

# CHECK POINT SANDBLAST AGENT

## CHECK POINT SANDBLAST AGENT WITH **ANTI-RANSOMWARE**

The Power to Protect.  
The Insight to Understand.

### Product Benefits

- Comprehensive EDR\* solution with advanced prevention capabilities
- Prevents and remediates evasive ransomware attacks
- Proactively blocks unknown and zero-day malware
- Provides instant actionable understanding of attacks
- Automatically remediates infections
- Protects users credentials

### Product Features

- **Threat Emulation:** Evasion resistant sandbox technology
- **Threat Extraction:** Delivers sanitized risk-free files to users in real-time
- **Anti-ransomware:** Prevents and remediates evasive ransomware attacks
- **Zero-Phishing:** Blocks deceptive phishing sites and alerts on password reuse
- **Anti-Bot:** Identify and isolate infected hosts
- **Forensics:** Records and analyzes all endpoint events to provide actionable attack forensics reports

\* *Endpoint Detection and Response (EDR)*

## INSIGHTS

The rise of breaches caused by malware, ransomware and sophisticated social engineering attacks has made endpoints a prevalent entry point for threats on organizations. Those attacks may be hidden in web-downloaded content, webmail attachments, removable storage devices or network shares. Your employees may unknowingly become victims of ransomware, phishing and social engineering attacks resulting in major financial losses, data breaches and lost productivity. Even the simple action of employees reusing corporate credentials and passwords for non-business web services can put your organization at risk. On the other hand, users demand real-time security protections that can support their need for unconstrained access to the internet with immediate delivery of business-critical files and emails.

Additionally, with more employees using corporate devices to work remotely, and as more contractors, and consultants bring their own systems into the enterprise, cybercriminals target weaknesses in traditional endpoint security to infiltrate and infect these workers' systems. Once inside, hackers leverage lateral communications through the network to infect additional devices. As threats evolve, organizations must find ways to continuously detect, prevent, and respond quickly to attacks on the endpoint in order to limit and remediate damages.

So how can you keep your employees safe from these emerging threats while allowing them to work at the pace your business demands?

## SOLUTION

Check Point SandBlast Agent provides purpose-built advanced Zero-Day Protection capabilities to web browsers and endpoints, leveraging on Check Points industry leading network protections. SandBlast Agent ensures complete real-time coverage across threat vectors, letting your employees work safely no matter where they are without compromising on productivity. Threat emulation capability emulates unknown files in contained environment to detect malicious behaviors and prevent infections while Threat Extraction provides sanitized risk-free files to the users instantly.

Check Point SandBlast Agent includes Anti-Ransomware – a purpose-built ransomware protection that stops ransomware in its tracks and reverses the damage automatically, ensuring organizations are protected against malicious extortion attacks that encrypt business data and demand ransom payment for its retrieval.

Using Zero Phishing technology, SandBlast Agent proactively blocks access to new and unknown deceptive websites, as well as safeguards user credentials by preventing the use of corporate passwords on external websites.

SandBlast Agent captures forensics data with continuous collection of all relevant system events, and then provides actionable incident analysis to quickly understand complete attack lifecycle. With visibility into the scope, damage, and attack vectors, incident response teams maximize productivity and minimize organizational exposure.

## PREVENTS ZERO-DAY ATTACKS

Check Point SandBlast Agent extends the proven protections of SandBlast Zero-Day Protection to endpoint devices, as well as to web browsers. Threat Extraction reconstructs downloaded files in seconds, eliminating potential threats and promptly delivering a safe version to users. At the same time, Threat Emulation discovers malicious behavior and prevents infection from new malware and targeted attacks by quickly inspecting files in a virtual sandbox.

