Android for Enterprise
Digital Transformation Opportunity

Phil Hochmuth
Sponsored by: Android
January 2019
IDC OPINION
IDC identifies Android as a strategic platform for enterprises to digitally transform their corporate workforces, key operational functions and tasks, as well as core business models, with pervasive mobile technology. Expanding upon the secure technical foundation and ecosystem Google has built around Android (with OEM and software partners), businesses can take advantage of the extraordinary breadth and diversity of device types, price points and specialized features and functions, which evolve from Android’s open architecture.

IN THIS WHITE PAPER
This whitepaper analyzes the opportunities for businesses to deploy the Android mobile device OS, powered by Google, in large-scale deployments, and across a broad set of use cases. Android is examined in the context of three key pillars of technology consideration for an enterprise mobile operating system: underlying security, flexibility and availability, and management/administration functionality in the context of modern mobile workers’ attitudes around control, privacy and ease-of-use.
For a platform or technology to take off in widespread deployment in most enterprises, functionality, efficacy, pricing and user acceptance are all important aspects. However, security is the most critical factor for the success of any technology or platform in an enterprise. Businesses simply won’t deploy technology they do not trust. This trust must start at the underlying operational security of the technology, and extend to the reliability of vendor maintenance as well as confidence in the technology’s overall extended ecosystem.
Top mobility challenges

Mobility has always challenged enterprise IT and security, dating back to the first days when sparingly-deployed Wi-Fi and USB drives were the main concerns. When the smartphone came on the market, IT professionals, already skittish about increased mobility and portability of end-user technology, became even more concerned.

Today security is the top challenge cited by enterprise IT professionals with regards to mobility, according to IDC’s 2017 U.S. Enterprise Mobility Decision Maker Survey (see Figure 1). Nearly 40% say this is the top challenge to mobility in general, ahead of issues such as complexity of mobile technology, or cost. There’s good reason for concern; businesses now put their most sensitive corporate assets, data and resources at the fingertip swipe of mobile devices, as greater than 70% of businesses in IDC’s mobility survey said they have deployed at least two mission-critical applications on mobile devices.

Figure 1. Top 5 Enterprise Mobility Deployment Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/compliance issues</td>
<td>39%</td>
</tr>
<tr>
<td>Backend system integrations</td>
<td>30%</td>
</tr>
<tr>
<td>Project scope over extended</td>
<td>28%</td>
</tr>
<tr>
<td>Cost overruns, budget issues</td>
<td>28%</td>
</tr>
<tr>
<td>Lack of IT resources</td>
<td>26%</td>
</tr>
</tbody>
</table>

Source: IDC 2017 U.S. Enterprise Mobility Decision Maker Survey (n=501)
There is a lot at stake for businesses to get mobile security right. Regulatory/compliance challenges are the most frequently encountered issues they face with regards to running a mobile-enabled business. While compliance requirements vary widely industry to industry, the key factor with most regulations around IT usage is security of data — from PCI-DSS in retail to HIPAA in healthcare, to the more broad-reaching GDPR in Europe (and affecting most businesses that touch the EU in some form).

Beyond compliance, data loss is still a major issue in enterprise mobility. Employees will lose devices; greater than 40% of U.S. enterprises say they’ve had this issue in the last 12-18 months. However this is a problem most businesses can easily solve with basic mobile device management (MDM, i.e. remote device wipe/reset) and more advanced enterprise mobility management (EMM) functions. However, businesses are increasingly seeing some of their most valuable data in unusual and unwanted places.

A majority of businesses, according to IDC research, have experienced issues with unauthorized access to sensitive corporate data via mobile apps. This can include communications apps sending data in clear text, storing information in untrusted or unknown cloud repositories, or at worst, the transmission or upload of sensitive data to unknown IP addresses or servers.

The lack of management and security controls on devices is part of these problems. According to IDC’s mobility study, nearly half of corporate-liable mobile devices in enterprises are not connected to management and security platforms, such as EMM. The problem is worse with BYOD smartphones and tablets, with fewer than one-third of such devices being managed in the enterprise.
Mobile OS security perceptions

Many businesses look for the path of least resistance, or most recent known-good outcome. This applies to mobile from the perspective of a somewhat blind trust that technology used in the past, without incident, will predict future success in terms of data and IT operational security outcomes.

