IDC OPINION

Android is a highly-secure device operating system. It is based on fundamentals of separated system processes, trusted OS architectures, and is backed by a powerhouse of advanced threat analytics, machine-learning-based analysis and cloud processing power exploring different techniques and leveraging new knowledge from all across Google. Given these factors, businesses should carefully consider the facts and data around the state of the inherent security strengths and capabilities of Android as well as its broad ecosystem and IT security industry partnerships and integrations.

IN THIS WHITE PAPER

This IDC whitepaper analyzes the most pressing mobile security challenges facing enterprises today, in the context of commonly held perceptions about mobile security in general. This report aims to debunk some myths around mobile security, and looks at some of the advanced, preventative security measures Google takes to control malware and compromised devices across its ecosystem. In the final section, the paper provides enterprise IT professionals with a framework for thinking about how to best adopt Android in enterprise mobility deployments and put its security features and supporting services to work.
Security challenges facing enterprises

Many businesses will soon widen their mobile technology deployments with more deployed devices and advanced use cases, according to IDC’s 2017 U.S. Enterprise Mobility Decision Maker Survey. The majority of enterprises plan to spend more money on mobility over the next 2-3 years, with an eye towards digital transformation. Instead of chasing new mobile trends and employee habits, businesses want to harness mobile technologies to make real productivity and efficiency gains.

Even as enterprise mobility matures, security remains a top concern and barrier to deployments, according to IDC’s mobility study. Compliance challenges, lost/stolen devices, and unauthorized access to sensitive data via mobile apps are among common issues businesses face when deploying mobility (see Figure 1).
The idea that a company’s most sensitive data and systems are a few finger-taps away is a concern for many IT security and risk professionals. This is why mobility in general comes up as a top security challenge, and makes IT decision-makers skittish about the technology. If there’s any doubt as to the integrity or security underpinnings of the platforms they look to support, enterprises move to the safest perceived path.

BYOD, shadow IT and the blurred lines of personal & work

Bring your own device (BYOD) is prevalent in most businesses; 84% of U.S. enterprises IDC surveyed said they allowed at least some degree of personal device usage in the workplace. While BYOD adoption varies by region (i.e., lower in Europe, higher in APAC), use of personal technology in the workplace is a trend touching most IT departments. While BYOD helps businesses reduce costs and can improve employee satisfaction, it
can also be a security challenge. According to IDC data, enterprises with large BYOD deployments experienced more frequent security issues. Among organizations with predominantly BYOD deployments, mobile security incidents were 10-12% more frequent than the survey mean (40%). Among firms limiting or barring BYOD, response rates of security issues were lower than the mean by 7%.

The blurred work/personal technology boundary extends beyond devices to apps and cloud services as well. Users commonly bring to work personal or preferred mobile apps, cloud storage, SaaS apps and other technology which they feel makes them more productive. According to the 2017 IDC Mobile IT Managers survey (sponsored by Google), more than 70% of businesses in the U.S. and Europe allow some degree of shadow IT in their organizations. These firms realize that a permissive, but watchful approach to non-corporate cloud and app technologies used by employees can drive productivity and increase user satisfaction.

Mobile security perceptions & reality: FUD vs facts

Security is often a major blocking objection around wider Android use in enterprises. But the narrative and state of Android security, as told through technology news and the blogosphere, does not stand up to facts and analysis of data on the presence of malware, rooted/unsafe devices or Android vulnerability growth or prevalence.

According to CVEdetails.com, which aggregates reported vulnerability disclosures in software products, the total number of vulnerabilities discovered for any given operating system can vary widely year to year. While the number of reported Android vulnerabilities rose in 2017, so did the the number of reported vulnerabilities among all major end-user device OSes. Meanwhile, the percentage increase for discovered vulnerabilities in Android was one of the lowest among all major computing device OSes (mobile and PC) used in enterprises, according to CVEdetails.com.
Over the same time period (2009-2017) the total number of vulnerabilities reported for all actively-supported PC operating systems (Windows and Mac) was more than double the number for either Android or iOS. Following the money, in terms of security technology spend, also shows where enterprises see the real end-user threat. According to IDC PC shipment and endpoint security market data, nearly $40 was spent on security software for each of the 260 million PCs shipped in 2016; shifting this lens to mobile, only $0.16 was spent for each mobile device shipped that same year (1.8 billion devices).

