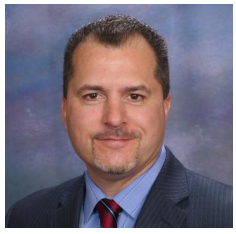
the Viewpoint mobility

Going mobile: How to boost productivity and data integrity

Q What are the essential ingredients of a mobile security program?

A An effective mobile security program combines strategy, architecture, technology, policy and people to ensure security at every stage — from design to daily implementation. An enterprise strategy should encompass mobility and security to maintain an acute level of awareness of the mobile environment and take control of it. Technical architecture should be designed to enable the business vision. Architecture and business strategy are then enabled through technology, including the mobile device management systems, app stores, cloud/server processing, secure end point devices and security auditing capabilities. To secure this technology, enterprises must establish a security policy, something that Samsung and its ecosystem of partners support 'out of the box.'



Johnny Overcast, Director Government Sales, Samsung

Q Is it possible to enable employees to access both agency and personal resources on one device without compromising the security?

A Yes, Samsung Knox provides the ability to have a secure workspace container that totally secures and cordons off government enterprise applications and protects from malicious attacks and data leakage. Government employees can use the 'personal' side of the device as they wish without fear of altering the Samsung Knox container and its applications or content. Integrity of agency data is protected no matter how the device is used. With Samsung Knox, agencies have the technology to enable a Bring Your Own Device model or allow for personal use on government-owned devices.

Q What tools are available to help government customers that have custom mobile program requirements?

A Samsung has a broad ecosystem of mobile solutions providers, and we have provided them with industry leading Software Developer Kits (SDKs) and various levels of developer support from our enterprise technical teams and R&D labs to enable unique and highly customized use cases. One example is our support of the PM Nett Warrior program. The U.S. Army uses the Galaxy Note line of smartphones as part of a solution that provides situational awareness for the warfighter. Through the Samsung Solutions Exchange, we work with mobile solution providers to enable unique and highly customized solutions on Samsung devices.

Q What mobile security controls do the various government certifications address and why are they important?

A Government certifications are important because they provide assurance that certain aspects of security are being performed correctly. FIPS certifications address the strength of encryption solutions—the algorithms, key lengths, and implementations of the algorithms. The Mobile Device Fundamental Protection Profile (MDFPP) under the 26-country Common Criteria program addresses the robustness of security functions on mobile devices. The Virtual Private Network Protection Profile (VPNPP), also under Common Criteria, addresses the security of how VPN tunnels between the mobile device and enterprise are established, executed and torn down. The Department of Defense Security Technical Information Guide (STIG) is an annex to the National Information Assurance Partnership's protection profile, and describes how users and IT departments should configure the capabilities to operate securely. Samsung mobile devices comply with FIPS 140-2, MDFPP, VNPP and STIG requirements.

Q To what extent can mobile solutions be integrated with the traditional work environment?

A There are several ways to consider wireless integration in the traditional work environment, or in the place of the traditional work environment. Within a more traditional office space, most of the products and tools available today are already connected or can be connected wirelessly. Wireless and mobile technologies can be integrated further into the workplace by leveraging capabilities that connect them to printers, displays and other IT products. Samsung is innovating in this arena at a tremendous pace, for example, providing the ability for mobile devices to connect via Near Field Communication (NFC) to our displays and other IT products.