THE DEFINITIVE GUIDE TO MAM®

MOBILE APPLICATION MANAGEMENT

Best Practices for Driving Secure App Adoption in the Enterprise and Managing the Complete Mobile App Lifecycle



Executive Summary

Organizations of all sizes are recognizing vast opportunities to use enterprise mobile apps to foster collaboration and drive new levels of productivity. However, many IT administrators, developers, and organizational leaders are struggling to find the most effective way to securely deploy and distribute mobile apps while stimulating user adoption. This guide is intended to help educate anyone who is interested in mobile apps while providing best-in-class techniques for achieving exceptional ROI on their mobile investments. By the end of this paper, you should feel confident sourcing a mobile application management solution based on the set of requirements best-suited for your organization.

Enterprise Mobile "Apps that Matter" While hardware certainly plays a role in driving enterprise mobility, it is the apps that deliver value to the user, not the device. Early uses of smart devices at work centered on a few core apps: email, calendar, and contacts. Users then started bringing their "personal apps" into the workplace, and software providers recognized this trend and began offering apps that were purpose-built for the workplace. IT organizations and business leaders began seeking ways to leverage those apps while also building company-specific apps. When "apps that matter" are delivered to a workforce it can redefine the way business gets done.

Mobile-enabling the "Extended Enterprise" Organizations are increasingly enabling contracted teams, business partners, franchisees, and/or dealers with the same apps that full-time employees use. Today's IT organization is tasked with securing and supporting corporate apps on devices they do not own or do not entirely control, and it is vital to ensure security and governance of corporate assets – the apps and data.

Limitations of Legacy Mobile Management In the early days of mobility management, the only option to secure content and apps on a mobile device was with Mobile Device Management or MDM. In order for device-centric tools to do anything, an MDM "profile" must be installed on a device, and the industry has realized two major limitations with MDM-based mobility management solutions: limited reach as well as limited security and management of apps.

Need for Mobile Application Management (MAM®) As mobile apps become more widespread, sophisticated, and integrated, an approach is needed to provide an enterprise "system of record" for mobile apps that secures, deploys and manages apps throughout their entire lifecycle. A comprehensive MAM solution provides the distinct benefit of being able to distribute apps to any device, regardless of whether it is under corporate management via MDM.

MAM Capabilities and Your Requirements The center of the universe for a MAM product is the mobile app, and a strong solution must approach app management with the full app lifecycle in mind. Each app's lifecycle stages include: app onboarding, app inspection, app protection, app signing, app deployment, app analytics, and app administration. Understanding the broad range of best-of-breed MAM capabilities, combined with your specific business needs and mobile environment, will determine your MAM requirements.

Mobile Apps Are Taking Center Stage

There are millions of iTunes, Google Play and Windows apps used by people every day. This wave of "consumer apps" has entered the business landscape, too. Consider how often you use your own phone or tablet to get work done instead of your laptop or workstation. Why is this? The increasingly robust functionality and consumer-like mobile experiences extended to employees, coupled with a growing portfolio of task- or occasion-specific apps, offer tremendous opportunities to create value in the enterprise.

The trick is how best to tap into this potential and deliver real impact in the workplace. There are a lot of components that feed into this progressively app-centric environment, which we will explore in this paper.

Early forays into using smart devices at work generally centered on a few core apps: email, calendars, and contacts. Users saw the promise and started bringing their "personal apps" into the workplace. The utility of "consumer" apps, such as Evernote and Dropbox, exposed a critical enterprise need. Software providers recognized this trend and soon began offering apps that were purpose-built for the workplace. These were often mobile front-ends to existing enterprise apps such as SAP, CRM, or Salesforce.com.

Upon witnessing the early adoption of these 3rd party apps made available via the public app stores, IT organizations and business leaders began seeking ways to leverage the viral adoption of those apps while also building or commissioning company-specific apps. Today, the mix of potential enterprise mobile apps is limitless and as varied as the companies using or creating them.

What has become increasingly clear as the mobility marketplace evolves is that the real value to the enterprise is embedded in the mobile app and content. Every business has employees using smartphones, but it is the apps on their employees' devices that will serve to differentiate the services they provide to their customers. Mobile hardware (smartphones and tablets) evolves at a rapid pace and is replaced by users every year or two. The device is essentially an enabler to connect the users to their apps and content, which are increasingly stored in the cloud. Users require apps that create, access, and present important content and support important business processes. Innovations in mobile hardware have led to some really interesting and valuable new kinds of mobile apps, leveraging hardware-enabled data such as accelerometer, location, camera, augmented reality and so on. While hardware certainly plays a role in supporting the evolution of apps, it is the apps that deliver value to the user, not the device.



What has become clear is that as the mobility marketplace evolves, the real value is in the mobile app and content.

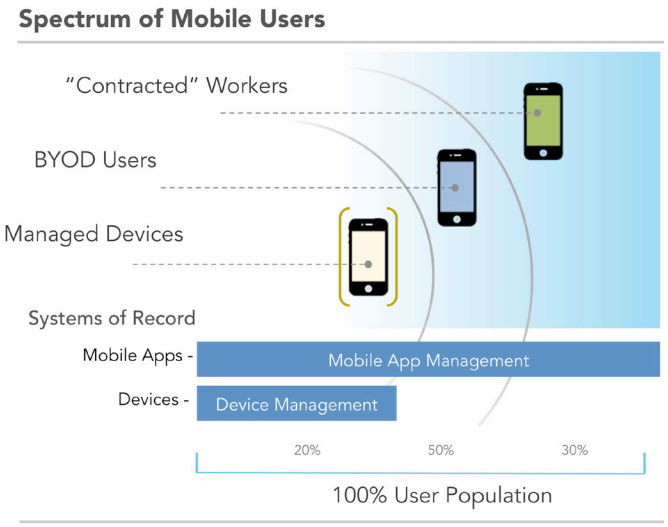
Focus on the "Apps that Matter"

With apps as the true focal point for users, it is important to understand which apps will have an epochal impact on your organization. Employees may use note-taking apps or want a mobile version of the company directory or conference room booking. These are all helpful utility apps that can make users feel more productive. They are not likely to be the types of mobile apps that will lead to profound business impact for your company.

