YESsafe AppProtect+

Runtime Mobile App Protection

App Shielding | Code Protection | Android, iOS & HarmonyOS App Protection

YESsafe AppProtect+ detects and protects the mobile app from threats, such as reverse-engineering, tampering, code-injection and more. In an insecure OS environment, apps integrated with YESsafe AppProtect+ have rooted and jailbreak detection mechanisms that allow a mobile app to operate securely without compromising the app's integrity and confidentiality. Protecting apps even in the absence of an internet connection or without an updated virus database, AppProtect+ protects mobile apps against static and dynamic attacks (e.g. repackaging, source code modification), and respond by taking necessary measures when real-time attacks are detected. Moreover, AppProtect+ is EMVCo SBMP certified. An EMVCo certified app solution ensures that mobile apps can withstand real-time threats and attacks.

3 Core Functions

App Shielding

- Protect your app against static and dynamic attacks, preventing tampering, reverse engineering and malware attacks
- Detects and prevents real-time attacks. App shielding protects your app in any environment, including an untrusted environment

Code Protection

- Code obfuscation conceals the logic and purpose of an app's code, making it harder for an attacker to find vulnerabi lities and retrieve sensitive app data
- Code hardening renders your code illegible without affecting its functionality, making the app more resistant to reverse engineering and app tampering, protecting against intellectual property theft, loss of revenue and possible reputational damage.

App Data Protection

- Secure Local Storage (SLS) - a security feature that enables the storage of sensitive app data (e.g. session tokens, API keys) locally on the end-user devices in a secure and encrypted manner, even on rooted/ jailbreak devices
- Secure Application ROM (SAROM) - Protects fixed assets inside your app, such as certificates and API keys. With SAROM, assets are automatically encrypted during shielding and only decrypted at application runtime when needed by the application code

Integrated with AccessMatrix, YESsafe AppProtect+ responds promptly to any risk detected on the client side. Fulfilling app protection, risk detection and respond actions requirements, providing the complete app protection cycle.

Protection

Prevent Malicious

- ✓ Code obfuscation
- ✓ App Binding
- ✓ Repackaging detection
- ✓ App communication
  - › TLS certificate pinning
  - › Client certificate authentication
- ✓ Storage of encrypted data
- ✓ Binding the data to be encrypted to the device
- ✓ Whitebox cryptography
- ✓ App Management Solution
  - › Trusted binding between user, app and device
  - › Ensuring app is trusted and legitimate
  - › Registration / activation – securely pair the app / device with the user

Detection

Detect Runtime Attack

- ✓ Ensure app is running in safe environment
  - › Debugger detection
  - › Jailbreak / Root detection
  - › Emulator detection
- ✓ Ensure app is not altered or tampered with (e.g. by malware) at runtime
  - › Checksum
  - › Hook detection
  - › App integrity check

Respond Action

Counter Attack

- ✓ Shutdown (Exit / Fail)
- ✓ Custom reactions
- ✓ Screenshot detection / blocking
- ✓ Anti-keylogger
  - › Blocking screen readers
- ✓ Alert / reporting
- ✓ Screen mirroring detection/ blocking
- ✓ Prevent brute force decryption of sensitive data

All-Round Protection

Code Injection

Prevent hackers from modifying code and changing the course of execution, resulting in data loss or even a complete host takeover.

App Repackaging

Prevent repackaging of applications and imposter from publishing repackaged apps in official app stores.

Emulators & Debuggers

Protect applications from attackers using emulators and debuggers with intention to intercept data before it is encrypted.

Reverse Engineering

Multiple layers of security check to hinder any reverse engineering attempts.

Jailbreak/ Rooted Devices

Automated detection of jailbroken and rooted devices, ensuring app is executed the way you configure it to be.

Runtime App Self-Protection (RASP)

- AppProtect+ isolates applications from the runtime environment to proactively scan and protect mobile apps against malicious attacks, allowing apps to run securely even on rooted/ jailbreak devices. E.g. upon detection of the presence of an untrusted screen reader, AppProtect+ blocks the screen reader from receiving data from the protected app.
- The uniqueness of AppProtect+ lies in the ability to detect risks even in the absence of an internet connection. AppProtect+ can avoid possible risks caused by a desynchronized database.

Secure Android, iOS and HarmonyOS Applications

Global Headquarter
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
China, Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus