AppProtect+

AppShield+

Evaluated Mobile App Security – More Features & Stronger Shield

Proven Platform for Securing Mobile Apps

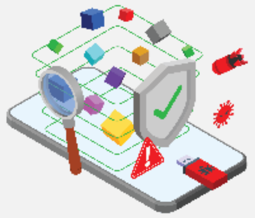
AppShield, a core module of the **AppProtect+ Suite**, delivers a comprehensive mobile application security using a **Detect–Protect–Respond** framework.

Going beyond traditional **Runtime Application Self-Protection (RASP)** solution, it takes mobile app security further by safeguarding both the code and the environment level, ensuring real-time protection even on rooted or compromised devices.

AppShield isolates mobile apps from risky environments, detects tampering, prevents reverse engineering, and responds instantly to block malicious activities, ensuring continuous in-app protection during execution time.

Supports iOS, Android and HarmonyOS NEXT

Key Features



Threat Protection

Protects against static, dynamic, and run-time attacks – including tampering, reverse engineering, malware injection, emulators, and debuggers - to maintain app integrity even in compromised environments.

Stronger Source Code / IP Protection

Uses code obfuscation and hardening to conceal an app's logic, making it difficult for attackers to find vulnerabilities or extract sensitive data, without affecting functionality.

Secure Execution Environment

Offers a highly secure approach that goes beyond file-level encryption by using method-level encryption, or control flow obfuscation, to ensure sensitive information and confidential business logic are never exposed.

Simple Post Compilation Deployment

Supports a post-compilation, self-contained shielding approach that eliminates dependency on server components for ease of deployment and our strong app binding technology prevents the by-pass of our app protection technology.

Core Capabilities

DETECT

Identify Runtime Attacks and Monitor App Integrity

Environment Checks
prevent apps from running in debugger, Jailbreak, Rooted, and Emulator environment

Runtime Integrity Monitoring
ensure apps are free from tampering, alteration, Emulator environment exploits, and Hooking framework attacks

Keylogger Protection
eliminate data leakage due to keylogging malware

Screen Capture Detection & Blocking
fend off data leakage from screen-capturing malware

Screen Mirroring Detection & Blocking
stop remote control malware and data leakage

PROTECT

Prevent Malicious Access, Tampering and Data Theft

Code Obfuscation
block reverse engineering and exposure of critical business logic

App & Device Binding
restricts execution to verified devices within secure environments

Repackaging Detection
forbid apps that have been tampered with from execution

Secure Communication
encrypts all data exchanged with severs and local apps

Secure Execution Environment
safeguard sensitive data, functions, code within an isolated environment

Whitebox Cryptography
protect cryptographic keys and algorithms within apps to keep data secure

RESPOND

Counter Attacks with Real-Time Defensive Reactions

App Shutdown or Fail - Safe Exit
configure actions to execute when threats are detected

Customizable Response
tailor in-app responses based on specific risk scenarios

Alert & Reporting
sends real-time alerts to SIEM platforms or delivery mechanisms

Malware Scanning
highlight malware detected based on the configurable malware policy

OTA Updatable Configurations
implement updated security policy without recompiling or republishing

Air - Gapped Environment
secure mobile apps on offline devices

Global Headquarters
Blk 750D Chai Chee Road #08-01
ESR BizPark@Chai Chee (Lobby 1)
Singapore 469004
☎ +65 6244 3900
✉ enquiry@i-sprint.com

For a complete list of our offices in
Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus

Scan for more information

www.i-sprint.com iSprintInnov iSprintInnov company/i-sprint-innovations

i-Sprint Trust without Boundaries