Samsung Knox Mobile Security White Paper

Revision 1.0

Contents

Introduction to Samsung Knox mobile security

In 2013, Samsung introduced Samsung Knox, a pioneering mobile security solution that set out to provide business-ready Android devices in the enterprise. This marked the beginning of a new era in mobile security, as organizations sought to harness the power of mobility while maintaining the high levels of data protection and control.

Since our inception, Samsung Knox has continuously evolved to address the shifting needs of enterprises. Initially, our focus was on developing isolation technology that enabled secure separation of work and personal data. As mobile adoption grew, so did our solution set, incorporating advanced enterprise manageability and productivity features alongside additional layers of protection on top of Android Enterprise.

We implemented cutting-edge security features to safeguard sensitive information, ensuring that our customers could confidently deploy mobile solutions across their organizations. Recognizing the need for a cloud-based solution that helps IT admins manage mobile devices securely and efficiently, we developed a suite of cloud services that simplify every step of the mobile device management journey for IT admins.

Key among these are:

- Knox Mobile Enrollment, which allows for automated device setup and EMM enrollment
- Knox E-FOTA, which lets you schedule and deploy firmware and security patch updates to your entire device fleet
- Knox Manage, which provides powerful cross-platform device management capabilities
- Knox Asset Intelligence, which provides detailed analytics related to device utilization and critical device issue and security vulnerability reporting.

As organizations sought to deploy mobile solutions in more demanding environments, such as frontline settings, we expanded the scope of Samsung Knox to include more business productivity offerings. This period also saw a significant focus on partnerships with major system integrators, who worked closely with us to deliver tailored solutions that met the unique needs of their clients. Today, we continue to innovate by developing devices built for specific industries or use cases, presenting unique solutions to their respective challenges. For example, with Samsung Galaxy Tactical Edition devices, soldiers can carry out mission-critical operations by leveraging our highest-security capabilities and controls.

With the rollout of Android 14, Samsung introduced the Knox Zero Trust Framework, enhancing Samsung Knox's security by ensuring that only authorized access and actions are permitted. With Android 15, we are taking significant steps forward to enable mobile devices in an increasingly connected security ecosystem, providing prioritized security alerts directly into the security operations center.

For Samsung Knox mobile device users, we are dedicated to driving the mobile security bar forward and working closely with industry partners to further secure both enterprises and consumers. For example, Samsung Auto Blocker and Samsung Message Guard make security a default on all Samsung Knox devices, ensuring that devices are in a secure state. Through these efforts, we remain committed to delivering mobile security solutions that are tailored to meet the expectations and specific demands of our diverse customer base.

Privacy policy

At Samsung Knox, we prioritize the safeguarding of user data through a multifaceted approach consisting of four core strategies:

1. Our policies let you predict how your data will be utilized.
2. Our privacy services make it easy to manage your data.
3. Our Knox technology adds multiple layers of confidentiality protections.
4. Our vulnerability program expedites our ability to quickly fix reported issues.

To review our privacy policy, manage your personal information, and access, delete, or correct your data, please visit Samsung Privacy. There, you can also opt-out of targeted ads and appeal Samsung's decisions with respect to your privacy rights requests.

If your device is configured for enterprise use with activated Knox features, you can also consult our Knox Privacy Policy. If you would like to report a security or privacy issue, please refer to the following section on the Bug Bounty Program.

Samsung Knox Security Principles

Trusted Computing Platform

The Samsung Knox platform is built upon Trusted Computing principles, ensuring that devices only execute authorized and validated code (such as cryptographic keys protecting enterprise data) during startup. This code is stringently measured and cross-referenced against a database of approved components (hashes) specific to each platform. In the event of unauthorized firmware compromise, access to critical data would be denied.

As both a device hardware and software manufacturer, Samsung is uniquely positioned to establish a trusted computing environment across all Samsung Knox devices. Our robust supply-chain-guarantees enable us to embed cryptographic keys and code directly into the hardware during manufacturing at the factory. This foundational element is referred to as a **Hardware-based Root of Trust** in trusted computing terminology.

Upon initial boot, a Trusted Boot chain is established, where each Samsung Knox boot component undergoes measurement and authentication before subsequent components can run. Once this chain of trust is formed, features like Real-time Kernel Protection (RKP) maintain the trust-chain integrity by regulating requests between the kernel and critical system components, thereby preventing attackers from compromising the kernel and accessing sensitive data.

After completing the boot process, Samsung Knox devices establish a secure connection with a trusted server to verify their integrity through Knox Device Health Attestation. This step enables enterprises to confirm that the device has booted correctly and hasn't been compromised.

The following diagram describes how Samsung Knox devices adopt trusted computing platform principles in greater detail:

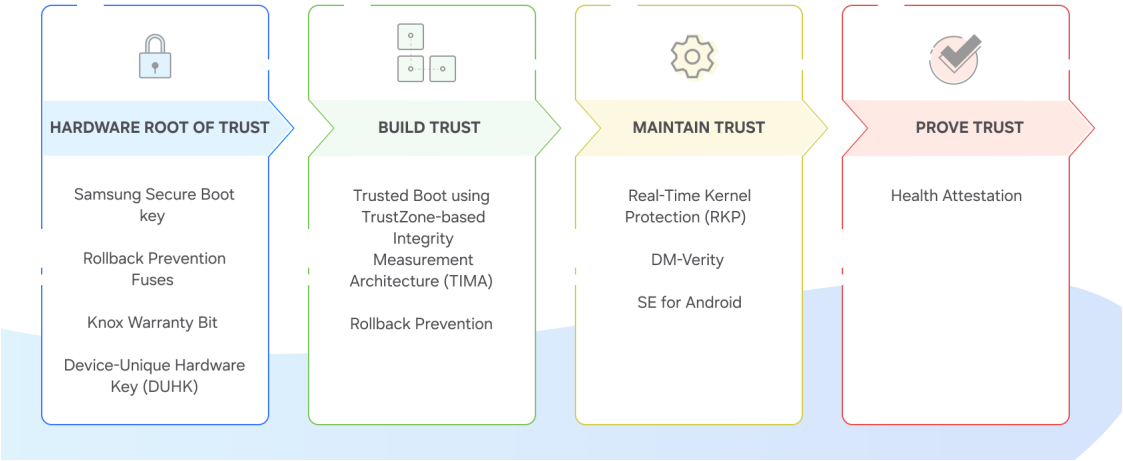

Figure 1: Trusted computing principles in Samsung Knox devices

Defense-in-Depth

Defense-in-Depth, also known as layered defense, is a fundamental security strategy that emphasizes the implementation of a multi-tiered defense framework, wherein each successive defense layer acts as an additional hurdle for would-be attackers. Should an attacker manage to infiltrate one defensive layer, they immediately face another. Consequently, this layered approach renders cyber-attacks progressively more challenging and economically unattractive, effectively discouraging attackers from continuing with their efforts.

Organizations must integrate devices supporting Defense-in-Depth frameworks due to four primary factors:

- Software retains hidden flaws exploitable by attackers.
- Suboptimal configurations expose vulnerabilities.
- Users remain prone to manipulation via social engineering techniques such as phishing emails or fake websites.
- Hardware embeds undetected weaknesses that can be targeted by adversaries.

The following diagram describes a typical malware infection cycle and the various stages in which malware passes through a device:

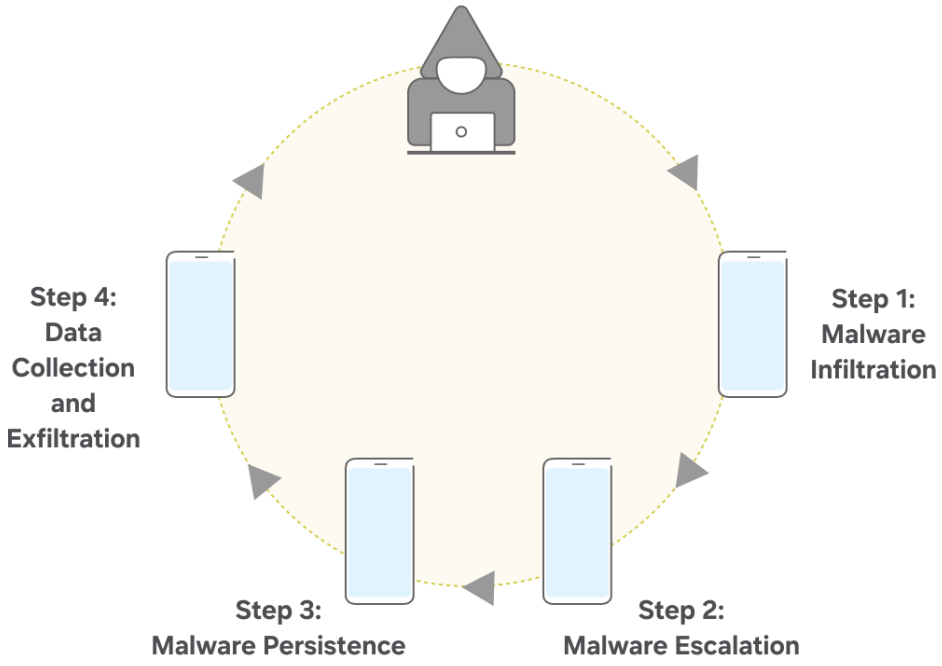

Figure 2: Cycle of typical malware infection

Samsung Knox devices come equipped with multiple defense mechanisms to combat malware infections at various stages. Below, we outline these features categorized by attack phase:

Infiltration

Malware can infiltrate devices through various vectors. Samsung Knox addresses each vector with dedicated defenses:

- **Phishing**: Knox Suspicious URL Detection helps protect against phishing attacks by providing on-device detection of malicious or potentially harmful links, and sending alerts to IT and security admins for immediate review and response actions.
- **Network**: Knox Firewall blocks HTTP traffic, Secure Wi-Fi automatically protects insecure Wi-Fi connections, and Samsung Internet supports content blocker plugins that can filter out harmful web traffic.
- **Peripherals**: Hardware Device Manager, implemented in the hypervisor, disables peripherals such as USB, Bluetooth and cellular modems, while the Auto Blocker, implemented in the Android framework, blocks malicious AT commands sent over USB.

- **Zero-Click Exploits**: Message Guard protects messaging apps (including SMS and other third-party messaging apps) from exploits that can coerce message-parsers into running malicious code without any user interaction.

Escalation

Once inside, malware seeks elevated privileges using rooting or kernel exploits. Samsung Knox counters these attempts with:

- Real-time Kernel Protection: A hypervisor-based protection feature that prevents privilege-escalation to the Linux kernel.
- DEFEX: A Linux kernel-level protection feature that allows only authorized binaries to run with superuser (root) privileges. Knox Security Log monitors suspicious activity indicative of malicious intent.

Persistence

Persistent malware reinstalls itself during reboots. Samsung Knox combats persistence via:

- Knox Verified Boot: Ensures that the device boots up with only authorized code components, starting from the very first piece of code that runs when the device is switched on to the Android framework system components.
- Knox Warranty Bit: Stores a tamper-proof record of whether a device has ever booted up with unauthorized code. Additionally,
- Knox Health Attestation: Proves to a remote verifier whether a device is running authorized code.

Data Collection and Exfiltration

Finally, malware collects and transmits stolen data. Samsung Knox defends against this with:

- HDM: Disables peripherals, preventing them from being used for data collection or exfiltration.
- Knox Firewall: Allows flexible firewall customization, restricting unwanted data transfer.

Additionally, Samsung Knox incorporates Dual Data-At-Rest (Dual DAR) encryption and Universal Credential Management for enhanced data confidentiality and integrity.

Zero Trust

Zero Trust is a security strategy that aims to minimize implicit trust in entities that handle enterprise data. Entities, such as users and endpoints[1], need to continuously prove their trustworthiness to the enterprise to be allowed access to resources[2].

Defining Zero Trust

NIST's Special Publication 800-207 on **Zero Trust Architecture** defines a core Zero Trust tenet as follows:

> "Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes."

In other words, a key principle of Zero Trust architecture states that an enterprise must regulate access to their resources by continuously evaulating *user and device identity*, *device health*, and other contextual information such as *location* and *frequency of access*. In more simple terms, just because a device is authenticated within the enterprise VPN, it doesn't mean that the device should be trusted automatically.

This approach (as described in the following diagram) allows dynamic access control in contrast to traditional perimeter-based approaches such as VPNs, where any entity within the enterprise's VPN perimeter is fully implicitly trusted to handle enterprise data.

[1] Endpoints are user-facing devices that request access to enterprise resources. Endpoints include laptops, desktops, mobile phones, and tablets. In this white paper, we use the terms "device" and "endpoint" interchangeably.

[2] Enterprise resources include enterprise data, apps, and services such as printers.

Figure 3: Zero trust architecture

For each resource request, the device evaluates its health and user identity, and gathers other context. The device then sends this information to a **Policy Decision and Enforcement Point**, which decides whether to allow the device access to the requested enterprise resource. If access is allowed, the requested resource is sent back to the device.

With a traditional perimeter-based security strategy, if an attacker compromises a single device or user credential, they can easily breach the entire enterprise network. With a Zero Trust strategy, access is granted *dynamically* (at time of request), which dramatically reduces the impact of a compromised endpoint or credential.

Zero Trust with Samsung Knox devices

Zero Trust security principles are designed into the architecture of all Samsung Knox devices, allowing organizations to leverage Samsung devices as secure and reliable entry points into any network. When Samsung Knox devices are utilized as endpoints in an enterprise, they can:

- Continuously monitor and authenticate user and device context by connecting the Knox Asset Intelligence Security Center to your organization's Security Operations Center (SOC).
- Send augment-network-requests through our Knox Zero Trust Network Access (ZTNA) framework. These requests contain user and device context metadata that gets used by the **Policy Decision and Enforcement Point** to decide whether to allow or deny access to enterprise resources.

Enterprises often deploy multiple security solutions across various teams, creating complexity and requiring specially trained security professionals to manage threats across different device platforms. Samsung Knox aims to eliminate the complexity associated with enterprise mobile device management. Whether it's through our robust in-house endpoint management solutions, or our continued collaboration with industry-leading security solution providers, Samsung Knox is leading the charge towards a more secure future for all customers.

System Security

Secure Hardware Supply Chain

Samsung's secure hardware supply chain and manufacturing is a foundation for the strong security guarantees offered by Samsung Knox. Several hardware components that are a basis for Samsung Knox's security guarantees, such as security chips, secure storage, and per-device cryptographic keys, are integrated and provisioned in the factory.

As a device hardware manufacturer, Samsung is uniquely positioned to provide strong hardware supply chain guarantees. We utilize an end-to-end security approach, overseeing and controlling the entire process of designing, manufacturing, and delivering our equipment—including chips, hardware, and software.

Furthermore, the robust physical access controls and real-time monitoring systems employed at our manufacturing facilities ensure Samsung products are safely and securely assembled and delivered to our customers.

Multi-layered physical security

Samsung's manufacturing facilities and production lines follow a high level of security standards, including conveyance security[3], security seals[4], inspection processes, locking mechanisms, and detection devices.

The entire supply chain is protected with thorough container-specific security and storage protocols. Secure Samsung and designated supplier facilities are specifically built and monitored to resist unlawful and forcible entry and protect against outside intrusion. A range of physical access controls is employed to ensure that only authorized personnel gain entry within the scope of their responsibilities.

[3] Conveyance security prevents cargo from being tampered during transportation through management, inspection, and training.

[4] Security seals protect cargo against tampering and theft.

Hardware-Backed Security

Hardware components

Knox leverages the following hardware components to create a trusted computing platform.

Bootloader ROM

The Primary Bootloader (PBL) is the first piece of code to run during the boot process. The PBL is trusted to measure and verify the boot chain. To prevent tampering, the PBL is kept in the ROM of the secure hardware. The device hardware loads and runs the PBL from ROM at boot, and the PBL starts the Secure and Trusted Boot processes.

Arm TrustZone Secure world

The Secure world is the environment in which highly sensitive software runs. Arm TrustZone hardware ensures memory and components marked secure (e.g., a fingerprint reader) can only be accessed in the Secure world.

Most of the system, including the kernel, middleware, and apps, runs in the Normal world. Secure world software, on the other hand, is more privileged, and can access both Secure and Normal world resources.

Knox Vault

The Knox Vault is an independent, tamper-proof, secure subsystem with its own processor, memory, and an interface to dedicated non-volatile storage. It stores sensitive data such as cryptographic keys and authentication data. Even if the main application processor that runs Android is compromised, the Knox Vault protects secrets and guards against hardware attacks such as probing and fault injection.

The Knox Vault is available on select devices.

Hardware keys

Device-Unique Hardware Key (DUHK)

Samsung incorporates the DUHK, a device-unique symmetric key, in the device hardware during the initial manufacturing of the device. The DUHK binds data (e.g., cryptographic keys) to a particular device, is accessible only by a hardware cryptography module, and isn't directly exposed to any device software.