According to IDC’s mobility study, among businesses that deploy corporate smartphones, Apple iOS is the predominant brand of devices businesses hand out to employees. This is also reflected in device shipments — among the 11.8 million business smartphones shipped in the U.S. in 2016, 57% were iOS vs 41% Android based on IDC research.

According to IDC data, there is also no correlation between device OS types and frequency of mobile security incidents involved. Among the top 4 data-related breach incidents enterprises said they experienced in 2016, the numbers do not shift significantly when analyzing subsets of companies employing different mobile operating systems. (Between 35%-40% of respondents from both “Android-majority” and “iOS-majority” businesses said they experienced mobile data loss incidents and other security incidents.)

Reports in the media and blogosphere also create a negative perception around Android. News of the latest Android kernel exploits, with ominous-sounding code names — Stagefright, QuadRooter, Dirty COW — spread quickly. Whether a real threat or not, cumulative reports on the weakness of Android OS code and apps, or overall mistrust of software downloaded from Android app stores, can stick in the minds and perceptions of many IT decision-makers.
Data and facts behind Android security

While perception and instinct guide some initial thinking around business technology choices, data and facts ultimately drive many more decisions. And the data and facts on Android security actually line up much more in favor of the mobile OS than against it.

Android is the most popular mobile OS on the planet, with over 2 billion active Android devices in use, according to Google. Shipment data on Android devices from IDC research shows a worldwide increase of 130% over the past 7 years, with commercial shipments growing 57% over that time period. Many businesses are thriving with majority-Android device deployments. Among such businesses, 50% said their mobile deployment efforts met expectations, and 47% said they exceeded expectations.

Another outdated Android perception is that malware is pervasive across Android app stores, and on installed devices. Google’s data show that fewer than .001% of apps in the Google Play store are malicious, which has been at a consistent threshold over the past 3 years. According to Google’s more recent Android security report, from 2016 to 2017, the frequency of potentially harmful apps installed on devices sourced from

Android is the most popular mobile OS on the planet, with over 2 billion active Android devices in use, according to Google.

50% said their mobile deployment efforts met expectations, 47% said they exceeded expectations.
Google Play decreased from .04% to .01% (among Android users that activate additional installation limiting controls on devices, the presence of unwanted software drops to .005%). Through Google Play Protect Service, Android now provides active feedback resulting from “on-device security” scans that happen continuously in the background in the form of visible messages on the health status of devices. Apps installed from the Play Store will be visibly marked as “safe,” or scanned as a result of the rigorous vulnerability and malware inspection processes of the Google Play Protect service.

Google’s security success has been a two-fold strategy; one is removing unwanted apps from the Google Play store via vigilant monitoring of the code and app behavior; the other is constant iteration and improvement in the underlying Android operating system. This work continues in the latest versions of Android, the eighth and ninth major version releases of the software named “Android Oreo” and “Android Pie” respectively.

A major security focus in Oreo was the reduction of the attack surface of the Android kernel, along with an application and services whitelisting framework for external system calls to the OS kernel. Beyond kernel hardening, Google also addressed recurring bugbear vulnerability in Android — the “mediaserver” software stack for processing audio/video files (the target of the widely publicized 2015 Stagefright exploit). Oreo furthers the mediaserver hardening in N, or Nougat, by protecting each individual subprocess of the whole framework, strictly limiting the types of data that can be passed between modules in the stack.

Some additional new security features and capabilities in Android Oreo are:

- **WebView running in an isolated process in a tight sandbox that protects the rest of the system from attacks that originate in untrusted web content**
- **Rollback protection, preventing the device from booting if it is detected that its OS has been rolled back to an earlier version of Android**
- **Extending tamper-resistant hardware support on devices, which can be used to perform PIN/pattern/password checks and make it harder for a physical attack to bypass the lock.**
Google’s years of iterative security improvements continues with the 2018 introduction of Android Pie. Android Pie introduces a number of features that address enterprise security needs:

- The ability for IT administrators to require different PINs and timeout rules for personal and work profiles
- Additional policies that can prevent data sharing across work and personal profiles
- New APIs that work with keys and certificates to securely identify devices accessing corporate resources.

