Application Security

Product Brief

Digital.ai Application Security

Prevent threat actors from tampering with the applications you create by adding protections to your AI-powered DevOps Platform.

Application Owners are charged with efficiently developing applications that delight customers. The combination of digital transformation and a global pandemic has accelerated the need to create more applications, faster. One challenge that these apps present is that they contain working examples of how to bypass your security perimeter. In order to prevent theft of customer data, company IP, or even money, the working examples must be obfuscated from threat actors and must offer some means to prevent tampering. Meanwhile, most app owners are under pressure to develop new versions of their applications to meet changing customer/competitive/market demands. Apps in a fully Agile organization might be released twice a month or even daily. Larger apps or apps in orgs that are just beginning their Agile/DevOps journey might be released quarterly or yearly. So while adding security to apps that you create is necessary, depending on the maturity of the organization, an App Owner might 1) not think about security as a part of the DevOps process at all, 2) see security as an impediment to getting to market efficiently, or 3) want to add security but not know where to start.

The primary challenge for the CISO, meanwhile is to protect the organization against breach. Protecting against a breach means preventing reverse engineering and tampering with the "working examples" that live in the apps his/her company creates. The second challenge the CISO faces is hiring and retaining talent. Info Sec professionals were in short supply even before the pandemic, and “the Great Resignation” has exacerbated this problem.

Challenges

- Business pressure to create more apps faster
- Apps required for mobile, desktop, web in variety of OSes and languages
- Apps, by definition, contain working examples of how to bypass traditional security measures
- Threat actors use applications as attack vectors
- Security added to apps as an afterthought

The third challenge the CISO faces is maintaining customer satisfaction. If his/her security controls take too long to implement and thus delay the delivery of software that is in customer demand, he/she will face scrutiny. Further, if the security controls the CISO implements adversely affect the user experience in terms of functionality or speed, he/she will lose credibility. Meanwhile, if the CISO does nothing to protect the apps his/her company creates, the CISO faces risk of a breach that will result in the loss of customer data, company IP, or revenue. Further more, CISOs are often the public face of security for large enterprises and as such their jobs are at risk when a breach is publicly disclosed. The secondary risks the CISO faces are loss of morale among employees, or worse employee resignation – especially in the face of a public breach or an internally embarrassing disclosure regarding a breach.

Digital.ai Application Security Solution

Build Secure Software at the Speed of DevOps

Digital.ai App Security solves the challenges App Owners and CISOs face. The most important benefit we provide is that we protect the working examples of how to bypass the perimeter security that your apps contain. We do this by obfuscating code. How do we obfuscate code? We take unprotected code and feed it, along with the protection blueprint that you create (or we create for you) into an engine that produces the protected code. The protected application contains obfuscated machine code that runs as originally designed but is virtually unreadable by threat actors – even after it has been fed into a disassembler.

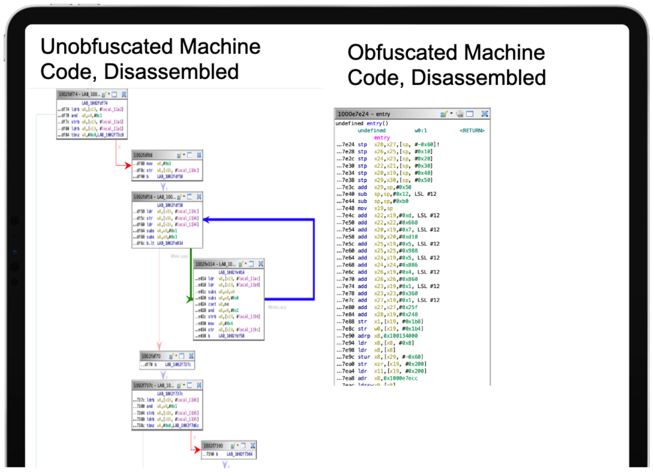
You can build as many customizations and added protections into your Protection Blueprint as you like, or you can use our auto configuration option to use a pre-built Protection Blueprint -- one that requires no customization or configuration -- to obfuscate your apps automatically. Using the auto configuration option allows you to build protected apps faster.

