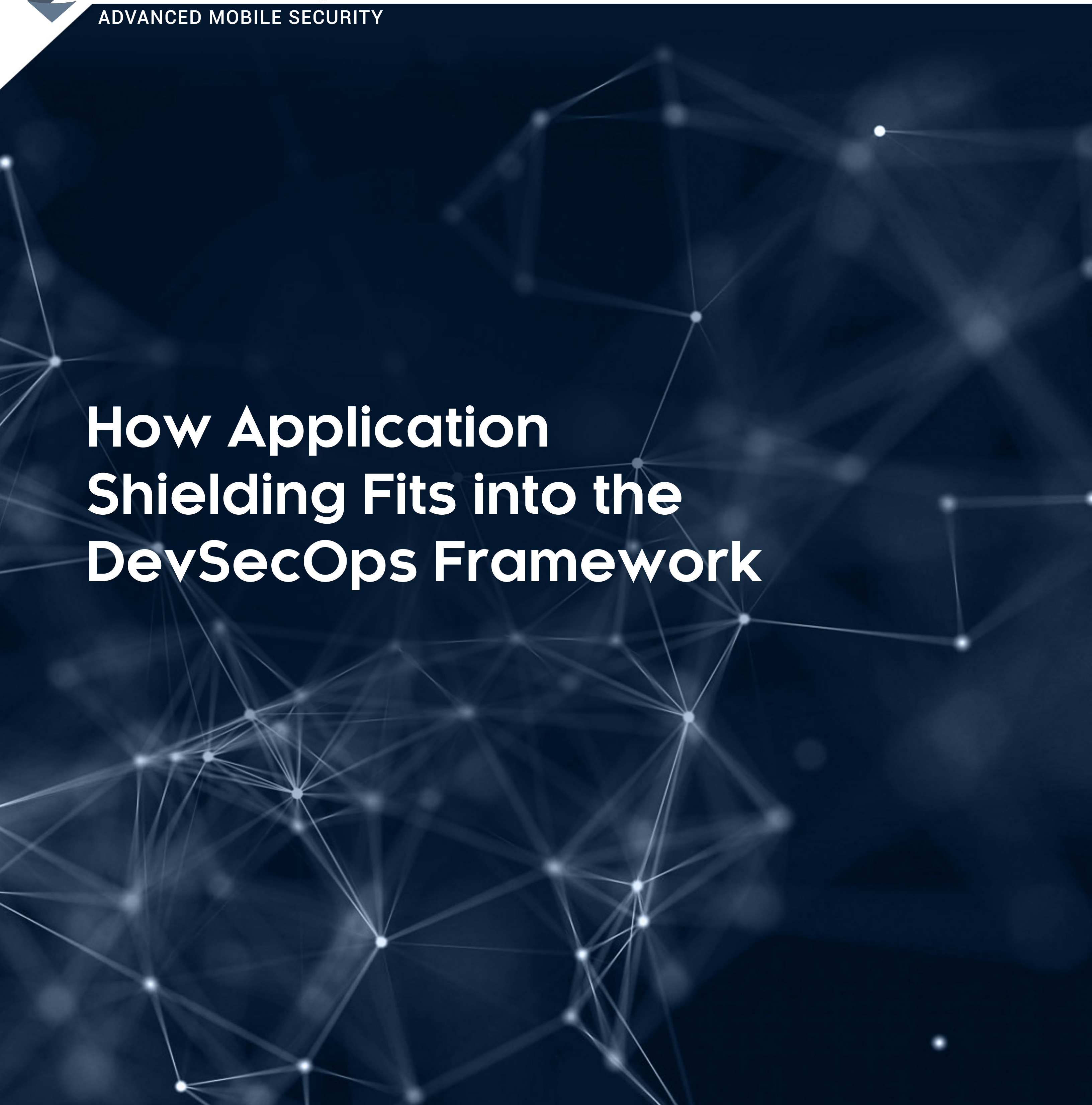
ZIMPERIUM®
ADVANCED MOBILE SECURITY



How Application Shielding Fits into the DevSecOps Framework

What is a DevSecOps framework?

The DevSecOps framework integrates security into the standard DevOps cycle for application and program development. A more traditional approach to development positions security as a discrete department that protects an organization's systems overall, under which security testing of applications is one role among many. DevSecOps embraces the shift-left approach to security, making it an integral part of the software development lifecycle (SDLC) from the start.

