

eGuide

2019 Ultimate Guide to Mobile Apps in the Digital Workplace

appdome



Industry Backdrop

Mobile Apps in the Digital Workplace.

Today's workforce has used consumer mobile devices and mobile apps for 20+ years. Millennials, Gen Z and other mobile natives expect to use mobile apps to perform and participate at work. At the same time, Shadow IT as well as new and more diverse mobile apps are emerging to improve all facets of work and streamline engagement. As a result, a new wave of critical corporate data is now cascading into mobile apps, elevating mobile apps to the core of the enterprise landscape.

Securing mobile app data and use is now a top priority. Enterprise IT, security and mobility professionals face consumer-like challenges and must consistently deliver secure and sanctioned mobile apps across the entire organization fast. The immediate demands of a mobile-native workplace are forcing new security, management and authentication models to emerge quickly.

Single vendor and single implementation modalities are becoming outdated. Organizations must now deliver "any vendor" and "any solution" into mobile apps on demand. The ability to create user-specific, security, mobility and identity solutions in mobile apps is on the rise.



Trend #1

New Mobility Models Emerging Fast



The new mobile workforce is placing a real strain on the traditional model of managing devices. Organizations now need to deliver a common set of mobile apps to all employees, including those that use managed- and non-managed BYOD. Mobile Application Management (MAM) is gaining ground. Zero Management Mobility™ models have also emerged to overcome end user privacy, mobile app adoption and compatibility issues. Zero Management Mobility adds security, authentication and VPN capabilities directly inside mobile apps, to secure and control mobile apps without a management console.

Appdome allows users both options: (1) adding and enhancing any EMM-MAM, or (2) using Appdome's industry-first Zero Management Mobility solution to protect the data, connection and the codebase of all apps.



IBM **MaaS360**



vmware® airwatch®



MobileIron

Trend #2

Critical Frontier - Mobile SSO

Organizations recognize the need to deliver easy and familiar authentication workflows inside mobile apps. However, mobile apps are not built to authenticate to the same corporate environments used by desktops, or by the same methods used by other apps.


Lack of authentication compatibility often stops mobile deployments. On top of that, fragmented sign-on experiences require employees to pass several, often different and unfamiliar, steps to authenticate and use mobile apps. This degrades the usability and usefulness of that app as well as it unnecessarily complicates the mobile app infrastructure.

Using appdome SSO⁺, organizations can quickly achieve true, unified mobile single sign-on (SSO) easily, using any of the following inside mobile apps: Microsoft Azure AD, ADAL, Active Directory, NTLM, and ADFS, as well as SAML, OpenID Connect, and OAuth, including proprietary implementations from leading vendors like Okta, Ping, OneLogin and others.



Trend #3

Redefining Mobile App Access

Organizations already have networking devices, firewalls, gateways, proxies, and other advanced systems to gate and grant access to the corporate network. Up until recently, this infrastructure was dedicated to desktops and laptops, as well as the wireless infrastructures needed to run the business. Organizations are now exploring ways to use this infrastructure for mobile apps. The need for  **MicroVPN™** inside Android and iOS apps has emerged to allow mobile apps to natively use the existing corporate gateways and infrastructure.

Appdome supports a full range of conditional access and in-app MicroVPNs, including specific implementations for select vendors like Microsoft's Mobile App Proxy and F5 AccessPolicy Manager. Appdome also supports adding conditional access, proxy-based routing (PAC files), and remote route configuration via an EMM, all directly inside mobile apps. Without deploying any extra servers, proxy-based routing, custom configuration, remote configuration, and PAC files can all be added easily during the build process via the Access tab on the Appdome platform.



Trend #4

Claiming the App Lifecycle

Enterprises have now embraced the need to control and manage the mobile app lifecycle themselves. No longer willing to wait for vendor supplied solutions, organizations are adopting Appdome to consistently deliver mobile apps with the needed security, management, authentication and other features across users and environments.

Two distinct use cases have emerged - appdome  for managing continuous improvements to 3rd party apps, and appdome  for deep integration with existing CI/CD systems to repeatably build apps with security, authentication, management and other implementations inside apps. Build-to-publish APIs enhance each use case, allowing continuous improvements to all mobile apps.

