Welcome to
CSO Perspectives

Dave Lowe, Vice President of Enterprise Sales

Samsung Telecommunications America

May 15, 2012

THE WALL STREET JOURNAL.

Tuesday, November 15, 2011

Debate: Should Employees Be Allowed to Use Their Own Devices for Work?

Yes: It Is Inevitable

“Fight it all you want, but employees are going to be bringing their own smartphones, tablets and other technology to work with them. So it's time to stop resisting and start preparing.”

Vs.

No: It's a Legal Mess

“This idea is so fraught with technical, operational, security and legal risks, and promises so little quantifiable in return, that something bad is bound to happen.”

CIO

Tues, March 06, 2012

The BYOD Sea Change Has Already Started

Trending Opportunity

“Enterprises may see cost savings as employees pay for their own devices in the brave new BYOD world, but that doesn't mean a free lunch for IT. This emerging trend only increases the pressure on IT to manage and secure devices and data.”

Trending Risk

“CIOs face many concerns, ranging from mobile device management to data security. Given the newness of the trend, as well as the relative immaturity of enterprise solutions, CIOs must find ways to tackle these challenges.”

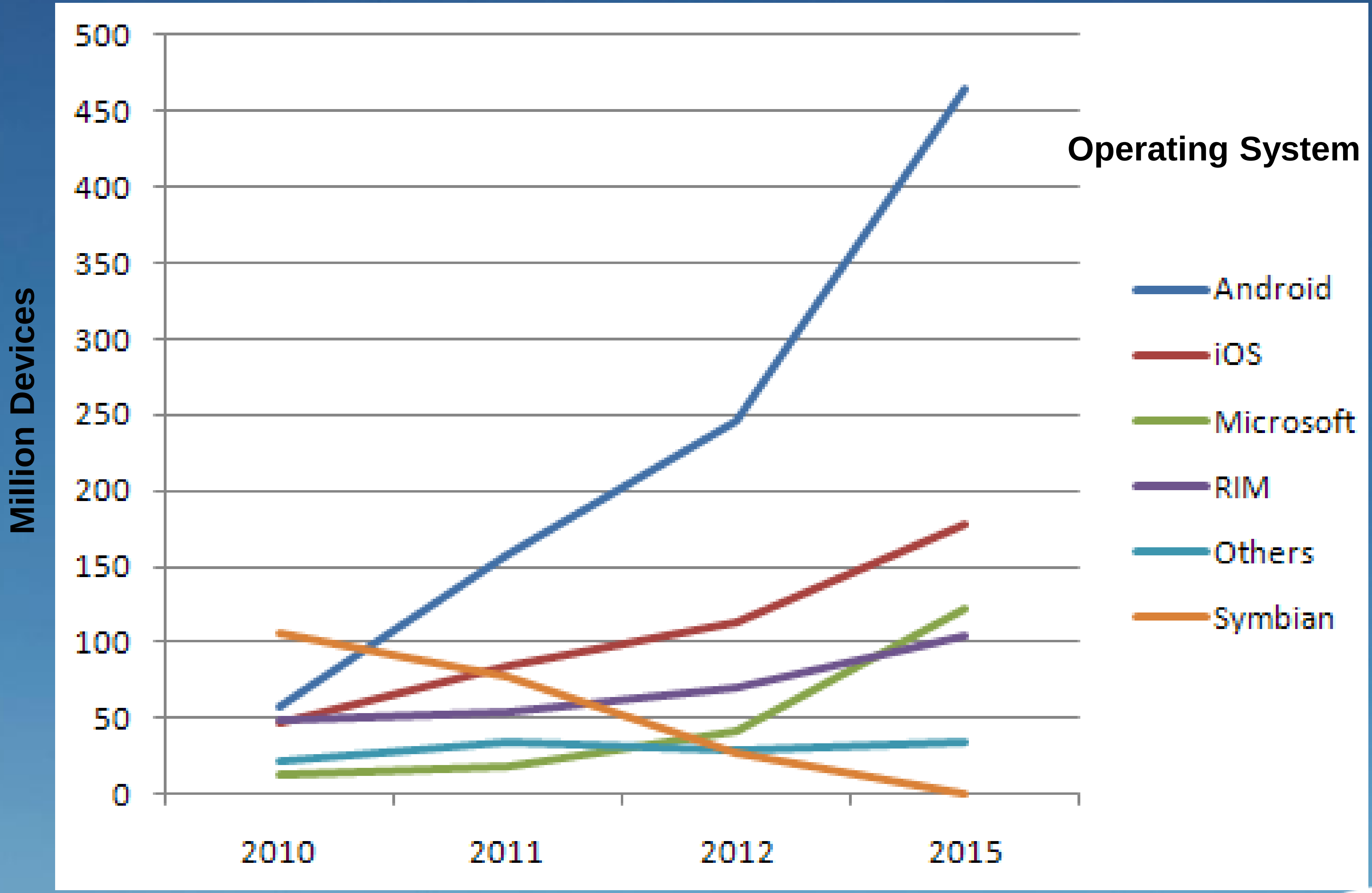
The BYOD Phenomena

- More than **80%** of employed American adults use a personally-owned device for work-related functions
- Of that 80 percent, **38%** are smartphones and **15%** are tablets
- **24%** of respondents use their smartphones to access or store company/employer information; **10%** use their tablets
- A recent survey showed that **two-thirds of businesses** that allow personal devices to be used at work do not have a formal policy in place to manage them

Source: Harris Interactive Feb. 2012

Smartphone OS Forecast

Android OS projected to grow 300% by 2015

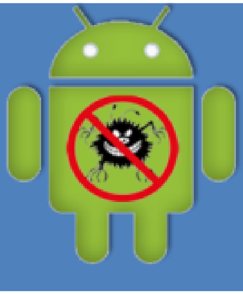


Source: VDC Research

Key Pillars for IT Compliance

- Mobile Device Management (MDM)
- On-Device Encryption (ODE)
- Virtual Private Network (VPN)
- Corporate Email Functionality (Microsoft Exchange Active-Sync)

MDM – 3 Critical Areas



Application Management

- Deploy and control the applications that run on Samsung Android devices
- Control access to the Android Market

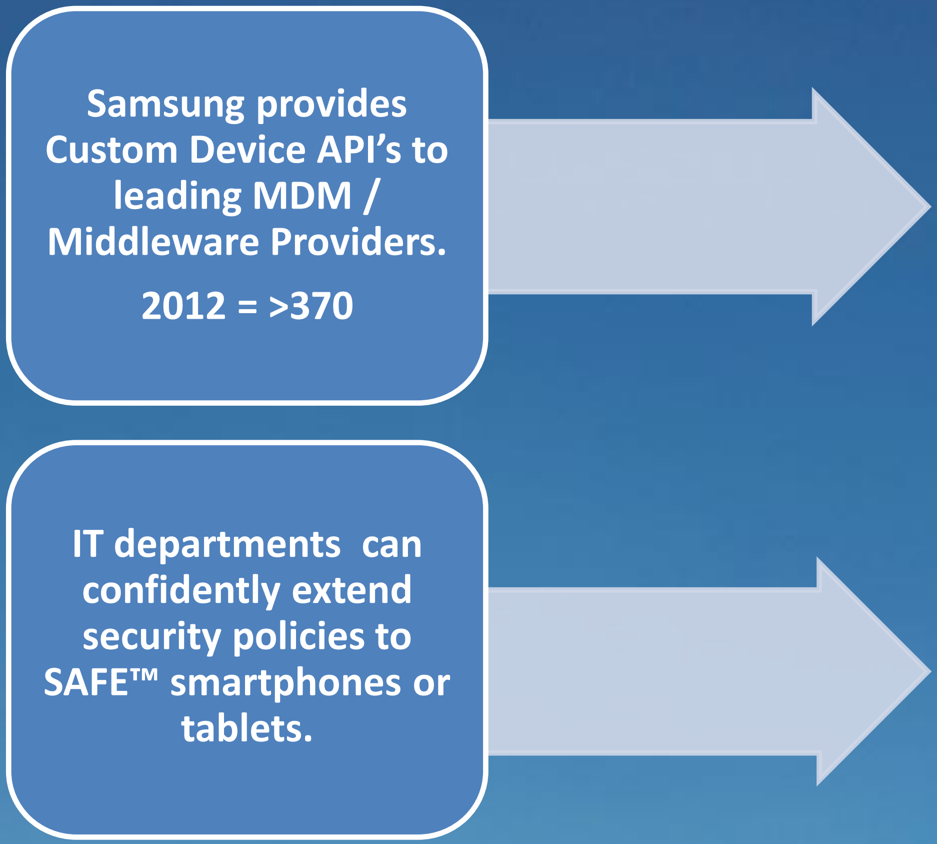
Configuration Management

- Provide control over various functions (Bluetooth®, WiFi®, camera, microphone), roaming, and network configuration
- Exchange Client Configuration – configure native email client

Security Management

- Enable password protection, on-device encryption, remote lock and wipe, and certificate installation
- Track Asset Usage – device info, network info, roaming restrictions, and more

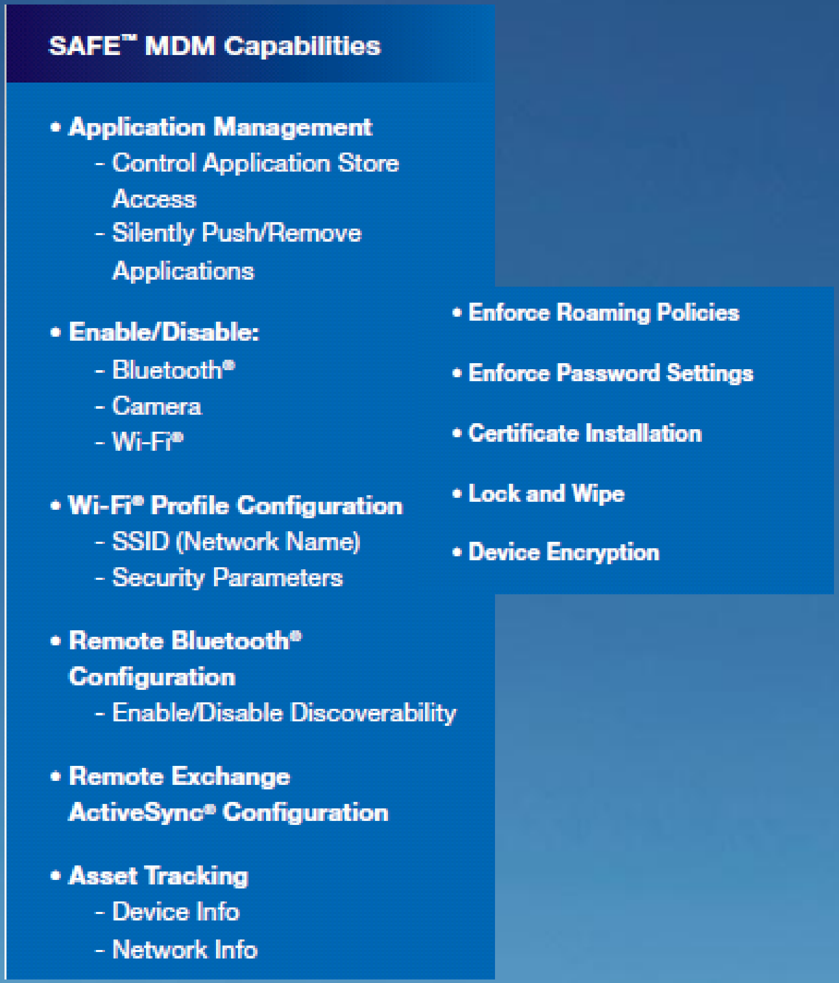
MDM



Samsung provides Custom Device API's to leading MDM / Middleware Providers.

2012 = >370

IT departments can confidently extend security policies to SAFE™ smartphones or tablets.



SAFE™ MDM Capabilities

- **Application Management**
  - Control Application Store Access
  - Silently Push/Remove Applications
- **Enable/Disable:**
  - Bluetooth®
  - Camera
  - Wi-Fi®
- **Wi-Fi® Profile Configuration**
  - SSID (Network Name)
  - Security Parameters
- **Remote Bluetooth® Configuration**
  - Enable/Disable Discoverability
- **Remote Exchange ActiveSync® Configuration**
- **Asset Tracking**
  - Device Info
  - Network Info
- **Enforce Roaming Policies**
- **Enforce Password Settings**
- **Certificate Installation**
- **Lock and Wipe**
- **Device Encryption**

On-Device Encryption & VPN Connectivity

On-Device Encryption

- Encrypts all data stored on device & SD card
- Enabled via EAS or MDM IT Policy
- Manually enabled on Android 3.X or higher
- AES-256 encryption
- Fast conversion & boot-up

