

MobileIron for Android





Roll out Android securely:

Track inventory of devices, apps

Block out-of-compliance devices from email access

Sliently enforce security policies

Selectively wipe enterprise data*

Protect against rogue apps

Secure with certificates*

Control roaming costs

Recent Recognition

Gartner: Positioned in Leaders Quadrant of the Magic Quadrant for Mobile Device Management Software 2012

IDC: New Paradigm for Mobile Device Management

"[MobileIron] was built from the ground up with the dynamics of today's mobility market in mind and therefore does not have legacy issues that others face in terms of re-architecting their solutions." — IDC

MobileIron, Inc.
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel +1.650.919.8100
Fax +1.650.919.8005
info@mobileiron.com
www.mobileiron.com

THE CHALLENGE: Users love the Android experience and want that same experience at work. IT departments must now provision, secure, and manage corporate- and employee-owned Android devices as they do other platforms.

THE SOLUTION: MobileIron enables organizations to deploy Android devices at scale by bridging the gap between the security and control IT needs and the experience endusers demand.

Manage at Scale



- · Provision at scale
- Know what's out there
- Configure and secure silently
- Block out-of-compliance devices

Secure Apps



- Track installed apps
- Protect against rogue apps
- Distribute in-house apps
- Recommend Google Play apps

Control Cost



- Monitor international roaming, with alerts
- Generate alerts
- User self-service
- Automated actions

The MobileIron platform includes a server that is up and running in your enterprise network in less than a day, plus a MobileIron Android app that is available for download on Google Play.

IT Management Features

Broad Device/Manufacturer Support

Android 2.2 - 4.0

Device Management

- Inventory & asset management
- Role-based access

Provisioning

- Exchange account settings*
- Wi-Fi settings
- VPN settings*

Access Control (Sentry)

- ActiveSync connection monitor
- Allow/Block actions by OS version or policy compliance

App Delivery Network (AppDN)

Deliver apps at scaleSecure, global network

• Passw

- Password and encryption policy
- Silent enforcement in the background
- Remote device lock, unlock, wipe
- · Root detection
- · Lost device location

Certificate Management

- Auto-enrollment & renewal*
- Certificate distribution for Exchange, VPN* and enterprise Wi-Fi (EAP-TLS)

Selective Wipe and Privacy

- Enterprise email/PIM*
- Enterprise configs (Wi-Fi, VPN*)
- Privacy policy

International Roaming Monitor

Lockdown

- Camera*
- Wi-Fi*Rhuotooth
- Bluetooth*

Monitoring and Reporting (Atlas)

- Delegated administration
- Security and policy compliance
- Application inventory

App Management

- Securely distribute, update, and control access of in-house apps
- Inventory of installed apps
- Recommendation of Google Play apps
- Rogue app protection
- Mandated presence of mission-critical apps

End-User Features (MyPhone@Work)

Self-service

- Enrollment of new devices
- Lost device location

App Discovery

- In-house apps with direct download
- Recommended apps with Google Play download

©2009-2012 MobileIron. All rights reserved. MobileIron, MyPhone@Work, and Connected Cloud are registered trademarks of MobileIron. All other product or company names may be trademarks and/or registered trademarks of their respective owners. While every effort is made to ensure the information given is accurate, MobileIron does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. 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.

^{*} May require NitroDesk TouchDown, Samsung S.A.F.E device, or Cisco AnyConnect