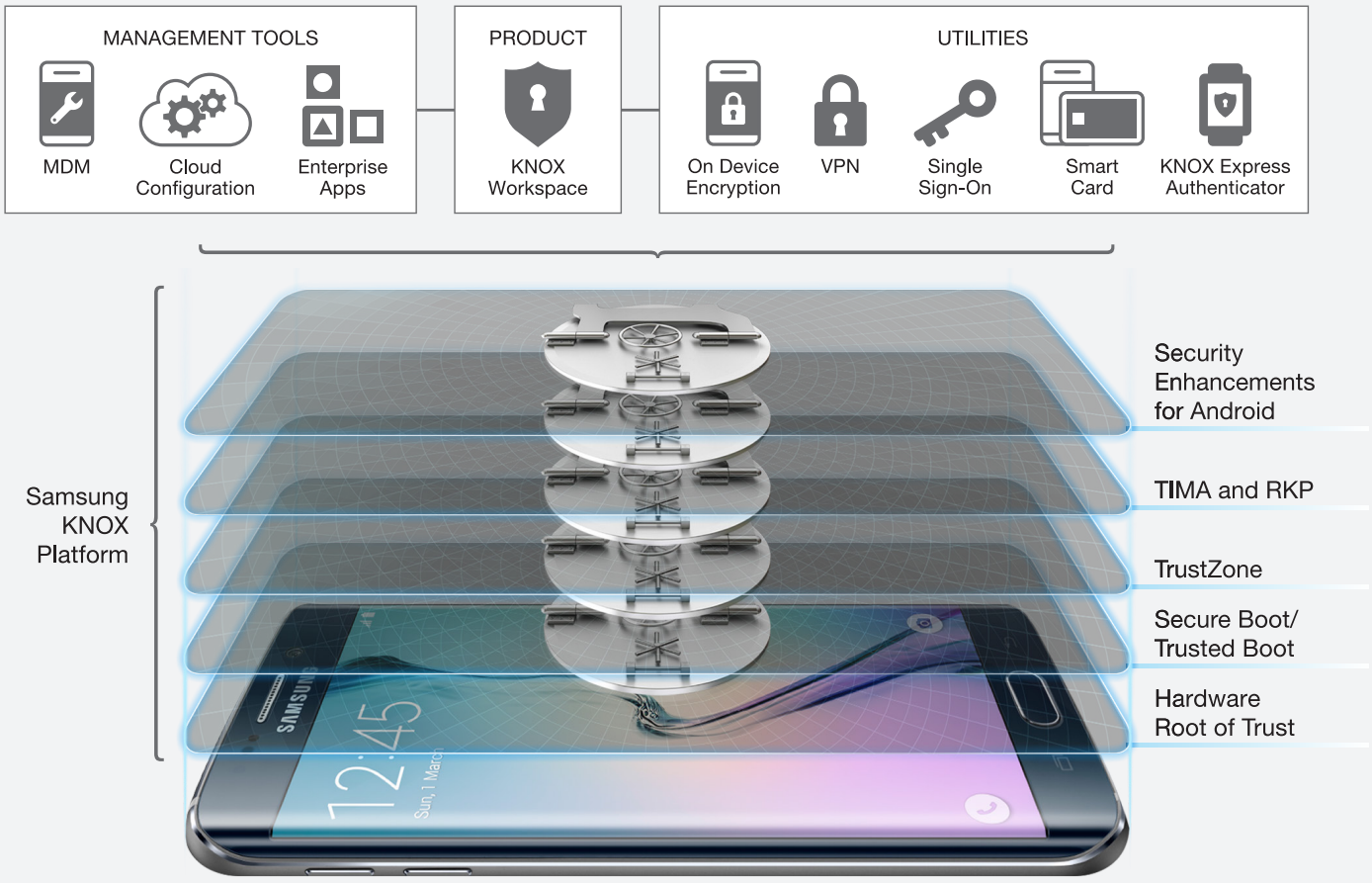
In-Depth Look at Capabilities:
Samsung KNOX and Android for Work