Standardization on a single OS within an enterprise (e.g., majority iOS or Android) does not lower rates of mobile security incidents. One-third of enterprises in IDC’s mobility survey said their company experienced leaked or exposed data as a result of mobile app usage incident, and 40% saw incidents of unauthorized access via mobile. Analyzing the data by predominant OS type (organizations identifying as predominantly Apple or Android-only shops) revealed no significant difference in the rate of security incidents experienced.

The specter of mobile malware may be the ultimate strawman in terms of enterprise mobility and mobile security threats. While security is still the top concern among enterprises, according to IDC’s 2017 mobility survey (nearly 40% cited this as a concern) mobile malware is not a top-of-mind challenge for the day to day incidents businesses face. In 2017, fewer than one-third of enterprises experienced such a security incident.
Myth-busting Android OS insecurity notions

For its part, Google’s continuous scanning and identification techniques for detecting potentially harmful apps (PHAs) has improved Android security by multiple measures. According to Google data, from 2016 to 2017, the frequency of PHAs installed from Google Play on devices decreased from .04% to .01%; this is approximately one out of every 60,000 Android devices in the world having a PHA detected.

A note on PHAs: although malware is included in the definition, these are broadly-classified as any app which may execute undesirable actions. This could include an app which grants more permissions than expected, often an app development oversight than an intentionally malicious action. As for actual malware, the presence of such software is nearly infinitesimal. Ransomware, for example, was found on one in 300,000 Android devices worldwide. These numbers also declined rapidly over the past year: the number of installed Trojans detected dropped by 51.5%, hostile downloaders dropped by 54.6%, backdoors dropped by 30.5%, and phishing apps dropped by 73.0%.

Another Android security myth is the perception that rooted devices are widespread among the OS installed base. A rooted devices is one in which the operating system has been modified to grant OS permissions and access beyond normal end-user usage. Rooted devices are generally untrusted by enterprises, as they break down the inherent data/app sandboxing and isolation of processes on smartphones, and make them more susceptible to malware and unwanted software.

The presence of malware software on Android devices is nearly infinitesimal.
Android detects rooted devices via its Google Play Protect Attestation API. Per Google data, this API — invoked over 200 million times a day to test the worldwide installed base of Android devices — reports that fewer than 6% of the 2 billion devices in the world are rooted (Figure 3). This includes devices intentionally rooted by users, or devices sold as rooted devices. Installation of software that intentionally roots devices was detected at less than half of a percent of all devices.

**Figure 3.** Detected rooted Android devices worldwide

![Detected rooted Android devices worldwide](image)

*Source: Google, 2017*
App security on devices, in the cloud and in between

While Android devices have strong security underpinnings, a range of cloud-based services support Android devices to further strengthen and secure the platform overall. Google Mobile Services (GMS) is a package of apps Google licenses to third-party Android OEMs and partners, which allows for easy and controlled pre-installation of apps such as Gmail, Hangouts, Maps, Photos, YouTube, the Google Play Store, and other core Google apps. Less obvious to Android users are the underlying security capabilities that come with GMS. Any device licensing GMS also gets device- and cloud-based anti-malware and security scanning features — an underlying set of services and functions called Google Play Protect. These range from on-device scanning for PHAs and app exploits, to the Find My Device app (formerly Android Device Manager) for finding lost or stolen devices and rooting detection. Google Play Protect includes a set of APIs which interact and broker information among apps on devices, built-in device security functions, and cloud-based security and intelligence services. In 2017, Google Play Protect automatically disabled PHAs from roughly 1 million devices. Google reviews all apps before publishing them in the Google Play store. In addition to reviewing apps submitted to Google Play, its cloud-based systems look for apps in publicly available sources. Google Play Protect also reviews the apps it finds outside of Google Play for PHAs. According to Google, Google Play Protect prevented Android users from installing a PHA from outside of Google Play about 1.6 billion times in 2017. Google Play Protect encompasses all the security protections that have kept Android users and devices safe behind the scenes for years. For example, the Verify Apps service in Google Play Protect scans apps for PHAs before users install them, regardless of their origin.

