android

Android provides powerful, multi-layered security to protect enterprise customers

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

Challenge

Android is the most popular mobile enterprise platform, powering four out of every five devices shipped for business use. The challenge for businesses is they need to trust their mobile devices to complete critical workflows and handle sensitive corporate data in their day-to-day use. Organizations need to find a way to protect their data against a range of risks and threats on these devices.

The Android difference

Google provides powerful, multi-layered security built into every device to protect data. Combining hardware security with Android OS hardening ensures device integrity. Industry leading exploit mitigation, sandboxing, and remote attestation services help detect and prevent exploitation and data loss. Google Play Protect, the world's largest threat detection system, runs on all devices, protecting against potentially harmful apps. Finally, we deliver a robust set of enterprise APIs that provide controls to secure data, preserve privacy, and help ensure device integrity.

Hardware backed security

Hardware based protection is the foundation to help secure the rest of the platform. Android devices utilize a trusted execution environment (TEE) to run privileged and security-sensitive operations such as PIN verification. As of Android 8.0, compatible devices can optionally use tamper-resistant hardware to verify the lock screen passcode. If verification succeeds, the tamper-resistant hardware returns a high entropy secret that can be used to derive the disk encryption key. Verified Boot confirms the device's integrity during boot up with a cryptographic chain of trust. Each stage is verified and combined with rollback protection, which prevents persistent exploits. Hardware components also protect private keys and prevent brute-force attacks of screen lock PINs and passwords. To further enhance protection, the SafetyNet remote attestation service can use hardware to detect compromised devices.

Operating system

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

Application sandboxing - Every Android app is contained in an application sandbox, which is enforced by SELinux. This ensures apps can only access data within their own sandbox unless explicitly authorized. In Android 10, we've introduced "constrained sandboxes," which further isolate components granting them even fewer privileges. Media Codecs now run in these constrained sandboxes, significantly reducing the severity and impact of any attempted exploitation.

Encryption - Encryption is mandatory and always on out of the box. Android 7.0 introduced support for AES 256-bit file-based encryption, which is now mandatory with Android 10. A user's encryption key is derived by using their lock-screen PIN or passcode and is backed by secure hardware. In Android 9.0 and higher, the use of Smart Lock, biometric unlocking, and notifications on the lock screen are temporarily disabled by holding the power button and selecting Lockdown mode. End users can easily evict the work profile encryption key by turning off the work profile, or this can be performed remotely by an EMM Admin.

Userspace hardening - Every Android device utilizes various technologies to protect user applications and data. ASLR (address space layout randomization) and DEP (data execution prevention) protect the OS and applications from exploits and many code reuse attacks. Android also implements KASLR (kernel address space layout randomization) to harden the kernel from attacks. In Android 9, Control flow integrity (CFI) for the userspace and kernel were introduced. In Android 10 additional hardening techniques were added such as execute only memory (XOM).

Regular, consistent updates - Google releases monthly security patches to help ecosystem partners keep their devices updated. Project Treble, released in 2018, provided OEMs a method to deliver updates much faster. In Android 10, we introduced Google Play System Updates, which enables Google to update OS security components using Google Play without requiring a full operating system update. Android 10 also introduced the ability for offline device updates directly from their EMM provider.

Google Play Protect

Google Play Protect continuously works to keep your device free from PHAs (Potentially Harmful Apps) 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 from unknown sources. Carrier OTA (Over The Air) updates that include new or updated apps are also scanned at the time of installation. Google Play Protect will even scan devices when devices are offline and not connected. Google Play Protect has helped keep installs of PHAs in 2019 to under 0.033%.

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, which is a component in most Android apps that renders web content, further extending the protection inside applications.

SafetyNet Attestation - SafetyNet attestation is a free service from Google which tests a device's integrity. 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. Verify Apps APIs, part of SafetyNet, can be used to query the status of Play Protect for mitigation and remediation by applying automatic compliance rules controlled by their EMM solution.

Management

Android offers robust management and policy controls to secure devices deployed with many deployment models. There are controls for admins to enable that meet specific security requirements at every layer of the Android security model from hardware, OS, apps, and services.

Network security - Android apps on Android 9 and higher devices default to using TLS for network connections. Android apps on Android 10 default to TLS 1.3, which encrypts more of the handshake and can be up to 40% faster than previous versions. DNS over TLS in Android 10 prevents DNS query leaks and the ability for users to change DNS settings. VPN controls in Android 10 can now force apps to only use the VPN with optional controls for connections to be allowed if the VPN is down. Finally, in Android 10, IT admins can also disable the ability for users to turn off always-on VPN connections.

App management - Managed Google Play provides powerful and secure app management features. 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 apps and associated data and scan applications for vulnerabilities. Finally, managed Google Play is ISO 27001 certified and has SOC 2 & 3 reports to ensure customer data is safe.

Conclusion

Android has been recognized as the leader in mobile device security by many security ecosystem partners and independent analyst firms. The platform offers multiple layers of security to help enterprise customers protect their data. From hardware-backed security for sensitive operations to a robust OS that isolates and effectively mitigates threats to maintain device integrity, Android provides a firm foundation so you can be confident your devices and data are secure. Android also delivers services such as always-on app analysis and scanning through Google Play Protect, remote attestation services with SafetyNet, and a host of enterprise grade management APIs for every deployment scenario and every enrollment type.

Powered by Google intelligence, Android security gets smarter each day and provides peace of mind to enterprise customers and users.

Get started today. For more information, visit Android.com/enterprise