However, TrustZone Secure world software can request that the DUHK encrypt and decrypt data. This DUHK encrypted data is bound to the device, and thus can't be decrypted on any other device.

Samsung Secure Boot Key (SSBK)

The SSBK is an asymmetric key pair used to sign Samsung-approved boot executables:

- The private key is used by Samsung to sign secondary and app bootloaders.
- The public key is stored in the hardware's one-time programmable fuses when the device is manufactured in one of Samsung's factories. The Secure Boot process uses this public key to verify whether each boot component it loads is approved.

Knox Device Health Attestation Key (SAK)

The SAK is a device-unique, Elliptic Curve Digital Signature Algorithm (ECDSA) asymmetric key pair. The public key is signed by Samsung's root key, which proves that the SAK was produced by Samsung.

The SAK is generated when the device is manufactured in one of Samsung's factories and is either stored in the Knox Vault (on supported devices), or encrypted by the DUHK, which binds it to the device. It is only accessible from within the Knox Vault or the TrustZone Secure world and is an important part of the Root of Trust, as it derives other signing keys.

Because the SAK is device-unique, it can tie data to a device through cryptographic signatures. Signing keys derived from the SAK is used to sign data for various purposes. Most notably, the SAK is used to sign the Knox Device Health Attestation that indicates if the device is in a trusted state. This signature proves that attestation data originated from the TrustZone Secure world or Knox Vault on a Samsung device.

Knox Rollback Protection Fuses

Knox Rollback Prevention Fuses encode the minimum acceptable version of Samsung-approved bootloaders.

Once a bootloader containing approved new software is installed, it fuses the version of that bootloader to hardware, preventing old software from being loaded. Without this feature, old firmware, which could have known vulnerabilities, can be exploited.

The Rollback Prevention fuse version number is set during initial installation of system software and is adjusted following specific software updates. Once the fuse version number is set, it is impossible to revert back to legacy software versions.

Knox Warranty Bit

The Knox Warranty Bit provides a tamper-resistant and persistent record of when a device runs in a non-approved state. This record is stored in a one-time hardware e-fuse, permanently marking the device as having a non approved configuration, regardless of any future actions.

Samsung continually monitors the integrity of several different components, detecting if any particular component is in a non-approved configuration. For example, the Trusted Boot process sets the Knox Warranty Bit when it detects that an unsigned kernel is loaded, or when a critical security feature such as SELinux is disabled.

These types of checks are critical as non-approved components could lead to vulnerabilities such as privilege escalation or access to normally protected peripherals. Non-approved components can also lead to vulnerabilities being persistent over reboots or even future updates (e.g., returning to an approved component).

For enterprises, having a feature like Knox Warranty Bit ensures that a previously compromised device *cannot* be brought back into a seemingly compliant state and used normally. Samsung integrates Knox Warranty Bit measurements into several checks on the device, both during and after boot. This ensures that some actions can only be taken *after* the device status is verified, actions such as:

- **Gaining access to device-bound data within the KeyStore**: The Knox Warranty Bit value is used in the decryption of device-bound (wrapped) keys stored in the KeyStore, along with all data protected by those keys. If the Knox Warranty Bit is set, then any device-bound data stored on the device becomes completely inaccessible.

- **Accessing certain Knox services**: Knox Device Health Attestation reports whether a device has been compromised, and relays this status to other requesting services. In the event a device has its Knox Warranty Bit set, you may be able to use the device after a factory reset, but certain Knox functions (like creating a work profile), or functions that rely on Knox security (like Samsung Pay) are blocked.

As a persistent record of a device's state, the Knox Warranty Bit helps you ensure that your Samsung devices remain in a trustworthy state during its lifecycle.

Knox Vault

Samsung's Knox Vault is an evolution of the hardware-based security that Samsung has been building within Galaxy smartphones for years. Knox Vault extends upon the protection offered by our TrustZone, the Trusted Execution Environment (TEE) pioneered by Samsung to protect sensitive data such as passwords, biometrics, and cryptographic keys. Whereas the TrustZone runs a different OS alongside Android on the primary application processor, Knox Vault operates completely independently from the primary processor running the Android OS.

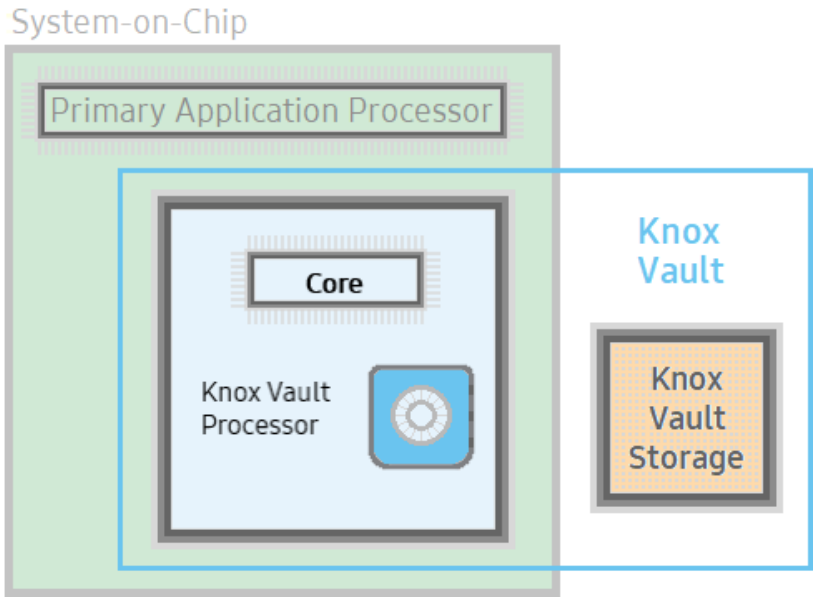

Figure 4: Knox Vault architecture

As a core component of the Knox security platform, Knox Vault is an isolated, tamper-proof, secure subsystem with its own processor and memory. It also includes an interface to dedicated, non-volatile secure storage, which provides a secure location for storing sensitive data, such as cryptographic keys and credentials. Knox Vault can:

- Store sensitive data such as hardware-backed Android Keystore keys, the Knox Device Health Attestation Key (SAK), biometric data, and blockchain credentials.
- Run security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.

Knox Vault is integrated into select Samsung devices starting from the Galaxy S21, and is comprised of components that are Common Criteria evaluated to the requirements in BSI PP0084 at EAL4+ or higher. These components are tested by an independent lab against a wide array of hardware attacks and through a review of their software and firmware.

Knox Vault provides strong security guarantees against both software and hardware attacks, as it is independent from the primary processor that runs Android. This isolation ensures that code running on the Knox Vault Processor is resistant to attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor. This separation means Knox Vault protects sensitive data even if the primary processor itself is completely compromised.

In addition to being resistant to software attacks, Knox Vault is also designed to be tamper-proof to thwart hardware attacks, which require that an attacker have physical possession of a device to extract secrets. Knox Vault is resistant to hardware attacks such as physical probing, side channels, and fault injection. For details about these attack types, see Protection from Hardware Attacks.

Knox Vault Features

Samsung Weaver

Samsung Weaver is used for secure password authentication to Android. Running on the Knox Vault Processor, Weaver's data and secrets (passwords) are stored encrypted in the secure Knox Vault Storage. When Weaver receives the secret data to be stored, it also receives a key, and this key must be provided to read the secret data again from Weaver.

To prevent brute-force attempts to extract secrets, Weaver uses a binary exponential back-off algorithm. When attempting to read a secret, if the proper key is not provided, Weaver declines read operations for a time period decided by the back-off algorithm. A non-bypassable secure timer is used to track these time periods.

Credential Storage

This feature securely stores data encrypted by the Knox Vault Processor in the Knox Vault Storage. A secure channel is used to protect data transferred between the Knox Vault Processor and the Knox Vault Storage.

The following data is stored in the Knox Vault Storage:

- Cryptographic keys to protect biometric data
- Blockchain keystore credentials
- Knox Device Health Attestation Key (SAK)

All data in credential storage is encrypted using a Knox Vault-unique key. This prevents the data from being decrypted in other devices.

StrongBox Keymaster Support

The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.

The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

Knox Vault Architecture

Knox Vault is made up of the following:

- **Knox Vault Subsystem** implemented as part of the System-on-Chip (SoC).
- **Knox Vault Storage**, an integrated circuit physically outside the SoC.

Through a secure interface, the Knox Vault Subsystem communicates with the Knox Vault Storage.

Knox Vault Subsystem

The Knox Vault Subsystem is designed to operate separately from other SoC components. It has its own secure processing environment consisting of the Knox Vault Processor, SRAM, and ROM. It also provides enhanced security and data protection against various hardware-based attacks, by monitoring the hardware status and its environment using a series of security sensors or detectors including:

- High and low temperature detectors
- High and low supply voltage detectors
- Supply voltage glitch detector
- Laser detector

The Knox Vault Subsystem also includes a dedicated random number generator, and its own Crypto Engine. The Knox Vault Processor can access system DRAM though the External Memory Manager.

Knox Vault Processor

The Knox Vault Processor provides the main computing power for Knox Vault. To provide the strongest isolation, the Knox Vault Processor is separated from the primary processor on the SoC. This separation helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

By executing the instructions and managing data on SRAM, the Knox Vault Processor also guarantees a physically isolated execution environment. The Knox Vault Subsystem ROM where the secure boot loader code is located is also separated and protected by the hardware protection mechanisms. When the Knox Vault Processor starts, the ROM code is loaded to SRAM. While the ROM code loads the Knox Vault Processor firmware, with the help of the modules running on the SOC main processor, the software stack of Knox Vault Processor has its own secure boot chain.

Hardware Monitor

The Hardware Monitor checks for abnormal hardware status from the security sensors and detectors. The monitoring and detection cannot be affected or bypassed by any application running on Knox Vault Processor.

Crypto Engine

A hardware cryptographic module provides the following cryptographic functions:

- Advanced Encryption Standard (AES) encryption and decryption
- Deterministic random bit generator (DRBG) random number generation
- Secure hashing algorithm (SHA) hashing
- HMAC keyed hashing for message authentication code
- RSA and ECC key generation and services

Knox Vault unique key

The Knox Vault unique key is written into one-time-programmable bits. This unique key is used for protecting keys imported into or generated in the Knox Vault Subsystem. Thus, a key generated in Knox Vault on one device cannot be used outside of that device.

External Memory Manager

The Knox Vault Subsystem can read or write to external memory using the External Memory Manager.

Knox Vault Storage

The Knox Vault Storage is a dedicated, secure, non-volatile memory device that stores sensitive data such as the following:

- Cryptographic keys such as Blockchain keys and Device keys
- Biometric data
- Hashed authentication credentials

Like the Knox Vault Processor, the Knox Vault Storage is designed to prevent various physical and side-channel attacks, using its own secure processor, SRAM, ROM, cryptographic module, and hardware monitor which detects physical tampering.

Secure Core

The Secure Core is the Knox Vault Storage processor used to do the following:

- Execute the ROM code

- Provide cryptographic operations for public key algorithms (RSA, ECC) and SHA algorithms with software libraries
- Safely store data in dedicated SRAM and ROM

Crypto Engine

The Crypto Engine supports symmetric encryption to verify authentication codes after receiving packets from the Knox Vault Processor and also to enhance performance.

Hardware Monitor

As with the Hardware Monitor of the Knox Vault Subsystem, the Hardware Monitor of Knox Vault Storage also detects physical or side-channel attacks related to power, temperature, and electromagnetics. If the Hardware Monitor detects an attack, the Knox Vault Storage is automatically wiped.

Non-volatile memory

The non-volatile memory is a bank of NOR flash used to store data received from the Knox Vault Processor.

Knox Vault intercommunication

The Knox Vault Subsystem and Knox Vault Storage communicate securely over a dedicated I2C (Inter-Integrated Circuit) bus. All traffic on this bus is encrypted and transmitted with an authentication code. Additionally, all communications are protected against replay attacks.

Protection from Attacks

Knox Vault is tested to provide protection against the following classes of hardware probing attacks.

Physical probing

An attacker might physically probe secure hardware to disclose user data or other critical information, while the data is stored in memory or being processed. The attacker directly measures information using electric contact with the secure hardware internals, using techniques commonly employed in Integrated Circuit (IC) failure analysis and IC reverse engineering.

Physical manipulation

An attacker might physically modify the secure hardware to change user data, secure hardware software, or security services or mechanisms. The attacker might make modifications through techniques commonly employed in IC failure analysis and IC reverse engineering. To make these modifications, the attacker identifies hardware security mechanisms, layout characteristics, or software design, including how secure hardware treats user data. Changes of circuitry or data can be permanent or temporary.

Forced information leakage

An attacker might exploit information that is leaked from the secure hardware in order to disclose confidential user data, even if the information leakage is not inherent but caused by the attacker. For example, fault injection or physical manipulation might cause information leakage from signals which normally do not contain significant information about secrets.

Side-channel attack

An attacker might exploit information that is leaked from the secure hardware during its operation to disclose confidential user data. Direct contact with the secure hardware internals is not required. Information leakage might occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time. One example is the Differential Power Analysis (DPA). This leakage can be interpreted as a covert channel transmission but is more closely related to the measurement of operating parameters. These operating parameters might be derived either from direct measurements or measurements of emanations. The attacker can associate the measurements with the specific operation being performed.

Fault injection

An attacker might cause a malfunction of the secure hardware software by applying environmental stress like light or a power glitch. This attack type could modify the hardware and software functions or deactivate or affect security mechanisms of the secure hardware. Thus, the attacker could disclose or manipulate the user data existing in the secure hardware. For example, the modification of the security hardware function might affect the quality of random numbers provided by the random number generator, and then the software may get constant values or values with low entropy.

Trusted Boot

Trusted Boot is a Knox Platform feature that identifies and distinguishes *authorized* from *unauthorized* boot loaders, segregating out-of-date boot loaders *before* they can compromise your mobile devices.

Enterprises can check device integrity on demand through Knox Device Health Attestation, which reads Trusted Boot collected measurement data, along with an Security Enhancement (SE) for Android enforcement setting, to form the basis of a device health verdict.

Secure lockdown on tampering

Bootloader measurements are recorded in secure TrustZone memory during device boot. At runtime, apps operating in the secure TrustZone can use these measurements to make security-critical decisions, such as whether or not to:

- Release cryptographic keys from the Knox Keystore.
- Launch the Work profile app container.

The key derivation mechanism for the device's work profile contains a tamper fuse. If an unauthorized or out-of-date component version is detected, the fuse is set. Once the tamper fuse is set, sensitive work apps and data within the Work container are permanently encrypted and inaccessible as the integrity of the device is no longer guaranteed or validated. In addition, the encryption key will not be derivable.

The device user can still boot the device and launch personal apps. This flexibility promotes a nice balance between consumer functions, such as smartphone calls and personal apps, and the requirement to protect enterprise data.

Building on Secure Boot

Before adopting Trusted Boot to work along with Secure Boot, Samsung devices used Secure Boot to prevent unauthorized bootloaders and operating systems from loading during start-up.

Secure Boot is implemented by each bootloader cryptographically verifying the signature of the next bootloader in sequence, using a certificate chain with its root-of-trust resident in hardware. If verification fails at any step, the boot process terminates.

While Secure Boot is effective at preventing unauthorized bootloaders, it is unable to distinguish between different authorized binary versions. For example, Secure Boot can't distinguish between a bootloader with a known vulnerability as opposed to a later patched version, since both versions have valid signatures.

Trusted Boot was introduced to verify all the software components in the boot chain (bootloader, kernel, and platform build) intended to be deployed together.

Knox Verified Boot (KVB)

Knox Verified Boot (KVB) implements the Trusted Boot process on Knox devices. KVB both extends and enhances Android Verified Boot (AVB); while AVB only checks the integrity of the kernel and platform components, KVB extends checks to also validate earlier bootloaders.

This provides a more comprehensive guarantee the device is booting using properly signed components from the same build.

