Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT SANDBLAST MOBILE

SANDBLAST MOBILE 3.0 AT-A-GLANCE

Product Benefits

- Complete threat detection and mitigation, the best mobile catch rate, and full visibility.
- Keeps business assets and sensitive data on devices safe from cyber attacks
- Simple deployment and seamless integration with all leading UEM vendors

Product Features

Advanced app analysis

Runs apps downloaded to mobile devices in a virtual, cloud-based environment to analyze behavior then approves or flags them as malicious.

Network-based attacks

Detects malicious network behavior and automatically disables suspicious networks to help keep mobile devices and data safe.

Device vulnerability assessments

Analyzes devices to uncover vulnerabilities that cyber criminals exploit to attack mobile devices and steal valuable, sensitive information.

DETECT AND STOP ATTACKS BEFORE THEY START

Smartphones and tablets give us unprecedented access to the critical business information we need to work faster and more accurately. Providing your employees with access to that information on the mobile devices they choose has many benefits, but it also exposes your business to risk.

Check Point SandBlast Mobile, an innovative approach to mobile security for iOS and Android devices, detects and stops mobile threats before they start. Whether your data's at rest on a device or in flight through the cloud, SandBlast Mobile helps protect you from vulnerabilities and attacks that put data at risk.

HIGHEST LEVEL OF MOBILE SECURITY FOR THE ENTERPRISE

Advanced app analysis

You can trust your employees to access your sensitive business assets, but can you trust their apps? SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation, and machine learning. The solution captures apps as they are downloaded to devices, and runs each in a virtual, cloud-based environment to analyze its behavior before being approved or flagged as malicious. Easy to understand, exportable analysis reports help your security teams ensure apps employees use are safe.

Device vulnerability assessments

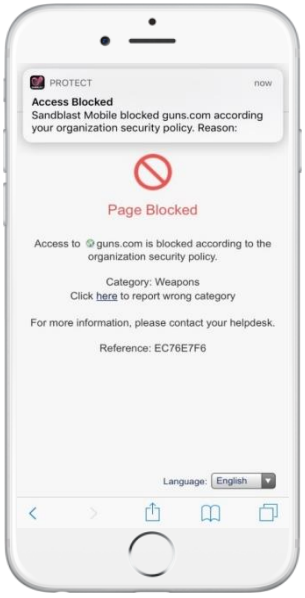
Cybercriminals make it their business to know the weakest link in your security before you do. That often includes weaknesses in operating systems and apps that other security solutions may not detect. Our solution uses real-time risk assessments at the device-level (OS) to reduce the attack surface by detecting attacks, vulnerabilities, changes in configurations, and advanced rooting and jailbreaking. With better visibility into the threats mobile devices face, you can reduce the overall attack surface and risk.

November 14, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

Network-based attacks

SandBlast Mobile's unique network security infrastructure – On-device Network Protection – allows businesses to stay ahead of new and emerging Gen V threats by extending Check Point's industry-leading network security capabilities to mobile devices. The SandBlast Mobile application constantly validates cellular traffic on the device itself without routing the data through a corporate gateway. This ensures user and data privacy, allowing for a seamless browsing experience. SandBlast Mobile offers a broad range of network security capabilities, which include:



URL Filtering blocks access to website based on company's policy

Anti-Phishing: Blocks phishing attacks on all apps: email, messaging, social

Safe Browsing: Blocks access to malicious sites on all browsers based on the dynamic security intelligence provided by Check Point ThreatCloud™, the world's largest threat database.

