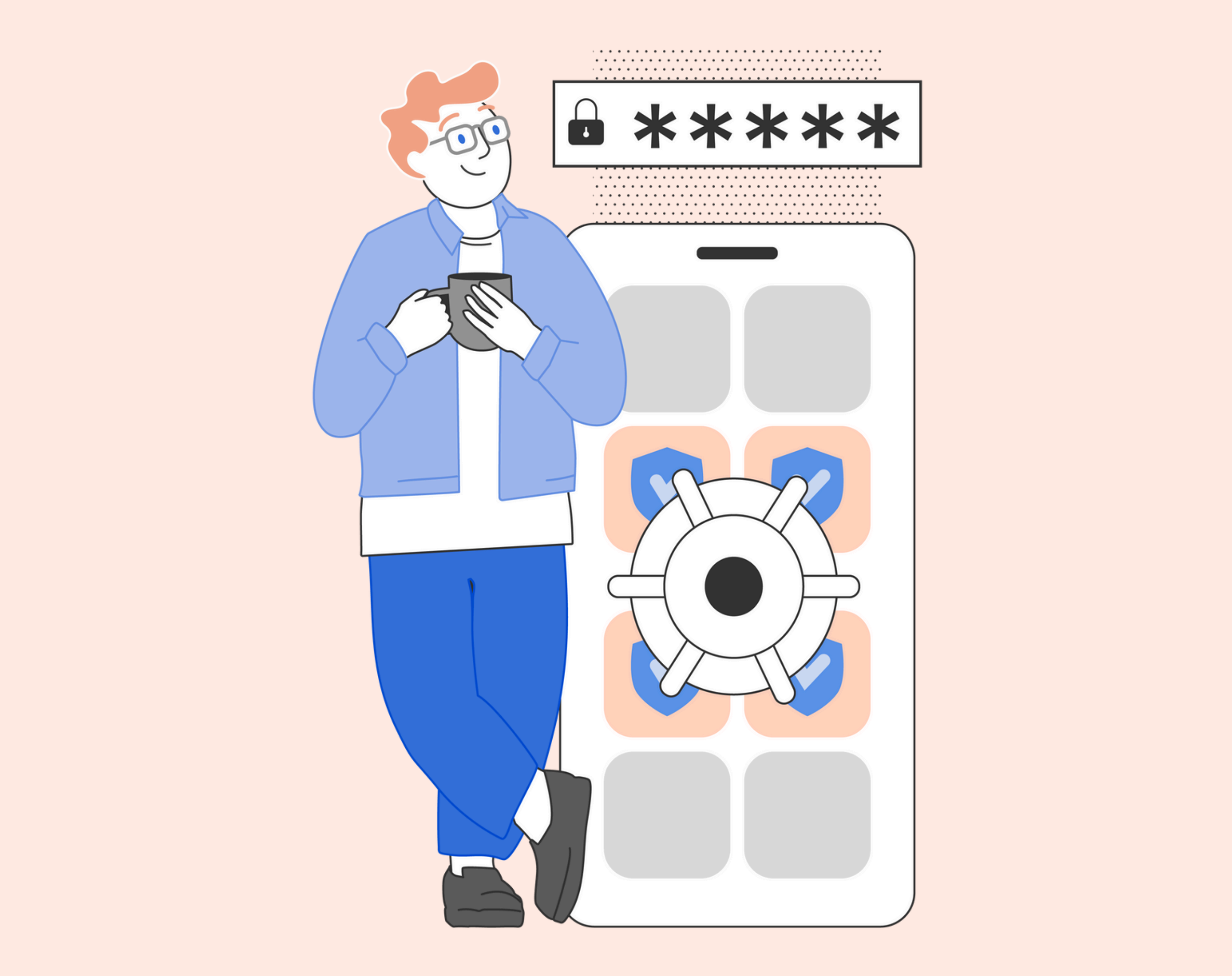
PROMON

Promon Data Protect™

Protect sensitive data. Secure your app from the inside out.



Promon Data Protect™

Promon Data Protect™ safeguards sensitive data, API keys, certificates, and other app assets stored on users’ devices. By combining Secure Local Storage (SLS) and Secure Application ROM (SAROM), it ensures that critical app data and secrets remain encrypted, isolated, and accessible only to your protected app—never to attackers.

Built as an extension of Promon Shield for Mobile™, Data Protect adds an additional layer of in-app data security to prevent data leaks, credential theft, and key extraction, even on rooted or jailbroken devices.

Platforms	Android, iOS
Frameworks	Native (Kotlin, Swift, Objective-C) Hybrid (React Native, Cordova, Ionic) Multiplatform (Flutter)
Data Types	API keys TLS certificates Tokens Configuration data Personal or session data

Why Promon Data Protect™

Secure sensitive data at rest

Data Protect keeps locally stored data encrypted and device bound. Even if a device is compromised, attackers can’t extract or reuse sensitive information. Data is decrypted dynamically in memory only when required by the app.

Protect app secrets and credentials

API keys, certificates, and configuration data are encrypted during app shielding and securely accessed at runtime. This ensures secrets never exist unencrypted on disk or in memory longer than needed.

Seamless, hardware-independent protection

Data Protect works across all devices, operating systems, and frameworks, without relying on hardware modules, hardware keychains, or secure enclaves.

Components of Promon Data Protect™

1. Secure Local Storage (SLS)

SLS provides secure, device-bound storage for dynamic app data, such as tokens, user information, and session data.

- Encrypts data using runtime-generated keys that are never stored on the device.
- Keeps data accessible only to the Shield-protected app, even if the device is rooted or jailbroken.
- Fully self-contained as it does not rely on Android Keystore or iOS Keychain.
- Ideal for storing session tokens, personal information, or cached app data securely on-device.

2. Secure Application ROM (SAROM)

SAROM protects static assets embedded in the app, such as API keys, TLS certificates, and configuration files.

- Encrypts fixed assets during the shielding process; decrypts them only when accessed by the app.
- Uses dynamic, runtime key derivation for each access, preventing extraction through static or dynamic analysis.
- Protects secrets that must exist in the published app without exposing them in plain text or memory.
- Ensures encrypted assets are never statically accessible, drastically reducing attack surface.

Together, SLS and SAROM create a dual-layer data protection framework that keeps both static and dynamic app data secure at rest and at runtime.

What sets Promon Data Protect™ apart

Dual-layer protection for all sensitive app data

Combines SLS for runtime data and SAROM for fixed assets, ensuring end-to-end data security within your app.

Dynamic, on-demand decryption

Encrypted assets are decrypted only when needed, limiting exposure and preventing data extraction.

Device-bound encryption

Ties data cryptographically to each device, preventing data cloning or transfer.

Independent from device security features

Does not rely on OS keychains, hardware modules, or cloud services, ensuring consistent performance and coverage.

Fully integrated with Promon Shield for Mobile™

Data Protect works natively within the Shield architecture. Encryption and decryption are handled automatically during the shielding process via Integrator and Shield APIs.

How it works

During the shielding process, Promon Shield for Mobile™ encrypts data and assets using symmetric keys derived from unique elements such as customer-specific seeds, tokens, and data IDs. At runtime, Shield for Mobile regenerates these keys dynamically, decrypts data securely in memory, and destroys the keys immediately after use.

This means app data, API keys, and certificates are never stored or accessible in plaintext, even under reverse-engineering attempts.

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 »