FROST & SULLIVAN

Governments Embrace the Mobile Workplace

An increasingly mobile workforce requires that government agencies give their employees mobile devices, services and apps.

WITHIN GOVERNMENT ORGANIZATIONS

20% of employees work from small satellite offices

More than **13%** are mobile workers

Nearly **25%** work full time or part time from home

66% allow employees to use smartphones for work purposes

50% allow regular tablet use

IT DECISION MAKERS IN GOVERNMENT ARE CONCERNED ABOUT

Business Alignment
The biggest challenge facing government agencies is making effective and timely investments in IT

Deliberate Attacks
Malware, crime and espionage are most feared security risks

Mobile Apps, Services and BYOT
The most important issues facing mobility managers

Defense and Highly Classified
Those working in highly sensitive areas have even stronger concerns around data management and protection

GOVERNMENTS DEPLOY MOBILE APPLICATIONS FOR THEIR EMPLOYEES

75% of government organizations issue smart phones

Android is the most common OS supported for government owned devices

15% of Government agencies' IT budgets are allocated to mobile devices and applications

20% of Government agencies' IT budgets are allocated to network security

50% of all government agencies have a BYOT policy in place

66% enforce those policies with network technologies

41% use mobile device management

24% use mobile workspace management tools

USE CASES

Transform citizen-facing services by allowing employees to meet citizens wherever they live

Office | Virtually | Home

Improve repair times and other productivity measures for in-field service and support

Fleet Management | Regulatory Checks | General Maintenance Tasks

Boost workforce management

Leverage real-time data to make staffing decisions → Improve team communications → Analyze data to optimize successful outcomes

Deployed military personnel and law enforcement:

Gather and analyze data on their colleagues' positions

Track the enemy, criminals and suspects

Leverage location-based services while in the field

Communicate with superiors in the office or behind enemy lines

Record encounters for verification and validation

GOOD HYGIENE PRACTICES FOR ANDROID DEVICES

Mobile devices present unique challenges

Central processing units (CPUs) | Baseband radio | Near-field communication (NFC) | Cellular technologies | Wi-Fi and Bluetooth

Use Roots of Trust to perform one or more of the following

Measure/verify software, ideally in boot-and-launch environments

Protect cryptographic keys

Perform device authentication

Look for the following features in a mobile security solution:

Boot Firmware Protection
Protects and isolates the boot firmware from being accessed by the system. Ideally "hardwired" into the mobile processor.

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, code.

Secure Storage
Includes trace data protection in hardware, protecting against memory-snooping software and reset attacks.

Attestation
Validates platform credentials to complete the trust verification process and support compliance.

MOBILE SECURITY SERVICES SHOULD INCLUDE:

ANTI-VIRUS

CONTENT FILTERING

CALL AND MESSAGE FILTERING

REMOTE WIPE AND LOCK

ANTI-LOSS AND ANTI-THEFT

CONTENT CONTROLS

MOBILE VIRTUAL PRIVATE NETWORK (VPN)

ENCRYPTION

APPLICATION REPUTATION SCANNING

JAILBREAK AND ROOT DETECTION

ENTERPRISE APP STORE

MOBILE DEVICE MANAGEMENT

CLICK HERE TO DOWNLOAD THE WHITE PAPER:
"MOBILITY MANAGEMENT MAKES GOVERNMENT WORK: SECURITY, MANAGEMENT AND CONTROL"

BLOG
insights.samsung.com

TWITTER
@SamsungBizUSA

WEBSITE
www.samsung.com/government

SOURCE
Frost & Sullivan research

FROST & SULLIVAN

SAMSUNG