Android for Work Capabilities

Capability	Description
Silent Install	Using the EMM console, IT admins can silently install, remove, and update apps inside Android for Work. This capability greatly simplifies the user experience (and makes life easier for IT admins) because no user intervention is required to update or remove apps.
Application Configuration	Once applications are installed, they are configured on the device via setApplicationRestrictions. When developers create an app, they can specify which settings the app can accept. On the EMM console, the IT admin can configure the settings for a particular application. When Android for Work is configured, app settings are pushed to the device.
Secure App Installation from Google Play	Google has introduced a whole new set of Google Play APIs for EMM providers to enable app management and distribution. EMM providers are also the only mechanism for app deployment in Android for Work. As a result, apps cannot be side-loaded into the native client, which adds greater protection from malicious apps. This new process, combined with the Lollipop Android for Work Profile, enables IT managers to deploy any Play app in the Google Play Store to a secure Android container without any additional wrapping.
Separate Container for Work Apps	Android for Work simplifies mobile app management and security by providing a secure profile, or container, to Android devices running Android 4.0 and higher. Through an EMM vendor, IT admins can securely provision and containerize apps on any device with an Android for Work Profile (Android Lollipop), or the Android for Work app (Android 4.0 - 4.4).
Suite of Productivity Apps (email, calendar, etc.)	Android for Work features a suite of secure, badged PIM apps designed to help workers easily distinguish between personal and work apps on the device.
Data Loss Prevention	The ability for the user to share into and outside of Android for Work is managed by EMM governance policies. This includes the ability to block copy/paste or block screen capture for apps inside the managed profile. (Note that copy/paste can be disallowed from the managed profile to the personal profile, but not vice versa.)

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

Container VPN	Android for Work enables more granular VPN capabilities within the managed profile, which eliminates the need for a device-wide VPN. With these new capabilities, IT can maintain greater security and control over corporate app communication on the device
Selective Wipe	Android for Work enables IT administrators to easily retire lost or stolen devices and remotely wipe all work data while leaving personal content intact on the device. With corporate-owned devices, IT has total device-wide controls, which include a full device wipe if necessary.
Privacy for Self-hosted Apps	Organizations concerned about security for their private, in-house apps can choose to self-host these apps either internally or through their EMM provider. Either way, self-hosted apps can be excluded from public search results in the Google Play Store.
Protection Against Malicious App Downloads	Android for Work protects business apps and data from the user's personal activity outside the profile, such as side-loading web apps, ordering from unknown websites, and other potentially insecure activity.
Unified App Management Across Devices	Enterprise management is easier with a consistent, secure work container across different Android device manufacturers. Android for Work gives IT a unified way to secure enterprise apps, manage disparate devices, and enforce security policies on any device.
EMM Requirement	Successfully deploying Android for Work requires a multi-OS EMM platform