MOBILE SECURITY SUITE: APP SHIELDING & RASP

Defeat mobile application attacks with complete protection from the inside out

Businesses develop and market their own mobile apps at a feverish pace, driving a significant increase in the attack surface and related fraud. At the center of this threat are hackers who release malware exploiting mobile OS vulnerabilities. Runtime Application Self-Protection (RASP) and App Shielding by OneSpan equip businesses with strong, natively integrated app security that dynamically detects and mitigates these attacks.

Secure sensitive data

RASP and App Shielding by OneSpan proactively protects against zero-day and other targeted attacks, allowing mobile business apps to run securely, blocking the foreign code from working or shutting down the application if a threat to data exists. Integrating RASP and App Shielding into mobile apps ensures the complete integrity of the apps and fully protects sensitive business and personal data from cybercriminals.

Integrated protection

RASP wraps around the application code to protect against foreign code injection. Even if a device becomes infected with malware, including system components such as screen-reader or key logging on Android, RASP technology will detect and prevent that code from running.

Strengthen application security

RASP provides an extensive list of features that are easy to integrate and invisible to the end user. As a result, RASP allows businesses to extend and strengthen application security, protect customers and meet aggressive application development timelines.

Mobile Security Suite

RASP is available as an optional feature in OneSpan Mobile Security Suite. OneSpan Mobile Security Suite provides the most extensive list of features that seamlessly integrates identity/authentication, application protection, secure communications and electronic signing into almost any mobile application.

Runtime Application Self-Protection includes:
- Overlay Detection
- Jailbreak & Root Detection
- Active Memory Zeroing
- Secure Storage + Device Binding
- Anti-Code Injection
- Anti-Key Logging
- Anti-Screen Reader
- Anti-System Screen shots
- Anti-Screen Mirroring and External Monitors
- Anti-Re-Packaging Protection
- Debugger & VM Debuggers Prevention
- Runtime Protection– Integrity Check
- Emulator Detection
- Obfuscation
How it works

RASP ensures the integrity of mobile apps in three ways: Protect, Detect and React. It protects the trusted mobile application by preventing reverse engineering techniques via code obfuscation and anti-repackaging technology.

It actively detects malicious key logging, screen readers, repackaged applications, debuggers and emulators, and jailbroken or rooted devices. It can then react to prevent screenshots, block screen duplication, or enable customized actions based on business policy (i.e. Application shut down).

TECHNICAL SPECIFICATIONS

**iOS**
- RASP supports iOS as of version 6.0 that needs to be linked to a host application. The framework is currently provided for the following architectures:
  - armv7
  - armv7s
  - arm64
  - i386
  - x86_64

**Android**
- RASP supports Google Android 2.3 and later. The following CPU architectures are currently supported:
  - armeabi
  - armeabi-v7a
  - armeabi-v8a
  - mips
  - x86
  - x86_64