digital.ai™

Solution Brief

Digital.ai for Federal and Federal System Integrators

Application protection is critical

Digital.ai Application Protection is a defensive cyber security software solution. The Digital.ai Application Protection software is applied at the binary code level delivering multi-layer protection against static and dynamic attacks. This process hardens applications and is ideal for Software Development Teams (SDTs), Mission Application Teams (MATs), and Mission Defense Teams (MDTs) where protecting specific applications and weapons systems are mission-critical for Defensive Cyberspace Operations (DCO).

Digital.ai is well positioned to work with the U.S. Department of Defense's Enterprise DevSecOps initiative (DSOP), which involves creating 'Security as a Code' culture with ongoing, flexible collaboration between release engineers and security teams. DevSecOps aims to create a cultural shift in engineering to unify software development (Dev), Security (Sec), and operations (Ops). Since Digital.ai software can be deployed with minimal initial configuration and setup, it can be seamlessly integrated into continuous integration and continuous development (CI/CD) processes running in DevSecOps environments.

Digital.ai Application Protection solutions have been built with the understanding the Federal Government and Federal System Integrators are increasingly interacting with their contractors, employees, and soldiers via an app — whether it's mobile, web, or desktop. Securing these new endpoints' applications and data against exploitation is key to preventing intelligence theft, privileged data breaches, and malicious hacking from adversaries.

Traditional app security and network defenses cannot protect apps running in zero-trust environments. Traditional security perimeters no longer exist in today's geographically distributed and technologically diverse — cloud, IoT (Internet of Things), and mobile — workforce. Remote employees need to access applications, systems, and devices which open up vulnerabilities and multiple points of entry for attackers — against which firewalls and other security measures stand no chance. Yesterday's insider threat has evolved into today's threat actor with stolen credentials.

Digital.ai code protection hardens applications with patented guarding and threat detection capabilities. Digital.ai obfuscates code to protect against reverse engineering and delivers the ability to self-repair attacked code, automatically disable app functionality, insert honeypots, and implement other deceptive code patterns to deter and confuse threat actors when attacked. From the moment the app is downloaded, it can also detect and alert on jailbroken or rooted devices as well as active code threats including debugging or other reverse engineering techniques. Additionally, Digital.ai provides white-box cryptography to protect static and dynamic keys and sensitive application data by obscuring critical key and data elements with obfuscation and encryption.

Digital.ai Application Protection solutions include:

Digital.ai Application Protection for Android — application code protection and threat detection against reverse engineering and tampering for Java and Kotlin apps.

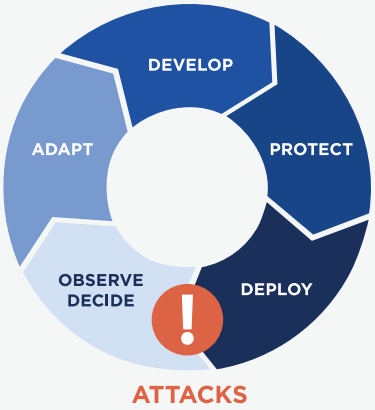
Digital.ai Application Protection for iOS — delivering app protection and threat detection for all major iOS development language apps.

Digital.ai Application Protection for Hybrid — protecting all components of apps designed to run on iOS and Android, alerting on compromised devices, and in-progress code attacks.

Digital.ai Application Protection for Web — protecting browser-based web apps by securing "open text" JavaScript with obfuscation, alerting on reverse engineering or HTML page attacks, and preventing browsers from connecting to hostile websites to prevent data exfiltration.

Digital.ai Application Protection for Desktop or Server — protecting apps running across all major desktop and server operating systems — macOS, Windows, Red Hat, and Ubuntu, utilizing the most common development languages — without requiring changes to source code to prevent reverse engineering attacks. The app can be located on-premises or in the cloud.

Digital.ai App Aware is integrated into Digital.ai protection solutions and provides visibility into the security posture of protected applications the moment they are published. It detects reverse engineering threats as well as cyberattacks in real-time allowing corrective action to be implemented before an attack is completed or becomes widespread. Digital.ai App Aware provides timely and actionable information, confidence through verification, a rapid time-to-protection, and global intelligence. It also enhances the data available to Security Information and Event Management (SIEM) and Business Intelligence (BI) software solutions with API level integrations.



Digital.ai's FIPS 140-2 certified White-Box Cryptography can also be added to protect encryption keys or data stored inside an application. While significant effort has been applied to securing data in transit, from secure transport layers to encrypting data from the source, the weak link is the endpoint: the app. If cipher keys are uncovered, they can be copied, re-distributed, and used maliciously — which is nearly impossible to detect. This could happen if a device falls into an adversary's hands or a weapon system falls behind enemy lines. The unsecured threat vector must be remediated, since existing data protection methods were not designed to defend keys from being discovered via reverse engineering or compromised app code.

Digital.ai White-Box Cryptography compliments existing encryption technologies used to provide strong in-transit protection and is designed to protect encryption/decryption keys stored within an app. Using mathematical techniques and transformations, white-box cryptography blends together app code and the keys to secure cryptographic operations, so keys cannot be found or extracted from the app to be used elsewhere. This adds protection to mobile, desktop, and server apps whether they are located on a device or inside of a weapons system. Digital.ai's White-Box Cryptography supports all major ciphers, modes, and key sizes and can directly interoperate with cryptographic packages (such as OpenSSL) and devices in an agency or command's environment without requiring server-side changes. Digital.ai White-Box Cryptography is available on iOS, Android, Windows, Mac, and Linux platforms.

In addition, **Digital.ai App Management** provides a private app store for commands and agencies where the application deployment and app-level security policies can be set by the agency or command. While custom-built apps improve workforce productivity or military effectiveness, some apps may be utilized on devices owned by contractors and partners. Unsecured apps deployed by an organization creates an ongoing management struggle to find effective ways to securely deploy mobile apps to maximize adoption and maintain privacy — without requiring Mobile Device Management (MDM) or device enrollment. This challenge is addressed by (i) onboarding apps to ensure they are free of malware and privacy risks, (ii) wrapping custom and COTS apps with security, analytic, and management policies allowing governance at the app level, and (iii) making vetted and wrapped apps available via an agency-wide enterprise app store to maximize distribution control and user adoption.

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**