CHECK POINT SANDBLAST AGENT

CHECK POINT SANDBLAST AGENT

The Power to Protect.
The Insight to Understand.

Product Benefits

- Simple, non-intrusive solution with intuitive user interface
- Proactively blocks new and unknown malware from reaching endpoints
- Maintains business productivity by promptly providing safe versions of downloaded files to users
- Protects user credentials by stopping phishing attacks in real-time
- Delivers a comprehensive view of attack history prior to discovery
- Drives full understanding of root cause, malware entry points, and scope of damage
- Accelerates response time and reduces chance of reinfection

Product Features

- Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content
- Threat Extraction reconstructs incoming files using only safe elements
- Identifies and contains infected hosts to limit damages and malware spread
- Uses dynamic analysis and heuristics to block deceptive phishing sites
- Automatically builds actionable forensics reports with key information
- Keeps credentials safe by alerting when users attempt to utilize corporate passwords on external sites

INSIGHTS

The rise of breaches caused by sophisticated social engineering and web-based malware attacks have made web browsers a prevalent entry point for threats through endpoint devices. Malware may be hidden in web-downloaded content or webmail attachments. Your employees may unknowingly become victims of phishing and social engineering attacks. 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 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 extends industry-leading network protections, including the advanced capabilities of SandBlast Zero-Day Protection to web browsers and endpoint devices. This ensures complete real-time coverage across threat vectors, letting your employees work safely no matter where they are without compromising on productivity. SandBlast Agent protects from threats delivered via web downloads, content copied from removable storage devices, links or attachments in email messages, lateral movement of data and malware between systems on a network segment and infections delivered via encrypted content.

Using Zero Phishing™ technology, SandBlast Agent proactively blocks access to new and unknown deceptive sites on the web, as well as prevents the misuse of corporate passwords to safeguard user credentials.

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

August 2, 2016

PREVENTS ZERO-DAY MALWARE

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.

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

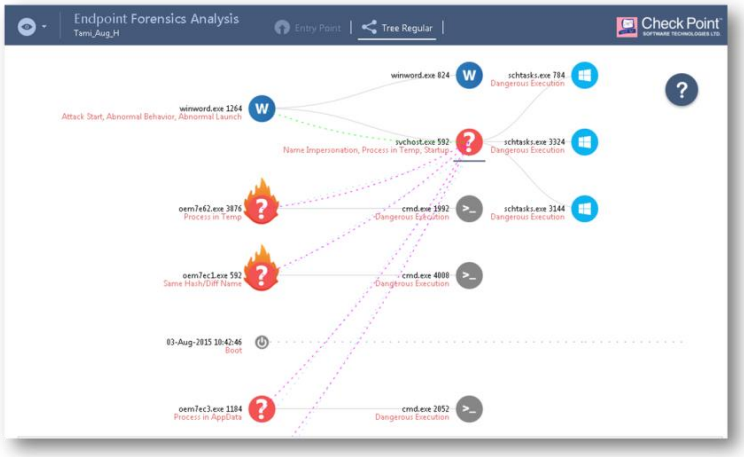
With a local version of Anti-Bot security protection, continuously updated with the latest Threat Intelligence data via ThreatCloud, SandBlast Agent identifies and blocks bot communications with command and control servers to contain and quarantine any infected hosts.

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

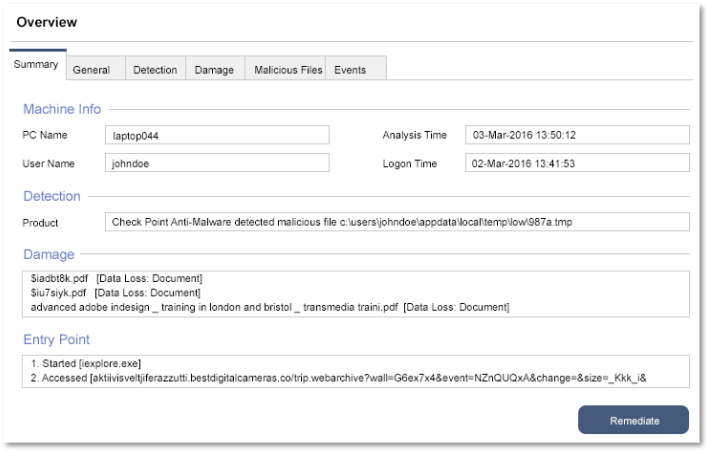
The forensics analysis process automatically starts when a malware event occurs. Using a combination of advanced algorithms and deep analysis of the raw forensic data, it builds a comprehensive incident summary. The summary provides key actionable attack information, including:

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.

August 2, 2016

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 and cloud applications.

EASY TO DEPLOY AND MANAGE

SandBlast Agent provides flexible deployment options to meet the security needs of every organization. SandBlast Agent for Browsers can be quickly deployed as an integral part of the SandBlast Agent on the endpoint, or with a minimal footprint as a standalone solution for web browsers.

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.

SandBlast Agent for Browsers Package
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 Complete Package
SandBlast Agent prevents threats on endpoint devices. It includes the capabilities of Threat Emulation, Threat Extraction, Forensics, Anti-Bot, as well as Zero Phishing and credential protection.

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.

August 2, 2016

TECHNICAL SPECIFICATIONS

SANDBLAST AGENT - PACKAGES	
Available Deployment Packages	• Standalone package - **SandBlast Agent for Browsers** which includes Threat Emulation, Threat Extraction, Zero Phishing, Credential Protection • Full package - **SandBlast Agent Complete**, includes all capabilities of SandBlast Agent for Browsers plus Anti-Bot, Forensics and Automated Incident Analysis • Full Endpoint protection package – **Endpoint Suite**, adds Full Disk Encryption, Antivirus to the SandBlast Agent complete package
ENDPONT SECURITY - SANDBLAST AGENT	
Operating System	• Windows 7, 8, and 10 • Windows server 2008 and above
BROWSER PROTECTION - SANDBLAST AGENT FOR BROWSERS	
Supported Browsers	• Google Chrome • Internet Explorer *(Coming soon)*
DOWNLOAD PROTECTION - THREAT EMULATION AND THREAT EXTRACTION	
Supported File Types – Threat Extraction	• Adobe PDF • Microsoft Word, Excel, and PowerPoint
Supported File Types – Threat Emulation	• 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
Threat Emulation and Extraction Deployment Options	• SandBlast Service (Hosted on Check Point cloud) • SandBlast Appliance (Hosted on-premise)
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 user credentials
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)
FORENSICS	
Analysis Triggers	• Anti-Bot detection on the network or on the endpoint • Threat Emulation detection on the network • Check Point Antivirus detection on the endpoint • Third-party Antivirus detection on the endpoint • 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
MANAGEMENT	
Policy Management	• Endpoint Policy Management (EPM)
Event Monitoring	• SmartLog • SmartEvent
Endpoint Management Version	• E77.30.02 and above
Endpoint Management - Available Packages	• Included as standard with SmartCenter and Smart-1 appliances • Available as a software license

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

August 2, 2016