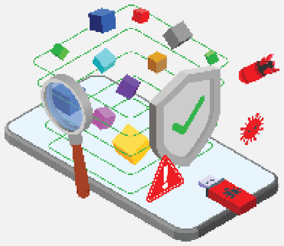
AppProtect+

AppShield

Real-Time Mobile App Security

AppProtect+ AppShield is an advanced Runtime ApplicationSelf-Protection (RASP) solution that defends mobile apps in real time—even on rooted or compromised devices. Compatible with iOS, Android, and HarmonyOS NEXT, it isolates apps from risky environments, detects tampering and reverse engineering, and blocks malicious activity instantly. Key features include code obfuscation, integrity checks, secure app binding, and offline protection without relying on cloud updates.

Key Features

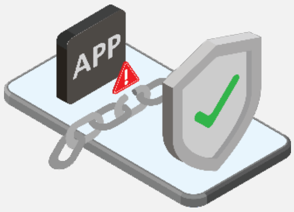


Run-Time Threat Protection

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.

Code 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.



App Data Protection

Secure sensitive app data using encrypted Secure Dynamic Data (SDD) and Secure Static Data (SSD), even on jailbroken or rooted devices.

App Repackaging Prevention

Detects and prevents unauthorized clones or altered versions from being published on official app stores.

Core Capabilities

DETECT

Identify Runtime Attacks and Monitor App Integrity

Debugger Detection

Jailbreak Detection

Root Detection

Emulator Detection

Environment checks to ensure app runs safely.

Checksum

Hook Detection

App Integrity Check

Runtime integrity monitoring to ensure app is not altered or tampered with.

PROTECT

Prevent Malicious Access, Tampering and Data Theft

Code Obfuscation
to prevent reverse engineering

App Binding
to ensure app runs only in trusted environment

Repackaging Detection
to prevent modified or unauthorized apps

Secure Application Communication
with TLS pinning and client authentication

Encrypted Data Storage
for added protection

Whitebox Cryptography
to secure operations on exposed devices

App Management
to ensure trusted relationship between user, app, and device

RESPOND

Counter Attacks with Real-Time Defensive Reactions

App Shutdown or Fail - Safe Exit
when threats are detected

Custom Reactions
based on specific threat scenarios

Alert & Report
issues to security teams promptly

Anti-Keylogger Protection
by blocking screen readers

Screen Capture Detection & Blocking
for data protection

Screen Mirroring Detection & Blocking
to stop data leaks

Brute Force Protection
to prevent decryption of data

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 f iSprintInnov X iSprintInnov in company/i-sprint-innovations

i-Sprint
Trust without Boundaries