

agencies give their employees mobile devices, services and apps.

20% of employees

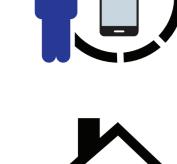
ORGANIZATIONS

WITHIN GOVERNMENT



satellite offices More than 13%

work from small



are mobile workers



time from home

Nearly 25% work

full time or part



50% allow regular

66% allow employees

to use smartphones

for work purposes



Business Alignment The biggest challenge facing government

GOVERNMENT ARE CONCERNED

IT DECISION MAKERS IN



ABOUT

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



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

Highly Classified

GOVERNMENTS DEPLOY MOBILE APPLICATIONS FOR THEIR EMPLOYEES Android is the most common OS supported

smart phones for government owned devices

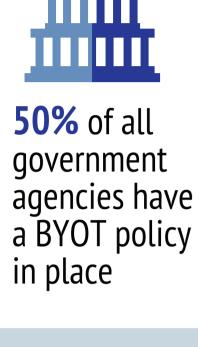


15% of Government agencies' IT budgets are allocated to mobile devices and applications



agencies' IT budgets are allocated to network security

20% of Government



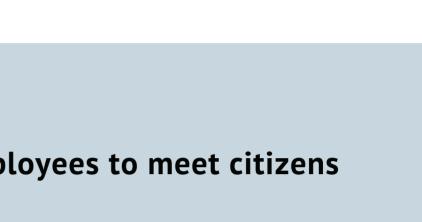
USE CASES

wherever they live

66% enforce those policies with network technologies







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







Improve team

communications

Regulatory Checks

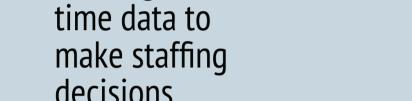
General Maintenance Tasks

Analyze data

to optimize

successful

outcomes



Fleet Management

Boost workforce management



Leverage real-

Gather and analyze data

on their

colleagues'



Leverage

locationbased services while in

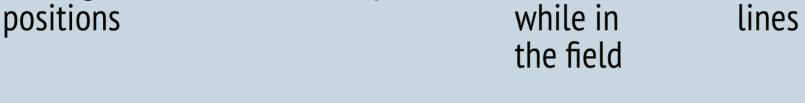


behind enemy

GOOD HYGIENE PRACTICES FOR ANDROID DEVICES



Record



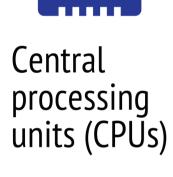
Track the

criminals

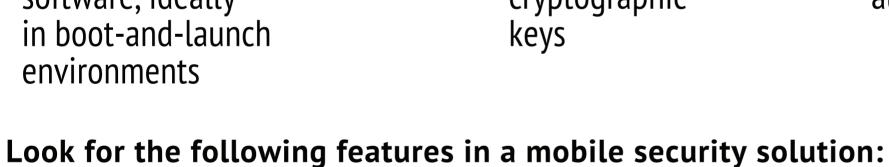
and suspects

enemy,

CPU



Measure/verify software, ideally





Mobile devices present unique challenges

Near-field

(NFC)

communication



Protect



Verifies and enables a known good state. System changes are detected

Includes trace data protection in hardware, protecting against memory-

Validates platform credentials to complete the trust verification

Cellular

technologies





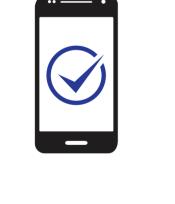
Wi-Fi and

Bluetooth

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

Validated System Boot

Boot Firmware Protection





Secure Storage

snooping software and reset attacks.

process and support compliance.

through cryptographic measurements.



ANTI-VIRUS

Attestation

CONTENT FILTERING

DENIED

REMOTE WIPE AND LOCK

CONTENT CONTROLS

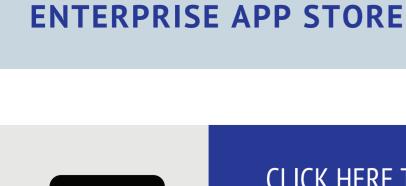


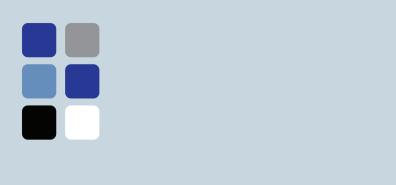
MOBILE VIRTUAL PRIVATE

NETWORK (VPN)

CALL AND MESSAGE FILTERING

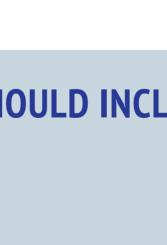


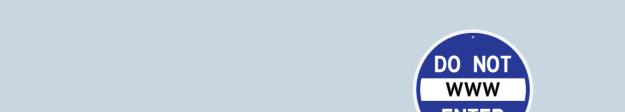




BLOG

insights.samsung.com







MOBILE DEVICE MANAGEMENT



Frost & Sullivan research

FROST

& SULLIVAN

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

TWITTER

@SamsungBizUSA

WEBSITE

www.samsung.com/government

SAMSUNG

tablet use

75% of government organizations issue









