Android security maximized by Samsung KNOX

Safeguard enterprise mobility with tightly integrated security, compliance, and control features

SAMSUNG

Contents

Google and Samsung are both committed to mobile enterprise security, each bringing its own considerable expertise on protecting devices and data.

Google Android™ Lollipop

The Lollipop release improves the default security of the Android platform with new security features including:

- Verified Boot defenses against unauthorized modification of the operating system during the boot process.
- Basic VPN functionality for secure connections to enterprise networks.
- Google Safe Browsing technology to block phishing and malware attacks.

Google supports and even encourages device manufacturers, including Samsung, to build upon this solid base to provide solutions that fully address the security issues facing enterprise customers:

- Regulatory compliance
- Liability
- Risk tolerance
- Peace of mind

As the clear leader in security and enterprise readiness among all Android OEMs, Samsung KNOX builds on Lollipop to deliver a comprehensive security solution that addresses these real-world issues for the most demanding enterprise customers.

Samsung KNOX

KNOX is Samsung's defense-grade mobile security platform built into its newest devices. Just turn the device on and you're protected.

Cyber-attacks are generally designed to exploit weaknesses in device software implementation and architecture, or the attack surface. KNOX is designed to minimize the attack surface of devices by:

- Fortifying weaknesses that known attacks have commonly exploited in the past.
- Anticipating and defending against other more insidious categories of attacks.

With large classes of common attacks rendered ineffective against properly configured KNOX-protected devices, would-be attackers are forced to quit or attempt increasingly sophisticated attacks that require more time, money, and expertise.

KNOX is always vigilant

To combat attacks, KNOX establishes defense mechanisms at the time of design, time of manufacture, boot time, software load time (from disk to RAM), and run time as described in the following sections:

Time of design

By design, Samsung KNOX fully leverages the hardware Trusted Execution Environment (TEE) capabilities found in Samsung's flagship mobile devices, as well as many others. Without a TEE or equivalent, secure computing cannot be meaningfully achieved. For example, TEE uses ARM® TrustZone®.

Warranty bit

The KNOX warranty bit is a one-time programmable fuse that is blown when evidence of tampering is detected of bootloaders or the kernel. Thereafter, the device can never run Samsung KNOX, access to the Device Root Key, and access in the TrustZone secure world is revoked. In addition, users cannot access enterprise data on the device.

Time of manufacture

Samsung manufactures and configures its devices in its own factories. This means that Samsung has total control over the state of the device software leaving the factory.

In addition to provisioning the software, Samsung provisions each device with certain cryptographic data upon which nearly all higher-level security processes depend. These include a Device Root Key (unique per unit manufactured) and a Samsung Secure Boot Key (unique to Samsung, but the same on all Samsung devices).

Other device manufacturers that outsource hardware cannot guarantee the same end-to-end control of these critical security elements.

Figure 1. Samsung KNOX makes Android secure for enterprises

Boot-time defenses

One of the most fundamental requirements of mobile security is to ensure the authenticity and integrity of the software that is allowed to run on the device. This includes the stock operating system as well as all the modules that the OEM is required to provide.

KNOX employs its Secure Boot and Trusted Boot to ensure that they verify both the authenticity and integrity of the bootloader modules and the Android kernel. It does this by sequentially verifying chunks of code against previously-generated cryptographic signatures stored in secure memory of the TEE.

Load-time defenses

Smartphones and tablets have a large amount of preloaded system software beyond the operating system kernel. The size of this system software makes it impractical to verify its integrity and authenticity at boot time as it would introduce unacceptable start-up delay for the user.

Like all Lollipop devices, KNOX employs a technique called DM-Verity to ensure the integrity of system software not covered by the boot time checking described earlier. However, Samsung's implementation of DM-Verity differs from stock Lollipop in several important ways:

1. Modified to accommodate the real-world need for devices to accept firmware over-the-air (FOTA) software updates.
2. File-based instead of block-based to support carrier-specific and region-specific software builds
3. Its use is optional for non-enterprise consumer users of devices.

With Secure Boot, Trusted Boot, and DM-Verity, enterprises can feel confident that the software is authentic and uncompromised by the time it is loaded into RAM for execution.

Run-time defenses

Some more sophisticated attacks seek to compromise the system or intercept data at run time.

Periodic Kernel Measurement (PKM)

TrustZone-based Integrity Measurement Architecture (TIMA) PKM performs continuous periodic monitoring of the kernel to detect if legitimate kernel code and data have been modified unexpectedly.

Real-time Kernel Protection (RKP)

TIMA RKP performs ongoing real-time monitoring of the operating system from within TrustZone to prevent tampering of the kernel. RKP intercepts critical kernel events that are then inspected in TrustZone. If an event is determined to have unauthorized impact on the integrity of the OS kernel, RKP either stops the event, or logs an attestation record that tampering is suspected. This protects against malicious modifications and injections to kernel code, including those that coerce the kernel into corrupting its own data.

