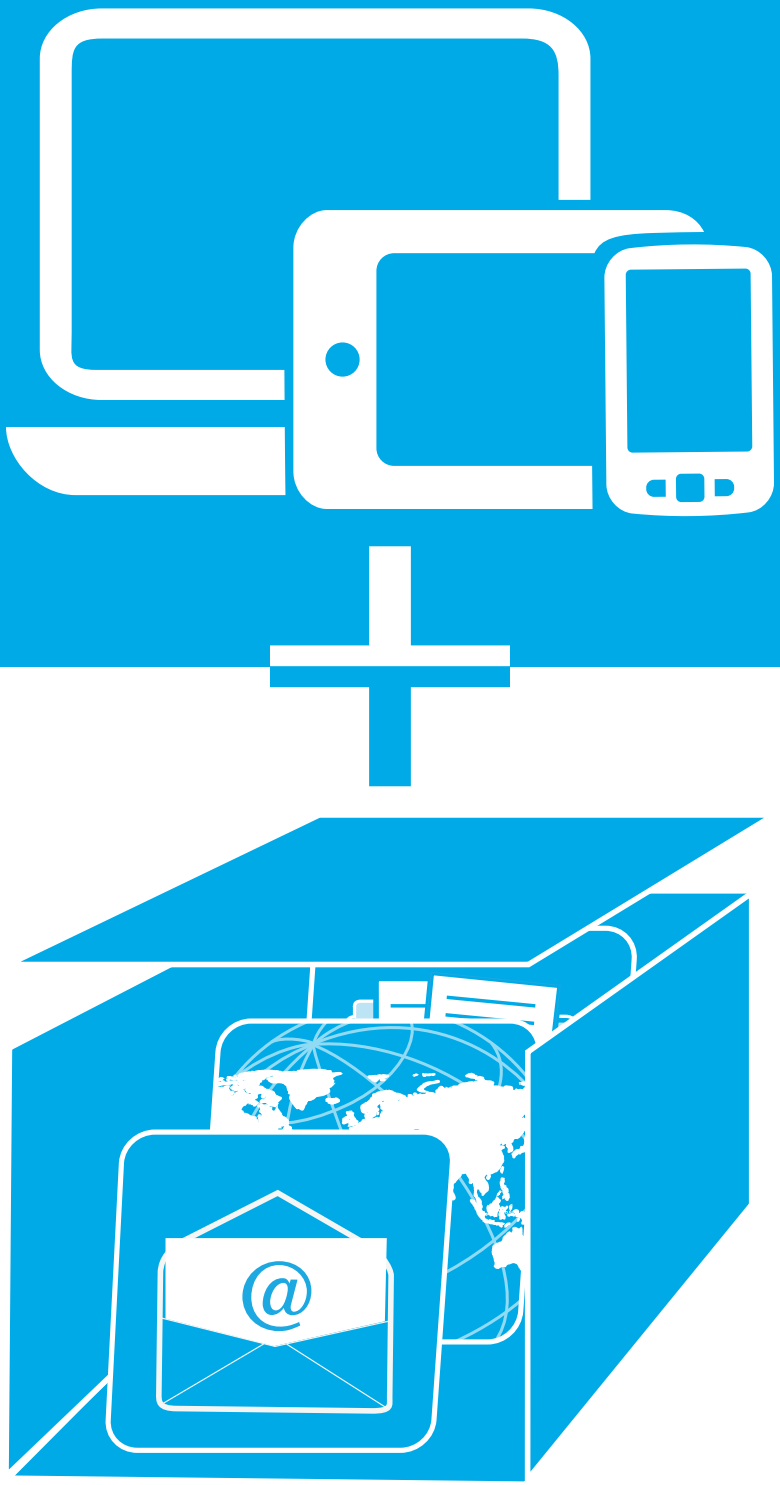
Enterprise Mobility Best Practices: MDM, Containerization or Both?



airwatch®
We Simplify Enterprise Mobility™

Enterprise Mobility Best Practices: MDM, Containerization or Both?

Less than a year ago, analysts' predictions had mobility enthusiasts believing doomsday was approaching for the mobile device management (MDM) industry. At the 2013 Gartner Security and Risk Management Summit, a panel of analysts told attendees that the bring your own device (BYOD) phenomenon would lead to slashed prices, plummeting sales and the death of an industry. "Mobile device management is in chaos right now, and I think this market is going to die," Gartner analyst John Girard told attendees (**as reported by CRN.com**). Girard predicted a shift toward application-level management necessitated by the BYOD trend and employee resistance to management of personal devices.