Within a DevSecOps framework, security best practices get baked in at every phase of development, so apps are more secure, have fewer vulnerabilities, and require less patching. Notably, an Agile DevSecOps framework focuses on maintaining development velocity without incurring security debt which will have to be paid down by the organization later.

The need for DevSecOps

The focus on speed-to-market in the software world puts constant pressure on development teams. The pressure to keep up with changing demands, continuously improve features, yet ship apps quickly, often undercuts security concerns and testing. Research on mobile app security found that 83% of apps are distributed with at least one security flaw.

This constant time pressure lures some dev teams into taking a ship now, patch later attitude. However, as most teams know, once one project is finalized, it's straight onto the next one, and the time and resources to fix release-day issues never materialize.

On top of those initial security flaws, new problems always arise as flaws in underlying code, third-party components, or security libraries are uncovered. This creates a perfect storm of weak app security and poor app after-care, which ups the risk of data breaches, loss of user trust, and regulatory reprimand.

The benefits of a DevSecOps framework

In an environment of constant development, adopting a DevSecops framework is essential for several reasons:

1. Speed-up development time
Security problems discovered post-development can lead to serious delays. Integrating security processes and testing throughout the development lifecycle—from initial planning through release—minimizes the need for time-consuming and expensive fixes after the fact. It also eliminates bottlenecks between developers and security teams that commonly arise in non-DevSecOps environments.

2. Reduce costs
Publishing an insecure app with numerous flaws creates a security debt that accumulates as the app grows in downloads and structural importance. This debt will cost significantly more to pay down later in terms of risk created and potential costs of data breaches, productivity loss, and regulatory fines. Integrating security from day one through a DevSecOps framework may require a higher initial investment, but it saves on major post-production costs by producing apps that are less prone to security failures and meet compliance requirements.

3. Improved customer experience and trust
End users can have a complicated relationship with application security; they want their data protected but don't enjoy onerous measures that detract from their experience. However, research shows that, ultimately, poor security drives users away from your organization. PwC found that 85% of users will avoid doing business with an organization if they have concerns about its cybersecurity and privacy practices. A DevSecOps framework designs in security and finds and fixes issues at each stage, allowing time to address any usability consequences.

4. Faster security fixes
Taking a DevSecOps approach means integrating vulnerability scanning and patching as processes in an app's SDLC. This enables more secure and faster support after an app is released, as the team stays together to iterate through the post-release phase, rather than being broken up and moved to different projects. Ultimately, the knowledge and documentation standards of a DevSecOps framework allow teams to find and fix flaws more quickly.

How application shielding fits into a DevSecOps framework

Application shielding plays an important role in a DevSecOps team's efforts to improve app security without hampering development speed or increasing costs. Adding a sufficient number of security experts to keep up with development demand can be difficult; GitHub puts the developer to security pro ratio at 500:1. To keep pace with the security requirements of a DevSecOps framework, in-house teams need tools that are easy to integrate and won't hold up the development process.

Application shielding helps DevSecOps teams work more efficiently by embedding protections to secure source code and IP from reverse-engineering and tampering attempts:

- Code tampering
- Malware injection
- Encryption key extraction
- Reverse engineering
- Side-channel attacks
- Data theft

By incorporating a robust application shielding solution into the build process, security teams can better prioritize and manage vulnerabilities discovered during testing. They can focus on fixing critical issues, secure in the knowledge that their software can resist attacks against any remaining unfixed vulnerabilities.

It also provides protection against future vulnerabilities that have not yet been discovered. No security testing solution can catch every security bug and hackers develop new exploits all the time. A good in-app protection solution keeps software secure against these edge cases and unknown threats.

Zimperium's mobile app protection suite meshes with a DevSecOps framework through a multipronged approach to hardening software against attack. This includes:

- Advanced code obfuscation to frustrate reverse engineering attempts
- Rooting/jailbreaking detection, anti-debugging mechanisms, and other protections to prevent static and dynamic analysis
- White-box cryptography to keep encryption keys safe from exfiltration attempts
- Integrity checkers to detect attempted code manipulation

Conclusion

Adding application shielding to your DevSecOps framework improves your security capabilities without adding an extra burden to your security resources. This helps to reduce risk and meet compliance requirements by building security into your development processes right from the beginning.

To find out more about how our application protection can support your DevSecOps teams, contact us and talk to one of our security experts.

ZIMPERIUM®

4055 Valley View Dallas, TX 75244
844.601.6760
info@zimperium.com