In 2017, downloading a PHA from Google Play was less likely than the odds of an asteroid hitting the earth, according to Google.
AutoScan is another service which checks Android devices daily for PHAs and other signs of tampering. (This service scanned nearly 800 million devices per day last year, touching devices as diverse as smartphones, tablets and TVs running Android.) AutoScan works with Verify Apps as part of Google's multi-layer scanning approach to Android software and security. If AutoScan detects PHAs or other risk indicators on the device, it can trigger an added local Verify Apps scan to dig further into the issue.

While Google's device/cloud-based security architecture provides strong protections, it has largely operated behind the scenes to end-users. Google Play Protect was introduced in May 2017 to expose this functionality and help users understand the health state of their devices. Google Play Protect provides active alerts to Android users as to when scans happen on a device, the security state of each app viewed in, or downloaded from, the Google Play store, and the overall app health of the device. Table 1 summarizes Android's security features, APIs and initiatives.

Table 1. Android security tools, API and ecosystem initiatives

<table>
<thead>
<tr>
<th>Tool/Initiative</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play Protect</td>
<td>A powerful threat detection service that actively monitors a device to protect it, its data, and its apps from malware.</td>
</tr>
<tr>
<td>SafetyNet</td>
<td>A set of Google Play Protect APIs that protects apps against security threats. This series of APIs can mitigate against device tampering, bad URLs, PHAs, and fake users.</td>
</tr>
<tr>
<td>Google Play app review</td>
<td>Google's app distribution platform for Android. Together with Google Play Protect, the Play Store has policies in place to protect users from attackers trying to distribute PHAs.</td>
</tr>
<tr>
<td>Vulnerability Reward Program</td>
<td>Google works with hardware and carrier partners to quickly resolve security issues and push security patches. It also encourages and rewards researchers who find, fix, and prevent vulnerabilities on Android and pays developers when they contribute security patches to popular open source projects.</td>
</tr>
</tbody>
</table>
Spreading software updates quickly is a challenge in a device ecosystem as diverse as Android. Google disperses critical security updates via GMS, as this service operates independently of carrier or OEM software versions of Android. It can push new software as soon as new threats are discovered. Beyond critical updates, frequent underlying OS upgrades also keep users safe and productive. To that end, Google launched Project Treble in 2017 to make its underlying OS services stack more modular and uniform, allowing for easier implementation of software updates for carriers and device OEMs.

Treble changes the framework for how the Android OS and device-specific vendor components (silicon from Qualcomm, MediaTek, etc.) communicate with each other. This solves the problem of rapid updates by streamlining the process where OEMs work with silicon makers to validate new Android OS updates. 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 up update times. This strengthens security, as the need for the framework to directly access the kernel drivers that control media playback is removed, enabling stronger sandboxing and making it harder for a framework compromise to exploit the kernel. (However, enterprises can also intentionally delay OS updates on devices supported by the Android Enterprise Recommended program, to allow IT teams to test and update apps to run on the latest version of Android.)
Android: Security at the OS core

Android’s underlying platform for process, data and app sandboxing is based on SELinux — or, Security Enhanced Linux, to enforce mandatory access control (MAC) over all processes and apps system, therefore designed for workloads requiring strong security and high availability. The software operates by a least-trust principal, which limits permissions for applications or processes to share data or other resources, unless explicitly configured in the operating system’s settings. This extreme locked-down version of Linux is among the most secure operating systems available, according to numerous third-party security experts and researchers.

Verified Boot is another least-trust principled service in Android. Verified Boot mitigates attacks against devices by providing a boot process that verifies system software using a hardware root of trust. This makes it more difficult for software attacks to result in a persistent OS compromise, and provides users with a safe state at boot time. This stops persistent installation of rootkit software — cleverly-crafted, malicious code which can hide from detection scans and ultimately run any code or process on the device, or steal data from any app. Each phase of the boot process verifies the integrity of the subsequent phase, prior to executing that code. Any break in the trust chain prevents the device from booting, and alerts the user that something is wrong with their phone or tablet.

