appdome

Agile Enterprise Mobility With Appdome

FEATURING RESEARCH FROM FORRESTER

Bridge Your Enterprise Mobile Strategy To Partners And Contractors

New Forrester Research highlights the enterprise trend toward an App-Centric mobile application management (MAM) and app augmentation strategies to get more mobile apps into the hands of a broader and more diverse user population – faster.

GETTING AGILE WITH MOBILITY

The number of mobile apps in the modern enterprise is growing rapidly. Infrastructures, systems, vendors and standards for access, authentication, management, security and more are changing constantly. Delivering a consistent, high quality mobile experience for all users is a challenge for any mobile app owner, Mobile IT and mobility professional.

Agile Enterprise Mobility brings mobile application management (MAM) and app augmentation technologies together, combining them to offer organizations greater flexibility and speed in meeting mobility objectives. The goal of MAM is to allow App-Centric security and management controls, without the need for device level profiles or enrollment. The goal of app augmentation is to deliver vendor choice, feature richness, and implementation control inside Android and iOS apps, regardless who built the app and tailor made to the way apps are built.

With MAM and app augmentation combined, Agile Enterprise Mobility allows organizations to deliver any authentication, management and security implementation inside Android and iOS apps without regard to the nature or security of the device (managed, not managed, BYOD or employer provided). This means that organizations can create a consistent mobile app experience for all users, implementing the security, authentication and management features needed most by each organization.

In the report, "**Bridge Your Enterprise Mobile Strategy To Partners And Contractors:** *Grant Broader Access To Applications Without Mobile Device Management,"* Forrester states in its research that App Augmentation is a critical factor to achieving agile enterprise mobility.

App augmentation technology operates in tandem with containerization and standalone MAM products but offer additional integration and security functionality. "For example, Appdome fuses applications with additional security policies, such as anti-tampering and code obfuscation. I&O pros can also quickly add one or multiple EMM-specific SDKs to mobile apps, which speeds delivery and drives down costs," Forrester stated in the report.

IN THIS DOCUMENT

Spotlight: app security specialists

What it offers:

- ☑ Third-party SDK and app wrapping augmentation
- ☑ Mobile app fusion without changing the source code
- ☑ Bridge the gap between EMM services and apps (for example, VOIP might not work through EMM)

Use for:

- ☑ Layering additional security capabilities to an EMM or MAM suite
- ☑ Reducing burden on SDK testing and configuration, both short- and long-term
- ☑ Identifying and remediating attacks in real time, DLP
- ☑ Ensuring parity of application security functionality across operating systems

Don't use for:

- ☑ Providing a mobile application catalog
- ☑ Application management capabilities, such as app distribution, app updates, and license revocation
- ☑ Device-specific capabilities, such as geofencing

Sample vendors:

- ☑ Appdome
- ☑ Better Mobile
- ☑ Blue Cedar Networks

NO CODE APP AUGMENTATION BY APPDOME

Appdome puts mobile app owners, Mobile IT and Mobility professionals in control of their mobility strategies. Using Appdome, organizations control implementation, choose vendors, and select features and services as needed to support use cases and deliver the best mobile experience to users. No code or coding required.

Appdome provides a multi-service, multi-vendor, patented technology that has several advantages over outdated wrapping technologies. Appdome does not utilize swizzling or private APIs or any methods that prohibit apps from being submitted to public App Stores. A Fused Appdome app is an app, and features implemented via Appdome are added as if a developer natively coded the features to the app. Appdome Fused Apps can be submitted to all Public App Stores.

