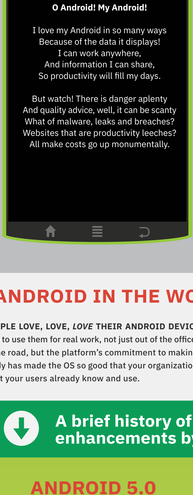
Put the SWEET FEATURES of Android™ to work

ENABLING THE WORLD'S MOST POPULAR[1] OPERATING SYSTEM (OS) IN THE ENTERPRISE



ANDROID IN THE WORKPLACE

PEOPLE LOVE, LOVE, LOVE *THEIR* ANDROID DEVICES—and they expect to be able to use them for real work, not just out of the office. There can be a few bumps in the road, but the platform's commitment to making these devices enterprise-ready has made the OS so good that your organization won't want to miss out on what your users already know and use.

A brief history of security enhancements by version

ANDROID 5.0

- **WORK PROFILES** were added to separate work from play, and to help protect user privacy. Only approved applications (apps) can be installed in these profiles, and work data is encrypted to keep it safe if the device is lost or stolen.
- **THE PROVISIONING PROCESS** was enhanced to allow managed enterprise apps alongside personal apps.
- **MANAGED GOOGLE PLAY** was added to streamline app deployment and grant greater efficiencies for IT.
- **HARDWARE-BASED ENCRYPTION** was added (AES-based, full-disk encryption).

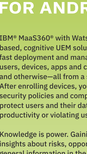
ANDROID 6.0

- **SECURITY AND MANAGEMENT ENHANCEMENTS** were added, including fingerprint access, which improves the user experience without risking security.
- **NEW APPLICATION PROGRAMMING INTERFACES (APIS)** were provided to improve certificate management.
- **APP ENHANCEMENTS** allow apps to authenticate users based on how recently they last unlocked their device, reducing the need to remember app-specific passwords. Apps can now be installed or removed without user intervention.
- **PURPOSE-BUILT SOLUTIONS** were added to support devices used for point-of-sale, inventory management and more.
- **WORK PROFILES** got shiny new updates, including simpler virtual private network (VPN) control, work status notifications and enhanced access to work contacts.

ANDROID 7.0

- **PRODUCTIVITY FEATURES** were added, including multitasking and improved notifications.
- **WORK SECURITY CHALLENGE** allows IT admins to implement a separate password for the work profile that would be different from the user-configured device password.
- **ALWAYS-ON VPN** sends all traffic from the work profile, or from specific apps, through a secure connection.
- **FILE-BASED ENCRYPTION** means that the OS, the personal profile and the work profile can be encrypted with different keys to provide an extra level of security.
- **TEMPORARY APP SUSPENSION** revokes access to work apps without removing the work profile until the user becomes compliant with corporate policies.

ANDROID 8.0



- **GOOGLE PLAY PROTECT** now checks apps to make sure there aren't any hidden dangers, and advanced forensics and encryption are available for company-owned devices.
- **SECURITY INTEGRITY FOR THE ENTIRE DEVICE:** Risky apps are blocked from the entire device, even the personal side, while users can decide if the source of an app should always be trusted.
- **ACCESS FOR PERSONAL USE** has been added for corporate-owned devices.
- **WORK PROFILE AND WORK-MANAGED DEVICES** can now be configured with unlock timeout periods or require a secondary, stronger authentication like a password, PIN or pattern for increased security.
- **ZERO-TOUCH ENROLLMENT** saves time and hassles for users.
- **ADVANCED SECURITY ANALYSIS** with network logging to help find emerging threats.

6 Tips to help maximize success for Android in the enterprise

DON'T GO IT ALONE

In the world of smartphones, tablets, laptops and desktops, you need a partner. A solution that can provide insight into all your smartphones, tablets, laptops and Internet-of-Things (IoT) devices, and deploy apps, documents, settings and more—without slowing down the user or IT. A unified endpoint management (UEM) solution can give you all that with the ability to deploy, lock, block and wipe devices with ease.

OVER-THE-AIR (OTA) AND REMOTE SUPPORT

You can't touch all devices (especially the ones you don't know about). By sending corporate apps, docs, settings and more OTA, you can save time and trouble for you and your users. Long gone are the days where users would bring their devices to IT for updates and troubleshooting.

ALLOW ONLY TRUSTED APPS

Apps on the Google Play Store have been vetted with Google Play Protect (new for Android Oreo), but others have not. A personal app with malware could be bad news for your environment. You want to encourage the good ones, though. Custom, home-grown apps can be a great productivity boon, especially if you put them in your own enterprise app catalog.

IMPLEMENT DEVICE AND DATA SECURITY

With each new release, additional features are added that can really help IT save time. Use zero-touch deployment and QR code scanning to streamline enrollment, work profiles and more. Depending on the device, you may be able to set up specific security policies for work apps, suspend access to apps and lock down network activity to ensure that work data is secure during transit.

BE A TROOPER, NOT A SNOOPER

Privacy is paramount, especially for personal devices or corporate devices where personal use is allowed. You need to see just enough to ensure safety without peering at someone's vacation pictures. Having an on-device container is a great start, and using privacy settings to manage what information to collect can relieve your users' privacy concerns.

MIND THE COSTS OF DATA LOSS

The costs of lost data or a breach can be extreme, not to mention the loss of customer trust and loyalty. Make sure corporate data can't wander off. Devices with removable SD cards and USB connections can lose data. Data transmitted in an unsecured Wi-Fi zone is also at risk. Make sure you can lock any open doors, but don't restrict user productivity.

IBM MaaS360 | With Watson

FOR ANDROID IN THE ENTERPRISE

IBM® MaaS360® with Watson™ is a cloud-based, cognitive UEM solution that provides fast deployment and management of all your users, devices, apps and content—Android and otherwise—all from a single console. After enrolling devices, you can implement security policies and compliance rules to help protect users and their data without impeding productivity or violating user privacy.

Knowledge is power. Gaining actionable insights about risks, opportunities and general information in the context of your environment is a huge bonus. With Watson, MaaS360 Advisor brings cognitive insights front and center, making it easy in the event of a security incident for administrators to see what happened and take immediate action—right from the MaaS360 dashboard.

Better yet, MaaS360 Advisor tells you which of your users, devices or apps could be affected, reducing the amount of time that is normally spent on research.

DELIVERED FROM A BEST-IN-CLASS-CLOUD, MAAS360 IS READY TO SUPPORT ALL NEW MAJOR OS RELEASES ON LAUNCH DAY.

Start your trial today!

Experience MaaS360 with Watson today by starting your no-cost 30-day trial. See for yourself how easy it is to enroll devices, deploy apps from a unified app catalog, enact policies and compliance rules to help protect your organization, and keep a watchful eye out for opportunities and threats.

[1] "Operating System Market Share Worldwide - October 2017," *StatsCounter.com*, retrieved November 8, 2017.

WGW12376-USEN-00