Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Agent

All the Endpoint Protection You Need

SandBlast Agent is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such as ransomware, phishing or drive-by malware, while quickly minimizing breach impact with autonomous detection and response.

This way, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution.

KEY PRODUCT BENEFITS

Complete endpoint protection: prevent the most imminent threats to the endpoint

Fastest recovery: Automating 90% of attack detection, investigation, and remediation tasks

Best TCO: All the endpoint protection you need in a single, efficient and cost-effective solution

UNIQUE PRODUCT CAPABILITIES

Advanced behavioral analysis and machine learning algorithms shut down malware before it inflicts damage

High catch rates and low false positives ensure security efficacy and effective prevention

Automated forensics data analysis offers detailed insights into threats

Full attack containment and remediation to quickly restore any infected systems

Market-leading Endpoint Security Solution

AA
NSS Labs

Check Point SandBlast Agent Achieves AA Product Rating in NSS Labs 2020 Advanced Endpoint Protection Test

LEARN MORE

FORRESTER®

Forrester Wave Recognizes Check Point as a Leader in Endpoint Security

LEARN MORE

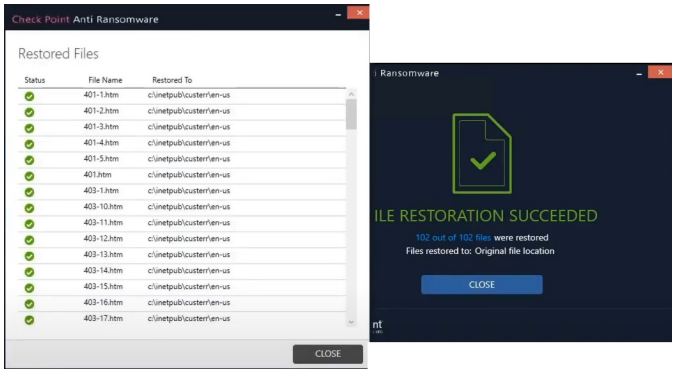
How it Works

Complete Endpoint Protection

Prevent the Most Imminent Threats to the Endpoint

- **Block malware** coming from web browsing or email attachments before it reaches the endpoint, without impacting user productivity. Every file received via email or downloaded by a user through a web browser is sent to the Threat Emulation sandbox to inspect for malware. Files can also be sanitized using a Threat Extraction process (Content Disarm & Reconstruction technology) to deliver safe and cleaned content in milliseconds.

- **Gain runtime protection against ransomware, malware, and file-less attacks, with instant and full remediation,** even in offline mode. Once an anomaly or malicious behavior is detected, Endpoint Behavioral Guard blocks and remediates the full attack chain without leaving malicious traces. Anti-Ransomware identifies ransomware behaviors such as encrypting files or attempts to compromise OS backups and safely restores ransomware-encrypted files automatically. SandBlast Agent uses a unique vaulted space locally on the machine that is only accessible to Check Point signed processes - in case the malware attempts to perform a shadow copy deletion, the machine will not lose any data.



- **Phishing Protection** - Prevent credential theft with Zero-Phishing® technology that identifies and blocks the use of phishing sites in real-time. Sites are inspected and if found malicious, the user is blocked from entering credentials. Zero-phishing® even protects against previously unknown phishing sites and corporate credential re-use.

Industry's best catch rate of known and zero-day malware

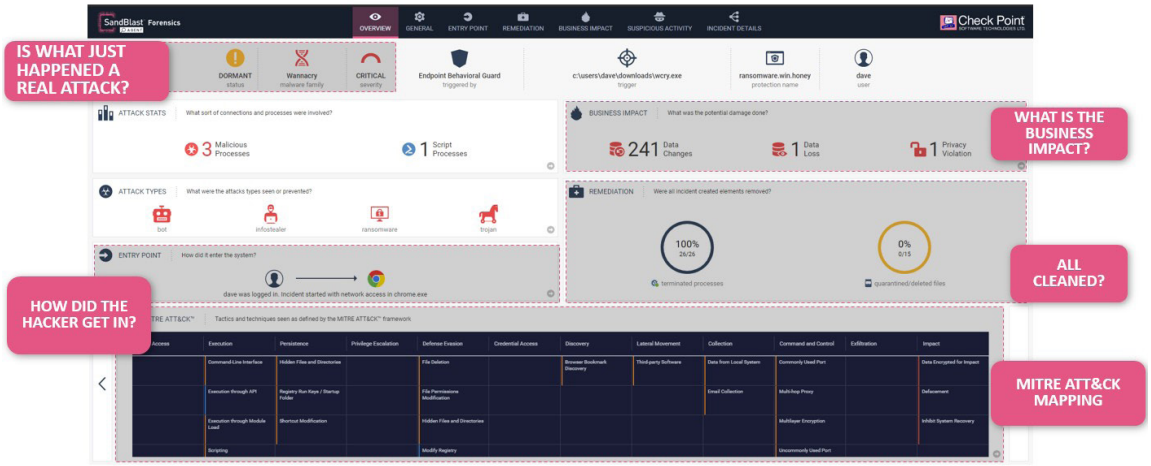
A recognized Industry Leader as seen in NSS Advanced Endpoint Protection lab test of 2020, SandBlast Agent is powered by over 60 threat prevention engines and fueled by Check Point ThreatCloud™, the world's most powerful threat intelligence to deliver the highest overall threat catch rate in the market.

