SPONSORED CONTENT

FCW

AN INTERVIEW WITH

Keith Fuentes
Vice President
Samsung KNOX

Mobile Security: Agency Workers on the Move

The proliferation of mobile devices has changed the modern workplace. Employees can stay fully engaged and connected no matter where they're working. However, supporting a seamless mobile workforce requires enterprise-grade mobile security. Keith Fuentes, VP of Samsung KNOX, tells FCW how advanced mobile security technology, and the processes to match, can pay off in increased employee productivity, cost savings and a truly secure mobile workforce.

Q What is driving the growth of mobile device usage in government agencies?

A Agencies are trying to increase productivity while decreasing costs. Mobile devices can achieve both of these goals by allowing employees to work out of the office, and by being more affordable than most other mobile-workstation solutions.

Q What are the trade-offs between maintaining security and providing comprehensive access?

A Conventional wisdom says that you can't have increased mobile employee productivity without sacrificing security. However, Samsung is bucking that trend with built in defense-grade, hardware security throughout its mobile solutions. Samsung KNOX safeguards mobile platform security without sacrificing user productivity. It delivers security and privacy across Samsung's Galaxy mobile devices throughout the digital workplace.

Q What sort of regulatory compliance issues govern mobile devices?

A There are a few that are considered standard. The first one is through National Institute of Standards and Technology (NIST). That's called FIPS certification (Federal Information Processing Standards). It is a must for regulatory compliance if you're doing any type of encryption.

The second one is NIAP (National Information Assurance Partnership). NIAP looks at the hardware and software to make sure it's compliant. For mobile devices, NIAP has what's called Mobile Device Fundamental Protection Profile (MDFPP). Samsung spares no expense in getting NIST and NIAP certifications.

The third level consists of the STIGs (Security Technical Implementation Guides) from the DoD. STIGs tell you exactly how to configure specific products.

Q How do you best protect the primary networks from attacks that may enter through mobile device or endpoints?

A You need security technology that starts at the hardware layer up, and ensures the device has never been rooted. Samsung KNOX protects the device every time it boots up or comes off standby, and it's always monitoring the hardware, the software and OS.

Q How do you involve your mobile users in security practices and protocols?

A The first and most important thing is to avoid cumbersome security practices. You don't want to stifle user productivity with security practices that conflict with their modern style of working.

Secondarily user education remains important as security accountability remains users' responsibility in people-centric security practices.

Q How should government agencies prepare to address mobile devices beyond smartphones and tablets?

A Smartphones and tablets are just the beginning. For instance, Samsung is looking at how we can use our Samsung Gear watch—the Gear S2—not only in the workplace, but with soldiers and first responders.

The Gear S2 can become your office badge, or another form of ID. It can also monitor heart rate and other medical parameters that could provide live saving, real-time information for military and public safety professionals. We have already started adding KNOX components to our wearable devices.

Q How can agencies streamline deploying devices to mobile workers?

A Many professionals have a tablet and a phone, and some carry multiple phones. Samsung has built devices with capabilities for mobile enrollment, bulk enrollment and custom configuration. This allows agencies to establish a mobile device master gold image, virtually configuring the device with a customized look and feel upon initial connection to any Wi-Fi connection—saving a ton of man hours.