android

Android invests in technologies and services that **strengthen the security** of devices, apps, and the global ecosystem

Challenge

Enterprise customers are challenged to safeguard their mobile devices while also preserving user privacy. Ensuring critical workflows and sensitive data integrity is not only a priority -- it's an expectation. Organizations must have strong security controls to protect company data from a wide range of risks and threats.

The Android difference

The Android platform provides a powerful, multi-layered security model built into every device. Google enforces strict security requirements for all Google Mobile Services (GMS) certified devices supplied by OEMs and Carriers. Mandatory hardware-backed security is required to ensure critical tasks, cryptographic operations, and key storage is secure. The Android OS is hardened with leading exploit mitigation and data isolation technology to prevent device compromise.

Google security services like SafetyNet, Google Play Protect, Verify Apps, and Safe Browsing are key components that prevent and detect threats. Finally, we have built a robust set of enterprise APIs that provide admins with enterprise-grade tools to manage their Android fleet.

Hardware-backed security

Hardware-backed security is the foundation that secures the rest of the platform by executing cryptographic functions in dedicated, tamper-resistant hardware. Verify boot uses a hardware-backed cryptographic chain of trust to confirm a device's integrity during the boot process. Version binding and rollback protection ensure keys created and stored in hardware cannot be used by older OS versions in attempts to compromise a device. Performing a brute force attack on a locked device's passcode is now infeasible due to rate limiting.

Android operating system

The Android OS utilizes industry-leading technology to harden the platform by providing strong app isolation and sandboxing processes, exploit mitigation, and separation of work and personal data.

Sandboxing and process isolation - An important component of the Android security model is enforcing isolation of applications and processes at runtime against potentially malicious code. This separation helps ensure data remains secure.

Encryption - Android devices have encryption enabled out of the box that users cannot disable. In Android 8 and above, a Google-built FIPS 140-2 validated encryption algorithm called BoringSSL is used by default. Android 10 and above devices are required to use AES 256-bit file-based encryption. This allows for a separate encryption key for the work profile which extends the separation and isolation model. Encryption keys are derived by using the lock-screen passcode and are backed by secure hardware.

Anti-exploitation - Every Android device utilizes various technologies to protect user applications and data. Address space layout randomization (ASLR) protects the kernel, OS, and applications from exploits by loading apps into random memory address locations at runtime.

Regular, consistent updates - Google releases monthly security patches to help ecosystem partners keep their devices updated. In Android 10, we introduced Google Play System Updates, which enabled Google to update OS security components directly from Google Play. Android 11 now supports 21 components, including 9 additions focused on improving privacy, security, and developer consistency.

Google Security Services

Google Play Protect - Google Play Protect uses a prevention model by scanning apps before they are actually installed.

Detection and removal scanning continuously works to keep your device free from Potentially Harmful Apps (PHAs) and is active on over 2.5 billion devices. It automatically scans devices every day to include system apps, apps from Google Play, and sideloaded apps. Google Play Protect will even scan devices when devices are offline.

Verify Apps API - Verify Apps allows EMMs to query managed devices to obtain a list of any known potentially harmful apps that the user has installed on their device. This list includes categories for the identified potentially harmful apps. The results can be used by an EMM to remediate with automated compliance policies.

Safe Browsing - Safe Browsing in the Chrome browser protects users against phishing attacks and sites that push malware. Users are warned when visiting a potentially dangerous site before it loads. Safe Browsing protection is also extended into webview and can be controlled by EMMs via policy.

SafetyNet Attestation - SafetyNet attestation is a free service from Google which tests a device's integrity and provides anti-abuse services. Developers and EMMs can add SafetyNet attestation into their apps and solutions to provide strong assurance that a device's integrity has not been compromised.

Management

Android offers robust management and policy controls to secure devices enrolled with many deployment models. Controls for admins enable them to meet specific security requirements at every layer of the Android security model from hardware, OS, and Google security services.

Network, WiFi, and VPN - Android apps on Android 9 and higher default to using TLS for network connections. Apps on Android 10 and higher default to TLS 1.3, which encrypts more of the handshake and can be up to 40% faster than previous versions. DNS over TLS prevents host name enumeration eavesdropping on DNS queries. VPN controls can force apps to only use the VPN with optional controls for connections to be allowed/disallowed if the VPN is down. IT admins can disable the ability for users to turn off always-on VPN connections.

Application management - Managed Google Play provides powerful and secure app management features. Admins can securely distribute and remotely configure internal private and public applications. A rich set of policy controls allow admins to secure apps and associated data. Admins have visibility and control over every permission of an app that they deploy.

Certification and validation - The managed Google Play Store is ISO 27001 certified and has SOC 2 & 3 reports to ensure customer data is safe and Google adheres to industry cloud security best practices. Android 9, 10, and 11 have attained NAIP certification with Pixel devices as a reference model. Android's security is validated by the partner and analysts. For example, Gartner gave Android the highest rating of strong for 27 out of 30 categories. Android was the first platform to be certified by ioXt (Internet of Secure Things) in 2020.

Conclusion

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 with Google security services to protect business apps and data. 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. 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.