android

Work Profile Security on Company-Owned Devices in Android 11

android

Overview

Enterprise customers must ensure their fleet of devices meet high levels of security. They must also ensure that a user's privacy is preserved, as noted in our blog on user privacy, when deploying a device that is used for work and personal use cases.

An increasingly common deployment model is company-owned, personally enabled devices (COPE), also known as fully managed devices with a work profile, where employees have both work and personal information on a single device. Often in this use case, IT and Security admins seek full visibility over the entire device. This can create a challenge, pitting company security against employee privacy.

Since its debut in Android 5, the work profile has separated work and personal apps, giving IT full control over work apps and data, but with no visibility into or control over personal apps. We introduced work profile support for COPE in Android 8, giving admins complete control over the device to include deep visibility into the personal use of the device. In Android 11, IT organizations can utilize the strong security and privacy protections on company-owned devices as well, in addition to new asset management and personal usage policies to keep company assets in compliance with corporate policy while helping ensure personal privacy.

With Android 11, organizations can achieve three key outcomes of a successful COPE deployment: protecting corporate data with strong device security; preserving employee privacy; and enforcing asset compliance with corporate policy. That's because the work profile provides strong anti-exploitation and data loss controls on any device, regardless of who owns it, as well as the tools to identify a compromised device and protect against malware. Therefore, IT doesn't need full device visibility to protect corporate data and company assets; instead they can focus on protecting work data while respecting the privacy of personal data owned by users.

The security of a work profile is built on top of many layers of security found in all Android devices.

- First, Android uses a security model that includes isolation and separation of data, processes, and applications. The goal of sandboxing is to keep an application's data isolated from other apps, and prevent access from outside of the sandbox by other applications and processes.
- Second, there are key OS platform technologies that protect user and work data, such as government grade encryption. OS level data-at-rest protection can further extend the separation of personal and work data on the file system.
- Google security services like Google Play Protect and SafetyNet attestation are added to protect against malware and device compromise which could introduce means for data exfiltration.
- Lastly, a secure management framework that enables enterprise grade controls over critical business data is in every Android device running Google Mobile Services, or GMS. This ensures that all OEMs support modern management with Android Enterprise.

Sandboxing - A building block for profile separation

An important component of the security model on Android is to enforce isolation of applications and processes at runtime against potentially malicious code. Hardware components like a Trusted Execution Environment (TEE) help isolate sensitive processes and data like cryptographic operations and key storage. SELinux provides the foundation and structure of Android's security model where process isolation provides the fundamental security framework for sandboxing. This boundary is where security decisions are made and enforced based on access controls and permissions. Userspace applications are also separated and isolated using sandboxing technology.

- **Verified boot** begins by implementing separation and isolation processes when powering on an Android device. Verified boot works to ensure a device starts up safely by cryptographically checking each stage of the bootup process before handing over execution at each consecutive step. This helps maintain device integrity and prevent attacks during the boot process.
- **The SELinux enabled kernel** on Android enforces a Mandatory Access Control (MAC) permission model. The kernel has a security policy that dictates what actions are allowed and only permits actions explicitly granted by policy.
- **Kernel Sandboxing** hardens the kernel against potential privilege escalation attacks via vulnerable hardware drivers provided by System on a Chips (SoC) vendors. Driver code that might be exploited are still sandboxed which significantly reduces the effectiveness of any exploitation.
- **System Process Sandboxing** applies the same type of sandboxing technology applied to the kernel in order to protect critical system services from processing untrusted content. The media framework, telephony stack, WiFi services, and Bluetooth components are examples of these system processes that use sandboxing.
- **Application Sandboxing** on Android continues using the MAC (mandatory access control) permissions implemented in the SELinux kernel and system process isolation. Applications are separated from each other by providing each application with a unique UNIX user ID, or UID, and a directory owned by the app. The unique per-app UID combined with run-time permissions granted to the app keep the application and its data secure.
- **Other areas of separation** include the TEE and userspace components. For example, the Android Keymaster integrates the key store into the TEE, which guards cryptographic key storage from exposure and tampering. An attacker cannot read key material stored in the Keymaster even if the kernel is fully compromised. Beginning with Android 9, devices with dedicated tamper resistant hardware can store keys in the StrongBox Keymaster. This implementation mitigates against the most sophisticated attacks such as cold boot memory attack, power analysis, and other invasive attacks that can allow privilege escalation.

