CHECK POINT

SandBlast Agent Endpoint Protection

CHECK POINT
SandBlast Agent
Endpoint Protection

Advanced Threat Prevention

SandBlast Agent prevents and automatically remediates evasive cyberattacks, giving you instant actionable insights of attacks and the protection of user credentials.

Key Product Benefits

Mature endpoint capabilities to protect against known and unknown cyberattacks

Industry best practices elevate endpoint security to combat targeted and evasive attacks

Advanced behavioral analysis and machine learning algorithms shut down malware before they inflict damage

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

Automated forensics data analysis offers detailed insights into threats

Full attack containment and remediation quickly restore any infected systems

Cutting-edge threat prevention capabilities

SandBlast Agent uses a fleet of threat engine technologies to help defend against the full scope of known and unknown zero-day malware. Here are some of the key threat prevention technologies and how they work:

Threat Emulation / Threat Extraction
Every downloaded file using a web browser is put through threat emulation, or a sandboxing process where it is quarantined until deemed safe. Threat extraction ensures users receive “clean” files; the same downloaded file minus dangerous components. The sanitized, risk-free file can then be used normally, plus the option to access the original file.

Anti-Malware
Protect endpoints from unknown viruses, worms, and Trojan horse malware.

Anti-Ransomware
Monitors changes to files on user drives to identify ransomware behavior such as file encryption. Anti-Ransomware can also recover encrypted files regardless of the encryption used by taking smart snapshots of a user’s file when a change is being made to the file by an unknown application.

Zero-day Phishing Protection
When a user browses a website and prior to typing in his/her credentials, the zero-phishing engine will inspect, identify, and block phishing sites. If the site is deemed malicious, the user will not be able to enter credentials. This engine offers zero-day protection based on site characteristics, such as known malicious URLs. Even brand-new phishing sites can be identified.

Advanced Threat Prevention
Anti-Bot detects and prevents communication by processes to malicious command and control server (C&C server) in the wild. Anti-Bot monitors all the network traffic coming from all the processes executed on the endpoint, and is able to detect malicious communication to C&Cs. Detection is based on two layers by comparing communication signatures to a known malicious communication signature and using Check Point Threat Cloud to identify malicious accessed IPs or domains.

Once a malicious communication is detected, Anti-Bot can block the communication immediately, kill the process, and put the process’s file in quarantine. A log is then sent to the log server to notify the system administrator.

Anti-Exploit
Protects against application threats that exploit memory vulnerabilities. Anti-Exploit protects widely targeted applications such as Microsoft Office, Adobe PDF Reader, Browsers, and Adobe Flash. Anti-Exploit uses four technologies to protect against existing and new exploits:

- Import – Export Address Table Parsing
- Return Oriented Programming
- Stack Pivoting
- VB Script God Mode

Behavioral Guard
Detects and remediates all forms of malicious behavior. When detected, it generates a forensics report with automatic or manual remediation.

Cluster-based forensics
Detects and classifies known and unknown malware families based on minimal forensics trees, including:

- Evasion attempts based on malware detection
- Expending Machine Learning-based context aware detections (for EXEs, file-less script based attacks, and more)
- Baselining behavior of legit apps to detect malicious use of them
- Forensics data behavioral anomaly detection
- Static analysis of EXE for faster detection
- ROP exploit protection
- Attack reputation intelligence
- Expanding Machine Learning-based behavioral models for Behavioral Guard detection logics
- MITRE attack integration into Forensics Records; analyzes endpoint events to provide actionable attack forensics reports

Data Protection
Provides access control and port protection.

Endpoint Detection and Response
Uses signature-based protection against known malware.

Robust Incident Detection and Response

The SandBlast forensics analysis process starts automatically when a malware event occurs. Advanced algorithms and a deep analysis of the raw forensic data helps build a comprehensive incident summary with actionable attack information, including:

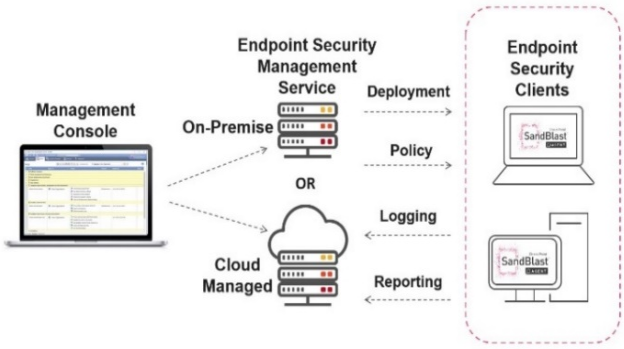
- **Malicious events** – Evidence of suspicious behavior detected throughout the attack lifecycle
- **Entry point** – How the attack was initiated, how it entered and the main elements used
- **Damage scope** – Once activated, the malware's path, its impact on the business, and what data was compromised and/or copied externally
- **Infected hosts** – Who else or what else was affected

Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks. Our incident summary event reports, triggered from the gateway or the endpoint itself, can be viewed centrally using SmartEvent.

