Android is ready for the enterprise

Executive summary

Android powers a mobile, connected workforce, with multiple layers of security, comprehensive management, and a range of devices to fit any job. In recent years, the steadily growing popularity of Android with users has meant an influx of Android devices into the enterprise, creating opportunities for IT to devise a scalable plan to securely roll out these devices. In this whitepaper, MobileIron explores the state of Android security and management through the lens of how Google has systematically addressed concerns and inhibitors to Android adoption in the enterprise. Google's increased focus on security and flexibility, and the growing momentum towards Android enterprise - a newer and more effective Android management solution - means that Android is now here and ready for the enterprise. And, the powerful combination of Android with an Enterprise Mobility Management (EMM) platform that brings all of these new capabilities to life means that enterprises can now roll out Android devices at scale with confidence.

In this whitepaper we cover:

- Growing Android adoption in the enterprise
- Enhancements in security capabilities
- Reduced management fragmentation
- Strong separation of work/personal data for greater end-user privacy
- Drastically improved enrolment processes with reduced support burden

With these topics and more, read on to see why MobileIron believes Android is truly ready for the enterprise.

MobileIron

MKT EN-US v1.1

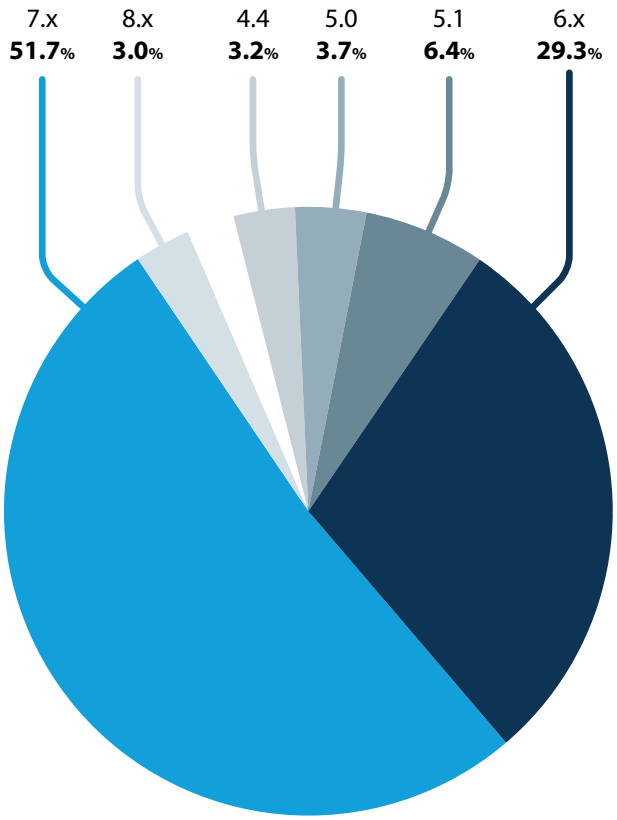
Introduction: The power of Android and EMM

The extreme consumer popularity of Android inevitably meant that many of those devices were soon headed into work. With this trend, Google made the strategic decision to bring focus to Android as an effective business device, making it easier for IT to manage and ensuring strong data security in a work environment. Looking back at the introduction of Android 5.0 Lollipop a few years ago, it marked a pivotal shift setting a new trend for every major Android version release since.

With over 77% of business device shipments in 2016 running Android (IDC, March 2017), organisations the world over were clearly starting to embrace Android for their business needs. As the adoption of Android has continued in the enterprise, many of the newer devices are flooding into work. According to Google, roughly 50% of Android devices in the enterprise are Android 6.0 or later. And our own MobileIron's aggregated customer data suggests that approximately 83% of organisations are using devices with Android versions 6.0 or later.[1] With the introduction of the newer, more expensive Android handsets in the workforce, there are more advanced security and management capabilities baked into the Android platform versus the older and cheaper offerings on the market.