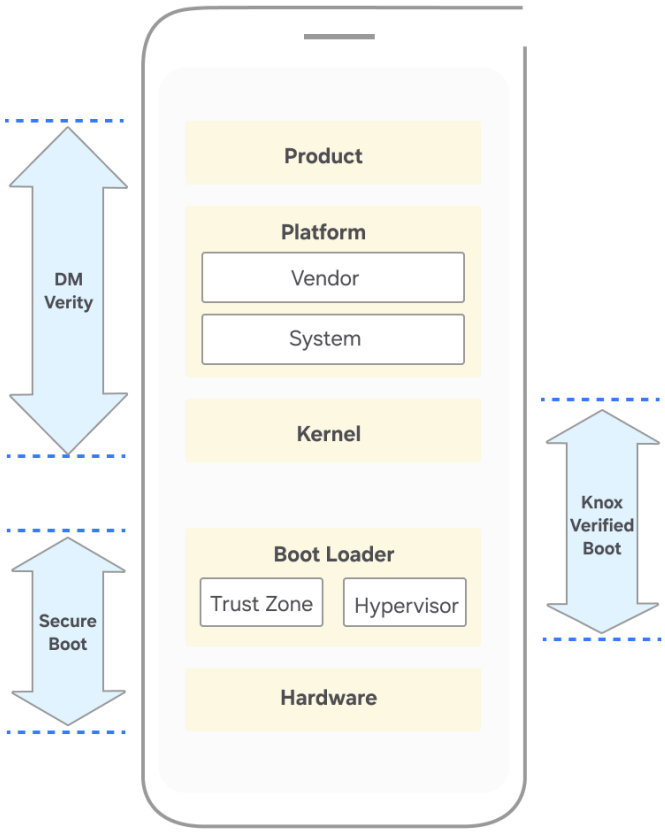

Figure 5: Knox verified boot process

Biometric authentication

Traditional user authentication relies on factors such as passwords or ID cards, which are susceptible to human errors, phishing, and duplication. Biometric authentication validates a personal trait, such as fingerprints, irises, or facial features, to enhance security. All biometric data collected by Samsung Knox complies with the highest security level as defined by Class 3 in Android.

Samsung Knox provides the following security features for biometric data protection:

- Ensures that raw biometric data or its derivatives, such as templates, are never accessible outside the secure isolated environment, such as the Trusted Execution Environment (TEE) or Secure Element.
- Encrypts all the stored biometric data using a device-specific key known only to the TEE.

- Restricts hardware access to the secure isolated environment and its communication channels—Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C)—based on device hardware support. Explicit Security-Enhanced Linux (SELinux) policies enforce this restriction on all device files.

Users must still enter a pattern, PIN or password as a backup to their biometrics.

- Face recognition requires re-authentication every 24 hours or after the device has been idle for 4 hours.
- Fingerprints require re-authentication every 72 hours.

For additional information, see biometric implementation in Android.

Enterprise controls for biometrics

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

The Knox Platform provides the following features in addition to standard Android capabilities:

- **Secure storage**: On Samsung devices, biometric authentication software doesn't share or distribute biometric measurements of any user. Measurements are stored in a format that prevents reproducing the original biometric, they can only be accessed and decoded within a specific TrustZone partition that has access to the biometric hardware. This prevents biometric spoofing.
- **Enforced Two-Factor Authentication (2FA)**: The Knox Platform enables IT admins to enforce biometric-based two-factor authentication for Work containers. For example, a user may be required to authenticate with iris recognition in addition to a standard device unlock method, such as password, PIN, or pattern. While Android supports some two-factor authentication combinations, the Knox Platform enables you to enhance security with biometric integration.
- **Enterprise credentials override**: In accordance with enterprise policy, Samsung Knox devices allow you to enforce the use of enterprise Active Directory (AD) credentials for unlocking a device or Work container. This setting overrides any biometric authentication methods configured by the user, ensuring that enterprise credentials remain the sole authentication mechanism.

Real-time Kernel Protection

Kernel protection is critical for device security and enterprise data protection. Software vulnerabilities get exploited by attackers to escalate privileges, leading to kernel-level compromises that jeopardize the integrity of the OS.

A compromised kernel can significantly impact enterprise data and security due to the following issues:

- Sensitive data leak.
- Remote monitoring and controlling of affected device.
- Hardware security protections such as Secure Boot and hardware-backed keystores become ineffective when the kernel is compromised at runtime.

Samsung Knox Platform's patented Real-time Kernel Protection (RKP) is an industry's leading security feature designed to protect against kernel threats and exploits. It is an out-of-the-box solution enabled by default on all Knox devices, requiring no additional setup. It operates seamlessly, and enhances device performance without impacting customer experience.

When a Samsung Knox device powers on, RKP provides real-time threat detection and attack mitigation to safeguard the kernel. It also supports the rest of the Knox security features, ensuring full security coverage at runtime.

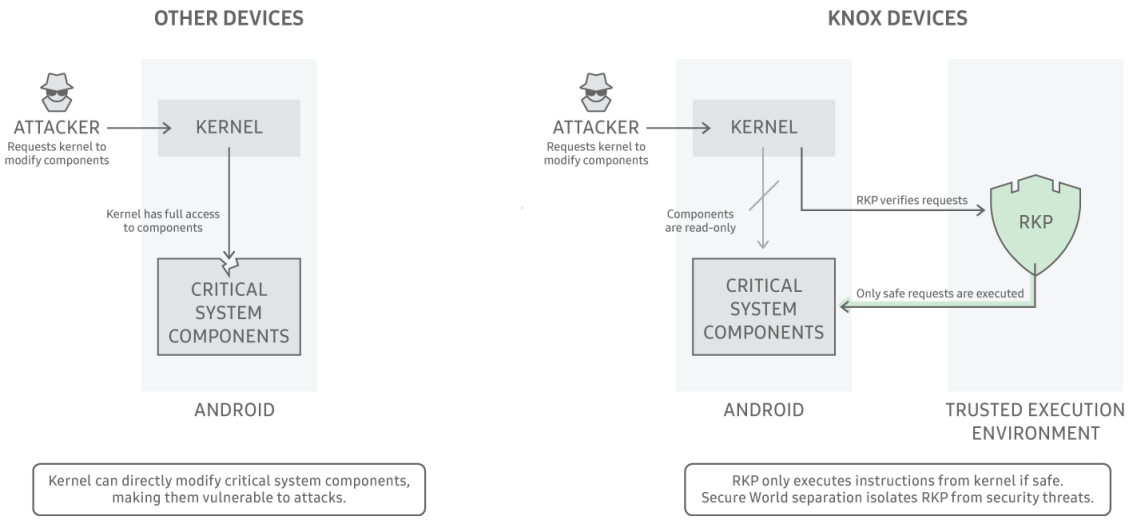

Figure 6: RKP explained

How RKP works

RKP uses a security monitor running in an isolated execution environment. This ensures the kernel protection mechanism doesn't exist in the kernel itself, reducing the risk of circumvention by attackers exploiting kernel vulnerabilities.

The kernel operates at the lowest granular level of the OS, hence conventional security solutions can't effectively monitor it. RKP overcomes this limitation by using the following patented techniques:

- Control device memory management.
- Intercept and inspect critical kernel actions before execution.

Due to these, a compromised kernel can't bypass traditional security protections, and the exploit impact is significantly reduced.

Defeat Exploit

Due to the intricate nature of modern devices, it is impossible to anticipate every potential threat. Effective protection requires a delicate balance between robust security measures and seamless system functionality. To achieve this, security frameworks must proactively prevent malicious activity, while minimizing disruptions to legitimate actions and performance.

To strengthen the Samsung Knox platform, Defeat Exploit (DEFEX) safeguards the Android kernel against tampering and corruption, preventing unauthorized behavior whenever the kernel is activated.

How it works

System calls are service requests executed by an operating system, such as Android, on behalf of applications. Since invoking system calls requires elevating the processor to kernel mode, they run with higher privileges and are prime targets for exploits.

Samsung DEFEX mitigates this risk by intercepting and filtering system call requests:

- Authorized invocations proceed normally.

- Unauthorized ones generate a report and typically result in termination of the offending process.

Core components

Samsung DEFEX includes the following core components:

- **SafePlace (executing processes)**: Ensures that only authorized programs are launched by root processes. SafePlace secures the root account, ensuring that only authorized programs are launched by root processes. This is particularly important because programs loaded and executed by root processes through the “execve” system call inherit their privileges, making them a prime target for exploits.
- **Privilege Escalation Detection (PED)**: Monitors attempts to change credentials and terminates non-root processes attempting to elevate privileges. PED monitors privileges for Android processes, which are primarily defined by their real or effective user, group, or file system identifiers. These credentials dictate which resources system calls can access on behalf of a process. PED tracks these identifiers throughout the process lifecycle and terminates non-root processes attempting to escalate privileges.

In addition to these core components, Samsung DEFEX includes auxiliary tools for maintaining and generating policies, exception lists, and runtime facilities supporting PED and other features. Samsung DEFEX policies, described by “allow lists”, implement Mandatory Access Control (MAC) strategy and explicitly permit or deny access depending on the component.

The core engine is built into the device binary and performs runtime loading and verification of Samsung DEFEX policies.

Knox Device Health Attestation

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Maintaining device trust requires methods to reliably check and attest the current security state of the device. Enterprise devices can be compromised by malicious actors, which can put mobile apps and enterprise data sent to the endpoint at risk. To ensure unauthorized actors don’t receive controls or data that could impact your enterprise, it’s important to take a zero-trust approach to monitoring the health of the endpoint. Unauthorized actors might include:

- A malicious user deliberately accessing a device they're not authorized to, for example, while the user is away.
- A bad actor who manipulates the software or hardware of the device, or its firmware in transit.

As captured in the threat model for Samsung Knox, advanced actors can—through a robust attack chain—gain full control over the device firmware, files, user interface (UI), and apps. Such malicious actors can exploit these scenarios to:

- Install malicious applications.
- Steal passwords and credentials.
- Extort user and enterprise data on the device.
- Laterally move to other assets in the enterprise.

Enterprises with **Bring Your Own Device** (**BYOD**) programs are especially at risk, as employees may potentially use compromised Android devices in the workplace. Unlike managed corporate devices, personally owned devices may be compromised prior to enrollment. Once enterprise applications are enrolled, admins are unable to limit applications and device policies on these devices.

To help address these concerns, Knox Device Health Attestation provides a fail-safe way to detect if a device or its firmware is compromised before allowing the device to be used the workplace.

Knox Device Health Attestation provides the following security benefits for enterprises:

- **Prevention of replay attacks**: Health measurements guaranteed per request through a nonce, a unique number randomly generated by the Knox Device Health Attestation Server.
- **Prevention of device ID falsification**: Knox Device Health Attestation forms a chain of trust using the Samsung Root Key, Knox Device Health Attestation Key, and Attestation Key. It signs attestation results using the Attestation Key and appends the Attestation Key certificate and Knox Device Health Attestation Key certificate.
- **Detection of systemless rooting**: Rooting methods like Magisk store system file modifications in the boot partition, which can go undetected by tamper detection methods other than Knox Device Health Attestation.
- **Correlation of results per device**: Health results that easily map to device identifiers like IMEIs. Unlike other solutions on the market, with Knox Device Health Attestation, IT admins can correlate attestation results with a device without having to painstakingly map

IDs manually. When results are returned for separate devices, IT admins can't differentiate between devices. Consequently, the results are not actionable. In contrast, Knox Device Health Attestation returns a single device ID, enabling IT admins to prevent or contain issues promptly.

- **Historical tamper record**: Knox Device Health Attestation guarantees not only the current health of the device, but also a record of whether the device ever ran a non-approved configuration in the past, through the Knox Warranty Bit.

Reliable detection of compromised devices

Malware can potentially intercept and forge the results of a device health check, making a compromised device seem secure. To guard against these types of scenarios, Knox Device Health Attestation provides the following:

1. The Knox platform leverages its hardware-backed trusted environment to reliably detect and report compromised devices. Knox Device Health Attestation verifies the integrity of devices during deployment, bootup, and operation using the following:
    - **Root of Trust**: Starts in our factories, when devices are manufactured, with device-unique hardware keys providing a foundation of trust.
    - **Trusted Boot**: Detects unauthorized and out-of-date boot loaders before they compromise devices using bootloader measurements recorded in secure TrustZone memory.
    - **Knox Vault**: Stores sensitive data such as the Knox Device Health Attestation Key in tamper-proof storage that resists both hardware and software attacks.
2. Through our secure hardware supply chain, Samsung provisions a device-unique Elliptic Curve Digital Signature Algorithm (ECDSA) asymmetric key pair—the **Knox Device Health Attestation Key**—in the device hardware during the initial manufacturing of the device.
3. The public key is signed by a Knox Device Health Attestation Root Key to generate an X.509 certificate, and this certificate is also provisioned on the device.
4. The private key is directly available to only either the Knox Vault (on supported devices) or the TrustZone Secure world.
5. On request, trusted Knox Device Health Attestation software signs the current device health data and a challenge nonce (to prevent replay attacks) with the SAK to prove that the health data originated from the TrustZone Secure world or Knox Vault on a Samsung Knox device.

6. The signed health data is sent to the Knox Device Health Attestation server. To protect data-in-transit, Knox Device Health Attestation uses Transport Layer Security (TLS) encryption. To validate device health data, the Knox Device Health Attestation server verifies the Knox Device Health Attestation Key certificate, Attestation Key certificate, challenge nonce, and signatures to ensure the integrity of the attestation result.
7. Highly secure or firewalled operations that don't want to access the web-based Knox Device Health Attestation server can install an Attestation Validator tool onto a local server to parse the Attestation Result and keep device verdicts within the firewall.

Security-sensitive Samsung systems like Knox services, Samsung Pay, and Samsung Pass, have trusted components that use the result of health attestation locally to disable themselves if device health is compromised.

On devices enrolled in Microsoft Intune Mobile Application Management (MAM), applications can leverage the on-device components of Knox Device Health Attestation to validate that the device is in a good state. Knox Device Health Attestation provides the conditional launch and access features of Intune MAM with the Knox Device Health Attestation payload to ensure device health is good. We highly recommend any enterprise leveraging Intune MAM for Managed/BYOD scenarios to turn this feature on to apply Zero Trust principles to your mobile deployment. For more information on this joint integration, see the Microsoft Intune Blog.

> **Note**
> Knox devices that aren't enrolled in Intune or any other UEM/EMM can still use MAM to validate devices are in a good state before launching specific apps. To learn more about using MAM with unenrolled devices, see the Intune MAM documentation.

How Knox Device Health Attestation works

Samsung Knox partners such as Enterprise Mobility Management (EMM) vendors or Independent Software Vendors (ISV) can use our Knox APIs to deploy attestation checks. Admins can enable device checks manually using a web console or automatically through a regularly scheduled process. With Knox Asset Intelligence's Security center, Knox Device Health Attestation is automatically turned on and ran daily for all enrolled devices.

1. The web server that initiated the check requests a nonce from the Knox Device Health Attestation server and instructs the device to begin a check, passing the nonce as a check identifier.
2. The Device's Keymaster Trusted Application (TA) in the Secure world gathers:
    - The requesting app's package name, version code, and developer key.

- Signed info about the device's current state and expected environment.
- Hardware fuse readings indicating if untrusted firmware was ever loaded onto the device.

3. The TA compiles this information into an Attestation Result and signs it with a key that can be verified using the Samsung Root Certificate.
4. The device communicates with the Knox Device Health Attestation Server using TLS encryption to protect data-in-transit.
5. The Knox Device Health Attestation Server validates the Attestation Result's signature to ensure that it was generated on Samsung hardware and by Samsung's TA.
6. The Knox Device Health Attestation Server analyzes the Attestation Result to determine if the returned nonce matches the one sent out and whether the data within it can be trusted.

Managing compromised devices

On detecting a compromised device, the Knox platform fuses a one-time programmable warranty bit that signifies whether or not the device has ever booted into an unapproved state. Once this bit is fused, the work profile and Keymaster no longer operates, preventing access to the secured enterprise apps and data.

The original requestor of the device check can take further action based on how Knox Device Health Attestation is integrated into your enterprise. We recommend the following actions:

- Report the verdict to the device user.
- Immediately prevent the device from accessing other enterprise systems.
- Uninstall any enterprise apps or assets already on the device.

If the device is enrolled into Knox Asset Intelligence and has security events and log enabled, we highly recommend reviewing the telemetry and triaging the incident. After a device is compromised and the Warranty Bit is blown, the work profile becomes unavailable and Knox Asset Intelligence is unenrolled as a result. For this reason, you will be unable to get any additional telemetry (for example, dump the log remotely) once the device is compromised without physical access to the device.

Samsung Auto Blocker

Samsung Auto Blocker is designed to prevent and block smartphone security threats by activating various security settings at once, making it easy for anyone to quickly improve device security. Auto Blocker is only available on Galaxy devices running One UI 6.0 (Android 14) and higher, and is enabled by default. You can choose to disable it in the initial setup menu or on your device's **Security & Privacy** settings page.

Auto Blocker enables the following basic functions:

- **Blocks apps from unauthorized sources**: Only apps from official stores such as the Google Play Store and Galaxy Store can be installed. If you try to install an app from an unauthorized source, a warning message will be displayed, and the app will not be installed. This feature effectively prevents the installation of malicious apps, which are the main attack route for voice phishing.
- **Blocks commands by USB cable**: Blocks commands from being passed through USB cables when devices such as chargers and PCs are connected. This prevents users from unknowingly receiving commands delivered by hacking tools disguised as chargers in public places.
- **Blocks malware images in message apps**: Enables Samsung Message Guard, which blocks malicious payloads disguising as images when you receive a message.
- **Blocks software updates by USB cable**: Prevents installation of unauthorized system software using a physical USB cable (e.g., unauthorized Android OS). This can stop malicious actors with physical access to your device from installing software without your knowledge.

