Enterprise mobile app security

Use mobile application management (MAM®), standalone or alongside mobile device Management (MDM), to deliver the highest level of mobile security

Executive summary

For any leader in today's digital and increasingly mobile economy, there are significant advantages to putting corporate or other sensitive data in the hands of mobile workers. There are also risks as the value of that data increases. Chief security officers, IT organizations, IT architects, and mobile app developers need to be aware of risks, and have ready access to the right tools to mitigate them.

App-level security

Mobile security tools must have the ability to apply security and management at the individual app-level so that organizations can trust apps. Security protocols such as two-factor authentication and derived credentials are often required in high profile organizations and should be available to mobile administrators. Along with security, management policies are necessary to provide visibility into individual app usage. Lastly, to ensure a high level of trust by employees, these tools must provide a secure channel for corporate apps while leaving personal apps and data untouched.

Enhance device-level security

Organizations can increase their overall security posture with the inclusion of app-centric security methods and tools that can be used in conjunction with or without mobile device management tools. Device security helps organizations trust that the device will not leak confidential data or restrict access to authorized users, and will eliminate the chance of other robust tampering of the device. Also extremely critical is trusting that the app, specifically that it behaves the way it was intended to, it doesn't access resources and data that it shouldn't, and that the data within the app is secure.

Mobile Application Management (MAM) security

MAM supports the deployment of secured, policy-enabled, and managed apps to any device in an enterprise or government organization. The key to this capability is that it applies additional protection around apps and data that goes beyond the device control provided by mobile device management (MDM), enabling even the most regulated industries to achieve the necessary level of app and data security.

MAM makes it easier for app administrators and developers to apply fine-grained security policies such as:

- FIPS certified encryption
- VPN
- Two-factor authentication
- Derived credentials
- Mandating specific OS functions prior to app launch

Extend the reach of security

All of this can be done without requiring app code modifications or the use of an SDK – making it easier for IT to consistently apply security to apps while allowing app developers to focus on application business logic. More importantly it can be done without requiring device management – extending the reach of security and management of all users without requiring a profile be installed on the device.

Securing, deploying, and managing mobile apps in highly secure settings

For organizations in regulated or highly secure settings — such as public sector, healthcare, and financial services — the risk of data leakage or attack has been a barrier to considering wide-scale deployment of mobile apps for front-line workers.

With mobile security and management capabilities rapidly improving, supporting workers in regulated environments can be done without significantly impairing the usability of mobile devices. With suitable security approaches now available, organizations can begin creating mobile apps that transform the way that work gets done in highly sensitive environments. At the same time, organizations can broaden the range of workers that can be mobile enabled — even securely supporting distributed workers in the "extended enterprise," such as contractors, dealers, agents, and others using unmanaged devices. Mobile security does not have to end at the edge of an organization. IT can now extend mobile security to all users in an ecosystem.

These mobile workers can benefit from secure instant access to critical back-end systems. Lag time is reduced, as workers don't have to wait until they are back in the office or on their laptops before critical information is brought up to date, benefiting other mobile workers and centralized workers relying on field-based data entry. In today's fast paced business environment, limiting users to certain capabilities based on their location may be secure, but it will significantly impact efficiency and competitiveness in an increasingly mobile world.

When enabling teams in sensitive settings, ensuring data and mobile app security is essential. In the early stages of mobile development, a combination of built-in app security and device-level security measures, such as passcode complexity rules and "on-the-fly" disk encryption, were commonplace. For the early adopters of enterprise mobility, device security settings were handled by MDM software.

These first-generation approaches may still be in use in highly secure settings; however, they are only part of the puzzle. As this paper will cover, advancements in app-level security and management now make it possible to ensure high levels of security — even for reaching workers with unmanaged devices.

For example, consider:

Intelligence community: Research analysts benefit from timely information that is provided by field agents in near real-time.

- Cross agency teams can securely collaborate and receive data in real-time with those in the field via mobile devices.

Healthcare: Providers can instantly gain access to patient records, trade treatment notes, and coordinate care with other physicians.

