IDC OPINION

As the most popular mobile operating system (OS) in the world, IDC identifies that the flexibility of the Android platform and the adaptability provided by the large Android ecosystem present enterprises worldwide with a broad range of device manufacturers and partners to choose from. Vast in choice and deep in configurations, Android allows enterprises to deploy the platform in various ways and select specific technology solutions that are tailored to fit their business needs with increasing flexibility and granularity. The diversity of Android’s deployment options, form factors, price points, and global reach allows enterprises to leverage the tools and solutions necessary to thrive in their pursuit of digital transformation, enabling a more flexible and productive mobile workforce.

IN THIS WHITE PAPER

This white paper analyzes the unique and pervasive opportunities the Android mobile operating system presents for businesses across a wide range of use cases and deployment scenarios. Android is examined in the context of its flexibility in terms of mobile hardware deployments, management modes, and its large-scale availability worldwide in terms of device diversity, price points, and form factors.
Mobile Device Use Cases Are Everywhere: Digital Transformation Is Mobile Enablement

The evolution of mobility over the last decade has become fundamental in shaping modern business strategies around the world. According to IDC’s business use mobile device forecasts (smartphone, tablet, and rugged), over 386 million business use mobile devices were shipped worldwide in 2017, and this number is expected to increase 30% by 2022. In the United States alone, the number of mobile workers currently account for over 70% of the total workforce, and in 2017, U.S. enterprise IT decision makers identified acquiring new mobile hardware as the top spending priority regarding mobility. In short, IDC finds that mobile devices are ingrained throughout business workflows and continue to enable new business processes on a global scale.

Over 386 million business use mobile devices were shipped worldwide in 2017, and this number is expected to increase 30% by 2022.
New business processes are driving a need for different device types capable of meeting complex business demands across a wide variety of vertical and horizontal use cases, and Android is well positioned to address these demands from both a hardware and an OS perspective. In addition, device ownership has an increasing influence on how devices are managed and deployed by IT, whether it be a corporate-liable device, BYOD, or dedicated device. Demand for new mobile devices is not solely driven by an IT desire to get more mobile devices into the hands of executives and knowledge workers; there is an increasing appetite among enterprises worldwide for purpose-built rugged to dedicated devices that can handle multiple applications. Deployments of these devices are on the rise. Owing to Android’s ability to operate across a multitude of device form factors, price points, and OEMs, Android is currently driving this market, with Android rugged/dedicated device shipments forecast to grow at 23% CAGR over the next five years, over five times the rate of the ruggedized market overall. Android is projected to be the largest OS for rugged devices by shipments starting in 2019.

According to the annual IDC survey data, over 60% of enterprise organizations in the United States have deployed rugged/dedicated devices, and nearly another 25% plan to deploy technology to manage dedicated deployments in locked-down roles such as kiosks, ATM machines, retail POS, and other function-specific or purpose-built roles. Many businesses are thriving with majority Android device deployments. Among such businesses, 50% of businesses said their mobile deployment efforts met expectations, and an additional 47% said they exceeded expectations.

Many of these devices break away from traditional smartphone and tablet form factors, pushing design features and priorities well beyond the familiar standards of consumer-centric flagship mobile devices. Android device OEMs can allow for workflow and use case demands to dictate device form and function, resulting in highly specialized devices or peripherals optimized for their given tasks. The commonality here is that all of these various form factors and use cases still run the same stock Android OS from Google, which provides economies of scale for application development and management operations in enterprise businesses. Android OEM diversity is core to mobile enablement, as it not only allows OEMs to build different devices that meet a variety of evolving business demands but also allows enterprises to control costs, as they have the freedom of selecting an appropriate device for a given deployment based on their needs, from a wide range of form factor and use case options.
Device-centric digital transformation use cases for mobile enablement span most industries with little exception, as the sheer usefulness of arming workers with increasingly powerful, capable, and connected devices is beneficial to business strategies. Mobile use cases for industries include (but are not limited to):

