

PROMON



# Promon Code Protect™

Protect your code. Preserve your competitive edge.



## Promon Code Protect™

Expanding the capabilities of Promon Shield for Mobile™, Promon Code Protect™ adds deep code obfuscation for your app's code, defending against reverse engineering and tampering at the binary level. It integrates seamlessly post-compile, protecting native and hybrid apps on Android and iOS without slowing development or impacting performance.

|                      |                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------|
| <b>Platforms</b>     | Android<br>iOS                                                                                       |
| <b>Languages</b>     | Swift<br>Objective-C<br>C/C++<br>Rust<br>JavaScript (ES2020-compatible)                              |
| <b>Frameworks</b>    | Native apps<br>Hybrid frameworks (React Native, Cordova, Ionic)<br>Multiplatform framework (Flutter) |
| <b>Architectures</b> | ARM<br>Intel                                                                                         |

## Why Promon Code Protect™



### Defend your IP

Your app logic, algorithms, and proprietary frameworks are your competitive advantage. Code Protect hides them from attackers through advanced, multi-layered obfuscation, safeguarding your business from cloning, fraud, and piracy.



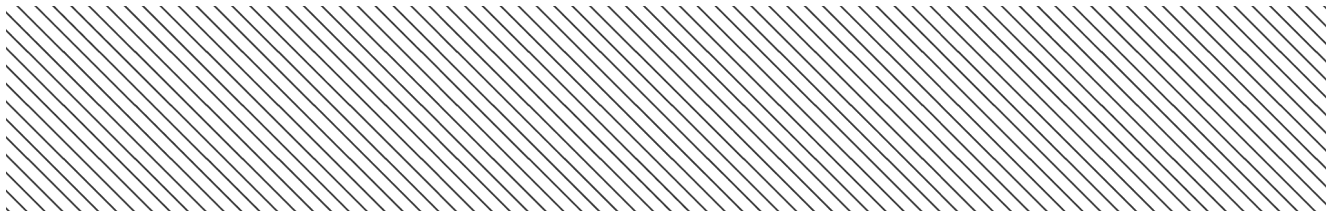
### Secure every build

Code Protect operates post-compile and integrates directly into your CI/CD process for automatic, consistent protection in every release. Whether you're protecting native (Swift, C/C++, Rust), hybrid (React Native, Cordova, and other JavaScript-based frameworks), or multiplatform apps (Flutter) Promon Code Protect works seamlessly with no toolchain disruption.



### Stay compliant and resilient

Meet standards like OWASP MASVS and regulations such as GDPR and CCPA. Code Protect strengthens your apps' resilience against tampering and reverse engineering, keeping them compliant and trustworthy, even as threats evolve.



## What sets Promon Code Protect™ apart



### Post-compile binary obfuscation

Code Protect secures your mobile apps after build, protecting compiled binaries and third-party SDKs on both Android and iOS. It supports multiple languages, including Swift, Objective-C, C/C++, Rust, and JavaScript. Optimized for ARM and Intel architectures, it delivers consistent protection with minimal maintenance.



### Seamless integration, no toolchain changes

Code Protect fits directly into your CI/CD pipeline with a low-configuration setup and no disruption to your existing build system. You can protect apps in minutes: no SDKs, no source code changes, no extra training.



### Cryptographic binding for integrity

For additional assurance, Code Protect cryptographically binds its security features to the protected app. If tampering is detected, the app automatically fails to launch, preventing unauthorized modification or misuse.



### Complements Promon Shield for Mobile™

As an extension of Shield for Mobile, Code Protect forms a complete in-app defense, combining code-level protection with real-time runtime security, for layered resilience against reverse engineering, tampering, and malware.

## How it works



Promon Code Protect™ applies multiple layers of protection to make your app's code unreadable and resistant to static and dynamic analysis, without impacting performance or functionality.

**Multi-layered obfuscation:** Protects native and/or JavaScript logic from reverse engineering while maintaining functionality.

---

**Section encryption:** Encrypts compiled sections of binaries to prevent static analysis.

---

**Control flow abstraction:** Conceals execution paths to make logic reconstruction impossible.

---

**Anti-debugging and anti-tampering:** Randomized traps and integrity checks block attempts to inspect or modify code.

---

**Integrity checking:** Verifies runtime integrity and triggers tampering responses.

---

**Debug stripping:** Removes debug metadata to minimize attack surface.

---

**Cryptographic binding:** Ensures apps fail safely if security mechanisms are altered.

---

# PROMON

## About Promon

Promon leads the way in proactive mobile app security. For 19 years, we've been making the world a safer place by securing any app, on any device—in no time at all. Today, we protect over 2 billion users, secure 13 billion monthly transactions, and safeguard \$2.5 trillion in market cap. Promon is headquartered in Oslo, Norway, with offices in more than 15 countries around the world.

## Would you like to talk to an expert?

Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

[Book a meeting »](#)