- Healthcare workers in hospitals often collaborate across business units and company lines. Therefore mobile security can not be limited to organizational boundaries, as workflows often cross them.
- Global healthcare privacy concerns can be addressed by securing mobile workflows that span the entire healthcare value chain.

Financial services: Analysts and portfolio managers can leverage up-to-the-minute market information to improve communications with clients, perhaps conducting in-person portfolio reviews.

- Providing a high level of personalization and responsiveness for high net worth individuals can have a significant impact on company performance.

Mobile App Lifecycle Management

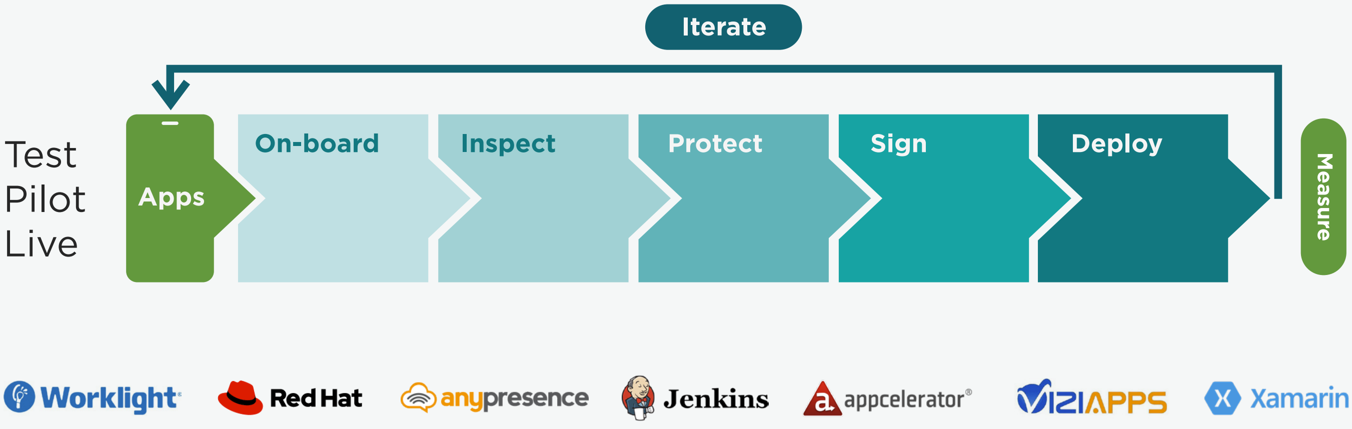

Figure 1. Mobile app lifecycle & governance

New approach to mobile security

The core principles of security involve considering possible attack vectors, assessing which are likely risks for the organization, and determining which should be addressed. Applying security and management policies at the app level provides new options for organizations to secure a wide range of potential attack vectors and risks.

MAM products enable comprehensive, fine-grained security policies, visibility, and management controls to be applied to individual apps, effectively bringing apps “under management.” These controls can be built around in-house apps as well as third party apps to allow organizations to take advantage of a larger app eco-system, while ensuring the appropriate level of security. Distribution of these apps through private enterprise app stores provides a familiar and secure channel for accessing custom apps that are not viewable or available to the general public. Security does not need to come at the cost of usability. Only MAM allows IT to target designated and authenticated users with corporate apps and data on mobile devices.

Mobile app lifecycle & governance

As organizations continue to develop a greater number of mobile apps, a standalone, standard governance and security platform to vet, secure, and deploy these apps becomes crucial to organizational control and security.

A mobile app lifecycle platform and its underlying components allows organizations to onboard apps into a centralized location, creating a system of record of all apps in their environment. Here administrators can inspect the app for malicious code or malware, sign and apply fine-grained security policies to the app, and get insight into how and when the app is being used, significantly saving time across the entire lifecycle of the app.

Evolving definition of mobile security

As mobile technologies mature and grow in use, so do the threats that will impact both users and organizations that depend on these technologies. Fortunately, the major mobile operating systems were designed in the post-PC world. These OSes are designed to inherently silo data, preventing third party apps from accessing critical system folders and other device data. For this reason, most out-of-the-box mobile devices are more secure, and will remain so, than traditional computing devices. However, there is also a downside to this OS architecture — very few tools are effective in deploying and enforcing custom security policies on mobile devices, particularly at the app level.

