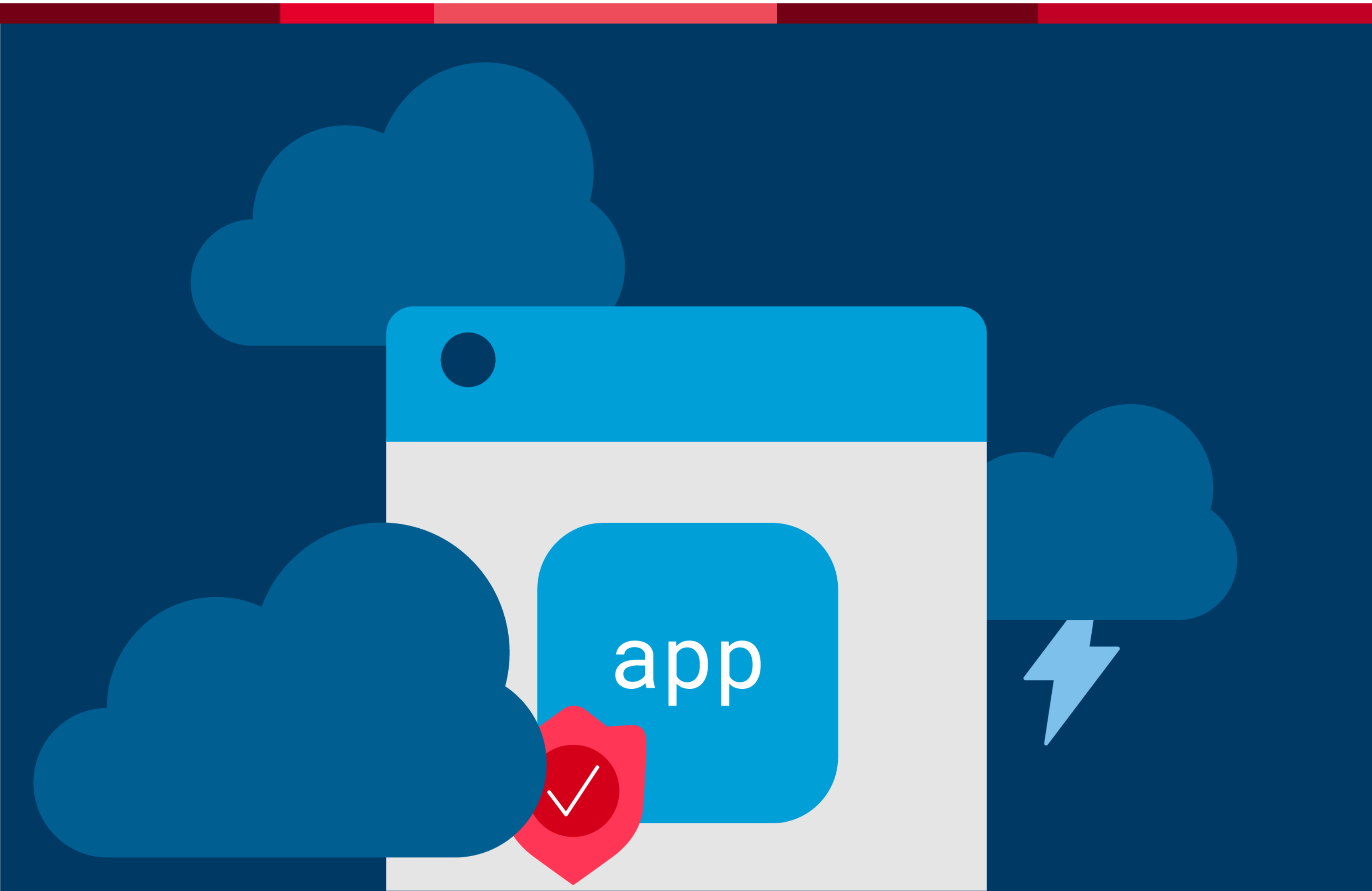
DATASHEET

Protecting Mobile Apps Within Untrusted Environments

F5 Distributed Cloud Mobile App Shield protects your mobile apps from targeted attacks without impacting user experience.



Protecting mobile apps that run within untrusted environments is increasingly crucial as mobile devices become ubiquitous. Hackers and their targeted malware pose a growing threat to the mobile revolution. With the explosive growth of the mobile channel and user demand for anytime/anywhere access to mobile services, app providers face significant challenges in maintaining security which, in turn, increases exposure to malicious attacks.

Why choose F5 Distributed Cloud Mobile App Shield?

Defeats targeted attacks

F5 Distributed Cloud Mobile App Shield proactively protects your apps against targeted attacks, ensuring apps run securely. In the event of a hacker attack, Distributed Cloud Mobile App Shield responds by taking necessary measures to fully protect your apps.

Doesn’t affect the user experience

Distributed Cloud Mobile App Shield protects multiple business apps and is not limited to one application with a specific business logic. It allows for effective scaling across multiple apps within the organization while maintaining an optimal user experience.

