



CORPORATE PROFILE

Seciron: End-to-End Mobile Application Security Solutions

Trusted protection across the entire mobile application lifecycle.

About Us

A leading mobile application security provider, SecIron offers end-to-end solutions that help businesses and organisations discover, avoid and mitigate security risks associated with their mobile applications. Founded in Tokyo, Japan, in 2010, we earned a reputation as a reliable partner in securing all kinds of mobile applications as well as the peace of mind of clients.



OUR TRACK RECORD

**15+**

years' of experience

**10,000+**

mobile apps protected

Trusted by **70+**

Global Fortune 500 companies.

SERVICE COMMITMENT

The SecIron team comprises mobile application security professionals who are committed to delivering customised solutions tailored to clients' specific needs and circumstances. We continuously strive to build long-term relationships with all stakeholders, providing the highest level of service possible.

OUR MISSION



"Our mission is to provide the most comprehensive mobile application security solution on the market. This means combining meticulous health scans, customised protection measures, and an intelligent, real-time control centre – all orchestrated to deliver unparalleled security."

Nicole Ban, COO of SecIron

A Comprehensive Mobile Application Security Solution Provider

SecIron's main focus is on helping businesses build **safe, secure and trusted mobile applications** through a full range of mobile app security services, which include:

- Mobile app security consultation
- Mobile app security monitoring
- Manual audit and penetration testing
- Mobile app assessments, and more

Our comprehensive security solutions protect enterprises from data breaches, cyberattacks and other potential threats, with the assurance of complete protection throughout the application development life cycle. We also help safeguard users against mobile threats and malicious parties by ensuring the integrity of apps and preventing any unauthorised access or tampering of user data within them.

OUR SOLUTIONS

A full range of mobile app security solutions

IRONSCAN

MOBILE APPLICATION SECURITY ASSESSMENT

Helps diagnose and identify vulnerabilities in mobile applications to facilitate remediation.

- Versatile and thorough reporting
- Enhanced risk management and IT governance

IRONWALL

MOBILE APPLICATION HARDENING PLATFORM

Encrypts and protects apps against threats such as app tampering and reverse engineering.

- Codeless integration
- Multi-dimensional approach to security protection

IRONSKY

REAL-TIME MONITORING AND RESPONSE SYSTEM

Provides complete analysis and critical resource-based information in real-time.

- Helps organisations promptly respond to threats
- Adaptive capabilities to counter ever-evolving threats

