WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT SANDBLAST MOBILE

SANDBLAST MOBILE AT-A-GLANCE

Product Benefits

- Complete threat prevention with market's best mobile catch rate
- Keeps assets and sensitive data safe from mobile breaches
- Seamless integrations with existing mobile and security solutions

Product Features

Advanced app analysis
Reverse engineers apps in a virtual, cloud-based environment to determine malicious behavior

Device vulnerability assessments
Analyzes devices to uncover vulnerabilities that cyber criminals can exploit

Network attacks prevention
Analyzes all networks and automatically disables connections to malicious networks

THE WORLD HAS BECOME MOBILE

Smartphones and tablets give us unprecedented access to the critical business information we need to work faster and more accurately. Providing employees with access to that information on mobile devices has many benefits, but it also puts businesses at risk, and exposes them to loss of sensitive information.

Check Point SandBlast Mobile prevents mobile threats before they start. Whether data is at-rest on a device or in-motion, SandBlast Mobile protects against vulnerabilities and attacks that put data at risk.

ENTERPRISE-GRADE MOBILE SECURITY

Protection from Malicious Apps

Check Point's unique Behavioral Risk Engine (BRE) runs applications in a cloud-based environment to scan for threats. The BRE uses machine learning and AI, sandboxing, advanced static code flow analysis, anomaly detection, and app reputation among other techniques to determine if an app is malicious. Additionally, in case the device is offline, there are on-device mechanisms to provide the same protections.

Every time a user downloads an app, they will see a detailed analysis of the app and its access privileges. SandBlast Mobile also blocks downloading apps from unknown sources or third-party app stores, relieving the dangers associated with sideloading apps.

Protection from OS and Device-based Risks

SandBlast Mobile uses real-time risk assessments of the device to reduce the attack surface by detecting attacks, vulnerabilities, changes in configurations, as well as advanced rooting and jailbreaking. With better visibility into these threats, administrators can granularly configure security and compliance policies for devices at risk.

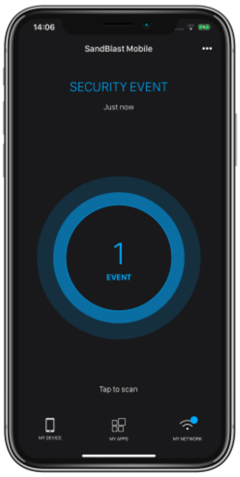
Protection from Network-Based Attacks

SandBlast Mobile's unique network security infrastructure – On-device Network Protection (ONP) – allows businesses to stay ahead of emerging threats by extending Check Point's industry-leading network security technologies to mobile devices.

The SandBlast Mobile app continually validates traffic on the device without routing data through a cloud or on-premise gateway. This ensures user and data privacy is protected, while allowing for a seamless browsing experience.

February 20, 2020

SandBlast Mobile offers a broad range of network security capabilities, which include:



Anti-Phishing with Zero-Phishing: Blocks phishing attacks across all apps, both from known and unknown zero-day phishing sites, and sites that use SSL

Safe Browsing: Blocks access to malicious sites from any web browser, leveraging the dynamic security intelligence provided by Check Point ThreatCloud™

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 servers

URL Filtering: Allows websites to be blacklisted and whitelisted, preventing access on any browser to websites deemed inappropriate by an organization's corporate policies

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

MARKET-LEADING THREAT INTELLIGENCE AND FULL MOBILE RISK VISIBILITY

SandBlast Mobile's cloud-based dashboard makes managing supported devices and controlling mobile threats fast and easy. It provides real-time threat intelligence and visibility into the mobile threats that could affect your business or users.

Powering the solution is Check Point ThreatCloud, the world's largest cyber intelligence network. ThreatCloud is dynamically updated daily with intelligence contributed by a network of more than 100,000 security gateways, 100 million endpoints, Check Point Research labs, and threat feeds from dozens of industry sources. ThreatCloud identifies both known and unknown threats and helps block phishing attacks, malware, and malicious Wi-Fi networks.

PRIVACY BY DESIGN AND BEST USER EXPERIENCE

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 in order to keep it protected. 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.

SANDBLAST MOBILE FITS IN YOUR CURRENT ENVIRONMENT

SandBlast Mobile supports any device-ownership program (BYOD, COPE), and integrates with any mobile management solution (UEM, EMM, MDM). This makes the solution highly scalable, and delivers operational and deployment efficiencies for managing mobile security within a broader security infrastructure. The integration with mobile or endpoint management solutions allows the solution to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices that UEMs can't deliver. SandBlast Mobile also integrates with SIEM solutions such as ArcSight and Splunk, and fully supports Android Enterprise deployments.

Enabling a secure mobile workforce has never been easier!

Learn more: checkpoint.com/mobilesecurity

February 20, 2020