android

CORTADO

Android makes it easy to manage every use case

Android management options allow enterprises to support a range of use cases from BYOD to corporate-liable.

Challenge

Enterprises are constantly looking for ways to improve their operations and become more competitive and are seeking devices to help reach these goals. Whether it's increasing employee mobility and efficiency by allowing connections to company assets with personal devices or using kiosks for customer interactions to improve satisfaction, IT has been tasked with securing and managing these devices and ensuring they comply with their organization's requirements and security posture.

The Android difference

Android offers flexible options for any deployment, from personal BYOD devices to fully-managed and dedicated scenarios. With an Enterprise Mobility Management (EMM) provider, you can leverage a standardized set of robust APIs to secure and manage data and applications. This allows enterprises to deploy, manage, and secure devices to support a broad range of use cases.

Personally-owned devices

Unlocking the promise of BYOD or personal enablement comes down to successful separation of data so users enjoy privacy and protection for their content while IT can still secure corporate information.

Work profile - From Android 5.1.1 Lollipop and later, Android devices support a data separation model called a work profile. The work profile contains all corporate applications and data and ensures that the data is separated from any personal apps and data a user may have. The work profile runs simultaneously with the personal profile, with work apps and notifications badged with a briefcase. Users can also multi-task between work and personal apps while data remains separate.

The work profile offers a number of benefits including:

- **Data separation** - Separation between a user's personal data and work data is enforced at the OS kernel level across processes, memory and storage. All applications from Google Play work out of the box with separate data storage and there is no need for modification of applications, such as app wrapping.
- **Data loss prevention** - Android provides a set of DLP policies and controls that can be applied to the work profile via an EMM. These policies include:
    - **Work profile passcode** - Enforce minimum complexity with PIN, pattern, password, or biometrics on the work profile.
    - **Copy/paste** - Prevent data from being copied from work apps into personal apps.
    - **Inter-app sharing** - Specify which work apps can share data with personal apps or block entirely.
    - **VPN** - Apps in the work profile may be secured on the network through various VPN options, including the ability to ensure only work profile apps can use the VPN.
    - **Device wide-integrity controls** - Require Google Play Protect anti-malware service to be switched on; define screen lock complexity.
- **User privacy** - On a BYO device, IT manages only business applications and data. Employees can continue to use their own apps in the personal profile. Personal apps and data may not be inspected or controlled by IT. If IT needs to remotely wipe corporate apps and data, they may do so confidently without affecting personal apps and data.
- **Work-life balance** - Users or admins can toggle off work mode, which suspends the work profile, stopping all work apps from running, syncing in the background or presenting notifications.

Corporate-owned devices

For corporate-liable devices, organizations may need full device and app management for granular control for a variety of deployment scenarios.

Fully managed device - From Android 5.1.1 Lollipop and later,

Android devices support a comprehensive OS-level fully managed device mode for corporate-owned devices, bringing consistency across device manufacturers.

Fully managed device mode offers benefits including:

- **Whole device management** - Apply 80+ management controls to everything that happens on the device, from lock screen to encryption, VPN to app installs.
- **Remote diagnostics and forensics** - Remotely audit activity on devices or debug issues for users. Log network activity and processes to monitor data loss prevention and device health and usage.
- **Work-only device** - Option to prevent users from adding personal accounts to devices, to maintain the device as only for work purposes.

Personally enabled device - From Android 8.0, Android devices support a work profile on a fully managed device to allow users to use personal applications and data, while ensuring that corporate applications and data remain separate. The work and personal profiles run simultaneously on the home screen of the device, with work apps and notifications badged with a briefcase.

This provides the functionality and benefits of the work profile while IT retains overall control and visibility of the device.

Dedicated device - From Android 6.0, Android offers lock-task mode to lock an app to the screen for devices that are dedicated to a specific app, such as kiosks or task worker devices. IT can also hide system navigation and settings to avoid distracting users. Apps are managed entirely remotely, with no browsable app store made available.

In Android 9, improved lock-task features enable devices to be shared by multiple users, for shift workers or for public sessions. Any app can be used in lock-task mode with no extra work required from the original developer. This allows the organization to manage the device with a fine degree of control over the Android UI elements shown to the user.

App distribution and management

Organizations need to be able to equip employees with approved applications, from publicly available apps to privately developed software.

Managed Google Play - Android offers a standard way to distribute apps and integrates with major EMMs through managed Google Play. With managed Google Play, admins can securely distribute and remotely configure internal private applications as well as public applications. A rich set of policy controls allow admins to secure the apps and their data.

IT admins can whitelist applications in a curated managed Google Play store app or silently push applications to employee devices. Apps can be remotely provisioned and configured for specific employees with no user intervention.

Conclusion

Android provides a flexible and robust management platform, enabling enterprises to support any scenario from locked down to personally enabled devices. The work profile gives enterprises greater IT control over data separation and DLP. That makes it an ideal option for employee-owned devices and corporate owned, personally enabled devices. Fully managed devices are the best way to deploy corporate-owned Android devices with control over everything that happens on the device.