In the same panel session, Gartner fellow Neil MacDonald said that the sharpest MDM vendors "know the end is in sight, and they are building containers. They're building out a mobile application management solution to start going down that path." The analysts predicted a paradigm shift, in which CIOs and mobility experts would drop device-level management entirely, instead choosing more granular management of data and applications through an encrypted corporate container. Enterprise mobility, they predicted, would focus on managing the data, not the device.

Today, the market tells a slightly different story. MDM is still the preferred method for BYOD security, according to a **Technavio report**. As application-level management through containerization has continued to grow in popularity, MDM has kept pace. Rather than replacing one with the other, companies have realized that both MDM and application-level management are still relevant for different device deployments, and in some cases, provide additional functionality and security if they coexist together on the same device.

Instead of having the MDM vs. containerization debate, enterprises should define device use cases and security requirements within the organization, and then decide which solutions best suit their needs. Organizations with all kinds of deployments – corporate-owned devices, BYOD or a combination of the two – are finding that MDM and containerization together provide flexibility, user enablement and enhanced security. Many organizations are choosing to deploy MDM and containerization together on the same devices, for a layered approach to security. Below, we'll discuss common enterprise use cases and define the advantages of MDM, containerization and the layered approach to security that both can provide.

MDM

MDM enables mobile security at the most foundational level: the device itself. With MDM, IT has the ability to configure advanced device management and monitoring settings through profiles, which can be applied based on operating system or device ownership type, enabling enterprises to take more control of corporate deployed devices. MDM protects data stored on the device or in applications at the device level by prohibiting unauthorized actions, such as attempts to root or jailbreak the device, download malicious applications or install malware. With **AirWatch® Mobile Device Management**, enterprises can perform device-level actions such as:

- Enforce data encryption
- Require a device passcode
- Remotely reset the passcode
- Remotely lock the device
- Enforce device restrictions
- Track the device's location
- Set roaming restrictions to reduce telecom costs
- Perform an enterprise or device-level wipe
- Send push notifications

Once a device is enrolled in AirWatch Mobile Device Management, profiles that have been pre-set by the administrator based on device type, ownership model or organization group automatically begin downloading. Administrators create profiles from the AirWatch console that push enterprise applications, enable monitoring and enforce automated compliance through the AirWatch compliance engine. If an end user downloads an application that the administrator has blacklisted, AirWatch can automatically send a notification prompting the user to remove the application. If the application has not been removed after a pre-set period of time, administrators can set escalating actions that will automatically restrict access to resources such as enterprise content or email until the application is removed. Administrators can also set restrictions to device features and native applications.

Administrators can also limit the time a device remains unlocked without requiring the end-user to re-enter the passcode, or remotely lock a device that has been lost or stolen. Administrators can apply profiles that limit the number of incorrect passcode attempts. After the pre-determined limit has been reached, a pre-set profile can reset the password or perform an enterprise wipe. Some operating systems offer advanced kiosk modes, silent installation and removal of applications or even remote control.

AirWatch integrates with existing directory services, such as Active Directory and LDAP. Administrators can import existing directory structure to ensure users receive the appropriate access based on organization group, and users can enroll in AirWatch using their existing corporate credentials.

Devices in an enterprise deployment can be given different management profiles and access to corporate resources based on job title, region, device ownership and other factors. All devices in an enterprise deployment can be monitored through a single web-based administrative console, regardless of management settings, device type, organization group, language, location or ownership model.

MDM provides some unique benefits over other management models. AirWatch Mobile Device Management enables employees to automatically connect to corporate Wi-Fi and enterprise VPN networks without user interaction. AirWatch allows administrators to configure Wi-Fi and VPN profiles to download automatically or on demand to user devices. Profiles can be assigned based on user group, location within a defined geofence or time of day. For example, if employees should only be accessing Wi-Fi or virtual private networks (VPN) during defined business hours, AirWatch enables IT administrators to set that restriction.

AirWatch also provides the ability to provision a VPN profile to devices to automatically configure access to corporate networks and file systems. The advanced VPN On Demand capability allows mobile users to securely access specific websites through a VPN tunnel. This process is invisible and seamless to the user, allowing them to continue working without interruptions. App-level VPN capabilities for Apple iOS devices now also enable administrators to connect single apps to the VPN.