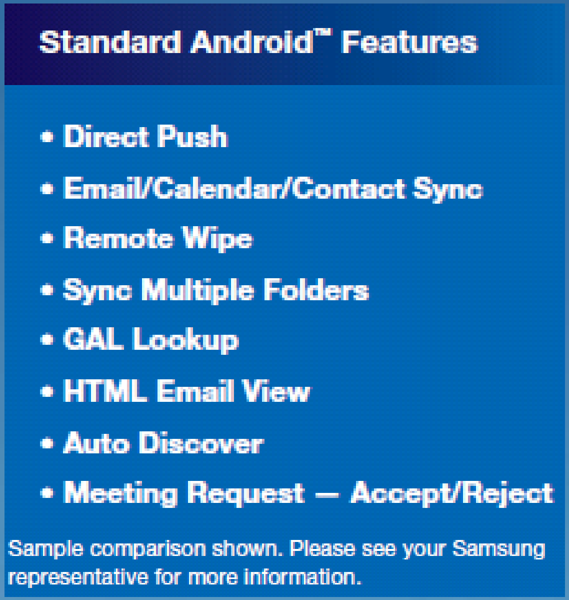
VPN Connectivity

- Support for the following clients:
  - Cisco® – SSL only (IPSec coming)
  - F5
  - Juniper – Junos Pulse Client

Corporate Email / Calendar / Contacts

95% of Exchange IT Policies are covered by SAFE™ devices

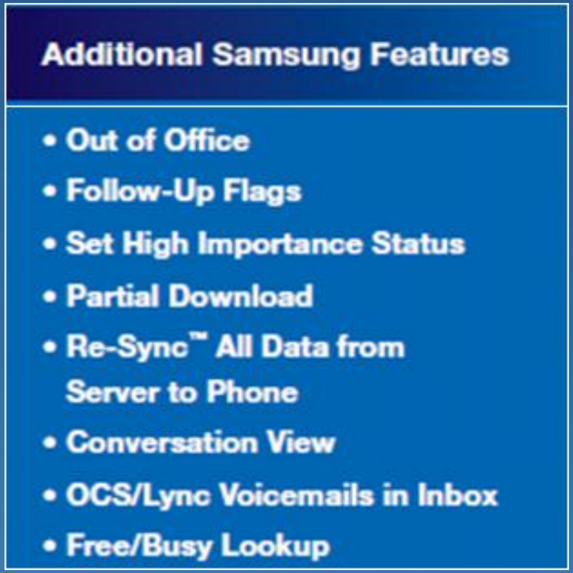
SAFE™ devices offer extensive support for communication systems such as Microsoft® Exchange ActiveSync® and extend beyond the native capabilities of standard smartphones and tablets.



Standard Android™ Features

- Direct Push
- Email/Calendar/Contact Sync
- Remote Wipe
- Sync Multiple Folders
- GAL Lookup
- HTML Email View
- Auto Discover
- Meeting Request – Accept/Reject

Sample comparison shown. Please see your Samsung representative for more information.



Additional Samsung Features

- Out of Office
- Follow-Up Flags
- Set High Importance Status
- Partial Download
- Re-Sync™ All Data from Server to Phone
- Conversation View
- OCS/Lync Voicemails in Inbox
- Free/Busy Lookup

This represents only a SMALL portion of the overall EAS feature set Samsung has implemented

Samsung B2B SAFE™ Program

Samsung & Third Party Accessories

Vertical Solutions

AIRSTRIP TECHNOLOGIES
Allscripts
DYKNOW
pyxis|mobile
voalté
EPOCRATES
Bb Blackboard
Mc Graw Hill
silanis

Healthcare, Education, Finance, Hospitality, Retail, Transportation, Etc

Horizontal Solutions

CiTRiX
webex
SAP
CHARGE Anywhere®
xora
vmware
ORACLE
salesforce.com Success On Demand
ANTENNA SOFTWARE
LogMeIn

IT Compliance

Microsoft Exchange ActiveSync
JUNIPer NETWORKS
SYBASE An SAP Company
CISCO
MobileIron
SOTI.net
airwatch
Good

Samsung Software

EAS

ODE

Horizontal Application Hooks:

MDM VPN Application Security

Samsung Smartphones & Tablets
Good, Better, Best Device Options at Each US Carrier

SAMSUNG

Samsung Approved For Enterprise

enhanced security, accessibility, flexibility and efficiency

Thank You!

Dave Lowe, Vice President of Enterprise Sales

Samsung Telecommunications America