The "apps that matter" will redefine the way business gets done and have a considerable impact on revenue, customer support, process efficiency, and/or costs. Because they are specific to your organization, they will likely be custom built – either by your company's developers or outsourced to a contractor creating the app on your behalf – and tied into back-end systems. The apps may improve existing processes (e.g., open, work, and close a customer trouble ticket remotely) or they may allow your organization to create an entirely new way to address an operational function (e.g., enabling field sales reps to sell side-by-side with their prospects and create a more intimate and engaging sales experience.) Their impact will be so dramatic that you will want 100% of the potential users to obtain and use these apps.

The Need to Mobile-Enable the "Extended Enterprise"

The demand for custom enterprise mobile apps — apps that are specific to a company or set of users— is increasing. But so too is the need to get those apps into the hands of a wider population of end users. Organizations are increasingly enabling contracted teams, business partners, franchisees, and/or dealers with the same apps that full-time employees use. Coupled with the fact that many employees are using their personal devices in the workplace via BYOD, today's IT organization is tasked with securing and supporting corporate apps on devices they do not own or do not entirely control. In this new world, it is vital to ensure security and governance of corporate assets —the mobile apps and content— used by this distributed enterprise.

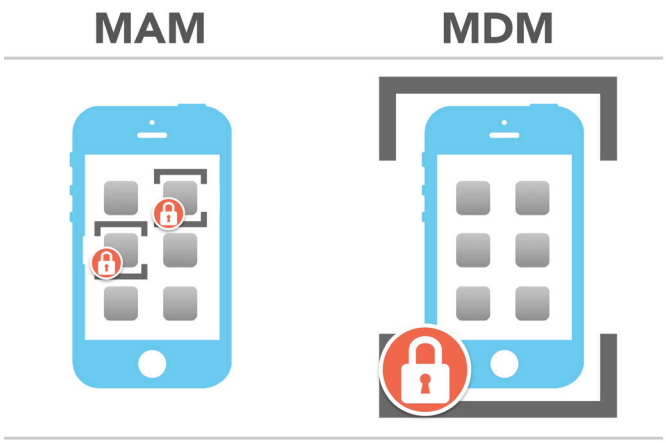


The Limitations of First Generation Mobility Management

In the early days of mobility management, the only option to secure content on a mobile device was with Mobile Device Management or MDM. Support for MDM was offered by operating system vendors to allow IT organizations to apply a level of management and control over a device, whether personal or corporate-owned. This would allow any administrator to lock down a device, wipe it, automatically set or override system configuration settings, force install or delete apps, or view installed apps and other content on the device.

As the name implies, MDM-based systems are inherently focused on device-level capabilities, and any innovations have been focused on the device itself. MDM provides IT with the ability to configure devices in an attempt to secure the entire device and all data on it. In order for device-centric tools to do anything, IT or end-users must first install an MDM "profile" or "agent" on a device. Once the profile has been accepted or acknowledged by the user, the device is "under management" and the MDM system administrators may view and control the device via the aforementioned MDM commands.

The industry has realized two major limitations with MDM and MDM-based mobility management solutions: limited reach and limited management functions for apps.

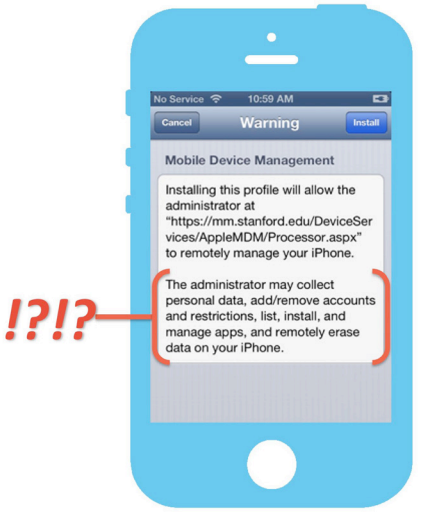


Limited reach involves an architectural restriction that prevents the ability to reach any user who does not have their device under management. Depending on the organization, this may constitute a high percentage of potential users for a particular mobile app. Many would-be users either do not want (BYOD) or cannot technically allow (the extended enterprise) their devices to accept these restrictive controls.

MDM tools make the distinction of management status at the device level, which does not allow multiple parties to manage the various apps and data they have provided. With one device = one MDM profile, there is limited flexibility, especially in the situations mentioned above, where contractors and others with an arms-length relationship are using apps and data. Put simply, if there is already MDM on a device, no other organization can manage or secure that device with MDM.

As mobile workers and particularly BYOD users become more aware of the downsides of accepting an MDM profile on their device, they do not want to run the risk of IT accidently or intentionally viewing, retaining, or erasing their personal data. Plus, personal privacy concerns around MDM are increasingly publicized as personal data breaches have gained notoriety. As a result, users are refusing to allow their devices to become restricted, unions are setting policies for their workers, and countries and governments are beginning to take a stance. In Europe, many national privacy regulations severely restrict the capabilities of MDM to secure devices, leading companies to reduce their reliance on device level monitoring.

MDM Gets Full Device Access



An organization's response may be to eliminate email access for users who do not accept the MDM profile/agent. Consider the scenario where a user relies on email in the field transacting with customers and then loses that and other access when one draconian policy forces opt-out. Ultimately, restrictive policies such as these lead to heightened user frustration and lower worker productivity.

Meanwhile, other would-be users may be unreachable because of their roles —contractors, consultants, or franchisees— and, as such, cannot technically be forced to accept MDM. To enable these workers with the power of mobile apps, many IT organizations now prefer alternative methods for securing and managing corporate apps and content through a means that does not require full device management.

Forcing users to install and accept MDM on their devices creates confusion and frustration – and ultimately leads to lower levels of device usage and app adoption.

The second limitation of MDM-based mobility management solutions—limited management functions for apps—is also the result of the traditional focus on device-level controls. MDM may offer powerful capabilities for controlling the device itself and what runs on it but, as the volume and complexity of enterprise apps continues to increase and user base broadens, there is a transformation of variables around an organization's app portfolio that must be managed. With multiple permutations of device ownership, user groups, and app portfolios, varied management approaches are required. Basic app distribution features in MDM are simply ill-suited for anything beyond very small deployments or the distribution of a relatively simplistic mobile app. As one industry analyst puts it, "MDM-based approaches 'major' in device management and only 'minor' in app management."

