digital.ai™

Solution Brief

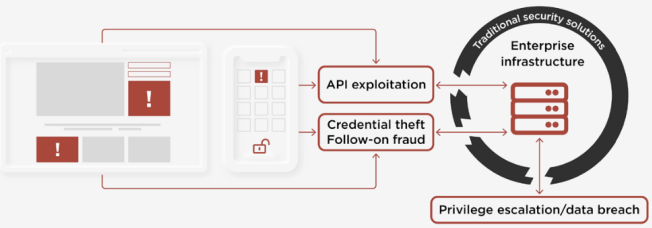
Digital.ai Application Protection (formerly Arxan)

Protecting apps in a zero-trust world

Customers and employees are increasingly interacting with organizations via an app — whether it's mobile, web, or desktop. As apps become more sophisticated and integrated with corporate infrastructure, the need to protect customer information and business data is greater than ever. Securing this new endpoint is key to preventing breaches, brand damage, financial loss, intellectual property theft, and government penalties.

Traditional app security and network defenses cannot protect apps from reverse engineering nor attacks that originate from within the apps.

These attacks can lead to direct data breaches, compromised IDs from skimming attacks, and stolen IP.



Apps for anyone

Millions of apps have been created for customers, employees, and partners that are critical to industries such as mobile banking, payments, eCommerce, connected medical and automotive, entertainment, and gaming. These apps are valuable targets because they are access points to corporate infrastructure that contain everything from customer credentials to intellectual property. Applications are vulnerable to attack when they operate outside of the traditional security perimeter, such as when they are made available via public app stores, or when web applications are run in browsers.

Bad actors can exploit unprotected apps through reverse engineering to gain an understanding of an app's code and how it communicates with back office systems. Once understood bad actors can insert malicious code to steal personally identifiable information, intellectual property, or via follow-on attacks utilizing exposed keys.

Protect

Comprehensive code-level security

- Obfuscates source code, inserts honeypots, and implements other deceptive code patterns to deter and confuse threat actors
- Triggers defensive measures automatically if suspicious activity is detected, including app shut down, user sandbox, or code self-repair
- Injects app code protections and threat detection sensors the app binary after code development, without disrupting DevOps processes

Alert

Real-time threat data

- Notifies organizations of real-time attacks on apps, and provides the ability to shut down apps or trigger step up authentication
- Insights help optimize and adapt protection based on attack insights and trends including how, when, where, and by whom the app is targeted
- Delivers threat data feeds end to end, making threat data accessible via a browser or easy integration with existing SIEM, BI, and fraud prevention platforms

Encrypt

Key and data protection

- Encrypts static or dynamic keys and data embedded or contained within app code
- Protects sensitive data at rest within an app or in transit between the app and server
- Supports all major cryptographic algorithms and modes with FIPS 140-2 certification

Apps are today's endpoint — and your most vulnerable attack vector.

Digital.ai Appplication Protection solutions include:

Digital.ai Application Protection for Android — providing protection against reverse engineering and tampering, key and data encryption, and malicious package detection for Java and Kotlin based apps.

Digital.ai Application Protection for iOS — delivering app protection, key and data encryption, and threat detection for apps developed with all major iOS development languages.

Digital.ai Application Protection for Hybrid — protecting JavaScript and native code for apps designed to run on iOS and Android, with key and data encryption for native code and threat detection for all protected apps.

Digital.ai Application Protection for Web — protecting browser-based web apps by securing "open text" JavaScript with obfuscation, alerting on reverse engineering or HTML page attacks, along with an in-app firewall to prevent data exfiltration by blocking browsers from connecting to hostile websites.

Digital.ai Application Protection for Desktop or Server — protecting apps running across all major desktop and server operating systems without requiring changes to source code to prevent reverse engineering attacks. The app can be located on-premises or in the cloud.

Apps for the workforce

Custom-built and commercial productivity apps to improve workforce productivity typically run on unmanaged devices owned by employees, contractors, and partners. These unsecured apps deployed by an organization pose a significant business risk. This threat creates an ongoing management struggle to find effective ways to securely deploy mobile apps to maximize adoption and maintain privacy without requiring device management or enrollment. To address this problem, businesses need to adopt a three-phase app management approach.

Digital.ai App Management

First, apps need to be properly onboarded to ensure they are free of malware and privacy risks. Secondly, custom and off-the-shelf apps need to be wrapped with security, analytic, and management policies. These app wrapper enhancements allow IT teams to manage governance at the app level to enforce enterprise single sign-on, app usage and analytics, app-level VPN, app-expiration, copy/paste disable, jailbreak detection, and more. Lastly, vetted and wrapped apps need to be made available to users via corporate-branded enterprise app stores to maximize distribution control and user adoption.

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