Conditional Access: Blocks infected devices from accessing corporate applications and data, independent of UEM solutions

Anti-Bot: Detects bot-infected devices and automatically blocks communication to command and control (C&C) servers

URL Filtering: Prevents access to websites deemed inappropriate by an organization's corporate policies. It allows businesses to blacklist and whitelist websites in granular detail and enforce polices on mobile devices across all browser apps and on non-browser specific apps

Wi-Fi Network Security: Detects malicious network behavior and Man-in-the-Middle attacks, and automatically disables connections to malicious networks

Cellular Surveillance Protection

The global use of the SS7 protocol means that potentially every mobile phone user is exposed. Cellular network attacks allow hackers to target individual mobile devices and organizations to gain access to sensitive corporate data. SandBlast Mobile's cellular surveillance protection blade detects and mitigates sophisticated attacks that exploit cellular network vulnerabilities, such as SS7 attacks that include: hacking cloud services; call interception; and high-jacking SMS messages used for two-factor authentication. The cellular surveillance protection blade is an add-on capability for SandBlast Mobile.

FULL MOBILE VISIBILITY AND THREAT INTELLIGENCE

SandBlast Mobile's cloud-based dashboard makes managing supported devices and controlling mobile threats fast and easy. It provides your security and mobility teams with real-time threat intelligence and visibility into the quantity and types of mobile threats that could impact your business or users.

Centralized Threat Intelligence

ThreatCloud is the first and largest collaborative network to fight cybercrime. It is a knowledge base that delivers real-time, dynamic security intelligence. That intelligence is used to identify emerging outbreaks and threat trends. ThreatCloud powers the Anti-Phishing, Safe Browsing and URL Filtering technologies for SandBlast Mobile, by investigating malicious IP, URL, and DNS addresses. ThreatCloud's knowledge base is dynamically updated daily using feeds from a network of more than 100,000 security gateways and 100 million endpoints worldwide, Check Point research labs, and the industry's best threat intelligence feeds.

Check Point
SOFTWARE TECHNOLOGIES LTD.

WELCOME TO THE FUTURE OF CYBER SECURITY

DEPLOYING MOBILE SECURITY HAS NEVER BEEN EASIER

SandBlast Mobile is designed to secure mobile devices quickly and confidently through integration and cooperation with Unified Endpoint Management (UEM) solutions. This helps make the solution highly scalable, and delivers strong operational and deployment efficiencies for managing mobile security within a broader security infrastructure.

Deploy advanced mobile security with ease

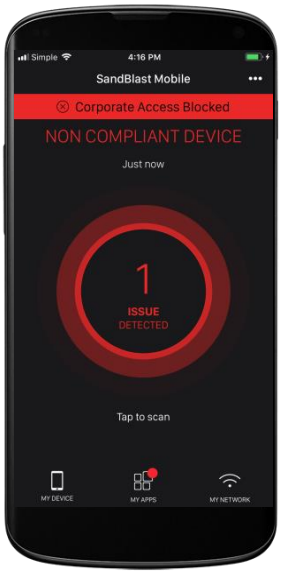
Integrating SandBlast Mobile with your UEM is fast and easy. Deployment and management can be done through your UEM automatically, accelerating adoption and reducing overall operational costs. The solution scales with your UEM, seamlessly protecting enrolled mobile devices.

Mitigate and eliminate threats right on the device

When a threat is identified, SandBlast Mobile automatically mitigates any risk until the threat is eliminated. Most threats can be eliminated on a device, without any user action or reliance on mobile device management platforms. Integration with your UEM platform allows the solution to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices that UEMs on their own can't make. SandBlast Mobile also activates an on-demand VPN to tunnel data traffic away from cybercriminals and to avoid data exfiltration while still keeping users connected.

Respect user privacy and device performance

End-user privacy is critical, so SandBlast Mobile never analyzes files, browser histories, or application data. The solution uses state and context metadata from operating systems, apps, and networks to determine if a device is compromised. It anonymizes the data it uses for analysis to keep it and security intelligence information separated. The analysis is performed in the cloud to avoid impacting device performance, and since protection runs in the background, users are protected without having to learn anything new.



Corporate access is blocked when device is at risk

Learn more:

www.checkpoint.com/mobilesecurity

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

November 14, 2018