KEY BENEFITS - APPDOME FOR ENTERPRISE MOBILITY	
Vendor Choice	Appdome provides no-code implementation options for all leading vendors in enterprise mobility, including Airwatch WorkSpaceONE, Blackberry UEM, IBM MaaS360, Microsoft Intune and MobileIron. This allows any Android and iOS app to work seamlessly with the organization's vendor(s) of choice, easily supporting a consistent mobile experience inside a single vendor, multi-vendor or vendor-to-vendor migration.
Implementation Control	Appdome allows organizations to build custom versions of Android and iOS apps to suit the internal and specific use cases demanded by their users. Organizations have full control over the relevant EMM or MAM SDK implementation and choose what and what not to add to apps. In addition, organizations configure apps, adding critical elements like support for remote configuration, private certificates, private urls, Proxy-PAC support, branding (e.g., custom logos, favicons, etc.) and more. The Appdome platform also allows organizations to sign and deploy apps, enabling a complete end-to-end platform for delivering customized apps to internal users.
Guaranteed Outcomes	Appdome Mobility Suite is a proprietary service that guarantees that every Android and iOS app will work inside the EMM or MAM system of choice. Appdome extends EMM vendor support to all mobile apps created in any development environment. Appdome Mobility Suite allows latency sensitve features such as VoIP, instant messaging, legacy frameworks, push notifications and more to work inside the EMM. Customers can then bridge the gap between EMM services and mobile apps needed by corporate users.
Ecosystem services	Using Appdome's Boost-EMM™ service, organizations have the option to add secure browsing, email, document sharing and other EMM or MAM ecosystem services to Android and iOS apps. This is extremely powerful for organizations that leverage productivity apps from their chosen EMM vendor, or for organizations that want to promote collaboration or sharing among apps. Several EMM and MAM vendors also maintain other services such as analytics, which can be added on top of traditional management-class services, all in one workflow.

SERVICES TO MEET TODAY'S MOBILITY NEEDS

Appdome has a growing list of no-code service implementation choices for developers and mobile organizations.

Management: Appdome for EMM automates the implementation of leading EMM SDKs such as BlackBerry Dynamics, Microsoft Intune, IBM MaaS360, AirWatch and MobileIron into any Android and iOS mobile app. This allows internally built and 3rd party apps to be deployed and managed by EMMs in minutes. On top of implementing EMM SDKs, Appdome offers it's Appdome Mobility Suite to bridge the gaps between EMMs and apps, and Boost-EMMTM to connect EMM vendor ecosystem services such as secure browser and secure email to apps. This allows apps to function as if fully designed to support the EMM from the ground up – all without writing a single line of code.

Security: Appdome's Mobile Security Suite is a comprehensive mobile security offering that delivers best practice mobile security functionality to any Android and iOS mobile app. Appdome's Mobile Security Suite includes multiple categories of mobile app protections including: data loss prevention, data-at-rest encryption (FIPS 140), OS integrity, secure communication (MiTM and Certificate Validation), mobile privacy (application blurring, pin-code, and Touch ID). These features can be applied in an always-on or managed implementation and include developer options to design in app experiences for users.

Identity: Appdome's Identity service enables customers to securely integrate mobile identity, modern authentication, 2FA, MFA and biometrics functionality to new and existing mobile apps. A core component of this offering is Appdome for SSO+, which includes the ability to instantly add cloud identity services (e.g., Okta or Microsoft Azure AD) and portal-based authentication (e.g., Kerberos and KCD) to apps without code or coding.

Threat Defense: Appdome for Mobile Threat Defense automates the process of adding anti-malware, bot protection and fraud prevention SDKs and APIs to iOS and Android apps. Enterprises and ISVs can select from a list of best-of-breed Mobile Threat Management providers like F5, Check Point and Symantec and add their service to any mobile app in seconds – with a single click. It gives end-users a truly native in-app protection against malware that is secure by design.

Bridge Your Enterprise Mobile Strategy To Partners And Contractors

Grant Broader Access To Applications Without Mobile Device Management

by Andrew Hewitt

May 15, 2018

Why Read This Report

Employees aren't the only group that needs enterprise mobile support. Your business' growth depends on constituencies outside your workforce, such as contractors and other B2B partners — and you need a way to safely expand the scope of your enterprise mobile efforts to reach them. Traditional tools that infrastructure and operations (I&O) uses to secure access to mobile apps, such as mobile device management (MDM), can't effectively help here. This report helps I&O leaders expand the scope of their mobile transformation using an app-centric approach.

Key Takeaways

MDM Can Take Your Mobility Strategy Only So Far

While MDM is a key technology for brokering access to mobile applications, there are some groups for which MDM enrollment isn't possible or desirable, such as contractors and privacy-minded employees.

Employ An App-Centric Strategy To Open Up Mobile Access

Containerization, standalone mobile application management (MAM), and app augmentation technologies help I&O pros enable workers with access to mobile apps without MDM enrollment.

