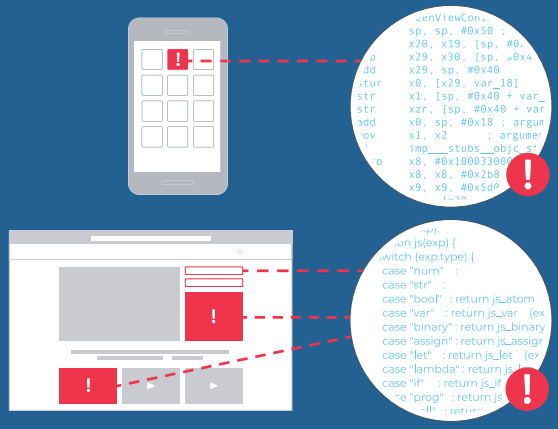
ARXAN

Arxan Application Protection

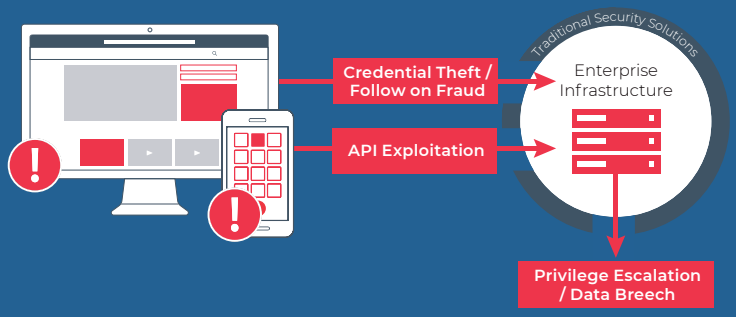
Protecting Apps in a Zero-Trust World

Customers and employees are increasingly interacting with organizations via an app—whether it's mobile, web or desktop. As apps become more sophisticated and integrated with corporate infrastructure, the need to protect customer information and business data is greater than ever. Securing this new endpoint is key to preventing breaches, brand damage, financial loss, intellectual property theft and government penalties.

Traditional app security and network defenses cannot protect apps from reverse engineering nor attacks that originate from within the apps.



These attacks can lead to direct data breaches, compromised IDs from skimming attacks & stolen IP.



Apps for Anyone

Millions of apps have been created for customers, employees and partners that are critical to industries such as mobile banking, payments, eCommerce, connected medical and automotive, entertainment and gaming. These apps are valuable targets because they are access points to corporate infrastructure that can expose customer credentials and business information.

Applications are vulnerable to attack whenever operating in zero trust environments — directly downloaded, made available via public app stores or when web applications are run in a browser. Bad actors can exploit unprotected apps through reverse engineering to gain an understanding of an app's code and how it communicates with back office systems. Once understood bad actors can insert malicious code to steal personally identifiable information (PII), intellectual property (IP) — or via follow-on attacks utilizing exposed keys and API locations.

PROTECT

Comprehensive Code-Level Security

- Obfuscates source code, inserts honeypots and implements other deceptive code patterns to deter and confuse threat actors
- Triggers defensive measures automatically if suspicious activity is detected, including app shut down, user sandbox, or code self-repair
- Injects essential app code protections and threat detection sensors into CI/CD cycle after code development, without disrupting DevOps process

ENCRYPT

Key and Data Protection

- Encrypts static or dynamic keys and data embedded or contained within app code
- Protects sensitive data at rest within an app or in transit between the app and server
- Supports all major cryptographic algorithms and modes with FIPS 140-2 certification

ALERT

Real Time Threat Data

- Notifies organizations of app reputation, real-time attacks, and provides the ability to suspend accounts or step up transaction or access authentication
- Insights help optimize and adapt protection based on attack insights and trends including how, when, where and by whom the app is targeted
- Delivers threat data feeds end-to-end, making threat data accessible via a browser or easy integration with existing SIEM, BI and fraud prevention platforms

Apps are today's endpoint—
and your most vulnerable attack vector.

Arxan Application Protection Solutions include:

Arxan for Android — providing application code protection, key and data encryption and threat detection against reverse engineering and tampering for Java and Kotlin based apps.

Arxan for iOS — delivering app protection, key and data encryption and threat detection for apps developed with all major iOS development language.

Arxan for Hybrid — protecting JavaScript and native code for apps designed to run on iOS and Android, with key and data encryption for native code and threat detection for all protected apps.

Arxan for Web — protecting browser-based web apps by securing "open text" JavaScript with obfuscation, alerting on reverse engineering or HTML page attacks along with an in-app firewall to prevent data exfiltration by blocking browsers from connecting to hostile websites.

Arxan for Desktop & Server — protecting apps running across all major desktop and server operating systems without requiring changes to source code to prevent reverse engineering attacks. The app can be located 'on prem' or in the cloud.

Apps for the Workforce

Custom-built and commercial productivity apps to improve workforce productivity typically run on unmanaged devices owned by employees, contractors and partners. These unsecured apps deployed by an organization pose a significant business risk. This threat creates an ongoing management struggle to find effective ways to securely deploy mobile apps to maximize adoption and maintain privacy without requiring device management or enrollment. To address this problem, businesses need to adopt a three-phase app management approach.

Arxan App Management

First, apps need to be properly onboarded to ensure they are free of malware and privacy risks. Secondly, custom and off-the-shelf apps need to be wrapped with security, analytic and management policies. These app wrapper enhancements allow IT teams to manage governance at the app level to enforce enterprise single sign-on, app usage and analytics, app-level VPN, app-expiration, copy/paste disable, jailbreak detection, and more. Lastly, vetted and wrapped apps need to be made available to users via corporate-branded enterprise app stores to maximize distribution control and user adoption.

About Arxan Technologies

Arxan, the global trusted leader providing the industry's most comprehensive application protection solutions, works with organizations looking to protect applications and to securely deploy and manage business-critical apps to the extended enterprise. Arxan currently protects more than five billion application instances across many industries including financial services, mobile payments, healthcare, automotive, gaming and entertainment. Founded in 2001, the company is headquartered in North America with global offices in EMEA and APAC.

For more information, please visit **www.arxan.com** or follow **@Arxan** on Twitter.