App Protection & Hardening

Mobile apps are both one of your greatest assets – and vulnerabilities

Market Challenge

Your consumer-facing mobile apps often contain valuable intellectual property, and more importantly, connect your organization to your customers. They allow your users anytime, anywhere access to your services and the data they need. However, with this portability comes increased threat of hacker abuse.

Solution: Combine mobile app protection with trusted digital identity

You can protect against harmful breaches by deploying a trusted identity assurance platform that extends beyond multi-factor authentication with mobile app protection to validate and protect the user's identity and the mobile app being used.

BENEFITS

- Address regulatory requirements for app hardening, including PSD2

- Protect your customers and brand from costly app breaches

- Avert static and dynamic attacks with code hardening and RASP

- Get integrated mobile app protection and trusted digital identity assurance from a single vendor

LEARN MORE AT ENTRUST.COM

Trusted Digital Identity Assurance with Mobile App Protection

Trusted identity assurance platform at a glance

Identity assurance extends beyond a single authentication endpoint. It brings in elements that include establishing trust before a credential is issued and then maintaining trust after authentication occurs. The net result is stronger security, an improved user experience, and the ability to extend new digital services.

These three elements provide a comprehensive approach to digital trust across all of your initiatives:

Establish trust – Verify the integrity of the user and their device before digitally onboarding with solutions like identity proofing and device reputation.

Transact – Secure access to everything and everyone with a flexible solution that allows you to easily provision a wide range of authenticators across your entire user population.

Maintain trust – Continuously authenticate identities with adaptive authentication that's transparent to your users.

Protecting against vulnerabilities

Once published, your app leaves your control.

Even if your app is posted on preferred app stores, it's vulnerable to being hacked because it's circulated outside your secure network perimeter.

Hackers download your app and look for vulnerabilities to exploit.

Attackers look for vulnerabilities and can inflict a whole variety of abuse, including:

Dynamic Attacks
Hackers gather knowledge of app behavior and modify the runtime using emulators and debuggers.

Offline Attacks
Hackers look at your code flow to find vulnerabilities and to steal valuable data and IP by reverse engineering your apps.

App Cloning
Hackers try to clone your app, insert malware and credential harvesting code, and republish fraudulent app versions.

LEARN MORE AT ENTRUST.COM

Trusted Digital Identity Assurance with Mobile App Protection

**Breaches can be incredibly damaging - costs add up fast.**

Unprotected apps are vulnerable to harmful breaches, which can lead to fines and penalties, stolen IP, reputation damage, lost revenue, and incident handling costs.

**Regulators are starting to incentivize those who protect their apps.**

Industries and agencies are recognizing the threats that mobile apps introduce into platforms such as banking and healthcare. Regulations are emerging to incentivize organizations to go the extra mile to protect their apps. PSD2, for example, requires organizations take steps to protect their customers, including their mobile apps.

Entrust mobile app protection

Our integrated protection consists of two complementary defense mechanisms:

Offline attacks
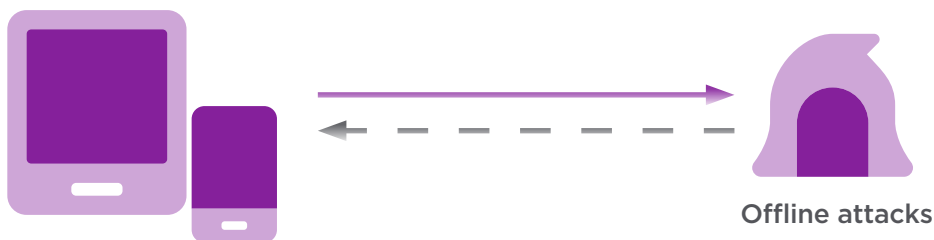
Code hardening (encryption and obfuscation) protects your applications from static analysis. It makes source code unreadable to hackers that manage to decompile or disassemble them, preventing hackers from gaining insight into the structure of your applications, extracting or altering the code, or exploiting vulnerabilities.

On-device attacks

Network MITM attacks
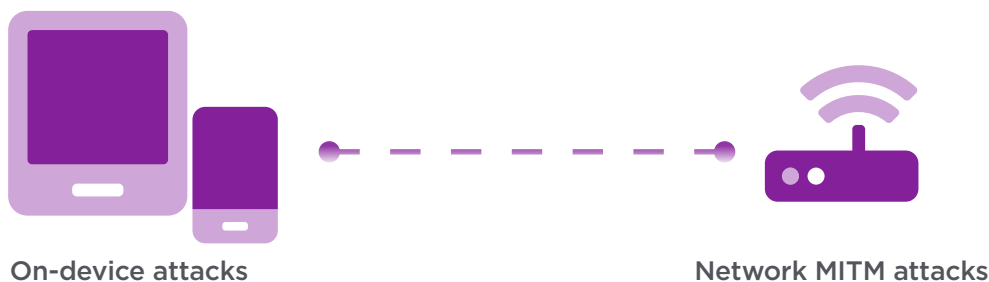
Runtime application self-protection (RASP) detects and prevents dynamic analysis and real-time attacks. It enables your applications to monitor their own integrity and the integrity of the device on which they are running and to react to potential threats. RASP also allows them to exchange information with a server in a secure manner.

Trusted Digital Identity Assurance with Mobile App Protection

Partnering with the best

To ensure our solution offers the most advanced security on the market without compromising UX and performance, we partner with Guardsquare, the gold standard for mobile app protection.

- **DexGuard -** The most advanced security solution for Android applications, integrating seamlessly into your build process and adding multiple layers of protection to your apps

- **iXGuard -** Specifically designed to shield iOS apps from reverse engineering and hacking, protecting without impacting their usability

GUARDSQUARE
Mobile application protection

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com   **entrust.com/contact**