Bridge Your Enterprise Mobile Strategy To Partners And Contractors

Grant Broader Access To Applications Without Mobile Device Management

by Andrew Hewitt
with Christopher Voce, Clare Garberg, and Diane Lynch
May 15, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Enterprise Mobility Management, Q4 2017

Organize For Mobile Development Success

The State Of Enterprise Worker Mobility, 2017

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

FORRESTER®

Device-Centric Mobility Strategies Limit Mobile Transformation

Customer-obsessed I&O teams know that providing employees with access to mobile applications is good for business, but they're missing a greater opportunity.[1] Today's mobility managers rely heavily on device-centric technologies such as mobile device management — but MDM can't help when device management is neither feasible nor desirable for groups such as:

- **Contractors and B2B partners to which you want to extend mobile services.** Unlike typical full-time employees, these groups might work for multiple companies simultaneously or may have to follow their own companies' mobile policies. Because a mobile operating system can accept only one MDM profile at a time, it's difficult to enroll these workers and give them access to the apps they need. This was the case for one large energy company that developed 30-plus mobile apps for its global population of contractors, only to find that the workers couldn't access the apps in a secure way.
- **Privacy-minded employees who use personal devices for work.** Forrester's clients routinely report that their employees worry about the company's ability to view and remotely wipe personal data from their devices. One large manufacturing company found that only 60% of employees would accept MDM enrollment on a personal device, which left them unable to access the company's nearly 100 mobile apps. While employees' concerns might be more emotional than practical, organizations need to explore alternative options for privacy-minded employees who will never accept MDM enrollment.[2]

App-Centric Solutions Bring Mobile To Underserved Groups

How can I&O teams give application access to employees who can't or won't enroll? The easiest answer: Add security functionality into the apps themselves. Today, there are three ways to do this, but all of them involve using either a software development kit (SDK) or "app wrapper" to add an additional layer of security and manageability into the application (see Figure 1, see Figure 2, and see Figure 3). When implemented, these controls help I&O professionals ensure access to mobile applications even if a device is unmanaged. The three main approaches are:

- **App containerization.** Containerized solutions from traditional enterprise mobility management (EMM) vendors like BlackBerry, Citrix, and IBM are easy to recognize. Employees log into a single encrypted portal application that grants access to many other apps.[3] This partition allows employees to easily distinguish between work and personal apps, but constantly switching between their containerized and personal apps can be disruptive. I&O teams frequently deploy containerization when employees need access to both public and custom-built applications or if the apps are hosted on-premises.

› **Standalone mobile application management.** Vendors such as Appaloosa and Apperian use app wrapping to add additional security and management functionality on an app-by-app basis. These sit alongside personal apps on a worker's device rather than in a container. Provided the app is compatible with the wrapper, these solutions offer the most native experience for users. They're an excellent fit for organizations that have large estates of custom-built applications and want visibility into who's downloading and using those apps. Because of the potential limitations of wrapping third-party apps, I&O pros who oversee a large, diverse group of them must evaluate whether standalone MAM is a fit.[4]

› **App augmentation.** These technologies operate in tandem with containerization and standalone MAM products but offer additional integration and security functionality. For example, Appdome fuses applications with additional security policies, such as anti-tampering and code obfuscation. I&O pros can also quickly add one or multiple EMM-specific SDKs to mobile apps, which speeds delivery and drives down costs. Other vendors, such as Better Mobile, offer an SDK that integrates with EMM solutions to provide real-time discovery and remediation of malware and other vulnerabilities within the apps.

FIGURE 1 App Containerization Is Ideal For Separation Of Personal And Business Apps

Spotlight: MAM from EMM

What it offers:

- ☑ SDK-based monolithic container
- ☑ SDK-based app wrapper
- ☑ Additional SDK framework championed by AppConfig for MDM-enrolled devices
- ☑ Fully brandable enterprise app store, with option to enroll in MDM (preferred method)

Use for:

- ☑ Custom, vendor, virtualized apps
- ☑ On-premises or hybrid environments
- ☑ Groups that require basic levels of security through an SDK
- ☑ Better visibility into application adoption through a single management console

Don't use for:

- ☑ Large mobile environments with heterogeneous operating systems
- ☑ High security environments without add-ons
- ☑ Organizations that can't afford testing and configuration of SDK updates

Sample vendors:

- ☑ BlackBerry (Dynamics)
- ☑ Citrix (MDX)
- ☑ IBM (MaaS360)
- ☑ Microsoft (Intune MAM)
- ☑ MobileIron (Apps@Work)
- ☑ Sophos (MAM)
- ☑ VMware (WorkspaceOne)

FIGURE 2 Standalone MAM Is A Good Fit For Many Custom-Built Apps

Spotlight: standalone MAM

What it offers:

- ☑ SDK-based app wrapping
- ☑ Binary-based app wrapping
- ☑ Fully brandable enterprise app store
- ☑ App management capabilities such as license management, app signing, user reviews, etc.

Use for:

- ☑ Large populations of contract workers
- ☑ Populations who won't enroll in MDM
- ☑ Layering time-specific app policies, such as app expiration
- ☑ Large environments of custom-built apps

Don't use for:

- ☑ On-premises environments
- ☑ High-security scenarios where encryption of data at rest is necessary
- ☑ App ecosystems that are 100% vendor-built

Sample vendors:

- ☑ Appaloosa
- ☑ Apperian (Arxan)
- ☑ Pulse Secure

FIGURE 3 App Security Specialists Add Additional Integration And Security Capabilities

Spotlight: app security specialists

What it offers:

- ☑ Third-party SDK and app wrapping augmentation
- ☑ Mobile app fusion without changing the source code
- ☑ Bridge the gap between EMM services and apps (for example, VOIP might not work through EMM)

Use for:

- ☑ Layering additional security capabilities to an EMM or MAM suite
- ☑ Reducing burden on SDK testing and configuration, both short- and long-term
- ☑ Identifying and remediating attacks in real time, DLP
- ☑ Ensuring parity of application security functionality across operating systems

Don't use for:

- ☑ Providing a mobile application catalog
- ☑ Application management capabilities, such as app distribution, app updates, and license revocation
- ☑ Device-specific capabilities, such as geofencing

Sample vendors:

- ☑ Appdome
- ☑ Better Mobile
- ☑ Blue Cedar Networks

Use App-Centric Solutions To Increase Your Enterprise Mobile Reach

As I&O teams evaluate their mobile app management needs, it's useful to examine the business benefits that organizations achieve when they make app-centric mobility management part of their strategy. For example:

- **A US-based cable company uses containerization to improve contractor productivity.** A large cable company used IBM's MaaS360 container to deploy apps to contractors installing cable services in the field. The solution supports 14,000 personally owned tablets that contractors use to get product information, interface with customers, and order new parts. How does it work? Contractors authenticate using a URL, which then grants access to a set of custom-built apps. Because the apps are using MaaS360's SDK, sensitive data is encrypted, and the company's mobility team has visibility into app downloads and usage.
- **Leroy Merlin uses standalone MAM to improve the employee experience.** Leroy Merlin is a French retailer that recently gave 7,000 employees access to 40-plus apps on unmanaged BYOD devices.[5] The company uses Appaloosa's enterprise app store to allow employees to download apps in a self-service manner. The solution helps Leroy Merlin monitor app usage and performance, and employees can submit reviews to drive continuous improvement of the applications. If an employee leaves the company, Leroy Merlin simply revokes access through credentials or remotely wipes all corporate data within the apps.
- **A financial services firm augments apps to speed delivery and increase performance.** After moving to BYOD, a leading financial services company opted to use app wrapping to secure apps.[6] However, the process was manual, and the wrapper caused many apps to perform erratically. Recognizing the need to provide a better experience, the firm now uses Appdome to quickly integrate MAM policies to its applications. The effect is twofold: I&O teams can secure and distribute new applications faster, and employees have a consistent app experience across operating systems.

