Mobile App Security Hardening | IRONWALL

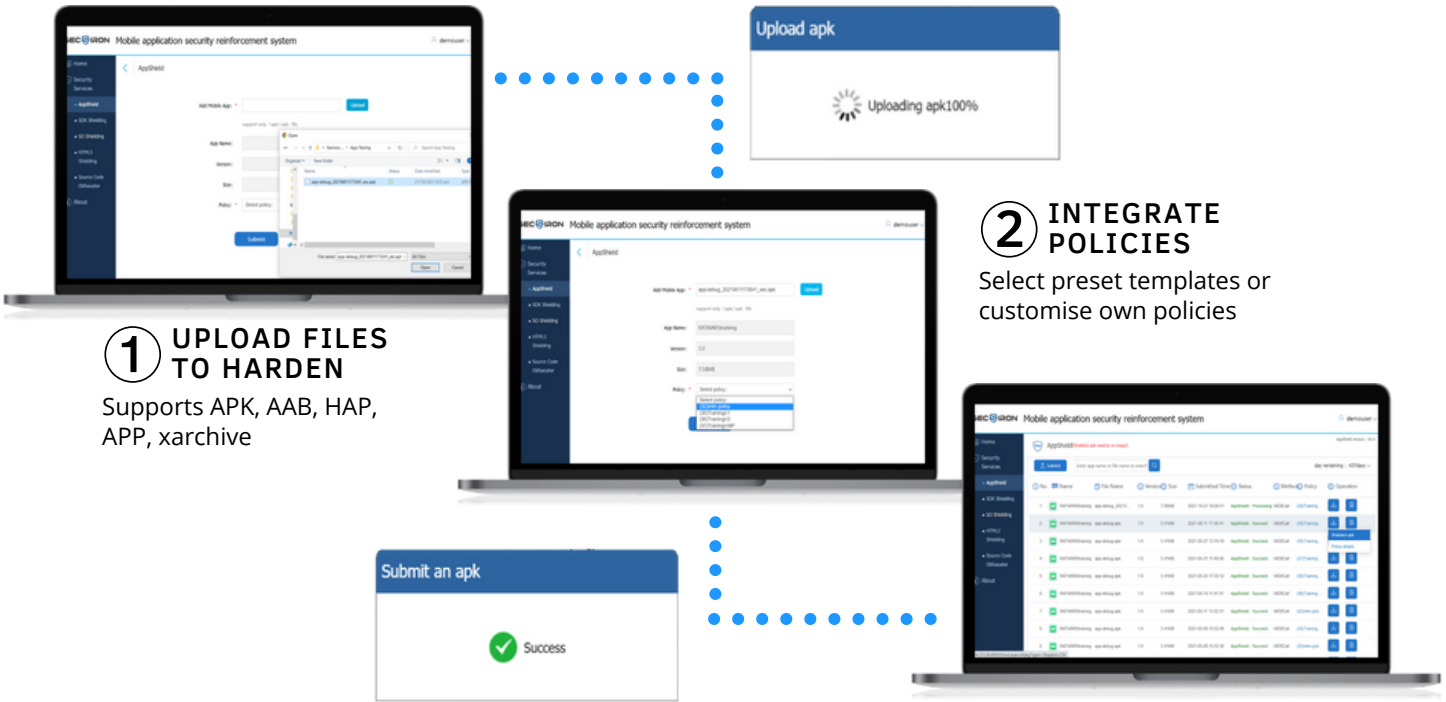
DEFEND & PROTECT WITH THE LATEST IN VIRTUAL MACHINE PROTECTION (VMP) TECHNOLOGY THAT EFFECTIVELY MINIMIZES ATTACK SURFACES EXPOSURE.

Highlights

ULTIMATE PROTECTION	UNINTERRUPTED USER EXPERIENCE	COMPLIANCE READY	CODE-LESS INTEGRATION
Best solution to fight against malware, injections, app tampering and more.	Security policies that protects without compromising user experience and performance.	Off the shelf security policies that meets regulatory standards.	Reduce development efforts for integration with newer security options through a simplified platform.

Digitalization of business and services, which has grown rapidly since 2020 has changed the way people do business, shop and interact with each other. This change dramatically impacts the security posture of mobile applications and data. There is no doubt that consumers want to use new and exciting applications, but the effectiveness of this development is challenged by the risk of data breaches and cyber-attacks that can leave users vulnerable to identity theft or financial losses. The success of mobile app security is driven by its ability to detect and prevent data breaches and cyber-attacks. The requirements for a more secure tools and solutions for both data and application security will be fundamental in the coming years. And the need for a higher level of security on data and applications will be on top of the agenda.