Figure 7: Autoblocker notification

Maximum restrictions

For users looking to have additional security protections, Auto Blocker has the option to enable **Maximum restrictions**. Enabling this setting may impact app usability and various device capabilities. Maximum restriction is disabled by default and can be enabled in Auto Blocker's settings menu. When enabled, the following security features are activated:

- **Turns on App protection**: Checks for any suspicious apps during installation and post-installation. The specific antivirus solution on each device can vary by region.
- **Blocks device admin apps**: Disables device administrator apps and work profiles on your device. This protects against attacks that use these features to access or remotely control your phone.
- **Blocks auto downloading attachments**: Blocks the automatic download of files attached to messages. You can still manually download attachments from messages sent by trusted individuals.
- **Blocks hyperlinks and previews**: Prevents you from seeing previews for messages containing web addresses or accessing websites by selecting hyperlinks. If a trusted person sends you a message with a web address, you'll need to copy and paste or type the web address in your browser.
- **Removes location data when sharing pictures**: Removes location information when sharing photos from the **Gallery** or **Messages** app. The recipient will not be able to know where the photo was taken.
- **Blocks shared albums**: Blocks the shared album menu and others cannot invite you to a shared album. This protects you from accidentally sharing pictures that might contain sensitive information or accepting invitations from unknown or deceptive senders.

Data Protection

Data encryption

Your data on a Samsung Knox device is encrypted by default through numerous different layers, supported all the way down to the hardware layer. On Samsung devices, we support Android File Based Encryption's (FBE) Direct Boot, which maintains encryption of data in two separate locations:

- **Credential encrypted storage (CE)**: The default location where data is stored and is encrypted with a key based on the user's PIN, password, or pattern. The device encryption key is required to access the Keystore.
- **Device encrypted storage (DE)**: A location where data is encrypted only with a device key generated when the device boots (prior to user login). Applications must register themselves in order to store specific data in this location. This mainly serves apps or services that need to run prior to login, such as urgent notifications and accessibility services.

With Android File Based Encryption, each individual file on a Samsung device uses a unique key that is generated based on a hierarchy of key derivations rooted in the user PIN, passcode, or pattern, and the hardware's device encryption key. Samsung leverages our secure environment, Arm TrustZone and Knox Vault to derive these keys and ensure no one can access your data without breaking both the user secret and device secret. For credential encrypted storage, rate-limiting is applied to the key derivation process to prevent against brute-force attacks trying to guess the user's login credentials. For more information, see Android's documentation on Gatekeeper.

Samsung Knox devices also leverage metadata encryption for each file. This allows for the filesystem metadata and file content (name and body) to be encrypted with separate keys. This is particularly useful for maintaining confidentiality at rest for scenarios where the operating system needs to reason about details such as a file's size or permissions without completely decrypting the file using the per file key.

Both traditional storage (physical storage on the device) and adoptable storage is supported as part of FBE on Samsung Knox devices. Enterprises leveraging Knox Dual Data-At-Rest Encryption (DualDAR) can add additional encryption layers to this process.

For more information on File Based Encryption and how data is kept secure within Android, see Encryption in Android's documentation.

Android Enterprise Profiles

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Mobile apps have changed the way we work by providing new channels of communication, innovating customer engagement, and empowering organizations with critical data in real-time. Enterprise IT admins and their users want to leverage one device for both personal and work use cases; a common device provides enhanced convenience while maintaining strong security.

This requirement presents a challenge for enterprises, which need to ensure that they fully protect their confidential corporate assets while also preventing liability issues by accidentally interfering with a user's personal privacy. Specifically, business-critical apps such as Samsung Email, Internet browser, Calendar, and Contacts are often the focus of the enterprise IT admins. Admins can secure these apps within the Work Profile, along with other apps used by the enterprise.

The Knox Platform secures enterprise apps and protects confidential app data by leveraging the following methods:

- **App installations and updates**: Apps are pre-installed within the mobile device's secure Work Profile and users can update these apps independent of firmware updates through Google Play.
- **App isolation**: Apps are sandboxed within the Work Profile, which uses Security Enhancements (SE) for Android to prevent personal apps from interfering with business apps in the Work Profile.
- **App permissions**: Knox provides app permission monitoring to help users prevent malware from using powerful permissions to gain unauthorized access to the device and Work Profile.
- **Data at Rest**: Through Knox's data protection, the files and data used by an app can remain encrypted until device users authenticate when unlocking the device or logging in to the Work Profile. Individual apps can further deploy an app-specific password as another line of defense.
- **Data in Transit**: App data sent through the public Internet can be secured using Knox's advanced VPN features.
- **DeX integration**: Not only are all Samsung native apps optimized to work within DeX, enterprises can secure apps while they're displayed in DeX.

Work Profile security

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

The Android Enterprise Work Profile provides enterprises with a solution to securely isolate work apps and data on a device. The Knox Platform for Enterprise provides more granular management policies for Work Profiles on Samsung devices.

Data transfer

With the isolation of work and personal data, a device user has access to two separate spaces. To increase productivity, it is often necessary to share data between these spaces. For example, it may be necessary to call a work contact saved in the secure workspace while using a phone app in the personal space. With the Work Profile, IT admins have granular management policies to control the movement of data to and from the Work Profile. This data can include apps, files, clipboard data, call logs, contacts, calendar events, bookmarks, notifications, shortcuts, and messaging services (SMS).

Password policy

Setting strict password requirements is essential towards ensuring enterprise data is only accessed by authorized individuals and isn't subject to trivial attacks. To achieve enterprise needs, the Work Profile supports advanced authentication mechanisms that help further secure enterprise data.

An IT admin can enforce and configure:

- Complex passwords or code schemes by requiring a diverse set of alphanumeric characters, alongside other options.
- Two-factor authentication by requiring facial or fingerprint alongside a password.

Should an issue arise with the work container, an IT admin can lock the container to restrict access. This includes when a device has reached its password attempt limit, is out of compliance, lost, or stolen.

Dual Data-At-Rest Encryption (Dual DAR)

> Note
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

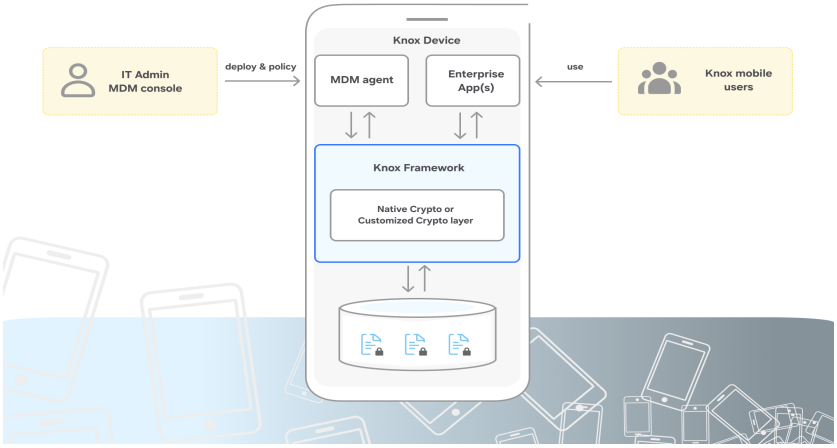

Figure 8: DualDAR explained

Protecting Data-At-Rest (DAR) on mobile devices is a major concern for security conscious enterprises. Android File Based Encryption (FBE) addresses this issue by only decrypting data after user authentication, providing per-file and per-data decryption keys, offering per-app password checks, and meeting Mobile Device Fundamentals Protection Profile (MDFPP) requirements for United States government and military use.

Knox DualDAR adds two separate layers of encryption, further meeting the requirements of classified deployments. Knox DualDAR secures all Work Profile data on devices with two distinct levels of encryption. The solution also protects data by restricting apps from writing or saving data to the unencrypted space on the device.

> **Note**
> Currently, DualDAR only secures data placed inside the designated Work Profile.

The DualDAR solution provides two separate layers of encryption and key generation; the outer layer and the inner layer. All data placed inside the Work Profile is dually encrypted by both layers:

- **Outer layer**: The outer layer of the DualDAR solution is built on top of Android's FBE and enhanced by Samsung to meet MDFPP requirements. This layer is implemented through the System on a Chip (SoC) dedicated to flash storage encryption. In this context, the SoC could be Qualcomm Integrated Crypto Engine (ICE) or Exynos Flash Memory Protector (FMP). Data encryption at this layer is AES 256 XTS and file encryption keys are encrypted using AES-GCM 256.
- **Inner layer**: The inner layer of encryption is based on a framework that allows an independent third party to install a separate cryptographic module. If no third-party

module is installed, a separate inner layer of encryption is secured by a FIPS 140-2 certified cryptographic module included with the Samsung Knox framework.

DualDAR is supported on the Galaxy S10, N10, S20, and subsequent flagship models, and is compatible with Android FBE.

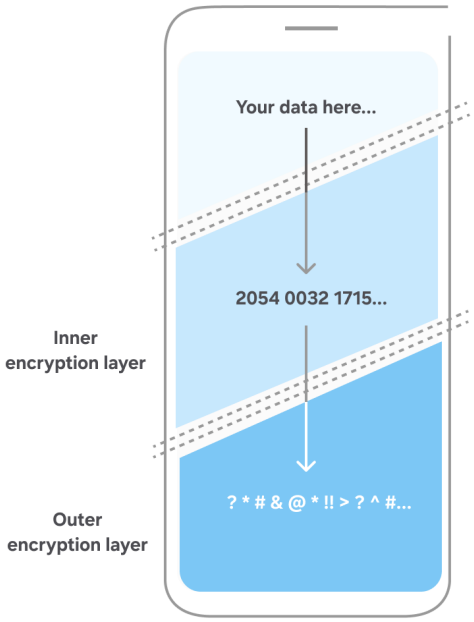

Figure 9: Inner and outer encryption layers

How it works

DualDAR's inner and outer security layers are independent and protect all information stored in the Work Profile when the device is in a powered off or unauthenticated state. Samsung Knox DualDAR leverages Android File Based Encryption (FBE) architecture.

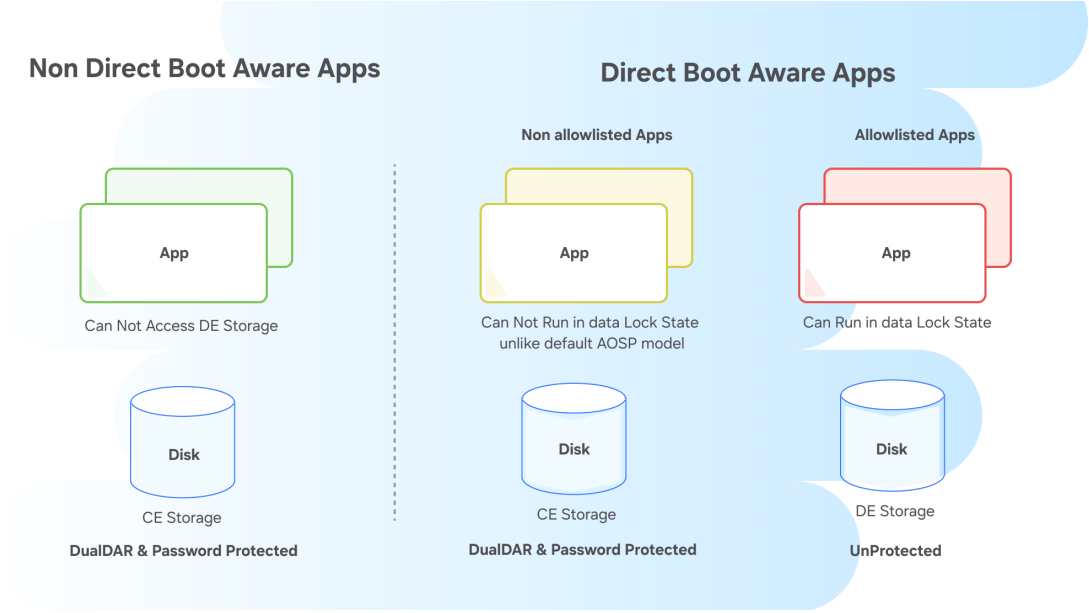

Figure 10: How DualDAR works

From an app point of view, the DualDAR Work Profile functions as CE storage. The Knox framework prevents apps from writing data to non-DualDAR protected DE storage. In some cases, an app is aware of both CE and DE storage and needs to write unclassified content to DE storage. In such cases, IT admins can allow that app to write to DE storage. This strict allowlist process ensures that no app can write sensitive or classified content to DE storage without explicit IT admin approval.

When the work container is configured for DualDAR, the secured data is available as follows.

1. On a device that supports and is configured for DualDAR, access to app data inside the container is only available when the container is unlocked, that is when the user is actively using the container.
2. When the container — or device as a whole — is locked, the container encryption keys are evicted from memory.
3. In a data lock state, the Samsung device remains powered on, but the user is locked out of both the work container and the device. All sensitive data is protected in credential encrypted storage within the Work Profile. CE storage is not available until the user provides both their device and Work Profile credentials.

Unique advantages of Knox DualDAR

DualDAR encryption has significant advantages over traditional single layer encryption methods:

- **Mitigate risks of implementation flaws**: DualDAR reduces the likelihood of unauthorized data access by mitigating the risks that arise from vulnerabilities in a single encryption layer. While one of the many methods available for unauthorized data access may crack through a single layer of encryption, the chances are very low that such vulnerabilities are available on both layers of encryption.
- **Mitigate risks of password configuration flaws**: Both layers of encryption on a DualDAR configured device use separate and distinct authentication methods to allow access. This separation of authentication methods reduces the likelihood that a single misplaced or misconfigured password is exploited on both layers of data encryption at the same time. Two layers of encryption and two methods of authentication ensure that encrypted data remains protected even in the event of breach on one layer.
- **Provide access using strict security evaluation criteria**: DualDAR meets the standards laid out in the FIPS 140 certification requirements. Both the inner and outer layers use FIPS 140 certified cryptographic modules. GCM is used to encrypt the key while data is encrypted using XTS or CBC.
- **Ease of deployment**: DualDAR leverages the in-built Android FBE framework and builds additional layers of security on top of this framework. This solution is available on devices that use a work container in profile owner (PO) mode and fully managed devices that include a PO mode. For more information on configuring this solution for your supported device, see DualDAR architecture.
- **Customize the second layer of encryption**: DualDAR allows IT admins to implement third party encryption solutions at the inner layer of encryption. This freedom of implementation means IT admins can use and configure any third-party cryptographic modules, including solutions that meet FIPS 140 certification criteria.
- **Flexible deployment methods**: IT admins can implement and configure DualDAR on all kinds of devices, including Bring Your Own Device (BYOD) and company-issued devices. DualDAR is compatible with both device using a work container in PO mode and fully managed devices that include a PO mode. This flexibility means IT admins can use this superior data security solution on a wide variety of devices within their enterprise.

For more information on DualDAR and its unique design, see DualDAR architecture.

Knox Framework

The Knox Framework contains numerous changes Samsung has made in the operating system and is the central location and interface point for device management, Knox services, and Knox unique APIs.

Device management

Since its inception, Samsung Knox has been at the forefront of developing Android mobile devices for enterprise use. Over time, we've refined our policies and features to enhance the management and capabilities of our devices through the collaboration of three major frameworks:

- **Android Management API (AMAPI)**: The default management framework supported on all Android Enterprise enrolled devices. This includes many device policies as well as numerous device level APIs. For more information on Android Enterprise, please refer to their documentation.
- **Knox Platform for Enterprise (KPE)**: A set of system services which allow for numerous APIs, device policies and controls to be set for device under management. KPE is supported all device deployment modes beyond just Android Enterprise. For more information see the the Knox Platform for Enterprise documentation.
- **Knox Service Plugin (KSP)**: A framework that works directly with MDM, EMM, and UEMs to provide day zero support of new Knox device policies and controls for interfacing with KPE. For more information see the following documentation.

Knox Mobile Enrollment

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Given the scale of mobile deployments within enterprises, a seamless device enrollment experience is crucial. Today, admins can use Android Zero Touch on Samsung devices for a standard enrollment experience. However, to streamline the enrollment process and activate and meet numerous security requirements, we recommend using Knox Mobile Enrollment (KME).

