Achieving Mobility Management Balance with Android

Phil Hochmuth
Sponsored by Android
January 2019
IDC OPINION
Enterprises are more productive when employees can choose the technologies they like best to do their jobs. However, a complete free-for-all IT environment won’t stand up to compliance audits, security policy requirements, and generally accepted safe mobile computing practices. To that end, enterprises should consider the Android operating system’s (OS’) strong data separation, multiple device management options, and easy system enrollment capabilities as ways to balance IT controls with user satisfaction and device/app choice.

IN THIS WHITE PAPER
This white paper examines what IDC defines as the third pillar of enterprise mobile computing requirements: balancing IT enforcement with user acceptance. Following pillars 1 and 2 (Android security capabilities and Android solution breadth, respectively), this document in the series highlights some of the top IT and security management challenges that businesses face as the workforce increasingly brings personal devices, applications, and cloud services into the workplace. It outlines steps enterprises can take to help enforce security and compliance requirements in mobile enterprise computing without sacrificing user satisfaction with technology.
Businesses give employees technology to be productive and achieve business goals — basically, to do their jobs. This seems obvious, but the nuances of worker habits and preferences and human behavior in response to introducing and deploying digital technology complicate this simple concept. This has been true since the mainframe and client/server eras of business end-user computing (what IDC calls the “1st and 2nd Platforms”). IDC defines the 3rd Platform — which began in 2007, when smartphones emerged — as the era of mobile, cloud, big data, and social technologies (IDC’s four pillars of the 3rd Platform). In this era, end users can do much with mobile digital technology, in terms of both driving productivity and causing trouble.
User Productivity Thrives When Freedom of Choice Is Allowed

Looking the other way to let workers be productive is not only a common IT management practice but almost institutionalized as an accepted standard in a large number of businesses, especially small and midsize firms. According to the IDC 2017 survey of IT administrators, commissioned by Google, nearly half agreed that allowing the use of unofficially sanctioned mobile technology is good for business and end-user productivity overall.

Letting people work the way they want, with their preferred digital tools, leads to more productive outcomes. By several measures, organizations that take a more permissive approach to mobile technology usage and choice see better results from overall user satisfaction and success of mobile programs. According to the IDC study commissioned by Google, nearly 60% of firms allow users to either install any app they want on devices or download any app they want, as long as there is a productivity reason or valid use case for the software. From a device perspective, organizations that support end-user choice when deploying phones (so-called choose-your-own-device [CYOD] programs) said that their mobile technology deployment efforts and projects exceeded expectations 15% more frequently than organizations not supporting device choice. Similarly, according to the IDC study commissioned by Google, firms with higher tolerance for user choice in terms of installing mobile apps or allowing non-IT-approved tools (i.e., “shadow IT usage”) had better outcomes than those that did not allow these practices, such as increased user productivity and overall satisfaction.
Businesses Must Enforce Policies for External and Internal Compliance Reasons

While businesses want to lean toward openness to end-user productivity, the average business is governed by a myriad of compliance and regulatory standards specific to IT deployments and technologies, according to IDC research. Devices deployed in use cases involving sensitive data — medical information and processing payments or other financial transactions — as well as knowledge worker devices with sensitive email and data are all under compliance scrutiny. Compliance is consistently the top barrier to enterprise mobility deployment efforts and ongoing operations; according to IDC’s Enterprise Mobility Decision Maker Survey, over 40% of enterprises named security/compliance as their top issue (HIPAA, SOX, PCI, etc.). Lost devices, data loss due to leaky apps, and unauthorized system access via mobile were among other top incidents enterprises said they experienced. All these challenges enterprises experience amplify the need for balance between user experience/acceptance and strong security policy enforcement. Going too heavy one way or the other either hinders productivity and stifles growth or opens firms up to breaches and compliance audit failures.
Smartphones have been called the most “personal” computing device ever. Given the opportunity, users will work with mobile technology that is the most familiar to them. This is reflected in terms of business device shipments and adoption trends; employee-owned devices (or BYOD) worldwide have outpaced corporate-liable (CL) devices by 15% consistently for the past five years of IDC business device shipment tracking. As such, more than 90% of U.S. enterprises allow some form of BYOD, and the large majority of enterprises have BYODs as the majority of their mobile employee device installed base. The most important letter in the acronym is B, in that users have the choice to bring their preferred devices in to work. A BYOD policy enables choice.

