Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
SandBlast™
AGENT

SandBlast Agent

ENDPOINT SECURITY WITHOUT COMPROMISE

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 it inflicts 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

COMPLETING YOUR ENDPOINT SECURITY EXPERIENCE

- Flexible and scalable integrated management offered in the cloud or installation on your site
- ThreatCloud™ threat intelligence database helps identify and prevent threats
- Integration with other Check Point solutions and third-party anti-virus to enhance incident response and remediation

NAVIGATING THE THREAT LANDSCAPE

Cyberattacks strike swiftly and relentlessly. Each wave grows more targeted, evasive, and potentially more lethal to your organization. According to IDC's *Cybercrime: The Credential Connection*, over 70 percent of successful data breaches start on endpoints, so the need for effective endpoint security is clear.

SandBlast Agent is advanced endpoint protection that offers various threat prevention technologies for top-line defense from advanced known and unknown zero-day cyberattacks. A threat prevention-first strategy thwarts attacks before they can unleash their destruction on your organization.

UNIQUE PRODUCT CAPABILITIES

THREAT PREVENTION

Behavioral Inspection for Post-execution Detection and Remediation: Behavioral Guard uses a unique proprietary language that describes malicious behavior in the same way processes interact with each other and with system resources. Its rules identify malware families, fileless attacks, and other generic malicious behavior. Once an anomaly or malicious behavior is detected, Behavior Guard blocks and remediates the attack.

Cyber-Extortion Defense: Anti-Ransomware prevents cyber extortion attacks that bypass antivirus and other malware protection solutions. It monitors changes to files on user drives. Together, with behavioral analysis, it identifies ransomware behaviors such as encrypting files or attempts to compromise Windows backups. Anti-Ransomware also recovers encrypted files from attacks regardless of the encryption used.

Achieving Malware-free Files: Every file downloaded by a user through a web browser is sent to the Threat Emulation sandbox to inspect for malware. Files are sanitized using a Threat Extraction process to deliver files safe to use.

Preventing Exploits: Anti-Exploit protects applications from being exploited. It makes sure common applications such as Browsers, MS Office applications, Adobe Reader and Flash player vulnerabilities cannot be leveraged to attack endpoint.

Machine Learning-based Static Analysis: Offers rapid visibility into every executable. Static features are extracted from the files and scanned against a machine learning model built based on Check Point's comprehensive attack intelligence information. Malicious files are blocked within milliseconds.

User Credentials Protected: Zero-Phishing 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.

Collaborative Threat Intelligence: ThreatCloud is an up-to-date global threat intelligence database using a worldwide network of threat sensors, proactively mitigating threats in real time based on global information.

VISIBILITY, REMEDIATION, AND RESPONSE

Infections Identified and Contained: Anti-Bot detects infected machines by continuously monitoring outgoing traffic and identifying communications with command and control (C&C) servers. If an infection is detected, it blocks traffic, remediates the attack, and isolates the machine to prevent lateral infection spread.

Automated Incident Response: When detected by a SandBlast Agent engine, forensic analysis determines the details of an incident. It monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity. Forensics also allows for the remediation of the steps taken by known and unknown malware.

REDUCING THE ATTACK SURFACE

Full Disk Encryption: Combines pre-boot protection, boot authentication, and strong encryption to ensure that only authorized users are given access to information stored on desktops and laptops. This capability can also manage and monitor native disk encryption technologies such as FileVault and BitLocker.

Media Encryption and Port Protection: Protects the data stored on computers by encrypting removable media devices and providing tight control over computer ports, including USB, Bluetooth, and others.

Remote Access VPN: Establishes secure, seamless connection to a corporate network. Privacy and integrity of sensitive information is ensured using authentication, compliance scanning, and encryption.

Endpoint Firewall and Compliance: Protects endpoints by controlling inbound and outbound traffic and ensuring policy compliance, with centralized management from a single console. Desktop Firewall policies protect endpoint systems from unauthorized access. Integrated stealth technology makes endpoints invisible to attackers.

Application Control: Enables organizations to adopt an application blacklisting/whitelisting strategy. It also recommends applications to allow or block based on application reputation information collected and analyzed by Check Point. Admins can customize additional applications in addition to more than 300 applications supported out-of-the-box.

SECURITY MANAGEMENT OPTIONS

Being able to rapidly provision, update, and troubleshoot endpoint devices are critical security management tasks. To meet your specific security and compliance requirements, we offer endpoint management via on-premise deployment or via a cloud service. Both options offer easy-to-use, robust functionality to maintain efficient and secure endpoints.

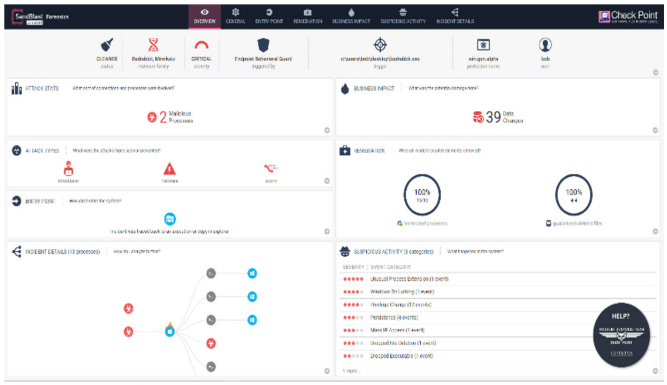

Figure 1. SandBlast Agent Forensic Report

SANDBLAST ADVANCED THREAT PREVENTION

SandBlast Threat Prevention also includes protection for networks (SandBlast Network), mobile devices (SandBlast Mobile), and SaaS applications (CloudGuard SaaS). Each solution provides multilayered security, offering zero-day protection against fifth generation cyberattacks.

BUILD ON CHECK POINT INFINITY

SandBlast Agent is an integral member of Check Point Infinity, a fully consolidated cyber security architecture that provides maximum prevention against Gen V mega-cyberattacks. The architecture is designed to resolve the complexities of growing connectivity and inefficient security.

To get more information on SandBlast Agent, contact your local Check Point representative or go to:

https://www.checkpoint.com/products/advanced-endpoint-threat-prevention/

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com