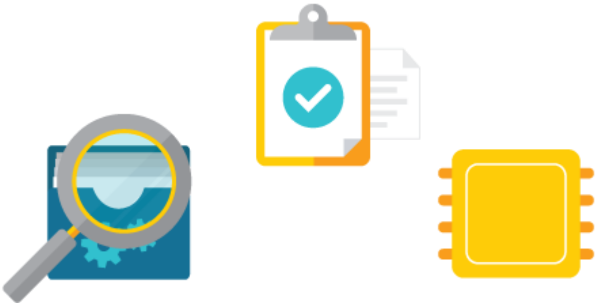
Run-time protections

Samsung KNOX provides security features that carefully monitor your device while it’s up and running. How does it work? Let’s take a look at the core software of the Android operating system – the kernel. When any software tries to access your data, such as your documents or messages, the kernel is responsible for deciding which requests should be allowed. The kernel is software we trust to protect our information.

To bypass security protections, a hacker could find a problem in the kernel that they can use to their advantage, or they could modify the kernel itself. A successful attack on the kernel gives the hacker complete control of the device and the information it contains.

Fortunately, KNOX provides protection from these threats. Periodic Kernel Measurement, or PKM, and Real-time Kernel Protection, or RKP, constantly look for attacks on the kernel.



PKM periodically looks for changes in the kernel, and alerts the user of a possible security issue when a change is detected.

RKP inspects requests from the kernel to the hardware. If RKP sees a request that lowers or disables device security, the request is blocked and recorded. These records are submitted for attestation, a process where enterprises check the device security before trusting it with sensitive information.

KNOX security tools detect kernel attacks to ensure that your sensitive data is protected.