For the enterprise, many IT organizations want to lock down devices to put them in a compliant state. MDM has been deployed by approximately 29% of US companies[1], largely because IT had very few ways to protect mobile users. Device controls are effective at turning off capabilities when IT deems some aspects of those capabilities as unsecure. This can become problematic because the more a device is locked down, the less likely a user will be effective using it – negating investments made in devices, wireless services, and management infrastructure.

New kinds of mobile apps, new possibilities for knowledge workers

With trusted and secure mobile access to critical backend systems established, work that previously required being on a managed device or working in a restricted office can now be accomplished in the field. Using an app- and data-centric approach to security and management allows organizations to create new applications and increases the range of knowledge workers that can take advantage of these innovations.

For example, communication and collaboration apps that capture information, such as location, photographs, content, voice, and more can provide a new lifeline of real-time content streaming. This can synchronize distributed teams and enable collaboration between users by enabling information sharing in the field.

App-centric security and management enables such scenarios because the apps don't just rely on a certain device security posture; they create a safe and compliant app space with an app-level security layer, while still enforcing device security posture as appropriate.

The future for mobile security is not through locking down devices, but rather securing the deployment and usage of mobile apps.

Why is app-level security so critical?

With the ability to implement an additional app security layer that deals with data-at-rest, data-in-use, and data-in-motion encryption, in addition to — or instead of — device-level capabilities, organizations have choices to create and deploy secure apps to:

- Devices that are not under MDM software, such as for BYOD devices or contracted workers
- Devices that are being managed by MDM systems not under the organization's direct control, such as intra-agency apps in the public sector space, or visiting physicians from other healthcare systems
- Devices under the organization's MDM deployment, but have a need for additional security and management controls at the app level

[1] 451 Research IT Decision Maker Survey, December 2015

Why MDM is not mobile security on its own

MDM has grown in use because it gives IT the ability to provision and mandate device-level policies on multiple devices that are powered by Android, BlackBerry, iOS, and Windows-based operating systems. When it comes to securing apps and data, MDM falls short given its focus on the device.

The primary focus of MDM is to set up devices to be compliant with IT policies and in many cases this compliance means turning off features, removing app stores, enforcing the use of specific browsers, and using onerous pin/passwords to access the entire device. This is something to avoid in any mobile strategy because in order for them to be effective, security and usability must be balanced.

For many security strategies, the goal is to identify and reduce the number of potential attack vectors. Additional layers of security reduce the surface area that IT needs to be concerned about. MDM is one layer (the device layer) and should not be seen as a standalone cure for mobile security. To be effective, MDM needs to be paired with standalone MAM, that is able to provide secure app lifecycle management. In other words, securing apps from development through to deployment provides a separate layer of security beyond device-level controls.

A big draw for MDM is it's ability to wipe a device should it be lost, stolen, or the user leaves the organization. As a mobile strategy best practice, IT should avoid wiping the entire device and instead perform a targeted wipe of corporate data. This is a more palatable option, particularly in the case of employees leaving an organization.

In the following table MDM and MAM policies and their relative security value are compared:

MDM policy	Security value	Can this be done with MAM?	MAM alternative approach	Security value
Device-level policies	**Medium**	Yes	**App-level security policies**	**High**
Require encryption of device	**Medium**	No	**Encrypt only corporate apps**	**High**
Remote wipe of entire device	**Low**	No	**Remote wipe of corporate data**	**High**
Remote wipe of corporate data	**High**	Yes		
VPN configuration	**Medium**	Yes	**App-level VPN — securing corporate data in motion**	**High**
Jail-break/root detection	**High**	Yes	**Check device status with corporate app start**	**High**
Disable native apps on device	**Low**	No	**Silo enterprise data with separate encryption library**	**High**
Inventory all apps installed on device	**Medium**	No	**Inventory and manage corporate apps installed on device**	**High**

