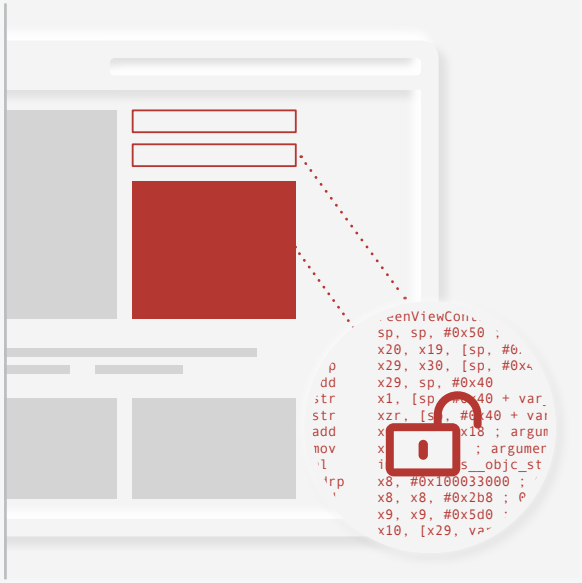
digital.ai™

Solution Brief

Digital.ai Application Protection for Web (formerly Arxan)

Developers want to build web apps that have fast, seamless user experiences and can be easily maintained. One of the most effective ways to achieve that goal is to use JavaScript, HTML5, and APIs. From one-page apps heavily utilizing APIs, progressive web app development projects, or to simply improve performance by pushing validation processes to the client, modern app development is focused on how to efficiently improve performance and user experience. However, with all the benefits these tools bring to web app development, it also opens up a new set of issues with regards to security.



The web security problem

Web 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 by formjacking, DOM tampering, session abuse, overlay attacks, API abuse, and more. Web apps and APIs 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 to identify vulnerabilities and access back office systems. To secure their entire IT ecosystem, organizations also need to protect client-side web apps and APIs to prevent them from becoming an attack vector. From a security standpoint, all code residing in a client browser should be considered running in a zero-trust environment, and security measures should be taken to protect sensitive data or infrastructure access points. For example, data access methods utilizing APIs, such as payment forms or credential verifications, are vulnerable to exposure when applications are reverse engineered. These attacks can expose customer data, intercept and alter communications, and ultimately lead to the exfiltration of sensitive data.

Other forms of attacks can also be created using the knowledge of how web apps interact with back office systems. Most notable are targeted malicious code attacks, like Man-in-the-Browser (MitB) malware designed to steal credentials. Understanding where the inputs occur and are verified can provide attackers all they need to know to design malware to steal a user's credentials and access their accounts.

In today's zero-trust world, the need to protect customer, business, and IP data is greater than ever. Securing applications and APIs against data exfiltration is key to preventing brand damage, financial loss, intellectual property theft, game cheating, replay-attacks, government penalties, and more.

Protecting web apps

To counter the threats against web apps and APIs, organizations need to secure their application code, integrate threat detection capabilities, stop browsers from connecting to unauthorized websites, and enable built in defenses to disable app functionality. Digital.ai Application Protection for Web can quickly protect JavaScript code to help stop client-side threats before they can be used to compromise critical back office assets — all while not impacting continuous integration and continuous development environments.

Protection capabilities

- **Passive protection** to prevent 'in-the-clear' JavaScript code from being easily understood by attackers through a range of obfuscation techniques
- **Active protection** to protect against browser data exfiltration with an in-app firewall by only allowing the app or API to connect with legitimate servers, and automatically respond with countermeasures when code analysis or tampering is detected by shutting down web app functionality or the entire browser
- **Real-time threat** notification to alert the business if code tampering or analysis is attempted to enable an immediate operational response — such as shutting down attacker accounts or updating web code protection to counter an attack

Digital.ai for Application Protection for Web is available on-premises or via the cloud and is compatible with all leading development frameworks. Either option allows post-coding JavaScript to be protected without getting in the way of development processesor timelines.

Benefits

- Defend against web app code attacks to deter app analysis, malware insertion, and API attacks
- Detect attacks in real time to allow an organization to get in front of attacks by:
  - Disabling account access
  - Developing and re-deploying code with updated obfuscation
- New in-app firewall prevents web applications from connecting to unauthorized servers and stops sensitive customer data or financial information from being exfiltrated from an API or web app via the browser

Inside out app protection

Digital.ai Application Protection for Web provides comprehensive, app-level security to protect against a range of threats or to enforce enterprise app governance — expanding the corporate perimeter of trust. Digital.ai provides a broad range of patented security capabilities to protect applications in the wild, such as a dynamic app policy engine, code hardening, obfuscation, in-app firewall, white-box cryptography and encryption, and threat analytics.

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**