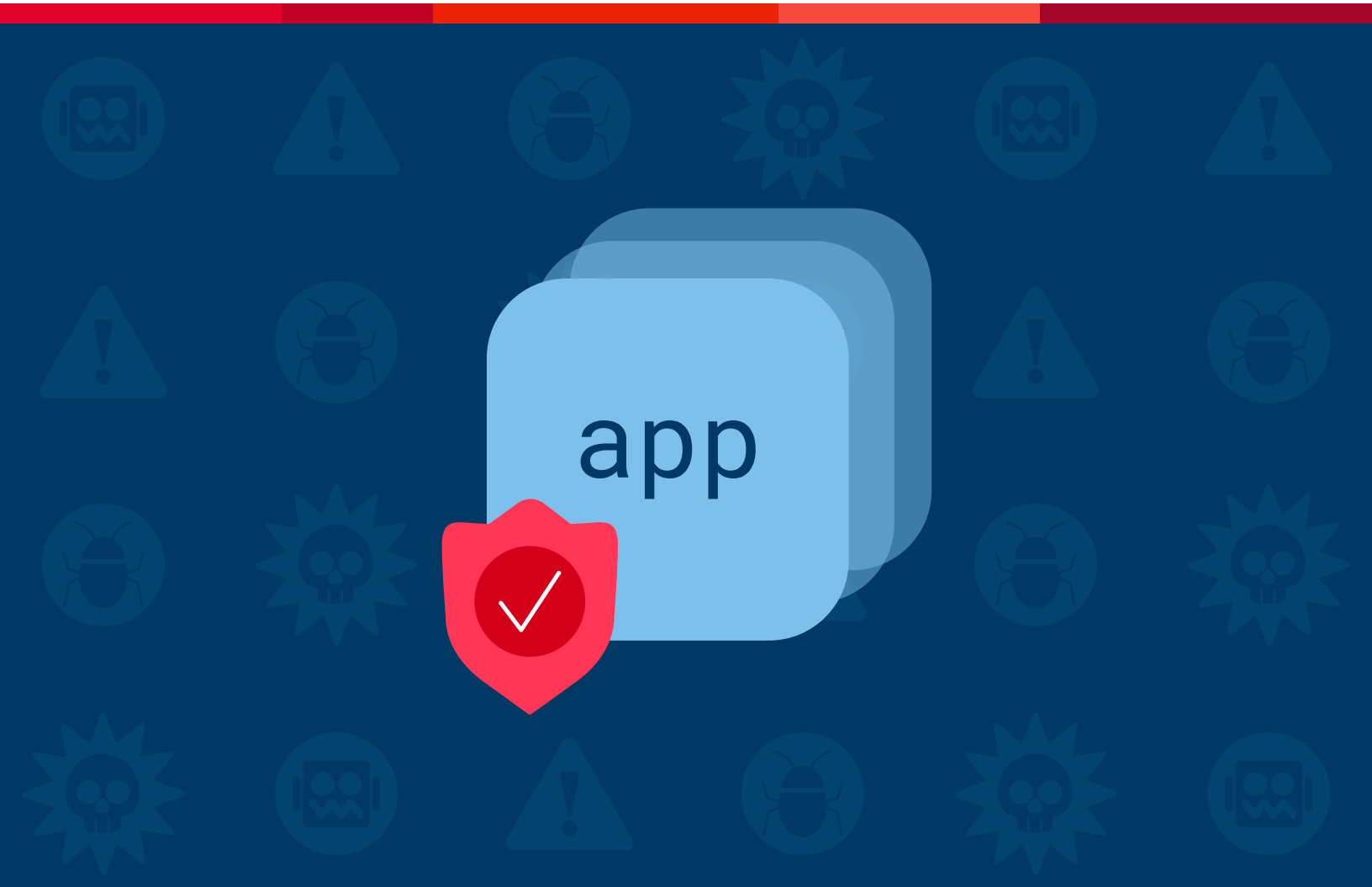
WHITEPAPER

Make Your Mobile App GDPR Compliant with App Shielding

App shielding is a comprehensive solution, giving your app layers of security to avoid tampering, malware, reverse engineering, and more.