Cryptographic hashing and keys also underlie other Android security features such as full-disk or file-based encryption, and trusted execution environments. Full-disk encryption (standard on Android 5.0 or higher) protects the entire contents of a phone, from OS to apps and data; only the user’s PIN/password can unlock it. File-based encryption allows for the same protection along with a better experience and finer granularity, for example to use different keys for a work profile. Underlying all of these structures is a Trusted Execution Environment (TEE) which is a secure area of the main processor on Android phones that isolates and protects sensitive information such as key material away from the user operating system. Additionally, some Android devices also leverage a separate security module which is analogous to a Secure Element (SE) which completely isolates cryptographic operations on to a separate tamper-resistant chip that has its own CPU, memory, and secure storage.
Security applications of Google-scale computing power

Google has large and sophisticated deployments of machine learning and data analytics in the IT industry. These technologies power intelligence and automation capabilities to a wide range of commercial and consumer services and platforms. Google has integrated this powerful ML engine with the Google Play Store and Android device scanning architecture to accelerate and automate the finding of threats in code which users could potentially download and install.

The Google Play Protect system, which provides a wide range of security checks on Android, also feeds Google's extensive ML and data analysis engines with telemetry data from over two billion Android devices to create a real-time snapshot of the health state of the Android ecosystem. In 2015, Google used its extensive cloud computing capabilities to spin up what it calls its Anomaly Correlation Engine (ACE) — a ML-based system that feeds off of Google Play Protect data and other inputs to detect changes in app behaviors on installed devices and predict if an app could potentially be malware. If the app is determined to be malware, ACE finds and removes the software from devices, and from the Google Play store before it spreads widely.

Though rare in actuality, rooted devices are a major concern to enterprises. To decrease likelihood of device rooting, Google trained ACE last year to specifically detect the most dreaded type of malware infection on a device — apps that root Android phones without the user's knowledge or awareness. This malware inserts other bits of code on rooted devices to intercept communications and steal data. A specially-designed neural network trained ACE to look at the multi-stage nature of rooting/take-over malware leading to 90%-level detection of these sophisticated PHAs in lab tests and on the live Google Play store.
Beyond rooting detection, Google’s ML-based techniques are applied to other types of PHAs and exploit families to block the installation of the code in the first place, or to detect and remove the code if it had previously eluded detection. Google created a statistical baseline for Android app behavior to determine when software behaviors fly off the handle -- i.e. a seemingly benign or mundane app making strange calls to the Android kernel or other types of anomalous activity. Google used these techniques to preemptively block installation of some of the most dangerous malware — HummingBad, Ghost Push or Googlian — with between 92%-99.9% accuracy.

Google’s extensive cloud-based ML analysis and detection capabilities make Android one of the most sophisticated threat analysis, detection and remediation platforms in the market. Proof of this model’s success is in the statistics on malware reduction in the Google Play Store and on devices:

- Fewer than one-tenth of one percent of PHAs detected on installed devices
- 50%-70%-plus reduction of installed Trojans, hostile downloaders and backdoor malware
- More than 94% of the two billion Android devices passing system OS integrity checks

These data points, the steps and safeguards Google has in place around Android, and the inherent safety in the OS itself, disprove most notions that Android devices are major vectors for malware in an enterprise, or that the devices themselves are easily susceptible to compromise and rooting.
Patching the world in faster-than-hacker time

Enterprise security often comes down to a patching race, where administrators rush to apply the newest software code and updates to systems and apps before vulnerabilities are discovered and exploited. From a mobile security and management perspective, this means having the latest software on devices from carriers or OS suppliers. Increasingly, businesses are adopting strict rules around mobile device access based on installation of software updates.

