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

VERISTOR
Brought to you by Veristor
veristor.com | contact@veristor.com

# SANDBLAST APP PROTECT

## SECURITY INFRASTRUCTURE FOR YOUR MOBILE APPS

### WHY SANDBLAST APP PROTECT

- **Mobile users do careless things that can compromise the security of their apps**. They can expose their apps to compromise by installing malicious apps, authorize vulnerable device configurations, expose themselves to privilege escalation by jailbreaking or rooting their devices, or fall prey to Man-in-the-Middle traps. In order to prevent compromise to your mobile app, you need to understand the environment in which your app is running.
- **Mobile security is not a DIY project** – it requires specialized skills and expertise
- **Security is not a one-time effort** – protections against new vulnerabilities and attack vectors need to be adapted in real-tin
- **Mobile security should be part of your application infrastructure** – just like authentication and authorization, analytics, storage, etc.

SandBlast App Protect provides mobile security as a standard development tool, so businesses can ensure that mobile application security is expertly implemented and maintained over time, and so app developers can focus on releasing new product features instead of becoming security experts.

## SECURING MOBILE APPS

In the new digital era, providing customers with the needed mobile services to perform operations from the comfort of their mobile devices is key. However, mobile devices are controlled by users that are not always security minded, and businesses don't always have the needed security infrastructure to protect their mobile apps. As a result, attackers are increasingly focusing efforts on the mobile channel to carry out fraud, harvest credentials, and gain unauthorized access to sensitive data.

## A SECURITY INFRASTRUCTURE FOR YOUR MOBILE APPS

With SandBlast App Protect, mobile developers can secure their iOS and Android customer-facing apps with an easy to integrate SDK. The SDK effectively detects both known and unknown threats, including malicious apps like keyloggers or banker malware that may be present on the device, vulnerabilities in the operating system, Man-in-the-Middle attacks, or tampering attempts to your mobile app. As a result, the application is able to understand the environment in which it is operating, assess its risk, and prevent compromise of data.

SandBlast App Protect enables companies to take their apps' security into their own hands. Instead of relying on users to be careful and implement security measures on their mobile devices, the application itself detects and prevents relevant threats.

## HOW IT WORKS

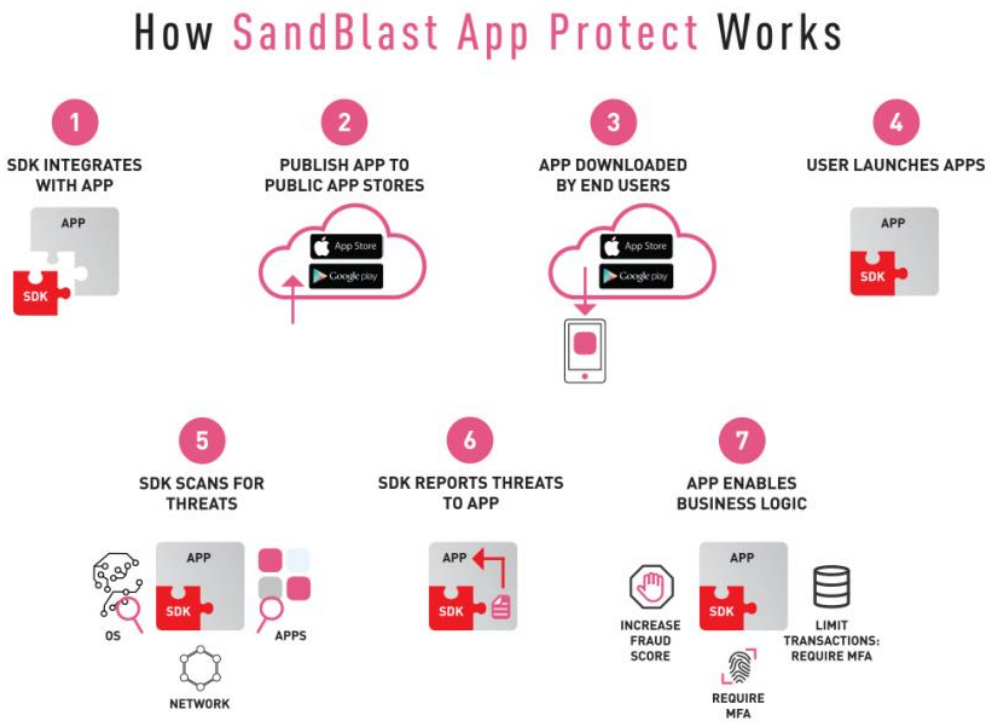
SandBlast App Protect is architected as a combination of on-device and cloud-based capabilities. On-device capabilities enable the detection of device vulnerabilities, including advanced jailbreak/root, vulnerable configurations, iOS malicious profile detection, Man-in-the-Middle attacks, mobile malware and tampering attempts. Cloud-based capabilities deliver malicious app detection using advanced threat prevention technology, while ensuring that resource intensive analytics are not taxing device performance. Advanced app analysis includes static code flow analysis, dynamic analysis (application sandboxing), and machine learning – all provided by Check Point's Behavioral Risk Engine (BRE). Underpinning both on-device and cloud-based capabilities is Check Point's market-leading threat intelligence delivered via ThreatCloud.


April 1, 2020

The list of threats and risk indicators identified by on-device and cloud-based analysis is shared with the host app, at both a high level (threat category) and at a granular level (threat factor).

Granular policy controls enable app owners to maintain a good balance between user experience and security. For example, one might choose to ignore a late software update and not restrict the user's access to an app, while wiping locally stored data when a device is jailbroken or rooted, or alerting a user when a banking Trojan is installed.

SandBlast App Protect fully preserves user-privacy as all sensitive security analytics are performed on-device and no private data is ever analyzed or collected.




## ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

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