



Effective: July 24, 2025

Application Protection for Mobile: Pro and Premium Editions

Application Protection for Mobile (available in Pro and Premium Editions) provides Customer with a license key and associated on-premise Software that can be used to harden mobile Customer Applications with runtime self-protection, anti-tampering, and obfuscation code system protections. Application Protection for Mobile: Pro provides Customer with injected protection of iOS, Android, and Hybrid Apps; and Digital.ai-defined application protections. Application Protection for Mobile: Premium provides Customer with injected protection of iOS, Android, and Hybrid Apps; and Customer customizable application protections.

Product	License Metric	Deployment
Application Protection for Mobile (Pro & Premium Editions)	Per Application	On-Site

Product or Service Limits

Limit Metric Type	Limit Metric Quantity	Impact
Customer Application(s) / Target Application(s) Protected (Pro & Premium Editions)	1	Protections beyond the limit metric are prohibited without additional purchase.

Optional Purchases

Product	License Metric	Deployment
AppAware	Per Customer site or named account	On-Demand

Requirements: Use of Application Protection for Mobile - Pro requires that Customer's Host Platform (Host System Requirements) and Customer Application (Target App Requirements) meet the specifications provided for in the support matrix (system requirements) of the applicable Documentation:

- [Application Security for Mobile: Pro](#)

Requirements: Use of Application Protection for Mobile - Premium requires that Customer's Host Platform (Host Platform Specifications) (Host System Requirements) (Host Operating System and Toolchain) and Target Platform (Target Operating Systems) meet the specifications provided for in the support matrix (system requirements) of the applicable Documentation:

- [Application Security for Apple](#)
- [App Security for Mobile: ARM](#)
- [App Security for Android App](#)
- [App Protection for Android Native](#)
- [App Protection for Linux ARM](#)
- [Java Bytecode Protection](#)



Additional Terms:

Artificial Intelligence Features: If the Product or Service includes features that utilize artificial intelligence (“AI Features”), Customer acknowledges that: (i) Digital.ai does not guarantee the accuracy, completeness, or reliability of any outputs generated by AI Features; (ii) Customer is solely responsible for any decisions made or actions taken based on outputs from AI Features; and (iii) Customer agrees not to use AI Features in any high-risk or critical environments where errors or inaccuracies could lead to significant harm or damage.

Definitions:

“Host Platform” means the operating system (e.g., Windows, MacOS, and Linux) and hardware architecture on which Customer installs Application Protection for Mobile (Pro or Premium Edition).

“Hybrid Apps” mean a software application built with JavaScript frameworks (e.g., Ionic, Cordova) capable of running on multiple operating systems (e.g., iOS, Android).

“Target Platform” means the operating system (e.g., iOS, Android) and hardware architecture on which the Customer Application is intended to run.