Samsung
KNOX



SAMSUNG
BUSINESS

Capability	Samsung KNOX	Android for Work
Silent Install	Using the Samsung KNOX Workspace Mobile Device Management (MDM) APIs, IT admins can install and enable applications automatically. The simplified enrollment process supports the fully automated creation of an enterprise-grade Workspace and provisioning of apps and policies. **KNOX adds:** Samsung KNOX Mobile Enrollment allows IT Admins to stage and enroll hundreds or thousands of employees automatically by configuring device information in the cloud. Samsung also provides a web tool and an application to scan smartphone package bar codes (the device IMEI).	Using the EMM console, IT admins can silently install, remove, and update apps inside Android for Work. This capability greatly simplifies the user experience (and makes life easier for IT admins) because no user intervention is required to update or remove apps.
Application Configuration	KNOX provides the following capabilities to IT admins: • Install and uninstall applications. • Restrict installation and uninstallation of applications. • Disable and enable applications. • Query the current state of an application. • Control application behavior. • Control notifications of applications. • Configure the email client. • Configure the SSL VPN Client for Cisco, F5 and Juniper.	Using the EMM console, IT admins can configure the settings for a particular application. When Android for Work is configured, app settings are pushed to the device.
Secure App Installation from Google Play	With more than 1500 MDM APIs, KNOX gives IT admins control over which apps can be run inside the Workspace, thus eliminating the problem of sideloading of untrusted apps. Additionally, administrators can deploy any app from the Google Play store to the Workspace, or allow users to install the Google Play app inside the Workspace. IT admin can also install applications from a private app store.	Google has introduced a new set of Google Play APIs for EMM providers to enable app management and distribution and control app deployment in Android for Work. As a result, malicious apps cannot be sideloaded. This new process, combined with the Lollipop Android for Work Profile, enables IT managers to deploy any Play app in the Google Play Store to a secure Android container without any additional wrapping.
Privacy for Self-hosted Apps	KNOX enables private enterprise apps to be installed on a device.	Organizations concerned about security for their private, in-house apps can choose to self-host these apps either internally or through their EMM provider. Either way, self-hosted apps can be excluded from public search results in the Google Play Store.
Separate Container for Work Apps	The KNOX Workspace provides an isolated environment and UI for enterprise use consisting of a separate home screen, launcher, enterprise apps, and widgets. Data owned by apps in the KNOX Workspace is protected by extensive Data At Rest (DAR) protections. IT admins can use KNOX's extensive set of Workspace configuration APIs to provision and configure the Workspace and its DAR protections.	Android for Work simplifies mobile app management and security by providing a secure profile, or container, to Android devices running Android 4.0 and higher. IT admins can use an EMM to securely provision and containerize apps on any device with an Android for Work Profile (Android Lollipop), or the Android for Work app (Android 4.0 4.4).
Suite of Productivity Apps (email, calendar, etc.)	KNOX applies a badge to apps running in the Workspace to help the user distinguish them from personal apps.	Android for Work features a suite of secure, badged PIM apps designed to help workers easily distinguish between personal and work apps on the device.

Capability	Samsung KNOX	Android for Work
Data Loss Prevention	KNOX MDM policies can regulate sharing of information between the Workspace and personal apps. This includes sharing of calendar, contacts and notifications. Copy/paste clipboard data is blocked from the Workspace environment to the personal environment, and vice versa. **KNOX adds:** **Sensitive Data Protection** Any sensitive data received when the Workspace is locked will still be protected by Sensitive Data Protection (SDP). This works by using a public key algorithm in which the private part of the key is maintained in an encrypted partition, and the public part is used to encrypt the new sensitive data. Once the Workspace is unlocked, the data is decrypted with the private key, and re-encrypted using the usual symmetric key, which is guarded by the CMK. Currently, email subjects, bodies and attachments are marked sensitive. Additionally, the SDP Chamber provides a directory, in which all files are automatically marked as sensitive, and protected by SDP.	EMM governance policies manage a user's ability to share into and outside of Android for Work. This includes the ability to block copy/paste or block screen capture for apps inside the managed profile. (Note that copy/paste can be disallowed from the managed profile to the personal profile, but not vice versa.)
Container VPN	KNOX enables additional modes of granular VPN capabilities both for the Workspace and individual apps. The MDM-configurable KNOX VPN supports multiple concurrent VPN connections allowing for IPSec or SSL VPNs with configurable auto-reconnect and VPN tunnel chaining. The KNOX VPN subsystem also supports other forms of packet processing, including split billing and network access control. **KNOX adds:** Enterprise Billing provides enterprises a mechanism to separate enterprise data usage from personal data usage. This enables enterprises to compensate employees for costs generated because of work, particularly in BYOD cases, or to only pay only work-related data in COPE cases. **VPN features of KNOX include:** • Administrator-configured System VPN. • Administrator-configured Per-App VPN. • Administrator-configured Workspace VPN. • Multiple concurrent VPN connections. • IPsec and SSL VPN support. • Administrator-configured FIPS and non-FIPS VPN mode. • Common Access Card (CAC)-based authentication. • Always on VPN connections with auto-reconnect. • VPN tunnel chaining.	Android for Work enables granular VPN capabilities within the managed profile, which eliminates the need for a device-wide VPN. With these new capabilities, IT can maintain greater security and control over corporate app communication on the device.
Selective Wipe	IT admins can wipe internal and external SD cards and application data. The entire container can be locked when compromised and can be deleted with all its data.	Android for Work enables IT administrators to easily retire lost or stolen devices and remotely wipe all work data while leaving personal content intact on the device. With corporate-owned devices, IT has total device-wide controls, which include a full device wipe if necessary.