- **Financial services**: Automated/interactive teller services; secure mobile banking
- **Manufacturing**: Real-time assortment monitoring; factory floor management/data entry
- **Transportation and logistics**: Delivery POS; inventory management/scanning; asset tracking/scanning; fleet management and dispatch; freight monitoring/tracking
- **Retail**: Mobile client; self-serve customer checkout/item tracking; personalized customer outreach; showroom and merchandise showcasing; mobile POS; digital signage; inventory management
- **Hospitality**: Self-serve guest services and automated guest check-in; digital concierge services; in-room smart controls and entertainment
- **Field service**: Real-time communications with supervisors and dispatch (smartphone/rugged); augmented step-by-step workflow and maintenance assistance (tablet and augmented reality (AR) based); on-demand digital blueprint access; fleet management
- **Healthcare**: Clinician alerts and communications (smartphone/tablet/rugged); EMR access/input (smartphone/tablet/rugged); lab and medication barcode scanning (smartphone/rugged); patient check-in and monitoring; guest services and communications
Pricing Diversity Puts Android Everywhere

The ability to select devices from not only an extensive OEM pool but also an extensive range of price points is one of the core reasons Android excels in business implementations. At face value, pricing diversity makes it possible for businesses to address a broader range of digital transformation scenarios, from full knowledge worker enablement down to basic taskwork devices and even to digital signage and interactive displays.

According to IDC tracker data, in 2017, the ASP for Android smartphones worldwide was well under $500, with price points from $1,000 to as low as $100 across more than 20 smartphone manufacturers and over 35 international carriers. The diversity of price points offered by the Android ecosystem makes it possible to deploy top-of-the-line flagship devices when necessary and lower cost devices where workflows and deployment scenarios dictate fiscal restraint. Mobile enablement does not demand a $1,000 or even $500 device for every employee. Security requirements may very well justify that an executive-level employee use cutting-edge mobile technology and be armed with an encrypted device with advanced biometrics and receive regular security updates. However, if a company is looking to deploy a fleet of devices simply to expand voice communications or dispatch notifications for task-oriented workers, then a low-cost device might very well meet the company’s requirements while providing an advantageous TCO.

According to IDC’s 2017 Enterprise Mobility Decision Maker Survey, multinational organizations that support Android said they are eager to leverage its pricing diversity and include it as a driving factor in the decision to adopt the OS. Price points and brand popularity vary at a global level, and price sensitivity is important for all organizations with BYOD workforces. According to IDC data, “cost savings” is cited as a leading driver of BYOD adoption in the enterprise, and YoY, a marked reduction in capex and opex spending is reported by enterprises that support BYOD. In addition, organizations with BYOD workforces in developing or less economically developed countries are especially sensitive to hardware costs. Access to device brands vary greatly by country, making it
difficult to consolidate worldwide deployments unless the underlying OS can be widely accessed and securely managed within a consistent framework. Consistency is crucial for IT admins tasked with managing a heterogeneous mobile ecosystem, especially when device types vary across OEMs, carriers, regions, and use cases. In the case of Android, pricing diversity and platform consistency allow organizations to purchase the right device, at the right price, for the right worker, and manage those devices with consistency.

Looking beyond one-to-one mobile device use cases, price diversity enables digital transformation scenarios to be extended across a broader range of deployments. A company may choose to deploy a more expensive fleet of dedicated rugged devices designed to be used by multiple employees 24 x 7 or less expensive locked-down kiosk tablets or interactive digital signs to enhance customer experiences in retail environments. For example, in a discussion with IDC, one United States–based healthcare organization outlined how pricing and TCO played a significant role in the decision to deploy a fleet of purpose-built Android rugged devices to its clinicians and nursing staff. While the devices carry a larger per unit cost than average consumer-grade smartphones, they enable many of the hospital’s specialized critical patient care workflows, ranging from nursing alerts to lab and medication scanning. Features like extended removable batteries allow the devices to remain on the hospital floor 24 x 7 spanning three different hospital shifts per day. The ability to share devices across multiple users and shifts meant the hospital did not have to purchase a device for every individual employee, which drastically cut down on device costs. Early estimates concluded that the hospital would have had to spend nearly three times as much to deploy consumer-grade smartphones over the rugged devices in the same scenario due to hardware and battery limitations.