## PROTECTS AGAINST RANSOMWARE

SandBlast Agent's Anti-Ransomware protection prevents evasive cyber-extortion attacks which can bypass antivirus and other malware protection solutions. Ransomware impacts businesses by encrypting data files and demanding ransom for their retrieval. Anti-Ransomware uses a purpose-built behavioral analysis engine capable of detecting and remediating ransomware infections on endpoints. The signature-less technology does not rely on frequent updates and can work both online and offline. Ransomware infections are automatically and fully quarantined based on SandBlast Agent's forensic analysis. Anti-Ransomware automatically restores files that were encrypted prior to the attack containment.

## BLOCKS ZERO-DAY PHISHING ATTACKS

The Zero Phishing capability within SandBlast Agent uses dynamic analysis and advanced heuristics to identify and prevent access to new and unknown phishing sites targeting user credentials through web browsers in real-time.

In addition, this capability prevents theft of corporate credentials from potential breaches of passwords on third party sites by alerting users when violating the corporate password re-use policies.

## IDENTIFIES AND CONTAINS INFECTIONS

With a local version of Anti-Bot security protection, continuously updated with the latest Threat Intelligence data via ThreatCloud, SandBlast Agent identifies and blocks bot communications with command and control servers to contain and quarantine any infected hosts.

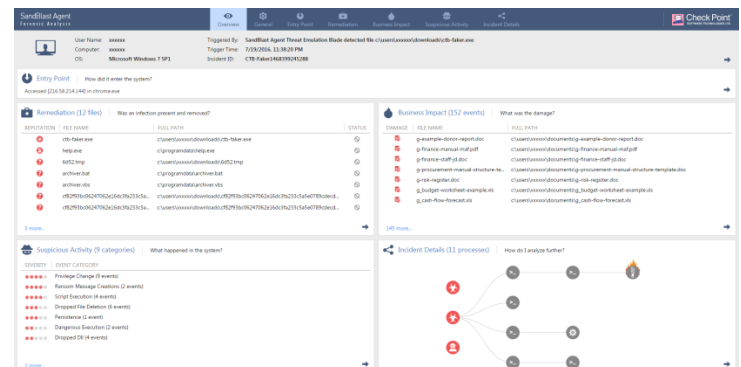
## COMPREHENSIVE COVERAGE ACROSS THREAT VECTORS

SandBlast Agent secures users from threats delivered via web downloads using techniques such as phishing, malicious content copied from removable storage devices, infections

caused by lateral movement of data and malware between systems on a network segment, as well as infections delivered via encrypted content.

## FULL VISIBILITY OF SECURITY EVENTS

Check Point SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity. SandBlast Agent can trace and report the steps taken by malware, including zero-day threats. Continuous monitoring by SandBlast Agent ensures that data is available after a completed attack, even those that remove files and other indicators of compromise left on the system.



## ACTIONABLE INCIDENT ANALYSIS

The forensics analysis process automatically starts when a malware event occurs. Using a combination of advanced algorithms and deep analysis of the raw forensic data, it builds a comprehensive incident summary. The summary provides key actionable attack information, including:

**Malicious events** – What evidence of suspicious behavior was detected throughout the attack lifecycle?

**Entry point** – How did the attack enter the network? What were the main elements used in the attack? How was the attack initiated?

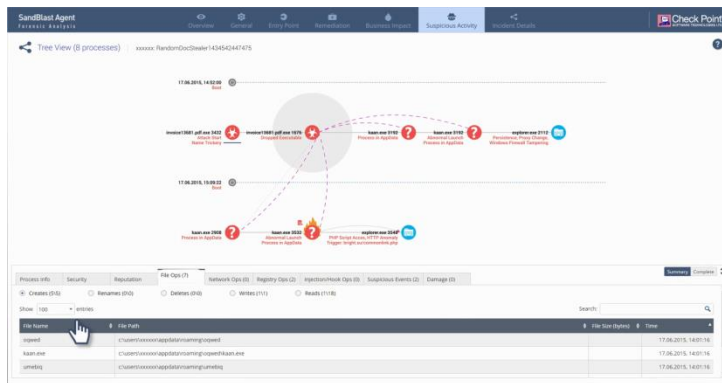
**Damage scope** – What did the malware do once activated that may impact the business? What data was compromised and/or copied externally?

