CHECK POINT SANDBLAST AGENT NEXT GENERATION AV

CHECK POINT SANDBLAST AGENT

NEXT GENERATION AV

The Power to Protect.
The Insight to Understand.

Product Benefits

- Advanced threat protection and automated endpoint forensic analysis for all malware types
- Prevents and remediates evasive ransomware attacks
- Proactively blocks known, 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
- **Anti-Exploit:** Protects applications against exploit based attacks
- **Behavioral Guard:** Detects and blocks malicious behaviors
- **Endpoint Antivirus:** Protects against known malware
- **Forensics**: Records and analyzes all endpoint events to provide actionable attack forensics reports

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 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 protect web browsers and endpoints, leveraging Check Point's 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.

Anti-Ransomware protection stops ransomware in its tracks and reverses the damage automatically, ensures organizations are protected against malicious extortion attacks that encrypt business data and demand ransom payment for its retrieval. Zero Phishing proactively blocks access to new and unknown deceptive websites and 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.

PROTECTS AGAINST EXPLOITS

The Anti-Exploit capability provides protection against exploit-based attacks compromising legitimate applications such as browsers and Microsoft Office. It detects exploits by identifying suspicious memory manipulations in runtime. Upon detection, Anti-Exploit shuts down the exploited process, remediates the full attack chain and triggers a forensics report.

ADAPTIVELY DETECTS AND BLOCKS MALICIOUS BEHAVIORS

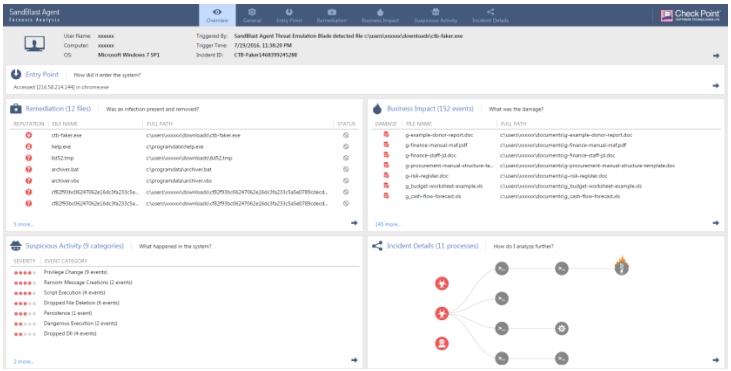
Behavioral Guard leverages forensics to effectively and uniquely identify unknown malware behaviors and accurately classify malware to its malware family. The detection and classification process is based on unique algorithms of minimal process execution tree similarities. This robust protection capability adapts to malware's evolution over time and can be used to detect and prevent endless types of attacks including those using legitimate scripting tools maliciously. Upon detection by Behavioral Guard, SandBlast Agent will block the attack, remediate it and automatically create a forensics report.

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 (IoCs) 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:

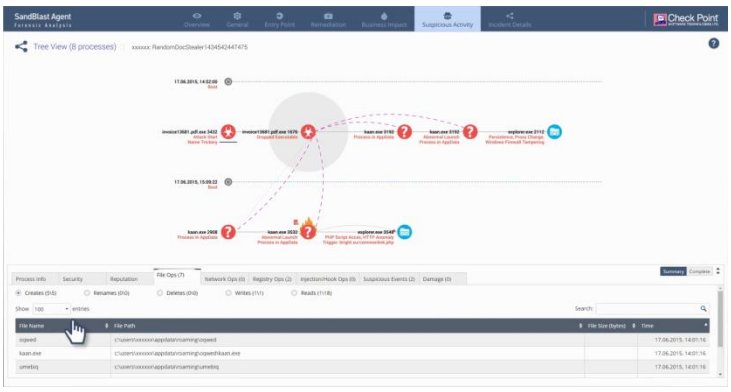
Malicious events – What evidence of suspicious behavior was detected throughout the attack lifecycle?

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 efficiently triage and resolve attacks, getting your organization back to business as usual quicker. The incident summery event reports, triggered from the gateway or endpoint itself, can be viewed centrally 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 other security solutions from Check Point and with Antivirus solutions from other vendors, enhancing the detection capabilities of existing Antivirus products. 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 mobile devices (SandBlast Mobile).

FLEXIBLE DEPLOYMENT AND EASY MANAGEMENT

SandBlast Agent provides flexible deployment options to meet the security needs of every organization. The following four packages are available:

SandBlast Anti-Ransomware

Prevents, remediates and restores evasive cyber-extortion attacks.

SandBlast Agent

SandBlast Agent prevents unknown and zero-day threats on endpoint devices. It includes the capabilities of Threat Emulation, Threat Extraction, Anti-Ransomware, Zero Phishing, Anti-Bot, Anti-Exploit, DNA Classifier and Forensics. It can be deployed besides a traditional AV and augment it with advanced prevention capabilities.

SandBlast Agent Next Generation AV

SandBlast Agent Next Generation AV incorporates all protections of SandBlast Agent and adds comprehensive Antivirus coverage to protect against known malware. It can be deployed as a full replacement for any endpoint security solution.

Endpoint Complete Protection

Check Point's endpoint complete protection suite adds Endpoint Firewall, Remote Access, Application Control, Full Disk Encryption, Media Encryption and Port Protection to the SandBlast Agent Next Generation AV package.

All packages can be quickly deployed and centrally managed. Event logs and incident reports are accessed through SmartEvent and SmartLog, providing deep insight to understand even the most advanced attacks. Regardless of which package you choose, 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	• **SandBlast Anti-Ransomware** – includes Anti-Ransomware only • **SandBlast Agent** – includes Threat Emulation, Threat Extraction, Anti-Ransomware, Anti-Exploit, Zero Phishing, Credential Protection, Anti-Bot, Anti-Exploit, Behavioral Guard, Forensics and Automated Incident Analysis • **SandBlast Agent Next Generation AV** – adds protections against known malware and can be deployed as a full replacement for any endpoint security solution • **Endpoint Complete Protection** – The endpoint complete protection adds Firewall, Remote Access, Application Control, Full Disk Encryption, Media Encryption, Port Protection and Antivirus to the SandBlast Agent package ***Endpoint Compliance** is provided with all Endpoint and SBA packages*
ENDPOINT SECURITY – SANDBLAST AGENT	
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)
BROWSER PROTECTION – SANDBLAST AGENT FOR BROWSERS	
Supported Browsers	• Google Chrome, Internet Explorer, Firefox
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 PHISHING AND CREDENTIAL 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 & hold modes)
ANTI-BOT	
Enforcement Modes	• Detect and alert, Block (background & hold modes)
ENDPOINT ANTIVIRUS	
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 3rd 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
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 • Available as a software license

CONTACT US EMAIL: INFO@CHECKPOINT.COM WEB: WWW.CHECKPOINT.COM