While these are some of the key highlights, there are many other security-focused APIs and features that will benefit those using Android as a company-issued device or personal device with the work profile. View more details on the full set of security enhancements at the Android developers site.
What enterprises expect from a mobile OS

Enterprises do not expect any IT product or technology to be perfect from a security standpoint. But they do expect quick fixes when weaknesses or exploits are discovered. Enterprise IT and security teams want upgrades; newer always equals more secure, and the constant stream of security-related software upgrades pushed from vendors makes enterprise IT conditioned to seek the latest upgrades and software fixes for all systems. Enterprises are used to receiving frequent decimal-place upgrades and software pushes, often with incremental security fixes, sometimes to only one or two facets. Cumulatively, this breeds the perception that other vendors have mastered the security/upgrading cycle with their closed ecosystem, and perpetuates the perception of better security.

Leveling barriers for OEMs to get the newest, most secure Android

One of the criticisms of Android in the past wasn’t that developers were not working to make the OS more secure and stable. It was that their efforts were too slow to market in the form of device upgrades and distribution of patched software to devices. This was a particular challenge to Android, as the ecosystem of devices is numerous: over 1,500 brands with more than 16 times as many individual device types.

To reduce cost/time/effort required for device OEMs to upgrade to the latest Android version, Google began Project Treble — a broad effort to streamline the process for Android handset OEMs to validate and update their hardware for the latest version of the OS. Treble re-architected the way that framework and device-specific vendor hardware components (silicon from Qualcomm, MediaTek, etc.) communicate with each other. In the past, OEMs had to work with silicon makers to validate each new Android OS framework update at the chip level. Treble creates a standard vendor interface for lower-level components to talk to the OS framework; OEMs and chip makers no longer have to rework this low-level code upon each release, speeding update times. This strengthens security, as the need for the framework to directly access the kernel drivers that control hardware is removed, enabling stronger sandboxing and making it harder for a framework compromise to exploit the kernel. Ultimately
this decreases the effort required of device makers to test and validate new updates to Android, allowing the latest "x" releases, as well as major "dessert" upgrades, to get to thousands of device types within days of the code push from Google.

**Trust in OEMs and partners**

Vendor partnerships play a strong role in promoting trust and reliance among enterprise customers. No single vendor has mastered security in its respective domain, and businesses require technologies to interoperate and work together from both a functionality and security perspective. Mobility is an extremely diverse market with thousands of OEM vendors and exponentially more mobile app and software creators. But from an enterprise perspective, most businesses lean on a few top IT solutions providers from an infrastructure and security standpoint.

According to IDC’s mobility survey, enterprises rank carriers, systems integrators and device OEMs 1, 2 and 3 respectively in terms of their most trusted partners with regards to enterprise mobility hardware projects and management. As shown in Figure 2, enterprises rank mobile operators, system integrators, and device OEMs as their most trusted partners for mobility software projects. Because of the interdependency of services, devices and software with regards to mobility, each type of provider/company is important to enterprise mobility success.

*Figure 2. Trusted Advisors in Mobile Software Deployments*

**Source:** IDC 2017 U.S. Enterprise Mobility Decision Maker Survey (n=501)

Q. Which type of suppliers do you consider your prime supplier or ‘trusted partner’ for mobile software selection and deployments?
Security benefits of open OS architectures

IDC considers open systems to generally be stable and secure platforms for enterprise computing, which allow for easier technology integrations. Rather than being an enigmatic "black box" to enterprise security, management and productivity technologies, Android’s open nature allows for deeper integrations with third parties, which makes the platform more secure, dynamic and, ultimately, of greater value to an enterprise deploying the technology.

With Linux as the underlying kernel of Android, the mobile OS enjoys the benefits of an extremely large community of professional developers, threat and vulnerability researchers, and curious hackers (the good kind) with eyes on the core system source code. Google works with app developers to improve the security of their apps. The App Security Improvements (ASI) program notifies developers about vulnerabilities affecting their apps in Google Play. Since 2014, the ASI program has supported the discovery of 27 different types of vulnerabilities and fixed nearly 383,000 vulnerable apps in Google Play. With the tremendous number of kernel OS developers, both professional and volunteer software maintainers are able to discover new vulnerabilities in the Android software stack quickly, and contribute patches and fixes back to the community. This goes beyond baseline security; the legion of open-source developers improving the Android kernel, along with Google’s own in-house development team, creates a more stable, functional and dynamic mobile OS.

