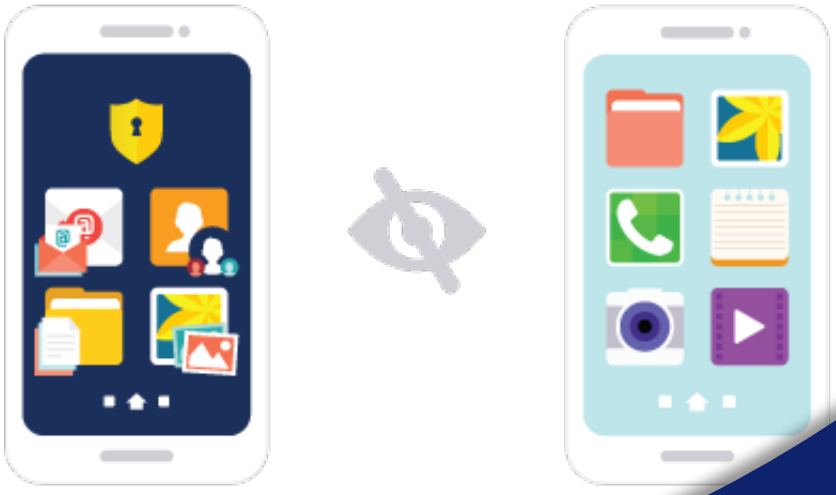
KNOX Workspace

Modern mobile devices help us work more productively. A key feature that enables us to be productive is sharing information. However, when we share private information, we introduce the possibility of malicious or accidental disclosure. So how do we isolate our private data while still maintaining productivity?

One of the important parts of the Samsung KNOX platform is a product called KNOX Workspace. This is a secure container that has its own separate home screen, applications and information. Any apps, emails, contacts, photos, or documents contained in KNOX Workspace are not visible from outside the Workspace.

KNOX Workspace encrypts your work data and isolates it from your personal data using a custom version of Security Enhancements for Android. SE for Android is in charge of enforcing standard rules provided by Android and KNOX security rules. Every time an application asks for resources, these security enhancements prohibit the exchange of data with applications that are outside of the workspace.



SAMSUNG KNOX

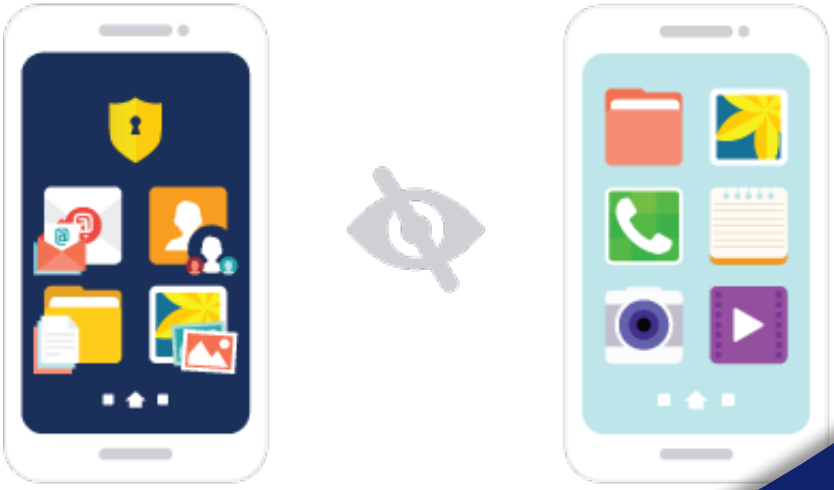
KNOX Workspace

All data within Workspace is encrypted when Workspace is locked. The data can be decrypted when a user unlocks KNOX Workspace using their fingerprint, password, pattern, or pin. If KNOX detects that device integrity has been compromised, KNOX Workspace data cannot be decrypted.

In addition to data isolation and encryption, IT Admins can apply policies using Mobile Device Management software. IT Admins can configure policies to control device behaviors including password rules, geofencing, and sharing restrictions. KNOX Workspace can be managed remotely without intruding on personal data.

KNOX Workspace protects your information while still maximizing productivity. Your sensitive data is kept isolated and encrypted while still being convenient to access and manage.

See our other KNOX videos for an in depth look at other KNOX features.



SAMSUNG Knox