



Security Overview

Enterprise Mobility Platform with
Enterprise-Grade Security

PowWow Mobile SmartUX™ Platform Architecture Overview

PowWow Mobile delivers enterprise mobility faster, simpler and at a lower cost than any other approach. Our SmartUX™ Platform accelerates mobile app development by transforming any enterprise application or workflow into a modern, app experience or; by creating net-new apps that connect to any third-party data source, API or SQL. With PowWow Mobile, companies can easily design, build and deploy personalized, intelligent and secure native apps that run anywhere, on any device (smartphone, tablet, PC, watch) and any OS (iOS, Android, Windows 10 or HTML5). No changes to existing applications, or the creation of any new APIs, are required.

The end-to-end architecture of the deployed solution consists of three components:

1. The Mobile App
2. The SmartUX Platform: SmartUX Studio, Smart Proxy, Smart Controller, Smart Connect / Container Layer
3. The Customer's Existing Application Delivery Infrastructure: Web or Application Servers, App or Desktop Virtualization Servers

Briefly the solution works as follows: the PowWow Container Layer virtualizes the existing application client (Web, Windows or Java), extracts the underlying UI and data elements through the client's front-end via the unified API layer (SmartConnect), applies a series of sophisticated transformations to construct a mobile representation of the data, and then ships the transformed data to the mobile app via the Smart Controller and optional Smart Proxy. The native mobile app renders the mobile web view with native UI/UX based on the user device's capabilities and status.