In other words, with the three major Android releases behind us - Marshmallow, Nougat and Oreo - we see that Android is steadily aligned to meet the needs of the enterprise. However, despite improvements to Android, as recently as December 2017, only 35% of devices are under management (Google, December 2017). This means a much smaller subset of businesses have understood the power of an Enterprise Mobility Management (EMM) platform to secure their Android estates. It is worth noting that all of these new security and management capabilities in the Android platform can only be turned on with an EMM solution. And with the growth in potential data leakage, shadow IT, and increasing malware and vulnerability exploits, allowing employees to use their Android devices to access sensitive corporate data without the protection that EMM offers is a major gap that leaves organizations exposed. Enrolling an Android device with EMM ensures data security while making security invisible to the end user.

MobileIron managed Android version distribution, Jan 2018



1 Overall Android version stats, showing 50% are using Android 6.0 or later

Android evolution: Systematically addressing customer needs stronger security

A persistent and inaccurate perception overshadows Android in the enterprise today: Android is not secure. While that may have been a valid argument back during the time of Android 4.4 and below, Android has drastically improved security capabilities since then to now becoming one of the most secure OS platforms available when managed properly with an EMM solution.

In fact, Gartner rated Android higher for mobile device security controls than iOS in 2016 and 2017, as can be read in the Gartner Mobile OSs and Device Security: A Comparison of Platforms Report

Major version milestones

In version 5.0, Android introduced Android enterprise work profile and work-managed deployment types. The work profile is targeted at BYOD deployments where user privacy is respected. By contrast, work managed devices are corporate-liable deployments where the enterprise controls the entire device. These options give IT the full range of tools and options to manage Android deployments by segmented populations. In this same version also came the requirement for default, full-disk encryption.

In Android 6.0 came remote application permissions management, improved certificate management for password-free enrollment and integration and Android's COSU (Corporate Owned Single Use) Kiosk implementation. In other words, Android 6.0 expanded the possible deployment options (with COSU) and improved the security configurations allowing major use cases to be addressed securely on Android.

Later in 7.0 Android introduced authentication for the work profile, allowing administrators to enforce a separate work challenge before access to corporate applications could be granted. In addition, always-on VPN was introduced and Google further improved encryption to now use file-based rather than full-disk encryption as standard. File-based encryption meant that work data could be protected with a different set of keys than the device. With full-disk

encryption, once the device was unlocked, both personal and work data was left unencrypted. With file-based encryption, the work data now remains encrypted until the work challenge is used to unlock the enterprise profile. In other words, in 7.0 further protected corporate data security giving IT peace of mind.

Most recently in 8.0, Android introduced zero-touch enrollment which meant all Android devices were protected by enrolling with EMM. In addition, work profiles on fully managed devices offered organisations the ability to both manage the device and contain required applications in a separate profile. And finally, the parent (device) profile and the work profile now utilise unique encryption keys to further secure the data within.

Monthly security updates

Since Android 5.0 Google has distributed monthly security updates independent of the Android framework. Originally seen as difficult to implement by Android OEMs, today a significant number of them align closely to Google's standards and patch their devices on a monthly basis. This brings greater consistency and security to customers worldwide.

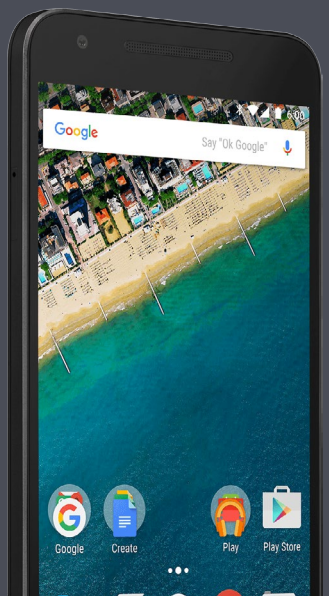
These security updates guarantee even devices still on older versions of Android today will be protected against threats discovered on a regular basis and Android's open-source nature means vulnerabilities can be quickly identified and resolved not only by Google, but any partner, OEM or the wider community and greatly contribute to the secure nature of Android today.

Mobile carriers and OEMs may impact the speed at which these security updates are applied. It is therefore a good practice to ensure that the devices bought into the business are those supporting the high standards required for enterprise adoption.

