outsystems

Safeguard Your Mobile Apps

Using OutSystems AppShield

Cybercriminals now target B2C mobile applications more aggressively, leading to downtime, data exposure, intellectual property theft, and damage to brand reputation. The data exposure and breaches they cause can expose companies to hefty regulatory fines, depending on their geography or industry:

- **GDPR:** €20 mil, or 4% of annual revenue
- **PCI DSS:** Fines up to $100,000 a month until compliance is achieved
- **HIPAA:** Fines up to $50,000 per violation
- **California Privacy Act:** Fines up to $7,500 per violation
- **PSD2:** Member states to define punishment for violating the law

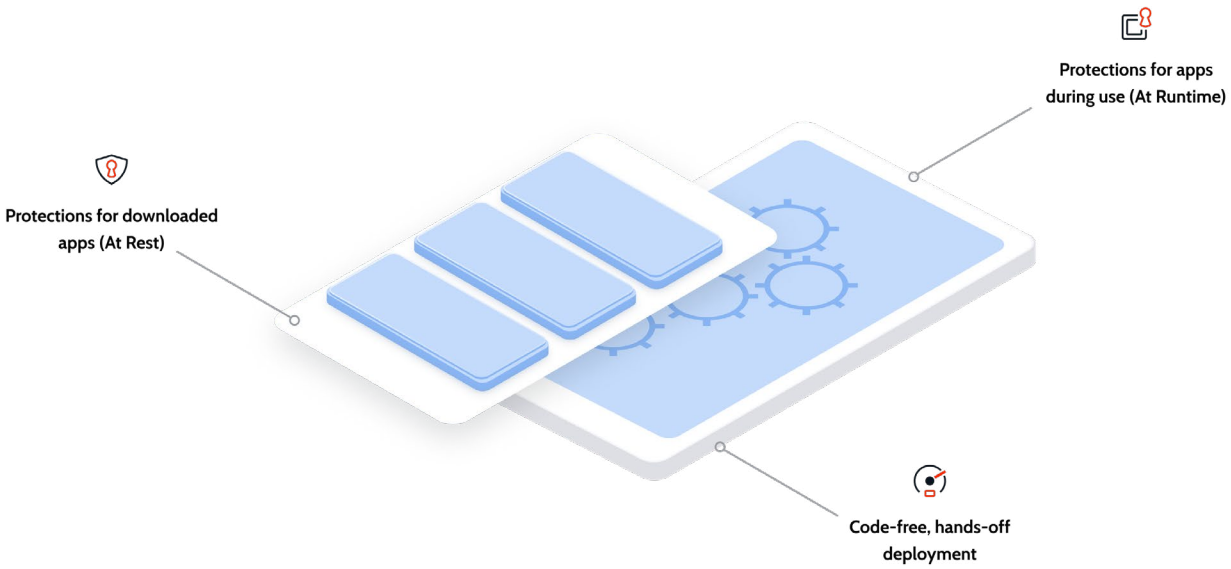
At the same time, building mobile applications that are protected from threats is not easy and requires highly specialized skills. There are no free or open-source solutions available. Going to a third party for a solution is one option for protection, but that can become costly. For example, the cost to secure a mobile app with fewer than 1 million users can be up to $200,000 **per application per year**. For apps with more than 1 million users, the cost is even higher.

To help you safeguard the mobile apps you build with our modern application platform, OutSystems offers AppShield.

What Is OutSystems AppShield?

Mobile devices are like laptop computers used for remote work, and mobile applications are like the software downloaded onto those machines. Your company can take certain security protections for the laptops, such as requiring a VPN, training employees on security practices, and protecting their software. But it just takes one email with a malicious link or the download of an unapproved application that solves an immediate problem to take down a network or unleash ransomware. Mobile applications are now being used as similar entry points into backend and data systems.

OutSystems AppShield, an additional cost add-on, automatically provides extra layers of security during the build process, making applications more resistant to intrusion, tampering, and reverse engineering. One of its compelling advantages is that it protects all the mobile apps you build using OutSystems — unlike the solutions that only protect one application. It also goes above and beyond industry standards to ensure your mobile apps are even better equipped to combat modern attacks.