The Need for Contemporary Enterprise Mobility Management

Much has been learned about enterprise mobility management over the past few years, along with the capabilities needed to support the modern enterprise, as the focus shifts from devices to apps and content. Before we dive into the technical requirements, consider these higher-level objectives, highlighted by research advisory firm, IDC[1], of an app-centric mobility initiative:

- Support the business requirements of mobile apps, such as return on investment (ROI)
- Protect the digital assets and data of the firm
- Respect and protect individual privacy
- Drive adoption and provide visibility
- Assist in support and cost reduction
- Integrate with corporate identity
- Facilitate best practices over the entire lifecycle, including reducing app events and providing seamless developer integration
- Reduce the complexity inherent in enterprise mobility by providing a common process for application management, security, and delivery across device platforms

Meeting these objectives can be a real challenge, yet they can be addressed with current technology. For many organizations, the value of getting started outweighs the cost of waiting. Technology providers have made significant advancements in these areas, and there are safe and scalable approaches for securely deploying apps to users across the extended enterprise. Some solutions are stronger at meeting particular requirements, while limited in addressing others. Ultimately, it will be up to you and your team to determine your priorities and most important requirements. The remainder of this guide is intended to help you map out the range of capabilities possible with best-of-breed Mobile Application Management (MAM) and the value they can deliver to your enterprise mobility initiatives.

Requirements for Best-of-Breed Mobile Application Management

As mobile apps become more widespread in the enterprise and sophisticated in function and back-end integration, an approach is needed to provide an enterprise "system of record" for mobile apps that secures, deploys and manages apps throughout their entire lifecycle. Systems of record are applied to critical enterprise systems and act as the authoritative source for a given data element or piece of information or process. [2]

1. Evaluating Requirements for a Life-Cycle Approach to Mobile Application Management November 2013 Adapted from 2013 Mobile Application Management and Security Technology Assessment by Stacy K. Crook, IDC #242183
2. http://en.wikipedia.org/wiki/System_of_record

In enterprise mobility, MDM systems have become a system of record for devices under management and act as the main point for device-level policy enforcement. While some such systems may offer select features for mobile apps, such as pushing app bundles to devices, their app management functionality is generally very limited and is also dependent on the device being under management with MDM. As such, they are generally only used in settings with corporate-issued devices.

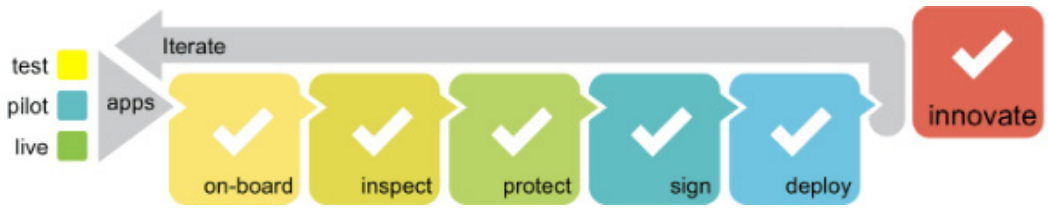
Why do enterprise mobile apps require a dedicated system of record for apps that is distinct from devices? Because the lifecycle and management needs of hardware and software are fundamentally different, and systems that track them are, and must be, architected differently with specific data elements and functionality as the primary system focus.

Consider other systems of record you may be familiar with and how they are optimized around their core mission – from the central data elements to core functionality. For example, many organizations use Salesforce.com as a system of record for sales prospects and customer selling activity. Other systems in use may also contain information about customers, such as helpdesk management systems and billing and GL systems, but the definitive source to customers' sales status is the system of record: Salesforce.com. Those other systems may very well integrate with Salesforce.com for exchanging data elements, but whenever there is a question about a customer's sales activity, users will turn to the system of record.

The complement to a system of record for devices is one purpose-built to manage all aspects associated with mobile apps and offer a counter-point to existing, device-centric systems of record. As discussed earlier, the growing diversity of the mobile population will demand more types of management than just device management, either as a sole system of record for managing the apps and data that users rely upon or augmenting and extending the capabilities of an existing MDM tool. Best-of-breed mobile app management platforms are designed to serve this role in the enterprise for both devices under management as well as unmanaged devices.

A robust MAM platform should provide a broad range of capabilities around securing and managing all mobile apps for an organization. Once believed to be suitable for only higher-end deployments, MAM capabilities have become must-haves for nearly every organization with the desire to support employees and other workers with mobile apps and content. A comprehensive MAM platform also provides the distinct benefit of being able to distribute apps to any device, regardless of whether it is under corporate management via MDM.

Mobile App Lifecycle Management

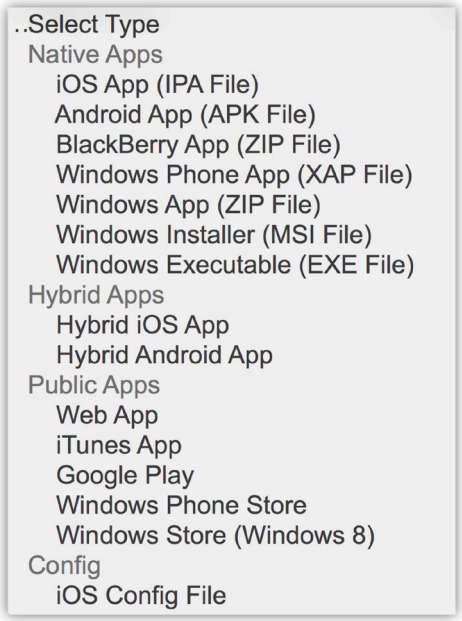


Since the center of the universe for a MAM product is the mobile app, a strong solution must approach app management with the full app lifecycle in mind. The app must be smoothly transitioned and managed throughout its "life."

Each app's lifecycle stages include:

- Adding apps to the system of record ("app onboarding")
- Inspecting apps to make sure they are safe ("app inspection")
- Securing apps with policies ("app protection")
- Adding credentials to apps so that they can run properly ("app signing')
- Distributing apps to all the users ("app deployment")
- Determining whether apps are being used, and obtaining user comments ("app analytics")
- Updating apps on a regular basis ("app administration")

Onboarding New Mobile Apps for Workers



As mobile apps are developed and ready for deployment or user-testing processes, they must be onboarded onto the management platform in order to get the apps "under management." Bringing new mobile apps under management should be straightforward and ideally performed without deep technical skills. As organizations scale app deployments, automating or shifting responsibility for app deployments away from highly technical staff can lead to significant savings. This enables any level of mobile administrators to make new apps available to workers from a variety of sources—whether internally developed, sourced from a vendor, or built by an app developer.

