EndCrypt™ for Mobile

www.procenne.com

prOLenne DIGITAL SECURITY

Most Common Security Pitfalls

01

Reverse Engineering

Over
90%

of the apps fail exposure to reverse engineering. Reverse engineering is a common occurrence with apps, especially those distributed through commercial app stores. Attackers reverse engineer apps to figure out how they function and how they may be exploited, as well as to steal data and clone them.

02

Sensitive Data Loss

Over
83%

of the apps insecurely stored data. Inadequately protected applications can allow attackers to get sensitive data contained in them, such as payment credentials and intellectual property, resulting in downtime, supply chain delays, lost business, reputational loss, and regulatory fines etc.

03

Code Obfuscation

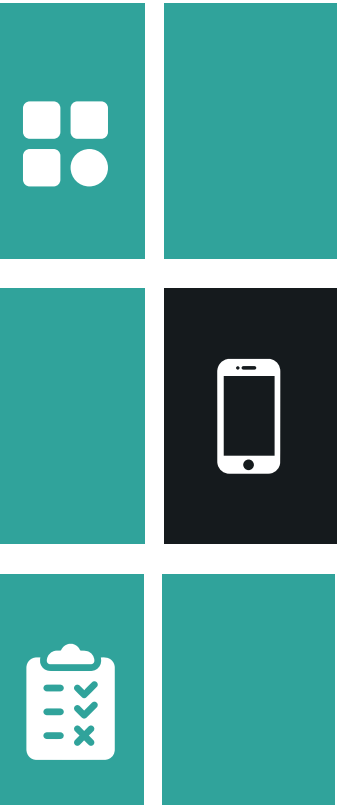
Over
76%

of apps do not use code obfuscation. Malicious actors that understand the inner workings of a mobile app can spread fraudulent applications, harvest sensitive data, steal intellectual property, and do other things. Along with this technique while the functionality of the code remains unchanged, the logic and the purpose of the app's code concealed.

What Is SDK?

Software Development Kits

SDK stands for "**Software Development Kit**", which is a collection of software development tools in one installable package. Think about putting together a model car or plane. When constructing this model, a whole kit of items is needed, including the kit pieces themselves, the tools needed to put them together, assembly instructions, and so forth. Main goal of SDK's are providing a set of tools, libraries, relevant documentation, code samples, processes, and or guides that allow developers to create software applications on a specific platform.

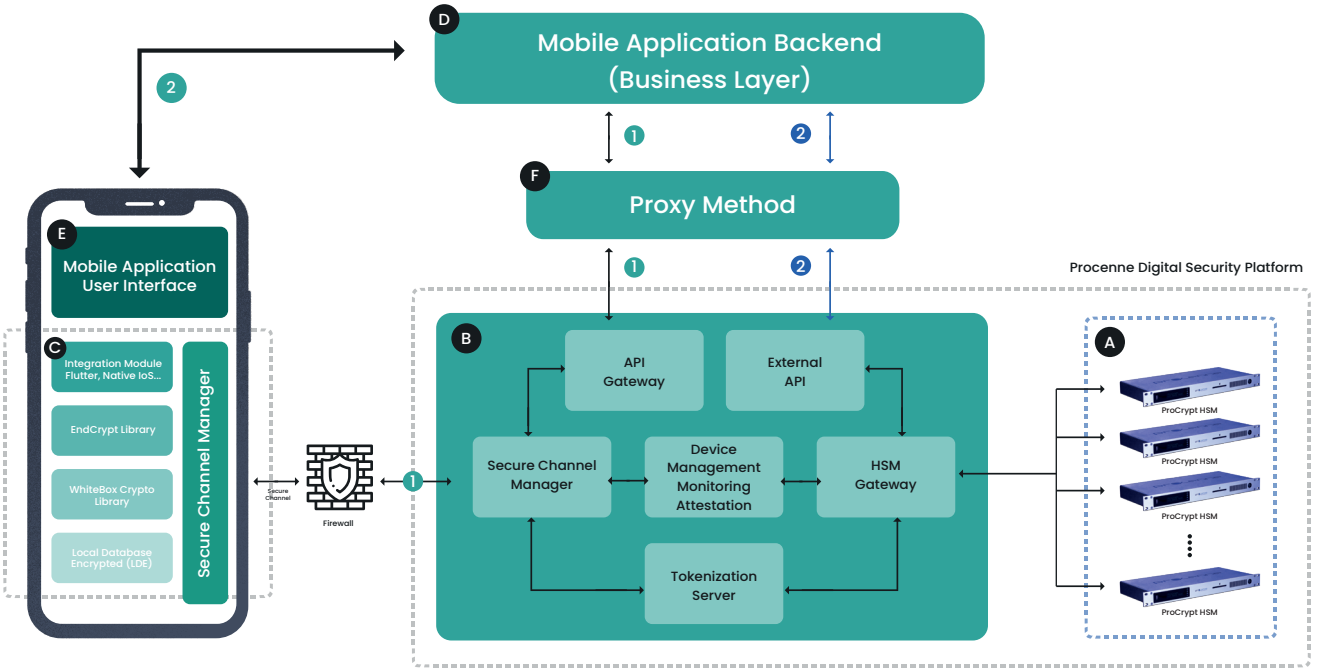


What is EndCrypt?

We bring the “**Security**” with our ready-to-use **SDK** called “**EndCrypt**” which installs into your **Mobile Applications**. EndCrypt **is not** only a **SDK** but also it has its own back office management platform that you can **manage, monitor** and **take actions** on your mobile devices **(endpoints)**.

EndCrypt provides a broad range of patented security capabilities to protect mobile applications by preventing reverse engineering techniques via anti-tempering and re-packaging detection technologies. It detects; debuggers, emulators, code-injection techniques, malicious behaviors from application permissions, hooked and jailbroken or rooted mobile devices.