**Infected hosts** – Who else or what else is affected?

This comprehensive attack diagnostics and visibility supports remediation efforts. System administrators and incident response teams can swiftly and efficiently triage and resolve attacks, getting your organization back to business as usual quicker.

## DETAILED INCIDENT REPORTS

The forensics capability within SandBlast Agent allows you to view event reports, triggered from the gateway or endpoint itself, from a central location using SmartEvent. Security Administrators can also generate reports for known malicious events, providing a detailed cyber kill chain analysis. These reports provide actionable incident analysis, accelerating the process of understanding the complete attack lifecycle, damage and attack vectors.



## THIRD-PARTY INTEGRATION

SandBlast Agent works in conjunction with Antivirus and other security solutions from Check Point, as well as from other vendors. It enhances the detection capabilities of existing Antivirus products, enabling protection from advanced threats and providing actionable incident analysis.

When triggered by an event or investigation request by another Check Point component or third party solution, endpoint forensics logs are analyzed to generate reports viewable in SmartEvent and SmartLog.

## SANDBLAST FAMILY OF SOLUTIONS

The SandBlast Zero-Day Protection solution suite also includes additional products that provide advanced threat protection for enterprise networks ([SandBlast Network](#)) and cloud applications ([SandBlast Cloud](#)).

## FLEXIBLE DEPLOYMENT AND EASY MANAGEMENT

SandBlast Agent provides flexible deployment options to meet the security needs of every organization. Following three packages are available:

### SandBlast Agent for Browsers

SandBlast Agent for Browsers is a browser extension focused on preventing attacks that use web browsers as a main entry point. It includes the capabilities of Threat Emulation, Threat Extraction, Zero Phishing and credential protection.

This stand-alone solution can be implemented using a simple browser plugin and is an ideal fit for organizations looking for rapid deployment with a minimal footprint. SandBlast Agent for Browsers utilizes standard endpoint management tools, such as GPO (Group Policy Object) to push policy to user endpoints.

### SandBlast Agent

SandBlast Agent prevents threats on endpoint devices. It includes the capabilities of Threat Emulation, Threat Extraction, Anti-Ransomware, Zero Phishing, Anti-Bot and Forensics.

SandBlast Agent can be quickly deployed, and all policies are managed centrally through SmartCenter. Event logs and incident reports are accessed through SmartEvent and SmartLog, providing deep insight to understand even the most advanced attacks.

### Endpoint Complete Protection

Check Point's endpoint complete protection suite adds Full Disk Encryption, Antivirus and Firewall to the SandBlast Agent package.

Regardless of which package you select, the non-intrusive, low-overhead deployment utilizes a SandBlast remote sandbox running as a service – on either the SandBlast Service or your own private appliances – resulting in minimal impact on local performance and full compatibility with installed applications.

