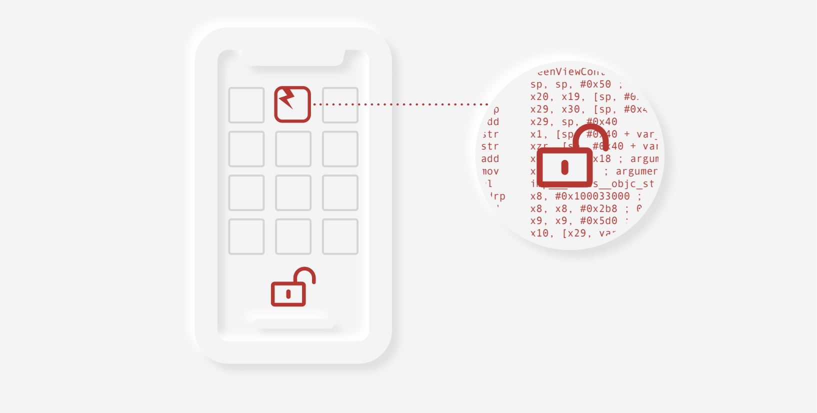
Solution Brief

Digitial.ai Application Protection for iOS (formerly Arxan)

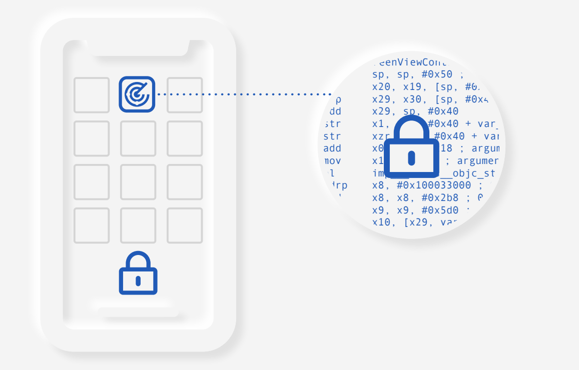
iPhones and iPads are primary customer touch points across all industries, and as a result, have created an expansive attack surface. The Apple App Store alone offers millions of apps to end users to download to their iOS devices — outside any secure perimeter — and run them in zero-trust environments. Today's cybercriminals are exploiting this distribution environment to expand their operations to attack mobile apps for financial gain by stealing customer identities, intellectual property, or by gaining access to back office systems. A recent report from Accenture Consulting found that a majority of iOS banking apps contained moderate to severe app risks.



Mobile app attacks all have a common threat vector: they all start with reverse engineering — the disassembly of apps back to the original code. Reverse engineering of an iOS app can be executed using commonly available developer tools running on a jailbroken iOS device. Once disassembled, bad actors can uncover critical algorithms, discover keys and sensitive data, obtain API access, and understand how to best tamper with code. Once app code is understood, counterfeit apps can be created to steal user credentials. Or to execute even more insidious attacks, bad actors can utilize information gained from how apps interact with back office systems to stage attacks focused on an organization's servers.

iOS app protection

Digital.ai Application Protection for iOS features automated, comprehensive, and customizable protections for iOS apps developed using the most popular development environment and languages. Digital.ai's application protection solution goes beyond traditional runtime application self-protection (RASP) by providing jailbroken device detection, layered and adaptive app protection, data encryption and threat alerting, and analytics.



iOS code protection

Digital.ai code protection can rapidly harden iOS applications with patented guarding technology, self-repair capabilities, and tamper resistance using a unique, configurable guard network methodology and threat detection. Alerting the business to attacks in progress is key to preventing damage, and Digital.ai integrated threat detection can alert organizations if apps are operating on jailbroken devices at the first sign of code compromise.

Digital.ai code protection consists of interconnected guards and sensors that together create a protection blueprint. This protection blueprint is applied without requiring source code modifications. Initial code protection can deliver an essential level of protection within minutes that includes threat detection and can be applied without the need for complex security configurations or deep security knowledge. Digital.ai's protection process is straightforward to implement, has minimal impact on the software development lifecycle, and can be easily integrated into DevSecOps production environments. Once created, protection blueprints can be automatically updated for inclusion in successive builds — improving follow-on app security without requiring additional development resources.

Once deployed, identified app threats can be dealt with in the short-term with defensive tactics, such as locking account access and disabling app functionality. Longer term corrective action can then include enhancing protections with code, and/or data and key encryption, to remediating and tailoring future protections to specific threats.

Digital.ai App Aware (formerly Arxan)

Digital.ai App Aware provides unique, timely visibility into where, when, and how apps are being attacked with integrated threat detection. This capability enables app developers to be proactive and respond to risks and app reverse engineering attacks before they turn into large scale attacks.

Digital.ai Application Protection for iOS

Rapid time-to-protection that can be integrated into the DevSecOps process without disrupting development or production with smooth, post-code integration into existing development operations and frameworks

Supports C/C++, Objective C/C++, Swift along with Xcode, and delivers app code-level protection that does not require source code changes and has minimal impact on the software development life cycle (SDLC)

Static and runtime protections to safeguard applications against reverse engineering attacks and tampering

Self-protection code guards monitor and defend apps against attack — eliminating single point of protection failure

Integrated threat analytics for real-time threat detection and alerting that delivers an understanding of the threat posture of every published app

Jailbreak detection and notification to alert the business to apps running in compromised environments, so the business can take appropriate action

Platform support that keeps pace with the latest versions of iOS operating systems and tools

Digital.ai White-Box Cryptography (optional) to encrypt key and sensitive data to protect in-app information and secure back office interactions

Digital.ai White-Box Cryptography

Optional Digital.ai White-Box Cryptography can also be applied to enhance protection by encrypting static and dynamic keys and protecting app data with mathematical techniques and transformations so they cannot be found or extracted from the app.

Protecting apps from inside out

Digital.ai provides comprehensive, app-level security to protect against a range of threats or to enforce enterprise app governance — expanding the corporate perimeter of trust. Digital.ai provides a broad range of patented security capabilities to protect applications in the wild — such as a dynamic app policy engine, code hardening, obfuscation, white-box cryptography and encryption, and threat analytics.

About Digital.ai

Digital.ai enables enterprises to focus on outcomes instead of outputs, create greater business value faster, and deliver secure digital experiences their customers trust. The Digital.ai Value Stream Platform seamlessly integrates all the disparate tools and processes across the various value streams, uses data and AI/ML to create connective tissue between them, and provides the real-time, contextual insights required to drive and sustain successful digital transformation. With Digital.ai, enterprises have the visibility they've been seeking to deliver value, drive growth, increase profitability, reduce security risk, and improve customer experience.

Learn more at **Digital.ai**