IRONLAB

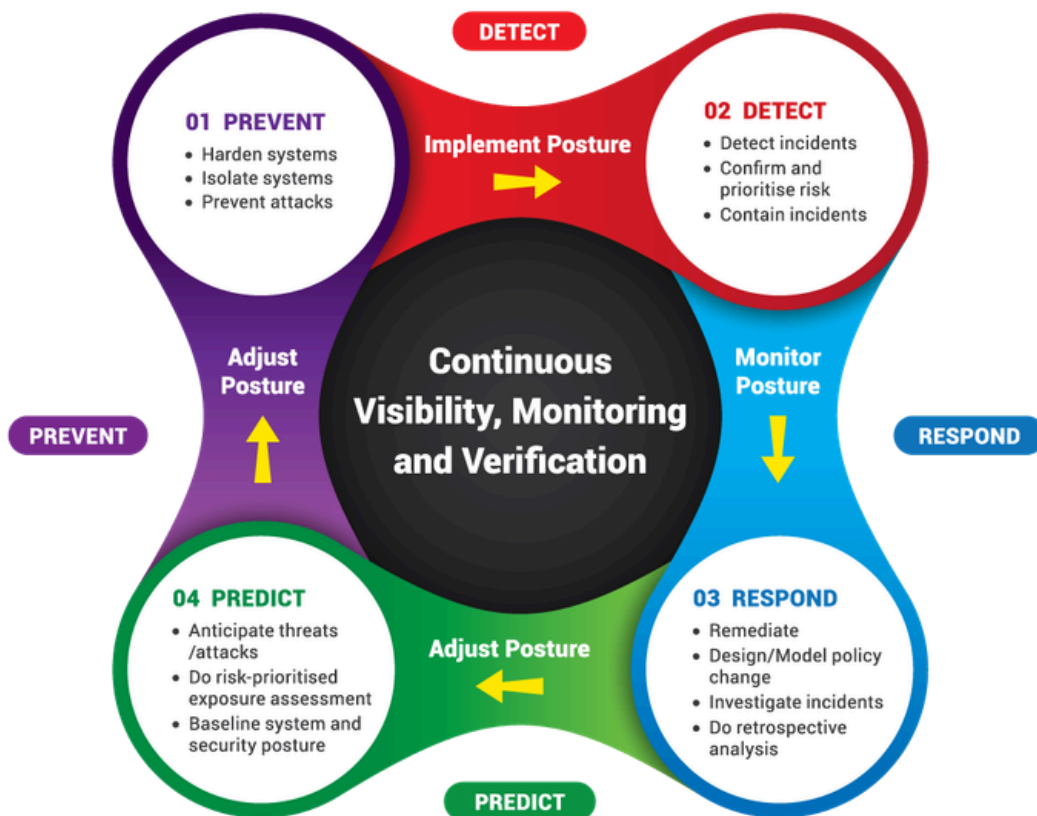
DEVICE COMPATIBILITY TESTING

A dedicated research team tests and validates mobile device performance and security protections before release.

- Broad device coverage
- Reduces compatibility risks before users are impacted

Fortified Next-Generation Security Architecture

SecIron applies an Adaptive Security Architecture (ASA), embedding security through every stage of the application development life cycle. **Continuous monitoring, automation and integration with CI/CD pipelines keep protection in step with your release cycle**, guiding teams through four continuous phases: **Prevent, Detect, Respond and Predict**.



ADAPTIVE SECURITY ARCHITECTURE (ASA)

Multi-Layer Protection. Minimal Integration. Zero Code Changes.

01 Anti-SDK-removal enforcement

Strip the protection out of the app and **the app knows — it alerts, or it exits.**

03 Multi-layer application hardening

Encryption, obfuscation and integrity enforcement working together **against reverse engineering, tampering and runtime manipulation.**

05 Real-time visibility and response

IronSKY provides detailed insights into threats, devices, and locations **in real-time** — with an incident log your auditor can read.

02 Codeless protection

No SDK integration, no source-code changes — nothing for your development team to rewrite.

04 Behaviour-based runtime detection

Catches what an attacker is doing right now like **hooking, debugging, spoofing and whether or not it has been catalogued before.**

06 Deployment flexibility

Cloud or on-premises: Where **policy requires binaries to stay inside your own network**, they do.

THREAT COVERAGE & INDUSTRIES WE SERVE

Against the app itself

- Reverse engineering
- App tampering
- Repackaging and cloning
- Debugging

Against the runtime

- Hooking and instrumentation
- Root and jailbreak
- Runtime manipulation
- Location spoofing

Against your user

- Overlay attacks
- Accessibility abuse
- Screen sharing and streaming
- SMS interception
- Malware and trojan activity



Industries we serve

- Banking
- Financial services & Digital Payments
- Government
- Insurance
- Healthcare
- Retail & e-commerce
- Telecommunications & digital platforms