Code-Less Security Integration For Simplification



1 UPLOAD FILES TO HARDEN

Supports APK, AAB, HAP, APP, xarchive

2 INTEGRATE POLICIES

Select preset templates or customise own policies

3 DOWNLOAD HARDENED APP

business@seciron.com www.seciron.com

IronWALL provides a dynamic application security layer that allows enterprises to easily build secure business-critical applications.

APPLICATION HARDENING & PROTECTION

ANTI-STATIC CRACKING TECHNOLOGY

- ANTI-REVERSE ENGINEERING
- DEX FILE SHIELDING
- DEX CLASS EXTRACTION - SHIELDING
- VIRTUAL MACHINE - PROTECTION (VMP)
- SO. AND LIBRARY FILE - PROTECTION
- DATA FILES ENCRYPTION
- SOURCE CODE OBFUSCATION
- STRING ENCRYPTION

ANTI-DYNAMIC ATTACK TECHNOLOGY

- ANTI-DEBUGGING
- ANTI-ROOT/JAILBREAK
- ANTI-TAMPERING (HOOK & INJECTION)
- ANTI-INTERFACE HIJACKING
- FRAMEWORK SOFTWARE DETECTION AND PREVENTION
- ANTI-EMULATOR

Defend Applications Against Known & Unknown Threats

CORE CODE THEFT

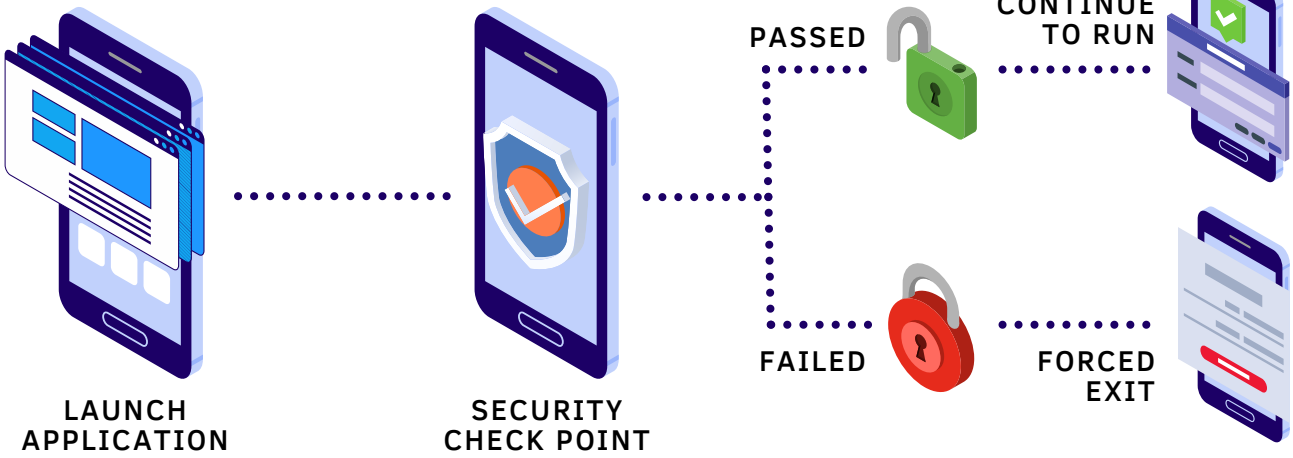
MALICIOUS CODE INJECTION

API INTERFACE EXPOSURE

PROGRAM LOGIC CRACKING

Securely Deploy Apps & Improve User Experience

IronWALL application hardening prevents the application to run in the event of failed security policy checking, and the application is isolated from the platform. This approach prevents attackers from successfully installing malware or malicious code on the device during runtime, and thereby eliminates the risk of the occurrence of an attack (e.g., zero-day attack). In addition, it prevents leakage of sensitive data from the device due to a failed security policy check.



business@seciron.com
www.seciron.com

Total Security Solutions To Mitigate Potential Attacks On Your Mobile Application Software Against Threat Actors.

