android

Android delivers powerful security built in to protect enterprise customers

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

Challenge

Android is where the world goes to work. In the last year, 78 percent of all devices worldwide shipped for business use were Android devices. The challenge for businesses is that these devices are increasingly used for critical workflows to help optimize operations. That means more and more sensitive data resides on the devices, which can be taken anywhere, can connect to all sorts of networks, and can be easily lost, damaged or stolen. 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 security, built into every device, that leverages multiple layers of protection. Beginning with the hardware layer, there are dedicated hardware-enforced secure isolated environments to protect and carry out critical cryptographic tasks. The OS platform ensures device integrity by using industry leading exploit mitigation and sandboxing techniques to prevent bugs from being exploited and reduce their impact. Next, we add Google Play Protect on all devices, which is the world's largest threat detection system. Finally, we deliver a robust set of APIs to provide enterprise IT the controls they need to secure their data, users, and devices.

Hardware backed security

Android devices utilize a trusted execution environment (TEE), to run privileged or security-sensitive operations such as PIN verification. Tamper-resistant hardware support has been added in Android 8.0 for greater protection. Upon startup, Verified Boot confirms that the device software hasn't been tampered with by using a key that's built in to the device hardware ensuring that software always comes from a trusted source. Hardware components also protect private keys in the KeyStore and provide brute-force protection of screen lock credentials. The OS establishes a chain of trust and utilizes cryptographic methods to ensure the hardware and platform have not been compromised with verification through the SafetyNet API.

Operating system

The Android OS utilizes app isolation, device integrity, exploit mitigation, device encryption, and more to provide robust platform security.

Application sandboxing - Every Android app is contained in what's called an application sandbox, which is enforced by Security Enhanced (SE) Linux. Apps can only access data within their own sandbox unless explicitly authorized.

Encryption - Full disk encryption has been available since Android 5.0 and enforced by default from Android 6.0. Android 7.0 and higher utilize AES 256-bit file-based encryption that isolates and protects individual users. A user's encryption key is associated with their lock-screen credential, backed by hardware. Android 8.0 can can programmatically eject encryption keys if a device goes out of compliance.

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 against memory corruption and many code reuse attacks. By incorporating integer overflow sanitization, the stack is much more robust against malformed content, and sandboxing of media processes protects the operating system against privilege escalation.

Monthly security updates - To make Android even safer, Google shares security patches every month with device manufacturers. Android devices can automatically stay current with the latest security updates and when an update becomes available, via the manufacturer, it's automatically downloaded and installed. IT admins can check to see that purchased devices receive regular updates. They can also use their EMM to put devices out of compliance if they are not current with the latest security patches.

One way to identify regularly updated devices is to use the Android Enterprise Recommended program, which guarantees validated devices receive security updates at least every 90 days with many providing monthly security updates.

android

Google Play Protect

Google Play Protect continuously works to keep your device, data, and apps safe. It actively scans your device and is constantly improving to make sure you have the latest in mobile security. This continual protection ensures your users' devices are safe from PHAs (Potentially Harmful Apps). Play Protect is currently active on over 2 billion devices running Android 4.3 and higher. The rate of potentially harmful app installs is just 0.01 percent for devices that rely solely on Google Play for app downloads.

Application scanning - Play Protect automatically scans devices every day, even on sideloaded applications and apps that are delivered as part of the system partition. The scanning takes place even if the devices are offline.

Safe Browsing - With Safe Browsing protection in Chrome, you can browse with confidence. If you visit a site that's acting out of line, you'll be warned and taken back to safety.

Attestation - The SafetyNet attestation API provides application developers with the ability to evaluate if their app is running on a genuine Android device. Developers can also use the Verify Apps API to query the status of Play Protect for mitigation and remediation.

Management

Android offers management and policy control options for any deployment, from fully managed devices to personally-enabled and single-use scenarios. Multiple enrollment methods are available to meet the needs of deploying Android devices for enterprise use. Combining the flexible management capabilities, wide range of deployment options, strong application management, and robust set of security policy controls, Android can be deployed easily into an enterprise environment.

Flexible management options - Deploy an extensive range of policy controls over the entire device for corporate liable devices or work profiles for a BYOD scenario. These options provide full control over apps and data on devices owned by the organization. Full device management, personally enabled, dedicated device and BYOD deployments are all supported.

Deployment made simple - Companies can use various enrollment methods for fully managed devices that are simple and easy. Zero-touch enrollment, NFC bump, QR code scanning, and other methods are available to ensure easy enrolling for users and simple configuration by IT Admins.

App management - Managed Google Play offers a standard way to distribute apps and integrates with major enterprise mobility management providers. 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.

Conclusion

Android is recognized as a leader in security. The platform offers multiple layers of security to help enterprise customers protect what's important to them. From hardware-backed security for sensitive operations to a robust OS that isolates threats and maintains device integrity, Android provides a firm foundation so you can be confident your devices and data are safe. Android also delivers always-on app analysis and scanning through Google Play Protect along with a host of management APIs for every deployment scenario.

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