digital.ai

Solution Brief

Digital.ai Application Protection for Android (formerly Arxan)

Mobile computing continues to grow across all industries, and at the same time it's creating an even bigger attack surface. Public app stores enable end users to download them to their own devices — outside the business perimeter — and run them in untrusted environments. Today's cybercriminals are exploiting this distribution environment and have expanded 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 more than 60% of mobile banking apps are at risk for reverse engineering attacks.

Mobile app attacks are all executed through reverse engineering — the disassembly of apps back to the original code through the use of commonly available tools. Once disassembled bad actors can uncover critical algorithms, understand how to best tamper with code, uncover keys, sensitive data, and obtain API access. To counteract these threats, apps must be hardened to protect against reverse engineering, defend against compromises, and respond to threats. Additionally, to close the loop and prevent threats from becoming large scale attacks, apps need to be able to report back to the business about the kinds of threats being encountered.

Android app protection

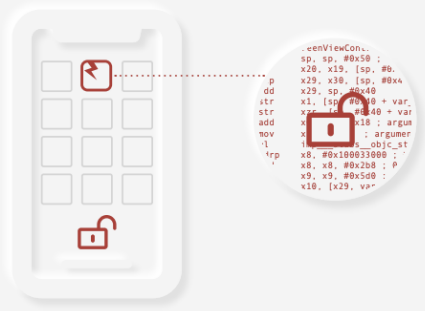
Digital.ai Application Protection for Android features automated, comprehensive, and customizable protections for applications developed using Java or Kotlin.

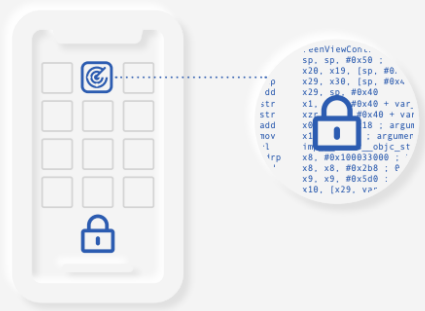
Digital.ai's application protection solutions go beyond traditional runtime application self-protection (RASP) by providing rooted device detection, layered and adaptive app protection, data encryption, and threat alerting and analytics.

Android code protection

Digital.ai code protection hardens Android applications with patented guarding technology, enabling RASP, tamper resistance, and self-healing measures using a unique, configurable guard network methodology. This not only protects against attacks, but also detects and alerts the business at the first sign of code compromise.

Digital.ai code protection consists of interconnected code protection units that together create a protection blueprint. This protection blueprint is applied to the final application after the build process without requiring source code modifications. Initial code protection delivers a level of protection within minutes that includes threat detection and is applied without requiring app security expertise. Digital.ai's protection process is straightforward to implement and 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.





Zero-trust is a concept centered on the belief that organizations should not trust anything inside or outside their perimeter and instead verify anything and everything trying to connect to its systems before granting access.

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, data, and key encryption to provide remediation to the specific threats identified.

Digital.ai threat intelligence

Digital.ai provides unique, timely visibility into where, when, and how apps are being attacked. Digital.ai App Aware (formerly Arxan) 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 Android capabilities

- Rapid time-to-protection that is integrated into the DevSecOps process without disrupting development or production with smooth, rapid post-code, on-premises, or cloud-based integration into existing development operations and frameworks
- Java and Kotlin based app code-level application protection that does not require source code changes and has minimal impact on the software development life cycle (SDLC)
- Static and Active protections to safeguard applications against reverse-engineering attacks
- Self-protection code guards that monitor and defend apps and themselves against attack — eliminating single point of protection failures
- Integrated threat analytics delivers real-time threat detection and attack alerting to provide an understanding of the threat posture of every Digital.ai deployed app
- Root detection and notification to ensure apps are running in secure environments, so the business can take appropriate action
- Malicious Package Detection
- Platform support that keeps pace with the latest versions of Android operating systems

Digital.ai key and data protection

Digital.ai provides unique, timely visibility into where, when, and how apps are being attacked. Digital.ai App Aware (formerly Arxan) enables app developers to be proactive and respond to risks and app reverse engineering attacks before they can be turned into large scale attacks.

Protecting apps from the 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