90% of U.S. enterprises allow some form of BYOD, choice.
The Emergence of Choose Your Own Device

Choose your own device (CYOD), an emerging option in an increasing number of enterprises, provides more user choice and autonomy over what kinds of smartphones workers use while keeping the ownership, management, and control of the device with the organization and the IT department. CYOD can apply to both corporate-owned models (where users can choose from a list of company-provided devices) or employee-owned models (where workers are given a list of approved devices they can bring to work). Overall, CYOD adoption has grown steadily over the past several years among businesses, increasing from under 40% of U.S. enterprises in 2015 to over 67% of firms now having this model, according to IDC survey data.

Android Is the Most Common BYOD Platform in Business

In a majority of instances, when end users are given a choice of device type they can use or bring to work, Android devices are the most chosen smartphone category in terms of BYOD and CYOD, according to IDC. In the worldwide business-use smartphone installed base, there were 195 million Android devices deployed in BYOD scenarios (more than any other device type by over 80 million). And in IDC’s 2017 Enterprise Mobility Decision Maker Survey, 66% of respondents said the Android operating system was the most requested OS among CYOD types deployed.

Enabling Preference Begets Corporate Policy Enforcement

While the presence of enterprise mobility management (EMM) is relatively high (60%) among U.S. enterprises, the average number of devices managed by EMM remains below 50% (66% for CL devices/32% for employee-owned devices), according to IDC’s 2017 Enterprise Mobility Decision Maker Survey. User resistance is among the top reasons that more devices are not enrolled in management. This is actually the main driver for CYOD programs, according to an IDC study; 50% of businesses said they deployed
When given the opportunity to choose device OS type, brand, and models, end-users are more willing to concede to stronger IT management and control over their devices.

CYOD to drive device management enrollment, and this works. CYOD enrollment with EMM has a higher rate of adoption than BYOD (50% versus 32%) and is on par in terms of EMM penetration rate with standard CL devices. This reflects a give-and-take dynamic in many enterprises. In interview research with businesses deploying CYOD and EMM together, IDC has found that end users, when given the opportunity to choose device OS type, brand, and models, are more willing to concede to stronger IT management and control over their devices (beyond basic provisioning, such as Microsoft Exchange ActiveSync or Office 365 management configurations). It’s a classic carrot-and-stick scenario.
Strong separation of company/user data is critical to successful IT deployments and ongoing operations. Businesses are taking a range of approaches to meet this demand. On the one hand, user demands and preferences for personal and familiar technology are strong (and ultimately good for business). On the other hand, keeping corporate data safe, and/or enforcing usage policies and restrictions on the mobile devices that users are given a “choice” to use, is helping IT meet security/compliance checks.

The Android operating system offers a rich set of management options for a wide range of deployment scenarios:

- **Work profile**: A containerized work/life separation primarily aimed at BYOD; work/personal profiles run side by side on the device’s home screen (with corporate apps and notifications highlighted with a briefcase icon)
- **Fully managed device**: A fully locked down, managed mode for complete corporate ownership with no personal space
- **Dedicated device**: A single-use mode (Android Kiosk, but within a work-managed device) for Kiosk-like applications (These devices are also known as corporate-owned, single-use [COSU] devices.)
- **Work profile on a fully managed device**: Bringing together work managed and work profile to provide a fully managed device with a personal space (These devices are often referred to as company-owned, personally enabled [COPE] devices.)
These models can address many of the previously discussed use cases, keeping in mind factors such as user choice and enablement. For example, work profile on a fully managed device (COPE) and fully managed device can satisfy many levels of IT policy control and security while providing device choice and end-user autonomy over users’ mobile experience, from strictly locked down devices to personally enabled and single-use cases.

Android Enterprise is deployed in concert with an EMM provider, meaning IT can use a standardized set of APIs to control devices and data separation on managed Android devices across all of these scenarios. This combination becomes the fulcrum of the IT/end-user balancing act: businesses can distribute, control, and secure a myriad of device types and deployment models while allowing for simple, familiar access to apps via the managed Google Play store and the native Android OS experience.

**Android Enterprise Provides Strong Separation of Work/Personal Data and Apps**

The inherent controls and separation of data and apps in the Android work profile can help businesses achieve a strong data segmentation and isolation. Separation between a user’s personal data and work data is enforced at the OS kernel level across processes, memory, and storage. All applications from the managed Google Play Store run on this device data separation. No app modifications are necessary. Data loss prevention (DLP) policies can be applied to the work profile via an EMM platform (e.g., preventing copy/paste from a corporate app to a non-managed app).

