

Mobile Security Trends

Michael Soto
Mobile Security Architect



Agenda

- About Me
- What's Happening? / Mobile Trends
- Enterprise Challenges
- Mobile Threats
- Mobile Awareness
- Mobile Security Technology

About Me

- Mobile Security Architect with FishNet Security
- 20+ Years of Enterprise IT Experience
- 4 Years of Enterprise Mobility Experience
- Work with SMB to Fortune 500
- Electrocuted twice with 10,000 volts



What's Happening?

- Apple
 - iOS 7
 - iOS 8
- Samsung
 - KNOX?
 - Tizen
- Google
 - KitKat



Samsung KNOX



What's Happening?

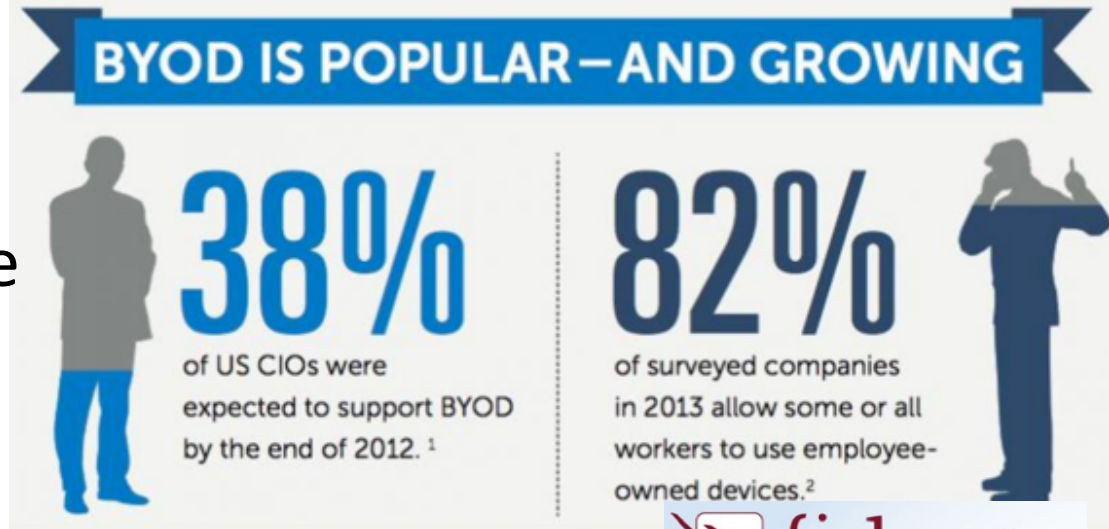
Market Leader Consolidation

- AirWatch
 - VMware (\$1.4B)
- MaaS 360
 - IBM (unknown)
- Zenprise
 - Citrix (undisclosed)



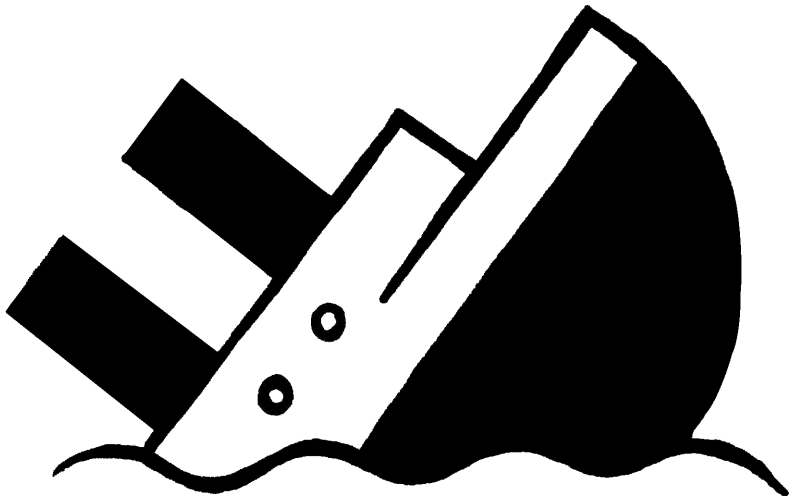
Mobile Trends

- Demand for “Any, Any, Any!”
- BYOD
- Productivity increase?
- Increased demand to resources
 - Public
 - Private
- Work/Life balance