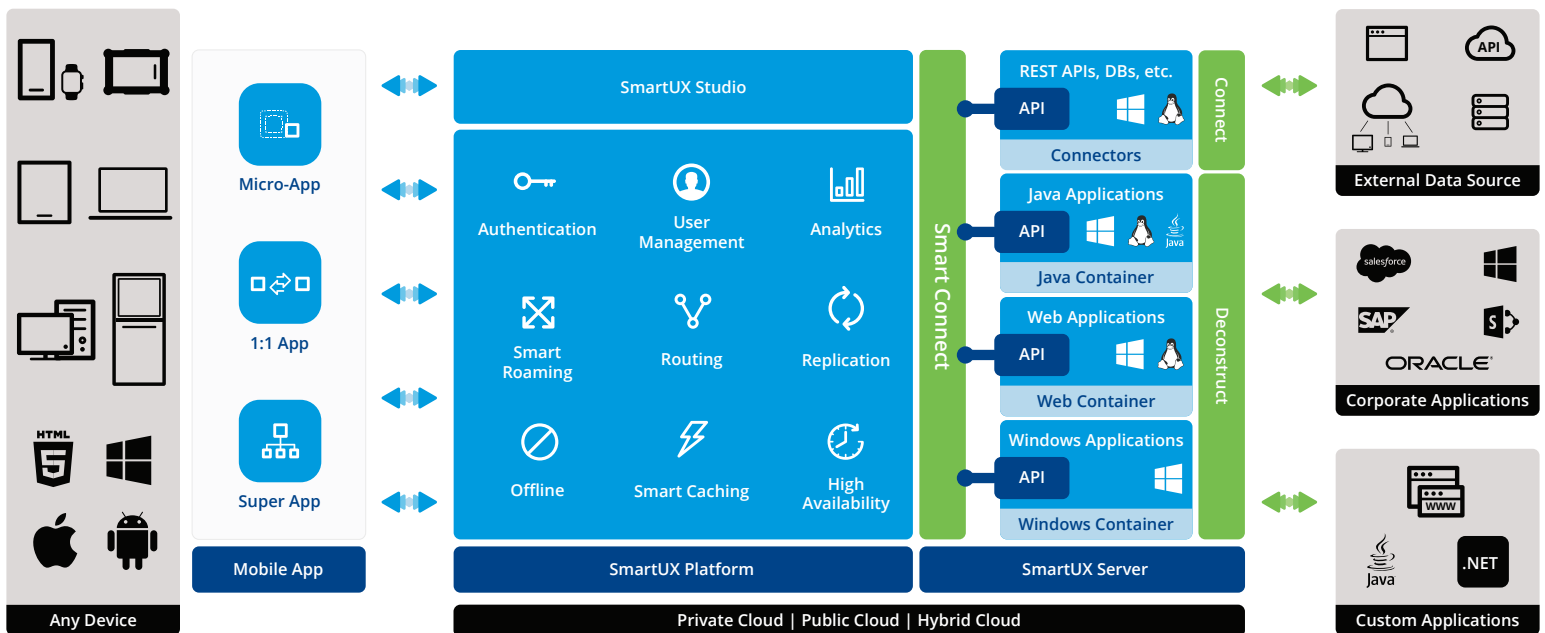


Figure 1: PowWow Mobile SmartUX Platform Architecture Overview

Bearing in mind that the overall security of any solution is a function of the security strength of each of the individual components, considerable care has been given to secure each of the individual components of the SmartUX Platform to the highest levels. In tandem, the security mechanisms deliver true enterprise-grade, end-to-end security. The rest of this security brief outlines the security mechanisms that protect each of the constituent components.

1. The Mobile App

The PowWow mobile app is a native app in the form of an IPA, APK or Windows10 package, that is custom branded with the enterprise customer's UI standard. There are several security mechanisms in place to protect the mobile app.

No persistence of data or logic: The PowWow generated mobile app does not persist any data or logic on the user device. The app simply renders views that are created with the SmartUX Studio, using data delivered by the SmartUX Platform. Thus, having access to the user device and the app does not allow for any information disclosure.

Existing Enterprise Authentication: The SmartUX Platform proxies existing app authentication mechanisms to the mobile app. Using MDM integration (described below), SSO capabilities can be leveraged to provide both authentication to a customer's private cloud infrastructure (VPN), and any app specific authentication.

Integration with enterprise MDMs: The PowWow generated mobile app is fully compatible with all major MDM platforms available in the market such as VMware AirWatch, MobileIron, Good, Citrix XenMobile, etc. MDMs offer a suite of security mechanisms such as profile based app distribution, identity management, per-app VPNs, geo-fencing, content lockers, etc. Integrations with MDM providers allow mobile apps constructed using the SmartUX Platform to leverage all such security capabilities.

Additional authenticated access: Enterprise customers can choose to add to their existing security mechanisms such as multi-factor authentication and encryption by requiring users to authenticate themselves when using any PowWow generated mobile app for the first time. This authentication stage would be in addition to any authentication that would be required by any existing application server.

2. The SmartUX Platform: SmartUX Studio, Smart Proxy, Smart Controller, Smart Connect/Container Layer

The SmartUX Platform is an enterprise-grade, scalable, highly available, and secure platform. Several mechanisms combined deliver the best in class security.

Dedicated container per session: For each mobile user, a session is served by its own dedicated container on a PowWow server. For existing web applications the sessions are served from Phantom JS, for Windows they are served on Citrix XenApp or Microsoft RDS. Each container has complete isolation of the data and state from other containers on the platform. Moreover, dynamic just-in-time container assignment adds another layer of security since the mobile session to instance mapping is not discoverable. This provides unparalleled protection for every mobile user session.

No data and logic persistence: Just as with the mobile app, there is no data, logic, or other state persistence in the SmartUX Platform. Only application client views are processed and transformed, eliminating any exposure of data or logic. When a user's session is closed or terminated, the container provisioned for that session is not reused.

Secure logging: The SmartUX Platform stores no Personally Identifiable Information (PII) data in the system and event logs. Only data that is authorized by an individual customer is written to the log file.

Network path to the mobile app: The SmartUX Platform relies on enterprise-grade RSA-2048 certificates, advanced encryption standard (AES) session-based encryption, and secure hash algorithms (SHA). The certificates enable secure authentication, while encryption preserves the confidentiality of information sent over the network, and hash algorithms enable both secure integrity checks and verification. Furthermore, server authentication, symmetric key exchange, encryption, and verification are all respectively performed on a per-session basis. Thus, keys are generated on a per-session basis ensuring that they cannot be compromised and reused across sessions.

