SPONSORED CONTENT

GCN

AN INTERVIEW WITH

Keith Fuentes
Vice President
Samsung KNOX

Mobile Security: Agency Workers on the Move

The prevalence 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 GCN 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 components must any mobile security program include?

A First and foremost, there must be some type of central management. You want options, and the ability to customize and set policies. With our KNOX solution, we've come up with a very agnostic approach that can be managed with every major mobile device manager to provide the most security enforceable policies in the market.

The second component involves the client side—how secure the device is when it's in the hands of the users and outside the brick and mortar office. Samsung KNOX is built in at the hardware level, so device managers know they can trust that the devices are secure wherever they are. Security needs to be certified and proven. Encryption, VPNs, firewalls, and data/application isolation are a must.

Q Are there any limitations agencies should impose on access to agency networks and data for their mobile users?

A They need to have a mitigated risk program, depending on user roles and type of data and networks being accessed. Certified VPNs and data encryption must be enforced 100 percent of the time. Through endpoints and access points, someone could imitate your device and pretend to be you. That's a very dangerous scenario. Therefore, mobile devices must be secured while connected to agency networks and equally important, they must have integrity monitoring to ensure they are safe before connecting to the network. Samsung devices have a hardware based root of trust and real time integrity monitoring below the operating system.

Q Are mobile devices a necessity or a luxury for agency workers and why?

A They are a necessity. Mobile devices increase productivity, and help reduce costs, because they allow work to get done from just about anywhere. They can even save lives. It's as simple as that.

Q Is there any single greatest risk to having mobile devices accessing agency networks?

A Organizations can sometimes be like people who tend to wait to act until they're bitten—even if they heard the approaching dogs' bark over and over again. When it comes to mobile device security, you have to protect against something the second you realize it's a threat.

What's more, there are a lot of weapons out there today that can hit you without you even knowing it—so be proactive in developing protocols and solutions that exceeds that threat.

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

A t the baseline, there shouldn't be any difference—the same fundamental principles apply when looking at mobile device security. Any type of device that has storage, network connectivity and data transmission requires security.

Of course, there are some minor differences. State and local agencies may have their own unique regulatory standards. You can take solutions certified for federal use and reconfigure those for usage at the state agency level.

The biggest difference is that federal agencies get involved in international situations. From an MDM standpoint, that means being conscious of the different carriers, and their own rules. Samsung is working with 97 carriers around the world to come up with security parameters.

How can agencies streamline deploying devices to mobile workers?

A Samsung has built devices with capabilities for mobile enrollment, bulk enrollment, and custom configuration. When the phone powers on, it immediately pulls that profile down and configures the device—saving a ton of man hours.