appdome

Stop Mobile Threats with Appdome for Check Point SandBlast App Protect

No-code, Instant Protection for all Android and iOS Apps

THE CHALLENGE OF SECURING MOBILE APPS

Mobile apps are ubiquitous, they live in uncontrolled and sometimes hostile environments. Mobile apps also contain sensitive and valuable data. Attackers are increasingly focusing their efforts on the mobile app as the first place to carry out attacks, harvest credentials, and gain unauthorized access to sensitive data. At work, vendor provided apps that scan-to-protect the device, can be used to protect users and data from mobile threats. But, this works only if the user agrees to download and install the security vendor's app and keeps that app turned on. In the consumer world, app makers simply cannot require a separate scan-to-protect app to provide mobile threat defense. Consumers demand mobile threat defense built into each app, a step that places a large burden on mobile app developers.

APPDOME FOR CHECK POINT SANDBLAST

Appdome for Check Point SandBlast App Protect (SBAP) eliminates the complexity of mobile threat defense in the enterprise and in consumer apps. Using Appdome, enterprise IT and mobile developers can instantly build Check Point's mobile threat defense service into iOS and Android apps in seconds, without coding the SDK into the app.

Check Point SBAP protects against known and unknown mobile threats, including malicious apps, Man-in-the-Middle, keylogging, mobile malware, OS vulnerabilities, command & control exploits, and more. By adding the SBAP SDK to mobile apps on Appdome, mobile applications are upgraded to recognize threats, assess risk, prevent compromise.

DON'T CODE MOBILE THREAT DEFENSE

Manually coding any mobile threat defense solution, including Check Point SBAP, requires months of highly specialized developers and lots of trial and error. Instead of that, let Appdome's NeverForget ™ AI-coding engine build the full SBAP SDK into any mobile app in seconds, without any pre-requisites, learning curve, or manual effort. Appdome doesn't require specialized expertise in security or app development, allowing Check Point customers to implement the SDK using existing staff into 1 or 1000s of mobile apps simultaneously.

FAST, EASY & SELF-DEFENDING PROTECTION

Appdome is the best, fastest, and easiest way to protect Android and iOS apps with Check Point SandBlast App Protect. Appdome is a self-service, SaaS platform that's easy to use. Simply upload any app binary (.apk or .ipa) to your account, select the SBAP SDK, and click "Build my App." Appdome is compatible with all mobile apps; native, non-native and hybrid. And because Appdome doesn't require source code, customers can easily protect all mobile apps with SBAP - internally developed & 3rd party apps.

Appdome for Check Point SandBlast App Protect is also self- defending, meaning the implementation is protected from the ground up from tampering, altering, reversing and other hacking attempts designed to disable the SBAP service inside apps. No other method on the market today, can add the SBAP SDK in seconds and protect SandBlast App Protect from alteration inside apps.

TOP BENEFITS OF APPDOME FOR CHECK POINT SANDBLAST APP PROTECT

Instant Mobile Threat Defense	Use Appdome's NeverForget™AI-coding engine to accelerate mobile threat defense and build Check Point SandBlast App Protect into Android and iOS apps, without any development experience or coding.
100% App Coverage	Appdome for Check Point SandBlast App Protect is compatible with any native, hybrid or non-native Android or iOS apps, including Xamarin, Cordova, React Native, Flutter, etc. out of the box. No plug-ins, special SDKs or coding prerequisites.
Protection Against Top Mobile Threats	SandBlast App Protect uses threat data to detect and defend against: Advanced Jailbreak/ Root, Device Misconfigurations, Known and Unknown Malware, Malicious Profiles , MitM Attacks, Debuggers, Emulators and Hooking Frameworks.
Self-Defending App and MTD	Appdome for Check Point SandBlast App Protect is self-defending and self-protecting. It comes with advanced app shielding, anti-tampering and protection from reverse engineering, ensuring that both the App and the MTD cannot be changed or compromised.
Easy Repeatable MTD Outcomes	Appdome for Check Point SandBlast App Protect is easy to use and completely no (zero) code. Eliminate SDK integration, framework dependencies, building secure stores and more. Templates allow users to simplify and scale MTD projects to dozens or 100s of apps quickly and easily.

UPGRADE PROTECTION WITH APPDOME MOBILE APP SECURITY

Complement Check Point SandBlast App Protect with Appdome's comprehensive, no-code mobile app security suite.

Appdome's mobile app security suite provides mobile data encryption, native and non-native code obfuscation, secure communication, OS integrity and more.

Use Appdome to instantly stop hacking attempts, static and dynamic analysis tools and more, all without coding a thing.

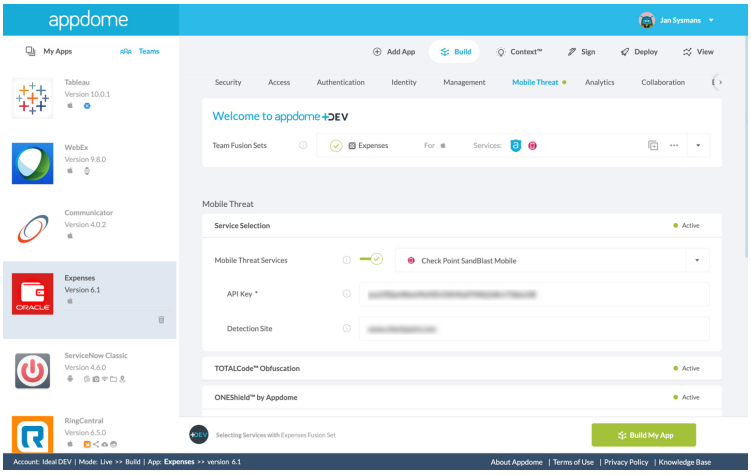

Image: Implement the Check Point SandBlast App Protect SDK without coding on Appdome

Learn more about Appdome for Check Point SandBlast App Protect at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

ABOUT APPDOME

Appdome changes the way people build mobile apps. Appdome's industry defining no-code mobile solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new security, authentication, access, enterprise mobility, mobile threat, analytics and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 150+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles. For more information, visit www.appdome.com.

*Yehuda et al. Method and system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.