The external community specific to security is also large; more than 200 independent Android security researchers, white-hat hackers and other analysts constantly probe and pry at the Android code base for weaknesses, and work with Google to quickly implement security updates and fixes. This robust open security ecosystem around Android, in part, makes the OS a victim of its own success from a reputation standpoint,
as vulnerabilities in the Android ecosystem gain quicker media attention and publicity in general. This is, in part, the basis for Android’s past reputation as a less-secure OS platform. But the fact is the code is more secure because of this environment.

Aside from improving the code itself, Android’s open nature — advanced via the Android Open Source Project — has distinct advantages from a technology integration standpoint, which directly benefits enterprise customers. Working with security technology partners at the device, app and network levels, Google and Android OEMs can offer partners deeper levels of access to core OS functions, such as monitoring activities and behaviors on devices from the OS and processor level to the network layer. Such integrations can lead to advanced mobile endpoint traffic monitoring, on-device heuristics and behavior analysis, and intra-application and app-to-OS communications monitoring beyond what’s possible with more closed competing mobile operating system technologies.

Such Android-exclusive integrations include Cisco’s ability to monitor Android application packets at the network level for anomalous/unauthorized behavior and activities, as well as integrations with vendors such as Symantec and Zimperium for monitoring specific Android activities at the processor and memory level on devices.

These types of integrations can provide enterprises greater levels of visibility and situational awareness of real-time mobile device usage. Such integrations can be fed into security information and event monitoring (SIEM) platforms for enterprise threat analysis, as well as into proactive enforcement systems, such as Network Access Control and on-device remediation tools to help control unwanted mobile user behavior.

To improve upon and foster these types of multi-vendor integrations, Google uses its own sophisticated technology resources and capabilities, such as machine learning (ML), used widely to identify malicious or potentially harmful applications (PHAs) installed on devices, or in terms of anomalous behavior of smartphone activity or resource utilization. Google can share intelligence gleaned from these types of advanced detection techniques with integration partners to help improve security and compliance. Additionally, Google’s compute scale and sophistication also allow the company to massively simulate and test how partner software and technologies interoperate with Android iterations, as well as specific devices, such as Pixel phones.
With a baseline of trust in Android established, enterprises can take advantage of the flexibility and availability of a broad ecosystem of device makers and OEM partners. This goes beyond simply putting more devices into the hands of employees, and touches on broader trends in digital transformation with a more flexible, dynamic and manageable mobile workforce.
Mobile device use cases everywhere: digital transformation is mobile enablement

According to IDC’s 2017 Mobile IT Administrators Survey (sponsored by Google), 77% of enterprises said that the number-one spending priority from a mobility perspective was devices. However, this intent goes beyond simply getting more devices into the hands of executives, sales teams and knowledge workers. Deployments of ruggedized and company-owned, single-use (COSU) devices are on the rise. Android, in particular, is the growth engine in the market, with shipments of Android ruggedized/COSU devices forecasted to grow at 12% CAGR over the next 5 years — 3x the rate of the ruggedized market overall based on IDC research.

Nearly two-thirds of enterprises have these devices deployed, according to IDC data. And nearly three quarters of enterprises plan to deploy technology to manage COSU deployments in locked-down roles such as kiosks, ATM machines, retail POS, and other function-specific tasks. Not all of these devices will be flagship smartphones, traditionally targeted at mobile knowledge workers. And such hardware is much less likely to be an employee’s personal premium-brand BYOD smartphone. Digital transformation of traditional workflows, functions and daily business routines will mean deployment of COSU devices at scale, where cost, security and manageability will be three critical components.