MDM Use Cases: Corporate-owned

The device-level approach is a no-brainer for organizations that distribute devices to employees. Managing the whole device enables organizations to track and maintain a real-time inventory of their assets. Because corporate-owned devices are usually dedicated to only corporate use, most enterprises choose MDM for its added device-level controls, such as device and enterprise wipe, remote passcode lock, and the ability to monitor a fleet of devices in real time.

MDM also offers organizations the ability to limit telecom expenses. AirWatch enables companies to reduce wireless expenses through real-time data monitoring. Administrators can set a profile that automatically disables the ability to use data or make calls when a device is roaming.

MDM Use Cases: BYOD

However, there is a perception in the market that MDM can be too heavy-handed an approach for devices that employees own and use to access corporate content. Both Apple and Windows platforms are built to accept device-level management, while keeping ultimate control in the users' hands. Under settings, users can see all profiles that are installed on the device, so the end user can view what profiles IT has installed on their device. Neither Apple iOS nor Windows platforms allow access to the content of text messages, phone calls or personal email. Administrators cannot read, listen to or record any conversations that take place on the device. The more open Android platform does allow additional MDM controls, so many organizations choose to provide the containerization option on employee-owned Android devices.

Many users do not want to give IT the ability to remotely wipe their device because they are afraid of losing valuable personal content. AirWatch provides a remote enterprise wipe option, which enables IT to wipe only enterprise content from the device while leaving personal content untouched. To ensure peace of mind, many organizations will choose to deploy enterprise content in a separate corporate container on managed devices so there is a clearly defined managed space on employee-owned devices. It is ultimately up to the organization to create a BYOD policy that clearly defines what data the organization collects and monitors. AirWatch recommends BYOD policies that prohibit IT access to personal content. AirWatch also provides organizations with a set of privacy policies, which can be customized for employee-owned devices.

Containerization

Containerization offers organizations the ability to securely deploy and manage corporate content in an encrypted space on the device. All corporate resources, including proprietary applications and corporate email, calendar and contacts reside within this managed space. The password protected container gives users access to all corporate applications through single sign on (SSO), providing a convenient way for users to access the managed space. The containerization approach allows IT to not only secure corporate data on a device, but also control which apps can access data and how that data is shared. If the data is compromised, the entire container or a specific application can be removed remotely.

Deploying managed applications outside of an encrypted container opens the data housed within the apps to vulnerabilities because IT cannot control how those applications communicate with other, unmanaged applications on the device. For example, a secure file sharing app may require a partner application to perform actions such as editing and annotating. If the apps are used together to edit a file, data may be copied from the secure file sharing app to the public cloud of the editing app, thereby leaving IT's control.

AirWatch® Secure Content Locker™ is a secure file sharing container with built-in editing and annotating capabilities, so users can perform these actions without data ever leaving the app. AirWatch® Inbox is a secure email container that enables organizations to separate users' corporate email into an encrypted, managed container. Hyperlinks in files or emails can be restricted to opening in the secure **AirWatch® Browser**. All apps can be housed in the **AirWatch® Workspace** to enable single sign on. Using **AirWatch® Application Management** solutions such as the AirWatch® Software Development Kit or AirWatch® App Wrapping enables an organization's internal applications to function securely within AirWatch Workspace.

AirWatch Workspace, available for iOS and Android, is a container that can house all enterprise apps on a device, enabling secure access to corporate data – including email, applications and content, a secure browser and custom applications. Housing applications such as AirWatch Inbox, Secure Content Locker or other enterprise apps in AirWatch Workspace limits those applications to sharing data only with other secure, managed applications. All applications inside the container can be accessed via single sign on.

Use Cases: BYOD

Containerization is commonly referenced as a solution for employee-owned devices. Because it offers a managed space on the device, employees who want to use their own devices to access corporate content are generally more confident that their privacy will be respected, whether they are enrolled in MDM or not.

Use Cases: Collaboration in the Extended Enterprise

Containerization also provides a way to share content and applications securely in the extended enterprise to end users who are not enrolled in MDM. Administrators can deploy a secure container to consultants, contractors, vendors, business partners, board members and other collaborators without managing their devices.