In this framework, IT only touches business applications and data; employees keep using any app they choose to in the personal profile, and everything is shielded from IT inspection, visibility, or control. If an employee leaves the organization, only corporate apps and data are wiped. Personal applications and data remain after a remote wipe. This can help an organization avoid legal controversies or issues around wiping out, or even viewing, personal photos, contacts, or other personal information from BYODs used in the workplace.
Since Android N, users have been able to show, disable, and gray out whole screens of work-centric apps provisioned via Android Enterprise. (When work is “shut off,” the apps consume no device resources, making the device essentially 100% personal.) Enterprises can allow for a work profile on a fully managed device (a COPE device) by deploying a work profile onto fully managed devices. That allows end users to bring their own applications while ensuring the integrity of corporate data. In the latest Android P, or version 9 of the mobile OS, this switching is now easier, as part of Google’s overall digital well-being initiative.

Android provides a flexible and secure management platform which offers a range of fully managed experiences and a work profile which gives users more control. These technologies allow for a range of flexible deployment scenarios, from locked down–dedicated devices to BYODs. The work profile gives enterprises a BYOD option with strong policy enforcement over the use of corporate data on personal devices, maximizing worker productivity with nonintrusive security on their own familiar mobile devices. In dedicated scenarios, IT can control every aspect of the device’s function to securely use smartphones and tablets to digitally transform business processes, workflows, and tasks.

The work profile enables businesses to allow personal applications and data on corporate-liable devices while keeping corporate apps and data separate. This capability is a powerful tool to create a more personal feel and familiarity for corporate-owned/managed devices, especially in CYOD scenarios, which can extend near-BYOD user experiences (users choose the device and get their own apps/data on them) while keeping the hardware and business apps and data under corporate control.
Zero-Touch Enrollment Speeds Deployments

A key aspect to user acceptance and satisfaction with a technology is to have it set up in the required managed state prior to deployment. Even in scenarios where corporate mobile devices are deployed to end users prior to enrollment and setup, there is an opportunity for resistance, or at least dissatisfaction, with the perceived imposition of IT on “their phone.”

Android zero-touch enrollment allows an IT organization to preconfigure devices so that apps can be easily pushed to and installed on devices (via an EMM connection and delivery via managed Google Play), with correct settings and privileges already in place. This removes the step of an employee having to request access to internal systems (e.g., corporate email) or external apps (such as salesforce.com). Zero-touch can also be used to set up complex access control settings, such as device-based certificates or other single sign-on provision, for on-premises or cloud resources, thereby allowing workers to be productive with their devices straight from the box. Zero-touch involves your carrier or reseller uploading identifiers for purchased devices and then using a portal to connect these devices to a back-end EMM platform, which enrolls the device automatically and pushes all preconfigured policies and settings to Android devices over the air.

Simplifying authentication and log-ins for devices and corporate apps is a top challenge for businesses. Less than a quarter of enterprises use advanced tools such as device-based digital certificates, or multifactor authentication, to manage log-ons to mobile apps and enterprise-provisioned resources. These approaches can be complex and cumbersome to deploy and setup. According to IDC research, close to half of organizations want to get to a more advanced state of authentication and security in the near future, but few are at that stage today. The combination of zero-touch and Android work profiles can be used (in conjunction with an EMM platform) to provide out-of-the-box capabilities that support strong, multifactor authentication, with minimal end-user frustration and IT involvement. With the release of Android P, provisioning has become even more seamless, with QR reader and support for WiFi configuration shaving off deployment time.
Broad EMM Support Is Critical to Improve Experiences for the Broadest Range of End Users

EMM technology is a critical component in enterprise Android deployment, as an EMM implements much of the advanced policy enforcement, security, access control, and other settings supported by Android work profiles and managed device functions. The EMM software marketplace is a wide-ranging field of vendors; many covering a broad range of enterprise use cases, and others offering specialized solutions for specific use cases or verticals. Overall penetration of EMM platforms in enterprises is high — more than 60% of enterprises in the United States and Western Europe have an EMM platform in use, according to a Google-sponsored study on EMM usage across both regions. In addition, among those using an EMM platform, more than 77% of enterprises use more than one EMM provider’s products. Multi-EMM platform usage is often prevalent among divisions or subsidiaries in an organization (often through acquisitions) or specific platforms may be deployed for certain groups of users, such as EMM platforms specializing in ruggedized/warehouse device types, or platforms with additional security or systems integration capabilities. Android Enterprise supports over 50 EMM platforms to help ensure that the powerful security, provisioning, and data separation features of the Android OS can be unlocked under a wide range of EMM installed bases and multi-EMM scenarios.

