MICRO FOCUS

Flash Point Paper

Security

MAM: The Key to Balancing Mobile Security and Usability

The main focus behind mobile application management (MAM) solutions is to solve problems arising from ever-expanding bring your own device (BYOD) scenarios. MAM helps secure corporate assets while minimizing the impacts necessary controls have on mobile users' productivity and experiences.

What is MAM?

To understand what MAM solutions are and what they do, it's helpful to discuss what they aren't and don't do. MAM solutions are not mobile device management (MDM) solutions. To protect corporate data that resides on and flows in and out of users' mobile devices, MDM gives the organization complete control over those devices, including how the user authenticates and the ability to wipe all business and personal data at the slightest hint of a device being lost or stolen. MAM takes a more user-friendly approach to protecting that corporate data.

Rather than enforcing security controls at the device level, MAM typically enforces controls at the application level. While implementation varies among vendors, MAM solutions create a separation between the personal assets and the corporate assets that reside on the mobile device. This allows organizations to implement security controls and rules that govern access and usage of the device's corporate apps and data in a way that doesn't interfere with user's normal use of the device or put their personal files, music, photos, and videos at risk of ever being wiped by corporate. In other words, the user maintains control of their device and stuff, while allowing the organization to control and secure its stuff.

One of the predominant and most effective methods that MAM solutions use to create the necessary separation between personal assets and the corporate assets on mobile devices is to use containerization, also known as application sandboxing. In this type of implementation, the MAM solution creates a secure portion of the device's storage—the secure container—that is separate from the rest of the device's storage. Inside the secure container is where corporate applications execute and corporate data resides. This keeps personal and corporate apps and data from mingling, prevents malware and intruders from accessing corporate resources, and protects sensitive corporate data from accidental or intentional exposure.

What to Look for in a MAM Solution

- *Enables mobile productivity with full respect to user privacy and device freedom*
- *Offers out-of-the-box integration with company infrastructure and systems*
- *Simple to manage*
- *Compatible with enterprise mobility management*

MAM solutions create a separation between mobile users' personal assets and the organization's assets to allow users to control their personal mobile usage, while allowing the organization to control and secure corporate usage.

Contact us at:
www.microfocus.com

Why Use MAM?

Minimal User Impact

One of the most appealing aspects of MAM is the low impact it has on mobile workers. Not only does MAM allow workers to productively use their personal mobile device for business purposes, but it allows them to continue to use their device the way they please. To get to their personal stuff, they can authenticate the way they've always authenticated. To get to the MAM secure container where the business apps and data reside, they authenticate however the business prescribes. And if they make a mistake authenticating, they don't ever have to worry about their personal stuff being wiped off the device. If a wipe occurs, it only wipes the contents of the MAM container.

Additionally, with MAM your mobile workforce doesn't have to worry about restrictive policies that affect their personal use of the device, such as expiring passwords, limited or no camera use, disabled voice commands, social media blocking, inability to copy and paste email contacts, and more. These types of policies might make sense for corporate-owned devices, but enforcing them on workers using their personally owned mobile devices and personal apps can disrupt their way of life and incite resistance against corporate security policies.

User Mistrust

Whether it's warranted or not, some users don't like the unfettered access and control over their personal mobile devices that MDM might seem to give an organization. Will IT be viewing my personal files and photos? Will they be tracking and monitoring my location wherever I go? Even if the organization has no intention of tracking its workers' location, some simply feel uncomfortable that the organization has that ability if they choose to. There are also more likely concerns too, such as what if IT locks me out of my device if I quit working for the organization or I authenticate incorrectly? Or worse, what if they wipe my device unintentionally or intentionally for whatever reason they choose. The issue of trust depends largely on the culture and atmosphere that is fostered within the organization, but even in organizations with positive climates and healthy business-to-worker relationships, user mistrust can still be a concern. MAM solutions can help alleviate these concerns since they do not give the organization device control. Rather, access and control are limited to business apps and data.

Corporate Security and Data Privacy

While MAM gives mobile users the freedom to use their personal devices the way they choose, MAM also gives organizations the controls they need to secure corporate assets and resources. While specific controls and details will vary among different solutions, some capabilities to look for include the following:

- Secure encrypted container/workspace for isolation of corporate apps and data
- Secure built-in corporate network access or browsing that eliminates the need for a VPN
- Secure camera for business related photos
- Secure email, calendar, and contacts
- Corporate app portal/store for access to secure corporate apps
- Centralized container/workspace management policies and controls

Putting MAM to Work

ZENworks® Mobile Workspace from Micro Focus® gives you a MAM solution that focuses on empowering you to secure and control your corporate assets, while keeping your mobile workforce happy and productive. It ensures personal and corporate workspaces on mobile devices stay separate, allowing users to retain control of their personal mobile use and files, as well as enabling you to control corporate mobile use and resources. For more information on ZENworks Mobile Workspace, as well as other mobile management offerings from Micro Focus, contact your local sales representative or visit **www.microfocus.com/products/zenworks/mobile-workspace/**.