Fastest Recovery

Automating 90% of Attack Detection, Investigation, and Remediation Tasks

- **Automated attack containment and remediation:** the only Endpoint Protection solution that automatically and completely remediates the entire cyber kill chain. Once an attack has been detected, the infected device can be automatically quarantined to prevent lateral infection movement and restored to a safe state.

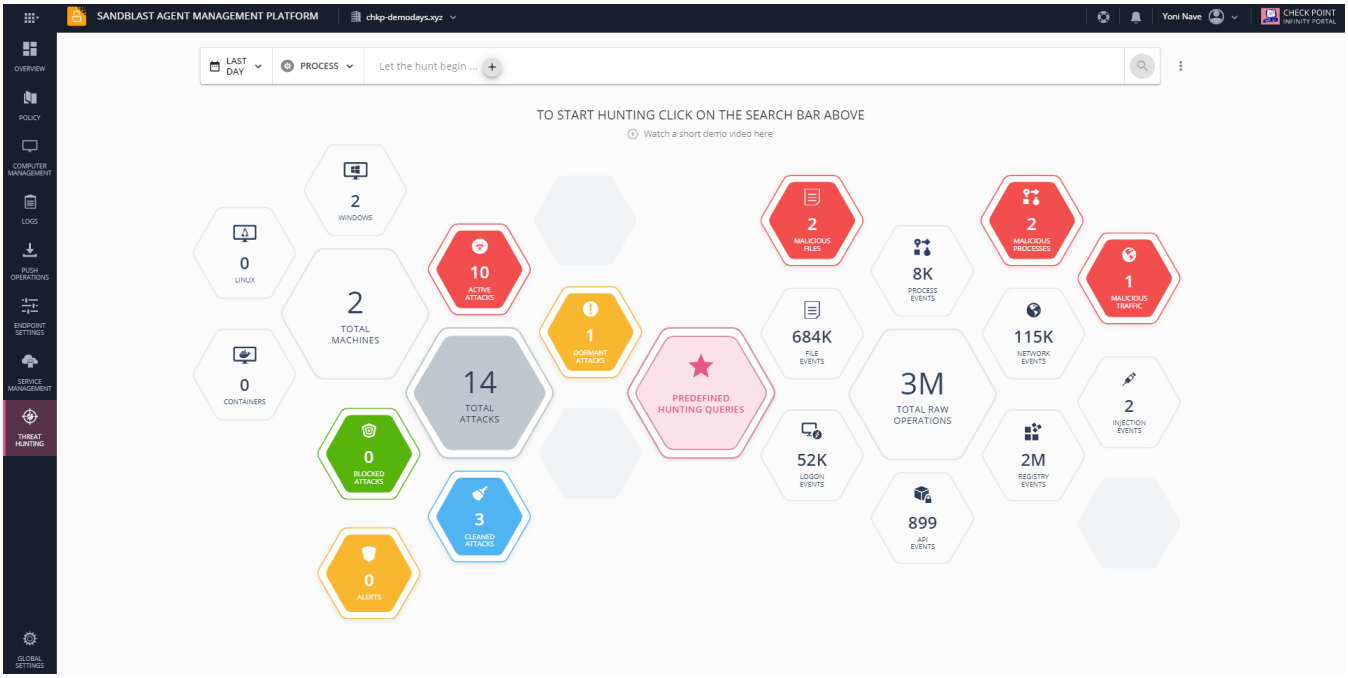
- **Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.



SandBlast Agent Forensic Report

> *"The biggest advantage to using Check Point SandBlast Agent is that we don't need to worry about ransomware attacks on our environment. It provides total peace of mind, and you can't put a price tag on that. We know it will be there, and that our data will remain safe."*
>
> David Ulloa, Chief Information Security Officer, IMC Companies

- **Threat Hunting:** powered by enterprise-wide visibility and augmented by globally shared threat intelligence from hundreds of millions of sensors, collected by ThreatCloud™. With the Threat Hunting capability, you can set queries or use predefined ones to identify and drill down into suspicious incidents, and take manual remediation actions.



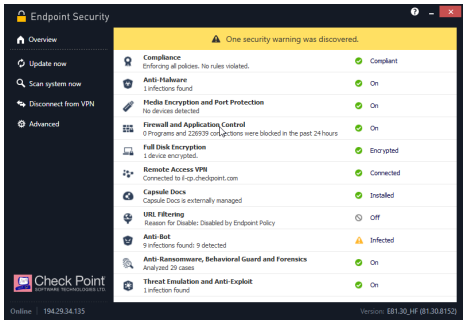
SandBlast Agent - Threat Hunting

> *"Since we deployed SandBlast Agent, we have not had a single advanced malware or ransomware incident in almost a year."*
> Russell Walker, Chief Technology Officer, Mississippi Secretary of State

Best Total Cost of Ownership

All The Endpoint Protection You Need In a Single, Efficient and Cost-Effective Solution

One single, unified agent for EPP, EDR, VPN, NGAV, data, and web-browsing protection, so your organization can streamline processes and reduce TCO.