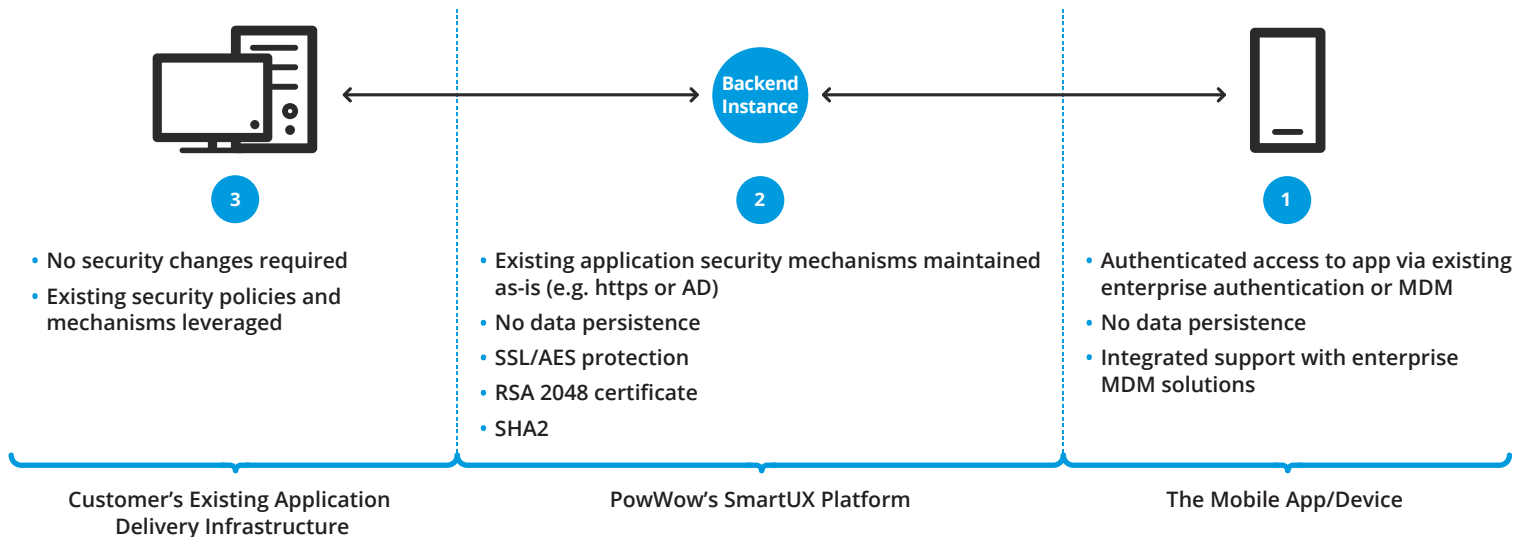


Figure 2: Security Architecture for Web Facing Applications

3. The Customer's Existing Application Delivery Infrastructure: Web or Application Servers, App or Desktop Virtualization Servers

The SmartUX Platform does not require any changes whatsoever to the customer's existing enterprise Application Delivery Infrastructure. The Application Delivery Infrastructure itself is entirely protected by the enterprise customer's existing security policies and mechanisms. All authentication mechanisms are adhered to entirely, and challenges are simply passed on to the user for responses. Hence, the customer can trust that their existing security policies are fully enforced when using the SmartUX Platform.

The SmartUX Platform fully inherits, leverages, and re-uses all existing security policies and mechanisms instituted by the enterprise customer. This includes application level and transport layer security mechanisms such as TLS/SSL, and network level security mechanisms such as IPSec. If an application server is accessible only through a VPN, the SmartUX Platform can be deployed behind the VPN boundary. Thus, the server to PowWow pathway stays fully inside the VPN, requiring the user device to successfully join the VPN before being able to use the PowWow app.

Summary

The SmartUX Platform delivers enterprise-grade security with complete end-to-end protection from the Application Server to the user device. With zero persistence of data (in cloud and the user device), best-in-class encryption and authentication, and full inheritance of the enterprise's existing security policies and mechanisms, the SmartUX Platform offers unparalleled security to the enterprise while mobilizing its applications.

About PowWow Mobile

PowWow Mobile allows enterprises to transform business applications into modern, mobile app experiences. PowWow Mobile eliminates business-IT friction as enterprises seek competitive advantage and increased productivity through mobile for today's digital workplace. SmartUX Platform accelerates enterprise application transformation by creating new, native mobile apps from any web or Windows app, quickly without sacrificing quality, and at a lower cost than custom solutions or other tools. PowWow Mobile works with customers across industries, including financial services, healthcare, telecom, software, consulting and public sector.

594 Howard Street, Suite 301
San Francisco, CA 94105

+1 877 800 4381

www.powwowmobile.com

info@powwowmobile.com

[@powwowmobile](https://twitter.com/powwowmobile)