SANDBLAST - THREAT EMULATION APPLIANCES

STOP 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

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. New and undiscovered threats require new solutions that go beyond signatures of known threats.

SANDBLAST ZERO-DAY PROTECTION

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 (sandboxing) and Threat Extraction (Content Disarm & Reconstruction) that take threat defense to the next level.

Evasion-resistant Sandbox

As part of the Check Point SandBlast solution, the Threat Emulation engine detects 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.

Content Disarm & Reconstruction (CDR)

In addition, the SandBlast Threat Extraction (CDR) 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.

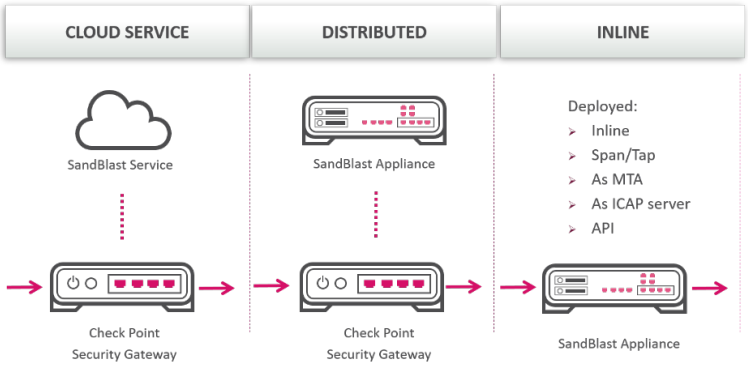
SANDBLAST APPLIANCES

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.

Deployment Options

Emulate threats in one of two deployment options:

1. Private cloud: Check Point security gateways send files to an on-premises 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 threat prevention technologies, including IPS, Antivirus, Anti-Bot, Threat Emulation, Threat Extraction, URL Filtering and Application Control.



SandBlast Deployment Options

Complete Threat Pevention Solution

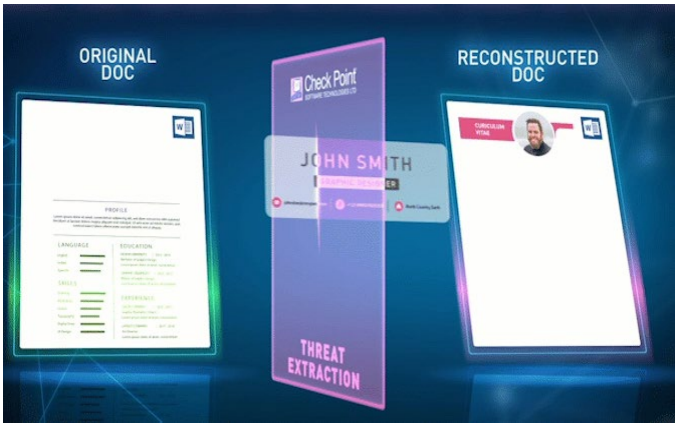
SandBlast Appliances protect you from both known and unknown threats utilizing IPS, Antivirus, Anti-Bot, Threat Emulation (sandboxing), and Threat Extraction (CDR) technologies.

KNOWN THREAT DETECTION

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

UNKNOWN THREAT 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. 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.



SandBlast Content Disarm & Reconstruction (CDR)

PROMPTLY DELIVER 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 REPORTS

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.

PART OF THE 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 products. 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.

SANDBLAST SPECIFICATIONS

Threat Emulation

Emulation Environments

- PC: Windows XP 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

Protocols

- HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP

Threat Extraction

Extraction Modes

- Clean and keep original file type
- Convert to PDF

Threat Extraction (continued)

File Types

Web downloads and email attachments in these formats:

- Microsoft Word
- Microsoft PowerPoint
- Microsoft Excel
- Adobe PDF
- Image files

Extracted Content

Over 15 extractable component types including:

- Macros and Code
- Embedded Objects
- Linked Objects
- PDF JavaScript Actions
- PDF Launch Actions

Protocols

- Web downloads: HTTP, HTTPS, ICAP
- Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment

SANDBLAST APPLIANCE SPECIFICATIONS

	TE250XN	TE2000XN	
			
		TE2000XN-28VM	TE2000XN-56VM
Unique files per hour	1,300	5,000	8,000
Virtual machines	8	28	56
Throughput	1 Gbps	2.6 Gbps	5.2 Gbps
CPU cores	1x 16 physical, 32 virtual	2x 12 physical, 24 virtual	
Storage	1x 960GB SSD	1x 2TB SSD	
Memory	16 GB	128 GB	
Power supplies	2x AC, DC option	2x AC, DC option	
LOM	Optional	Included	
Slide Rails	Included	Included	
Network			
1GbE Copper RJ45	10x 10/100/1000 RJ45 on-board	2x 10/100/1000 RJ45 on-board	
Expansion Slots	NA	-	
100GbE QSFP28	-	2	
100G QSFP28 port configurations			
10GbE SFP+	-	2x with Included 10GbE SR transceivers	
25GbE SFP28	-	2x with optional 25GbE transceivers	
40GbE QSFP+	-	2x with optional 40GbE transceivers	
Dimensions			
Enclosure	1U	1U	
Metric (W x D x H)	438 x 580 x 44mm	442 x 610 x 44 mm	
Standard (W x D x H)	17.2 x 22.83 x 1.73 in.	17.4 x 24 x 1.73 in	
Weight		13 kg (28.7 lbs.)	
Environment			
Operating	32º to 104ºF / 0º to 40ºC, (5 - 95%, non-condensing)		
Storage	-4° to 158°F / -20° to 70°C, (5 - 95% non-condensing)		
Power			
Dual, hot swappable	Included	Included	
AC input	100-240V, 47-63 Hz	100-240V, 47-63 Hz	
Power supply rating	500W	850W	
Power consumption avg/max	144W/270W	188W/438W	
Max thermal output	921 BTU/hr.	1494 BTU/hr.	
Certifications			
Safety	UL, CB, CE, TUV GS		
Emissions	FCC, CE, VCCI, RCM/C-Tick		
Environment	RoHS, WEEE		