Google Play Protect

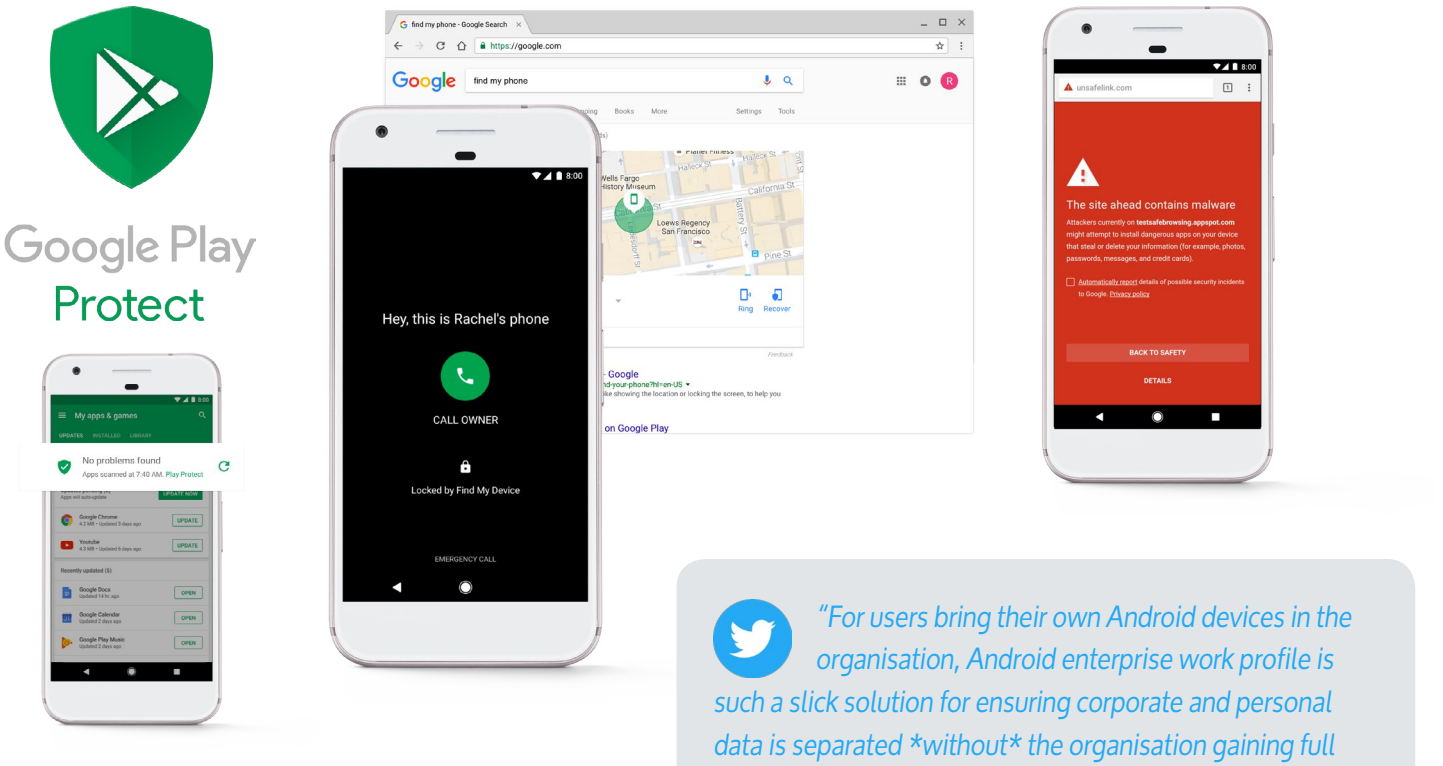
Google Play Protect, Google's suite of security tools used to safeguard users and devices from threats, scans over 50 billion applications both on and off the Play Store per day. It comes pre-installed on all Google Mobile Services (GMS) certified devices and scans for threats locally on the device day and night.

Play Protect also includes recognisable features such as Find My Device and Google Chrome Safe Browsing Protection. With it monitoring both devices and the Play Store, administrators can rest assured devices are protected.