Architecture



How It Works?

EndCrypt infrastructure consists of two main components, namely “HSM Pool”(A) and “EndCrypt Backend”(B). Within an operational setup aiming an end-to-end mobile application security, these two main system components are complemented with “EndCrypt Mobile SDK”(C), “Mobile Application Backend”(D), “Mobile Application User Interface” (E), and “Proxy Method”(F). All these components are depicted in architecture page within an operational setup for highly secure Mobile Applications.

How It Works?

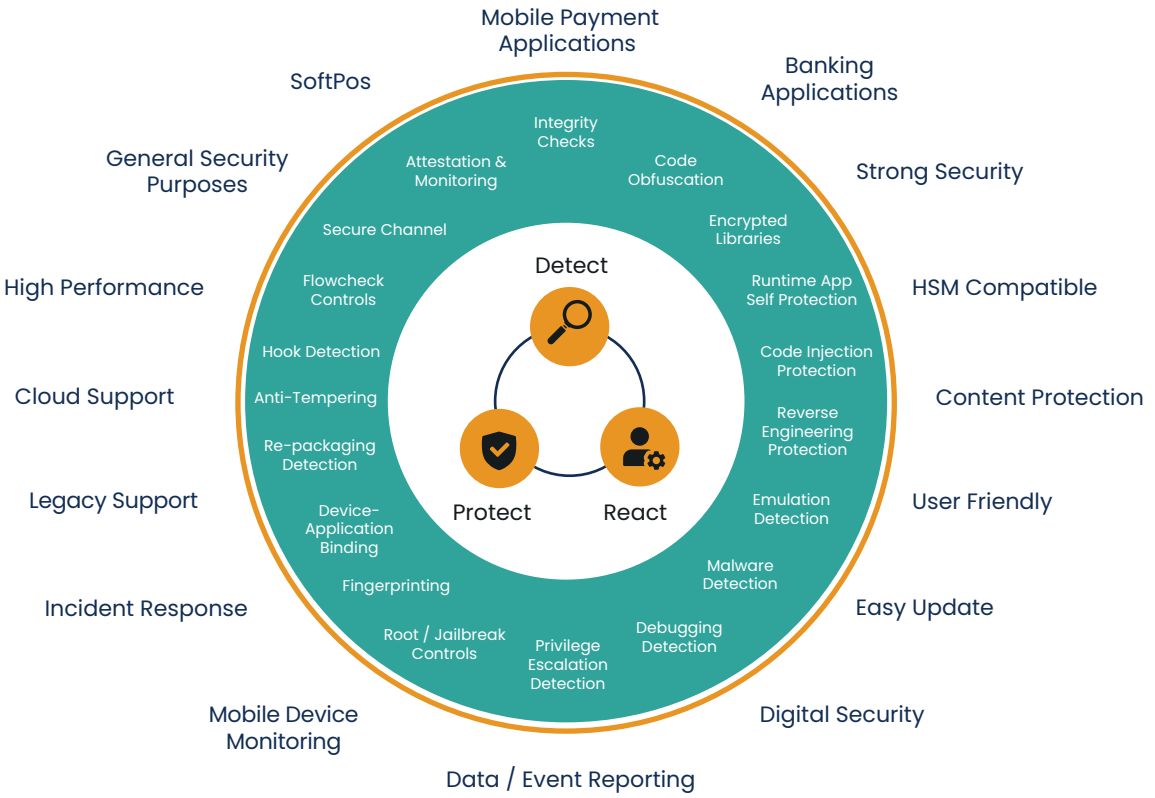
Components A and B together constitute “Procenne Digital Security Platform” serving as an end-to-end application security backbone system. Components A, B, and C together constitute the Procenne system of an end-to-end application security for mobile applications.

The components, “Mobile Application User Interface”(D) and “Mobile Application Backend”(E) are considered to be any-purpose custom applications that can be developed by the customers utilizing EndCrypt product. Please check out the Architecture page now.

Why EndCrypt?

1. Protects valuable application data and cryptographic keys.
2. Protects customer brand reputation, maintains trust.
3. Protects confidential data and builds customer confidence.
4. Protects sensitive data from leaks, keeps data secure.
5. Stands up against growing external threats, such as hacking or cyber-attacks.
6. Meets the security requirements of data regulations.

How Is EndCrypt Used?



Standards Compliance

OWASP®

NIST SP 800-208

PCI PCI-CPoC / SPoC

mastercard VISA AMERICAN EXPRESS DISCOVER

About Procenne

Turkey's digital security R&D center Procenne produces digital security products and solutions of critical importance for many sectors from public to finance, from education to telecom. Headquartered in Istanbul, Procenne was established in 2013 and after a 5-year R&D process, it produced the ProCrypt HSM family, which meets the need for general purpose and payment systems HSM on a single platform, and received CC EAL4+ certificates in 2019 and PCI HSM v3.0 certificates in 2021.

Working to meet the ever-increasing needs with its mobile application security SDK, EndCrypt, HSM Gateway CryptAway, and cloud HSM products, Procenne is on its way to becoming a global school committed to the values of the first day with its more than 100 employees.

According to Gartner, it is estimated that there will be 1.31 billion mobile payment transaction users worldwide and $200 billion will be spent on the SaaS side in 2023. It is an unavoidable fact that in such a large infrastructure, there will be leakage. To avoid this, choose us and our solutions now.

Resul Yeşilyurt, CEO of Procenne

EndCrypt started as a challenging thrill for me and turned into an adventurous journey. All my colleagues in the team have experienced the pleasure of creating a product by devoting effort. If you don't mind, of course; we prefer to be "us" with you.

Kutlu Durmuş, Product Manager

procenne
DIGITAL SECURITY