The next most important way we protect our customer's apps is through the addition of anti-tampering techniques. By anti-tamper we are primarily referring to the ability to detect two conditions. First, we detect when your app is run in an unsafe environment that might ALLOW it to be tampered with. Classic examples of these types of environments are debuggers, emulators, or rooted/jailbroken devices. Second, we detect when the code in your app has been modified. Anti-tamper protections can be added on premises at build or by digital.ai in the cloud.

We also provide you with visibility into 1) attacks on your apps and 2) attempts to run your apps in unsafe environments. For example, if a threat actor attempts to modify your code, you'll receive an alert. You'll also see a wealth of detail about where and on what device, OS, and browser the modification took place. You'll also see the IP address of the device and the geographic location of the threat actor. You'll also see the time that the modification occurred and the time it was detected. Finally, you'll see the browser, the User Agent within that browser, the URL where the mod occurred, and the name of the specific script that was modified.

Taken together as part of our AI-powered devops platform, these protections are added to your apps without unduly slowing down either your app dev process or the apps themselves, all while preventing your apps from being used as attack vectors to steal your IP, customer data, or revenue.

App Code Disassembled in Ghidra


Unobfuscated Machine Code, Disassembled
Obfuscated Machine Code, Disassembled

Key Benefits: Protect, Monitor, React

Protect by Embedding Security Into the Application Development Process

Protect code, keys and data within your mobile, web and desktop apps.

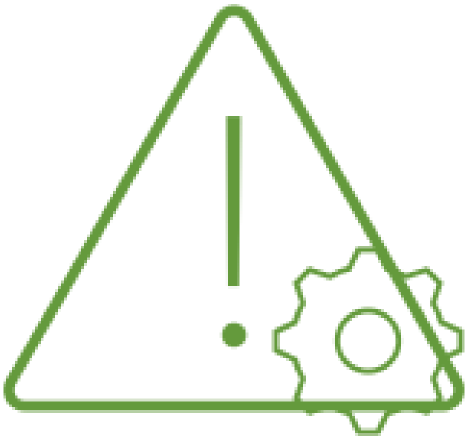
- Obfuscate code to prevent reverse-engineering
- Prevent tampering by detecting unsafe environments and code changes
- Configure customized or automated protections on-premises or in the cloud

Monitor by providing visibility into at-risk apps

Provide visibility into when your apps are at risk.

- Product stand-alone reports or integrate with existing Security Operations Center tools
- Create searchable logs
- See which guards and protections are activated

React By Automatically Responding To Threats



Automatically respond to threats in real-time with Runtime Application Self Protection (RASP)

- Force step-up authentication
- Alter app features
- Shut down applications that are under attack

Key Capabilities

Guard Network	Ensure threat actors have to dismantle each of your protections simultaneously in order to crack your application through the application of the Guard Network.
Application Security support across multiple platforms	Build security into mobile applications, web clients, and desktop applications.
App Security support across multiple OSes	Build security into apps written for the the widest range of operating systems including iOS, WatchOS, tvOS, Android, Mac, Windows, and Linux desktop,
App Security support across multiple development languages	Build security into apps written in C, C++, C#, Java, Javascript, HTML5, and Kotlin
Key and Data Protection	FIPS 140-2 compliant white box cryptography for private keys ensures that your communications are secure even if your applications are hacked.
Add Security as part of AI-driven DevOps	Digital.ai provides functional and performance testing for your secure apps as well as AI-driven insights into attack trends.
Apply protections in the cloud or on-premises	Apply your own customized protections on premises or have protections added for you, automatically, in the cloud.
Malicious Package Detection	Protect yourself from spyware, keyloggers, and the many other types of malware with this dynamic protection