Custom mobile apps can be developed using a cross-platform Mobile App Development Platform (MADP) from software vendors. They can also be developed using native tools, such as Xcode or Eclipse. Most organizations have multiple development platforms concurrently in use in their own development environments while also procuring apps from 3rd party vendors or contractors. This underscores the value of a single system of record to allow administrators to onboard and manage new apps and maintain an ability to track them over the course of their useful life. This is where the use of a MAM platform distinct from the development and build environment is invaluable. This also means your MAM platform needs to support a broad range of MADPs.

Seamless onboarding and integration of new apps eliminates manual handoffs while reducing the risk of incorrect versions making it into production. App developers—whether in-house or contracted—no longer need to use "sneaker net" or email to send around their finished apps. They also do not need to devote time side-loading apps onto users' devices. Simplified deployment also sets up a "best practice" for vetting apps and placing them under control. Given the diverse sources for purchasing or developing apps within the enterprise, a standardized approach to deployment will streamline the process.



Seamless onboarding and integration of new apps eliminates manual handoffs while reducing the risk of incorrect app versions making it into production.

Once an app is published into the MAM platform, an administrator can begin downstream app management tasks, such as inspection and testing. The administrator should also be able to set and migrate the app's status from test to pilot to production, making it clear how the app is to be used and by whom.

Inspecting Mobile Apps for Malware, Privacy, and Risky Behavior



Once new apps have been onboarded into the MAM platform, they should be immediately inspected for malware, privacy, risky behavior, and other security issues. App inspection, coupled with additional built-in workflow controls, prevents apps from going live until they pass a quality and security inspection. This will also ensure that all apps behave as intended. Issues caught during this phase may include detecting malware and malicious code, unauthorized server calls, or extraneous use of GPS. This provides another opportunity to enforce best practices and identify inefficiencies or subpar efforts that may lead to poor performance, excessive battery use, inefficient network usage, and more. Administrators should also be able to save inspection reports for each app/version that can maintain an archive to easily compare across app versions and document/observe changes. This capability makes it extremely easy for IT administrators to promote a kind of "social contract" for users through the ability to share information about how business apps are interacting with each user's personal (BYOD) device.

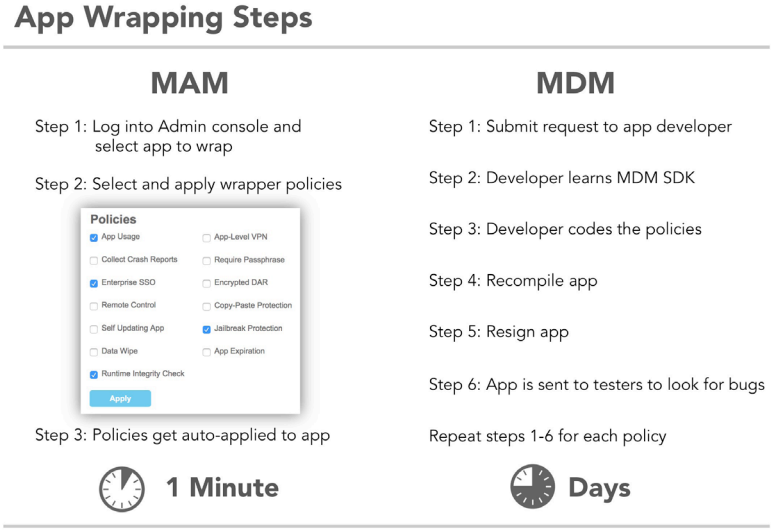
After an app has been inspected and meets the organization's criteria, the MAM platform should support the continuation of app approval workflow as each organization's governance process dictates. This allows for discrete approval of app QA and security review procedures that will likely be essential in both corporations and public sector deployments. In conjunction with app migration capabilities, detailed audit logs can keep a record of who approved each app and link to the appropriate app inspection reports.

App Security and Policy Management

After an app has been onboarded and inspected, the next step in the mobile app lifecycle is to apply appropriate security and app usage policies to each app. By applying fine-grained policies at the individual app level, a best-of-breed MAM platform can deploy the app safely to any user's device.

By applying fine-grained policies at the individual app level, a best-of-breed MAM platform can deploy the app safely to any user's device.

This step effectively enables the organization to distribute the app to any user throughout the extended enterprise—including those users where MDM-based approaches are not possible or desired, such as BYOD, contract workers, dealers, franchisees, and those who's devices are managed by another organization. Each app is essentially encapsulated in a virtual "container" that holds a set of policies in and around it so that MDM device management is no longer a prerequisite for app security. This effectively creates a logical management domain at the app level. This represents a management domain that can be extended very broadly to employees, contractors, partners, and anyone else using a device independent of MDM. Providing policy secured and managed apps whether MDM is on the device or not.



Examples of app security and usage policies may include enterprise single sign-on, app usage and analytics, app-level VPN, app expiration, copy/paste disable, self-updating apps, jailbreak detection, and more (for a more complete list of potential app policies, please see Appendix A.)

While they should be supported as a method to apply app policies, Software Development Kits (SDKs) can limit your organization's development choices – the SDK must be available for the tool. Getting third parties to standardize, include, and update when necessary is impossible. Additionally, since there is such a broad range of app sources, the entire user base is rarely on the same version of an app, especially when the releases are frequent. This results in a deployment scenario where 100% compliance cannot be ensured and users have multiple versions of apps at various states of policy compliance.

Your MAM platform should also support "no-code" application of app policy. These advanced app wrapping techniques eliminate the need to have a developer modify code while enabling a non-technical administrator to apply policies as needed. A set of policies should therefore be easily copied and applied to an entire set of apps with the click of a button.



In addition to supporting the use of an SDK, your MAM platform should also support "no-code" application of app policy.

An additional benefit of this no-SDK approach is that it allows the organization to separate an app's business logic (programmed by the app developer) from the app security and usage policy (applied by the system administrator or security or governance team). The policies can therefore be modified as needed without requiring the developer to modify the code.