Recommendations

Next Steps: Build A Plan To Drive Mobile App Adoption

"If you build it, they will come" is a famous line from the 1989 movie *Field Of Dreams*.[7] Sadly, it doesn't apply here. While it might be tempting to think that we can simply build and distribute applications and that employees will magically start using them, I&O pros know that never works. You need to develop an engagement strategy that encourages adoption of mobile services throughout the organization to avoid investments in apps that nobody uses. To successfully drive mobile app adoption, try:

- **Crafting a marketing campaign.** How will employees know when you publish a new app to the app store? An internally distributed electronic newsletter is useful for widely applicable apps. Savvy Forrester clients have also used mobile notifications through an enterprise app store to target specific roles that might find an app useful. If you're releasing many apps at once, hold a "new technology showcase" to demonstrate the value of new applications and allow employees to test them. Publish a video series for remote workers or contractors working on the other side of the globe. Think broadly here, and don't be afraid to experiment.
- **Nominating line-of-business evangelists.** While marketing campaigns do help drive awareness, word of mouth is still the primary avenue through which employees hear about and test mobile applications. If you have an employee who absolutely loves a mobile application that your mobility team has developed, consider formally appointing that person to evangelize the benefits of that mobile app in their line of business to help get the word out. Because these evangelists have seen the value in their work, they'll internalize and communicate the benefits in a way that you can't.
- **Engaging more deeply with the science of productivity.** Forrester's employee experience research shows that the No. 1 determinant of employee happiness is the ability to get work done.[8] If your apps don't serve that purpose, employees will neglect them. We recommend that I&O teams conduct regular sessions with employees to understand their daily journeys.[9] Strive to identify areas where employees could benefit from a mobile experience, where their apps currently succeed, and where they fall flat.[10]

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Endnotes

[1] Forrester's mobility research has proven that empowered mobile employees are happier and more productive and that they serve happier customers. For example, Forrester's Employee Mobile Mind Shift Index shows that, compared with the least mobile-intense users, mobile-enabled employees are 28 percentage points more likely to estimate their company's year-over-year revenue growth as 10% or more. See the Forrester report "The State Of Enterprise Worker Mobility, 2017."

[2] Forrester often speaks with clients who have trouble enrolling users in an MDM service. Employees frequently believe that the MDM service can see more than it realistically can. Photos, contacts, and personal application data typically don't fall under the purview of an MDM service. For example, an MDM tool can't see a password for a mobile banking application. Technology organizations must educate their employees and clearly delineate what the MDM can see versus what it can't.

[3] Forrester published a report in 2014 that illustrates the key differences between SDKs and app wrappers. This advice is still relevant, with the exception that mobile app augmentation platforms make SDKs much easier to implement than they were before. See the Forrester report "In The Mobile Security Bout Of The Year, App Wrapping Beats Containerization On Points."

[4] Apple and Google prohibit the modification of apps. It's illegal for an enterprise to take an application written and published by someone else and modify it without the developers' express permission. Apple terms and conditions enforce a similar concept when enterprises download mobile applications from iTunes, making it against the rules for an enterprise to modify the binary in any way.

[5] BYOD stands for "bring your own device."

Source: "Case Study: Leroy Merlin," Appaloosa, 2017 (https://gallery.mailchimp.com/112da966ecc1729b85efd5398/files/3bb9cdbc-af56-4e85-b361-55b0ed715df4/Use_Case_Leroy_Merlin_Final.pdf).

[6] Source: App Dome Case Study (https://www.appdome.com/lp/case-studies/financial-institution).

[7] Source: Field of Dreams, Universal Studios, 1989.

[8] See the Forrester report "The Employee Experience Imperative."

[9] For more information on the employee journey, see the Forrester report "Focus On Employees' Daily Journeys To Improve Employee Experience."

[10] Forrester has published in-depth research on how to design mobile applications according to the need of the consumer and the employee. See the Forrester report "Mobile App: How To Make A Call."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
- Infrastructure & Operations

Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

142938

appdome

Appdome is the industry's first no-code platform for mobile integration. Appdome enables the rapid integration of security, mobility, authentication, threat defense, app shielding and other features to Android and iOS apps on demand. Appdome shortens the mobile app deployment cycle and speeds app delivery for enterprise organizations, eliminating dependencies on compatibility, resources and standards inside apps. Appdome provides an intuitive and easy to use mobile integration workflow that allows users to complete full mobile integration projects on app binaries alone. There are no pre-requisites for any app. No source code or mobile development is required. The solution is currently used by the world's leading financial, healthcare and e-commerce companies to support productivity, compliance, and security for consumers and employees. For more information, visit www.appdome.com.