One US hospital estimates that it would have had to spend nearly three times as much to deploy consumer-grade smartphones over the rugged Android devices in the same scenario.
Device Choice Trends in Enterprises: Programs That Drive the Balance of User Productivity and IT Requirements

According to IDC’s 2017 Enterprise Mobility Survey, employee choice ranked as the number one factor regarding enterprise mobile device deployment strategies, and IT organizations are being tasked with striking a balance between employee satisfaction and the need to secure mobile devices accessing sensitive corporate data. Accounting for 77% of worldwide business use smartphone shipments in 2017, the growing appeal of Android is having a tremendous impact on both the choices of end users and IT decision makers alike.

Android accounts for 77% of worldwide business use smartphone shipments in 2017.

From an IT perspective, the need for comprehensive security solutions often overrides mobile workers’ desire for freedom of choice when it comes to mobile devices being used for work. Almost half of enterprises cite the ability to enforce security policies as the main reason for maintaining strict corporate-liable device policies within their organizations. While improved employee productivity remains the most important benefit enterprises expect to gain from their mobility investments, enterprises are investing most of their mobility budgets in devices for employees. Given the rate at which enterprises are investing in mobile hardware for their employees, employee satisfaction should be a high priority. In discussions with IDC, enterprises report that forcing employees to use a device or mobile ecosystem they dislike or submit to burdensome and tedious mobile workflows is the fastest way to harm employee engagement with mobile technology. Mobile devices are an increasingly personal aspect to daily routines, and as a result, business users expect to use the device and OS of their choice.
In some instances, strict security policy enforcement for corporate-liable devices is utilitarian and cannot be circumvented or wane in light of end-user considerations. For example, a physician who regularly accesses patient health records on his/her mobile device, or an investment broker who handles his/her customers' financial information is subject to a higher degree of security policy enforcement. However, this isn't to say that trampling end-user experience in the name of security is an unfortunate means to an end, or even necessary. Mobile workers have more choices than ever before with regard to how they access the content they need and on the devices they use to do so. This is especially true when choosing Android devices, as users are afforded the broadest range of mobile devices currently available in the market, comprising a legion of OEMs, models, price points, and features. Mobile workers’ freedom to choose their preferred device is contributing to the rise of choose-your-own-device (CYOD) program support among enterprises.

CYOD allows IT to balance the needs of the company against the wishes of the employee by providing employees with a list of devices that IT has vetted and deemed secure and manageable enough for business use. In addition, CYOD can be applied to both traditional corporate-liable device programs and BYOD programs. This allows companies to take advantage of greater security policy enforcement via corporate liable and the cost saving benefits of BYOD in parallel. In fact, according to IDC’s 2017 Enterprise Mobility Decision Maker Survey, 75% of U.S. enterprises currently offer or plan to offer a CYOD program to their employees in the coming years.

Multinational and multiregional enterprises (MNOs) based in the United States but with operations in two or more additional countries or regions have much higher instances of CYOD than U.S.-only firms (47% of MNOs have adopted CYOD versus 36% of non-MNOs). MNOs must contend with the added challenge that mobile device brand, form factor, and even screen size preferences vary across countries and regions, as does availability. As a result, Android is the most popular OS platform chosen by end users in CYOD deployment scenarios, with 49% of workers choosing the Android platform.
An Open Software Architecture Drives Ecosystem Innovation

IDC believes the open nature of the Android OS contributes to a diverse ecosystem of device types, as well as millions of mobile applications and their respective developer communities worldwide. Android Studio allows Java developers to build their applications in a mature and intuitive development environment, complete with sophisticated toolsets that allow developers to test, update, manage, and analyze their applications. The depth and variety of its device and software ecosystems present a fully customizable Android platform that can address the varying requirements of enterprise digital transformation, unrestricted by form factor or device OEM.