The Digital.ai Difference

UNIFIED DEVOPS PLATFORM

Integrate DevOps & Security capabilities to enable continuous delivery of software

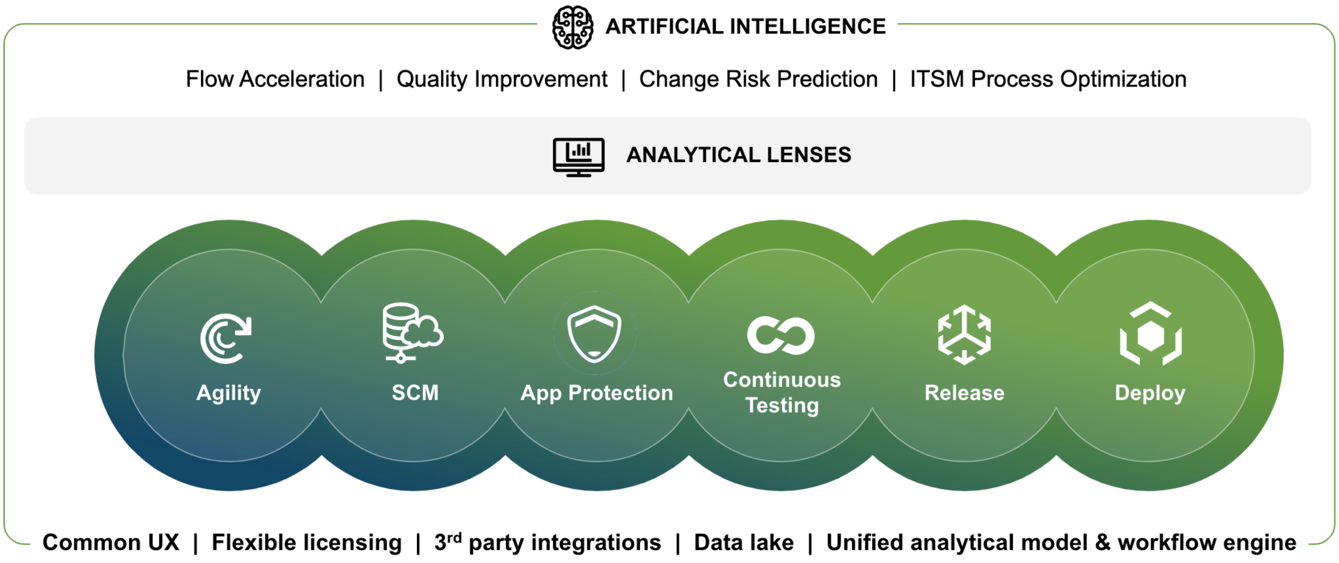
POWERED BY ARTIFICIAL INTELLIGENCE

Generate predictive insights that provide the intelligence to make smarter investments

CONNECTED TO THE ENTERPRISE

Connect to existing processes, applications and infrastructure to propel innovation that find new market opportunities

Digital.ai AI-powered DevOps Platform



ARTIFICIAL INTELLIGENCE

Flow Acceleration | Quality Improvement | Change Risk Prediction | ITSM Process Optimization

ANALYTICAL LENSES

Agility
SCM
App Protection
Continuous Testing
Release
Deploy

Common UX | Flexible licensing | 3rd party integrations | Data lake | Unified analytical model & workflow engine

About Digital.ai

Digital.ai is an industry-leading technology company dedicated to helping Global 5000 enterprises achieve digital transformation goals. The company's AI-powered DevOps platform unifies, secures, and generates predictive insights across the software lifecycle. Digital.ai empowers organizations to scale software development teams, continuously deliver software with greater quality and security while uncovering new market opportunities and enhancing business value through smarter software investments.

Additional information about Digital.ai can be found at digital.ai/ and on Twitter, LinkedIn and Facebook.

Learn more at https://digital.ai/application-security