What is the GDPR, and who does it apply to? The GDPR, or the General Data Protection Regulation, is the world's toughest privacy and security law. Passed by the European Union in April 2018, it strengthens and unifies data protection for all individuals inside the EU. It applies to all mobile apps that collect and process personal data of EU citizens, regardless of where a company is headquartered.

GDPR compliance requires constant vigilance. Companies must self-report all significant breaches within 72 hours, and each GDPR violation risks fines up to 4% of an organization's annual worldwide turnover, or €20 million, whichever is larger.

More damaging than the fines is the reputational risk, which can have a negative impact on growth, customer retention, and brand equity.

F5 Distributed Cloud Mobile App Shield protects sensitive data contained within an app	Proprietary EMVCo-certified white box prevents data cloning and lifting

The GDPR and Mobile Application Protection

The GDPR contains two articles that are especially relevant for mobile application protection, addressing app security and data protection for users:

- Article 25: Data protection by design and by default. Data processors and controllers are required to consider privacy while designing new applications, systems or processes that use personal data.
- Article 32: Security of processing. Application developers, data controllers and processors are required to implement necessary and sufficient organizational and technical measures to assure the integrity of processing data and deploy a level of security appropriate to the risk of breach, loss, unlawful destruction, or modification of data.

Learn more about app shielding

Make your mobile app GDPR compliant

Stay GDPR compliant with these recommended measures to protect your mobile applications.

Root and jailbreak detection

Rooting or jailbreaking a device opens the door for malicious actors to access the application code, modify it, inject malware, or repackage the app. To protect your app from this, you should have robust root/jailbreak detection.

Strandhogg is an example of a serious Android vulnerability which can exploit both rooted and unrooted devices. Read more here.

Prevent application repackaging and reverse engineering

If an attacker gains access to your app code, they can modify it (for example by adding malware), repackage the app and spread it to trick users into downloading the illegitimate app in place of your original app. You should therefore take steps to protect your app code so that it cannot be repackaged. Another reason why you should protect your app code is to prevent reverse engineering to lift existing security controls.

Once F5 Distributed Cloud Mobile App Shield security controls are implemented, hackers cannot remove them, even if the app is repackaged.

Detection for keylogging and screen reading

Keyloggers and screen readers are types of spyware that can be injected into an app. They are used to capture input from the user, typically PII such as banking details and passwords.

Prevent scraping of data on the client device by hardening your app code—this protects your users' credentials and blocks malware techniques designed to spy on user input.

Strong code obfuscation

Code obfuscation is a way of modifying an app's code to make it difficult for attackers to read and understand, should they gain access to it. The method conceals the logic and purpose of your app's code, while keeping its functionality.

This makes it harder for attackers to perform reverse engineering, analyze the code, and retrieve sensitive information.

Certificate pinning

When using SSL technology, data is encrypted through the operating systems. Relying on this leaves the door open for attackers to hook these functions in the operating system and get access to user data.

Employ certificate pinning to ensure that your deployed app instances are talking to a valid server at all times.

Application shielding supports GDPR compliance

App shielding is a comprehensive solution, giving your app layers of security to avoid tampering, malware, reverse engineering, and more.

Our multi-layered approach adds complexity to how we protect your app. Through employing heuristic algorithms, Distributed Cloud Mobile App Shield can defend against both known attacks and future attacks. This will prevent threats such as zero-day attacks, which exploit unknown flaws in your application code.

Distributed Cloud Mobile App Shield is a best-in-class app shielding software that provides your app with the security you need to avoid data breaches—defending your app against both known and future attacks. The solution is easy to integrate with your programming language of choice, and only takes minutes to deploy.

DC0420 | WP-GTM-1143515499-Mobile-App-GDPR-Compliant