Form factor flexibility, a strong and thriving application ecosystem with worldwide developer support, and ubiquitous user acceptance worldwide are all strengths that lend themselves to the requirements of vertical task-based device solutions, as well as purpose-built specialized devices. For example, a company can deploy a fleet of rugged devices in a warehouse environment that is specially designed for rapid barcode scanning and inventory management. Hardware ergonomics and function are a critical consideration for task-based workers with repetitive workflows, and because of this, specialized Android devices are available in a variety of “scan gun,” smartphone, and tablet form factors, with a host of peripherals ranging from wearable scanning rings to mobile barcode and receipt printers designed specifically to increase productivity and reduce downtime. In addition, because Android is hardware agnostic, companies that have built their own unique devices from the ground up can leverage off-the-shelf Android devices or the Android OS itself to integrate device or application functionality at a much lower cost than building it themselves. For example, a company that designs heart monitors can build an Android application that allows the patient to track heart monitor readings and then send those readings back to the hospital or physician. Companies are afforded the flexibility to choose which device or application configuration is best suited for specific workers, workflows, or devices.
Healthcare environments pose significant challenges with regard to mobile hardware deployments on both the security and capability fronts. Should a given device fail in a hospital setting, the inherent risks and dependencies of hospital workflows where a person’s safety or personal medical information could be put at risk means that there is much more at stake than a simple loss of productivity. From a software and security perspective, Android’s open architecture allows OEMs to build customized versions of the OS specifically for healthcare deployments that are not only HIPAA and VA healthcare security compliant but also stripped of any unnecessary applications or device features that may impede a clinician’s ability to focus on or complete a given task or prevent sensitive patient data from being leaked. From a hardware perspective, purpose-built devices for hospitals are made of impact-resistant antimicrobial materials and can withstand being repeatedly sanitized in compliance with hospital infection-prevention standards.
Google’s Global Scale Keeps Devices on the Forefront of Innovation

According to IDC research, Android is the most popular mobile operating system in the world in 2018, accounting for over 84% of all smartphones, 65% of all tablets, and 43% of all rugged mobile devices shipped worldwide. The scale of Android itself is testament to the scale of support Google brings to the platform, and the support is always a key consideration for large enterprises and multinational organizations looking to deploy business-class and enterprise-secure mobile computing platforms within their organizations. The familiarity of Android among consumers and mobile workers alike contributes to a ubiquitous and far-reaching user experience that spans this platform and multiple form factors, encompassing billions of devices and billions more applications.

At the forefront of AI research and development, Google leverages its expertise in machine learning through Google Play Protect, which scans over some half a million Play Store applications every day for malicious apps, powered by 20,000 dedicated processors running across its cloud computing network 24 x 7. Google also leverages its vast network of deployed Android devices for feedback, conducting app behavior analysis in real time and blocking malicious code on the device. As a core function of Android, all Play Store apps are scanned before install, and users can also initiate on-demand security scans of their devices, guaranteeing that devices are always protected.

As Android continues to evolve, Google is continually making changes to the underlying OS to drive continuity and security across the broader Android ecosystem. In recent months, security improvements to Android range from advanced kernel hardening to application sandboxing and the streamlining of how Android OEMs validate and update their hardware with each new version of the OS. These improvements are ongoing, and each new iteration of Android builds on marked success and emerging security priorities, standardizing baseline security features for all devices that access Google services.
Google Programs Help Navigate Android Device Selection for “Enterprise Ready” Deployments

Whether it be an enterprise IT decision maker, a line-of-business manager, or a BYOD knowledge worker, deciding on the right mobile device for a given deployment can be challenging given the host of device options, price points, and service providers available. The modern enterprise landscape is one where employee choice often clashes with the needs and requirements of enterprise IT and one where successful mobile deployments hinge on a combination of increasingly complex correct decisions. Google has assembled a range of enterprise-specific programs to assist companies in navigating the Android ecosystem with confidence.

The Android Enterprise Recommended program, a Google-led global initiative, creates broader enterprise deployment opportunities for large enterprises and multinational companies, advocating devices that meet strict hardware and software requirements for security and manageability. As one of its core strengths, Android is a permanently heterogenous mobile environment, and while enterprise mobility solution providers and device OEMs go to great lengths to appeal to many types of users, not all Android mobile devices are created with enterprise considerations at the forefront. The Android Enterprise Recommended program helps enterprises, interested in expanding Android device adoption quickly, zero in on devices that meet Google's standards for enterprise use. Specifically, Android Enterprise Recommended devices must run Android 7.0 or higher and meet certain minimum hardware requirements, and program partners must commit to guaranteed 90-day automatic security updates for three years. Android Enterprise Recommended requirements provide a baseline level of security and performance that enterprises can count on when deciding which Android devices to deploy.
Android Enterprise Recommended also helps enterprises address some of the unique challenges and requirements associated with rugged mobile devices, such as extended deployment life cycles, OS stability, and OS support. The average rugged mobile device remains deployed much longer than traditional consumer-grade business use devices, resulting in the need to extend support from an OS and security perspective beyond three years. In addition, given that these devices are often mission-critical tools that can’t suffer extended downtime, it may not be feasible or possible for IT to update the devices or associated business applications on a 90-day update cycle. To address this, the ability to freeze device and OS updates for an extended period of time has been built in to Android to ensure device stability during peak use scenarios.