Android Work Profile Security Model

The work profile takes advantage of all the previous sandboxing components within Android to ensure a secure and protected separation between work and personal apps on the same device. Enforcing policy is done via a Device Policy Controller (DPC) application installed in the work profile and controlled by an EMM Service. Device level security controls are managed by the DPC from within the work profile. The separation of personal data from enterprise data on a single device leverages a multi-user framework. Separate users combined with application permissions enforce strong data separation, much like how apps and processes are sandboxed. Data-at-rest separation can be enhanced further with different per profile encryption keys on devices that support File Based Encryption, or FBE. Because of containment at every layer, isolation is extended from each profile down to the kernel, thus providing strict separation between profiles that have stronger data loss prevention versus traditional containerization or MAM (Mobile Application Management) solutions.

Google Security Services

Google Play Protect and SafetyNet attestation are services on GMS certified devices that help prevent malware and device compromise. Exploitation code is often delivered to devices via malware. The combination of Google Play Protect and Verify Apps can help prevent malware and threats from being installed. Android devices using managed Google Play have a Potentially Harmful App (PHA) installation rate of only .004%. With the App Defense Alliance scanning capabilities of all apps in Google Play, and giving admins the ability to create

allow lists / block lists for the personal Google Play Store, malware getting on managed devices is very unlikely.

EMM partners can use these services to ensure users cannot sideload applications and must only install applications from Google Play. SafetyNet attestation services provide real-time device integrity checking, like root detection and checking for unlocked bootloaders. EMMs can receive the signals from these on-device services to help detect and mitigate compromises.

Android Enterprise management

The many areas of the Android platform that implement sandboxing and isolation are also controllable on managed devices. Android Enterprise APIs provide a feature rich set of policies that control how a work profile operates. A few examples are controlling data sharing, notification control, password requirements, and application management.

Work profile protection in Android 11

Regardless of who owns the device, the work profile provides consistent and industry-leading protections for company data. The principles of data separation described above ensure corporate data remains secure. Fundamental security features available to any work profile device such as preventing sideloading of apps, enforcing Play Protect, and blocking device access over USB, provide strong device security without the need for visibility into personal data.

Android 11 extends this model with improved work profile support for company-owned devices. If a work profile is added from the setup wizard using the provisioning tools added in Android 11, the device is recognized as company-owned and a wider range of asset management and device level controls are made available to the device policy controller. These capabilities enable easier management of both work and personal use on company-owned devices, while maintaining the privacy protections of the work profile.

Protecting and preserving a user's privacy does not impact a device's overall security but rather prevents an admin from viewing potentially sensitive info such as personal apps.

Preserving privacy without compromising security		
Common IT practice	**Privacy concern**	**Work profile solution**
Listing all applications on device, to audit for malicious or risky personal apps	Reveals private, personal apps	Only view work apps; Restrict personal apps to just Play verified apps; implement allow or block list of personal apps on company-owned devices
Prevent a factory reset to maintain ownership of devices	Prevents users from removing personal data	Configure Factory Reset Protection to ensure only IT can set up device after reset
Configure always on VPN	Reveals personal browsing history	Set VPN to just work apps

android

Summary

Android devices are built on a proven concept of isolating and confining many parts of the platform combined with granular application permissions. These techniques are found in hardware, the OS, the kernel, and user applications to protect access and confine exploitation to a single process or app. Work profiles are built with all of these principles and extended with a management layer for enterprise customers to control data separation while still protecting the entire device and preserving user privacy. Reduced visibility for admins does not reduce the security of a device, as the tools to protect a device are still present. Configuring the policies properly in an EMM and using signals from the Google Security Services on Android devices will provide strong integrity and malware detection. Combined with the many DLP controls and strong separation, admins can be assured full device security on devices deployed with a COPE model on Android 11, referred to as a Work Profile on Company-Owned Device.