Attestation

Attestation reads the Trusted Boot collected measurement data and the fuse value, then combines the data in a proprietary way to produce an Attestation verdict that can be requested on-demand by the enterprise's MDM, typically before creating the KNOX Workspace. This verdict, essentially a coarse indication that tampering is suspected, is returned to the requesting MDM. The attestation verdict is cryptographically signed to ensure its integrity and authenticity.

Update-time defenses

Rollback Prevention blocks the device from loading an approved but old version of boot components during Trusted Boot. Old versions of software may contain known vulnerabilities that attackers can exploit. Rollback prevention checks the version of the bootloader and kernel during both Trusted Boot and updates, and blocks these processes from continuing if versions are unacceptably old. The lowest acceptable version of the bootloader is stored in secure hardware fuses at the time of manufacture, and the lowest acceptable version of the kernel is stored in the bootloader itself.

Table 1 - Summary of KNOX Defenses Mechanisms

Feature	Description
Hardware	
Samsung Secure Boot Key	Verifies that all firmware is from Samsung before allowing the device to boot.
Device Root Key	Provides a unique key per device that is used to perform cryptographic operations (authentication and encryption) associated with that specific device.
Warranty Bit	Creates a one-time, writeable hardware "fuse" used to flag devices whose system software has been replaced, in part or in full, either intentionally or maliciously.
Rollback Prevention Fuses	Set at manufacturing time in the Samsung factory to prevent old firmware versions from overwriting newer ones.
Bootloader	
Secure Boot	Ensures the integrity of each component of the boot software until just before the Android kernel is launched. (Uses the Samsung Secure Boot Key). If anything else tries to run outside of the valid, trusted sequence, the boot process terminates.
Trusted Boot	Builds upon Secure Boot to ensure the end-to-end integrity and consistency of boot software—including the kernel—for the entire boot process. Any evidence of tampering is permanently logged.
Rollback Prevention	Uses rollback prevention fuses to ensure that an old (but valid) firmware image cannot overwrite more recent images.
TrustZone	
Periodic Kernel Measurement	Performs continuous periodic monitoring of the kernel to detect if kernel code or data has been modified by malicious software.
Real-time Kernel Protection	Maintains runtime integrity by monitoring critical events that occur in the Android kernel and enforces protection of the kernel code so that it cannot be moved, changed, or amended.
Attestation	Allows a device to attest to a remote server, such an MDM server, that it has loaded authorized images during boot time.
TIMA KeyStore	Provides applications with services for generating and maintaining cryptographic keys. The keys are further encrypted with the device-unique hardware key that can only be decrypted by the hardware inside TrustZone.
Client Certificate Management	Enables storage and retrieval of digital certificates for encryption, decryption, signing, verification, and other operations.
Fingerprint Authentication	Requires apps to use fingerprints as a primary or two-factor authentication with checks performed in the TrustZone.

Application-level security mechanisms

Once KNOX verifies device integrity, the next hurdle is to address the security of the applications and data. Organizations must ensure that data stored on devices cannot be breached or shared inappropriately, and that applications accessing company information can be used only for corporate purposes.

Android Lollipop provides baseline data and application security. There is an Android KeyStore, which can encrypt and store cryptographic keys. Android Work Profiles can isolate personal apps and data from enterprise apps and data. You also get basic VPN functionality for a secure connection to corporate resources, as well as a way to identify harmful apps by using the Google Safe Browsing scanner.

Samsung KNOX significantly builds and improves upon this foundation to provide enterprise-class mobile application and data security. Cryptographic keys and other important security data is stored hardware in TEE – allowing only authorized users to access confidential data. Encryption and container technologies also keep data and applications safe – preventing corporate data from being shared inappropriately.

Table 2 - Application-level security features

Feature	Description
TIMA KeyStore	Improves upon the standard Android KeyStore by denying access to its contents when Trusted Boot or Warranty Bit reports that the device has potentially been compromised. Stored keys cannot be cloned for use on other devices.
TIMA Client Certificate Management (CCM)	Enables cryptographic keys to be sequestered in a secure area of the device, so that private key information is never exposed to the Android operating system.
Workspace	Offers a defense-grade, dual-persona container product designed to separate, isolate, encrypt, and protect work data from attackers. This work/play environment ensures work data and personal data are separated and that only the work container can be managed by the enterprise. Personal information such as photos and messages are not managed or controlled by the IT department. Once activated, the KNOX Workspace product is tightly integrated into the KNOX platform.
Sensitive Data Protection	Builds upon Workspace encryption, defining a sensitive class of data, which the device cannot decrypt without user intervention. TIMA KeyStore used to manage cryptographic keys.
VPN Framework	Adds FIPS 140-2 certified cryptographic algorithms, or the option to use CCM to manage cryptographic keys, to establish secure VPN connections to corporate network resources. Integrates with Workspace to assure that applications route network traffic through approve channels.
SSO Framework	Enhances authentication of Workspace apps by providing a common framework. Backed by TIMA KeyStore and CCM.
On-Disk Encryption	Uses a derivative of the Device Root Key to strengthen Android's On-Disk Encryption feature, ensuring that copying the raw data from one device to another is not possible.
Hardware Attestation	Uses a derivative of the Device Root Key, plus measurements collected from Trusted Boot, Warranty Bit, and RKP, to securely attest the state of the device to a remote server.
No Mandated Cloud Connection	Eliminates the requirement to connect an employee's device to a third-party cloud server (Google Cloud). KNOX license server can be deployed as an on-premises instance to avoid any cloud connection.

