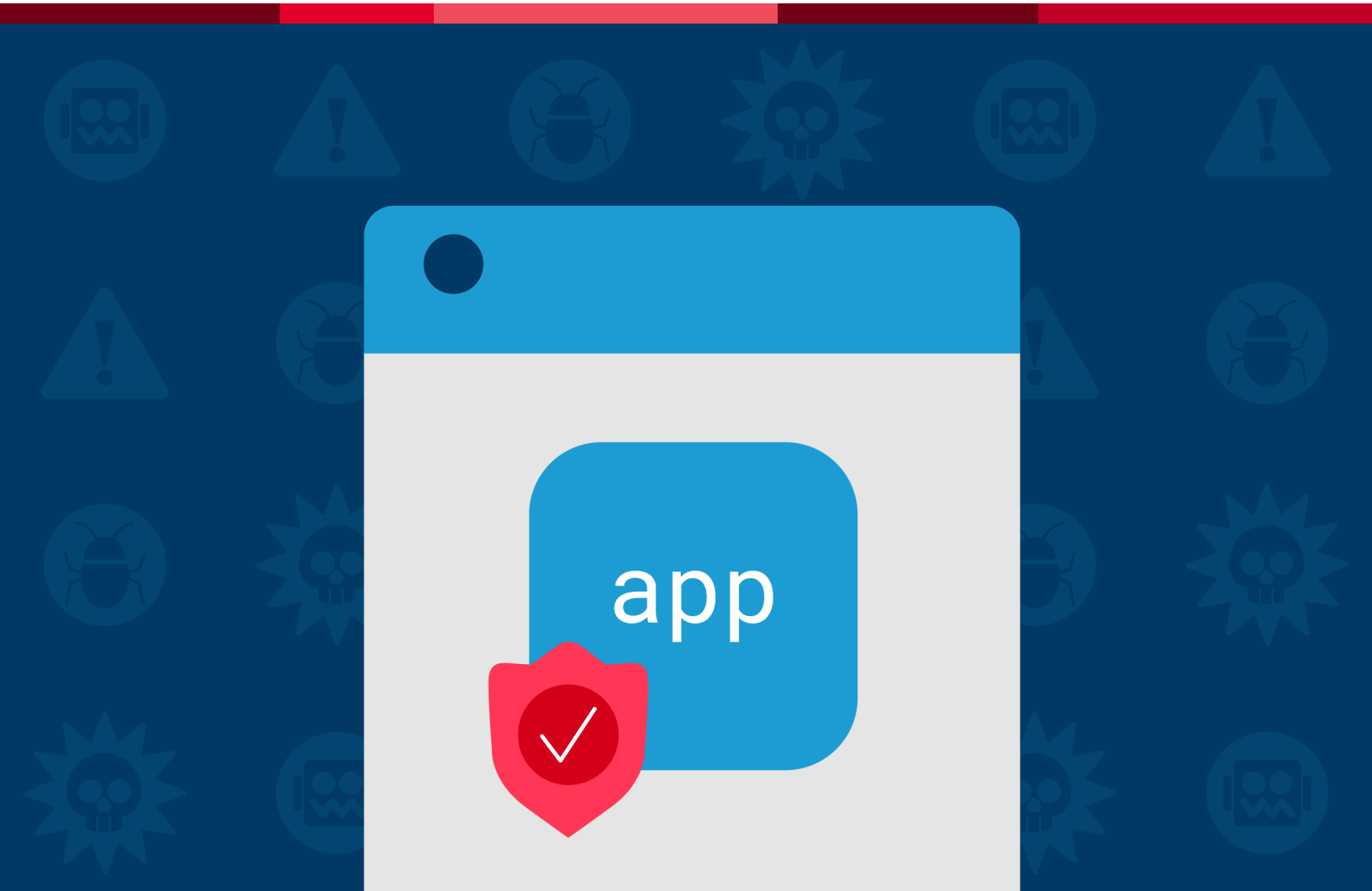
WHITEPAPER

Ensure CCPA Compliance for Your Mobile Apps with App Shielding

F5 Distributed Cloud Mobile App Shield is a comprehensive solution, giving your app layers of security to avoid tampering, malware, reverse engineering, and more.



CCPA and mobile app security

The California Consumer Privacy Act (CCPA) is a robust consumer protection law that has been in effect since the beginning of 2020. It applies to for-profit entities conducting business in the state of California. However, even if your business operates outside of California, it's crucial to take action. Since the CCPA's implementation, 15 other states have introduced privacy legislation, with proposals at the federal level as well. This underscores the importance for businesses to consider how they handle user data and ensure compliance.

CCPA offers a broad definition of Personally Identifiable Information (PII). Applications that handle any form of PII must explore methods to secure this data effectively, mitigating the risk of data breaches. PII refers to information that, when used alone or with other relevant data, can identify an individual.

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

What happens if you are not compliant?

Failure to comply with the CCPA may result in fines ranging from $2,500-$7,500 for each record, imposed by regulators. Additionally, the bill grants consumers the right to sue a company if their privacy rights are violated.

Even more costly than the fines is the potential loss of brand reputation, which can have long-lasting consequences.

Make your mobile app CCPA compliant

When it comes to app security, the CCPA requires businesses to follow "reasonable practices and procedures" to avoid a data breach. Data breaches often happen because malicious actors find ways into a company's server and uncover PII from the database. Mobile apps can be an entry point into your database. To deter malicious actors, it's important to make it difficult to scrape data from your app.

Root and jailbreak detection

Rooting or jailbreaking a device exposes the application code to potential threats, allowing malicious actors to modify it, inject malware, or repackage the app. Robust root/jailbreak detection is crucial to protect your app from these risks.

For instance, Strandhogg is an example of a serious Android vulnerability that can exploit both rooted and unrooted devices.

Prevent application repackaging and reverse engineering

If attackers gain access to your app's code, they can modify it (for example by adding malware), repackage the app, and deceive users into downloading the illegitimate version.

You should therefore take steps to protect your app code so that it cannot be repackaged.

Another reason to protect your app code is to prevent reverse engineering to lift existing security controls. With F5 Distributed Cloud Mobile App Shield 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 infiltrate apps and capture user input, including sensitive PII like banking details and passwords.

Prevent data scraping on the client device by hardening your app code, safeguarding your users' credentials, and blocking malware techniques designed to spy on user input.

Strong code obfuscation

Code obfuscation modifies an app's code to make it difficult for attackers to read and comprehend should they gain access to it. The method conceals the logic and purpose of your app's code, while preserving functionality.

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

Certificate pinning

To enhance 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 gain access to user data.

Employ certificate pinning to ensure that your deployed app instances always communicate with a valid server.

Distributed Cloud Mobile App Shield supports CCPA compliance

Distributed Cloud Mobile App Shield is a comprehensive solution, providing multiple layers of security to protect your app from tampering, malware, reverse engineering, and other threats.

Our multi-layered approach adds complexity to how we protect your app. By employing heuristic algorithms, Distributed Cloud Mobile App Shield can defend against both known attacks and future attacks, including zero-day attacks that exploit unknown flaws in your application code.

With Distributed Cloud Mobile App Shield, F5 offers a best-in-class solution that ensures your app is fortified with the security you need to prevent data breaches and defend your app against known and emerging threats. The solution seamlessly integrates with your programming language of choice and can be deployed within minutes.

©2023 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC08.2023 | WP-GTM-1143515499-Ensure-CCPA-Compliance-For-Your-Mobile Apps