Mobility Management Makes Government Work: Security, Management and Control

Increased security spending creates new opportunities in always-connected world
INTRODUCTION

As the world moves to an always-on, always-connected paradigm, government agencies are embracing the idea of equipping their employees with mobile devices, services, and applications. In doing so, they recognize that giving workers access to people and information from anywhere—whenever they need it—boosts productivity, drives collaboration, and improves outcomes.

A global Frost & Sullivan survey of 160 IT decision makers in the government sector reveals that the biggest challenge facing government organizations is making effective and timely investments in IT. But they recognize the value of mobile devices in the workplace: almost two-thirds report allowing employees to use smart phones for work purposes, and more than half say tablets also are regularly used.

Still, our survey respondents rightly expressed concerns over mobile technology. Deliberate attacks—whether through malware, crime, or espionage—are the most feared security risks. Mobile apps and services, as well as the Bring-Your-Own-Technology (BYOT) trend, are most concerning to these IT executives, who worry about what they might introduce to their networks and devices. And, of course, those who work in defense and other highly sensitive or classified areas have even stronger concerns around data management and protection.

"Government spending on computers and other IT technologies is gaining share as the sector shifts from traditional command-and-control technologies that utilize proprietary technology to products and services that use industry standards, and are less costly to develop and implement."

Government agencies that want to see value from their mobility initiatives and investments must put security and management first. But they must balance that with the need to create a program that is convenient for both end users and IT staff. That way, government can, with the utmost confidence, get beyond security concerns and utilize mobile devices for various line-of-business use cases, ranging from field service and logistics, to law enforcement and tactical military deployments.

This paper will address the criteria they should consider, including a robust enterprise mobility management solution that builds on basic MDM and offers end-to-end security from the device to the network; defense-grade security, including the certifications that meet those requirements; and a centralized system for efficiency and management to ensure any mobile rollout is not just secure, but also effective.

TREND WATCH: CLEAR BENEFITS IN A MOBILE WORKPLACE

With more than half of all employees working away from a traditional office, there can be no denying that the workplace has gone mobile. This is as true for government organizations as it is for enterprises: Frost & Sullivan research shows that within government organizations, 20% of employees work from small satellite offices (some quite remote), more than 13% are mobile workers, and nearly 25% work full time or part time from home.
Within Government Organizations

- 20% Employees work from small satellite offices
- 13% Employees are mobile workers
- 25% Employees work full time or part time from home

Mobile devices such as tablets and smartphones enable always-on connectivity and boost productivity in ways that employees expect to help them better perform their jobs. Frost & Sullivan research demonstrates how pervasive mobile is becoming:

- Almost three out of every four government organizations issue smartphones to at least some employees; more than half deploy tablets.

- Android has taken a strong lead as the most common mobile operating system supported for government-owned devices.

- Half of all government agencies have a BYOT policy in place. Two thirds enforce those policies with network technologies, 41% use mobile device management, and 24% use mobile workspace management tools.

Half of all Government Agencies Have a BYOT Policy in Place

- 2/3 Enforce those policies with network technologies
- 41% Use mobile device management
- 24% Use mobile workspace management tools
The government use cases for mobile devices and apps are almost endless:

They can transform *citizen-facing services* by allowing employees to meet customers wherever they “live,” processing forms, taking electronic payments, and sharing information on site.

They can improve repair times and other productivity measures for in-field service and support, whether employees are conducting fleet management, regulatory checks, or general maintenance tasks.

They can boost *workforce management* by allowing managers to leverage real-time data to make staffing decisions, improve communications within and across teams, and analyze data to optimize successful outcomes.

*Deployed military personnel, law enforcement*, and similar agencies can use tablets and smartphones to gather and analyze data on their colleagues’ positions, as well as track the enemy, criminals, suspects, and other people of interest; leverage GPS and other location-based services while on patrol or in the field; communicate with superiors located well behind enemy lines or off the street; and record encounters for verification and validation as needed in the future.

---

Frost & Sullivan research shows that short-term spending on communications in the government sector will rise sharply as commercial technologies like cloud computing and collaboration software are integrated. It is expected to reach $23.4 billion by the end of 2016.

---

**KEY CONSIDERATIONS FOR MOBILITY IN THE GOVERNMENT**

For all their benefits in enabling a virtual workplace, mobile devices, which for the purposes of this paper are defined as smartphones and tablets, pose different risks than traditional PCs—including laptops, which almost 80% of government agencies also deploy. For instance, some Internet-based application stores act as conduits for malware; when a user downloads a mobile app, the mobile device, the OS, and the application store are so tightly connected that they act almost as one entity. As a result, almost by definition mobile-device security also must include application and network security. And since malicious or compromised applications are the most significant point of attack for mobile devices, application and application-store management are especially important.