GMS certification

A GMS certified device is one that has passed the certification process Google requires of OEMs in return for being permitted to pre-install Google's suite of applications such as the Play Store, Gmail and Chrome.



> *"For users bring their own Android devices in the organisation, Android enterprise work profile is such a slick solution for ensuring corporate and personal data is separated *without* the organisation gaining full control over the device."*
>
> @Jason Bayton, Jason Bayton

What Play Protect doesn't do is prevent the installation of unknown sources, arguably one of the biggest threats to Android devices today as it allows the installation of Android application files (APKs) sourced from outside of the Google Play Store. However, unknown sources is in fact disabled by default for Android enterprise devices and is fully controllable through the EMM independently of the deployment types chosen.

With unknown sources disabled the malware infection rate reported recently by Nokia for Android globally drops from 68% to 0.05% (Source: Nokia). Should rogue applications find their way onto devices, the amount of potential damage is minimised by the secure manner in which they're installed. Applications are sandboxed, which creates separation from other applications. And, in conjunction with the Android enterprise work profile, apps can run within uniquely encrypted profiles with data stored at rest completely inaccessible from outside the profile, unless permissions have been granted.

Separating personal and corporate data

With a Device Administrator enrollment the organization fully owns the device it manages regardless of it is a BYOD or COBO (Corporate Owned, Business Only device). And, whether corporate applications are containerised or integrated, EMM admins can enforce policies, configurations, view details of applications installed and optionally fully wipe a device at will because full administrator privileges over a device are required in order to manage it adequately. This can naturally be a concern for BYOD users potentially having to forego privacy to use their own devices.

However, with Android enterprise work profile, the control and visibility that an organization has is considerably lessened to only a secure dedicated work environment on the device. While the initial

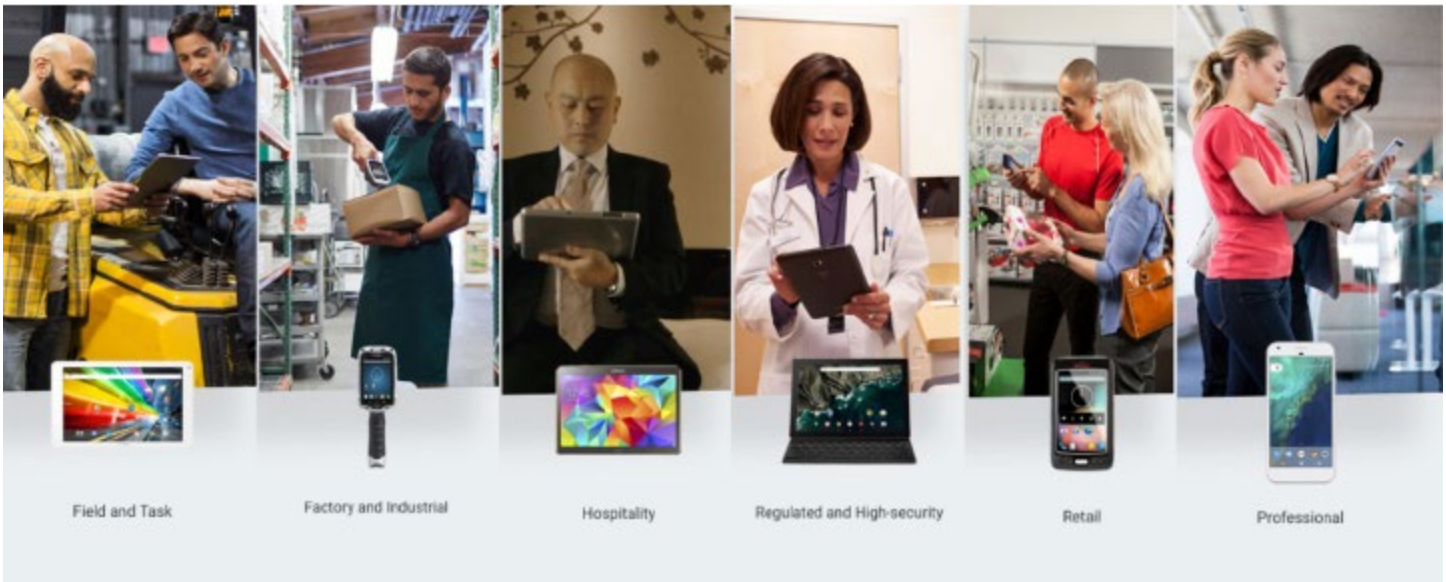
process is somewhat similar in that a corporate user will download the EMM agent from the Play Store, as soon as the corporate user authenticates, the EMM solution will create a second encrypted work profile, like a container, on the device and transition the EMM agent from the device to the new profile before enrollment completes.

