The Future Looks Bright for Android for Work
Since its inception, Android grew fast and by mid-2014, it had covered 80 percent of mobile phones in the market. Thereafter, its steady growth slowed due to the need for low-cost phones and the towering market share of Apple and Windows phones. Google addressed the former by launching $100 phones with AndroidOne. This move egged Android's growth to 88 percent. In order to increase its market share by garnering more users, Google has had to attract brand loyalists of its competitors with phones that have smarter features but are available at lower costs.

Abstract

Authors:
Krishna Kishore,
Senior Architect

Vidya Krithivasan,
Manager,
Portfolio and Pre-Sales,
Product Engineering Services
Table of Content

Introduction ............................................... 04
About the Authors ..................................... 08
About Sasken ............................................ 09
Introduction

With more than a billion Android smartphones in the world today, one of the major challenges organizations face is the lack of control over how much official data might be stored and used in the employees’ personal devices. Such data includes product images, demos, and whiteboard discussions captured using personal phones. The risk for organizations is that the official data gets automatically stored in the user’s personal cloud. Android for Work (AFW) is an elegant solution for organizations looking to protect their confidential data while providing the flexibility to employees to use their own devices.

Traditionally, enterprise users veered towards using Blackberry and Apple devices due to their advanced enterprise platforms supporting features such as:

- Keeping personal data separate from enterprise data
- Not providing system administrators access to their personal data
- Allowing system administrators to remotely:
  - Install applications
  - Wipe data
  - Configure enterprise user device and applications

- Restricting users to side load applications in enterprise profile
- Restricting users copying data from enterprise profile to personal profile

Figure 1: Personal devices used in an enterprise setup
As the number of Android users increased, it became more uncommon to see people using two phones – one for personal use and the other for business use. For a long time, Blackberry and Apple devices provided support for enterprise applications. On the other hand, Android devices were perceived as unsuitable for enterprise use due to the lack of security. Thus, Google started including AFW from its Lollipop version (5.0) and enhancing the features in each of the subsequent versions – Marshmallow and Nougat. Though there have been security features in Android even before Lollipop, AFW is based on managed profile and multi-user support. AFW uses multi-user framework where there is no need for users to switch users or login to toggle between work and personal applications tray as is the case in Apple and Blackberry devices. On the same launcher, work applications will appear with a badge on the icon and personal applications without a badge.

AFW is enabled through an ecosystem comprising of Google providing support in Android stack, companies like Google itself, Airwatch, Blackberry, Centrify, and IBM who are known as Enterprise Mobility Management (EMM) providers. In the Android stack, various components/interfaces/features such as SELinux, full device encryption, device policy manager, and device administration enable AFW feature. EMM provider has a support library called DPC (Device Policy Controller) that interacts with their respective components on the cloud and DPC App that can be directly used or enhanced based on needs of customer.

The Future Looks Bright for Android for Work

Figure 2: Android for Work Ecosystem
With AFW enabled devices, administrators can manage users and policies on registered devices through the EMM console. The console allows features such as:

- Add/remove/rename user
- Set password restrictions
- Chrome browser management to restrict accessible domains
- Wi-Fi, Ethernet, VPN settings
- Allow/Disallow external SD card, microphone, camera, speaker, factory reset

Though Google introduced enterprise features recently, it has brought in a lot of features that Apple and Blackberry enterprise solutions had for many years. Google acquired Divide in 2014 and included enterprise solution in Android. As of now, Google Android is predominantly catching up for enterprises with few differentiators. Some of the major features included by Google are:

Personal and Business Applications
On Android devices, enterprise applications are available with the ‘suitcase’ icon. If the same application needs to be used for personal as well as business purpose, there will be two icons on the launcher – one without the suitcase icon and one with it.

Apple does not have a specific separator between business and personal applications. They each have applications in a sandbox with provisions to restrict data access across containers. These applications are dependent on MDM APIs.

AFW uses containers built in Android. This enables Playstore applications to run in that container.

VPN Management
Android supports always-on VPN, per-user VPN, per-profile VPN, and per-application VPN. Other features include secure and silent installation of applications from server, device
and data encryption, wiping data remotely, and data leakage prevention by disabling copy-paste from work profile to personal profile.

While Google is going to introduce more features relevant for enterprises, Apple is trying to stay ahead by including features such as enterprise VoIP solution by partnering with Cisco. Google will also include such features and many more in future versions of Android.

Google has announced the inclusion of Rich Communication Suite (RCS) in Android. Though it will be starting with the messaging app, voice, video, screen/white board sharing will also be included.

From financial benefits perspective, G-Suite is competitive at 2.5 USD per user/device per month whereas other EMM providers offer at higher prices ranging from 4 USD. Without deploying solutions such as AFW, the risk of potential loss of official data is high which may have huge financial implications such as loss of business and customer confidential materials which may lead to penalties from customers. Additionally, in absence of such sophisticated infrastructure the manpower required to setup and manage employee devices manually will lead to higher costs.

Apart from the enterprise features supported by Apple, Blackberry and Google, enterprise mobile computers from companies such as Zebra, Honeywell, Datalogic, Bluebird also have features specific to enterprises. Google has included few features such as controlled installation/uninstallation of applications, blocking of applications from unknown sources, device-data-application security, and enforcing security policies which had been supported in enterprise mobile computers for many years. In future, Google may include features such as bar code scanning as well. Of course, these enterprise mobile computers may not want to have two profiles if they want to restrict usage of the devices to enterprise uses alone.

Sasken foresees the need to support its existing and prospective OEMs and retail customers in adapting AFW features for their needs. Sasken is preparing itself to extend this support to its customers by deploying AFW features among its employees and developing applications and policy manager/controller to interact with Google Apps for work (Google G-Suite) and enforce device policies set by the G-Suite administrator of Sasken. Sasken needs to help its customers in devising mechanisms through which customers’ legacy enterprise features and Google enterprise features co-exist till customers decide to move to Google enterprise features. It will be beneficial to customers to move to features supported by Google as innovation and maintenance for the software will be taken care of by Google.

The Future Looks Bright for Android for Work
About the Authors

Krishna Kishore
Kishore has over 18 years of experience in architecting, developing and delivering solutions in the domains of portable devices, consumer electronics, automotive, IoT and wearables. Kishore is always on track with emergence and advancements of technologies, assessing business prospects, conceiving solutions and authoring articles and papers for newspapers, magazines, and social media.

Vidya Krithivasan
Vidya’s experience spans more than a decade in embedded development across mobile and consumer devices market. She has contributed to the development and launch of some of the most successful smartphones in the industry. She is currently involved in creating innovative offerings and proposals with compelling case studies to showcase Sasken’s wide-ranging and unique embedded and digital expertise to its customers. A technology enthusiast, she is an avid follower of latest trends in mobile, digital, rugged, IoT and automotive industries and regularly shares her views in various internal and external forums via blogs, articles, tech talks and webinars.
About Sasken

Sasken is a specialist in Product Engineering and Digital Transformation providing concept-to-market, chip-to-cognition R&D services to global leaders in Semiconductor, Automotive, Industrials, Smart Devices & Wearables, Enterprise Grade Devices, Satcom, and Retail industries. With over 27 years in Product Engineering and Digital Transformation and 70 patents, Sasken has transformed the businesses of over a 100 Fortune 500 companies, powering over a billion devices through its services and IP.
The Future Looks Bright for Android for Work