---

As commercial wireless networks, mobility, cloud computing, social networking, data analysis, applications, and high-level encryption technology become more widespread, the use of commercial mobile devices by government organizations will become routine at all levels and for all functions.

---
Depending on their role, some government organizations must use a partner with defense-grade security, which typically requires specific certifications. These agencies must of course do their due diligence to ensure the vendor has those certifications, and will stay up to date on any and all of them—as well as achieve new ones as needed.

Finally, it is critical to remember that a well-thought-out security strategy enables productivity. When mobile security is seamless to the user, stronger than ever, and easily managed by the IT department, mobile employees can have access to apps and services that previously would have been blocked. That, in turn, can boost productivity and enable new functionality, improving outcomes for government agencies and the citizens they serve.

**Samsung Knox—a Variety of Options to Suit Every Organization**

Samsung’s flagship security offering, Knox, is available in multiple flavors to suit almost any organization’s needs.

- **Knox Express** is a free, cloud-based solution that offers quick and easy setup, compartmentalization for corporate and personal data, and a user portal, so that employees can take responsibility for their own mobile device management.

- **Knox Premium** is an end-to-end solution that lets IT administrators manage devices with a cloud-based console and offers an on-device secure workspace. It supports the separation of corporate and personal data, multi-layered device protection, and support for flexible add-ons such as rich IT policies and unlimited single-sign on capabilities.

- **Knox Workspace** is an on-device security offering that’s secure enough to run on a government-grade network. It supports two-factor identification; powerful-but-protected apps such as Contacts, Calendar, Camera, and Email; and integration with existing MDM, VPN, and Microsoft Exchange ActiveSync.

- Finally, **My Knox** helps employees who want or need to comply with their company’s security policies on their personal devices.

For more information, please visit [www.samsung.com/us/knox](http://www.samsung.com/us/knox)

**GOOD HYGIENE PRACTICES FOR ANDROID DEVICES**

According to Frost & Sullivan Stratecast’s report, “*Hardening* Android: Building Security into the Core of Mobile Devices”, mobile security hygiene should be any organization’s first step when it comes to preventing threats. Security professionals need to be especially vigilant when it comes to controlling and monitoring Android-based devices that are accessing government data, apps, and networks. And employees should be made aware of the potential problems created by downloading apps and content from public marketplaces.

---

1 “Hardening” Android: Building Security into the Core of Mobile Devices by Frank Dickson, SN 2-04, frost.com
But implementing good security hygiene will only go so far. Even the best tools can’t eliminate the so-called “human factor”; users still remain the weakest link in any security arena. Since the devices are inherently portable, the risk of physical attacks is greater, making hardware protections even more critical. As a result, forward-thinking organizations are implementing measures that harden the Android OS by using security embedded in semiconductors to go beyond traditional network or software solutions. The result makes mobile devices much more secure from end to end.

A critical component of hardened Android-based systems is a root of trust. Roots of trust are software components that are trusted and secure by design, which makes them ideally implemented in specific hardware endpoints like tablets and smartphones. In general, roots of trust perform one or more of the following functions:

- Measure or verify software, ideally in boot-and-launch environments;
- Protect cryptographic keys; or
- Perform device authentication.

Roots of trust are not new, but mobile devices present unique challenges because they are inherently open systems, with multiple processors and interfaces to protect, including central processing units (CPUs), baseband radio, near-field communication (NFC), multiple cellular technologies, Wi-Fi, and Bluetooth. Additionally, power and space constraints force the sharing of system resources, such as processing and memory.

Essentially, a root of trust provides a “known good” position to assess the integrity of the mobile device, its OS, and its components. The root then enables a secure comparison of software during the boot-and-launch sequences to known good software components, preventing the launching of unrecognized software and enforcing known good software configurations. After a root of trust and a known good condition is established, security verification is extended to other components of the system.

For Android devices, the root of trust should provide a cryptographically protected identifier for each approved software component, and then provide hardware enforcement mechanisms to block software that cannot be verified. Specifically, the root of trust and associated security component should provide the following services:

- **Boot firmware protection:** Protects and isolates the boot firmware from being accessed by the system. This functionality is ideally “hardwired” in the mobile processor, unable to be accessed by the user.

- **Validated system boot:** Verifies and enables a known good state. System changes are detected through cryptographic measurements.

- **Application control:** Creates and implements enforceable lists of “known good,” or approved, software, application, and executable code.

- **Secure storage:** Includes trace data protection, which removes residual data at an improper shutdown, protecting against memory-snooping software and reset attacks. Trace data protection is implemented in hardware.

