SECIRON

IRONWALL

Mobile Application Hardening Platform

Defend Applications Against Known and Unknown Threats

Organisations should make security a top priority right from the start of the mobile application development process. This is because once an app is released to the public, it becomes susceptible to attackers exploiting coding errors and other vulnerabilities.

Recognising the need for robust mobile app protection, SecIron developed IronWALL, a cutting-edge security solution that helps manage, prevent and protect mobile apps from security risks. IronWALL is designed to safeguard against a wide range of threats, including app tampering, reverse engineering, debugging, jailbreaks, app cloning, malware, repackaging and other attacks on untrusted environments. It also effectively mitigates potential risks by reducing attack surface exposure.

IronWALL utilises the following technologies to harden and protect mobile applications

- Code Protection (Reverse Engineering)
- Dynamic Protection/Runtime Attack Prevention
- Anti-Tampering/Repackaging
- Data Encryption

IronWALL's Multi-Dimensional Approach to Security Protection

- Leverages Runtime Application Self-Protection (RASP) technology to provide self-protection capability on the mobile app to defend against any attack even if it is offline
- 3-layer encryption prevents reverse engineering and reduces the chances of apps being tampered with
- Strengthens the mobile app protection with defense-in-depth

Codeless Integration for Seamless Security Integration

- Does not affect the App Development Life Cycle (ADLC)
- Reduces time and cost as developers do not have to spend time researching and developing the latest mobile app security
- Integrates transparently into the build process and requires no changes to the source code
- No compromise on performance and usability

IronWALL's Core Features

Flexible Deployment Models

- Solution can be deployed as SaaS or On-Premises

Comprehensive Portal Management

- Log and report generation
- Role-based access
- Visually appealing and intuitive user interface

Detection and Prevention

- Data encryption
- Code obfuscation
- Code encryption and concealing
- Hook and injection attack
- Tampering
- App repackaging
- Emulator detection
- Jailbreak detection
- Android rooting detection
- Dynamic debugging and many more

Secure Keyboard

- An added-value function to ensure keystrokes are securely encrypted; prevents data from being intercepted by keylogger

Supported Platforms

- Native, Cross platforms, Hybrid apps, Flutter
- Android, iOS, Harmony OS, SDK

SecIron is a leading mobile application security solution provider that offers an end-to-end service to help businesses and organisations discover, avoid and mitigate security risks associated with mobile applications.

IRONSCAN
Scans mobile applications for vulnerabilities in minutes

IRONWALL
Instantly encrypts and protects apps within minutes

IRONSKY
Monitor, analyse and take proactive actions against threats

IRONGATE
Enables better management of user credentials and authentications