Hardware Root of Trust

Unsecured mobile devices pose a great threat to the safety of personal or enterprise data. Fortunately, KNOX provides software to protect against hackers who want to access your sensitive data.

But, software can be replaced or modified, so how can KNOX be trusted?

The foundation of KNOX security is something called *Hardware Root of Trust*. This means that the security checks are *rooted in*, or *begin with* hardware checks. Hardware checks are very reliable and can't be attacked in the way software can. Upon device startup, Samsung uses hardware as a basis for checking all software components. The software performs a check on each KNOX feature before allowing it to run. Since this *chain of security checks* begins with the very first hardware check, each feature is protected by hardware root of trust. No matter which link in the chain an attacker targets, one of the security checks will detect it.

SAMSUNG
Knox

Hardware Root of Trust

When a security check detects an unapproved software change, either the boot process stops or the KNOX tamper-fuse is blown. The KNOX tamper-fuse, which is built into the device hardware, permanently blocks access to the KNOX KeyStore when blown. This prevents any encrypted corporate data on the compromised device from ever being decrypted and revealed. It also means that the device can't be used to encrypt and store enterprise data in the future. The device still runs, but won't be allowed to use most KNOX security features since detected modifications have broken our chain of trust.

Watch our other videos on **Boot Time Protections** and **Device Runtime Protections** for more information on how KNOX uses this hardware root of trust to provide tamper-resistant protections against boot- or run-time attacks.

SAMSUNG Knox