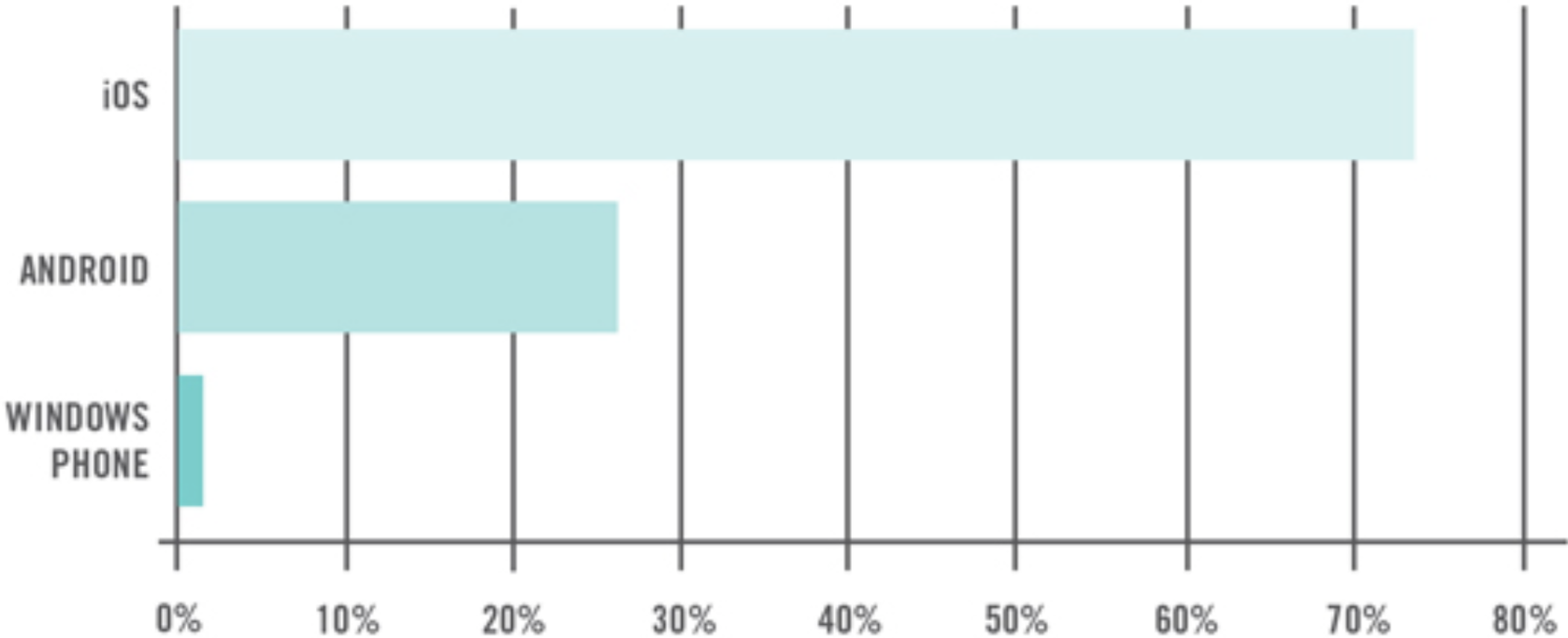
Mobile Trends

BlackBerry: It's a sinking ship!



- Significant installed base
- Widely viewed as the most secure mobile platform
- Tight integration between management components and devices
- No clear path forward for organizations relying on BB type security controls

Mobile Trends

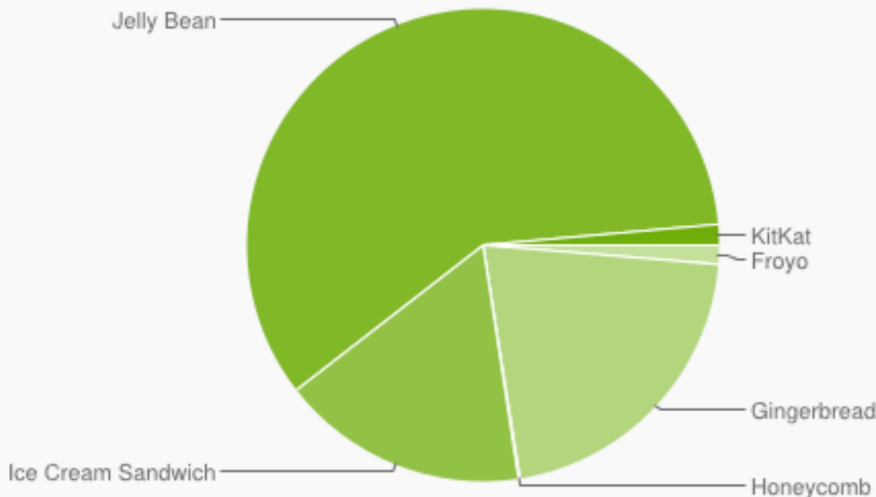


Device Activations Q4 2013



Mobile Trends

- **Android** – Choose your flavor!
 - Open Architecture
 - Over 80% on 4.x
 - Many Device Makers



4.4 - KitKat

- Distribution – 1.4%



4.1.x – 4.2.x – Jelly Bean

- Distribution – 59.1%



4.0.3 – 4.0.4 – Ice Cream Sandwich

- Distribution – 16.9%



3.2 - Honeycomb

- Distribution – 0.1%



2.3.3 – 2.3.7 - Gingerbread

- Distribution – 21.2%



2.2- Froyo

- Distribution 1.3%

Mobile Trends



What's improved?

