distributed to other Check Point connected gateways. Threat Emulation converts newly identified unknown attacks into known signatures, making it possible to block these threats before they have a chance to become widespread. This constant collaboration makes the ThreatCloud ecosystem the most advanced and up-to-date threat network available.

TECHNICAL SPECIFICATIONS

	TE100X	TE250X	TE1000X	TE2000X	TE2000X HPP
Performance					
Unique files per hour	450	1,000	2,800	4,200	5,000
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps	
Virtual machines	4	8	28	40	56
Hardware					
Storage	1x 1TB HDD		Redundant dual hot swappable 2x 2TB HDD, RAID1		
LOM	Not supported				
Slide Rails	Optional	Included			
Network					
10/100/1000Base-T RJ45 (base/max)	5/13	9/17	6/14	6/14	6/14
10GBase-F SFP+	NA	NA	2/6	4/8	4/8
Transceivers	-	-	Optional	Optional	Included
Expansion slot	1	1	1	1	1
Bypass (Fail-Open)	Optional 4x 1GbE copper or 2x 10GbE				
Dimensions					
Enclosure	1U	1U	2U		
Metric (W x D x H)	435 x 448 x 44 mm	438 x 621 x 44 mm	438 x 561 x 88 mm		
Standard (W x D x H)	17.13 x 17.64 x 1.63 in.	17.25 x 24.45 x 1.73 in.	17.24 x 22.1 x 3.46 in		
Weight	7.7 kg (16.9 lbs.)	9.8 kg (21.6 lbs.)	17.05 kg (37.6 lbs.)		
Environment					
Operating	32º to 104ºF / 0º to 40ºC, (5 - 95%, non-condensing)				
Storage	-14° to 158°F / -10° to 70°, (20 - 90% non-condensing)				
Power					
Dual, hot swappable	-	Optional	Included		
AC input	100-240V				
Frequency	47-63 Hz				
Power supply rating	250W	400W	400W		
Max power consumption	50.4W	104W	225.6W		
Max thermal output	172.2 BTU/h	355.7 BTU/h	771.5 BTU/h		
Certifications					
Safety	CB, UL, Multiple Listing, LVD, TUV				
Emissions	FCC, CE, VCCI, RCM				
Environment	RoHS				

Performance numbers are based on:

- **File blend:** A blend of unique files representing real-world mail and web traffic
- **Emulation environment:** Check Point recommended images for emulation
- **Topology:** distributed topology – inline security gateway sending files for emulation to a SandBlast appliance

Performance numbers are based on unique files scanned. Unique files typically represent 20 to 30% of the total number of files. Most files are retransmissions of files seen before. These known files are processed based on the file hash without impacting the appliance performance.

SANDBLAST NETWORK SPECIFICATIONS

THREAT EMULATION	
Emulation Environments	PC: Windows XP or later Mac: MacOS version 10.14.6 (Mojave) or later
File Types	Over 70 file types emulated, including: Microsoft Office documents and templates, EXE, DLL, Archives (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts and more.
Archive Files	Archived (compressed) files Password protected archives

THREAT EXTRACTION	
File Types	Web downloads and email attachments in the following formats: • 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

ADDITIONAL PROTECTIONS (included in SandBlast Network licenses)	
SSL Inspection	Included
Identity Awareness	Identity-based policies for users, groups and machines supported through integration with Microsoft Active Directory and Cisco Identity Services Engine
Management	Single-click policy setup – Supported in R80.40 and above Threat Extraction for web downloads – R80.30 and above
Threat Emulation (protocols)	HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP
Threat Extraction (protocols)	Web downloads: HTTP, HTTPS, ICAP Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment

ORDERING SANDBLAST APPLIANCES

BASE CONFIGURATION [1]	SKU
SandBlast TE100X Appliance, delivers SandBlast zero-day service to gateways covered by NGTX license (includes Microsoft Windows and Office license for 4 Virtual Machines)	CPAP-SBTE100X-4VM
SandBlast TE250X Appliance, delivers SandBlast zero-day service to gateways covered by NGTX license (includes Microsoft Windows and Office license for 8 Virtual Machines)	CPAP-SBTE250X-8VM
SandBlast TE1000X Appliance, delivers SandBlast zero-day service to gateways covered by NGTX license (includes Microsoft Windows and Office license for 28 Virtual Machines)	CPAP-SBTE1000X-28VM
SandBlast TE2000X Appliance, delivers SandBlast zero-day service to gateways covered by NGTX license (includes Microsoft Windows and Office license for 40 Virtual Machines)	CPAP-SBTE2000X-40VM
SandBlast TE2000X HPP Appliance, delivers SandBlast zero-day service to gateways covered by NGTX license (includes Microsoft Windows and Office license for 56 Virtual Machines plus 4 x CPAC-TR-10SR transceivers)	CPAP-SBTE2000X-56VM-HPP
SOFTWARE BLADE PACKAGE [2]	**SKU**
NGTX software renewal package for TE100X for 1 year, required to deploy a SandBlast Appliance inline	CPSB-NGTX-SBTE100X-1Y
NGTX software renewal package for TE250X for 1 year, required to deploy a SandBlast Appliance inline	CPSB-NGTX-SBTE250X-1Y
NGTX software renewal package for TE100X for 1 year, required to deploy a SandBlast Appliance inline	CPSB-NGTX-SBTE1000X-1Y
NGTX software renewal package for TE2000X for 1 year, required to deploy a SandBlast Appliance inline	CPSB-NGTX-SBTE2000X-40VM-1Y
NGTX software renewal package for TE2000X HPP for 1 year, required to deploy a SandBlast Appliance inline	CPSB-NGTX-SBTE2000X-56VM-1Y

[1] The SandBlast Appliance must be covered by an NGTX software package when deployed inline, as MTA or as an ICAP server

[2] SKUs for 2 and 3 years are available, see the online Product Catalog

Accessories

INTERFACE CARDS AND TRANSCEIVERS	SKU
8 Port 10/100/1000 Base-T RJ45 interface card	CPAC-8-1C-TE
4 Port 10GBase-F SFP+ interface card for TE1000X and TE2000X; requires additional transceivers	CPAC-4-10F-TE
SFP+ transceiver module for 10G fiber ports - long range (10GBase-LR)	CPAC-TR-10LR
SFP+ transceiver module for 10G fiber ports - short range (10GBase-SR)	CPAC-TR-10SR
4 Port 1GE copper Bypass (Fail-Open) network interface card (10/100/1000 Base-T)	CPAC-4-1C-BP
2 Port 10GE short-range Fiber Bypass (Fail-Open) network interface card (10GBase SR)	CPAC-2-10FSR-BP

SPARES AND MISCELLANEOUS	SKU
AC Power Supply for TE250X	CPAC-PSU-TE250X
Replacement parts kit (including 1 Hard Disk Drive and one Power Supply) for TE1000X and TE2000X	CPAC-SPARES-TE1000X/2000X
Extended slide rail kit for TE100X (24” to 36”)	CPAC-RAILS-EXT-5000