From an OEM perspective, this can involve specialized hardware built for ruggedized environments, or with built-in or integrated peripherals for specific tasks and roles (i.e. card readers, specialized sensors and other instrumentation, etc). OEM diversity also allows enterprises to control costs. A business may be replacing a fleet of aging PC-based POS machines with tablet- or smartphone-based hardware. However, these replacements are much different than mobile worker enablement. Economically, businesses will balk when scenarios get broader in terms of digital/mobile enablement, such as handing out tablets instead of paper clipboards in medical or logistical scenarios where cost sensitivity becomes even greater. A business is willing to accept marginally greater device deployment and support costs in digital transformation scenarios, but replacing clipboards with $800 mobile devices is not economically feasible.
Many digital transformation use cases are in retail, where so called "mobile clienting" approaches provide floor representatives with a full-blown smartphone or tablet for mobile enablement, replacing a $50 headset or walkie-talkie. New device-centric use cases also extend to other industries, with examples including (but not limited to):

- **Healthcare**: Secure clinician text messaging; tablet/mobile cart-based telemedicine and telepresence; healthcare kiosks/patient check-in
- **Energy, Oil & Gas**: Augmented maintenance (tablet- and AR-based)
- **Manufacturing**: Real-time assortment monitoring (tablet/smartphone); factory floor management/data entry (tablet/smartphone)

**Pricing diversity puts Android everywhere**

Pricing diversity of mobile devices makes it possible for enterprises to address a broader range of digital transformation scenarios, from full knowledge worker mobile enablement (up to PC/laptops replacement) down to basic task-work devices and even digital signage and interactive displays.

For businesses supporting multi-national/multi-regional workforces, device and brand preference can vary widely by region. Price sensitivity of mobile devices is especially a factor for organizations with a workforce in developing or less economically-developed countries. Workers making one-third the salary of workers in another region cannot be expected to bring their own devices with near-$1000 price tags. Businesses will have to accept diversity and heterogeneity of mobile OS and OEM smartphone brands.

A business may support a range of device ownership/deployment models across regions. For instance in Europe, where BYOD is much less common than in North America, an organization may have to adopt a choose-your-own or corporate-liable model of Android devices across brands not as known or widely used as in North America. Whereas in APAC, where BYOD is more widely accepted, businesses should be prepared to have a more diverse set of devices — again a more data/identity-centric approach to mobile worker security, provisioning and resource management.
Device choice trends in enterprises: programs that drive the balance of user productivity & IT requirements

Device choice, whether the permission of BYOD, or choose-your-own device deployment (CYOD) plans, is gaining in popularity among enterprises.

According to IDC’s mobility study, device choice correlates with mobile deployment success. Among organizations with CYOD installed, 89% said their overall enterprise mobile app and device deployment efforts were successful. For non-CYOD firms, 70% described their efforts as successful. Similarly, no CYOD-deployed firms said they “failed” in their mobile efforts — while 15% of overall respondents described themselves this way.

Multi-national and multi-regional enterprises — businesses based in the U.S. 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 vs 36% of non-MNOs). Among firms adopting CYOD, 77% said Android is the most popular OS platform chosen by end-users.

An open software architecture drives ecosystem innovation

Overall, the open ecosystem of Android drives a more diverse ecosystem of devices, device types and categories which can address the varying requirements of enterprise digital transformation.

IDC sees Android as being poised to transform enterprise business processes, models and overall operations similar to how Linux transformed the IT industry, first in corporate datacenters, then in the cloud, due to low cost and open-sourced licensing, architectures and application interfaces. The availability of Android, and its diverse form factors and wide-spread ecosystem, makes the platform a ubiquitous, connected computing platform for users interacting with on-device and cloud-based applications and services.
Google’s platform and global scale make many devices enterprise-ready

A key consideration for large enterprises and multinational organizations is the scale Google brings to its support around Android. As ubiquitous and far-reaching as the platform has become, Google has the capability to transform a wide range of modern Android devices into a business-class and enterprise-secure mobile computing platform. This includes Android devices running version 6.0 (Marshmallow) or higher that are certified for Google Mobile Services (GMS, a set of standard Google apps and APIs). These certified devices are deployed in wide range of scenarios — from mobile worker and personal productivity scenarios, to single-use deployments in task-oriented use cases.

This far-reaching capability is as ubiquitous, and available, as Google’s most well-known services, such as search, maps and mail. The Android update platform leverages Google’s massive global footprint of data centers, network capacity and software intelligence. When an Android device is enrolled and personally enabled (either BYOD or corporate-liable), the process automatically creates separate secure user spaces on a device, with strong data separation and management capabilities. This is known as the work profile.

