Effective: March 20, 2026

Mobile Application Hardening: Per APP

Mobile Application Hardening: Per APP provides Customer with a license key and associated on-premise Software used to harden mobile Customer Applications including run time modules through the injection of application protection technologies, including runtime self-protection, anti-tampering, obfuscation, and Customer-customizable system and application-level protections.

Product	License Metric	Deployment
Mobile Application Hardening: Per APP	Per Application	On-Site

Product or Service Limits

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

Optional Purchases

Product	License Metric	Deployment
AppAware	Customer site or named account (Customer Instance)	On-Demand
Annual Audit Option	1 Per Calendar Year	On-Demand
Key & Data Protection	Per Protected Application	On-Site
Quick Protect AI	Monthly Active User Block(s)	On-Demand
White Box Cryptography Agent	Per Application	On-Site

Requirements: Use of Mobile Application Hardening: Per APP 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:

- Quick Protect Agent
- App Security for Mobile: ARM
- App Security for Apple
- App Security for Android App
- App Protection for Android Native
- App Security for Hybrid JS

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 Mobile Application Hardening.

"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.