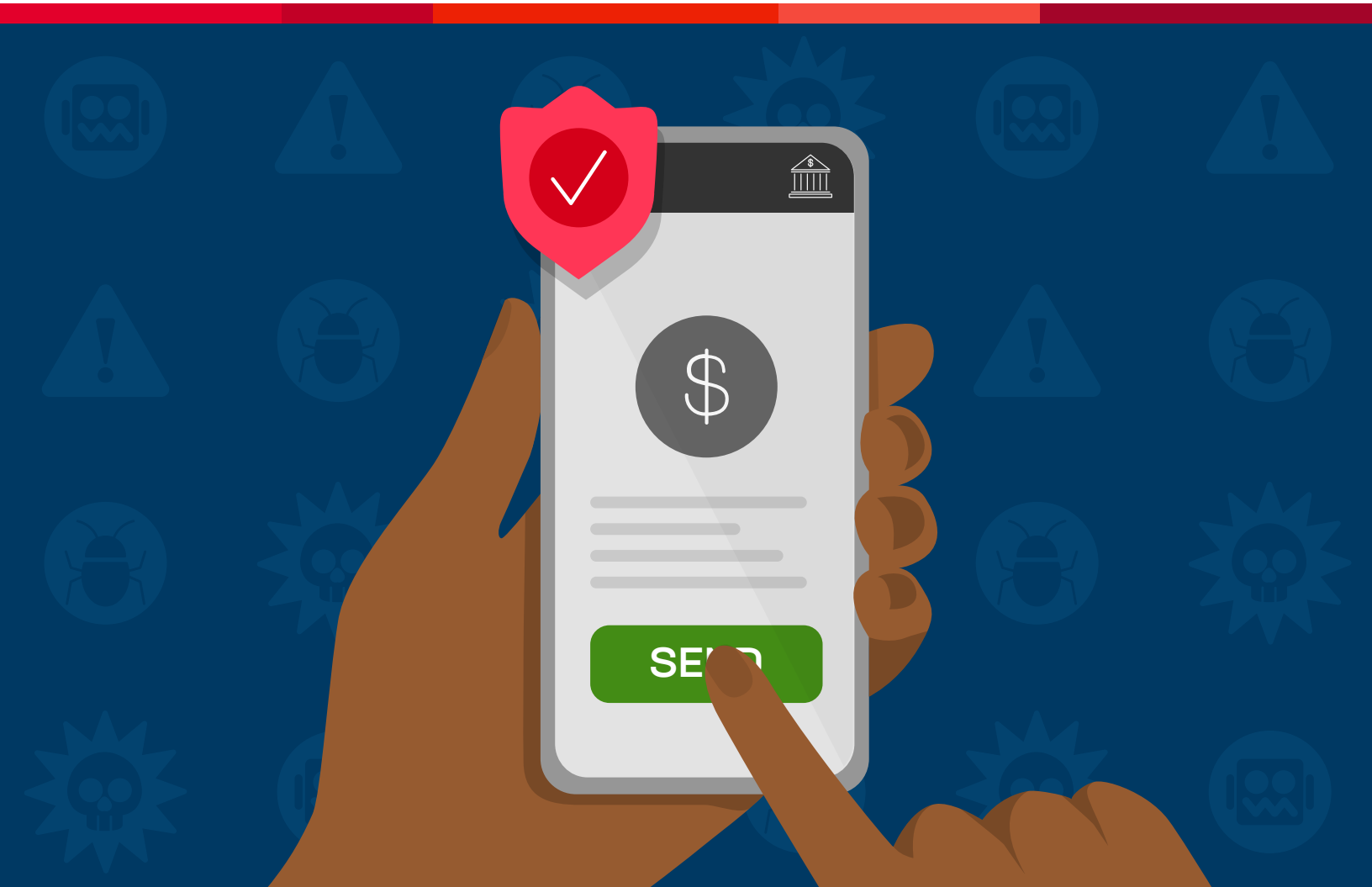
WHITEPAPER

Meet PCI Mobile Security Compliance with App Shielding

Meeting Industry Standards



Mobile payment methods have revolutionized various sectors, including banking, commerce, and retail, by simplifying transactions, purchases, and payments for consumers. However, these advancements also create opportunities for cybercriminals to access highly sensitive customer information.

To ensure PCI compliance, if your mobile application accepts, processes, stores, or transmits payment card information, you must adhere to accepted industry standards for handling and protecting such data.

Achieving compliance involves following a set of objectives and guidelines outlined in the PCI Mobile Payment Acceptance Security Guidelines for Developers. These guidelines cover the security of payment transactions and the risk and controls in the supporting environment.

Section 4 in the PCI Mobile Payment Acceptance Security Guidelines for Developers includes technical guidelines for applications accepting electronic payments on mobile devices. Below we provide a high-level overview on how F5 Distributed Cloud Mobile App Shield can help you meet these guidelines.

Prevent Unauthorized Logical Device Access–Section 4.1

This guideline emphasizes the importance of protecting mobile devices from unauthorized logical access. Employing in-app protection techniques can effectively prevent unauthorized access to a device by reducing the attack surface, making it more difficult for an attacker to modify or reverse engineer the software.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Distributed Cloud Mobile App Shield provides code obfuscation to conceal sensitive APIs and critical operations within your app. This significantly hinders attackers' ability to reverse engineer your app's functionality. Moreover, our state-of-the-art runtime protection promptly detects threats like application debugging, code injection, privilege escalation (device rooting/jailbreak), and application tampering in real-time.