Full flexibility to meet your specific security and compliance requirements.

- Managed either on-premises or via a cloud service, SandBlast Agent offers easy-to-use, robust functionality and fast deployment to meet your requirements
- Supporting Windows, macOS, Linux operating systems
- VDI capability (desktop instance emulation on a remote server), supporting VMWare Horizon, Citrix PVS/MCS
- The recently updated SandBlast Agent Installer allows seamless upgrades, rollbacks with no reboots or disruption for the end-users.
- Developer protection support – to help protect developers without integrating the continuous integration/continuous delivery (CI/CD) or integrated development environment (IDE).

Build on Check Point Infinity, the first consolidated security architecture designed to resolve the complexities of growing connectivity and inadequate security, delivering full protection and threat intelligence across networks, clouds, endpoints, mobile devices, and IoT.

CHECK POINT INFINITY

> *"Check Point Sandblast - the One And Only Advanced Endpoint Protection. Sandblast Agent was for us the best suited Advanced Endpoint Protection. It was deployed quickly within our worldwide organization. The management console has an intuitive user interface and easy to use"*
>
> Sr. Security Analyst, large global infrastructure enterprise

Technical Specifications

SANDBLAST AGENT PACKAGES	
Packages	• **Data Protection** – includes Full Disk Encryption and Removable Media Encryption, including Access Control and Port Protection • **SandBlast Agent Basic** – includes Anti-Malware, Anti-Ransomware, Zero-day Phishing, Advanced Threat Prevention, & Endpoint Detection and Response (EDR) • **SandBlast Agent Advanced** – includes SandBlast Agent Basic, plus Threat Emulation and Threat Extraction • **SandBlast Agent Complete** – includes SandBlast Agent Advanced, plus Data Security (Full Disk and Media Encryption) **Note: Endpoint Compliance** is provided with all packages
OPERATING SYSTEMS	
Operating System	• Windows Workstation 7, 8, and 10 • Windows Server 2008 R2, 2012, 2012 R2, 2016 • MacOS Sierra 10.12.6, MacOS High Sierra 10.13.4 (Threat Emulation, Threat Extraction, Anti- Ransomware, Chrome for Mac Browser Extension)
Content Disarm & Reconstruction (CDR) across email and web	
Threat Extraction	Removes exploitable content, reconstructs files to eliminate potential threats and delivers sanitized content to users in a few seconds
Threat Emulation	• Threat sandboxing capability to detect and block new, unknown malware and targeted attacks found in email attachments, downloaded files, and URLs to files within emails. • Provides protection across widest range of file types, includes MS Office, Adobe PDF, Java, Flash, executables, and archives, as well as multiple Windows OS environments. • Uncovers threats hidden in SSL and TLS encrypted communications.
Centralized Management	
Cloud & On-Prem Management	• SandBlast Service (Hosted on Check Point cloud) • SandBlast Appliance (Hosted on premise)
NGAV: Runtime Detection and Protection	
Anti-Ransomware	• Threat Prevention - constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature less. • Detect and quarantine - All elements of a ransomware attack are identified by forensic analysis and then quarantined. • Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity.
Anti-Exploit	• Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged. • Detects exploits by identifying suspicious memory manipulations in runtime. • Shuts down the exploited process upon detecting one, remediates the entire attack chain
Behavioral Guard	• Adaptively detects and blocks malware mutations according to their real-time behavior. • Identifies, classifies, and blocks malware mutations in real time based on minimal process execution tree similarities.
Web Protection	
Zero-Phishing	• Real-time protection from unknown phishing sites • Static and heuristic-based detection of suspicious elements across websites requesting private info
Corporate Credential Protection	Detection of corporate credentials reuse on external sites
URL Filtering	• Lightweight browser plugin, allow/block access to websites in real-time • Enforce organization policy for safe internet for users on/off organization premises, enforce regulation compliance, improve organization productivity • Full visibility to HTTPS traffic
THREAT HUNTING	
Threat Hunting	Collection of all raw and detected events on the endpoint, enabling advanced queries, drilldown and pivoting for proactive threat hunting and deep investigation of the incidents

Why SandBlast Agent?

Today more than ever, endpoint security plays a critical role in enabling your remote workforce. With 70% of cyber attacks starting on the endpoint, complete endpoint protection at the highest security level is crucial to avoid security breaches and data compromise.

SandBlast Agent is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such as ransomware, phishing, or drive-by malware, while quickly minimizing breach impact with autonomous detection and response.

This way, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution.

Learn more: https://www.checkpoint.com/products/advanced-endpoint-protection/

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com