Organizations are also placing a premium on the Appdome platform's full mobile app lifecycle feature set, including digital workflows, teams, templates, approval, and audit trails. These features empower functional groups - from development, to line-of-business, including IT, Security, Mobility, SecOps and DevOps - to collaborate and work together to create, improve and release mobile apps to the workforce.

Trend #5

Achieving The Versionless Outcome

Acquiring, building and delivering mobile apps that increase productivity, reduce operating costs and help organizations compete, all now sit at the center of every mobility strategy.

A proper mobility strategy must be future proof. Mobile apps and services emerge, evolve and change quickly. Organizations must support mixed environments and multiple vendors for management, security, authentication and access out-of-the-box, with zero risk to usability and compliance.

Only Appdome allows organizations to deliver “every app”, “any vendor” and “any version” on demand. Beyond security compliance and compatibility with any mobility and corporate infrastructure, only Appdome allows mobile apps to work together as a system of secure productivity for the user. As if they were coded to do so, even basic enterprise productivity apps such as secure browsers, secure email, secure document apps can now meld together with external apps for sign-on and use - every time any user launches any app.



Why appdome?

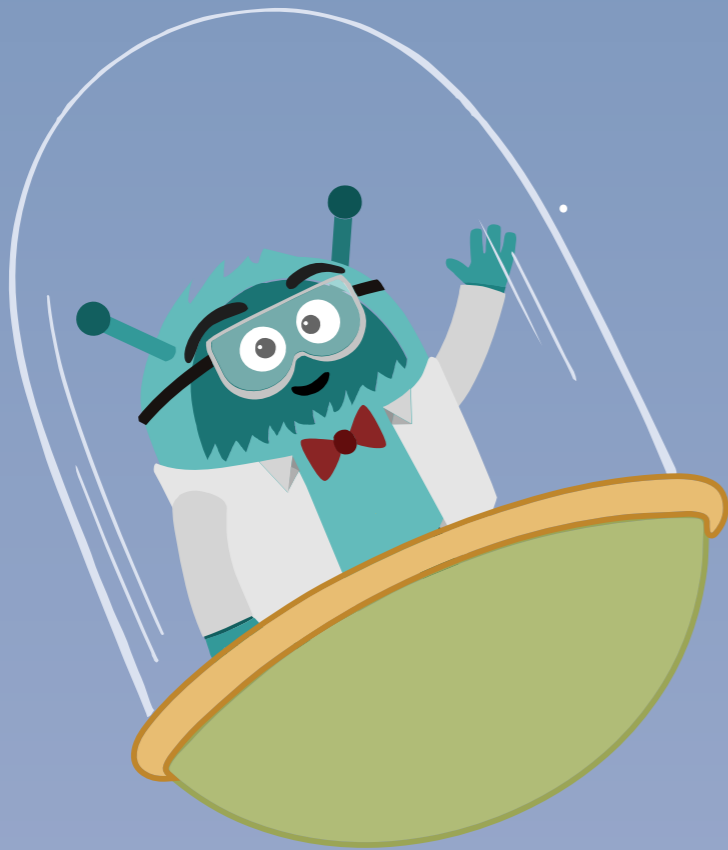
To deploy mobile apps in the digital workplace, agile mobility strategies that enable organizations to choose their mobility, management, authentication and infrastructure vendor, and employees to choose their devices and applications are now center stage.

Organizations are finding that legacy device- and vendor- based solutions are not enough to meet the demands of the mobile-first organization. Appdome's Mobile Integration Platform allows organizations to meet the immediate and diverse demands of the mobile workforce. With Appdome, organizations take control of the mobile app lifecycle and use AI to create, secure, enhance and deliver mobile applications themselves - on-demand quickly and easily.

Get started at **fusion.appdome.com**

“ Appdome's cloud-based fusion process enables the integration of compliance, security, mobility, Single Sign-On (SSO), mobile identity, VPN and analytic solutions, without coding...any purpose the customer chooses. ”

Gartner | Mobile Application Management Market Guide



Request A Demo
info@appdome.com

appdome

3 Twin Dolphin Drive
Suite 375
Redwood City, CA 94065

+1.650.567.6100
+1.844.360.FUSE (3873)
info@appdome.com

www.appdome.com

Appdome © 2019