- **Attestation:** Validates platform credentials to complete the trust verification process and support compliance.
For Android devices, a root of trust and associated security component should provide:

- **Boot Firmware Protection**
- **Validated System Boot**
- **Application Control**
- **Secure Storage**
- **Attestation**

**WHAT TO LOOK FOR IN A SECURITY PARTNER**

Government agencies spend about 15% of their IT budgets on mobile devices and applications and another 20% on network security. It stands to reason that they make those investments carefully, and they should choose their mobile security partner(s) with consideration.

Mobile security services should include:

- **Anti-virus**: An integrated or built-in technology that will proactively prevent malware from being installed and provide ongoing protection against potentially harmful applications and malware.

- **Content filtering**: Filter traffic from known malicious Web hosts.

- **Call and message filtering**: Block unwanted calls and short message service (SMS) and multimedia messaging service (MMS) communications.

- **Remote wipe and lock**: Users or administrators can remotely erase data or lock a mobile device that is lost or stolen.

- **Anti-loss and anti-theft**: Remotely locate a lost or stolen mobile device.

- **Content controls**: Monitor and limit user access to websites, messaging and calls based on location, time, or content maturity level.

- **Mobile Virtual Private Network (VPN)**: Enable secure VPN connections and session persistence over wireless and mobile networks.

- **Encryption**: Secure files and any data exchanged on the device.

- **Application reputation scanning**: Identify common risks, such as access to privacy settings, insecure network connections, and malicious code.
• **Jailbreak and root detection:** Provide protection through application wrapping or software development kit integration.

• **Enterprise app store:** Give employees easy access to company-approved public and custom-built internal applications.

• **Mobile device management:** Address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console.

### When BYOT Goes Bad

Most organizations have a BYOT policy in place, but most are not terribly good at enforcement. Government agencies that forbid the use of personal devices for work purposes have their work cut out for them when it comes to ensuring that employees are following the rules. Businesses and other organizations report that the use of unauthorized mobile apps is a growing problem, but they are at a loss about what to do about it.

The issue is not negligible. When employees use their own devices and consumer apps for work, they are putting the entire organization at risk. They may not be aware of the malware threats posed by app stores or take the necessary precautions to protect data and intellectual property. Depending on their use, they may not be projecting a professional image (if, for instance, their app pops up a photo grabbed from Facebook rather than the corporate logo). And when they leave the organization, so does everything they’ve used on their phone or tablet.

One solution is to deploy mobile devices to all employees who might currently be using their personal smartphones or tablets at work. Although this comes with a cost (for devices, apps, and support), that cost can pale in comparison to the “hidden” costs of a BYOT program—which include ad-hoc support services (which often take up way too much IT time), security risks and encroachments (which reduce productivity and put the larger business at risk), lost intellectual property (including client and partner contacts, which, if on a personal device, go with an employee when he leaves), and opportunity costs (such as a lost deal or negotiation, if the necessary employees don’t have access to information and communications when they need it). By taking control of mobile devices and apps, government agencies ensure that all data is secure and that all regulatory requirements are met.

### CONCLUSION

Like their enterprise counterparts, government agencies are embracing the need to support an increasingly mobile workforce by purchasing and supporting a range of devices, apps, and services for their end users. But many government organizations have strict security and control requirements, making mobile device management even more of a challenge than it is for private businesses.

Some of the biggest risks around smartphones and tablets are introduced by users, who often unknowingly download malware along with the apps and services they need to use for business and pleasure. Frost & Sullivan strongly recommends, therefore, that government agencies pay extra close attention to mobile security, including anti-malware, content filtering, remote wipe and lock, anti-loss and anti-theft, VPN, and encryption.
Ideally, that security should be literally built into the device, making for seamless protection end to end. And it should deliver a platform that is easy to use and manage, so that employees and IT staff can focus on the goals of the organization, using their devices to improve outcomes without having to worry about threats to the hardware, software, data, or network.

By embracing a hardened, holistic security approach, government agencies can support their growing population of remote and mobile workers, allowing them the freedom and flexibility to work from anywhere, collaborate with anyone, and leverage Big Data and the Internet of Things to deliver better outcomes for themselves and their constituents.

**Employee Use of Unauthorized Mobile Apps as a Problem: NA, 2014 and 2015**

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't Know</td>
<td>70%</td>
<td>60%</td>
</tr>
<tr>
<td>Yes</td>
<td>26%</td>
<td>36%</td>
</tr>
<tr>
<td>No</td>
<td>4%</td>
<td>4%</td>
</tr>
</tbody>
</table>
Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041