Quick to deploy

Distributed Cloud Mobile App Shield offers an automated implementation process. Once integrated, Distributed Cloud Mobile App Shield sifts through the business logic, event, and data flows of the app before binding itself to existing code. This allows organizations to quickly release protected apps without affecting the development timeline.

Trusted by Tier 1 clients worldwide

F5 works with a diverse range of industries, serving a variety of global Tier 1 clients in sectors such as finance, health, IOT, and the public sector. F5’s patented deep protection technology, Distributed Cloud Mobile App Shield, currently protects apps and applications used by more than 100 million users.

Meets regulatory compliance

With Distributed Cloud Mobile App Shield, your mobile apps are tamper-resistant and constantly monitored so you can meet mobile compliance requirements for payments (EMVCo SBMP, PSD2, and PCI), privacy (GDPR and CCPA), and healthcare (HIPAA).

DISTRIBUTED CLOUD MOBILE APP SHIELD PROTECTS YOUR MOBILE APPS AGAINST:

- Malware
- Debugger (Java debugger, native debugger)
- Emulator/fake execution environment
- Cloning of the device
- Rooting/Jailbreak
- Code injection (prevents runtime library injection)
- Hooking-frameworks
- Repackaging (fake, manipulated apps)
- System and user screenshots
- Keylogging: untrusted keyboards
- Keylogging and screen-scraping: untrusted screen-readers
- Native code-hooks
- External screen sharing (content being displayed ‘outside’ the device’s screen, e.g., during screen sharing)
- Man-in-the-app scenarios
- Man-in-the-middle scenarios

How F5 Distributed Cloud Mobile App Shield works

Distributed Cloud Mobile App Shield prevents tampering and hardens your mobile apps with sophisticated obfuscation, malware behavior detection, cryptography, and mobile RASP. You can lower mobile app security risk that results in compliance violations, financial loss, data leakage, fraud, customer churn, and reputational harm without impacting customers.

Tamper protection and shielding

Detect debuggers/emulators, privilege escalation, & app integrity compromises

Mobile app hardening

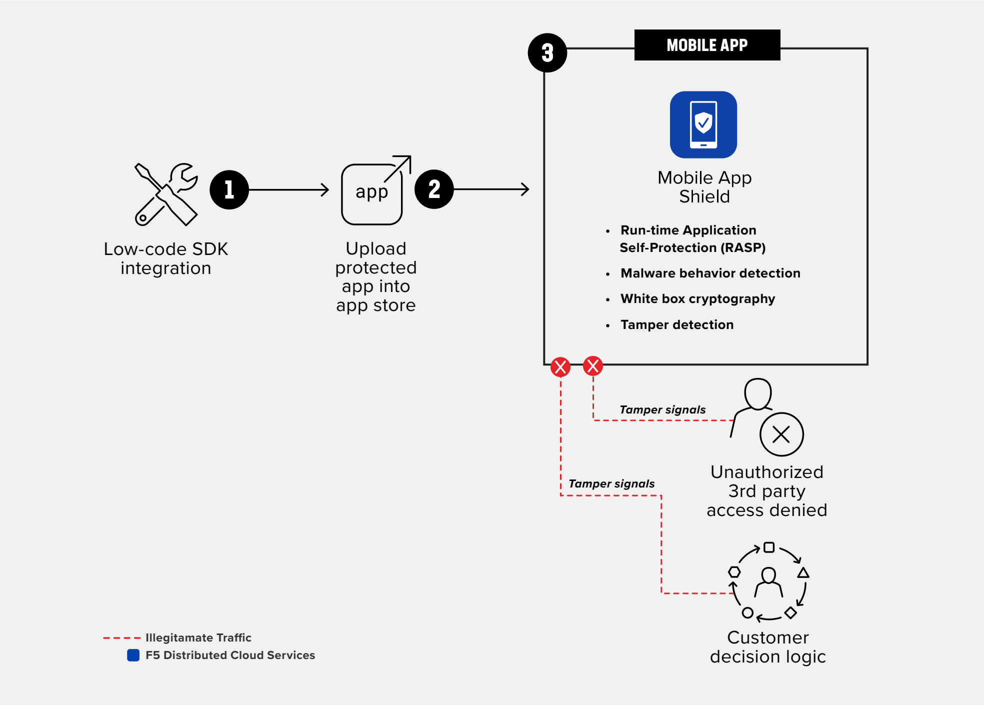
Code-obfuscation and dynamic app binding

Low-code integration

Enjoy fast time-to-value with low installation burden

Asset integrity checks

More in-depth integrity checks of files and assets inside the APK


MOBILE APP
3
1
Low-code SDK integration
app
2
Upload protected app into app store
Mobile App Shield
Run-time Application Self-Protection (RASP)
Malware behavior detection
White box cryptography
Tamper detection
Tamper signals
Unauthorized 3rd party access denied
Tamper signals
Customer decision logic
Illegitamate Traffic
F5 Distributed Cloud Services