Preserving Native App Experiences with Enterprise Policy Enforcement and Control

Preserving native app experiences with enterprise policy enforcement and control is another example of carrot-and-stick IT policy in mobility. Users will more likely accept and use corporate-provisioned and corporate-controlled apps and tools that look and feel like the familiar apps they choose to download in the first place (with or without IT permissions). Consumer-friendly interfaces and features can be part of corporate mobile computing experiences without sacrificing security, monitoring, control, and policy enforcement. Users don’t have to know the apps are “good for them” (and the company) from this perspective.
Mobile employees will be more productive and successful if they have access to hardware and software tools that are familiar and pleasing to use day to day. Businesses that do not consider the user experience factor when planning a mobility deployment (either hardware or software — or a combination of both) will hamstring their organizations’ initiatives and end up costing the company in tangible and intangible ways (either through lost productivity of end users or in hard costs of having to rip and replace technology that goes unused or is outright rejected by end users).

**Connecting Familiar with Secure**

Management and security technology that stifle worker productivity or radically alter or block consumerlike mobile experiences, functions, and tools that users are familiar with will be dead on arrival in most IT deployment scenarios. Strong, but unobtrusive, even unnoticeable, security technology is more effective at enforcing policy and identifying threats well. “Secure” or “well managed” should not mean a completely new or unfamiliar user experience. Users prefer to know a platform or system is inherently secure with underlying levels of trust and capabilities, rather than feeling that security measures are plastered on after the fact. Deploying apps to end users via managed Google Play provides this level of familiarity — the apps themselves may have no difference in features, look and feel, or user interface (UI), but they can be subtly tuned and configured to meet the security and compliance needs of IT.

Managed configurations are software hooks built into Android mobile apps that allow enterprise IT teams to apply security parameters, settings, and other controls to the apps when deployed in corporate devices/scenarios. When deployed to Android work profiles (such as personally enabled devices), EMM platforms are the interface used to apply changes and settings adjustments to Android business apps deployed through managed configurations via managed Google Play APIs.
End Users Get Secure Managed Apps with Familiar Play Download and Native App Experience

Managed Google Play is the app management platform for enterprise Android apps. This is where enterprises configure permissions and provision apps on business-use devices (both corporate-liable devices and BYODs).

Applications can be designated as required or optional for individual employees or departments and groups or classes of employees (i.e., those handling sensitive corporate data or intellectual property on mobile devices). Required apps can be installed on end-user devices without any involvement from the user (called a “silent push”). Public apps in managed Google Play appear the same as in the standard Play Store familiar to any consumer Android user. IT administrators can control what managed apps can be installed (i.e., whitelisting) from the managed Google Play Store. A Google Account, or managed Google Play Account credentials, is required to distribute apps to users, either through individual user downloads installs of apps or via bulk app purchases and deployments via an EMM platform.

Managed Google Play Store environments for business customers can also be customized in terms of layout. Enterprises can use managed Google Play to publish privately developed custom applications built by the organization or from an app development partner. This function can also be integrated into the app distribution or “enterprise app store” functions on various EMM platforms to privately publish or push custom apps to end users via an EMM console. In either case, the apps can be hosted in managed Google Play or the customer’s private app store, or on a server that can be configured to authenticate the download with JSON Web Token (JWT). The enterprise app store experience is still provided by managed Google Play.
Security versus user acceptance is not a binary choice for IT decision makers. Making the effort to find software, tools, and platforms that enable positive user experiences, technology choice, and strong, unobtrusive security and policy enforcement will help organizations reach greater worker productivity, employee satisfaction and adoption, and better business outcomes as companies navigate the churn and change involved with mobile computing technology.

Data separation and security controls enabled by Android allow mobile workers to keep the familiar apps and services they choose for personal use while maintaining strong corporate governance and management of business data and apps on the same mobile device. From this foundation, the four Android Enterprise management modes — work profile on a personally-owned device, fully managed work-only device, dedicated device, and work profile on a fully managed device — provide the management, provisioning, security, and control options for a wide range of use cases and deployment scenarios. Services such as Android zero-touch enrollment and managed Google Play enable Android devices to be deployed to users with specific profiles, configuration settings, and approved business apps in place right from device unboxing and activation. Managed Google Play also ensures familiar, native Android experiences over bolted-on containerized app experiences (which are also harder for IT to manage and deploy). Broad support from EMM platform providers allows Android devices to fit into most enterprises’ existing mobile device management software deployments.

Enterprise IT teams should assess all mobile device deployments throughout their respective organizations and consider what measures of security, management, and end-user openness and flexibility are right for each use case. Teams should then consider how Android features, services, and management technologies can improve the balance of end-user acceptance and IT manageability toward a more secure, productive, and digitally transformed enterprise.
To learn more about achieving a balance between IT and user experience and the other pillars for enterprise mobility success, visit www.whyandroid-enterprise.com/all

All papers sponsored by Android
About IDC
International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

Global Headquarters
5 Speen Street
Framingham, MA  01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice
External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.