Google regularly updates the Android Open Source Project (AOSP) code base with the latest security patches. It issues a series of frameworks, testing suites and best-practices outlines for all types of developers and technical teams that may come into contact with the source code — device OEMs, chip and subsystem component vendors, mobile operators and developers writing apps to run safely in Android environments. These efforts resulted in more than a quarter-million security-related upgrades to apps in the Google Play Store in 2017.

Accelerating this Android security update cycle is Google’s Android Enterprise Recommended program for OEM device partners. In AER, partner devices will have the latest OS patches and updates pushed to devices within 90 days of release. This 90-day update guarantee spans three years from the time the device is activated and extends up to five years for rugged devices.

Google also works closely with key enterprise mobility management (EMM) partners to integrate device-level controls for Android-based phones and tablets. Based on the health markers and data Google provides via Google Play Protect, businesses can create EMM policies to control what an Android device can connect to and see on a corporate network. For example, all Android smartphones not updated with a specific level of security update could be blocked from accessing a business VPN, and a specific corporate app. Such EMM controls can also come into effect if a device falls below a certain risk threshold in terms of PHA presence.
Oreo and Pie build on foundation of previous security improvements

Google’s years of iterative security improvements continued with the 2017 introduction of Android 8.0. Called Oreo, it brought a wide range of security features and capabilities, both at the fundamental OS/kernel level, and in terms of new security services and features.

A consistent effort in each Android revision is hardening the underlying Android kernel. Oreo reduces the attack surface of the Android kernel with a whitelisting framework for applications and services. Only approved kernel calls will be able to make kernel calls, limiting kernel exposure to potentially malicious activity. Oreo also protects against rogue lock-screen functions — sometimes used in mobile ransomware attacks — by removing the ability for any app to gain privileges to change a device’s passcode, or preventing an app from covering the unlock button or lock screen with blocking software.

A roll-back protection concept is also part of Oreo. If a device reverts to an older version of Android (once Oreo is installed, or if the device comes out of the box with Oreo) the system will prevent the phone from booting to protect against other attacks or activities that may try to take advantage of the absence of security features or measures not present on pre-Oreo Android builds. Further enterprise-focused improvements in Oreo also include expanded support for wireless (Bluetooth/NFC) second-factor authentication devices, such as FIDO-based fobs and keys such as YubiKeys.

In 2018, Android 9.0 Pie introduced 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.

Managed Google Play and zero-touch enrollment put Android to work

Google Mobile Services, Google Play Protect and Google Play features touch over 2 billion Android devices regardless of version. These features are broadly targeting both consumer and business users. For enterprises, all of the security capabilities and features behind Android’s protection architecture can also be delivered via a business-focused app store experience, in managed Google Play. This platform allows enterprises to control what Android apps (public and privately-developed) users can access, and how the apps are used once downloaded. Managed Google Play provides these management and policy enforcement controls without any developer intervention (i.e., alteration or add-ons to app code).

Businesses looking at large-scale Android deployments should consider managed Google Play as a strategic platform for providing users with both in-house and third party applications that enable worker productivity. According to the IDC/Google IT admin survey, more than 74% of businesses consider quick and secure app distribution to be an important capability. However, 43% of businesses in IDC’s mobility study said they struggled with this issue. Many issues businesses encounter with app distribution involve the ability to get the right apps to the right groups of workers — this includes both internally-developed, and extremal/off-the-shelf mobile software. Many businesses struggle with the decision to use a private, internally hosted app store (via a MAM platform), or to use app distribution and app store options from carriers or device OEMs.
According to Google’s data, apps downloaded via Google Play and managed Google Play have the least probability of containing mobile harmful code or unwanted settings or features. According to Q4 2017 Google data, fewer than 1% (.82%) of Android devices had PHAs installed. For devices that downloaded apps exclusively from the Play store, the number was even lower — .09%. Managed Google Play also provides policies and settings for app distribution based on end-user identity, job function and other parameters to limit availability of apps only to relevant teams and workers.

