MobileIron

Data Sheet

AppConnect and AppTunnel: Securing the Enterprise App Persona

Challenge

Prevent data loss as mobile apps become business-critical and widely adopted

Solution

A secure enterprise app persona thru:

- MobileIron AppConnect
- MobileIron AppTunnel

Benefits

- Secure the mobile app lifecycle while preserving user experience
- Protect app data-at-rest without touching personal data
- Protect app data-in-motion end-to-end
- Protect privacy thru data separation, especially for BYOD settings
- Configure apps silently and update policies dynamically without user action
- Support both SDK and wrapping methods for app containerization
- Support both iOS and Android
- Support both internal and 3rd party apps

Recent Recognition

Gartner: MobileIron positioned in the Leaders Quadrant of the Magic Quadrant for Mobile Device Management Software (May 2012)

Info-Tech: MobileIron listed as a Champion in the Mobile Device Management Suites Vendor Landscape (Aug 2012)

IDC: MobileIron named fastest-growing mobile enterprise management vendor in the world (Sept 2012)

Contact

MobileIron
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com
www.mobileiron.com

Mobile apps are transforming business. App developers must deliver great apps quickly, but many of the apps they build will include sensitive data and run on employee-owned devices. Business and personal data must be separated, and Mobile IT has to protect the business data while preserving the user experience.

Establishing the Enterprise App Persona

An enterprise app persona includes all the business apps and data on a mobile device. It is tied to a specific user, based on that user's identity, and it is managed through policy. A complete approach to enterprise app persona includes:

- Multi-OS methods to containerize app data
- Security of data-at-rest and data-in-motion for internal and third-party apps
- Protection of user privacy and native user experience

A "container" is set of data protected from unauthorized access. In the first generation of mobility, business data was in heavyweight, email-based containers that were secure but forced users into an experience they did not like. However, in the new generation of mobility, user experience is central to success and requires:

- For end user: Security must be invisible. The mobile experience must be integrated. Privacy must be preserved, especially on personally-owned devices.
- For Mobile IT: Business data must be protected. Device support must be broad. Helpdesk impact must be minimal. The business must be enabled quickly.

Securing the Persona through Connected Containers

The MobileIron ***connected container*** architecture provides fine-grained security that protects app data for Mobile IT but is invisible to the user. It has two components:

1. **MobileIron AppConnect:** MobileIron AppConnect containerizes apps to protect data-at-rest without touching personal data. Each app becomes a secure container whose data is encrypted, protected from unauthorized access, and removable. Because each user has multiple business apps, each app container is also connected to other secure app containers. This allows the sharing of policies, like app single sign-on, and the sharing of data, like documents. All app containers are connected to MobileIron for policy management.
2. **MobileIron AppTunnel**: MobileIron AppTunnel provides secure tunneling and access control to protect app data-in-motion. Fine-grained app-by-app session security protects the connection of each app container to the corporate network. It builds upon the proven MobileIron Sentry technology, which is installed at thousands of customers. MobileIron also supports 3rd party VPN, but AppTunnel is particularly useful in BYOD settings where organizations may not want to open up VPN access to all apps on the device.

AppConnect

MobileIron AppConnect creates a secure app container through the use of either an SDK or wrapper for iOS and a wrapper for Android. Fine-grained policy can be applied app-by-app or shared across containers, and includes:

- **Authentication**: Confirm identity through domain username and password or certificates so only approved users can access business apps
- **Single sign-on:** Enforce time-based app-level sign-on across app containers
- **Authorization:** Allow or block app usage or storage based on device posture
- **Configuration:** Silently configure personalized settings such as user name, server address, and custom attributes without requiring user intervention
- **Encryption:** Ensure that all app data stored on the device is encrypted
- **DLP controls:** Set data loss prevention (DLP) policies, e.g., copy/paste, print, and open-in permissions, so sensitive data cannot leave the container
- **Dynamic policy:** Update app policies dynamically
- **Reporting:** Provide app usage statistics
- **Selective wipe:** Remotely wipe app data without touching personal data

AppTunnel

MobileIron AppTunnel provides tunneling and access control to protect app data-in-motion. AppTunnel provides several layers of security:

- **Unique connection**: Connect only authorized apps, users, and devices
- **Certificate-based session authentication**: Prevent man-in-the-middle attacks
- **Access control rules**: Block network access if device-side security compromised

About MobileIron

MobileIron has been chosen by thousands of organizations that are transforming their businesses through enterprise mobility. Available as an on-premise or a cloud solution, MobileIron was purpose-built to secure and manage mobile apps, documents, and devices for global companies. MobileIron has been chosen by 7 of the 10 top global pharmaceutical companies, 4 of the 5 top global automotive manufacturers, 3 of the top 5 global retailers, and half of the 10 top global law firms.

MobileIron AppConnect containerizes apps to protect app data-at-rest without touching personal data. MobileIron AppTunnel provides tunneling and access control to protect app data-in-motion.

Customer Perspective

Apps: "MobileIron has been a very strategic platform for us to support and manage our mobile devices and apps."
Life Technologies (Life Sciences)

BYOD: "MobileIron provides exactly the framework we needed to let our people use the device of their choice."
Thames River Capital (Financial Services)

Innovation: "MobileIron is helping us become a technology innovator."
Norton Rose (Legal)

Multi-OS: "We needed a truly multi-OS solution. MobileIron was without doubt the most comprehensive."
Colt Car Co. / Mitsubishi (Automotive)

Scale: "[MobileIron] did a great job not only helping us getting the product scaled, but also fixing any kind of issues."
Lexington School District (Education)

Security: "In our sector, the right mobile security solution is not a nice to have, it's mandatory."
National Health Service (Healthcare)

Support: "In this day and age of bad customer service, my experience with MobileIron has been consistently great."
City of North Vancouver (Government)

User experience: "MobileIron's strength is its ease of use for iPad owners."
KLA-Tencor (Technology)

Note: AppTunnel for Android is targeted for a future release. Some AppConnect and AppTunnel features may differ between operating systems.

Gartner, Inc., Magic Quadrant for Mobile Device Management Software, Phillip Redman, John Girard, Monica Basso, May 17, 2012. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Info-Tech Research Group, Inc., Vendor Landscape: Mobile Device Management Suites, August 2012. Info-Tech Research Group Vendor Landscape reports recognize outstanding vendors in the technology marketplace. Assessing vendors by the strength of their offering and their strategy for the enterprise, Info-Tech Research Group Vendor Landscapes pay tribute to the contribution of exceptional vendors in a particular category.