Independently certified

Because of these security capabilities that allow users to trust their data, Samsung KNOX has been awarded multiple, internationally recognized security certifications from governments around the world.

Table 3 - Independent Security Certifications

Country	Certification	Issued by
USA/Canada	Federal Information Processing Standard 140-2 Certification – Level 1 certification for both data-at-rest (DAR) and data-in-transit.	National Institute of Standards and Technology (NIST)
USA	Security Technical Implementation Guides (STIGs), DISA Approved Product List	Defense Information Systems Agency (DISA)
USA	Common Criteria Certification for Mobile Device Fundamental Protection Profile (MDFPP)	National Information Assurance Partnership (NIAP)
USA	US Department of Defense Approved Products List	National Information Assurance Partnership (NIAP)
UK	End User Devices (EUD) Security Guidance	Communications and Electronics Security Group (CESG)
Finland	Finnish National Security Auditing Criteria (KATAKRI II)	Finnish Communications Regulatory Authority (FICORA)
Australia	Protection Profile for Mobile Device Fundamentals	Australian Signals Directorate (ASD)

Security that fits your existing IT infrastructure

Enterprises large and small have diverse needs when it comes to device management. Samsung KNOX provides enterprises comprehensive control to configure the Workspace to their needs using an extensive set of more than 1500 Mobile Device Management (MDM) APIs.

Samsung KNOX also provides utilities that allow ready deployment in enterprises such as per-application VPN controls, a smartcard framework, and Single Sign-on (SSO) integration with Microsoft Active Directory. These features enable Samsung KNOX to easily integrate into any enterprise.

Table 4 - Defense-grade security features

Enterprise Mobility Infrastructure	
Identity/Email Registration	KNOX allows you to avoid registering an email address with Google to manage user identity on a device.
Exchange/ActiveSync	KNOX supports use of Exchange/ActiveSync for messaging.
LDAP Support	KNOX has explicit built-in support for LDAP account configuration and credentials. KNOX also supports Microsoft Active Directory.
VPN	KNOX provides tailored support for a growing list of industry-leading VPN clients from Cisco, Juniper, Mocana, F5, OpenVPN, StrongSwan and more. The VPN framework also allows easy adoption of additional VPN solutions.
Third-party Container Support	KNOX enables third-party container solutions to benefit from various KNOX security features.
Firewall Configuration	KNOX provides APIs to configure firewall policies.
User Experience	
Multiple Simultaneous Containers	KNOX supports multiple simultaneous containers/profiles, while Android alone can only accommodate one profile.
Kiosk and Container-Only Mode	KNOX kiosk and container-only mode allow clear work/personal boundaries.
Container UX	KNOX allows the user or enterprise to choose between three different user experiences, depending on the needs of the individual or organization: Classic (separate, isolated UX), Folder (pop-up UX), or Full Screen (continuous feed).
Mobile Device Management	
Onboarding/Enrollment	KNOX never requires devices to connect to Samsung servers to authenticate or register an identity for onboarding or enrollment.
Device Control	KNOX includes a fully integrated set of management tools that offer deep device control of security, usability, hardware, and application policies. KNOX also offers easy integration with third-party Mobile Device Management solutions.
My KNOX	Individual mobile professionals can use Samsung My KNOX to separate work and personal data separate.
Application Management	KNOX supports Google Play, Samsung App Store, KNOX marketplace, MDM solutions, and manual side-loading to deploy applications. All transactions are 100% anonymous in an enterprise-managed model. Android requires you use Google Play for every app management transaction and prohibits side-loading.
Telephony	KNOX enables policies to block incoming/outgoing voice and SMS.
Password Policy	KNOX extends Android password policies with more granular control over precise requirements for character sets, repeated characters, refresh periods, and reuse.
User Privacy	KNOX Workspace limits the employer's visibility into and control of the Workspace, putting the non-Workspace data and apps beyond the reach of the employer.

Comprehensive enterprise mobile security and productivity

When implementing your enterprise mobile strategy, Android devices alone are not enough. While the security features in Lollipop have improved Android's position with competitors such as iPhone, most enterprises find that their security and compliance requirements are not met.

Samsung KNOX augments Lollipop security features to produce a tightly integrated and holistic security architecture. By enabling all of the security, compliance, and control features enterprises require, organizations can use Samsung KNOX to enable worker productivity while also protecting corporate assets.

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of TVs, smartphones, tablets, PCs, cameras, home appliances, printers, LTE systems, medical devices, semiconductors and LED solutions. We employ 286,000 people across 80 countries with annual sales of US $216.7 billion. To discover more, please visit www.samsung.com.

For more information

For more information about Samsung Enterprise Mobility and Samsung KNOX, visit: www.samsung.com/enterprise and www.samsung.com/knox

SAMSUNG

Samsung Knox