Figure 2: Comparing MDM and MAM security approaches

Mobile app security & deployment to support highly secure settings

There is unquestionable value in enabling knowledge workers in highly secure settings with mobile apps and access to critical systems. Mobile devices are the platform of choice for users and their processing power is increasing and reliable network coverage is improving. Security requirements have historically been a limiting factor that has slowed innovations for front-line workers. However, advancements in mobile security and management techniques have made new kinds of apps and broad deployments within reach for most organizations – even those with the highest levels of security. As a result, more innovative apps are being created and deployed, making secure data collection, consumption, and collaboration a reality.

Mobile app security policies

Mobile app security refers to the enforcement of access and data protection measures for individual apps. This can be done by applying security policies during app development, later with software development kits (SDKs), or after the app is compiled with app wrapping. Only MAM can provide these capabilities with a security layer that protects a critical endpoint – corporate mobile apps and data. The following capabilities are critical for a secure enterprise mobile deployment, and cannot be delivered by MDM:

- **Single Sign-on (SSO) integration** — SSO that extends corporate authentication to mobile apps, and dynamically requires users to enter their corporate credentials before the app will open.
- **Data-at-Rest (DAR) encryption** — Allows data stored by the app to be encrypted separately from device-level encryption that is used by all apps on the device. The entire app and any local data (sandbox container) are encrypted with FIPS 140-2 encryption and Suite B algorithms, the strongest encryption used by the US government and approved for export.
- **App-level VPN** — Provides a secure connection from the app to your company gateway for both authentication and access to data behind the firewall without giving access to the entire device.
- **App expiration** — Allows an app to remain enabled for a predetermined amount of time and then disable it from being run.
- **Self-updating apps** — Checks for new versions of an app at run time and prompts the user to update that app ensuring 100% update compliance for a particular app version.
- **Mobile app analytics** — Understanding who is using apps, particularly on devices that are not under management, which is critical for security and app development teams.

It is important to note that only MAM can provide these security policies for mobile deployments that involve users outside of an organization — no device registration is required.

Identifying and authenticating users at the app level

After building, buying, or customizing a mobile app, the biggest challenge for IT is getting those apps into the hands of users. In most cases IT needs a mechanism to enable and promote new and updated apps. From a security perspective, it's not just about getting mobile apps into the hands of users, but getting them into the hands of the right users. A private enterprise app store is the ideal vehicle for this as it provides a critical authentication layer ensuring that only valid users are accessing your critical mobile apps. Additionally, app stores powered by advanced MAM platforms can push apps to specific employees, for example based on their role, as defined by IT. The ability to authenticate the user of a device is a critical security component of enterprise mobility management (EMM). This is best done by requiring a user to enter a pin or password to access a device, and allows IT to effectively restrict usage to appropriate users. In the world of mobility where consumer and enterprise apps sit side by side, a device-level password, such as a complex alpha-numeric password, can be seen as onerous by users. The addition of biometric passwords has sped up device-level authentication, but that level of authentication gives a user access to the entire device, and all apps on that device. In many cases, IT will want to provide an additional level of authentication for specific applications. With MAM, a separate encryption library for app-level encryption of data-at-rest within mobile apps can be provided.

MAM security policy	Security value	Can this be done with MDM?
Mobile app analytics	High	No
SSO for corporate apps	High	No
App-level data-at-rest (DAR) encryption	High	No
App-level VPN	High	No
Copy/paste protection	High	No
App expiration	High	No
Self-updating app	High	No
Secure apps for users outside organization	High	No

Figure 3: MAM Security Policies vs. MDM

Derived credentials

Derived credentials are the PIV credentials that are derived from government access cards and are stored as digital or soft tokens on users' mobile devices, allowing them to access critical apps and information.

When accessing an information system, a PIN code that unlocks the soft token is entered and that soft token verifies the user's identity. If the credentials are still valid, the system allows access. Alternatively, access is blocked if the user is unauthorized or has left the agency.