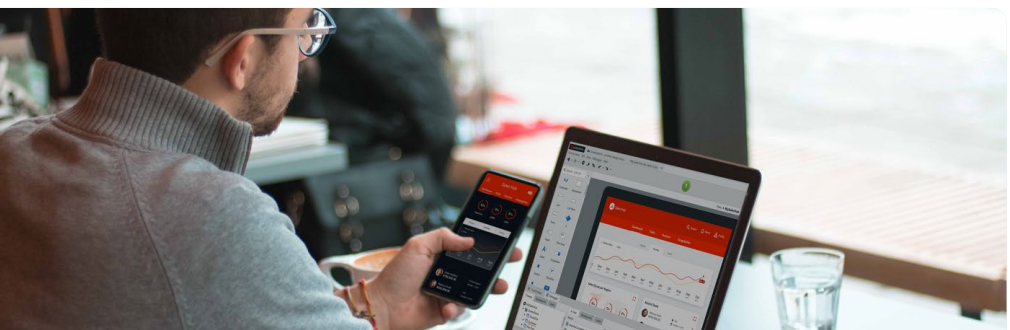


AppShield makes it more difficult for attackers to spoof your app, tamper with its security controls, or inject malicious code. AppShield also prevents your app from running in an insecure environment such as on a rooted (Android) or jailbroken (iOS) device—securing your mobile apps both at rest and at run time.

For IT leaders,
AppShield ensures that teams deliver secure apps that can protect organizations from potential risks and regulatory fines without compromising project timelines.

For developers,
AppShield reduces the manual coding work and valuable development time needed to produce secure mobile apps. Developers without highly specialized training and skills can also build secure mobile apps confidently.

For the business,
Appshield helps protect your company from data leaks and other mobile application security issues that can affect your brand reputation.



Secure Your Mobile Apps Faster With These Features

AppShield and its features support a software development lifecycle (SDLC). Also, OutSystems continuously monitors the latest security attack methodologies and evolves OutSystems AppShield to combat them. Here are the main protections it currently offers for Android and iOS operating systems.

Android

The protection available for Android builds includes:

- **Root detection:** Rooting an Android device allows anyone to gain access to normally restricted data, but it also puts the device at risk. Root detection lets you know if this is the case.
- **Repackaging detection:** Repackaging is when attackers obtain a copy of your app's source code, add malicious functions to it, and redistribute it to users. Detection allows you to protect your app from these evil twins.
- **Code obfuscation:** Obfuscation makes your source code more complicated, preventing hackers from reading it like the Sunday paper.
- **Code injection protection:** Attackers can take advantage of user inputs to take command of your app and make it execute as they wish. Code injection protection blocks these attacks, stopping them from making your app perform functions you never intended.
- **Debugger protection:** To hack your app, first an attacker must know how it works. One of the best ways to find out is with a debugger. Protection prevents hackers from using this troubleshooting software against you.
- **Emulator detection:** Emulators that simulate mobile operating systems are valuable for testing applications, but hackers can use them to look for entry points into your app. Emulator detection can let you know if your emulator is putting your app at risk of being cracked by those you want to keep out.

- **Keylogger protection:** Sometimes used by employers or parents to monitor users, hackers install keyloggers to steal sensitive info like passwords and account numbers. Protection prevents them from stealing your data from under your fingertips.
- **Screenshot protection:** Protect your app from malware that sends screenshots of personal information or your digital wallet to bad actors.
- **Task hijacking protection:** Task hijacking is a way to exploit Android apps when they're idling in the background. Malware asserts itself at the top of an app's back stack, or its history of actions. When the user hits the back button, the malware will send them to a malicious app in disguise.

iOS

Apple iPhones and iOS applications are somewhat harder to hack than Android because iOS is only deployed on mobile devices from one manufacturer. However, there are ways to hack iOS and apps from the Apple AppStore. Like Android, iOS apps also need these protections provided by AppShield:

- Repackaging detection
- Code injection protection
- Debugger protection
- Screenshot protection

Most importantly, the protection available from AppShield for iOS builds includes **jailbreak detection**. Like rooting, jailbreaking an iPhone gives the user access to restricted data areas on the device, also compromising the device. AppShield can let you know if this is the case so you can determine how your app will proceed.

Fully Integrated, Code-Free Deployment

With AppShield, you'll never again have to make the difficult decision between app security and time to market.

The real "secret sauce" of OutSystems AppShield is its seamless, pre-built integration with our **Mobile Application Build Service (MABS)**. After a **simple initial setup** that only takes minutes, iOS and Android applications packaged and released with MABS will automatically include OutSystems AppShield's advanced protections, making it an essentially code-free and hands-off experience.

What Risks Does AppShield Address?