Capability	Samsung KNOX	Android for Work
Protection Against Malicious App Downloads	The KNOX Workspace isolates enterprise apps and data from personal user apps. Untrustworthy personal user apps outside the Workspace cannot affect the Workspace. **KNOX adds:** Real-time Kernel Protection (RKP) achieves three important security features: • First, RKP completely prevents running unauthorized privileged code (i.e., code that has the kernel privilege) on the system, which is accomplished by preventing modification of the kernel code, injection of unauthorized code into the kernel, or execution of the user space code in the privileged mode. • Second, RKP prevents kernel data from being directly accessed by user processes. This includes preventing double mapping of physical memory that contains critical kernel data into user space virtual memory. This is an important step to prevent kernel exploits that map kernel data regions into malicious processes where they could be modified by an attacker. • Third, RKP monitors some critical kernel data structures to verify that they are not exploited by attacks. In particular, RKP protects the data that defines the credentials assigned to running user processes to prevent attackers from escalating this credential by modifying this data. **KNOX Warranty Fuse.** The KNOX warranty bit is a one-time programmable fuse that signifies whether the device has ever been booted into an unapproved state. If the Trusted Boot process detects that non-approved components are used, or if certain critical security features such as SELinux are disabled, it sets the fuse. Thereafter, the device can never run Samsung KNOX, device access to the DUHK and DRK in the TrustZone Secure World is revoked, and enterprise data on the device cannot be recovered. **TIMA Attestation** TIMA Attestation allows a device to attest facts about its state to a remote server, such as an MDM server. The attestation message contains state measurements that can be evaluated by a server, which can then decide whether to trust the device or not. This message contains: • Measurements collected by Trusted Boot to prove that only approved system software was loaded during boot. • Security violation logs from PKM and RKP since the last reboot. • Status of the KNOX warranty violation fuse. • Whether SE for Android is running in enforcing mode. • Device-identifying information such as the IMEI and Wi-Fi MAC address. • A locally-computed verdict whether the device believes it is in a trustworthy state.	Android for Work protects business apps and data from issues arising from the user's personal activity outside the profile, such as sideloading web apps, ordering from unknown websites and other potentially insecure activity.

Capability	Samsung KNOX	Android for Work
Protection Against Malicious App Downloads (continued)	**Trusted Boot-based KeyStore (TIMA KeyStore)** The TIMA KeyStore provides applications with services for generating and maintaining cryptographic keys. The TIMA KeyStore is only enabled if the Trusted Boot measurements match the known good values in the file tima_measurement_info, and if the KNOX warranty fuse is not set. Thus, cryptographic operations with keys in the KeyStore can only occur if the system was booted into an approved state. Keys stored in the TIMA KeyStore are further encrypted with the device-unique hardware key (DUHK), and can only be decrypted from within TrustZone Secure World on the same device. All cryptographic operations on the keys are performed within TrustZone Secure World. The TIMA KeyStore has the same API as the familiar Android KeyStore APIs. Therefore, the only modification necessary is to specify that the TIMA KeyStore be used to provide the service. **Trusted Boot-based Client Certificate Management (TIMA CCM)** The TIMA CCM enables storage and retrieval of digital certificates, as well as encryption, decryption, signing, and verification in a manner similar to the functions of a SmartCard. The certificates and associated keys are encrypted with a device-unique hardware key that can only be decrypted from code running within TrustZone. TrustZone-based CCM also provides the ability to generate a Certificate Signing Request (CSR) and the associated public/private key pairs in order to obtain a digital certificate. A default certificate is provided for applications that do not require their own certificate. Programming interfaces for certificate storage and management are provided in the KNOX Premium SDK. Application developers are provided with industry standard PKCS #11 APIs for certificate management, and therefore interact with the CCM as if it were a virtual SmartCard. Similar to the TIMA KeyStore, TIMA CCM operations are permitted only if the device was booted into an approved state.	
EMM Requirement	KNOX requires an EMM platform to manage KNOX policies on the device.	Android for Work requires a multi OS EMM platform.

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
BUSINESS