Android zero-touch enrollment is another key development in Android deployment technology for enterprises, allowing the enterprise to pre-configure Android devices with all required settings, required applications (both off-the-shelf and custom-built), mobile security tools and automatic enrollment in EMM enterprise mobility management platforms such as VMware AirWatch, MobileIron and BlackBerry. Enterprise IT teams deploying corporate liable Android devices can use zero-touch to have pre-configured EMM settings automatically delivered to deployed Android devices the instant they are powered on and connected to cellular services. All required device settings are configured via the zero-touch portal and devices can be drop-shipped in the box to users wherever they are. Unboxing and powering on the device automatically brings up the desired IT configuration, with automatic enrollment in EMM, installation of required apps, and other managed services.

This eliminates multiple layers of friction in onboarding new employees, or upgrading end-users with new devices, while eliminating the chance for proper security, compliance or management configurations to slip through the cracks. Moreover, devices enrolled in zero-touch cannot be unenrolled from their EMM provider; even a factory reset will simply cause the device to re-enroll. This is valuable to assure management of the device over its lifecycle and that reassigning devices between employees happens more frequently.
Open architectures provide deeper security integrations, broader benefits

With Linux as its base, the Android OS benefits from a massive community of volunteer and professional developers. With hundreds of thousands of kernel OS developers, both professional and volunteer, software maintainers are able to find 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 and proactive; hundreds of independent Android security researchers, white-hat hackers and other analysts actively pry at the Android code base for weaknesses, and work with Google and the open source community to quickly implement security updates and fixes.

Beyond the open-source community that develops and improves the Android codebase, via the AOSP, Google also rewards the discovery of security-specific flaws, vulnerabilities and bugs in the OS software, and in apps on its app store via a bug-bounty program. In 2017, over 100 independent security researchers and whitehat hackers contributed to code flaw discoveries in Android, with Google paying out over $1 million in bug-bounty security rewards.
Misconceptions and perceptions: Enterprise enablement/enhancement vs. securing “unsafe” Android

It’s an outdated notion that only “locked down” or “secured” Android is safe enough to use for business. IT decision makers should start from the position that Android is fundamentally secure enough for wide-scale deployment across multiple use cases — from mobile worker enablement (i.e., smartphones with productivity and LoB-specific apps) to corporate-owned/single-use scenarios, where Android-based devices are deployed in replacing PCs and other proprietary or purpose-built computing platforms (i.e., PoS/kiosk machines in retail), paper/clipboard-based workflow scenarios, or industry-specific computing/information display and input/output tasks (healthcare charts/monitoring; public safety, etc).

Beyond basic device security and software/app hygiene, Google enables more advanced security scenarios and capabilities across its Google enterprise services, especially with regard to securely deploying and managing a business’ critical mobile applications. This can include both off-the-shelf software for mobile end-users, as well as custom-built mobile apps developed specifically for a business’ workflows, specialized tasks or other revenue-generating or competitive-differentiating purposes.

Businesses should start with the assumption that Android is secure enough foundationally for wide-scale deployment across multiple use cases.
With underlying trust in the Google Play store, given Google’s extensive device scanning, app monitoring and advanced ML-driven security vetting processes, businesses can take advantage of enterprise-specific offerings around Google app distribution in managed Google Play. This is a business-focused solution that allows for control of both public and private apps that the IT department may want end-users to download to Android devices. Enterprise IT teams distribute custom-developed apps via the managed Play store, which only allows authorized employees, contractors, partners or specialized customers to see and access the software.

To end-users, the discovery and downloading of the software is exactly the same as the traditional Play store experience. However, enterprises can add layers of management, policy enforcement and control to the software that is accessed and downloaded beyond Google’s consumer-oriented app store experience. Google also offers a Private App Publishing API, which allows enterprise developers to create internal apps via their customary mobile application development platforms (MADPs) with API-based app delivery workflows without having to use the Google store interface. Apps can also be published in stages, or specifically targeted at regions, work groups/individuals in the organization, or other parameters where full distribution of an app needs to be controlled and monitored.

Enterprises want interoperability and flexibility with their IT products, and Google brings this capability with broad integration partnerships across enterprise mobility management (EMM). Both EMM and mobile threat management¹ (MTM) are widely used technologies, with platforms such as AirWatch, MobileIron, BlackBerry and Citrix XenMobile deployed in more than 44% of enterprises; similarly, 50% of business also use some form of mobile endpoint security technology in concert with EMM solutions. Android for enterprise provides key integration partnerships across these product categories, enhancing the security and detection capabilities with platforms that can enforce more complex and advanced EMM policies and security settings.