OWASP, or the Open-Web Security Project, is a non-profit foundation dedicated to identifying and addressing the biggest risks in software security. Helmed by cybersecurity leaders from across the globe, OWASP works to catalog the best security measures to promote better practices among the development community. AppShield addresses a number of OWASP's top ten security risks. Let's take a look.

Protecting Against Improper Platform Usage (OWASP M1)

When you're building an app for a mobile OS, there are standards to its build. If you don't meet them on iOS, your app will never make it to the App Store. Google's Android OS is more open, but there are still guidelines. When apps don't meet these standards, it's a security risk that OWASP has identified as improper platform usage. Therefore, if an app is run on a rooted or jailbroken device or through an emulator, suddenly your air-tight build is in jeopardy. That's why AppShield adds on root and jailbreak detection, blocks emulators, and identifies the permissions enabled on the device—providing an extra layer of security.

Addressing Insufficient Cryptography (OWASP M5)

Encryption is the root of any security strategy. Source code is scrambled, transferred, and decrypted on the other end with a key. Not all encryption algorithms are created equal, and OWASP identifies this issue as insufficient cryptography. If an attacker can break the encryption and see your app's code, that's when they can exploit it. Hackers can also use a jailbroken iPhone to freeze an app after the device decrypts it but before it loads, granting access to your unscrambled source code. Jailbreak detection in AppShield prevents foul play. And if a cybercriminal does break through, AppShield blocks the copying of local data. AppShield also includes proper encryption, repackaging protection and ensures security mechanisms can't be removed from your app.

Ensuring Client Code Quality (OWASP M7)

If your app's code isn't high quality, attackers can use your app against you. They might try a buffer overflow or code injection attack. OWASP identifies this as client code quality. When OutSystems generates your code, you can be sure it's up to snuff. But say you coded a custom addition to your mobile application by hand, or you're plugging in third-party code that isn't up to standard. In these cases, AppShield gives you the extra protection you need. It includes code injection protection, repackaging detection, and verification of the application signature. It removes debug information from the application code and blocks debugger and emulator access. It also allows the report of security controls and device anomalies to application code for specific handling.

Preventing Code Tampering (OWASP M8)

Should an attacker gain access to your app's source code, they might try a tactic called snooping—or copying your code, adding malicious functionality, and masquerading as you on third-party app stores. OWASP calls this code tampering, but you can think of it as app identity theft. With AppShield, you can be certain nobody but you can get access to your code, preventing them from modifying it and tainting your good name. How's that? AppShield stops copycats in their tracks with root, jailbreak, and repackaging detection. Also, it blocks hackers from accessing debuggers and emulators and using them to find entry points to your data.

Preventing Reverse Engineering (OWASP M9)

The easiest way to break something is to see what makes it work. In cybersecurity, that means reverse engineering. AppShield includes code obfuscation and blocks debugger and emulator access, thus preventing reverse engineering of your mobile app, so you can keep your code to yourself.

Is OutSystems AppShield Right for My Organization?

Web and mobile applications built using OutSystems already include an extensive set of built-in security features and are protected by default from the **top security threats identified by OWASP**. So, the fact of the matter is, not every application needs advanced app protection.

Answering these questions can help you determine if AppShield is right for you:

1. What sensitive data and features, such as a private key, token, and user-input (password, credit card, account number) are used by the app that you need to protect?
2. How is your app security structured to prevent data leakage from compromised devices?
3. How capable are you of maintaining your app's integrity and security?
4. How are you preventing your app from being repackaged and redistributed with malware?

5. How is the content of your app protected from screen readers and other apps that might troll for data?
6. How are you protecting against various methods of credential theft?
7. What measures are you taking to protect your app from the growing number of mobile malware threats?
8. How are you protecting your app from hooking mechanisms that capture API calls that include parameters that reveal user authentication credentials?
9. How are you preventing code injections into your app?

State-of-the-Art Protection From State-of-the-Art Attacks

Security is crucial in app development. AppShield is the suit of armor that goes over the chainmail—the extra layer of defense to protect your applications from advanced attackers. As they get better at breaking in, we get better at keeping them out. Implementation is easy and requires little maintenance, and that means developers can spend their time making sure apps are built fast and built right, without worrying about security gaps.

If your organization is handling sensitive data, is subject to privacy regulation, or works in an industry where security is priority number one, AppShield will provide the next-level protection you need.

To see AppShield in action, check out our **Accelerate Secure Mobile App Dev with OutSystems webinar**.

www.outsystems.com