A "dynamic policy" approach takes policy to the next level in terms of post-launch flexibility and ease of administration. This means that new policies can be applied—and the parameters of existing policies can be changed—without requiring users to re-download or re-install the app. This should be an essential requirement for deployments, as it enables policies to be modified once the app is deployed and being used by workers. That way business critical apps that are fixed to a specific version, are only updated infrequently, or are no longer supported by a developer, can continue to receive management and security updates while the core code remains unchanged.

The power of a policy framework should not be limited to pre-existing security and usage policies. The MAM platform should also provide flexibility for custom policy development via a documented, open API. This will enable the organization, business partners, and app providers to create organization-specific policies and apply them to any mobile app or set of mobile apps.

App Signing

One of the biggest complexities for app developers and administrators is the requirement to "sign" all apps before they can be deployed to a user's device. In Apple's iOS environment, signing an app is when the enterprise applies its enterprise credentials to each app. This is a way of signaling to the mobile device that it is a legitimate app and therefore allowed to run. Signing must occur after each app is compiled, recompiled, and distributed. In iOS, every app's provisioning profile must also be re-signed at every 12 months to ensure it is deployable.

The MAM platform should also provide a centralized way to manage app signing credentials and processes. Just as the policy engine enables administrators to apply policies independently without developers, an app signing facility should allow any authorized administrator to sign an app from an admin console and prepare it for deployment. This will greatly reduce the time and complexity of signing apps while enabling the signing process to be repeated easily with predictable results.



A centralized mechanism for administering App Signing will address one of the most significant complexities organizations face with enterprise mobile apps.

Deploying Apps to End Users

With one or more mobile apps onboarded, inspected, signed, and secured for the enterprise, it is time to deploy them into production for end-users. There are several ways in which a custom mobile app can be deployed to users in the organization and the extended enterprise.

Public App Stores Publicly available app stores, such as Apple iTunes or Google Play, can theoretically host custom private apps for workers. However, this approach will make your app viewable and downloadable by anyone and everyone. Even if your app has login requirements and other security measures, this is generally not a recommended approach. This method increases the risk of your app being downloaded by competitors. At a minimum, it signals very clearly to competitors which apps and functionality you are making available to your workers.

Customer feedback has consistently shown that public app stores are not a good option for private business apps as they make it confusing to employees who are trying to locate the proper apps. They hinder the "app discovery" process, by which a worker can easily discover the apps that are relevant and should be used. Public app stores also confuse end-customers, who may believe it is a consumer app, leaving them confused and frustrated with your brand.

Private Views to Public App Stores Apple recently introduced a "private" version, or private view, of their app store for use by enterprises and provides for flexibility tailoring the look and feel of the environment. While this approach does address the downside of public apps stores cited above (confusing employees and customers) it is essentially a private window to iTunes. It continues to require Apple approval (and the delays associated with waiting for approval) before apps are available there. Because it focuses only on basic branding and distribution, it does not provide the kind of rich app management capabilities that are required to manage your apps through their full lifecycle, as discussed above and below.

At the time this paper was published, equivalent private app store functionality was not generally available from either Google or Microsoft. This further limits options for clients using those platforms while compounding the complexity of distributing apps in mixed operating system settings.

App Store Approaches

	Private	Public
Intended For	Employees, contractors, agents, students, franchisees	Consumers
Publish Speed	Instant	Unpredictable from days to weeks
Custom Branding	Show corporate brand through out	None. Branded for Apple, Google, Microsoft
User Discovery	Only show apps appropriate for users of a particular role, group	Must search through all (Million+) apps
Access	Only members of the private app store can access the apps	Anyone can download and install the app
Testing	Multiple versions of an app may be made available for testing purposes	Only the final app

Direct Download Links If an app is hosted on a private server, then a direct download link to that app can be shared with target users. This requires a secure server for hosting the app as well as a mechanism for distributing and promoting the app's availability and for identifying and managing end users and their entitlements. A MAM platform should support this capability for organizations that need to directly distribute a single app and/or embed the download link in other media.

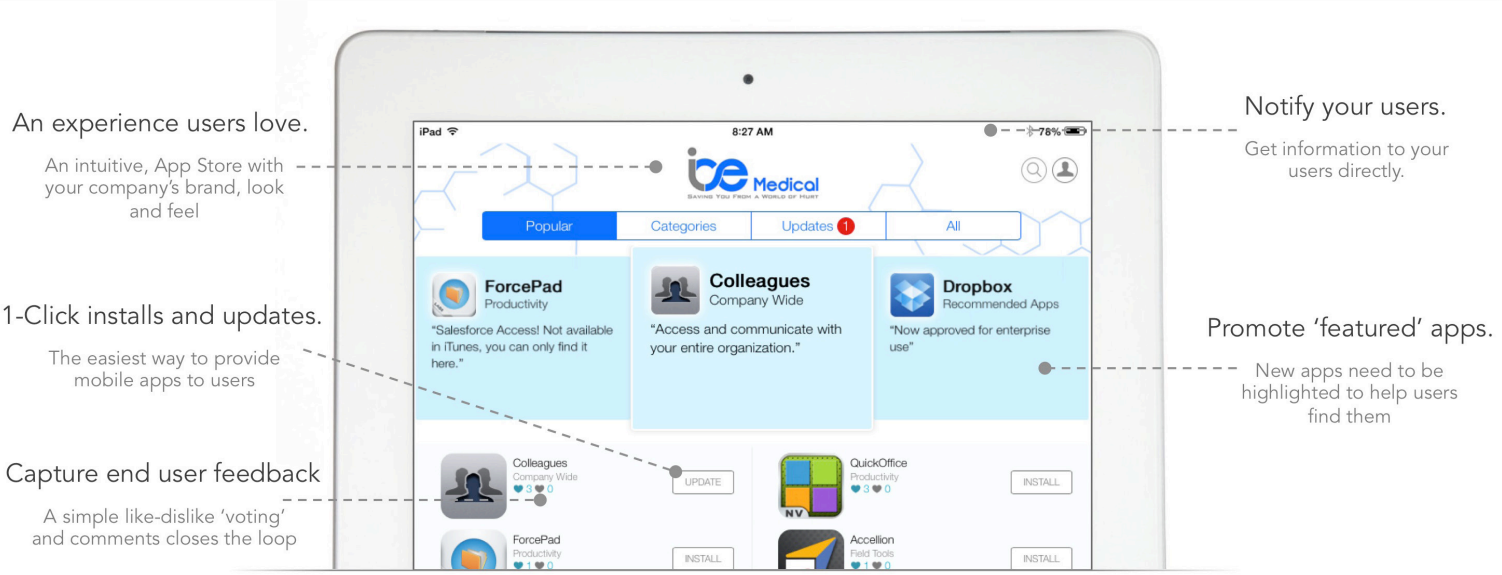
Enterprise App Stores For most organizations, a custom-branded and private enterprise app store is the optimal mechanism to display and distribute custom apps alongside a set of curated and recommended publicly available apps. The term "enterprise app store" has become popularized by media and analysts. This is peculiar since enterprise app stores are intended for all types of companies—not just large "enterprises." Besides, users are not really purchasing anything. Nonetheless, the term has become a synonymous with app delivery in the workplace.