Knox Mobile Enrollment provides an out-of-box solution for IT admins to enroll devices in their EMM or UEM tool. With numerous controls, admins can ensure that devices are properly set up in diverse IT ecosystems such as on-premises or low-connectivity environments. Additionally, Knox Mobile Enrollment is the only method that allows you to onboard devices to the Knox Cloud Services, included in the Samsung Knox Suite.

For more information on how to setup and deploy Knox Mobile Enrollment, see the Knox Mobile Enrollment admin guide. Additionally, you can view a list of all Knox features on Android on the Samsung Knox official site.

Key security features

Knox Mobile Enrollment is the only enrollment method that allows for some of Knox's key security features to be enabled. Some unique security advantages of Knox Mobile Enrollment include:

- **Knox Device Health Attestation**: During device enrollment, Knox Device Health Attestation is used to verify the device being enrolled into the EMM or Mobile Device Management (MDM) is in an approved state.
- **Knox DualDAR**: Knox DualDAR adds two separate layers of data encryption to devices. To enable Knox DualDAR, devices must have the proper device policy set during enrollment, which can only be enabled using Knox Mobile Enrollment.
- **Setting root or intermediate certificate**: During device enrollment, Knox Mobile Enrollment allows IT admins to setup a custom certificate with the root certificate storage, which can be a key requirement for high security networks requiring specific certificates to connect.
- **Automatic credentials**: IT admins can set prepopulated credentials for a user when they first sign in to their device.
- **Advanced device lock**: Admins can leverage device locking features, such as timeout periods for enrollment timeframes, in the event the device is offline. In addition, admins can lock the device if it is stolen.

Hardware Device Manager

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

The Challenge

Peripheral hardware devices, such as cameras, microphones, modems, USB, GPS, and Bluetooth and Wi-Fi devices are an increasingly significant privacy and security attack surface on mobile devices. While such peripherals allow rich user interaction with the environment and offer unique experiences on mobile phones, these same peripherals also expose a wide attack surface that attackers can abuse for malicious purposes to compromise privacy and security.

For example, a malicious insider could use the camera, mic, and GPS in the background to spy on meetings or to photograph sensitive data in controlled physical environments, and exfiltrate data through the cellular modem. Such concerns have unfortunately resulted in mobile phones being disallowed in classified and secure locations, especially in government settings, as well as security concerns around their use by journalists and leaders who are potential targets of surveillance.

While Android has permission controls for apps to access peripherals, and even allows disabling access to certain peripherals altogether, these controls can be bypassed by stealthy spyware that compromises the Android framework or the Linux kernel.

For example, the Pegasus spyware used a rooting exploit to escalate privileges to the Android operating system (OS) and bypassed Android's access controls to surveil live audio and covertly capture camera images. As another example, researchers demonstrated how an Android permissions bypass vulnerability allowed an app access to camera, microphone, and GPS data without having permission to do so.

The Solution

Hardware Device Manager (HDM) is a Samsung-exclusive security layer that provides high assurance peripheral device controls to an enterprise even if the OS is compromised and across factory resets. HDM leverages Arm hardware virtualization to interpose on peripheral access and allows or denies access according to enterprise policy.

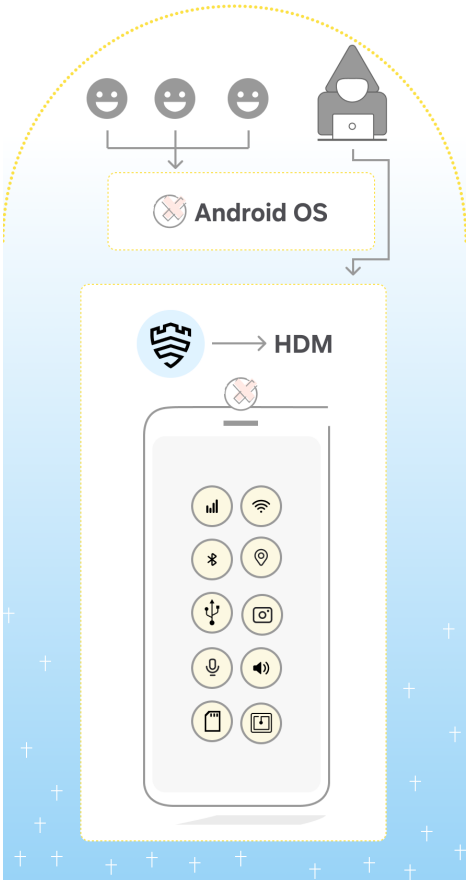

Figure 11: HDM explained

HDM mediates all accesses to peripherals even if an attacker bypasses Android OS access controls. Access is enforced based on an enterprise policy stored in tamper-resistant secure storage that persists even across factory resets.

This policy specifies whether specific peripherals should be enabled or disabled, and whether to trigger automatic physical lockout of peripherals upon detection of device rooting or compromise. This includes access control to physical sensors (cameras and microphones), communication chips (cellular modem, Wi-Fi, Bluetooth and NFC), and other peripherals (USB, speaker and GPS).

HDM achieves strong guarantees using a unique combination of techniques:

- **Controls are enabled before any potentially untrusted code can run**: HDM starts before the OS as part of Knox's hardware-rooted trusted boot process, which is the chain of trust that begins when the phone is powered on and ensures that each component is cryptographically validated before being loaded.

- **Complete protection even in the face of OS compromise**: HDM runs at a higher privilege than the OS by leveraging Arm's hardware virtualization extensions, and therefore mediates and controls all access to peripherals even if the Android framework and OS is completely compromised by malware.
- **Tamper-resistant and persistent policy across factory resets**: HDM stores its enterprise policy in a device secure storage that is protected from tampering and is preserved across factory resets and flashing. Even if the secure storage itself is broken by hardware attacks, HDM can apply a default protection policy.
- **Policy updates are cryptographically protected**: HDM uses cryptographic signatures and mutual authentication for policy updates. A trusted HDM server generates and signs the enterprise policy, which is verified by HDM on-device. In turn, HDM uses its own unique, hardware-backed key to prove its identity to the server and to cryptographically prove the hardware policy was successfully loaded.

Use cases

HDM enables several use-cases in a flexible and secure manner.

Fixed hardware peripheral customization

To avoid being detected or having their position compromised during military operations, operatives often require guaranteed disablement of certain radio services such as GPS, microphone, and Wi-Fi services. Using HDM to disable these subsystems on the device before troop or device deployment provides high assurance that these services cannot be activated in the field.

Dynamic context-based peripheral access

To maintain integrity and protect sensitive information or intellectual property theft, organizations restrict the usage of mobile devices in secure campuses or locations. HDM can be used to disable camera and microphone subsystems on the mobile device before entering these areas. Disabling of the hardware could happen automatically using external triggers or by tapping the device at an entry gate.

As another example, when a need arises to discuss confidential matters, mobile device users need to be able to quickly and securely restrict access to microphones and camera hardware. An on-device based HDM service can be used to enable or disable the hardware subsystems

ensuring the utmost secrecy is maintained. This can be thought of as a flexible privacy sticker and supports multiple peripherals where a sticker cannot be used.

Zero Trust and damage containment

A core principle of Zero Trust is “assume breach”, where enterprises have to anticipate that attackers can successfully compromise a system, and take measures to contain the breach. To meet these ambitious goals for realizing Zero Trust, enterprises require new endpoint capabilities for limiting damage and data loss in the event that a device compromise is detected. HDM enables robust disabling of peripherals such as Wi-Fi and cellular modem to prevent enterprise data exfiltration once a compromise is detected.

Knox Zero Trust Framework

> Note
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

The Knox Zero Trust Framework enhances security in enterprise environments by leveraging Android 14 to provide advanced security capabilities described here.

Knox Security Log

The Knox Security Log is an industry-first OEM security telemetry solution; it enables security workflows to facilitate real-time security alerts, and perform threat hunting activities. It’s our core continuous monitoring mechanism, consolidating all security telemetry data of Samsung devices in a centralized system.

The Knox Security Log operates as an on-device database, accessible only through the Knox Framework. This database resides in an isolated Linux domain outside the main operating system, ensuring that unauthorized sources resting at the application layer (due to Security-Enhanced Android) can’t access it. During operation, the Knox Framework collects various security signals and telemetry data from the system and stores them in the security log.

A privacy filter is applied upon data insertion to determine the origin of the data (such as personal profiles) and whether it contains identifiable information. This mechanism ensures that any sensitive data is redacted and excluded from being stored. As a result, the security log retains non-sensitive telemetry signals while preserving a trace of user actions for security auditing.

> **Note**
> This feature is available only for managed company-owned devices enrolled in the Knox Asset Intelligence and is supported on devices running Android 10 or higher.

The primary goal of the security log is to integrate mobile security telemetry into modern security operations workflows, and it has the following features:

Prioritized event alerts

When a new event is logged, it is evaluated against a severity threshold. If it meets the pre-configured push threshold, it is automatically forwarded to the Security Operations Center (SOC). Severity levels classify threats based on their potential impact:

- **HIGH** severity indicates a strong attack signal, events are pushed to the SOC in real time.
- **MEDIUM** severity indicates a potential attack signal, but events may not be pushed to the SOC immediately.
- **LOW** severity indicates a weaker threat, events are aggregated and pushed hourly in batches. The events that are not yet pushed can still be accessed through a SQL query or SQL query enrichment to the log.

For example, a phishing alert generated through Knox Suspicious URL Detection is classified as medium severity, as it could directly indicate an attack. Comparatively, a camera permission signal is classified as low severity, as it is generally benign but could indicate malicious activity when analyzed in context with other events.

> **Note**
> The severity classification is defined by Knox, and it is not based on any existing standard framework (such as MITRE ATT&CK).

To learn more about SOC integration options, please consult with your Samsung account representative.

Security event enrichment

Security event enrichment enables query-based requests, and SOCs can leverage the security logs to provide insights beyond basic event detection. By using cloud connector in Knox Asset Intelligence, IT admins can submit SQL queries, and retrieve security log data, without requiring any additional third-party setup.

For example,

1. A phishing event is detected and pushed to the SOC, indicating that an end user accessed a phishing website.
2. The SOC can then enrich this signal by sending an enrichment query to the device via the impacted app for Security information and event management (SIEM). This enrichment could request:
    - Recent events that occurred within a specific timeframe after the phishing event.
    - Process-level information to debug whether malware is injected into the device.

> **Note**
> Since enterprise environments use different security playbooks or SIEM providers, the individual query and workflow may vary.

Smart eviction

Due to the intermittent connectivity and limited resources available on mobile devices, the Knox Security Log employs a unique mechanism to manage on-device storage of security signals.

Each logged security signal is assigned a severity level, which indicates the potential impact of a security event. Additionally, whenever a signal is sent to the Knox Asset Intelligence server, the server's acknowledgement of its receipt is recorded in the Knox Security Log. If a signal remains unacknowledged, it continues to be periodically resent until acknowledgement is received.

To prevent log overflow, the system implements an eviction logic when the log reaches maximum capacity (log pressure). When this occurs, two actions are triggered:

1. A signal is generated to indicate that the log is nearing its maximum storage limit.
2. The system begins evicting entries based on the following conditions:
    - Signals that have been successfully sent to SOC and acknowledged by the server are removed first when additional log space is required.
    - If additional space is required, the system removes the oldest and least-severe entries.
    - If the log is left with only high-severity events, then no additional events are accepted into the log, with the goal of preserving the original adversary's actions.

By utilizing this eviction logic, it's ensured that the most severe security events are retained while handling log flooding concerns.

Privacy filter

Given the nature & use cases of mobile devices, privacy is a core design principle of the Knox Security Log. Strict guidelines are enforced for storing security-related events in the database. The security log uses an ingress privacy filter, that redacts all the information stored in tag tables (described in Zero Trust signals and events section below). This limits the storage of user identifiable data, while balancing visibility into security incidents.

A great example for this is SMS-based phishing. On Android devices, there is only one native messaging app per device, regardless of the deployment mode - work or personal profile. Specifically, on a device with both work and personal profiles, there is a single messaging app which is located on the personal profile of the device. When SMS-based phishing attempt occurs within this messaging app, it's impossible for IT admins to monitor it, due to privacy constraints.

With Knox Security Log, these phishing events can be logged locally on the device without exposing personal messages. The event stored in the log would captures the time of the event, but any information on the accessed URL and the origin application that triggered the phishing attempt is redacted.

Due to OEM-level visibility and control, these privacy filters are enforced on all the signals collected from managed devices. This ensures that enterprise receive relevant security insights without compromising user privacy.

Zero Trust signals and events

To enhance security visibility and strengthen the security posture of Samsung Knox devices, we have developed over 100+ signals that can be stored in the Knox Security Log for SOC ecosystems. These signals provide deeper insights into potential security threats and their detection. The Knox Security log offers access to these signals, which are not exposed via any API.

These signals range from outputs of processed detection engines to granular security information, such as process creation or termination events. By leveraging a diverse set of signals, enterprises can maintain a balance between detecting clear indicators of compromise and collecting fine-grained security telemetry for threat-hunting.

Signal content

Each signal consists of both common and specific data attributes:

- Common data is stored in a main database table and serves as the foundation for all signal information. It includes data such as timestamp, signal name, privacy indicators, MITRE ATT&CK techniques, and severity levels.
- Specific signal data, also known as tag table data, is stored in a separate database table and contains detailed information specific to each signal.

Knox Suspicious URL Detection

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Phishing continues to be a persistent threat since the rise of the internet, and has been more prevalent on mobile devices. Cybercriminals often employ deceptive techniques to trick users into clicking malicious links, thereby compromising their devices, and exposing sensitive data. The evolving nature of phishing makes detection challenging, particularly given the diverse range of mobile apps, browsers, and processes.

To mitigate this threat, Knox Suspicious URL Detection provides on-device detection of malicious or potentially harmful links, by generating security signals based on user or system scenarios. These phishing events can be configured to send alerts to the SOC, enabling IT admins to gain instant visibility into phishing attempts. This lets enterprises to investigate attacks based on URL, source app, and associated metadata, enabling appropriate response actions. The Security Operations Center (SOC) can also proactively detect concerted or unauthorized attacks on corporate devices.

The following are the capabilities of Knox Suspicious URL Detection:

- Supports detection of multiple phishing techniques, including SMS-based phishing (smishing) and QR code phishing (quishing).
- Leverages Android platform-level capabilities to capture links based on user interactions.
- Utilizes on-device machine learning (ML) models to infer whether a link is potentially malicious.
- Unlike traditional mobile phishing solutions, Knox Suspicious URL Detection operates entirely on-device, and eliminates reliance on cloud-based intelligence services for inference.

Knox Suspicious URL Detection identifies and mitigates the most common types of malicious URLs encountered by users, including:

- **Normal malicious URLs**: Websites with legitimate domain names but hosting harmful content.
- **Typo squatting URLs**: Designed to mimic popular websites by using typos or misspellings to deceive users.
- **Short or tiny URLs**: Shortened links that redirect to potentially malicious webpages.
- **Hypertext URLs**: Similar to short URLs, but instead of displaying the actual URL, they embed masquerading text that links to a malicious website.

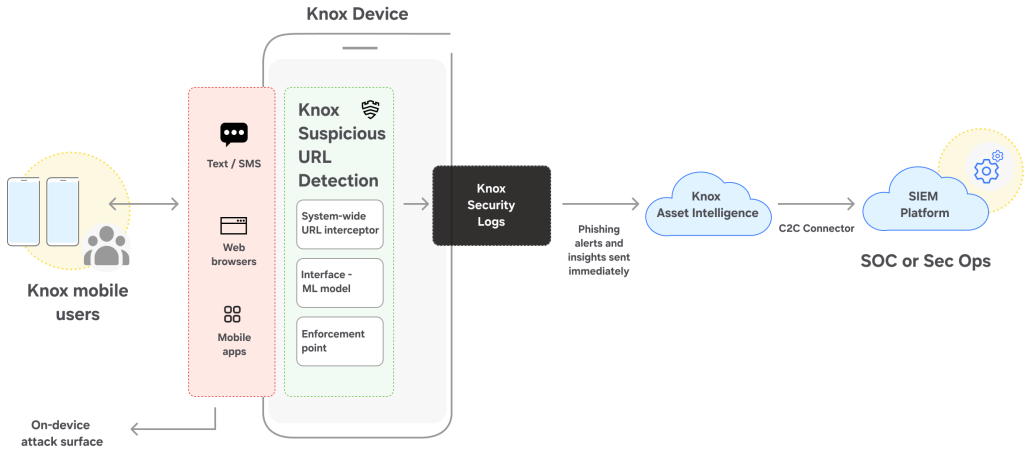

Figure 12: Knox Zero Trust Framework explained

Features

Knox Suspicious URL Detection can be enabled and configured for devices using Knox Asset Intelligence as a part of Knox Security Logs. It does not require any agent or app to be installed on the device, eliminating user friction. It offers various enterprise-grade enhancements, including:

- **System-wide coverage**: Knox Suspicious URL Detection solution operates at the framework level. It can monitor phishing events across both work and personal profiles, and doesn't require any separate configuration or setup.
- **Privacy preserving**: For malicious links accessed in a personal profile, only a phishing alert is generated and sensitive metadata, such as URL and app or package name, are filtered out before being stored in the Knox Security Logs.
- **On-device ML models**: URL analysis is critical to determine whether a link is potentially malicious or harmful. Knox ML models operate on-device to analyze URL strings and pre-

computed features before classifying links as potentially malicious. These ML models are regularly updated to keep pace with rapidly evolving threat landscape.

