Top 10 reasons to secure your enterprise with Samsung Knox

1. Three words: defense-grade security
   Samsung provides advanced Samsung Knox™ mobile security solutions which deliver the highest level of protection with a combination of Trusted Boot and ARM® TrustZone®-based Integrity Measurement Architecture (TIMA). Knox protects your infrastructure with multilevel hardware-to-application security via Trusted Boot and ARM® TrustZone®-based Integrity Measurement Architecture (TIMA).

2. It’s recognized as the best in the business.
   Knox Workspace was named the Best Secure by Innovation at the 2015 MDM World Summit.

3. It protects every Android layer, right down to hardware.
   Knox Workspace conveniently integrates with your existing MDM, VPN and Microsoft® Exchange ActiveSync, enabling you to tailor a security solution that best fits the needs of your enterprise. It’s easy to manage and customize.

4. In one platform, you get many solutions.
   Knox Workspace container data is protected by the highest level of security, including security for high-value, mission-critical data. The description key is stored in a device-unique hardware key. The decryption key for protected data is stored encrypted by a device-unique hardware key.

5. Nonstop platform encryption for the Knox Workspace
   Knox Workspace container data is protected by the highest level of security, including security for high-value, mission-critical data. The description key is stored in a device-unique hardware key. The decryption key for protected data is stored encrypted by a device-unique hardware key.

6. Sensitive data? It can’t be decrypted.
   Sensitive data protection builds upon Workspace encryption, defining a sensitive class of data that cannot be decrypted by the device without user intervention. The TIMA KeyStore is used to manage cryptographic keys.

7. In one platform, you get many solutions.
   Knox Workspace container data is protected by the highest level of security, including security for high-value, mission-critical data. The description key is stored in a device-unique hardware key. The decryption key for protected data is stored encrypted by a device-unique hardware key.

8. Active Directory integration
   Seamless integration with Microsoft® Active Directory simplifies user on-boarding and off-boarding.

9. It’s easy to manage and customize.
   Knox Workspace container data is protected by the highest level of security, including security for high-value, mission-critical data. The description key is stored in a device-unique hardware key. The decryption key for protected data is stored encrypted by a device-unique hardware key.

10. All your critical security elements are covered.
    Knox Workspace container data is protected by the highest level of security, including security for high-value, mission-critical data. The description key is stored in a device-unique hardware key. The decryption key for protected data is stored encrypted by a device-unique hardware key.

Stay secure with Samsung Knox and Verizon.

For more details about protecting your organization, contact your Verizon representative.