The enterprise app store has become the de facto location for employees and workers throughout the distributed enterprise to find and download apps and content. The use of enterprise app stores have been shown to drive higher levels of app adoption and will direct employees to suggested public apps (e.g. encouraging workers to use Box over Dropbox or Google Drive), thereby creating more consistency in the organization.

While there may be lightweight "app stores" available, they only serve as a simple browsable list of links to apps. For example, the app store offering by Salesforce.com provides a minimally customizable front-end, but lacks a rich set of back-end services and workflow to make it a complete solution and requires that users have a login to that provider. Some app stores are only mobile bookmark to a website (web clip for iOS) that is served thru the default device browser without a native app store application. This approach can serve to confuse users as the app store sits side by side with other browser tabs.

The front end of an enterprise app store truly needs to be part of a more comprehensive app management platform in order to provide the necessary security, governance, and management capabilities needed for deployment in a practical work setting. Enterprise-grade app stores integrate existing enterprise identity credentials, extend existing security standards, and present a customized view of apps based on a user's device/operating system and role, while offering higher levels of brand customization.

Branded, Private Enterprise App Store



Enterprise app stores should also offer a choice of native catalog or web/HTML-based catalogs, as well as device-specific versions of native catalogs that perfectly mimic the experience users have with public app stores. Consumer-like user experiences have been found to be another driver of user comfort and app adoption. Users are accustomed to, and expect, an intuitive, easy-to-use experience.

App stores are not just valuable for sharing and distributing production apps. They can also be excellent methods for presenting test and beta versions of apps. This allows organizations to present a set of alternative apps to app testers—supporting a fully functional A/B testing environment in order to collect usability feedback from users. Here, only authorized users are permitted to see such test apps, while unauthorized users are exposed only to production apps.

Collecting App Usage, Feedback and Analytics

Whether distributing test or production apps, collecting user comments and app ratings can provide invaluable closed-loop feedback to app administrators and developers. This enables developers to iterate with the app for the next version. The app store should make collecting and rating capabilities as easy and intuitive as they are in public app stores. App feedback mechanisms should aggregate all findings across the entire population of users in order to make it easy for administrators and developers to view and export such findings for reporting.

Beyond user-initiated feedback, app analytics can enable administrators to understand actual app usage patterns. This allows app owners and administrators to track usage patterns without modifying the app's code and instead apply analytics policies to any native and custom app. This permits instantaneous and consistent analytics and reporting capabilities across an organization's entire suite of apps. In addition to tracking actual app users, another helpful capability is the ability to track the number of target users. A visual and automated calculation can indicate when an app has been adopted and track adoption changes over time. Another important feature is the ability to track how often an app is actually opened or launched compared with how often it's been downloaded. These adoption metrics will enable the administrator and app owner to determine the app's true penetration and usage.



App analytics provide invaluable insights into actual app usage and app adoption -- key to documenting ROI and spotting areas for troubleshooting.

App Updates & App Administration

It's amazing how quickly individual apps change and need to be updated. This is actually great news to organizations and users alike, since new features can be quickly envisioned and implemented. Although this does present more moving parts and variables for app developers and administrators to manage—which a MAM platform will make manageable—app-level analytics can prioritize which apps or functions demand attention based on real usage. This is another area where a best-of-breed MAM platform will make a world of difference.

Consider this: every time an update—no matter how large or small—is made to an app, it must traverse nearly all of the app lifecycle steps again. In each case, the app needs to be onboarded, inspected, have policies applied and tested, signed, and made available to users. This is why having a standardized, automated, and easily repeatable process and framework makes the app update process seamless for you. When it is so easily repeatable, you will find yourself and your organization actually welcoming new apps and app updates since they will offer value to users and will not create a mountain of work and delay for app developers and administrators.

Some enterprise mobile apps will be created for projects or other initiatives that have a defined start and end date. Other apps may simply outlive their useful life. Regardless of the circumstances, most apps will need to be retired at some point in time, and a robust MAM platform will make this easy. If a user's device is managed by an MDM system, then the MAM platform should be able to issue a command to the MDM system to delete the app. In this case, the administrative console of the MAM platform will initiate the command and the MDM software will execute it.

If a user's device is not managed by the MDM system, then a leading MAM platform will offer a few options. For instance, if a "data wipe" policy was applied to the app then the MAM platform can remotely delete all of the app's data, rendering it useless. This command can be issued remotely and without user input and will eliminate any risk of the app being used in the future. In conjunction with the "data wipe" command, the MAM platform can also issue a message directly to app users requesting that they delete the app. This approach may not appear as clean as force-deleting the app like the MDM-enabled approach is. However, it is extremely powerful since it can effectively decommission an app, or de-provision a user, on any and every device—even those not under management by MDM.

Enterprise Integration and Platform Extensibility

Given the pace of evolution in the mobile landscape, decision-makers should be thinking about ways to adapt a particular solution to your organization's unique needs. In an enterprise setting, a powerful and scalable way to do that is by integrating a solution with existing enterprise systems and management tools. This can be accomplished if the MAM platform is easily integrated and extensible by offering an open set of APIs. IT organizations and business partners will be able to integrate with and extend their own solutions when needed. The API should be broad, secure, stable and well documented. For example, the API should make it easy to understand existing workflows, monitoring and performance solutions, security, and identity infrastructures. The following are just a few examples of a MAM platform that is extensible with APIs:

App Signing Automation As discussed previously, signing apps every time they are compiled, recompiled, distributed, can create a significant challenge for IT and line of business in large scale app deployments. A MAM platform should provide the ability to automate the signing process, allowing any admin to access the service from any device. This app signing service should be able to operate independent of any other IT platform.