- **Predefined lists**: Before URLs are analyzed by ML models, they are checked against predefined allowlists and blocklists. These lists contain:
  - Trusted links (frequently visited webpages or enterprise-approved sites).
  - Malicious links identified from threat intelligence feeds and repositories.
- **On-device sandbox**: When dealing with shortened URLs, the on-device sandbox provides an isolated environment to retrieve the full URL. This is critical to determine whether the shortened URLs are being used for phishing.

Knox Suspicious URL Detection provides security insights at the source of an attack, enabling enterprises to detect threats early in the attack chain. IT admins can customize and fine-tune the detection using metadata signals, such as confidence score. This helps meet SOC requirements, such as signal-to-noise ratio.

Service Security

Security and privacy dashboard

On all Samsung devices, users can access a consolidated view of various device security settings and overall device health. This dashboard provides transparency into the security settings available for end users and the interactions that could impact their privacy. Additionally, the dashboard recommends security and privacy settings that users can consider enabling or disabling for their device.

The dashboard provides insight into the following primary security settings:

- **Lock screen**: The passcode needed to unlock the device and change sensitive settings.
- **Account security**: For managing Samsung and Google Accounts registered to the device.
- **Lost device protection**: Configuring settings for finding your device in the event it is lost or stolen.
- **App security**: Features which regularly check applications for malware or other suspicious activities. This can manage both Samsung App protection and **Google Play Protect**.

- **Updates**: information into whether the current software available for the device from both a security update and Google Play system update.

The dashboard also provides access to **Additional security settings**:

- **Biometrics**: Manage facial recognition settings and fingerprints allowed to unlock the device.
- **Auto Blocker**: Prevents and blocks smartphone security threats by activating various security settings at once. For more information on this feature, see Samsung Auto Blocker.
- **More security settings**: Manage preferences for other security settings, such as **Theft protection**, **Samsung Pass**, **Secure Folder**, and more.

The following **Privacy** settings can also be quickly accessed from the dashboard:

- **Permissions used in last 24 hours**: Provides insight into which applications have accessed permissions in the last 24 hours. Also provides a list of every application and the permissions they have.
- **Permissions Manager**: Simplified view of all permissions and which applications are allowed or not allowed to access them. If an application is listed as **Not allowed**, permission access was denied by user.

Additional privacy settings can be configured on the **Additional privacy controls** and **More privacy settings** pages. This includes disabling microphone and camera access, accessibility controls, personalization services, and more.

The Samsung Security and privacy dashboard uses safety features developed by Android. To learn more about how these features protect user data, see Android's privacy features.

Samsung Internet Browser

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Samsung Internet provides enterprises with the following security features:

- **Biometric authentication**: Enforce biometric authentication for website logins, web payments, and access to **Secret Mode**.
- **Secret Mode password**: Enforce password access to **Secret Mode**, which can contain confidential bookmarks and saved pages.

- **Protected browsing**: Enable warnings to alert users if they attempt to view known malicious sites that may try to steal confidential data such as passwords or credit card information.
- **Content blockers**: Allow the use of third-party plugins to filter out content such as: ads, which can come with cookies, malware, and invisible trackers, which can monitor online activity.

Enterprises can additionally take advantage of the following capabilities to secure mobile browsing:

- Set up an HTTP proxy.
- Enable Transport Layer Security (TLS) encryption of browser traffic.
- Filter URLs or domains.
- Block pop-ups through extensions.
- Disable or enable JavaScript.
- Disable or enable the autofill of forms.
- Disable or enable cookies, saved sign-in data.
- Delete or preserve personal data.

Samsung Email

On Samsung Galaxy devices, the default email app in most regions is Samsung Email. However, your device may default to another app like Microsoft Outlook depending on your region.

The Samsung Email app is uniquely designed for customers requiring the secure synchronization of their mobile device's emails, calendar, and tasks. Samsung Email can use MS Exchange ActiveSync (EAS) to synchronize with the Microsoft Exchange server.

Samsung Email provides the following key benefits:

Productivity

- EAS synchronization of contacts, calendar, and tasks.
- Federated Lightweight Directory Access Protocol (LDAP) query support.

Security

- EAS certification for accounts.
- EAS certification for Secure/Multipurpose Internet Mail Extensions (S/MIME) messages.
- EAS certification revocation checks.
- Card certification support.

Management

- LDAP account management.
- EAS account management.

Knox Authentication Manager

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Knox Authentication Manager (KAM) is a managed app for shared Samsung devices that provides multiuser facial biometrics and sign-in automation for increased frontline worker productivity and safety. This allows end users to speed-up shared device sign-ins, securely syncs user profiles across shared devices, and eliminates authentication friction by saving and automatically filling user credentials for any productivity app that requires manual sign-in. Profile syncing enables users to enroll once on a single device, then pick up any other device and instantly make it their own for the duration of their shift.

KAM leverages the Knox platform to ensure a high bar of security for our customers:

- **Application Package (APK) Security**: Knox Device Health Attestation, code obfuscation, and access control ensures the app only runs on registered and trusted devices.
- **Data-At-Rest Encryption**: A three-layer encryption model ensures authorization to access Knox Authentication Manager data is checked at every stage. Separate encryption layers are specifically implemented for unlocking the device (credential encryption), unlocking Knox Authentication Manager on the device (device unique key in KeyStore), and for each user profile (user PIN or password).
- **Data-In-Transit Encryption**: All encrypted user profile data is shared by a secure channel over Transport Layer Security (TLS) 1.3.
- **Device Management**: Admins can use various unified endpoint management (UEM) policies to help establish security baselines across their devices. In addition, as devices

running KAM must be enrolled as fully managed devices in Android Enterprise, IT admins can remotely wipe the device if it is lost or stolen.

For more information on how to leverage Knox Authentication Manager in your enterprise, see the Knox Authentication Manager admin guide.

User profiles and syncing

Prior to deploying user profile syncing, all authorized devices must be enrolled into Knox Authentication Manager and assigned a device group.

User facial data and sign-in information in KAM profiles:

- **Requires end user consent**: Data is always encrypted at rest. Transit and keys needed to unlock data are derived ephemerally. Employees can opt-out of face login, reset their Knox Authentication Manager credentials, and delete their user profile at any time.
- **Never leaves customers' business devices**: Knox Authentication Manager never shares profile data directly to the customer, Samsung or its subsidiaries, or any third party. KAM achieves this by leveraging device-to-device syncing of profile data.
- **Can be managed by IT admins**: Through a managed application configuration, IT admins can enable or disable face login, both locally (e.g., per facility) or globally. In addition, they can implement a timeout period to automatically remove unused profiles in the event where an employee moves between device groups or leaves the company.
- **Is limited to only necessary data**: Each profile contains sign-in information for selected work applications (identity provider or Active Directory credentials) and facial data (after user consent). An end user can also choose to opt out of storing their credentials in selected work applications if desired.

Prior to syncing of user profiles across devices, devices with Knox Authentication Manager installed (via Google Managed Applications) must enroll themselves into the KAM server. Samsung Knox maintains a list of shared devices in an online server for device-to-device syncing based on the organization and the device group.

Upon enrollment, device boot-up, IP Address change, or a forced sync action, the device sends its encrypted IP Address to the KAM server. This IP Address is used to sync with other devices in the group. When the device group list changes, each device receives an updated list of device addresses in its group.

Once each device has a device address list for its organization and group, it can begin syncing credentials. Credential syncings between devices triggers when the device is plugged into power and on the same Wi-Fi subnet. A common example is when users return devices to docking stations at the end of a work shift.

Certificate Security

Automated Certificate Management Environment (ACME) protocol

> **Note**
> ACME features are delivered through the Knox Zero Trust Framework, and are only available for devices managed by an EMM or UEM.

ACME is a protocol that automates the creation, distribution, and installation of certificates without user interaction. ACME certificates are a core part of Samsung Knox's capabilities, as they can be used to securely authenticate mobile devices to servers, ensuring that only authorized devices can access restricted resources or perform privileged actions.

ACME certificates can be easily issued by IT Admins in a simple and scalable manner, and provide the following benefits:

- **Minimal User Friction**: Users can authenticate to enterprise apps via certificates, eliminating the need for users to repeatedly enter lengthy passwords during app usage.
- **Silent Installation**: ACME Certificates can be automatically provisioned and silently installed on devices, facilitating high volume deployments.
- **HW-Backed Security**: When a Knox device generates a Certificate Signing Request (CSR), a hardware-backed key is bound to the device and cannot leave its secure environment. When the ACME Server wishes to validate a certificate request, the server can leverage Knox Device Health Attestation information to ensure the device is in a secure state upon provisioning.

How It Works

The following diagram provides an overview of how ACME certificates are issued to managed devices.

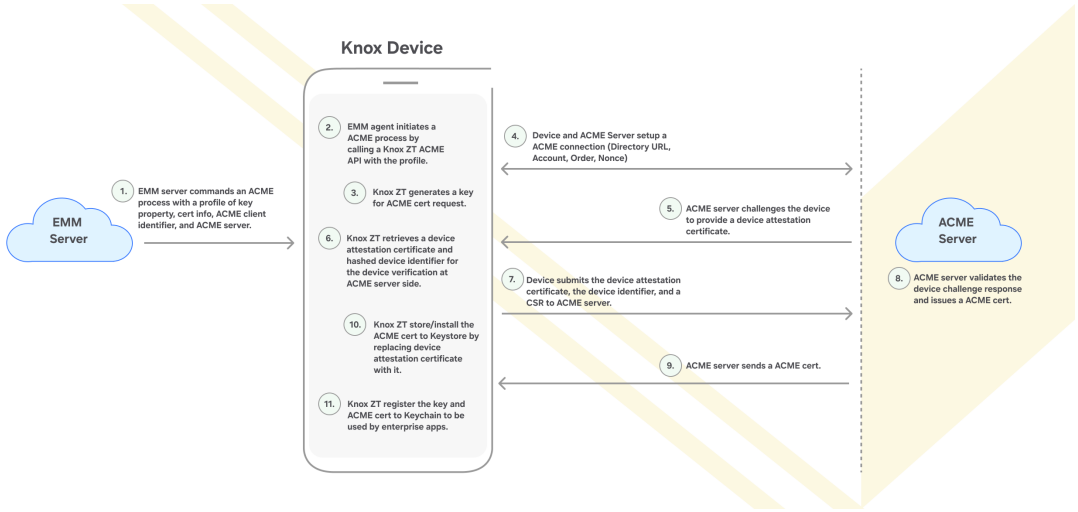

Figure 13: ACME communication flow

Every ACME client is expected to support key pair generation, device identity attestation, and Certificate Signing Request (CSR) by a private key. The Knox Zero Trust Framework provides all ACME client capabilities for designated enterprise apps configured by the EMM.

Enterprise apps that have permission to access a specific ACME certificate can make a request the Knox Zero Trust Framework API to perform certificate provisioning operations. These operations can be found in our SDK documentation.

Certificate requests can be initiated by the EMM agent, however, there is no way to expose the issued ACME certificate in Android Keystore to other enterprise apps, since the private key generated in Android Keystore is only accessible by the application owner. Due to this limitation, the Knox Zero Trust Framework serves as the ACME client, where it registers the issued ACME certificate and the corresponding private key to Android Keychain. This allows the installed ACME client certificates to be viewed and selected by explicitly defined enterprise apps.

Specifically, the Knox Zero Trust Framework:

- Installs the ACME certificate to Keystore by generating a hardware-backed key for the ACME server.

- Stores the ACME certificate in Keystore, by replacing the device attestation certificate with the ACME certificate.
- Registers the key and ACME certificate to Keychain to be visible by other enterprise apps.

Universal Credential Management (UCM)

> **Note**
> These features are only available for devices managed by an EMM or UEM.

The Universal Credential Management (UCM) framework enables Android apps to access all credential storage devices through the same standard programming interface—the Java Cryptography Extensions (JCE) API—via either:

- a specific provider to carry out supported crypto operations,
- the Android Keychain API for key and certificate operations.

The vendor providing the secure element solution (including the applet) implements a UCM plugin, which registers their solution as a Keystore provider. Apps can simply refer to the vendor's provider when calling the Keystore API.

UCM use case

A significant benefit of the UCM framework is that it uniquely enables storage vendors to develop a plugin that provides access to their storage space and cryptographic operations, without forcing app developers to change their code or forcing IT admins or end users to update their apps. The plugin essentially acts as the link between the UCM framework and a specific storage device. The UCM framework allows vendors to make their solution available to specialized apps on the device including:

- **Device lock (keyguard)**: The user inserts a PIN to authenticate themselves to the applet running in the secure element. If the PIN authentication is successful, the UCM framework retrieves a password from credential storage, which is used as the device password to unlock the device.
- **Data at Rest (DAR) encryption**: The applet provides another layer of protection for the device encryption keys. UCM allows for the device encryption key to be wrapped by the applet. The wrapped device encryption is unwrapped when the user provides the correct PIN on device boot.

The UCM framework consolidates and standardizes credential services to provide a streamlined interface for:

- **EMM or ISV apps**: These apps configure, provision, and consume credentials, managing credential storage access permissions, and activating advanced UCM permissions. The apps can enforce the installation, removal, or per-app access control of a credential.
- **Storage provider plugin**: These apps are provided by storage vendors to link the UCM framework to their storage solution, to manage stored credentials.
- **Secure storage**: This feature currently includes the Samsung eSE and Smart Card readers described in Secure elements section. You can easily support other storage options through additional vendor plugins.

The Knox SDK provides credential storage vendors a set of UCM APIs to make current and future storage options available on Samsung devices, hiding the implementation details of their solution so that mobile app developers can transparently access stored credentials through standard APIs, such as the Android Keychain.

Similarly, developers can use the Java Cryptography Extension APIs to offload cryptographic operations to a capable Smart Card. This abstraction, made possible by the UCM framework, eliminates the need for complex vendor-specific code within mobile apps, meaning enterprise customers have a wide range of existing apps available to them and can easily develop in-house apps without worrying about the underlying storage implementation.

UCM allowlists

The UCM framework uses two types of allowlists, which uniquely manage access controls for credential storage and offer fully customizable access permissions:

- App allowlist: Enforces which apps can access each secure storage type. Every secure storage device map to its respective UCM plugin, that a secure storage solution provider creates and maintains.
- Credential allowlist: Enforces each app's access to credentials, providing app-specific access permissions. By enforcing access control, admins can prevent credential usage by malicious or untrusted apps.

Certificates on Secure Elements

While Android apps are able to store digital credentials securely on Samsung Knox devices using the hardware-backed Keystore, some use-cases require credentials and secrets to be stored in a secure element, which can come in the following form factors:

Embedded (non-removable)

- Samsung embedded Secure Element (eSE)
- Universal Integrated Circuit Card (UICC)/eSIM

Embedded (removable)

- Micro SD card
- Universal Integrated Circuit Card (UICC)

External

- Smart cards

Certain customers, especially in government and related industries, have internal regulations requiring the use of approved secure elements for storing credentials and secrets. The secure element is provisioned with an applet that provides certain cryptographic functions.

> **Note**
> The Samsung eSE is not available with the following countries and carriers: USA-Verizon, Korea-All, Japan-All, Canada-TELUS.

Network Security

Wireless communication security

Wi-Fi security

Wi-Fi network is globally used for wireless data transmission and reception. However, public Wi-Fi networks are highly attractive targets for attackers who want to steal and manipulate wireless data. In such scenarios, attackers can collect plaintext data containing personal information, and further steal sensitive information such as login credentials. The following section describes the additional security features that we have on top of existing Android capabilities.

Secure Wi-Fi

An insecure Wi-Fi network is the one that has a security standard below Wired Equivalent Privacy (WEP) or is an open network without any password. To protect user data from such attacks, we have the Secure Wi-Fi feature, which is based on network data encryption technology. It provides a more secure environment for Samsung Galaxy users to use Wi-Fi networks.

Secure Wi-Fi protects your connection by creating a secure tunnel using symmetric encryption with Advanced Encryption Standard (AES) and asymmetric encryption based on Elliptic Curve Cryptography (ECC) as defined by National Institute of Standards and Technology (NIST). This encryption is certified by National Information Assurance Partnership (NIAP).