AirWatch Workspace can be custom-branded, so users can share documents and data with members of the extended enterprise in a container that is consistent with their corporate identity, rather than one that looks like a third-party application. By wrapping all enterprise apps and data in AirWatch Workspace, AirWatch enables administrators with added control and heightened security for enterprise data on unmanaged devices. With AirWatch Workspace, corporate data will never leave an organization's managed network environment, even when it is shared with collaborators in the extended enterprise. Should an unmanaged device housing corporate data become compromised, AirWatch Workspace enables administrators to perform

an enterprise wipe and remove all corporate data with a single action, while leaving personal data intact.

A Layered Approach: MDM + Containerization

As more business processes are extended to mobile, many organizations are finding uses for both MDM and containerization, either for different device deployments or on the same device.

Different Device Deployments

Administrators in large organizations with both corporate-owned and BYOD deployments may want to consider MDM for corporate-owned devices and containerization for BYOD devices and other use cases that do not require device management, such as collaboration in the extended enterprise.

MDM and Containerization Deployed on the Same Device

Organizations with highly sensitive proprietary content or in strictly regulated industries may prefer the added security that MDM and containerization on the same device provides. A corporate container deployed on a managed device provides an extra barrier to access corporate content. Users are required to enter both a device-level passcode and a container-level passcode, and administrators have both device-level controls and application-level controls that enable app-to-app collaboration with other managed and secure applications within the container. For example, a link sent in a secure email can be opened in the secure AirWatch Browser, and a sensitive attachment can be opened and edited in Secure Content Locker.

MDM and containerization are often thought of as mutually exclusive security solutions, but today's most innovative organizations are taking a layered approach to security by using the two in conjunction. Within an enterprise, IT can choose to adopt a hybrid model with several different management approaches. This may be necessary if some devices in your organization are corporate-owned devices, while others are employee-owned devices. For enterprises that have both BYOD and corporate-owned devices, administrators can still effectively monitor and manage devices that are secured through MDM, containerization or with both together in a single, integrated platform.

A Complete, Integrated Platform for Mobile

Each solution in the AirWatch® Enterprise Mobility Management Platform has been built from the ground up, with the same security framework at the core. The administrative console enables a bird's-eye view of all devices in a deployment. Whether devices are managed through MDM or containerization, IT administrators can manage the entire deployment through a single pane of glass from AirWatch's web-based console. Making it simple to manage and enable devices across the enterprise is what AirWatch is known for. A single platform for all mobile needs means simplified management, and simpler management means IT administrators are more likely to catch potential security breaches before they become major issues.

Business use of mobile devices is becoming more strategic and use cases are getting more complex. Enterprises are continually adding users and deploying content and applications in the extended enterprise. If an organization truly wants to scale, it is imperative to find an enterprise mobility management solution that was built using the same architecture on a single platform. AirWatch offers an integrated mobile platform for managing content and collaboration, as well as securing applications, browsing and email in

the extended enterprise. AirWatch also leverages organizations' existing infrastructure to enable access to corporate resources. AirWatch ensures the value of IT investments in VPN, Wi-Fi security, SharePoint and other content repositories, as well as enterprise resource planning (ERP) and customer relationship management (CRM) systems. By extending these resources to mobile, AirWatch both extends security and enables employee productivity through mobility.

When selecting an enterprise mobility platform, organizations should not only look at current mobile needs but also consider an extended roadmap that includes any future plans to develop apps, extend more business processes to mobile or expand collaboration with the extended enterprise. To prepare for a mobile-centric world, organizations today need a platform that is flexible, that scales, and that they can grow into as opposed to growing out of.

Whether enterprises choose MDM, containerization or a layered approach, AirWatch has created a platform that allows both enablement of business processes and the security that IT departments require, with a friendly user interface, deep enterprise integration and the flexibility to collaborate and grow.

Additional Resources

For additional information, visit:
www.air-watch.com/industries/solutions/mobile-device-management
www.air-watch.com/solutions/containerization

To get started with a free trial of AirWatch, visit **www.air-watch.com/free-trial**.

AirWatch Global Headquarters

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch

AirWatch is the largest Enterprise Mobility Management provider in the world with over 1,600 employees globally. More than 10,500 companies trust AirWatch to secure and manage their mobile enterprise. With market-leading solutions for mobile security, device, email, application, content and browsing management, we simplify enterprise mobility.