Also, enrolled devices take advantage of Google’s back-end security scanning as part of the Google Play Protect service. This includes a massive security intelligence engine from the combination of its gathered device telemetry — over 2 billion devices sending data on state, vulnerabilities and other critical measurements and statistics — coupled with Google’s expertise in machine learning and big data analysis.
A secure mobile platform, with diversity in form factor, regional availability and price, is only as useful to a business relative to the level of adoption, user acceptance and utilization of the technology. In order to transform how the business and workforce operate with mobile technologies, enterprise IT must find the balance between strong, secure device management and policy enforcement and user acceptance.
User resistance is the most-cited reason why devices used in business are not enrolled in enterprise mobility management platforms in enterprises. Among enterprises with EMM deployed, 43% cited this as an issue (see Figure 3).

**Figure 3.** Top 3 Enterprise Mobility Management Challenges

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>End users do not want personal devices managed by a corporate EMM platform</td>
<td>45%</td>
</tr>
<tr>
<td>Software licensing costs/can’t afford to manage every device</td>
<td>42%</td>
</tr>
<tr>
<td>End users do not want personal devices managed by a corporate EMM platform</td>
<td>25%</td>
</tr>
</tbody>
</table>

*Source: IDC 2017 U.S. Enterprise Mobility Decision Maker Survey (n=501)*

To address some of these issues, the Android OS lets enterprises provision, control, and secure an end-user’s entire mobile business computing environment without having to install another layer of app containerization or side-loading customer apps on devices. The Android OS provides strong separation of personal and work data, where personal and work profiles coexist. The work profile enables enterprises to create a separate, secure container on users’ devices where apps and critical company data are kept secure and separate from personal information. The work profile contains all managed apps provisioned, secured and controlled by the business. These are easily identifiable as work-related apps and notifications are labelled with a briefcase icon. Work and personal apps can be arranged in any way according to user preference within the launcher. This does not affect the data separation of the apps.

To help IT teams enroll more devices, Android zero-touch enrollment allows smartphones/tablets to be automatically provisioned out of the box (e.g., EMM enrollment) without IT staff having to come into physical contact with devices.
When setting up zero-touch enrollment, IT administrators can access a configuration portal which allows for the pre-configuration of devices. This can include automatic enrollment in enterprise mobility management (EMM) platforms once devices are activated.

Managed Play provides an IT-department curated enterprise app store for employees and also the ability for IT to push install and remotely configure apps on managed devices. Managed Play provides built-in hooks to validated EMM platform partners, allowing for non-wrapped mobile apps to be deployed to devices, and managed via native controls in Android. This simplifies the app deployment and management process, and provides a more seamless and consumer-like experience for end-users.

Beyond providing a better experience for the end-user, the Android and Google Play Store approach can save time for IT departments by not requiring apps to be wrapped or run through an SDK for adding additional security controls and management hooks. This frees up time and resources of IT teams and app developers to focus on more productive and business-centric tasks.

Navigating and downloading apps from managed Google Play is similar to the consumer-focused Play Store experience. Android users will need no special instructions on how to find or download new apps required for business. Enterprises can also easily mix private applications and off-the-shelf apps in this environment. This is a critical feature for businesses, as distribution of custom apps is still a challenge for over one-third of enterprises, even if they have an EMM solution in place. For enterprises using EMM, managed Google Play can simplify distribution of apps onto employees’ devices.
CONCLUSION

Now, over a decade now into the smartphone era, mobility is still a game-changing technology, both from a business and digital transformation standpoint, and from an IT operations, deployment and security perspective. This requires close scrutiny and attention to any new mobility technology introduced into a workforce, business process or overall enterprise use case. To that end, enterprises should evaluate mobility technologies — from devices and OS/app software, to management and security platforms — based on the three pillars of enterprise mobility requirements: security, flexibility/availability, and IT/user experience. From this perspective, the security, flexibility and manageability of Android make it a strong choice for standardization and/or pervasive mobile deployment for businesses across a wide range of industries and diverse a set of use cases.
To learn more about security 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.