This means once enrolled, administrators can only see and manage applications and settings within the work profile and not on the device itself. There are some exclusions to this, like being able to enforce a device-wide passcode or detect a compromised device, however user privacy and control are fully respected and enforced.

On the apps themselves, any applications the organization pushes out will show up on the device as any other application would on the home screen or in the app drawer, but will be marked with a work badge. If an app already exists on the device, a second work copy will be created and badged, indicating the application has access to corporate content and can store information separately from the personal side.

And when it's time to clock off users can disable the work profile with a simple toggle in quick settings when swiping down from the top of the screen. The work applications will grey out and all sync of emails and other corporate data will pause, thus empowering a work/life balance and assisting, along with MobileIron's work schedule feature, in the enforcement of local work laws for countries such as France and Germany.

Work profile additionally provides necessary control over corporate data with granular data loss protection (DLP) settings, offering the ability to limit sharing between the work profile and the device, including contacts and data, to ensure nothing can enter or leave the work profile without explicit consent.



Reduced fragmentation, greater consistency

Most organizations managing Android today will surely have a range of devices from various OEMs. And many of these OEMs may have slightly different implementations on Android in terms of how certain capabilities are executed. For example, the Device Administrator management model relies upon the OEM to incorporate management APIs in their Android images. Some OEMs have invested in this, while others have not. The autonomy of OEMs had led to to a lot of fragmentation in the Android world over time - not just the Android version fragmentation that is often talked about, but management fragmentation as well.

Organizations purchasing multiple devices from various OEMs have found themselves with no clear, consistent management experience in terms of being sure that what could be managed on one device could also be replicated on another type of Android device. This extended to OEM stock applications as well. For example, while email may be remotely configurable on one type of OEM Android device, it might not be possible on a different OEM, and so on. Seasoned EMM administrators may remember the days of selecting Android devices based on their management capabilities. If an organization bought a selection of devices from various OEMs it was almost guaranteed functionality on one device wasn't supported on another. To some extent this also happened between devices built by the same OEM! Ultimately this led to a lot of frustration, with organizations increasingly favoring other mobile devices for their consistent and reliable management capabilities.

When Android enterprise launched as Android for Work in 2014, Google set out to tackle what was clearly a disparate market and take the onus for enterprise support, for the most part, away from OEMs. This guaranteed a stable, reliable and replicable management experience no matter what devices an organization opted for. As Android has continued to mature, so too has the Android enterprise solution set, to the point where Google has confidently announced the deprecation of specific Device Administrator APIs in favour of Android enterprise.

Google isn't exercising full control over Android enterprise APIs however. With Zebra having already integrated their own APIs and Samsung following close behind, Google still empowers OEMs to add their own value-add over and above the base Google provides, enabling solutions like Knox Mobile Enrollment to live on when certain Device Admin APIs are no more.

What this all comes down to is an experience for administrators and end-users alike that will feel familiar across a broad range of OEMs; these devices may look and feel different, but the processes for managing devices are identical whether you pick up a Huawei or a Pixel.

OEMs taking enterprise seriously

More and more OEMs supporting Android are focused on meeting enterprise needs. Numerous OEMs, including those listed in the Google's"Android Enterprise Recommended" list are now committing to 3 years of patches. One example is Samsung releasing the Note 8 for enterprise towards the end of 2017. With this device, they have committed to supporting the device for 3 years of software and security patches, while making the device hardware available for 2 years which is far longer than normal consumer hardware.

