What is Knox?

Samsung Knox is an integrated suite of security features that protects sensitive data on a Knox-enabled device. Some protections are built into the hardware and software of the device, while other Knox protections can be activated later.

Knox protections satisfy five principles:

1. Software Integrity
2. Least Privilege
3. Data Storage Protection
4. Network Protection
5. Data Isolation

1. Integrity of platform software

Devices are preloaded with software from Samsung. This software can only be considered secure if it is from a trusted source, and remains unchanged. An attacker may attempt to make changes to the system software in order to bypass the security features protecting your data. A Knox-protected device can detect when modifications are attempted and lock down sensitive data to prevent it from being leaked. Knox includes features that ensure software integrity including Secure Boot, Trusted Boot, Security Enhancements for Android, Real-time Kernel Protection, and Periodic Kernel Measurements.

2. Least Privilege

Software needs access to device resources, such as data and peripherals, in order to work properly. If software has more privileges than it needs, an attacker could exploit them to cripple the system or steal sensitive data. The best way to prevent this is to ensure every software component has the minimum level of privilege necessary that still lets it do its job.

While Android provides some software restrictions, Knox has the ability to lock down access to your data even more, and when new attacks emerge, Knox devices can receive new software restrictions to block them. Knox accomplishes all this with Knox Workspace, Security Enhancements for Android, and SE Android policy updates.

3. Data Storage Protection

Unprotected private data that is stored on the device, such as email, photos, and other downloads, are attractive targets for hackers. Knox provides protections that encrypt on-device data. These protections include Knox Sensitive Data Protection, Knox Workspace, and On-Device Encryption.

4. Network Protection

Unprotected data that must travel across a network such as Wi-Fi, cellular data, or Bluetooth can be intercepted by hackers. Enterprise device security can also be compromised if a user exchanges data with a suspicious source. Knox provides network encryption and protections that only allow trusted devices to connect to an enterprise's servers. Additionally, Knox provides network encryption via the Knox VPN framework, and additional security for web traffic like Knox HTTP Proxy over VPN.

5. Data Isolation

Private data should be stored and managed in a secure space, away from untrusted apps. The Knox Workspace is a secure container for apps and data. Any app or data stored in the Knox Workspace is isolated from the rest of the device software. Separating private data ensures it won't be accidentally or maliciously viewed or leaked, since only apps inside the Workspace can access the data. IT Admins can manage the Knox Workspace and the apps and data that are protected by use of Mobile Device Management, or MDM, software.