Performance numbers are based on unique files scanned which 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. Performance based on:
File blend: A blend of unique files representing real-world mail and web traffic
Emulation environment: Check Point recommended images for emulation
Distributed topology; an inline security gateway sending files for emulation to a SandBlast appliance

ORDERING SANDBLAST APPLIANCES

Ordering TE2000XN

TE2000XN BASE CONFIGURATION [1]	SKU
SandBlast TE2000XN-28VM Appliance, delivers SandBlast zero-day service to gateways covered by SNBT license (includes Microsoft Windows and Office license for 28 Virtual Machines)	CPAP-SBTE2000XN-28VM
SandBlast TE2000XN-56VM Appliance, delivers SandBlast zero-day service to gateways covered by SNBT license (includes Microsoft Windows and Office license for 56 Virtual Machines)	CPAP-SBTE2000XN-56VM
TE2000XN SOFTWARE PACKAGES [2]	
SNBT software renewal package for TE2000XN-28VM for 1 year, required to deploy a SandBlast Appliance inline	CPSB-SNBT-SBTE2000XN-28VM-1Y
SNBT software renewal package for TE2000XN-56VM for 1 year, required to deploy a SandBlast Appliance inline	CPSB-SNBT-SBTE2000XN-56VM-1Y

TE2000XN NETWORK CARDS AND TRANSCEIVERS	
100G SWDM4, LC connector, 75m/OM3 fiber	CPAC-TR-100SWDM4
100G CWDM4, LC connector, 2Km/ single mode fiber	CPAC-TR-100CWDM4
QSFP28 transceiver module for 100G fiber ports - short range (100GBase-SR4)	CPAC-TR-100SR
QSFP28 transceiver module for 100G fiber ports - long range (100GBase-LR4)	CPAC-TR-100LR
QSFP+ transceiver module for 40G fiber ports - short range (40GBase-SR)	CPAC-TR-40SR-QSFP-300m
QSFP+ transceiver module for 40G fiber ports - long range (40GBase-LR)	CPAC-TR-40LR-QSFP-10Km
Bi-directional QSFP transceiver for 40G fiber Ports - short range (40GBase-SR-BD)	CPAC-TR-40SR-QSFP-BiDi
SFP28 transceiver module for 25G fiber ports with QSFP28 adaptor - short range (25GBase-SR)	CPAC-TR-25SR-ADP
SFP28 transceiver module for 25G fiber ports with QSFP28 adaptor - long range (25GBase-LR)	CPAC-TR-25LR-ADP
SFP+ transceiver module for 10G fiber ports with QSFP28 adaptor - short range (10GBase-SR)	CPAC-TR-10SR-ADP
SFP+ transceiver module for 10G fiber ports with QSFP28 adaptor - short range (10GBase-LR)	CPAC-TR-10LR-ADP
SFP+ transceiver module for 10G fiber ports with QSFP28 adaptor – extended reach (10GBase-ER)	CPAC-TR-10ER-ADP
SFP+ transceiver 10GBASE-T RJ45 (Copper) with QSFP28 adaptor	CPAC-TR-10T-ADP
TE2000XN SPARES AND MISCELLANEOUS	**SKU**
AC power supply for 16600HS, 26000, 28000, 28600HS Security Gateways	CPAC-PSU-AC-26000/28000
Dual DC power supplies for 16000, 26000, 28000 Security Gateways	CPAC-PSU-DC-Dual-16000/26000/28000
DC power supply for 16000 and 26000 Security Gateways	CPAC-PSU-DC-16000/26000/28000
Replacement 16GB RAM memory module for 16600, 28600 Security Gateways	CPAC-RAM16GB-16/28K-HS
Replacement Lights-Out Management Module	CPAC-NLOM-C
Slide rails for 16600 Security Gateways (22" - 32")	CPAC-RAIL-L
Extended slide rails for 16600 Security Gateways (24" - 36")	CPAC-RAIL-EXT-L

Ordering TE250XN

TE250XN SOFTWARE BASE CONFIGURATION [2]	SKU
SandBlast TE250XN Appliance, delivers SandBlast zero-day service to gateways covered by SNBT license (includes Microsoft Windows and Office license for 8 Virtual Machines)	CPAP-SBTE250XN-8VM

[1] The SandBlast Appliance must be covered by an SNBT 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

ORDERING SANDBLAST APPLIANCES (Continued)

TE250XN SPARES AND MISCELLANEOUS	SKU
Additional/Replacement AC Power Supply for TE250XN appliances	CPAC-PSU-AC-7000
Additional/Replacement DC Power Supply for TE250XN appliances	CPAC-PSU-DC-7000
Lights Out Management module	CPAC-NLOM-C
Slide rails for TE250XN Security Appliances (22" - 32")	CPAC-RAILS-6000/7000
Telescopic slide rails for 6000 and TE250XN Security Appliances (24" - 36")	CPAC-RAILS-EXT-6000/7000