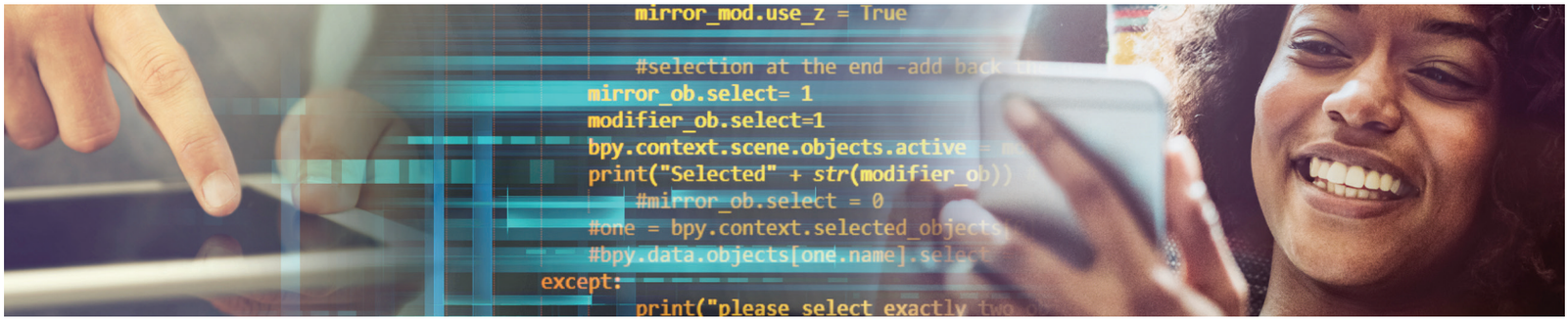
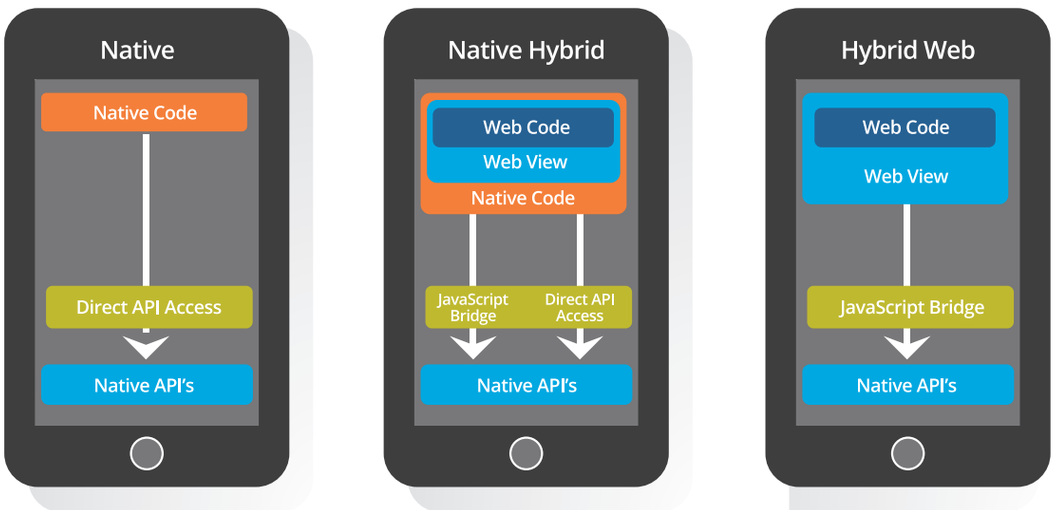


A Comprehensive and Differentiated Solution To Prevent Brand Damage, Financial Loss, IP Theft, & Compliance Risks

Ability to write code once that can run anywhere makes JavaScript widely popular. JavaScript powers a multitude of app, open source UI, and game frameworks, servers, terminal-based workflow tools, animation libraries, and many other applications. JavaScript is supported by every major browser and is the only web programming language built for both client-side and server-side. With the advent of Node.js and other similar platforms, JavaScript has become not just a viable back-end option, but also a formidable one.

Some of the primary mobile app architecture alternatives, or profiles, are shown in the following exhibit:



Why Do You Need to Secure Your JavaScript Application?

Hybrid apps offer lucrative business model and faster time-to-market, from financial services to gaming to digital media. However code running in the WebView is more difficult to secure due to lack of security features in the Web control. JavaScript is a very dynamic language that allows one to easily add/inject code to intercept the execution of genuine application at runtime and modify it for nefarious activities. Payment forms used on both web and mobile, in the form of e-commerce APIs, are vulnerable to reverse engineering & tampering attacks and may be used as attack gateway to expose applications and data on back-end. In addition to hybrid apps, JavaScript running in various other environments including IoT applications, and servers, is extremely vulnerable and low hanging fruit for hackers.

Arxan Secures JavaScript Apps for Mobile, Web, and IoT

Arxan Application Protection for JavaScript provides protection for JavaScript-based applications including Hybrid iOS and Android apps, and browser-based web applications. Arxan's proprietary technology protects businesses against numerous attacks including intellectual property theft of business logic and encryption material, and tampering including cheating & replay-attacks. Businesses developing JavaScript applications need to secure their application code, and Arxan provides the protection needed for JavaScript across Web, and IoT, in addition to holistic Mobile protection that leverages Arxan's suite of protection in Hybrid applications.

- **Prevents IP Theft**
- **Prevents Code Tampering**

Arxan Application Protection For Javascript Offers A Comprehensive Solution To Mitigate The Risks

- **Code protection to make it extremely difficult for hackers to reverse-engineer, analyze and exploit the JavaScript application**
- **Runtime protection to prevent malicious code modifications, bypassing of controls, tampering with the data integrity in JavaScript application**

Key Features And Benefits

- **Powerful: Market leading JavaScript Protection**
- **Differentiated: Proprietary Anti-Tampering and Debugger Detection**
- **Configurable: Highly-tunable protection to create the protection optimized to the customer's business needs**
- **Easy to Integrate: Integrates seamlessly into tool-chains**
- **Flexible: Cloud "as a Service" deployment options**
- **Compatible: Supports ES6**