SandBlast Network

Protection Against Zero-Day Threats

Product Benefits

- Best zero-day catch rate
- Protects users against sophisticated phishing emails
- Instantly cleans web downloads from risky elements
- Doesn't compromise productivity
- Single click setup
- Unified network security management

Product Features

- Threat emulation with AI-based analysis of unknown attacks
- Threat extraction for pre-emptive document sanitization across email and web
- Up-to-the-moment threat intelligence for blocking attacks (ThreatCloud)
- Evasion-resistant CPU-level emulation
- State-of-the-art management with actionable forensics, compliance stance visibility, logging and reporting

Can you Defend Against Zero-Day Threats?

Every day, 8,300[1] new, previously undiscovered cyber attacks emerge, including zero-day malware, zero-day phishing and social engineering attacks. With no associated file signatures, anti-virus, firewalls and other core security solutions cannot identify them as malicious and block them from entering the network. In fact, even the best AV solutions detect only half of malware strains in the wild. With no existing indicators of compromise (IOCs), how do you protect against what you do not know?

Common Network Security Approaches Have Limitations

To protect against zero-day threats, organizations use several approaches. These include:

- Conventional sandboxing solutions, which are susceptible to malware evasion techniques, and by default, are configured to let malware enter the network before analysis is complete.
- Endpoint security, which has its advantages but cannot protect datacenters running dedicated servers and enterprise IoT, such as cameras, elevators and HVAC systems—for which the network perimeter often serves as the only line of defense.

[1] Source: Check Point ThreatCloud: 8,300 "Zero day"/Unknown files per day

- A detection-first strategy that mainly relies on incident response, which is expensive, and often kicks in after the damage is already done.

With such critical limitations, how can you protect your network from zero-day threats?

Check Point SandBlast Network—Number One in Zero-Day Protection

Check Point SandBlast Network provides the world's best[2] zero-day protection, through a combination of evasion-resistant threat emulation, revolutionary AI engines and threat extraction that pre-emptively sanitizes email and web downloads.

Empowering organizations to take a prevention-first strategy to cyberattacks, SandBlast Network defends against the most devastating attacks, including unknown ransomware, Trojans, phishing and social engineering.

SandBlast Network deploys with your current infrastructure, offering fully automated policy configuration, without compromising business productivity and agility.

Best Zero-Day Catch Rate

To achieve the world's best malware catch rate at record speed, SandBlast Network employs numerous innovative, proprietary technologies. These include pre-emptive user protections, a vast network of up-to-the-moment threat intelligence and revolutionary AI and non-AI engines.

SandBlast Network Threat Emulation Report

[2] 2019 NSS Lab's Breach Prevention Systems (BPS) Group Test results, https://pages.checkpoint.com/nss-breach-prevention-report-2019.html

Pre-emptive User Protections

To protect users across email and web, SandBlast network employs pre-emptive user protections, namely threat extraction and advanced email protections.

- **SandBlast Threat Extraction** promptly delivers clean and reconstructed versions of potentially malicious files that are received by email or downloaded from the web. Maintaining uninterrupted business flow, while emulation continues in the background, SandBlast Threat Extraction eliminates unacceptable delays created by traditional sandboxes, offering a practical prevention-first strategy that blocks malicious content from reaching users at all. SandBlast Threat Extraction instantly cleans web downloads and email with the industry's only fully integrated document and image sanitization solution.

- **Advanced Email Protections**—With emails accounting for 94% of worldwide breaches[3], defending against phishing, business email compromise (BEC), social engineering and other email-based threats has become imperative. SandBlast Network protects users against these threats, using Threat Extraction to eliminate risk from all incoming email, as well as vetting all aspects of email messages before they enter your users' mailbox, including email attachments, email links, sender and recipient details and the text within. To this end, SandBlast Network evaluates over 300 parameters per email with multiple innovative technologies and rules-based engines, that include Natural Language Processing (NLP), Threat Emulation, AI-based phishing protection, AI-based fraud protection, URL reputation, emulating clicks on links and Click-Time Protection (also called URL rewriting) which analyzes and blocks malicious links in real time, as they are clicked.

ThreatCloud—Dynamic Threat Intelligence Repository

Comprising the largest repository of real-time, security intelligence—utilized in four billion security decisions daily—Check Point ThreatCloud examines suspicious files and emails with breakthrough AI engines to determine if they are malicious or benign.

Powering SandBlast Network's zero day protection, including anti-phishing and safe browsing, ThreatCloud gleans cyber attack data from:

- Hundreds of millions of protected assets worldwide across cloud, endpoints and networks
- Over 100,000 security gateways
- Top notch research by Check Point Research Labs
- The industry's best threat intelligence feeds

[1] 2019 Verizon Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

AI-Generated Threat Emulation Verdicts

Inspecting files and emails for which no threat intelligence exists, SandBlast Network performs deep CPU-level emulation that is resistant to the most evasive attacks, even by nation states. It also employs OS-level inspection to examine a broad range of file types, including executables and documents, and emulates threats across PC and Mac devices, ensuring the best zero-day protection for all enterprise users.

SandBlast Network leverages the power of data science to detect the newest threats with exhaustive AI engines and rich rule-based engines that process millions of parameters collected from runtime behaviors—reaching a single conclusive AI-generated verdict. AI heuristics are continually optimized against the latest threats unleashed to the wild.

