KNOX Mobile Security

Defence-grade security for an open world

People will be people. They like what they like, do what they do, and will get a little carried away sometimes. Naturally, they'll lose a work phone or two, or use them in places you don't want them to, but that's okay...

That's why we use Samsung Knox, mobile security from the chip up, now trusted by many governments worldwide, made for the way people really work. Because why attempt to change your employees' behaviour, when you can simply change their mobile security?

Trusted by governments and corporations around the world Samsung Knox delivers defence-grade security to safeguard your business.

It's built into the hardware and software, and performs multiple checks to ensure that your device is running as it should. Real-time monitoring and protection makes it virtually impossible for any unauthorised access to your phone's data.

Knox workspace

The Knox Workspace is a secure container which separates data stored within it from the rest of the operating system. It provides additional security features, over and above those of the underlying Android platform. Users can store all or some of their enterprise data in the Knox Workspace, providing enhanced protection.

A variety of approaches can be taken when using the Knox Workspace within an organisation.

- For users working primarily with sensitive data, the majority of their work will be within the Knox Workspace. The Android platform outside the Knox Workspace is used for non-sensitive work.
- Users who only access sensitive data occasionally can use the Knox Workspace when they are required to work with that sensitive data, doing the non-sensitive majority of their work outside the container.
- Enterprise applications and data should be kept within the Knox Workspace where possible. Unnecessary applications outside the container should be removed or managed using an appropriate whitelist.

This is what the **National Cyber Security Centre**, a part of **GCHQ** has to say about Knox.

"KNOX fulfils the 12 security principles for mobile devices [1]"

1. Data-in-transit protection
2. Data-at-rest protection
3. Authentication
4. Secure boot
5. Platform integrity and application sandboxing
6. Application whitelisting
7. Malicious code detection and prevention
8. Security policy enforcement
9. External interface protection
10. Device update policy
11. Event collection for enterprise analysis
12. Incident response

[1] - https://www.ncsc.gov.uk/guidance/end-user-devices-security-principles