Endpoint Security Management

SandBlast Agent endpoint security management is available via a simple, easy-to-use managed cloud service. Manage endpoints from any location, including office, home, or when on the road. The service is deployed, maintained, and optimized by Check Point and offers these benefits:

- **Elastic Growth** – Deploy endpoints without committing to a fixed size of the management server. The cloud management service grows with the expansion of your endpoints.
- **High Availability** – Enjoy optimal performance with full redundancy and automated backups.
- **Worry-free Updates** – Spend more time on threat prevention with automatic updates and upgrades to your management server.
- **Location Independence** – Upload updated endpoint policies and logs from any location without VPN-based connectivity.



Flexible Endpoint Protection options

Check Point offers four endpoint protection packages to meet your exact threat prevention needs. All packages can be quickly deployed and include endpoint security management with installation on premise or delivered as a managed cloud service. Package options include:

Endpoint Data Protection
Endpoint Data Protection offers Access Control and Port Protection capabilities.

SandBlast Agent Standard
This package prevents unknown and zero-day threats on endpoint devices using Data Protection (Access Control and Port Protection), Anti-Malware, Anti-Ransomware, Zero-day Phishing Protection, Advanced Threat Prevention, and Endpoint Detection and Response.

SandBlast Agent Advanced
The Advanced package includes all SandBlast Agent Standard protection capabilities, plus Threat Emulation and Threat Extraction.

SandBlast Agent Complete
This package includes all protection capabilities in SandBlast Agent Advanced, plus Data Security (Full Disk and Media Encryption).

Event logs and incident reports are accessed through SmartEvent and SmartLog, providing deep insights into the nature of the most advanced attacks. Each package offers non-intrusive, low-overhead deployment using a SandBlast remote sandbox as a service or placed on your own private appliances.

Technical Specifications

SANDBLAST AGENT PACKAGES	
Available Packages	• **Data Protection** – includes Access Control and Port Protection • **SandBlast Agent Standard** – includes Data Protection, Anti-Malware, Anti-Ransomware, Zero-day Phishing, Advanced Threat Prevention, & Endpoint Detection and Response (EDR) • **SandBlast Agent Advanced** – includes SandBlast Agent Standard, 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)
DOWNLOAD PROTECTION - THREAT EMULATION AND THREAT EXTRACTION	
Threat Extraction – Supported File Types	• Adobe PDF, Microsoft Word, Excel, and PowerPoint
Threat Emulation – Supported File Types	• 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
Deployment Options	• SandBlast Service (Hosted on Check Point cloud) • SandBlast Appliance (Hosted on premise)
ANTI-RANSOMWARE	
Anti-Ransomware	• Signature-less behavioral detection of ransomware, no Internet connection is required • Malicious file encryption activity detection and automated ransomware quarantine • Automated restoration of encrypted data (if encryption started prior to quarantine)
ANTI-EXPLOIT	
Anti-Exploit	• Provides protection against exploit based attacks compromising legitimate applications • Detects exploits by identifying suspicious memory manipulations in runtime • On detection, shuts down the exploited process and remediates the full attack chain
BEHAVIORAL GUARD – MALICIOUS BEHAVIOR DETECTION AND PROTECTION	
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
ZERO-DAY PHISHING PROTECTION	
Zero Phishing	• Real-time protection from unknown phishing sites • Static and heuristic based detection of suspicious elements in sites that request private info
Corporate Credential Protection	• Detection of reuse of corporate credentials on external sites
FILE SYSTEM MONITORING	
Threat Emulation	• Content copied from removable storage devices • Lateral movement of data and malware between systems on a network segment
Enforcement Modes	• Detect and alert, Block (background and hold modes)
ANTI-BOT	
Enforcement Modes	• Detect and alert, Block (background and hold modes)
ENDPOINT DETECTION AND RESPONSE	
Known Malware Protection	• Detects, prevents, remediates malware using signatures, behavior blockers and heuristic analysis
FORENSICS	
Analysis Triggers	• From the endpoint: Threat Emulation, Anti-Ransomware, Anti-Exploit, Behavioral Guard, Anti-Bot, Check Point Antivirus and third-party Antivirus • From the network: Threat Emulation, Anti-Bot, Antivirus • Manual Indicators of Compromise (IoCs)
Damage Detection	• Automatically Identify: Data exfiltration, data manipulation or encryption, key logging
Root Cause Analysis	• Trace and identify root cause across multiple system restarts in real-time
Malware Flow Analysis	• Automatically generated interactive graphic model of the attack flow
Malicious Behavior Detection	• Over 40 malicious behavior categories, hundreds of malicious indicators
Full Attack Chain Remediation	• Automatically, by tracking back and remediating all events the attack caused before detection
ENDPOINT SECURITY MANAGEMENT	
Policy Management	• Endpoint Policy Management (EPM)
Event Monitoring	• SmartLog, SmartEvent
Endpoint Management Version	• R77.30.03, R80.20
Endpoint Management - Available Packages	• Included as standard with Security Management and Smart-1 appliances; delivered as a managed cloud service or on-premise installation; available as a software license