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

FORTIFY 24x7
Cybersecurity Managed™

SandBlast App Protect

Security infrastructure for your mobile apps

Why SandBlast App Protect

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 business features instead of becoming security experts.

1. Mobile security is not a DIY project – it requires specialized skills and expertise
2. Security is not a one-time effort – new vulnerabilities and attack vectors need to be constantly researched and protections adapted in response
3. Mobile security should be part of your application infrastructure – just like authentication and authorization, analytics, storage, etc.

SECURING MOBILE APPS

Mobile devices are ubiquitous, hard to protect and controlled by users that are not always security minded. 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.

Mobile users will do careless and foolish things that will compromise the security of their device. They will expose their device to compromise by installing malicious apps, authorize device configurations that make them vulnerable to attack, expose themselves to privilege escalation by jailbreaking or rooting their devices, enable malicious profiles to be installed, or fall prey to man-in-the-middle traps. So in order to prevent compromise to your mobile service, you need to understand the environment in which your app is running.

Mobile devs are not necessarily security experts. And even if they were, they don't always have the time to implement proper security. Businesses therefore need to provide mobile developers with security tools to help them build and deploy better protected applications, quicker.

Security is not a one-time effort and requires continuous research and update. New software and hardware vulnerabilities are being discovered at an accelerating pace. Attackers are continuously innovating the way they attack. So to effectively secure a mobile app, you need professional threat research capabilities to anticipate attackers' next move, and a security solution that can quickly adapt to prevent new threats.

Your mobile channel needs a security infrastructure to protect it. As most business applications benefit from the protections provided by a professionally built and managed security infrastructure – i.e. Web applications are protected by web application firewalls (WAF) and internal applications are protected from outside threats by UTMs - mobile applications require similar security infrastructure to protect them.

A SECURITY INFRASTRUCTURE FOR YOUR MOBILE APP

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 host operating environment, man-in-the-middle attacks, and more. As a result, the application is able to understand the environment in which it is operating, assess its risk, and prevent compromise.

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 prevent relevant threats.

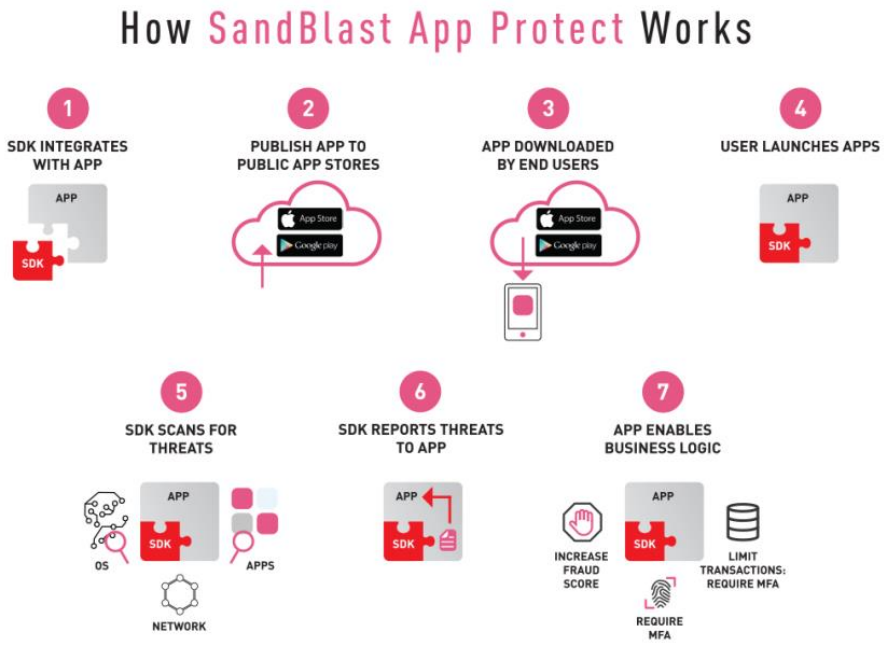
July 21, 2019

HOW IT WORKS

SandBlast App Protect is architected as a combination of on-device and cloud-based capabilities that deliver effective and up-to-date prevention, performance, and user privacy. On-device capabilities enable the detection of device vulnerabilities that can be exploited to carry out an attack, including advanced jailbreak/root detection, vulnerable device configurations, iOS profile detection, man-in-the-middle traps, and more. Cloud-based capabilities deliver highly-effective 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). And underpinning both on-device and cloud-based capabilities is Check Point's market leading threat intelligence delivered via ThreatCloud.

Risk indicators identified by on-device and cloud-based analyses are summarized in a risk-score that is shared with the hosting app. 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 preserves user-privacy by preventing privacy-compromising attacks on users, and by ensuring that all sensitive security analytics are performed on-device and that no private data is analyzed or collected.



ABOUT CHECK POINT

Underpinning SandBlast App Protect is Check Point's market leading threat research, intelligence, and prevention technologies, working to ensure the industry's highest threat catch rate[i] for known and zero-day threats.

To purchase or being a 30 day trial of the software, please reach out to Fortify 24x7 at (800) 989-2647 or info@fortify24x7.com