Boot-time Protections

Many KNOX security features are loaded during initial device startup, also known as boot-time. Attackers may try to modify the boot process to prohibit installation of security features. To prevent security measures from being bypassed, KNOX uses boot-time protections backed by Hardware Root of Trust. These boot-time security tools include KNOX Secure Boot, Trusted Boot and Attestation.

How do these boot-time protections work? Let's start with Secure Boot. When you turn your device on, software called bootloaders launch and configure the underlying operating system components. Many standard Android devices have a first line of defense called Secure Boot, a security check that begins with the trusted hardware. The hardware checks the first bootloader for a unique signature that cannot be forged. This signature certifies that the bootloader is from Samsung and that it has not been modified. Only if the hardware sees a correctly signed bootloader will it allow the device to boot. After completing its start-up tasks, it then checks the next bootloader for a valid signature. This chain of checks continues until the kernel is loaded.

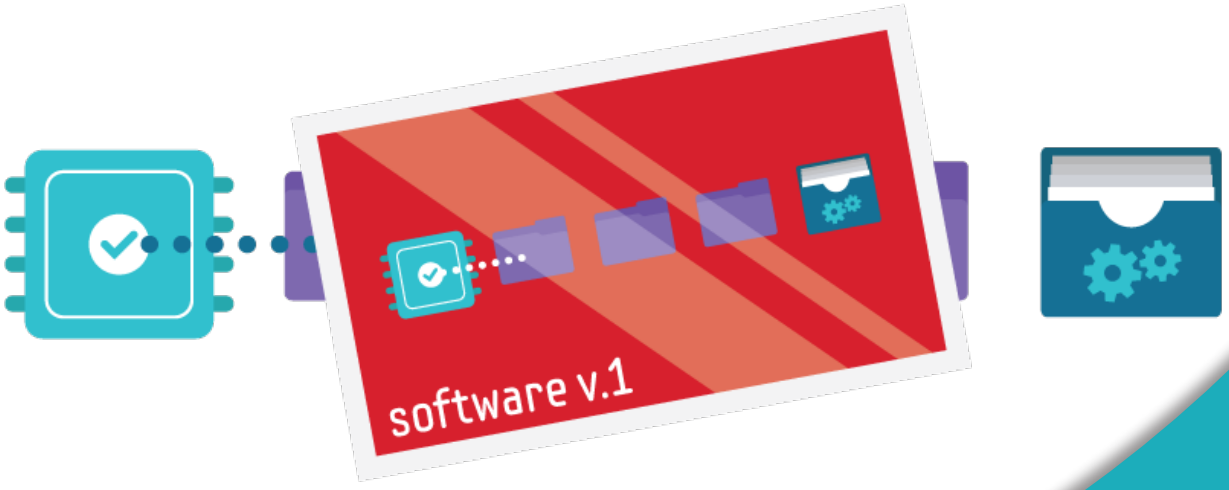
Though Secure Boot can reveal modifications in bootloaders, it cannot reveal if they are the latest version with the most recent security fixes. A hacker may try to roll back, or replace a bootloader with an earlier version that contains bugs, making the device vulnerable to attacks.

SAMSUNG Knox

Boot-time Protections

This is where KNOX Trusted Boot comes in. During the boot process, KNOX Trusted Boot takes snapshots of the state of each bootloader, which can be used to identify what software versions are being used. These snapshots are signed and stored. Enterprise servers can request these snapshots during a process called Attestation. The enterprise servers can then decide if the device should be trusted with their data. The enterprise can inspect a device's Attestation report to determine if the device's protections are up-to-date. If Attestation reveals evidence of unsupported device software, the device can then be denied access to sensitive data.

Watch our other videos on **Run-time Protections** and **Hardware Root of Trust** for more information on how KNOX continues to protect your device against run-time attacks and why our tools can be trusted on a hardware level.



SAMSUNG Knox