In addition, our security software can detect various factors that indicate a potential security risk, such as a device with developer mode enabled, active Android Developer Bridge, and apps from untrusted sources like Play Store.

Create Server-Side Controls and Report Unauthorized Access–Section 4.2

This guideline emphasizes developing a comprehensive payment-acceptance solution that includes capabilities for preventing and reporting unauthorized access attempts, identifying and reporting abnormal activity, and promptly discontinuing unauthorized access.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline

Distributed Cloud Mobile App Shield enables your applications to receive security event notifications through a callback interface. These notifications can be used to alert end-users or back-end systems about potential security issues promptly.

Prevent Escalation of Privileges–Section 4.3

This guideline suggests that controls should exist to prevent the escalation of privileges on the device. Bypassing permissions can lead to untrusted security decisions and increase the number of possible attack vectors. Monitoring the device for activities that defeat operating system security controls, such as jailbreaking or rooting, is essential. Hardening the app can effectively mitigate the risk of privilege escalation on a mobile device.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Our security software provides critical security checks to prevent the risk of privilege escalation. With several layers of root/jailbreak detection mechanisms, it handles both well-known approaches and heuristics-based indicators to identify symptoms of a compromised device. These security checks can also be configured to notify your back-end system, enabling detailed analytics of usage.

Harden the Applications–Section 4.7

This guideline underscores the need to harden mobile payment-acceptance applications to prevent unintended logical access or tampering with the app, such as code injection or reverse engineering.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Our solution uses various methods to harden your app. By performing tamper detection checks, F5 verifies the integrity of the application signature during launch. Leveraging heuristic analysis of the device, our software effectively detects debuggers and emulators, preventing app repackaging. Moreover, it detects the presence of code hooks and effectively blocks the injection of malicious code into the application process. Additionally, Distributed Cloud Mobile App Shield provides code obfuscation, making it harder for attackers to reverse engineer your application.

Conform to Secure Coding, Engineering, and Testing–Section 4.9

This guideline emphasizes the importance of training developers on PCI standards and secure coding best practices. Developers should document their implementation and create a formal response plan to identify and mitigate new risks. The guideline references the Mobile OWASP Top 10 Risks, which includes the threats "M8: Code Tampering" and "M9: Reverse Engineering," where runtime application self-protection and obfuscation are recommended as countermeasures.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Distributed Cloud Mobile App Shield empowers your application to become self-defending and capable of detecting and reacting to all threats defined in M8 and M9, including jailbreaks/rooting, malware, debuggers/emulators, and unauthorized modification of your application. It also helps prevent common coding vulnerabilities in software development processes, such as insecure cryptographic storage (outlined in M5), ensuring that local data and application data are non-copyable and adequately protected.

Protect the Mobile Device from Unauthorized Applications–Section 4.11

This guideline suggests that all authorized mobile apps should have a mechanism that permits authentication of the source and integrity of the executable file. Additionally, the system should prevent the loading and subsequent execution of applications that lack authentication.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Our tamper detection checks verify and protect the application's integrity, preventing unauthorized modifications. Furthermore, our solution offers the ability to detect and react when an app has been repackaged. In addition, it can detect if apps from untrusted sources are installed.

Protect the Mobile Device from Malware–Section 4.12

This guideline says it's ideal to deploy security software to protect the device from malicious software and applications. It also suggests application hardening/In-App Protection software, can be employed to prevent and/or remove malicious software and applications.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
By using our security software, you will have a protected mobile app that is able to modify its behavior in real-time to interrupt potential malware attacks. Distributed Cloud Mobile App Shield mitigates risks from common malware attack methods, including Android Accessibility API abuse / UI Spoofing, overlay attacks/screen readers, and keyloggers.

Provide an Indication of Secure State–Section 4.16

This guideline requires a trusted execution environment to include mechanisms that indicate to the mobile device user that the payment-acceptance app is executing in a secure state.

How Distributed Cloud Mobile App Shield Facilitates Meeting This Guideline
Distributed Cloud Mobile App Shield can verify the trust level of the execution environment and detect whether a device is in a secure state before launching the app.

Conclusion

Mobile applications have become integral to payment transactions, underscoring the utmost importance of safeguarding these apps and adhering to the PCI Guidelines. With our in-app protection solution, Distributed Cloud Mobile App Shield, app integrity is fortified, and robust defenses are put in place against reverse engineering and hacking attempts.

As detailed in this document, our solutions can help you meet several points in the PCI Mobile Payment Guidelines. Code obfuscation is a powerful measure to deter reverse engineering attempts, fortifying your app's security. Additionally, our tampering detection checks ensure meticulous verification, preserving the app's integrity and enhancing its defenses. Moreover, our solution detects and responds to instances of repackaging, effectively thwarting unauthorized modifications.

Furthermore, it's worth noting that the solutions mentioned in this checklist can also contribute to fulfilling several of the points in requirement 6 in the PCI DSS.

By leveraging F5 Distributed Cloud Mobile App Shield and the solutions mentioned here, your mobile applications can confidently meet the stringent PCI standards, ensuring a secure payment environment, and instilling trust among your value customers.

DC0420 | WP-GTM-1143515499-PCI-Mobile-Payment-Acceptance-Security-Guidelines