¹ Mobile Threat Management (MTM) is cloud-based security software which prevents threats against your mobile devices from any kind of malware attacks.
Innovations in security come not only from third-party ISVs in enterprise, but from mobile device OEMs as well. Android’s device diversity also applies to varying security capabilities, from fingerprint, retina and facial recognition biometrics, to unique security applications for managing secure content, passwords and identities. The diversity of OEMs in the Android market place also allows for adoption of advanced security features across a range device price points. Integrations for mobile operating systems with EMM, mobile security, network/infrastructure security platforms are maturing to the point where enterprises have real solutions they can explore in terms of interoperability of management and security technologies.

From this perspective, Android excels at cross-technology integration and interoperability, as the platform’s open nature allows OEMs, security and management software companies to integrate on a deeper level with third-party technologies. For example, Android devices allow third-party network security and threat detection platforms, such as Cisco, to monitor active mobile device traffic on a corporate WLAN for anomalous behavior or security threats — which could be from malicious software on devices, but more likely, tied to an end-user misbehavior (i.e., accessing unauthorized systems or applications).

**App and data security and privacy considerations**

For businesses to secure their mobile app and infrastructure architectures, enterprise IT teams must consider the underlying client/server nature of mobile applications, and associated security, policy and management repercussions. Client/server, a somewhat antiquated computing concept, isn’t often associated with modern mobile/cloud technologies. However, many mobile/cloud apps, especially business applications and productivity tools for mobile, have some core traits of client/server architectures. For example, application software is installed locally on a device, often with local on-device data caching and storage, since local storage, processing and RAM on mobile devices are used to optimize the user experience. According to IDC data, native mobile apps are the most popular type of app deployment in businesses, with 64% of enterprises saying
they deploy native mobile apps, as opposed to full browser-based phone apps (where no data is stored or installed locally) or even hybrid apps where some lightweight software resides on phones, but most processing and data presentation is done via remote web/cloud servers.

With this in mind, businesses must be aware of how devices are set up in terms of permissions for applications to access local resources. A company may not want data from an internal app or data repository to be available to share across other applications, or even allow for screenshots of the app to be taken.

Businesses should also pay attention to what types of data are transmitted via apps, and apply the right policies for either securing certain types of traffic, or simply blocking the transmission of data in certain scenarios. An app dealing with sensitive information or data might only be allowed to operate if a VPN is turned on — or situationally, if the device is attached to an untrusted Wi-Fi network, or is located in an untrusted specific physical location or region. Managed Google Play includes the ability to review default settings and permissions listings of apps by IT staff before apps are approved for distribution in the store. (See Figure 4 for best practices around evaluating apps.)
App evaluation best practices

Figure 4. Secure mobile app deployment strategies with Android

- Look for apps that use managed configurations to configure features such as selecting trusted cloud vendor for app to use
- Company policy, customer & regulatory/compliance consideration
- Control app settings and access via user identity via managed Google Play
- Use third-party security tools, pre- and post-deployment, to examine and observe app behavior in context of business use
- Use tools that examine the public reputation of apps from third-party stores
- Test the behavior and level of intrusiveness of an app prior to allowing it to be downloaded

Source: IDC, 2017

Managed Google Play provides enterprise IT teams with detailed and specific listings of user permissions apps request. Before deploying a new productivity or industry-specific app into the wild, businesses can see exactly what resources and permissions the software requires, or may request with the option to deny access. Often end-users who encounter apps asking for specific permissions flip through accesses request screens, especially those workers who are engaged in a specific task and using an app for the first time.