Universal App Distribution A MAM platform should be able to deploy policy managed apps to any device. Taken a step further, an extensible MAM platform should be able to deploy policy managed apps to any corporate app store, whether it is internally built or from another EMM vendor. Organizations that have infrastructure in place with which employees are familiar, can integrate with an extensible MAM platform to provide best in class management and security at the app-level.

Sourcing the Best MAM Platform for Your Organization

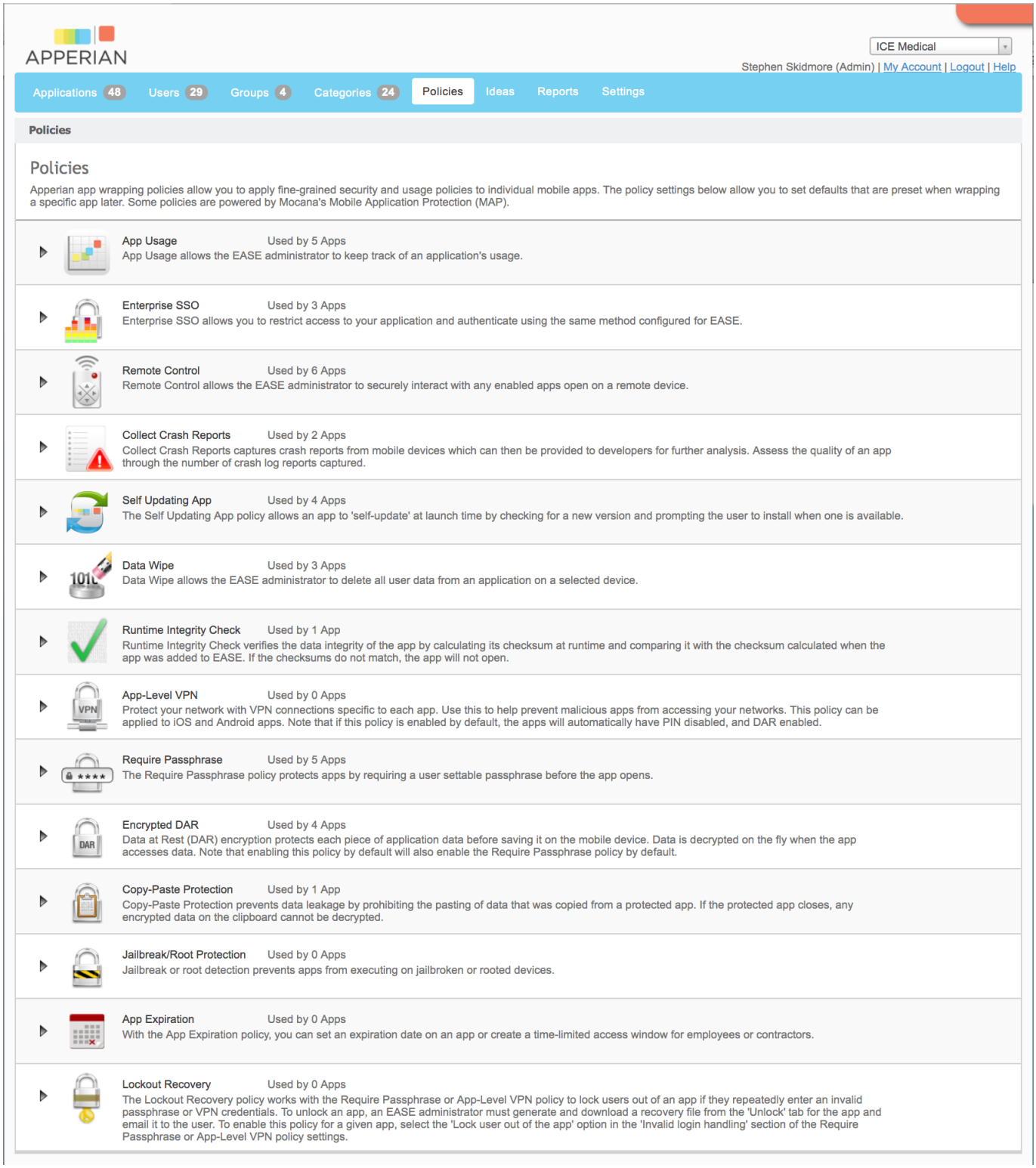
Because of the cross-functional and multi-disciplinary nature of mobile apps and their management and administration requirements, you may find a variety of vendors that offer some MAM capabilities. However, only a select number of vendors offer the full breadth covered in this paper.

We hope that this paper has enabled you to better understand the range of possible MAM capabilities and why they are important in your mobile app setting. As with any enterprise technology decision, it is essential to give careful thought to the unique requirements of your business objectives and which technology investments will support them now and in the future.

In Appendix B, we've provided an evaluation worksheet to assist in assessing your mobile app management needs and tracking a platform's ability to delivered required functionality.

If you have any questions, please don't hesitate to contact us directly at MAM-Guide@apperian.com

Appendix A: Sample Mobile App Policies



Appendix B: MAM Platform Evaluation Checklist

Platform Requirements:

- ☐ Mobile App Management (MAM) Platform must be available as a cloud-based service
- ☐ MAM Platform must not require device enrollment; must be deployed on both managed and non-managed devices
- ☐ MAM Platform must not require SDK to enforce app-level security
- ☐ MAM Platform must not limit number of apps, number of versions of apps, or size of apps secured and delivered through the solution
- ☐ Platform should enable enterprise app lifecycle management

