YESsafe AppProtect+

Runtime Mobile App Protection

Code Injection
Screen Reader
Debugger
Keylogging
Screenshot
App Repackaging
Jailbreak Root Detection
Emulator Execution
Code Logic Leakage

App Scanning | App Shielding | App Protection | App Usage Insight

YESsafe AppProtect+ provides vulnerability scanning service for apps, to detect security weaknesses such as hardcoded sensitive information that uses unsecured HTTP links. YESsafe AppProtect+ will also detect and protect mobile apps from a variety of threats, such as reverse-engineering, tampering, code-injection and more. In an unsecured OS environment, apps that have been integrated with YESsafe AppProtect+ will now have rooted and jailbreak detection mechanisms that allows the app to operate securely without compromising the app's integrity and confidentiality. These AppProtect+ shielded apps can even function securely in the absence of an internet connection or without an updated virus database. On top of that, AppProtect+ also 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. AppProtect+ has a build-in audit mechanism that allows auditor to easily review all apps shielding statistics, whilst the attack insight dashboard identifies and provides the user with alerts and critical information that their apps are facing in real time. Moreover, AppProtect+ is EMVCo SBMP certified. An EMVCo certified app solution ensures that mobile apps can withstand real-time threats and attacks.

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

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 vulnerabilities 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 Dynamic Data (SDD)- 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 Static Data (SSD)- Protects fixed assets inside your app, such as certificates and API keys. With SSD, assets are automatically encrypted during shielding and only decrypted at application runtime when needed by the application code.

App Scanning

- Scans the app and provide the user with a report highlighting any weaknesses and vulnerability found for the user to review and improve on.
- Checks the app's vulnerability against of the latest list of software and hardware weaknesses database compiled by leading open-source security communities such as OWASP and CWE.

App Pulse+

- **Application threat alarm and analysis :** Real-time collection of security threats detected by the application and its operating environment, and provide alarm information, including threat event type, device model, system version, time of occurrence, etc.; and other historical information can be combined on the statistical dashboard Overall analysis.
- **Application data collection and analysis :** Including user distribution, user participation, function usage and performance indicators, etc. Application owners and enterprises can easily understand the application usage status by querying the dashboard or customizing statistical reports, keep abreast of user dynamics, and help control the direction of business development.

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.

Mobile App Vulnerability Scan

PROTECT

Protect against compromise

- ✓ Code obfuscation
- ✓ App binding/Code injection prevention
- ✓ Resource verification
- ✓ Store data encrypted inside the app
- ✓ Binding the data to be encrypted to the device

Mobile App App Protection

DETECT

Detect Attack at Runtime

- ✓ Jailbreak / Root detection
- ✓ Repackaging detection
- ✓ 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
  - › Screenshot prevention
  - › Untrusted Keyboard detection
  - › Accessibility service detection

Mobile App Usage Information

REACT

Counter Attack

- ✓ Configurable actions
  - › Shutdown (Exit / Fail)
  - › Redirect user to the specific URL
- ✓ Custom reactions
  - › Data gathering at server side
  - › Alert / reporting
  - › Risk based contextual authentication

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.

About i-Sprint Innovations

i-Sprint Innovations (i-Sprint) established in the year 2000, is a leading provider in Securing Identity and Transactions in the Cyber World that enables individuals, organizations, and societies to build trust and identity assurance for powering productivity gain through digital identity and identity of things (IDoT).

i-Sprint's unique brand of security products, intellectual properties, and patents are designed to exceed regulatory requirements such as global financial services. By incorporating the latest mobility/ biometrics/ cloud/ identification technologies, i-Sprint provides solutions that ensure secure access and protection of data, transaction and assets. i-Sprint delivers trusty, versatile and strong authentication, and identity management platform to secure multiple application delivery environments based on a common security platform.

i-Sprint's digital identity product offerings include adaptive authentication (biometrics, multifactor authentication and more), single sign-on services, end-to-end encryption (E2EE) authentication and data protection for transaction data and to secure access to the web, mobile, and cloud-based applications. i-Sprint's IDoT product offerings provide the next-gen anti-counterfeiting, track and trace, and interactive consumer engagement that aims to help business in building consumer trust, improve brand protection, personalize consumer engagement and provide business intelligence.

i-Sprint's clients include leading global and regional financial service institutions, government agencies, telecommunications, public utilities, manufacturing, healthcare, education, multi-national corporations and others. Currently, i-Sprint has a direct presence and active authorized partners across Singapore, China, Hong Kong, Taiwan, Malaysia, Thailand, Japan and the United States.

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