Trusted partnerships are a keystone element to any enterprise initiative, and mobile deployments, in particular, demand solid vendor partnerships for success. To assist enterprise organizations in selecting the right partners, Google offers the Android Enterprise Solutions Directory, a tool designed to help enterprises find and learn about a variety of trusted Google ecosystem partners. The Android Enterprise Solutions Directory provides a customizable list of verified Android ecosystem partners composed of enterprise mobility management (EMM) providers, mobile carriers, and device OEMs. In addition to the solutions directory, Google offers the Android Enterprise Device Catalog, an online web portal designed to match Android devices to specific business needs, allowing businesses to filter devices by various criteria such as RAM, screen size, hardware features, OEM, and OS version.
According to an IDC mobility study, mobile carriers and device OEMs rank as the top most trusted partners when it comes to mobile hardware selection and deployments among enterprises. In addition to mobile carriers and OEMs, enterprise mobility management partners are an increasingly crucial requirement for large enterprises when it comes to securely managing mobile workforces and endpoints, and in 2017, 67% of U.S. enterprises either already deployed or are piloting an EMM solution.

Android zero-touch enrollment allows IT administrators to define device and user policies through their EMM solution, and automatically enroll the device out of the box, eliminating the need for tedious manual device provisioning. For enterprises using EMM, Android zero-touch enrollment enables secure deployment of corporate-owned devices in bulk, saving valuable time and effort.

When it comes to ensuring the separation of corporate and personal data, it’s not uncommon for employees and IT administrators to clash over privacy concerns and corporate security, especially in BYOD scenarios. In fact, the ability to enforce corporate security policies is the top reason U.S. enterprises decide to maintain their corporate-liable device programs in place of more inclusive BYOD programs. To address this, Android provides IT administrators with one platform and a variety of management tools and options to enable multiple deployment scenarios with ease:

- Work profile is a containerized solution for BYOD deployments that maintains a clear separation of work and personal data. IT only has control over the work partition of the device, allowing employees to use their personal devices as they see fit.
• Fully managed device is a mode designed for corporate-only use without a personal partition — IT can see and manage every aspect of the device to help keep corporate data secure.

• Dedicated device enables a dedicated “single use” kiosk experience within a fully managed device. IT has complete control of the device and its content with the ability to lock applications or device functionality for dedicated use.

• Personally enabled work device, also known as a COPE (company-owned, personally enabled) device, merges the personal freedom and privacy of a work profile device while allowing IT to maintain strict control over corporate data and applications as it would with a fully managed device.

The most recent Android 9 release added more management options and functionalities for dedicated devices, expanding use cases to include shift workers and shared devices, multi-app kiosks, and in general, a better work profile user experience. In Android 9, IT administrators will have the ability to show or hide elements of the Android interface, set custom home screens, and populate the UI with specific applications. This will allow for greater flexibility in deployments where devices are shared by multiple users with different workflows or customer interactions. For example, in kiosk mode, devices can be configured to wipe user data at the end of every session. Devices can also be configured for multiple employees who hand the device off at the end of their shift by preserving data between sessions while keeping individual user data fully separated.
CONCLUSION

The evolving demands of enterprise mobility continue to challenge IT decision makers worldwide, and never before have there been more considerations for IT to weigh when selecting the appropriate device for deployment. Employee preference, price diversity, capability, management, form factor, availability, and flexibility are all critical components of a successful mobile initiative, and the Android platform provides solutions for all of these components with a combined ecosystem of devices, software solutions, partners, and developers. Android’s global footprint, ubiquitous user base, and depth of mobile solutions across all enterprise mobility categories make it uniquely suited and positioned for business use.
To learn more about solution breadth 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.