Solution brief

Manage a diverse mobile ecosystem in highly regulated industries.

Samsung Knox offers security and control in financial, healthcare and other data-sensitive environments.

SAMSUNG Knox | verizon

In the past year, the number of mobile devices deployed in the business world has grown dramatically—and so has the number of mobile security threats. In particular, attacks on Android™ devices have been increasing at an alarming rate. As a result of its market share and more open development environment, Android is the main target for mobile threats. In 2012, Android was by far the most commonly targeted mobile platform, with 103 out of 108 unique threats.

IT administrators are tasked with trying to minimize risk and protect data and network resources. As a result, mobile security and manageability have become the top priorities for managers who are struggling to control a multitude of device platforms, applications and compliance policies. Companies are being prompted to:

- **Simplify and standardize operations** by focusing on the appropriate technology, implementing it across the organization and enforcing policies for application and endpoint management.
- **Manage security risks and protect against fraud** by complying with external regulations and internal policies to protect sensitive data, and proactively addressing vulnerabilities to critical information and assets.
- **Secure data end to end** by safeguarding information in motion and at rest, installing strong access controls and managing employee devices.

A three-tiered approach to security

Samsung Knox™ allows regulated companies and agencies to meet stringent security requirements with:

- **Platform security**. Knox isolates applications and data into different domains, prevents unauthorized operating systems and software from loading during startup and continuously monitors the device kernel.
- **Application security**. Knox features application containers, on-device data encryption and virtual private network (VPN) support.
- **Mobile device management**. Knox offers support for management via Active Directory®/Group Policy Manager; VPN and Wi-Fi provisioning; idle-screen and lock-screen configuration.

A sophisticated solution for protecting data

Knox provides additional security features to protect sensitive information, including:

- **Smart-card/Common Access Card (CAC) support**. Public Key Infrastructure (PKI) certificates enable employees to "sign" documents digitally; encrypt and decrypt email messages; and establish secure online network connections.
- **Certification and validations**. Knox meets the requirements for Federal Information Processing Standards (FIPS) 140-2 Level 1 certification for both data at rest (DAR) and data in transit (DIT).
- **Defense Information Systems Agency (DISA) MOS SRG compliance**. On May 2, 2013, DISA approved the Security Technical Implementation Guide (STIG)for Samsung Knox drafted for the Mobile Operating System Security Requirements Guide (MOS SRG).
- **Common Criteria**. The Common Criteria for Information Technology Security Evaluation, commonly referred to as Common Criteria, is an internationally recognized standard for defining security objectives of information technology products and for evaluating vendor compliance with these objectives. A number of governments use Common Criteria as the basis for their own certification schemes. Select Samsung Galaxy® devices with Knox embedded received Common Criteria certification.

Experience Samsung Knox on America's largest and most reliable 4G LTE network.

Choosing the right mobile device operating system and finding the right provider are equally important. Samsung Knox and the Verizon Wireless 4G LTE network can help businesses in regulated industries leverage mobility to increase productivity, enhance communication and promote collaboration.

Note: For the most recent updates to Samsung Knox certifications, see the following link: **https://www. samsungknox. com/en/security-certifications**

Learn more.

To learn more about Samsung mobile solutions for regulated industries, contact your Verizon Wireless business specialist, or visit us at **Enterprise.Verizon.com/ contact-us.**

Samsung and Verizon 4G LTE: reinventing security for Android devices.

- Encryption
- Access
- Control