With this enterprise-friendly approach to hardware availability and software maintenance, various OEMs are demonstrating their ability to align far more closely with the typical hardware lifecycle many organizations adopt. This offers a better solution to the age-old consumer/enterprise divide.

Android Enterprise Recommended

Refers to a list of recommended devices that meet minimum specifications for hardware, bulk enrollment, security updates and user experience, and can fit any organization's specific needs and budget. To view the list please visit:

https://androidenterprisepartners.withgoogle.com/#!/results/browse-all/2

Leaving Device Administrator behind

In December 2017 Google made a significant announcement with far-reaching impact: Device Administrator APIs, those powering Android management from Android 2.2, are being deprecated in two years with the launch of Android Q.

This has been a long time coming, with Android enterprise rapidly maturing it made little sense to maintain two competing management solutions, particularly given Device Administrator has a number of limitations and drawbacks when compared to not only Android enterprise, but other mobile operating systems as well.

MobileIron

Management made simple

Pain-free device provisioning

With Android enterprise, the pain points of legacy Device Administration enrollment are a thing of the past. Many EMM admins will have created enrollment documentation for the various mobile operating systems supported by the organisation. Android enrollment has rarely been less than multiple pages walking users through the initial setup wizard, Google account management, navigating the Play Store for distributed public applications and more.

End-users can skip steps at leisure, find the process too time-consuming or confusing and very often result in EMM admins pre-staging (or pre-enrolling) in order to reduce the support overhead.

Android enterprise aims to significantly reduce the time and effort involved with the introduction of new provisioning options, including NFC (5.0+), DPC identifier (6.0+), QR code (7.0+) and zero-touch provisioning (8.0+). These offer both administrators and users respite from the 30-40 step enrollment guides of years past.

NFC - A provisioner device bumps the device to be provisioned to initiate an NFC payload transfer. The NFC payload contains instructions for initiating work-managed provisioning.

QR code - Generated manually or via the EMM solution, a QR code is supplied containing the payload to provision a work-managed device. The device enters QR code setup with 6 taps of the welcome screen.

DPC identifier - While setting the device up normally, the end-user will input an identifier unique to each EMM in place of the normal Google account when requested. This will initiate a server call to Google and begin the work-managed provisioning of the device.

While some provisioning options work best when devices are being staged locally, such as the NFC bump, others are designed to offer reliable, remote provisioning such as QR and DPC identifier.

Zero-touch - This is a capability that is in a league of its own. Supported on Android 7.0 with Google Pixel devices and Android 8.0 and above, zero-touch offers - much like Apple's Device Enrollment Program (DEP) - the automated provisioning of a device completely hands-off for enrollment! EMM admins simply create and apply a zero-touch configuration in the zero-touch portal and can then ship the devices directly to end-users with zero-touch prepared to engage as soon as a network connection is established on a new or factory-reset device and cannot be bypassed.

A unified management experience

With Android enterprise utilising one set of APIs built into the operating system itself for all OEMs to leverage, Android enterprise promises a faster, more secure and easier management offering than ever before; organisations can rest assured no matter what GMS certified devices are chosen for business use, the devices will function and behave in a reliable, reproducible manner.

As the Android enterprise solution set continues to mature, OEMs will be increasingly joining the likes of Zebra and Samsung in building their own software and solutions on top of the Android enterprise base experience, meaning tools organisations may have used and relied on in the past will continue to work in the future.

Automated account management

Like iOS and iTunes accounts, arguably one of the biggest headaches an EMM admin can face is having to deal with Google accounts, either managed by the organisation or by the users themselves.

In order to diminish the effort involved in maintaining many Google accounts, some organisations would share accounts across devices or attempt to push application installation files (APKs) from the EMM console rather than Google Play. Both approaches were fraught with security issues, breaches of distribution rights and potential privacy nightmares!

Furthermore, since the introduction of Factory Reset Protection (FRP) in Android 5.0, more and more devices utilising the legacy Device Administrator APIs for Android management have been returned to the business locked out, requiring a visit to the local OEM service center for a costly repair.