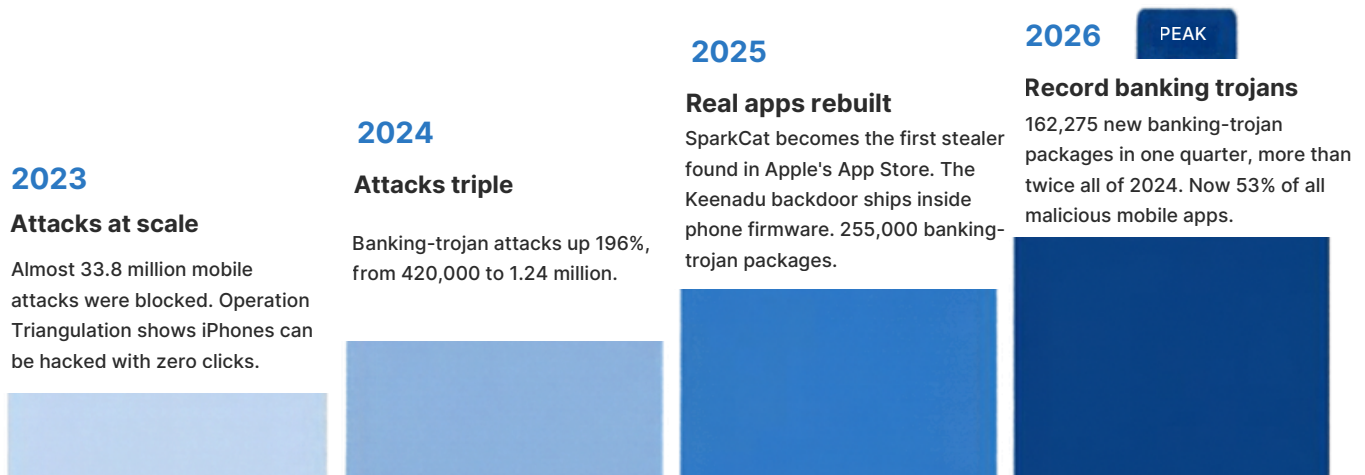
WHY THIS MATTERS NOW

As Mobile Adoption Grows, So Does the Need for Stronger Security.

(Source:

HOW MOBILE THREATS HAVE EVOLVED

Mobile threats are becoming **more sophisticated, targeting not only vulnerabilities in the app itself, but also how the app interacts with the device, user and runtime environment.** From overlay attacks and accessibility abuse to app cloning, hooking, screen sharing and location spoofing, attackers increasingly exploit legitimate mobile functionality to compromise users and transactions. **According to Kaspersky Securelist's mobile threat reports and research, banking trojans hit a record in Q1 2026,** capping three years of rising sophistication in mobile attacks. At SecIron, our goal is to make sure your app is not the way in.



BY THE NUMBERS

815k

malicious mobile app packages detected in 2025

306k

malicious app packages in Q1 2026 alone, over a third of 2025's total in one quarter

242k

downloads of malware-laced apps from Google Play in a single campaign (SparkCat)

DISCOVERED THREATS 2026

DarkSword

State-grade exploits, now in criminal hands

FakeWallet

Fake apps inside official stores

Rokarolla

137 commands: full device takeover

Mirax

Victims' phones turned into fraud proxies

Trusted to Protect High-Value Mobile Applications

Since 2010, SecIron have hardened more than **10,000 mobile applications** for organisations and is trusted by **70+ Global Fortune 500 companies**. Many customer engagements remain **confidential due to security and regulatory requirements**. What they have in common is a mobile app carrying money, identity or citizen data and a regulator who asks how it is protected.

Banking & Financial Services

Mobile banking apps are cloned and repackaged with overlay screens that harvest credentials. We detect and stop them at runtime, and log every event in a form your auditor can read.

Insurance

Claims and policy apps hold medical records, identity documents and payment credentials in one place. Multi-layer hardening keeps that data unreadable to anyone decompiling the app.

Telecommunications & Digital Platforms

Every cloned app is stolen revenue. Multiboxing, emulators and GPS spoofing are the three ways promo abuse eats margin — IronSKY shows you each one in real time, per device.

Retail & E-commerce

Loyalty fraud, account takeover and cloned storefront apps come from the same place: an app that can be decompiled and rebuilt. Harden the binary and the economics of the attack stop working.

Government & Public Services

Citizen-facing applications run on devices your agency does not own. We harden the app itself, so protection travels with it onto rooted phones, emulators and modified operating systems.

Fintech & Digital Payments

Bank-grade hardening without bank-grade timelines. Codeless integration means there is nothing for your developers to rewrite, so protection ships at your release speed.

