

Application Security for Web and Hybrid

Product Brief

Digital.ai Application Security for Web

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

Application Owners are charged with efficiently developing web and hybrid applications that delight customers. Digital transformation and customer demand has accelerated the need to create more applications, faster. One challenge that these JavaScript or HTML5 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, and market demands. Web and hybrid apps depend on JavaScript or HTML5 for simplicity of design and for delivering great user experiences. But these are interpreted languages, not compiled ones, which means that unless additional steps are taken to secure them, code can be easily intercepted, viewed and compromised through Formjacking, DOM tampering, session abuse, or overlay attacks. Web and hybrid apps are vulnerable to static app analysis (reading app code that's in the clear) and dynamic app analysis (using a debugger to understand how code operates). Once code designed to interface with APIs is understood, it can be compromised to create attacks that identify vulnerabilities and access back office systems. To secure their entire IT ecosystem, organizations need to prevent client-side web and hybrid apps and APIs from becoming attack vectors.

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 web and hybrid apps their company creates.

Challenges

- Business pressure to create more web and hybrid apps faster
- Web and hybrid apps are written in both HTML5 and JavaScript
- Apps, by definition, contain working examples of how to bypass traditional security measures
- Threat actors use applications as attack vectors
- Security is often added to apps as an afterthought

The second challenge the CISO faces is maintaining customer satisfaction. If their security controls take too long to implement and thus delay the delivery of web and hybrid apps that are in customer demand, they will face scrutiny. Further, if the security controls the CISO implements adversely affect the user experience in terms of functionality or speed, they will lose credibility. Meanwhile, if the CISO does nothing to protect the web and hybrid apps their company creates, the CISO faces risk of a breach. 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 tertiary 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.

Key Benefits: Protect, Monitor, React

Protect by Embedding Security Into the Application Development Process



Protect code within your web and hybrid 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

See when your web and hybrid apps are at risk.

- Produce 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.
	App Security support across multiple development languages	Build security into apps written in Java, Javascript, and HTML5.
	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 web apps as well as AI-driven insights into attack trends.

The Digital.ai Difference

UNIFIED DEVSECOPS PLATFORM

Integrate DevOps & Security capabilities to enable continuous delivery of software

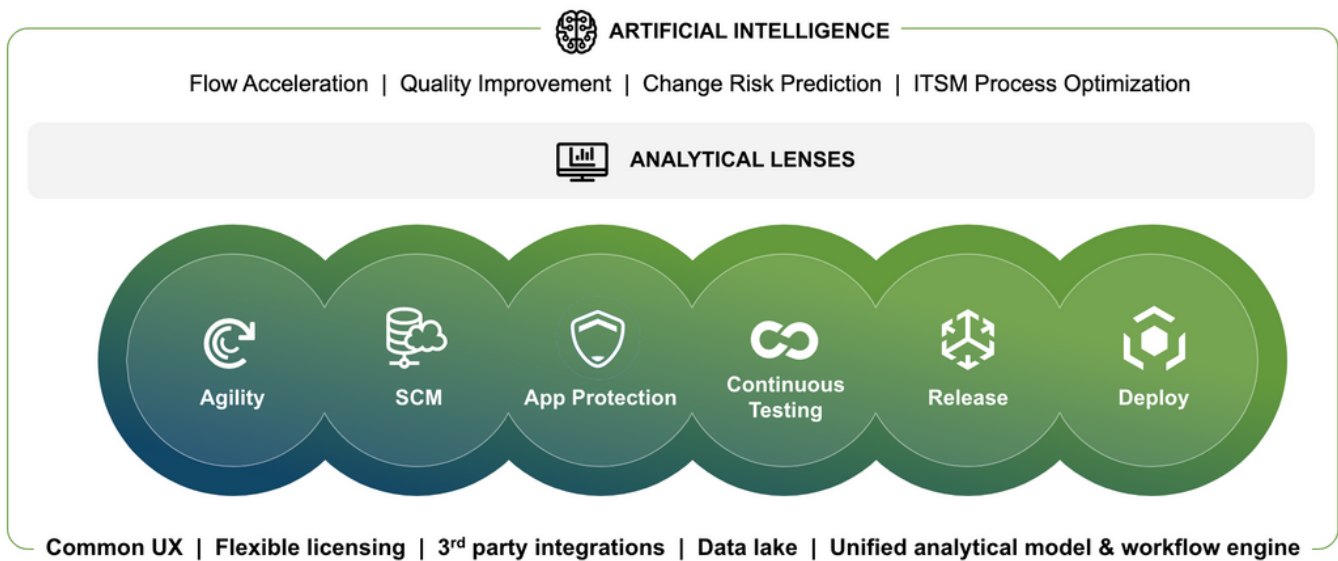
POWERED BY ARTIFICIAL INTELLIGENCE

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



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 DeSecOps 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>

