



CASE STUDY: BANKING

How SecIron Helps an International Bank Met Mobile Security Mandates

Explore how the bank met regulatory requirements, hardened its mobile app within weeks, and created a secure foundation for services expansion.



At a glance

Sector / Market	International commercial bank (A large network in Taiwan)
Driver	Central Regulatory mandate: Requires all banking mobile app to be protected
Deployed	IronWALL, On-premise, iOS and Android, customised policy per app
Integration	Codeless: No source code changes, no change to the development life cycle
Timeline	First protected app live two weeks after development. Every update since: minutes

The customer

An international bank with large networks in Taiwan. Its customers, increasingly, are in the app with activities like balances, transfers, cards, onboarding, **on a device the bank does not own, on a network it does not control, in an operating system it cannot patch.**

For customer confidentiality, the bank's name and identifying details are not disclosed.

The problem background

Bank regulators requires that banking mobile applications be protected, turning a long-term intention into a dated obligation measured in weeks. Compliance isn't a checkbox; it's the licence to operate.

That is the situation every bank currently manages. In this bank's market, the regulator made it explicit.

Underneath the mandate sat three problems the bank already knew about:

- Sensitive data lives inside the app.**
 On a rooted or jailbroken device, an unprotected app hands over customer identity, credentials and transaction data.
- So does the bank's own property.**
 Business logic compiled into the binary can be reverse engineered and rebuilt. Repackaged banking apps have been used against institutions across the region.
- The calendar wouldn't move.**
 Protection had to cover the full development cycle without becoming the reason a release slipped. Mobile hardening is a specialist discipline few in-house teams carry. The bank had weeks, not years, to build that bench.



What the bank deployed

The bank needed stronger mobile protection, but with **two conditions**: application binaries had to remain within its environment, and development couldn't be disrupted. Seciron addressed both with IronWALL, an on-premise, black-box hardening server. With **no SDK or source code changes required, it integrated seamlessly** into the existing development lifecycle, allowing the bank to **apply its security policies and harden applications within minutes**.

Code protection

Obfuscation, code encryption and concealing, three-layer encryption

Anti-tampering

Detects modification, cloned or re-signed copies distributed outside official stores

Runtime protection (RASP)

Detects rooting, jailbreak, emulators, hooking, injection and dynamic debugging, on-device, including offline

Data protection

Encryption of sensitive data plus a secure keyboard that encrypts keystrokes

Portal management

Role-based access, protection logs and reports per build

The impact

More services in the app.

With hardening proven and repeatable, the bank moved higher-value services into the mobile channel. The protection expanded the product, not just defended it.

Faster protection, release after release.

The first protected app went live in two weeks. Every update since could be hardened in minutes, without turning security into a release gate.

The thing that never happened, never happened: no cloned app in circulation, no customer letter, no regulatory finding.

Evidence when auditors ask.

Every protected build carries a record of what was applied and when, giving the bank clear evidence when questions arise.

Mobile security without adding headcount.

Seciron brought specialised mobile security capabilities through the platform, with protections evolving as the platform updates.

TIP: Five layers. Zero code changes.

Unlike traditional SDK integration, the codeless approach requires no changes to the customer's source code, reducing integration from potentially months to a much faster, simpler process, even for outsourced development.



Maps to RMiT, BSP and Other Banking Standards

IronWALL wasn't built to one market's rulebook. It converges with the mobile app control families in Bank Negara Malaysia's RMiT and the Bangko Sentral ng Pilipinas circulars. It applied at the binary, with no source code changes.

Reverse engineering resistance

Code obfuscation, encryption and concealing of the compiled binary

Tamper / repackaging detection

Tamper, repackaging and clone detection, with configured response

Refuses compromised devices

RASP: root, jailbreak, emulator, hooking, injection, debugging, even offline

Credential / data protection

Data encryption plus a secure keyboard that encrypts keystrokes

Logged, reviewable events

Protection logs with role-based access, extended to real time with IronSKY

Pre-release vulnerability testing

IronSCAN static and dynamic testing against OWASP, CVE and CWE in CI/CD

Policy is set per app, then reapplied identically on every build, so the control demonstrated at audit is the control that shipped last Tuesday. Hardening is one layer of a technology risk programme; the compliance assertion remains the institution's.

Your lineup for Mobile App Protection

IRONSCAN

Scans every app for vulnerabilities exposed secrets and risky third party libraries.

[Discover Now](#)

IRONWALL

Harden the release, applies protection to the built app and enforces its own presence.

[Discover Now](#)

IRONSKY

Monitor and respond in real time, with every detection logged for audit.

[Discover Now](#)

Ensure Your App Meets the Banking Standards

See how the same approach could apply to your mobile banking application. Talk to us about your current security requirements, identify potential areas of exposure, and explore how your mobile app protection can be strengthened.

[Talk to Our Expert](#)