



Effective: August 1, 2026

App Hardening for Web (formerly Application Protection for Web)

App Hardening for Web provides Customer with a license key and associated on-premise Software that can be used to harden web-based Customer Applications with runtime self-protection, anti-tampering, and obfuscation code system protections.

Product or Service	License Metric	Deployment
App Hardening for Web	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
Threat Monitoring	Per Customer site or named account	On-Demand

Requirements: Use of App Hardening for Web requires that Customer's Host Platform and Target Platform (e.g. Supported Target Environments and Supported File Types) meet the specifications provided for in the support matrix in the applicable Documentation:

- [App Hardening for Web](#)
- [App Hardening for Mobile: Hybrid JavaScript](#)

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 App Hardening for Web.