Adding New Mobile Apps for Workers

- ☐ Platform must be able to validate if an app has been correctly signed
- ☐ Platform should perform app validation on iOS Distribution Certificate type (developer, ad-hoc, enterprise), version information, certificate Expiration
- ☐ MAM Admin should be able to use a publishing API to add and update applications without using the Admin Portal
- ☐ Platform should have plugins to Mobile Application Development Platforms (MADP) including Appcelerator Titanium, IBM Worklight, Xamarin, ViziApps and AnyPresence to allow for one-click Developer uploads
- ☐ Platform should allow apps to be published directly from build systems including Jenkins
- ☐ Platform should support deployment of public apps from Apple's iTunes App Store and the Google Play Store
- ☐ Platform should support the deployment of web apps
- ☐ Platform should allow Administrator to create a hybrid app for iOS or Android from a web URL, and apply policies to this new app
- ☐ Platform should support internally developed or licensed native iOS, Android, Windows, Blackberry and HTML5 apps

Inspecting Mobile Apps for Malware, Privacy and Risky Behavior

- ☐ Platform should allow MAM Admin to screen an app for risky behavior and vulnerabilities, such as malware and Trojans, and generate a detailed report along with remediation recommendations.
- ☐ Platform should allow Administrator to inspect a binary app file (.ipa and .apk) for malicious or risky behavior and provide a detailed report on the level of risk

- ☐ Platform should allow Administrator to check what features an app is leveraging, such as the microphone or camera, and the data it's tracking such as location, SMS messages or email archives

Mobile Security & Management Policies

Administrators must have the ability to apply layers of protection to individual apps with the following mobile security policies post-development without requiring an SDK or any code modification:

- ☐ **Corporate Authentication** – Dynamically requires users to enter their corporate credentials before the app will open and can integrate with the company's single sign-on (SSO) provider
- ☐ **Data-at-Rest (DAR) Encryption** – Secures all data stored by the mobile app with FIPS 140-2 level encryption and Suite B algorithms
- ☐ **Mobile App VPN** – Provides a dynamic, app controlled, secure connection from the app to the company's gateway for authentication and access to backend data. Does not require a management profile or configuration from the user to set up the VPN
- ☐ **Two-Factor Authentication** – Highly regulated environments require the user to provide two forms of identification; one that is a physical token, like an ID card, and a second that you know, like a password
- ☐ **Copy/Paste Protection** – Enables the administrator to prevent unauthorized copying and pasting of data from an authorized app to an unsecure app
- ☐ **Data Wipe** – Remotely wipes data from an app should the device be lost, stolen or if the user no longer needs access to the app
- ☐ **Jailbreak and Root Protection** – Ability to disable an app from running if it detects the device is in a compromised state
- ☐ **App Expiration** – Enables the administrator to set an expiration date on an app, or define a range of dates within which users can use the app
- ☐ **Run-time Integrity Check** - Calculates the checksum of an app at run time and compares it to the checksum from when the app was first imported to detect a possible mismatch. If a mismatch is detected, it means the binary on the device was tampered with and therefore will not run
- ☐ **Self-updating App** - Checks for new versions of an app at run time and prompts the user to run an update to ensure all users are utilizing the latest version
- ☐ **Crash Log Reporting** - Captures crash logs and returns them to the mobile administrator without requiring user intervention
- ☐ **App Usage** – Tracks all app usage data including each time a user opens an app, brings an app from the background to the foreground, or returns to an app from the lock screen, and provides statistics in an analytic dashboard for mobile administrators

App Signing

- ☐ Platform should store enterprise signing credentials (for both iOS and Android) so MAM Administrator can sign and re-sign apps without requiring assistance from Developers

Deploying Apps to End-Users

- ☐ Platform must manage app versions and alert users that new updates are available, through both push notification and user notification
- ☐ Platform must be able to deploy apps to end users over the air
- ☐ Platform should be able to deploy apps one at a time or as bundle
- ☐ Platform should detect the mobile platform to display and deliver the appropriate apps Platform should not have limits on number of apps, size of apps, or number of users
- ☐ Platform should support deployment of public apps from iTunes App Store and Google Play Store
- ☐ Platform should support deployment of web apps as part of a native iOS or Android application, providing access to the app functionality without a fully developed browser experience
- ☐ Users should be able to authenticate against 3rd party identity providers through SAML 2.0 or OAuth
- ☐ App Store must be native for iOS, Android, Windows 8, and Windows Phone devices, as well as via HTML5 that can run in a web browser on multiple device platforms, including BlackBerry
- ☐ Both native and HTML5 App Stores must be fully customizable to incorporate corporate "look and feel", including brandable icon, splash screen, login screen and other user interface components
- ☐ Users of the App Store must be able to install and launch an app they are authorized to access
- ☐ App Store users must have access to screen shots and related media such as PDF files and videos
- ☐ App Store users must be able view apps by Category and search for apps
- ☐ App Store users must be able to rate and provide textual feedback on apps
- ☐ App Store users must be able to install updates from within the App Store
- ☐ App Store must support multiple languages

Collecting App Usage, Feedback and Analytics

- ☐ List details of End users
- ☐ Users by groups
- ☐ Device details
- ☐ App download inventory

- ☐ App download activity
- ☐ App inspection reports
- ☐ VPP Reports
- ☐ Most Popular Apps
- ☐ App Usage
- ☐ Signing Activity
- ☐ Password Change Activity

App Updates & App Administration

- ☐ Platform must be able to deliver and manage apps to thousands of users over the air
- ☐ Platform must provide mechanism to display user terms and conditions that are authored by individual IT departments
- ☐ Platform should provide the ability to invite users to the system via email, SMS, self registration or intranet site
- ☐ Administrator should be able to access the platform from anywhere with an Internet location
- ☐ Platform should allow the administrator to assign apps to one or more category
- ☐ Platform should allow the administrator to make updates mandatory or optional
- ☐ Platform should allow the administrator to manage VPP redemption codes in bulk
- ☐ Administrator should enable users to access apps through group membership or user attribute
- ☐ Administrator should have the ability to customize the invitation email to end users
- ☐ Platform must allow an affiliated organization created through the Admin Console by the administrator of another organization—a "parent" organization

Enterprise Integration & Platform Extensibility

- ☐ Platform should support Single Sign-On (SSO) integration leveraging SAML 2.0 to the enterprise's existing authentication method
- ☐ Integrate easily with existing infrastructure
- ☐ Identity driven to ensure authorization and entitlements regardless of device
- ☐ Reach all required users in a single management domain
- ☐ Administrator must be able to specify which apps users see in their App Store, using role-based user groups or other attribute(s)
- ☐ Platform must support individual or bulk user enrollment