Digital.ai Essential App Protection

The need has never been greater to protect the billions of app endpoints that drive customer engagement and employee productivity.

Unfortunately, a significant majority of the millions of business apps available from public app stores and countless websites are insufficiently protected against threats. A recent study conducted by Aite group found that **97% of financial apps lack binary code protections, leaving them vulnerable to even the most basic reverse engineering attack.**

Not only that, but DevOps teams are also not sure how to protect their apps due to a lack of visibility into how, where, and by whom their apps are being attacked. At the same time, with app security expertise in short supply, DevOps teams need an easy way to integrate runtime protection into existing CI/CD pipelines.

Bad actors can exploit unprotected apps 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 (PII), intellectual property (IP), and other sensitive data from the client side of the application. Or, they can steal encryption keys and API secrets to conduct follow-on attacks to gain access to critical infrastructure or databases.

A low-code approach to protecting your applications

Digital.ai Essential App Protection provides organizations with a quick and easy way to gain visibility into the security posture of apps. The solution prevents apps from running in unsafe environments while providing timely intelligence into how, when, and where they are being attacked. DevOps teams can rapidly integrate mobile app security into code pipelines — without heavy lifting or ongoing management.

With Digital.ai Essential App Protection, security can be applied after coding by non-technical team members rather than developers with security expertise. The result is that organizations can quickly protect every app, not just the most important ones.

Proactive app security with intelligent threat detection and response

The key to leveling the playing field with bad actors is knowing how, when, and where they are attacking apps. However, app owners are often blind to the threats their apps face once they are published, essentially creating an "open-loop" environment. The only way app security teams can respond to attacks is after the fact — after the damage has been done.

Unprotected "open-loop" environment   Secured "closed-loop" environment

Root & jailbreak detection
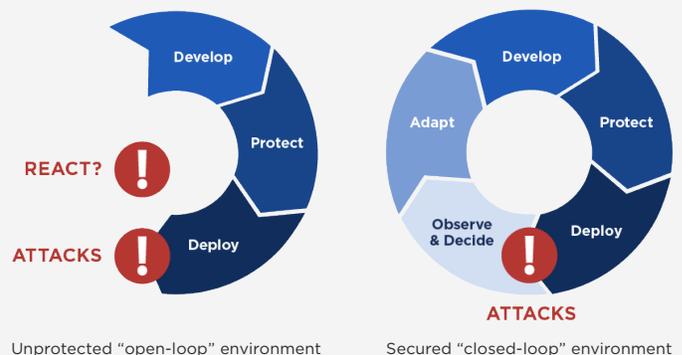
With Digital.ai Essential App Protection, app owners gain timely intelligence from the moment an app is downloaded into the security posture of their protected apps. App security teams can continuously assess potential threats and dynamically adapt security posture as appropriate.
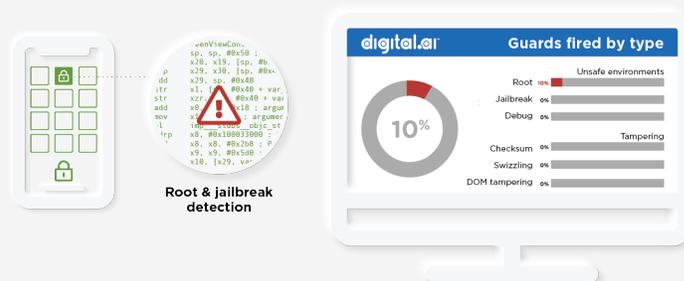
Erect the first line of defense against reverse engineering attacks

- **Runtime Self-Protection** Detect and prevent app instances running in unsafe environments like rooted or jailbroken devices and debuggers.

- **Actionable Threat Insights** Take action on timely intelligence into compromised devices with targeted follow-on response and protection.

- **Easy integration** Use a single script to integrate into CI/CD pipelines and instrument runtime protection without any code modifications.

Quickly protect every app and make intelligent decisions on the appropriate level of protection.

- **Low code** Does not require any configuration or source code modification, just a single script in the CI/CD pipeline.

- **Visibility** Threat insights that remove the guesswork out of pinpointing where your application is being attacked.

- **Compatibility** Platform and language agnostic solution that can protect both iOS and Android apps.

- **Extensibility** Upgrade to comprehensive app and data protection to prevent tampering, IP theft, and reverse engineering as security requirements evolve.

Two steps to understanding app threats

Step one — protect business-critical app code and underlying data they access and store against reverse engineering.

Step two — monitor these apps in real-time to understand the threat environment they are operating in from the minute they are downloaded from an app store or are loaded in a browser.

Digital.ai Premium App Protection solutions

As your App security teams continuously assess potential threats, they may determine that more comprehensive defenses are needed. To address this, Digital.ai also provides configurable, app-level security solutions to protect against a range of threats. These solutions provide a broad range of patented application and data protection capabilities to protect applications in the wild by preventing reverse engineering, code tampering, IP theft, data exfiltration, malware, and more in today's ever-changing threat landscape.

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