White Paper

Samsung On Android™

The Secure, Defense-Grade Alternative
Mobile malware is a concern for organizations embracing the connected enterprise, with headlines frequently warning about the growing threat from mobile malware. The popularity of Android™ has skyrocketed in the general market and Android now powers 81% of the world’s mobile devices, growing to an estimated 83% by 2019.¹ But despite its widespread use in the general market, erroneous mobile security assumptions dating back to the early days of Android and some negative press propagated by the media and security vendors are deterring some enterprises from leveraging the Android platform for competitive differentiation and business transformation.

Understanding the Android security landscape is paramount to realizing the full potential of the connected enterprise. This paper presents an overview of enhancements to the Android operating system, Google Play security services, and Samsung KNOX™. Together, these make Samsung devices running Android among the most secure mobile devices available to enterprises and government organizations alike.

Android Operating System Enhancements And Google Play Security

Google has always implemented a multi-tiered security model to include application sandboxing and security services provided by Google Play Services. Recently, Google has made significant improvements in Android security including:

1) enabling deployment of full disk, block-level encryption;
2) expanding the use of hardware-protected cryptography and removing older, exportable cipher suites;
3) securing the Linux kernel by requiring SELinux (Security-Enhanced Linux) in full enforcing mode, which requires policies in an environment of Mandatory Access Controls (MAC);
4) incorporating secure inter-process communications (IPC); and
5) implementing vulnerability exploit mitigation with ASLR (Address Space Layout Randomization).

Also inherent in the Android security ecosystem are Google-provided security services:

Verify Apps checks all applications that are installed on the device—even installations from unknown sources—to ensure that the device is protected against Potentially Harmful Applications (PHAs) prior to install. Additionally, all previously installed apps are regularly rechecked. Verify Apps performs over 200 million security scans of devices per day.

Safety Net validates that the device is operating as expected according to the Android security model and detects and protects against network-level attacks. Safety Net analyzes about 400 million network connections per day.

Safe Browsing, for Google Chrome on Android, protects against browser-based exploitation and websites attempting to deliver PHAs.

WebView updates are now provided via Google Play as needed to update, reduce and remove SSL vulnerabilities.

¹ Source: IDC Worldwide Quarterly Mobile Phone Tracker, December 2, 2015.
Google has also begun delivering monthly security updates for Android to address vulnerabilities and ensure enterprise customers get timely Android OS patching. Samsung also releases periodic security updates for select Samsung devices based on geographic region and carrier.

Google works continuously to reduce the existence of PHAs in the Android ecosystem by vetting applications offered via Google Play and expanding the set of security services for applications that run on the Android platform. All applications on Google Play are subjected to an in-depth security analysis before they are made available to the public. This pre-release security review includes static, dynamic and heuristic analyses; a third-party review; and, when needed, a manual review to identify and classify any potential threats. All applications in Google Play are reviewed on an on-going basis.

According to Google, of all installed PHAs detected on Android devices, a major portion originated from certain regions of Russia and China that have a large market for non-Google Play app stores. Verify Apps reduced the number of PHA installations outside of Google Play significantly. In fact, the number of infected apps hosted on these non-Google Play app stores fell by nearly half as a result of the deployment of Verify App, rendering the app stores an inefficient PHA deployment vector.

According to Google’s own analysis and the report [Android Security 2014 Year in Review](https://goo.gl/KmUzSb) unintentional installations of PHAs continued at low levels throughout 2014; less than 0.15% of devices that download only from the Google Play Store had PHAs installed. Devices that were infected typically used side-loaded applications or applications from unknown sources outside of Google Play. Only those applications thoroughly vetted and available on Google Play were afforded additional levels of protection.

As a result of these enhancements in the standard Android operating system in conjunction with the in-depth, continuous application review process, there are now more than 1.4 billion devices protected by Android’s holistic security ecosystem.

### Samsung KNOX Platform—Customizable, Defense-Grade, Hardware-Based Security Out of the Box

In addition to Google’s enhancements to the standard Android operating system, Samsung incorporates KNOX, a defense-grade, mobile security platform that protects Samsung devices from the hardware level up, starting at boot-up and running throughout the entire device lifecycle. It is a combination of platform-level security safeguards, as well as a suite of companion products and services that leverage the secure platform.

---

1Google. Android Security 2014 Year in Review. [https://goo.gl/KmUzSb](https://goo.gl/KmUzSb)
Samsung smartphones and tablets running KNOX employ Secure Boot, Trusted Boot, Security Enhancements for Android (SE for Android), and ARM® TrustZone®-based Integrity Measurement Architecture (TIMA).

**Secure Boot and Trusted Boot** verify both the authenticity and integrity of the bootloader modules and the Android kernel. This is now a mandatory implementation required by Compatibility Definition Document (CDD) and Compatibility Test Suite (CTS) from Google.

**TIMA Periodic Kernel Measurement (PKM)** performs continuous periodic monitoring of the kernel to detect unexpected modifications of legitimate kernel code and data.

**TIMA Real-Time Kernel Protection (RKP)** performs ongoing real-time monitoring of the operating system from within TrustZone to prevent tampering with the kernel.

In addition to the standard Samsung KNOX features, enterprises can enable enhanced KNOX capabilities to create an experience appropriate for the organization's needs.

Samsung KNOX Workspace establishes a protected environment for enterprise applications and data. It is an independently certified, defense-grade, hardware-anchored, dual-persona solution. Workspace is designed to separate, isolate, encrypt and protect enterprise data from attackers.

Samsung KNOX Customization provides purpose-built solutions that can both secure data and incorporate a set of tools and services to address specific industry requirements.

Samsung KNOX Enabled App is a transparent, secure container for individual applications.

Samsung provides enterprises the most secure devices out of the box with the Samsung KNOX platform. This platform-level protection is standard on all the latest Samsung flagship smartphone and tablet devices and can be tailored to address organization- and industry-specific needs.

**Conclusion**

Samsung, the world’s largest electronics OEM, and Google have undertaken a number of initiatives to build security into the core Android operating system, provide robust application screening and provisioning, and deliver innovative hardware-based security platforms. Together, these enhancements have positively affected perceptions of Android security and underscore Android’s enterprise worthiness.

Google’s ongoing commitment to providing monthly Android security patches, robust security services, and diligent application vetting with strict review processes, combined with Samsung’s device-based security features, position Android-based Samsung devices as the secure and logical choice for businesses and government agencies wishing to realize the potential of a digital enterprise.

**Additional Reading**

Find additional Samsung KNOX platform resources, including white papers, videos and more at samsungknox.com/en/support.

To read the Google report, Android Security—2014 Year in Review, go to https://goo.gl/KmUzSb.

For information on Android open platform security, visit http://goo.gl/YRN3wX.

For additional information about security, visit the Samsung blog at security.samsungmobile.com.