- **Protect Business-Critical Applications**
  From external threats such as malicious code injections and script kiddies from client side attacks that tampers the apps business logic.
- **Real-Time Protection**
  Against known exploits, reducing the impact of zero-day attacks.
- **Reduces The Risk of Data Leakage**
  By preventing memory dump by encrypting critical files, processes, and reducing the risk of spyware infection on business-critical mobile applications.
- **Leverage On Multiple Layers of Protection**
  Detects latest malware attacks by checking not only the signature but the behavior and tactics of the attacks with next-generation behavioral detection and attack blocking.
- **IP Protection**
  Shielding the core code of the mobile app and SO files, preventing the Intellectual Property (IP) from theft.
- **Reverse Engineering Prevention**
  Reducing the chance of the app from being tampered by increasing the difficulty level of reverse engineering and code analysis.
- **Meet Global Standards**
  Maintain compliance with federal laws, corporate policy, contractual obligations, information security standards, industry practices, and acceptable use policies.

Prevent Risk of Unprotected Codes

IronWALL uses 3 layer of technologies to protect the source code without compromising the performance of your app. IronWALL signature protection - Virtual Machine Protection (VMP) virtualizes the code to be an unreadable format, making it difficult for hackers to analyze the code and find vulnerabilities from there. IronWALL protects a wide range of different applications, be it Android, iOS, Harmony OS application to native app, hybrid app and SDK.

Runtime Application Protection

IronWALL application hardening platform minimizes security risks during application runtime. By preventing the application to run in the event of failed security policy checking, IronWALL eliminates security breaches caused by failed access controls in applications. IronWALL gives you the power to enforce a large number of security policy checks on your applications without compromising their performance or functionality.

Low Risks Environment and Compliancy

Application hardening enables you to achieve a low security risk environment that can be audited and tested by professionals. Hardening the application, the database, and other components should minimize your risk and also provide an audit trail to meet compliance requirements. Because mobile apps security is complex and steep learning curve, IronWALL makes it easier to meet your security requirements by just configuring with no coding needed. It is important to determine the priorities of these activities in accordance with your risk assessment, governance, regulatory compliance policies, industry practices, and common sense.

Operational Efficiency and Control

IronWALL code less integration does not affect the Software Development Life Cycle (SDLC). With just 3 clicks, the mobile app is well protected and ready to be published. It helps to reduce the time and cost where the developer does not require to spend time in researching and developing the latest mobile app security.

business@seciron.com www.seciron.com

ATTRIBUTES	FEATURES	
Deployment	- On-Premise - Online SaaS (Cloud) - Online SaaS (Private)	
Supported OS Platform Versions	- Android APK & SDK (Android 4.2 and above) - iOS IPA & SDK (8.0 and above) - HarmonyOS	
Supported Format Types	- Android Apps = .apk, .aab - Android SDK = .aar, .jar - iOS Apps = .ipa, .xcarchive - HarmonyOS Apps = .p7b - HarmonyOS HAP = pack.info	
	FOR ANDROID	**FOR iOS**
Supported Environment Types	- Android Studio 3.0.1 - Eclipse + ADT	- iOS Xcode version 9.0 + - iOS Xcode version 4.0 + **SDK only*
Supported CPU Architecture Types	- ARM, x86	- armv7, arm64, i386, x86_64
Supported SDK Dependencies	- JAR, SO, Zip	- libz, libresolv, libc++
Supported System Languages	- Java - Kotlin	- Objective-C (C/C++) - Swift
Product Functions	- Overall protection of DEX files - JAVA code virtualization protection - SO File protection - HTML/JS protection - Game related protection - Local data protection - Key protection - Security encryption and decryption - Secure file storage - Network communication data security - Anti-hijacking SDK - Anti-screenshot function - Anti-recording function - Secure keyboard SDK - Runtime protection • Anti-repackaging • Memory protection • Debugger monitoring • Device root monitoring • Code injection monitoring • Code hook monitoring • Android emulator detection • Android app multi-open Monitoring	- Code logic confusion - String encryption - Code virtualization - Anti-debugging - Anti-tampering - Integrity protection - Key protection - Security encryption and decryption - Secure file storage - Network communication data security - Anti-hijacking SDK - Anti-screenshot function - Anti-recording function - Secure keyboard SDK - Runtime protection • Anti-repackaging • Debugger monitoring • Device jailbreak monitoring • Code injection monitoring • Code hook monitoring

SECIRON

Over A Decade of Providing Security Solutions Across Asia

We are the industry leader in mobile application security across Asia. With over 10,000 applications across 9 countries protected using our End-to-End solutions, industries across Banking, FinTech, Insurance, Gaming & Government choose us to secure their applications across end-devices.

Connect with us to know more

Get In Touch
business@seciron.com
www.seciron.com