IT can preemptively set permissions to what is required by the business, or regulatory/compliance requirements, before deploying via managed Google Play. Enterprises must consider acceptable levels of data usage, privacy settings, app access and data usage in general when vetting apps — on any mobile OS platform — for widespread deployment.
When apps are approved, after the review/vetting process via the Play Store evaluation capabilities, businesses can use the managed Play store to approve what third-party apps are available to workers, based on identity, role and region (often with specific regulatory requirements, such as GDPR in Europe). Private apps can now be targeted to up to 10 different EMM deployments. This can help if an organization is managed regionally, by different user roles, or needs to deploy apps into various test environments.

**Look for apps that use managed configurations to configure features such as selecting trusted cloud vendor for app to use**

With managed configurations, app developers can specify aspects of an app’s behavior or settings -- such as how data is shared, accessed and manipulated in an app. For instance, managed configurations could allow IT administrators to specify which cloud storage platforms an app can sync with. Managed configurations can also be used to restrict what types of networks an app may use (i.e., limiting large-bandwidth apps to Wi-Fi only), enforce use of VPNs for sensitive apps or data transmission, or require encryption on a device.

Overall this approach helps business implement strong Android device and app restriction settings without requiring the use of app SDKs or specialized app wrapping. (Such approaches can introduce cost/inefficiency from an operational standpoint, and security vulnerabilities, as such apps typically have to be side-loaded via private app stores).

**Company policy, customer & regulatory/compliance considerations**

Mobile apps may have requirements beyond security and management settings. Policies must be in place to distribute to apps and services to workers based on roles and responsibilities (i.e., only customer service team members should see PoS apps in managed Google Play). This might go beyond company policy, to the level of regulatory and compliance rules (i.e., hospital front desk staff should not have download access to a clinical or pharmacy/prescription fulfillment app).
Managed Google Play can control app settings and access via user identity. When used in concert with an EMM platform, businesses could create sophisticated app access and usage policies, such as limiting access to certain apps based on role, department or region.

**Use third-party security solutions to evaluate on-device app behavior and data usage**

Third-party security tools can also be used both pre- and post-deployment of enterprise Android apps and devices to examine app behavior, observe app behavior in the context of allowed enterprise policy and security rules, and to provide ongoing monitoring of app activities and behavior.

As discussed earlier, Google itself has built antimalware, suspicious behavior monitoring and regular health check scanning into the Android OS and accompanying updating/security services themselves. These capabilities can broadly cover devices from malware and undesirable activities on devices (i.e. non-user initiated device rooting, execution of arbitrary code, etc) as well as enforcing more subtle or fine-grained policies on acceptable device, app and data usage.

Pre-deployment, tools exist that can examine the public reputation of apps from third-party stores, as well as test the behavior and level of intrusiveness of an app prior to allowing it to be downloaded, or made available via a managed Google Play deployment. Google’s anti-malware is tuned to protect the whole app ecosystem from malware. But, what’s considered a perfectly legitimate app in the consumer domain may exhibit behaviors that are against IT policy. For example, sending data back to URLs hosted in particular countries, or using certain third-party SDKs that are not appropriate such as social network login or ads, both of which are much more targeted to the consumer domain.

This is then a complementary service to GPP, and about IT policy implementation rather than malware protection.
CONCLUSION

Android has come far in terms of addressing past security issues and misconceptions. There is more behind Android security than most enterprises realize. From the protections in the operating system design, to how files are stored, to the applications that execute on the device, Google has taken various steps to ensure the security of Android in business environments. Numerous protections exist to limit the influence of malware and other threats. Android represents no more of a threat vector, and in some cases is less of a threat vector, than other operating systems in corporate IT.

IDC believes that the security fundamentals of the Android OS — separation of system processes, trusted OS architectures, and advanced threat analytics — make it a business-class mobile device OS, which enterprises can securely deploy at scale. Enterprise IT decision-makers should closely examine the current state, and the future road map, of Android security. Businesses deploying Android can benefit from its inherent security, but also take advantage of its broad ecosystem and IT security industry partnerships and integrations.

Overall, IDC defines the three pillars for enterprise mobility success as:
1. Secured OS platform
2. Adaptable and flexible platform
3. Balanced IT & user experience
To learn more about security and the other pillars for enterprise mobility success, visit [www.whyandroid-enterprise.com/all](http://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.