Secure Wi-Fi has the following core security capabilities:

- **Strong encryption**: Secure Wi-Fi uses Internet Key Exchange Version 2 (IKEv2) as its security key exchange protocol. Secure Wi-Fi supports IKEv2 rekeying, which means that a secret key can only be used for a specific amount of time, or for sending and receiving a certain amount of data.
- **Mutual authentication**: During the connection establishment process through IKEv2, the client can verify its connection to the correct server by validating the server's certificate. Simultaneously, the server verifies if the client is an authorized user by examining the identity information provided by the client.

- **Auto protection**: When your device connects to an untrusted or public Wi-Fi network, the Secure Wi-Fi automatically turns on. This is particularly useful when using your device at cafes, hotels, airports or any location with an insecure Wi-Fi network. This can be disabled for specific Wi-Fi networks defined by users.
- **Strong privacy guarantee**: While using the Secure Wi-Fi feature, device network traffic is routed through two separate internet relays. Your IP address cannot be used by anyone, including us, to determine the websites you visit or the services you access.

Users can view and configure Secure Wi-Fi feature by going to **Settings** > **Security and privacy** > **More security settings** > **Secure Wi-Fi**. Once enabled, users have the option to turn on Secure Wi-Fi protection for specific apps and view history of protection activity.

For more information, please refer to Secure Wi-Fi features.

Bluetooth security

All Samsung devices with Bluetooth enabled implement the full Bluetooth specification. For more information on the Bluetooth specification and its security capabilities, refer to Bluetooth specifications.

Ultra-Wideband security

Samsung devices leverage Ultra-Wideband (UWB) technology to establish wireless connections with precise location tracking, high-speed data transfer, and low power consumption. We've fully enabled the UWB capabilities, supported by the FiRa Consortium, to ensure seamless interoperability and robust security between compatible devices using UWB.

As a widely adopted specification, FiRa is supported by numerous mobile devices and Internet of Things (IoT) technologies. By integrating FiRa, we provide essential security features such as:

- Secure key storage within a trusted element.
- Key management to govern the cryptographic flow of keys used in conjunction with UWB.
- Secure ranging capabilities to guarantee the reliability of measurements on compatible devices.

Knox Firewall

> Note
> This feature is exclusively available to enterprise customers and specific use cases. It can be used for managed use cases.

Most mobile device platforms use built-in firewalls, but they often lack granular control over firewall settings and activity. With the Knox Platform, you can configure firewalls tailored to meet your enterprise security requirements.

The built-in firewalls may not provide the security and data protection your organization needs. In some cases, they may not even allow you to view the policies being enforced. By leveraging the Samsung Knox Platform, you can exactly know which policies are deployed, and take additional security measures to safeguard your enterprise systems.

With the Samsung Knox Platform, you can:

- Restrict and redirect Internet access to specific IP addresses and domains.
- Set firewall policies on a per-app or device-wide basis.
- Generate logs reporting the blocked domains accessed by users.

Granular control over Internet access

You can limit network connections to only trusted addresses by setting the appropriate Internet access restrictions. The Knox Platform offers multiple restriction methods, which can be used individually or in combination:

- **IP address filters**: Allow, deny, and redirect access to specific IP addresses. Configure these filters to apply to transmitted data, received data, or both. Allow or deny both IPv4 and IPv6 formatted addresses.
- **Domain name filters**: Allow or deny access to an entire domain or sub-domain.
- **Per-app and device-wide modes**: Give specific apps—for example, ones that handle confidential data—stronger firewalls, and all other apps on a device a more lenient firewall configuration.

Log unsafe domain access

The Knox Platform provides insights into denied attempts to access blocked domains, helping you stay informed about potential security breaches or insecure browsing practices within your organization.

The Knox Platform logs detailed reports containing the following information:

- App name: The package name of the app attempting to access a blocked domain.
- Blocked domains: The URLs of the domains blocked by your firewall.
- Timestamp: The time of the incident, to assist in troubleshooting.

Secure remote access

Knox ZTNA

> Note
> This feature is exclusively available to enterprise customers and specific use cases. This feature can be used in any deployment mode.

Traditional Virtual Private Network (VPN) solutions grant broad network access, increasing the attack surface and potential risks. These solutions lack the granular control and context-based access required to meet the needs of modern mobile workforces and cloud environments. Legacy solutions struggle to adapt to the dynamic nature of mobile devices, cloud applications, and evolving security threats.

As the global workforce becomes increasingly mobile, remote work and Bring Your Own Device (BYOD) is becoming a standard practice. So, ensuring secure remote access to corporate resources is critical for maintaining productivity, data security, and regulatory compliance.

Knox Zero Trust Network Access (ZTNA) framework is a network flow interception framework designed for advanced zero trust network access solutions. It allows for granular network controls on a per-app and per-domain basis, enabling protocols such as:

- Quick UDP Internet Connections (QUIC)
- Multiplexed Application Substrate over QUIC Encryption (MASQUE)

Knox ZTNA facilitates the networking redirection of the widely used protocols, such as User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Domain Name System (DNS). For integrating this framework, support from a service provider is required. For more information on supported partners and device configuration, refer to Zero Trust Network Access.

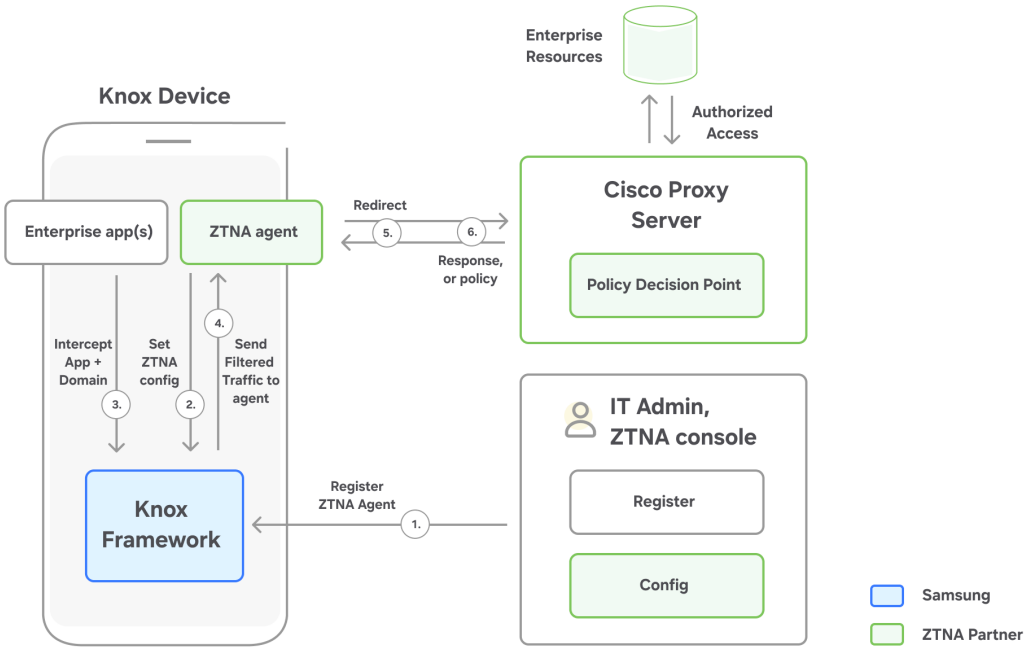

Figure 14 : Knox ZTNA explained

Capabilities supported by the Knox ZTNA Framework

- **Host based micro-segmentation**: Isolates network traffic on a per-app or per-domain basis. It enhances security by ensuring that apps and domains are only accessible to authorized users, thereby reducing the attack surface. Administrators can implement this as a device-wide or profile-wide policy.
    - **Split DNS tunneling**: Enables separation of DNS queries, selective DNS queries (internal and/or external) can go through respective ZTNA proxy servers configured by IT admin. This improves both security and performance by directing traffic appropriately.
- **Context-based metadata injection**: Dynamically adds metadata to network traffic based on the context, such as app package name, app signature, app version, and so on. It can be used for policy enforcement, logging, and enhancing security measures.

- **Dynamic firewall support**: Enables configuration of firewall rules dynamically by forwarding only DNS queries (allow/block/resolve) to cloud. It provides flexibility in managing security policies and adapting to potential threats swiftly.
- **Privacy presumed proxy**: Ensures that user data is protected by anonymizing or encrypting traffic as it passes through the proxy, thereby maintaining data privacy and enhancing data security.
- **Co-existence with VPN/Mobile Threat Defense (MTD)**: Operates independently of VPN framework, so it can function alongside VPNs and/or MTDs. It allows for secure remote access while maintaining the benefits of proxy-based architecture, such as improved performance and enhanced security management.
- **Robust enterprise VPN integration**: Seamlessly integrate with client VPNs through the built-in Knox VPN framework, with support for advanced features like per-app VPN, device-wide VPN with or without disallowed apps, and Proxy Auto Configuration (PAC) authentication.

Fields supported for metadata injection in Knox Proxy framework

The following fields are supported for metadata injection on traffic handled by the Knox Proxy framework:

- **App package name**: Identifier of the application that originated the network flow.
- **App signature**: Signature of the application that originated the network flow.
- **App version**: Version of the application that originated the network flow.

Knox VPN

Standard Android provides basic VPN capabilities that are adequate for most consumers. However, enterprises often require enhanced security and more flexible VPN controls for larger deployments.

The Knox VPN Framework

The **Knox VPN framework** offers the most advanced enterprise-focused feature set, ensuring that VPN connections are efficient, reliable, secure, and compliant with industry regulations and best practices. In addition to the built-in VPN client, the framework also supports the integration with third-party VPN clients.

The Knox VPN framework supports all common VPN types, protocols, and configuration options. When deploying VPN solutions, enterprise IT admins must:

- Ensure VPN deployments work smoothly.
- Optimize server resource usage.
- Limit the VPN solution licensing costs.
- Enforce strict security policies to prevent data leakage.

Unique advantages of the Knox VPN framework

The Knox Platform provides the following differentiators and advantages for VPN solutions:

- Cost-efficient on-demand VPN tunnels, used only when apps within a VPN profile are running.
- Convenience to bypass VPN tunnels when a device connects to a local corporate network on-premises.
- Applications that are added to the VPN configuration can't bypass the VPN tunnel.
- Ability to connect multiple tunnels simultaneously from different VPN clients within the same user space.
- Additional security by chaining VPNs which are also known as cascading or nesting VPNs. This is useful for classified deployments where greater anonymity is required.
- Web proxy configuration over VPN:
  - Web proxy configurations are VPN tunnel specific.
  - Web proxy support for New Technology LAN Manager (NTLM) authentication, basic authentication, PAC, and PAC with authentication.
- Advantage of extending VPN tunnels from a mobile device to a tethered laptop, enabling network connectivity even when the laptop lacks network access.
- Support built-in Android VPN client for Work Profile mode in both personal and corporate devices.

High security built-in VPN client

The built-in Android VPN client is available on all Samsung devices, and it's integrated with the Knox VPN framework. This integration enables additional properties in the Knox Platform. The built-in VPN client, even without the Knox VPN framework, is differentiated from what Android offers, providing these advanced VPN features:

- Federal Information Processing Standard (FIPS) 140-2 certified device cryptographic components.
- Commercial Product Assurance (CPA) certification at the Foundation Grade, based on its successful Common Criteria evaluation against the Protection Profile for Internet Protocol Security (IPsec) VPN Clients v1.4.
- Security characteristics of IPsec VPN client version 2.5, as set by the National Cyber Security Centre (NCSC).
- Internet Key Exchange version 2 (IKEv2) and Suite B algorithms:
  - IKEv2 with Pre-shared keys (PSK) and certificate-based authentication.
  - IKEv2 — pre-shared key, certificates, EAP-MD5, EAP-MSCHAPv2, EAP-TLS authentication methods, and mobile extensions.
  - IKEv2 and Suite B cryptographic algorithms supported with Elliptic Curve Digital Signature Algorithm (ECDSA) signatures.

Features dependent on the VPN client

The following Knox VPN features are also available, but are dependent on the VPN client:

- **Quality of Service (QoS) or traffic tracking and shaping**. The Knox VPN framework can notify the VPN client when installed apps generate traffic.
- **Automatic reconnection of VPN tunnels upon server-side disconnection**. Server-side disconnections are more difficult to detect and handle than device-side disconnections, which are often related to detectable conditions like connectivity loss or presence of new network connections, such as a new Wi-Fi network.

Robust handling of enterprise requirements

Regardless of the features you choose, the VPN should remain predictable and resilient, even during unexpected scenarios. The following are some common scenarios where Knox Platform enhancements ensure proper VPN behavior:

- VPN tunnels handle system events such as:
  - Power saving mode (entry or exit)
  - Package addition or removal
  - Connectivity changes
  - Admin app changes

- VPN profiles allow you to specify which non-present apps are permitted or restricted from using the VPN tunnel when installed.
- Even the free built-in VPN client supports all the advanced VPN features mentioned above.
- Ability to maintain uptime of the VPN connection even during app configuration changes.
- Robust blocking rules prevent data leakage outside the tunnel. Common gaps that are correctly handled include:
  - VPN client crashes or other client app issues.
  - DNS leakage during system events like network switches or configuration changes.
  - Proxy port blocks apps which are not added to VPN profile from accessing proxy server, this prevents potential network attacks.
- Handle captive portal interactions before establishing a VPN tunnel.

Application Security

Samsung Message Guard

Samsung Message Guard is an advanced feature which prevents zero-click attacks on messaging applications. This feature is included as part of Samsung Auto Blocker, and is enabled by default for all Galaxy devices running One UI 6.0 and higher.

Messaging apps contain various permissions, ranging from access to common utilities such as photo gallery and calendar to more sensitive utilities such as files, microphone, and camera. So, when an attacker compromises these apps, the damage can be catastrophic. Samsung Message Guard is used to mitigate these types of attacks on messaging apps.

Whenever an image file arrives via text, it is trapped and isolated from the rest of your device. This prevents malicious code from accessing your phone's files or interacting with its operating system. Samsung Message Guard checks the image file bit by bit and processes it in a controlled environment or sandbox, ensuring it cannot infect the rest of your device. It runs in the background and doesn't need any activation by the user.

To ensure defense in depth against threats, the following security principles are applied:

- **Broad coverage**: All image files received via messaging apps are considered untrusted data.

- **Never-trust**: All untrusted data received is isolated from the system. For isolation, the image decoders are separated from the messaging app. Thus, mitigating any vulnerabilities in parsing & decoding functions.
- **On by default**: All messaging apps are supported, without the need of any additional integrations.

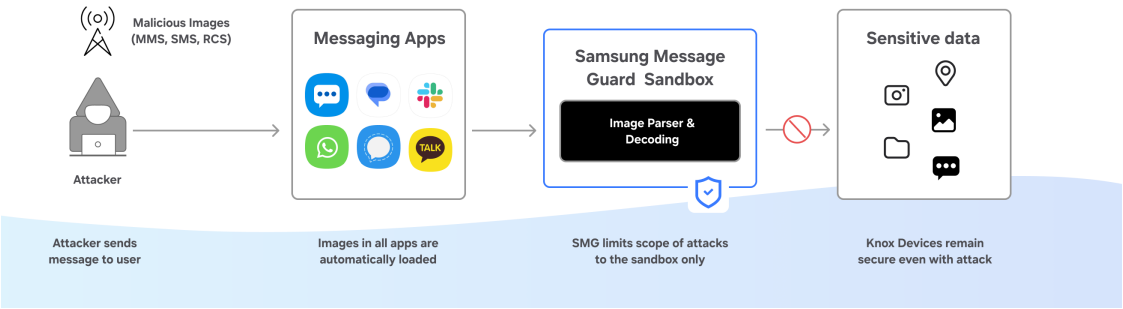

Figure 15: Message Guard explained

> **Note**
> Before the release of Samsung Message Guard, Samsung already isolated video and audio file types.

Samsung Wearables Security

Samsung Galaxy Watch

Before the release of Samsung Galaxy Watch4, our smartwatches used Tizen operating system. With the introduction of Wear OS in Samsung Galaxy Watch4, we adopted foundational security capabilities of Android, and brought enterprise-grade security to the wearable technology market.

This shift marked a significant milestone in wearable device security, enabling businesses to confidently deploy Samsung Galaxy Watches as part of their mobile ecosystems.

The Samsung Galaxy Watch boasts the following key security features:

- **Root of Trust**: The smartwatch's root of trust is anchored in Arm Trust Zone, providing a secure foundation for all operations.

- **Trusted Boot**: Trusted Boot ensures the device boots securely and that its firmware remains healthy, reducing the risk of malware or unauthorized changes.
- **Kernel Protection**: Security Enhanced (SE) Android and Samsung Defeat Exploit (DEFEX) work together to protect the kernel, preventing any malicious code from compromising the smartwatch.
- **Application Sandboxing**: Android application sandboxes isolate apps and prevent them from interfering with one another, like on any traditional Android device.