## TECHNICAL SPECIFICATIONS

SANDBLAST AGENT - PACKAGES	
Available Packages	<ul style="list-style-type: none"> <li>• <b>SandBlast Anti-Ransomware</b> – includes Anti-Ransomware only</li> <li>• <b>SandBlast Agent for Browsers</b> – includes Threat Emulation, Threat Extraction, Zero Phishing, Credential Protection</li> <li>• <b>SandBlast Agent</b> – includes Threat Emulation, Threat Extraction, Anti-Ransomware, Zero Phishing, Credential Protection, Anti-Bot, Forensics and Automated Incident Analysis</li> <li>• <b>Endpoint Complete Protection</b> – The endpoint complete protection adds Full Disk Encryption, Antivirus and Firewall to the SandBlast Agent package</li> </ul>
ENDPOINT SECURITY – SANDBLAST AGENT	
Operating System	<ul style="list-style-type: none"> <li>• Windows 7, 8, and 10</li> <li>• Windows server 2008 R2, 2012, and 2012 R2</li> </ul>
BROWSER PROTECTION – SANDBLAST AGENT FOR BROWSERS	
Supported Browsers	<ul style="list-style-type: none"> <li>• Google Chrome</li> <li>• <i>Coming Soon</i> - Internet Explorer and Firefox</li> </ul>
DOWNLOAD PROTECTION - THREAT EMULATION AND THREAT EXTRACTION	
Threat Extraction – Supported File Types	<ul style="list-style-type: none"> <li>• Adobe PDF</li> <li>• Microsoft Word, Excel, and PowerPoint</li> </ul>
Threat Emulation – Supported File Types	<ul style="list-style-type: none"> <li>• Over 40 file types, including: Adobe PDF, Microsoft Word, Excel, and PowerPoint, Executables (EXE, COM, SCR), Shockwave Flash – SWF, Rich Text Format – RTF and Archives</li> </ul>
Deployment Options	<ul style="list-style-type: none"> <li>• SandBlast Service (Hosted on Check Point cloud)</li> <li>• SandBlast Appliance (Hosted on-premise)</li> </ul>
ANTI-RANSOMWARE	
Anti-Ransomware	<ul style="list-style-type: none"> <li>• Signature-less behavioral detection of ransomware, no internet connection is required</li> <li>• Malicious file encryption activity detection</li> <li>• Automated ransomware quarantine</li> <li>• Automated restoration of encrypted data (if encryption started prior to quarantine)</li> </ul>
ZERO PHISHING AND CREDENTIAL PROTECTION	
Zero Phishing	<ul style="list-style-type: none"> <li>• Real-time protection from unknown phishing sites</li> <li>• Static and heuristic based detection of suspicious elements in sites that request user credentials</li> </ul>
Corporate Credential Protection	<ul style="list-style-type: none"> <li>• Detection of reuse of corporate credentials on external sites</li> </ul>
FILE SYSTEM MONITORING	
Threat Emulation	<ul style="list-style-type: none"> <li>• Content copied from removable storage devices</li> <li>• Lateral movement of data and malware between systems on a network segment</li> </ul>
Enforcement Modes	<ul style="list-style-type: none"> <li>• Detect and alert</li> <li>• Block (background &amp; hold modes)</li> </ul>
ANTI-BOT	
Enforcement Modes	<ul style="list-style-type: none"> <li>• Detect and alert</li> <li>• Block (background &amp; hold modes)</li> </ul>
FORENSICS	
Analysis Triggers	<ul style="list-style-type: none"> <li>• Anti-Ransomware detection on the endpoint</li> <li>• Anti-Bot detection on the network or on endpoint</li> <li>• Threat Emulation detection on the network</li> <li>• Check Point Antivirus detection on the endpoint</li> <li>• Third-party Antivirus detection on the endpoint</li> <li>• Manual Indicators of Compromise (IoCs)</li> </ul>
Damage Detection	<ul style="list-style-type: none"> <li>• Automatically Identify: Data exfiltration, data manipulation or encryption, key logging</li> </ul>
Root Cause Analysis	<ul style="list-style-type: none"> <li>• Trace and identify root cause across multiple system restarts in real-time</li> </ul>
Malware Flow Analysis	<ul style="list-style-type: none"> <li>• Automatically generated interactive graphic model of the attack flow</li> </ul>
Malicious Behavior Detection	<ul style="list-style-type: none"> <li>• Over 40 malicious behavior categories</li> <li>• Hundreds of malicious indicators</li> </ul>
MANAGEMENT	
Policy Management	<ul style="list-style-type: none"> <li>• Endpoint Policy Management (EPM)</li> </ul>
Event Monitoring	<ul style="list-style-type: none"> <li>• SmartLog</li> <li>• SmartEvent</li> </ul>
Endpoint Management Version	<ul style="list-style-type: none"> <li>• R77.30.03/E80.65 and above</li> </ul>
Endpoint Management - Available Packages	<ul style="list-style-type: none"> <li>• Included as standard with SmartCenter and Smart-1 appliances</li> <li>• Available as a software license</li> </ul>

### CONTACT US

**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