Authentication at the app layer ensures that the right users are accessing your enterprise mobile apps and services. For highly regulated environments, many companies turn to two-factor authentication by requiring a password, something you know, and then a token, something you have. This token can be physical or digital.

Government-grade security & derived credentials

The National Institute of Standards and Technology (NIST) provides guidelines for US government encryption and security standards. NIST requires that agencies use access cards (physical tokens) that have personal identity verification (PIV) credentials stored on them to access a secure building or information. Traditionally, card readers are used to verify the credentials. A card is held against a reader to verify the identity of the person entering a building, or it is plugged into the keyword to authenticate access to a computer.

This method works when the user is at a desk, but in a mobile environment it becomes much more difficult because there often isn't an available card reader, and credentials aren't readily verifiable. To overcome this, organizations have tried to use card readers that are plugged into mobile devices via a cable or Bluetooth, but often times that solution is neither practical nor reliable. This is where derived credentials come into play.

One approach to leveraging derived credentials as a mobile identity verification tool is by using a mobile application security and management platform that applies a dynamic security policy to individual apps. By focusing on the app layer, agencies can apply a number of security policies to individual apps to secure data-at-rest and data-in-motion, without requiring that the device itself is under management by the agency. A derived credentials policy could also be applied to specific apps that require a greater level of assurance that the person accessing these resources is actually who he or she claims to be.

Extending corporate identity to mobile users

To maintain a secure enterprise app store, organizations need to authenticate users before permitting access to the app store, and the many apps that are deployed from that app store. Creating a separate authentication process for mobile devices is unnecessary and cumbersome for users. However, providing a single identity for users across devices will be more palatable for users (only needing to remember one password), and easier to support from an IT perspective.

SSO leverages industry standards and existing organizational infrastructure to authenticate and authorize mobile users. This allows users to use their credentials to sign into a mobile app store. SSO offers multiple benefits including strengthened security, tighter integration, and easier user provisioning. With SSO, MAM vendors do not see or store users' login credentials; instead, MAM users authenticate with the same trusted authentication method used by their organization. SSO also improves the overall user experience. There is no additional login name and password for a user to remember — or forget.

Compliance does not equal security

Compliance is a key driver that security tools use in mobile deployments. Today, many organizations in regulated and unregulated environments are using device-level management tools as way to meet security requirements. These tools often fall short as their controls are too far from the point at which mobile apps connect to regulated data. Security practitioners should look to push encryption of data-at-rest and data-in-motion into an organization's apps. Those apps should be delivered in a private enterprise app store, avoiding the need to subject apps to inspection by third parties such as device or OS vendors.

Balancing usability with security

Unlike any other tool in the enterprise, mobile continues to be the most personal device that employees use to get work done. In many cases, employees use these devices to extend their work day. Putting unnecessary barriers in place to simply check security boxes but provide limited security value will reduce employee effectiveness. Pushing mobile security to the app layer, in a way that is transparent to the employee, and yet familiar in its approach to app distribution can help IT achieve the goal of protecting the organization, while at the same time making users more effective and increasing the return on their mobile investment.

Bottom line...

Today, organizations are investing in critical mobile apps that improve and transform how employees get work done, and in some cases, create a competitive advantage. Such apps access valuable corporate data, making the need for app-level security more critical than ever before. Using device-level management tools to secure mobile apps creates a security gap that can be closed by implementing a mobile app management strategy. By doing so you will be able to apply fine-grained security policies to individual apps, gain insight into the usage of those apps, and ensure compliance among end users, all while driving a familiar consumer-like end-user experience.

About Digital.ai

Digital.ai enables enterprises to focus on outcomes instead of outputs, create greater business value faster, and deliver secure digital experiences their customers trust. The Digital.ai Value Stream Platform seamlessly integrates all the disparate tools and processes across the various value streams, uses data and AI/ML to create connective tissue between them, and provides the real-time, contextual insights required to drive and sustain successful digital transformation. With Digital.ai, enterprises have the visibility they've been seeking to deliver value, drive growth, increase profitability, reduce security risk, and improve customer experience.

Learn more at **Digital.ai**