For enterprise IT admins, only smartwatches supporting Wear OS can be managed using Knox Manage. Device policies are applied to the watch through the paired mobile device, which receives updates from IT admin.

Samsung Galaxy Watch supports various device policies, including the following:

- **Remote Wipe**: Remotely wipe data and information from the watch, returning it to its factory state.
- **Device Setting Lock**: Lock the device into a specific setting profile, preventing changes to settings.
- **Feature Restrictions**: Restrict features like downloading new apps, granting permissions, or modifying default mobile device settings.
- **Application Management**: Manage which apps can be updated and installed on the watch.

Security Operations

Software Lifecycle and Updates

Frequent software updates are often necessary to resolve bugs, patch security vulnerabilities, and enhance device capabilities. However, updates can pose a stability risk. This may lead to productivity loss due to changes in underlying device functionality.

Starting with the Samsung Galaxy S24, devices will recieve 7 years of support and security patches. Device security updates are a top priority for Samsung as we continue to improve the operational processes for software updates. To view your device patching cadence, see Security Updates Scope.

Knox security patch lifecycle

The advanced software supply chain and lifecycle of Samsung mobile devices is a multi-faceted system involving the collaboration of numerous stakeholders. We address and patch security vulnerabilities by adhering to a simple, yet effective five-step lifecycle management plan:

1. **External & internal change identification and development** — Through Samsung's bug bounty program, internal testing, and chipset partner testing, security issues are identified and patches are developed. This process is constantly ongoing at Samsung.
2. **Software change propagation** — Samsung incorporates patches from third parties such as Android, Qualcomm, MediaTek, and others into all devices. These patches may be subject to software vulnerabilities that Samsung aims to address.
3. **Software binary construction and quality assurance** — Samsung builds the device firmware and begins quality assurance testing in accordance with the device's security update cadence. Different devices receive software updates at different cadences. For more information, see Samsung Security Bulletin. This process is constantly ongoing at Samsung.
4. **Carrier testing** — Device binaries are sent to mobile carriers to ensure they function to the highest capacity on their networks. If issues are identified, the device binary is fixed and retested.
5. **Firmware release and device update** — Firmware is released and devices can download the update as according to its system update configuration.

Due to the rich partnerships Samsung has formed with chipset vendors, carriers, and more, Samsung is able to consistently deliver software updates globally for hundreds of device models.

If you're an enterprise or user who would like to learn more about the cadence of software updates for your device models, detailed information for all Android Enterprise Recommended (AER) devices is available on the Devices secured by Knox page.

Security Patch vs Maintenance Release

Device firmware updates range from simple security updates to robust system operating system upgrades. Different types of updates can result in downtimes in productivity, application compatibility issues, and more.

For enterprise customers of Samsung, we provide clear visibility into the type of update a device is receiving. This allows IT admins to take relevant actions to ensure smooth firmware deployment. Device updates can come in three separate forms:

1. Security maintenance release (SMR)
2. Maintenance release (MR)
3. Operating System upgrade (OS upgrade)

With security maintenance releases, there is little risk in deploying the update as soon as it is available. SMRs only include security patches and don't include additional bug fixes on the platform.

For maintenance releases, some functions may be adjusted to improve performance and fix bugs. These changes always have a small risk for additional bugs—we encourage admins to stagger their deployments in order to identify any issues that may arise prior to deploying to all assets.

Operating System upgrades always contain significant changes to the platform. The content of these updates can vary. It's encouraged to identify a deployment strategy where admins can test OS upgrades to ensure stability of their environment prior to mass deployment.

Occasionally, to optimize on the number of times your device must upgrade its firmware, an SMR may be combined with a MR. With Android managed system updates, you'll be unable to see this level of information. Users concerned should leverage Knox E-FOTA to gain insight into the types of updates available for a specific device model.

Vulnerability reporting

Samsung Security Bulletin

Samsung provides vulnerability disclosures monthly. These outline Samsung Vulnerabilities and Exposures (SVEs) and Common Vulnerabilities and Exposures (CVEs) that may be patched with the next Security Maintenance Release (SMR). Given SMR versions are tied to the Android Security Patch Level (ASPL), some SVEs may not be patched on all devices in the subsequent month due to patch distribution from chipset vendors, carrier testing, or other factors. See the Security Updates bulletin for the latest information on patch rollout of SVEs.

The CVEs contained on Samsung's security bulletin are released following official disclosure from the Android Security Bulletin, alongside any relevant CVEs only applicable to Samsung devices. SVEs have a matching CVE that can be found on our security bulletin.

> Note
> Due to the rapid patching of Samsung discovered vulnerabilities, a matching CVE may be listed as pending until it's fully processed by the National Institute of Standards and Technology (NIST).

Vulnerability management

Due to limited insight into the patch distribution and vulnerability attribution for third party tools, vulnerabilities may be mapped incorrectly for Samsung Galaxy devices as a result of differences in device hardware, software, and other factors across device models. We strongly encourage our customers to leverage Knox Asset Intelligence for accurate vulnerability management and as a source of vulnerability information into third party tools.

Bug Bounty Program

To improve the security and privacy of our products and minimize risk to end users, Samsung offers a rewards program for eligible security vulnerability reports. Through this reward program, we hope to build and maintain valuable relationships with researchers who coordinate the disclosure of security issues with Samsung Mobile.

To ensure a smooth and timely operation when submitting an eligible bug to our program, please carefully read the requirements and guidelines captured on our Security reporting site.

Samsung Vulnerability Communication Program

The **Samsung Vulnerability Communication Program** (**SVCP**) is available for select partners and customers with mature security operations teams. Through this program, we provide additional insight into vulnerabilities that haven't publicly been disclosed or are currently discussed in the media.

This limited service is reserved for partners who leverage our devices for sensitive actions such as payment systems, medical devices, special operations, and more. The information provided by the SVCP provides early insight into patch rollout and mitigations for your enterprise until a patch is available.

An SVCP report may also discuss a vulnerability or incident that doesn't directly apply to our platform as part of an effort to help drive clarity towards the impact on Samsung mobile devices.

If you believe your enterprise should be included in this program, please reach out to your Samsung Sales Representative.

Knox Cloud Services & Integrations

KCS Overview for managed devices

> **Note**
> This feature is only available on managed devices, and requires the use of an EMM or UEM.

Samsung Knox offers a variety of cloud solutions to assist with enterprise device management. Our cloud solutions are complimentary to IT asset management solutions and have native integrations with leading MDM, UEM, and SIEM solutions.

Samsung Knox products include:

Samsung Knox Product	Use Cases	Device Management Type
Knox Mobile Enrollment	Device set up and EMM enrollment	Corporate owned managed devices
Knox Mobile Enrollment Advanced	Device set up and EMM enrollment with loss prevention	Corporate owned managed devices

Knox E-FOTA	Firmware management	Corporate owned managed devices
Knox Asset Intelligence	Enterprise device productivity, Security telemetry	Corporate owned managed device
Knox Manage	Unified device management	Managed devices (iOS, MacOS, Windows, Android)
Knox Remote Support	Remote access to a single device for troubleshooting	Corporate owned managed devices

All Samsung Knox cloud solutions are SOC2 certified and have supplementary controls for enterprises requiring additional compliance support (e.g., General Data Protection Regulation (GDPR) requirements). For more information, see Knox security certifications and guidance.

Managed software updates

It's important for enterprise customers to have a strategic software rollout plan and the controls to execute their plans. To assist with this process, Android Enterprise and Samsung Knox offer various tools to help understand the security risks associated with an out-of-date device, when a software updates are available, and controls to manage firmware over the air (FOTA).

Controlling the rollout of software updates allows IT admins to:

- Homogenize the firmware versions and capabilities of deployed device models.
- Carry out interoperability or compatibility testing with in-house or proprietary servers, apps, and endpoint settings.
- Ensure that known issues are patched before the deployment of major firmware version updates.
- Perform field tests of new firmware and software on a subset of devices before mass deployment.
- Force the use of firmware versions that have been validated to meet industry certification or regulation requirements.

Android Enterprise's managed system updates feature offers foundational controls for firmware management. Using these controls, many enterprises can achieve a robust firmware management plan without sacrificing productivity. Through Android Management APIs (AMAPIs), EMM solutions can:

- Enforce software updates and allow the user to temporaily delay an update and schedule it for a later time.
- Delay operating system (OS) upgrades and maintenance releases for up to 60 days.
- Allow firmware download over Wi-Fi only.

Beyond Android Enterprise controls, a wide range of EMM partners support Samsung's firmware management features by integrating firmware management with other asset management activities. IT admins can use these tools to test and deploy software updates in a consistent and low-risk manner. By using EMM solutions, enterprises can restrict users from loading unauthorized firmware through their devices or USB-connected computers.

Through the Knox platform, enterprises can also:

- **Disable automatic firmware updates**: IT admins can prevent users from using Android settings to enable or disable automatic firmware updates.
- **Disable all OTA updates**: IT admins can prevent users from using Android settings to enable or disable all software updates. This includes updates for firmware, security patches, bug fixes, and apps.
- **Disable USB-connected updates**: IT admins can prevent users from booting into **Download Mode** and manually installing a software update. This includes updates through the Odin, Kies, and Smart Switch update tools.

Samsung Knox firmware controls are complimentary to Android Enterprise managed system updates. While effectively managing firmware on Samsung devices doesn't require Knox cloud software or controls, there are numerous benefits for leveraging the Knox platform's added capabilities.

Knox E-FOTA

Samsung developed Knox Enterprise Firmware Over-the-Air (E-FOTA) to enable enterprises to efficiently manage mobile infrastructure, reduce support costs, and save time. With Knox E-FOTA, IT admins can ensure that device users can't independently update to unsupported firmware versions, preventing issues that could negatively impact employee productivity, support costs, and data security.

With Knox E-FOTA, enterprises can control device software updates in the following ways:

- **Select the target firmware version**: Knox E-FOTA provides a list of firmware options and their corresponding details based on your device model. You can set the target Android OS version or update to the latest version.
- **Force target firmware version update onto select devices**: Enterprises can push new firmware to specific devices to ensure interoperability and compatibility with proprietary systems and apps. This prevents any operational or performance issues that may arise due to incompatibility.
- **Schedule updates during non-peak work times and granular network resource management**: Knox E-FOTA offers setting granular control over when to download the update, and how. This ensures update scheduling prevents any interruptions to employee productivity. Additionally, Knox E-FOTA enables enterprises to manage network bandwidth restrictions through a set of configuration options, and deploy the updates entirely on-premises.
- **Mass deploy the target firmware version**: Mass deployment eliminates the issue of software version fragmentation, and there's no need to support multiple legacy firmware versions for every deployed device. You can ensure that all devices are updated to the desired firmware version, regardless of their current firmware version.

Recommended update cadence for users & enterprises

> **Note**
> Choosing the best update cadence for your enterprise requires alignment with your cybersecurity strategy. It's important to have a clear understanding of your goals and compliance requirements ahead of deciding the update cadence for your devices.

To effectively manage Samsung mobile devices, it's important to keep the following objectives in mind:

- Patching as soon as possible is a priority to reduce security risk.
- Maintain a control group and a test group for rolling out device updates (non-security).
- Ensuring device stability after a patch requires a feedback loop.

As described in Security patch vs maintenance patch, there are numerous types of software updates released. Maintenance releases and operating system upgrades can potentially impact

dependent software and systems that interface with the device. However, security updates don't carry this risk and are purely beneficial. It's important to not delay these types of updates and roll them out as soon as possible.

For handling non-SMR related updates, we encourage our users to leverage Knox Asset Intelligence and Knox E-FOTA.

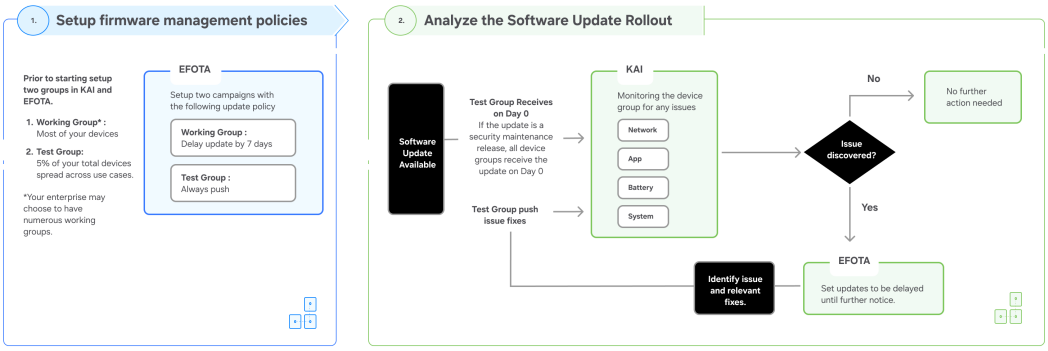

Figure 16: Knox E-FOTA and Knox Asset Intelligence flows

For OS upgrades and One UI updates, enterprises can enroll in the OS beta program and get a head start on the integration process. This can help you make necessary changes to in-house applications and configurations prior to deploying to a large-scale software update.

> **Note**
> When participating in the OS beta program, Knox E-FOTA and Knox Asset Intelligence will not be available for use.

For more information, please contact your Samsung Sales Representative.

Knox Asset Intelligence Security Center

> **Note**
> These features are only available for devices managed by an EMM or UEM.

To help Samsung Knox customers better manage their security risks, SecOps Teams can easily track the security posture of every device in their fleet with powerful insights like the total number of devices with vulnerabilities detected, which devices have outdated security patches, and which devices pose the highest security risk to the organization.

The Knox Asset Intelligence Security Center provides clear, granular mapping of device vulnerabilities, as well as routine attestation to track the health of enrolled Samsung Knox endpoints. SecOps Teams, in collaboration with IT admins, can prioritize security patching efforts based on security risks reported by the Knox Asset Intelligence Security Center.

For example, if an organization has a mixed device fleet consisting of XCover Pro and Galaxy S22 models, the Security Center can report the total number of vulnerabilities affecting each *specific* device model, and *omit* any devices that already have the latest security patches deployed, thus making it easier for SecOps and IT admins to identify only the devices that are at risk. IT admins can then launch Knox E-FOTA to deploy the correct security patch for each model, ensuring that devices are updated in the most effective way, with the least amount of business disruption.

The Security Center provides 3 benefits for enterprises:

- Granular mapping of vulnerabilities to individual device models
- Daily health attestation through Knox Device Health Attestation
- Knox Security Events & Log for Security Operations Centers

Vulnerability management

As many purpose-fit devices are deployed across the enterprise, the ability to manage security risks becomes increasingly complex due to differences in device vulnerabilities and patch cadence. Without an understanding of each device's hardware and drivers, enterprises have no way to accurately assess the risks posed by certain chipset vulnerabilities, or know which devices were—or could have been—exploited.

Security Center leverages Samsung's software and hardware supply chain to directly map vulnerabilities to devices. By hooking directly into our software supply chain, we can granularly track which vulnerabilities have an impact on each specific binaries, and specify which builds patch each vulnerability. This becomes especially important for devices impacted by Samsung Vulnerabilities and Exposures (SVEs) not bound to the Android Security Patch Level (ASPL).

Given the diverse set of Samsung devices across the globe, many device families often have differing hardware depending on the region. For example, a Galaxy S24 in the US has a Qualcomm chipset, while EU models have the Exynos chipset. This difference in chipset can have a significant impact on how vulnerabilities get patched, as one vulnerability reported in one chipset may not be reported in the other, despite being the same device model. In other words, a Galaxy S24 with a Qualcomm chipset will have different vulnerabilities than a Galaxy S24 with an Exynos chipset. With the Knox Asset Intelligence Security Center, you can trust that the

vulnerabilities reported are the actual vulnerabilities that impact the models in your fleet, right down to the root hardware and software level.

Daily attestation

Each device enrolled in the Security Center gets attested on a daily basis to verify its security posture. If devices are offline (no internet connection) or powered-off during the attestation request, these devices are categorized as **Unknown** in the Security Center dashboard. If attestation is successfully carried out, devices are categorized as either **Good** or **Bad**. Devices with a **Bad** attestation result should be investigated immediately, as this is a strong indicator of compromise.

Connecting Security Center to your SOC

To allow security telemetry to be gathered from your devices, a **Security Information & Events Management** (SIEM) solution must be connected to the Security Center. The Security Center itself does not store any data related to security events or logs, as it purely provides a passthrough architecture. For this reason, IT Admins and SecOps teams must connect Security Center to a third party service for events & log reporting. For more information on how to connect Knox Asset Intelligence with your SIEM solution, please contact a Samsung Knox sales rep.

Document history

Revision history

Document version	Release date	Change list
1.0	07 March 2025	Initial publication