Healthcare

Patient-facing apps carry health records under some of the strictest data rules in every market you operate in. Hardening protects data at rest; runtime detection protects it in use.

Regional Expertise. Local Accountability.

Mobile threats are not the same across every market. A banking trojan targeting users in one country may use different techniques, behaviours and attack paths from one targeting another, while regulatory expectations and incident-response requirements can also vary significantly across jurisdictions. SecIron has focused on mobile application security in Asia since 2010, giving us first-hand experience of how these differences affect organisations in practice. With an **established footprint and customers across more than 10 countries in Asia**, we bring regional expertise, local market understanding and support that is closer to where our customers operate.



Our regional teams work close to our customers, providing local market understanding, regional expertise and responsive technical support. When something needs attention, you have people nearby who can respond quickly and help you resolve it.

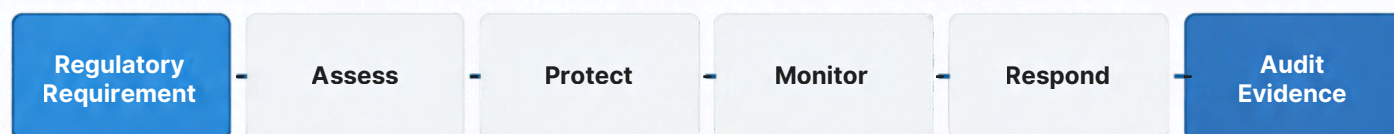
Built for Regulated Environments

SecIron supports organisations in addressing applicable mobile application security considerations across regional regulatory frameworks. BNM RMiT, MAS TRM, OJK, BSP, Taiwan FSC and HKMA CFI provide relevant guidance and reference points for organisations operating across these markets.

KEY REGIONAL FRAMEWORKS

 Malaysia BNM RMiT	Bank Negara Malaysia's Risk Management in Technology (RMiT) policy provides requirements and guidance for managing technology and cyber risks. SecIron capabilities can support organisations in addressing relevant mobile application security considerations under the framework.	 Indonesia OJK	Indonesia's Otoritas Jasa Keuangan (OJK) provides cybersecurity regulations and guidance, including SE OJK 29/2022, that are relevant to commercial banks considering mobile application security controls and third-party penetration testing.
 Singapore MAS TRM	The Monetary Authority of Singapore's Technology Risk Management (TRM) guidelines are relevant to financial institutions considering security controls for customer-facing mobile applications, including vulnerability assessment and tamper protection.	 Philippines BSP	The Bangko Sentral ng Pilipinas (BSP) provides regulatory guidance relevant to banks and financial service providers; organisations should consider applicable requirements for protection against unauthorised access and tampering.
 Taiwan FSC	Taiwan's Financial Supervisory Commission (FSC) provides cybersecurity standards relevant to financial institutions considering mobile banking security controls, regular assessments, and protection against app tampering and reverse engineering.	 Hong Kong HKMA CFI	The Hong Kong Monetary Authority's Cybersecurity Fortification Initiative (CFI) is a relevant reference point for banks considering a structured approach to mobile application hardening, monitoring, and protection against reverse engineering and tampering.

FROM REQUIREMENT TO AUDIT EVIDENCE



Stage	Capability	Where SecIron fits	Regulatory Requirement
ASSESS	Vulnerability assessment & security testing	IRONSCAN	Pre-release security validation, OWASP compliance
PROTECT	Hardening, anti-tampering, anti-reverse engineering	IRONWALL	App integrity protection, code protection
MONITOR	Real-time threat & device monitoring	IRONSKY	Continuous security monitoring, threat detection
RESPOND	Incident logs, investigation & audit support	IRONSKY	Forensic evidence, regulatory reporting



GET IN TOUCH

Learn More About Us

Stay connected with SecIron for the latest insights in mobile application security.



LinkedIn

linkedin.com/company/seciron



YouTube

youtube.com/@Seciron



SecIron Website

www.seciron.com



Email

business@seciron.com