Intuitive Management

SandBlast Network offers single click setup[4] of security policies thanks to out-of-the-box best practice profiles that eliminate the need to manually configure policies for each network segment, e.g. data center, guest network, perimeter, internal network etc. Network settings are optimized per business need to provide the most effective security while maintaining optimal network performance. By only deploying policies that are relevant to the specific network segment being protected, organizations save on bandwidth and processing power for a more cost-effective zero-day protection strategy.

And thanks to auto-updated threat prevention engines, organizations always run with the latest features, best practice policies and technology, as these are automatically updated in the background, with no need to push policy updates manually.

Supports Current SIEM and SOC Workflows

SandBlast Network offers advanced network forensics and actionable intelligence that integrate with your SIEM and SOC infrastructure, enabling security teams to:

- Quickly integrate logs and forensic reports into their SIEM platform
- Enforce private threat intelligence in SandBlast Network
- Accelerate investigation and time-to-remediation with advanced forensics
- Gain visibility into zero-day phishing and malware targeting the network, including malware families, MITRE ATT&CK techniques used and much more
- Build confidence in a prevention-first strategy through insights and transparency

Compliance and Reporting

Serving as the gold standard for efficient security management, Check Point's R80 console provides enterprise and government-grade compliance and reporting, including:

- **Compliance**—Easy-to-use best practices, mapped to a broad array of regulatory mandates, offer full visibility into your compliance stance with actionable configuration guidelines, and instant alerts that apprise of any policy changes in real time
- **Logging and Reporting**—Generate audit-ready reports, view logs online, integrate them right into your log server or SIEM with our broad integration ecosystem, or export them as needed

Smooth Business Productivity

SandBlast Network is the only zero-day protection solution that does not compromise business productivity, enabling a true prevention-first strategy. Letting users maintain their current email and browsing workflows, SandBlast Threat Extraction cleans email attachments and web downloads in 1.5 seconds, while slashing administration overhead by up to 70%.

Thanks to blazing-speed, AI-generated Threat Emulation verdicts, Sandblast Network protects user activity across email, web and networks, for powerful zero-day protection against multiple attack vectors.

Flexible Deployment Options

Whether you're using Check Point Next Generation Security Gateways or a third party's, SandBlast Network integrates with current security infrastructure for the best security, management and uptime.

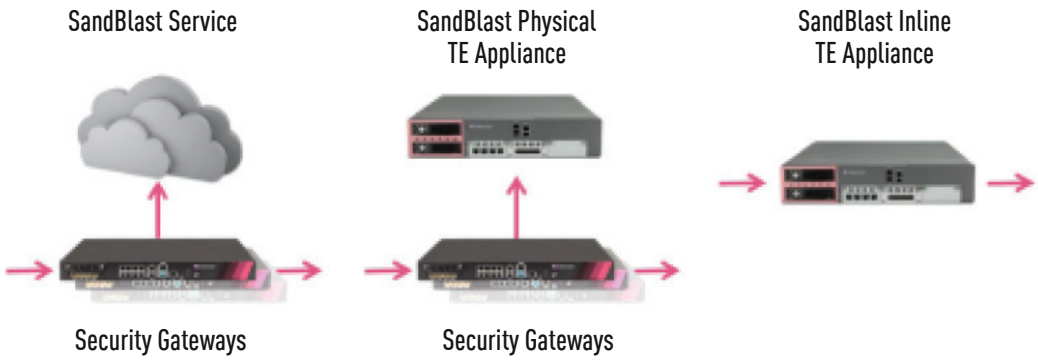
Network Security Controls Covered by Check Point Solutions

TECHNOLOGY	NEXT GENERATION THREAT PREVENTION (NGTP PACKAGE)	SANDBLAST NETWORK (NGTX PACKAGE)
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
Application Control	✓	✓
Content Awareness	✓	✓
URL Filtering	✓	✓
Anti-bot	✓	✓
Anti-Virus		✓
Anti-Spam		✓
SandBlast Threat Emulation		✓
SandBlast Threat Extraction		✓

SandBlast Network offers flexible deployment options, letting you add zero-day protection to your current security gateways as a:

- Cloud-based service
- On-premises physical appliance, suitable for regulated environments
- Standalone Threat Emulation inline appliance, or Mail Transfer Agent (MTA), when deployed with a third party security gateway

A technical migration path is offered to organizations with third party security gateways using a simple migration wizard.



SandBlast Network Specifications

Threat Emulation

Emulation Environments

PC: Windows:
- Win 7 32 bit, Office 2013
- Win XP
- Win 7 32 bit, Office 2003 / 2007
- Win 7 32 bit, Office 2010
- Win 7 64 bit
- Win 8.1

MacOS: MacOS OSx*

**static analysis*

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, ELF executable (MacOS, Linux) and more

Archive Files

- Archived (compressed) files
- Password protected archives

Threat Extraction

Extraction Modes

- Clean and keep original file type
- Convert to PDF

File Types

Web downloads and email attachments in these formats:
- Microsoft Word
- Microsoft PowerPoint
- Microsoft Excel
- Adobe PDF
- Image files

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)

GENERAL	
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
SUPPORTED PROTOCOLS	
Threat Emulation	HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP
Threat Extraction	• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS—MTA deployment

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com