User/corporate-managed Google accounts are no longer a requirement for Android enterprise, which equally extends to the G Suite domain verification needed when Android for Work was first introduced. Today, organisations can choose between continuing to leverage G Suite where an organisation has gone Google for integrated account management, or for those without G Suite, managed Google Play accounts offers seamless, fully-automated and user-agnostic account management with no admin intervention and a very quick setup process.

What's more, managed Google Play accounts aren't linked to additional Google services and aren't used for backing up device data, a clear benefit for organizations concerned about privacy and data leakage when compared to personal Google accounts.

MobileIron

APPCONFIG COMMUNITY

The role of the AppConfig Community

The AppConfig Community is a collection of industry leading EMM solution providers and app developers that have come together to make it easier for developers and customers to drive mobility in business. The community's mission is to streamline the adoption and deployment of mobile enterprise applications by providing a standard approach to app configuration and management, building upon the extensive app security and configuration frameworks available in the OS. See AppConfig,org/Android

Working together, the members of the AppConfig Community are making it simpler for developers to implement a consistent set of controls so that enterprise IT administrators can easily configure and manage apps according to their business policies and requirements. With AppConfig Community tools and best practices, developers do not require EMM-specific integrations for many enterprise use cases. End users also benefit from automated features such as an out-of-the-box experience to give the users instant app access without requiring cumbersome setup flows or user credentials.

Managed applications

With Android enterprise, users no longer need visit the Play Store for their applications. Rather the organization can push public and private apps down to devices silently with no end-user interaction by making use of automated account management above and Google's Play APIs integrated directly with the EMM.

Furthermore, where legacy enrollments may require additional steps for configuring applications as part of the enrolment process, Android enterprise supports managed application configurations in order to allow organizations to pre-configure app details in the EMM solution prior to installation.

With this capability, applications like Chrome may be configured to block known bad websites or disable pop-ups out of the box. Gmail can be installed already configured to fetch emails. Some apps will support kerberos integration for completely password-less application setup and integration with organisation services. Per-app VPN solutions will work without the need for complicated setup.

Indeed, managed applications with Android enterprise, whether obtained via the Play Store or hosted by the organisation as an internal, whitelisted app repository Android enterprise can leverage, can save considerable time in deploying devices to large and small estates. Further controls such as permissions management ensure a user can't deny a required permission, or allow a permission that the organisation doesn't deem suitable for the application being installed.

Finally with the capability to block uninstallation, accept application T&C's on behalf of users and prevent uninstallation, organizations can tailor the perfect ecosystem of corporate applications to their needs. All without a personal Google account on the device.

Conclusion

Android has greatly improved over the years to become a mature and stable mobile OS capable of meeting the most demanding of business needs.

With Android's inherent flexibility and open nature as a platform, it has empowered OEMs to create devices to suit all required form factors, feature sets and budgets while offering strong security and the peace of mind that corporate data is entirely secure, without hindering the end user.

Whether BYOD, COPE, COBO or otherwise, Android enterprise comes complete with solutions ensuring strong separation between personal and corporate data, universal and reliable management across OEMs and provisioning processes that significantly speed up the time it takes organizations to enroll their devices, thus saving time, money and lowering the support burden considerably.

As Android continues to evolve over the next few years, we expect this to only improve further.

Find out more..

Wherever your organization sits in the Android story today, whether it is evaluating solutions, running migrations or looking for support, MobileIron can help. Our customers with 10s of thousands of devices are leveraging the scale and flexibility of Android, please visit our Case Studies web page to learn more. All of the security and management capabilities available on the latest Android platforms can only be managed by an EMM solution. And with 15,000 customers, our award-winning MobileIron EMM provides the secure foundation required to meet both user demands and IT security requirements for any Android-based implementation.

Long-time MobileIron partner and friend Jason Bayton quoted above equally offers in-depth, solution agnostic content for learning about the range of capabilities and how they compare with legacy enrolment on his website here.

And for any other information or to speak to a human today, contact MobileIron

MobileIron

401 East Middlefield Road

Mountain View, CA 94043

globalsales@mobileiron.com

www.mobileiron.com

Tel: +1.877.819.3451

Fax :+1.650.919.8006