Jelly Bean (4.2.2)

- App Encryption
- Always-on VPN
- ASLR
- Smart App Update
- Improved HTML5 Support
- JavaScript Engine (8)
- Multi-user

Jelly Bean (4.3)

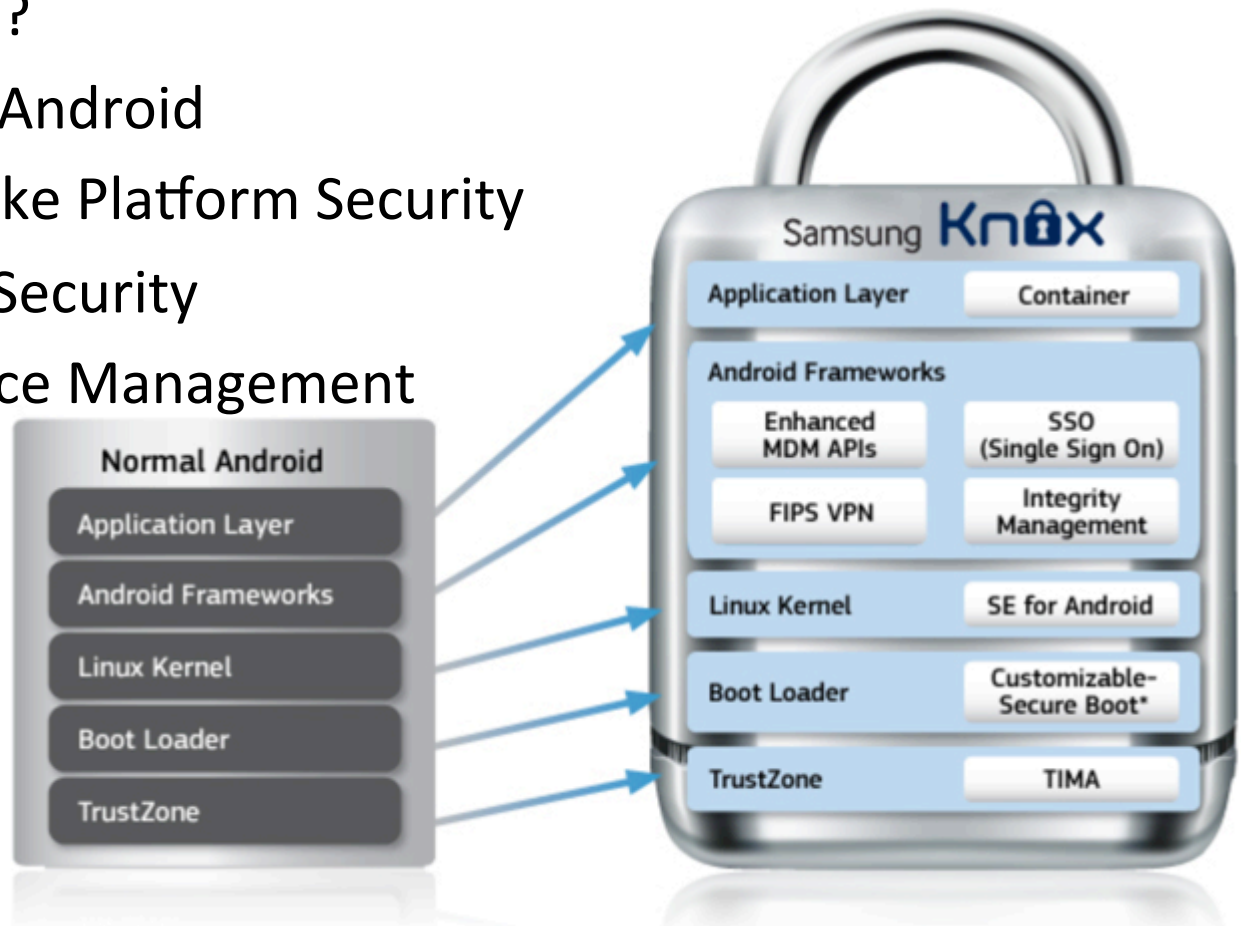
- Restricted Profiles
- Faster user Switching
- Additional Language Support



Mobile Trends

■ Samsung KNOX

- Most secure?
- SE Linux for Android
- BlackBerry like Platform Security
- Application Security
- Mobile Device Management



Mobile Trends

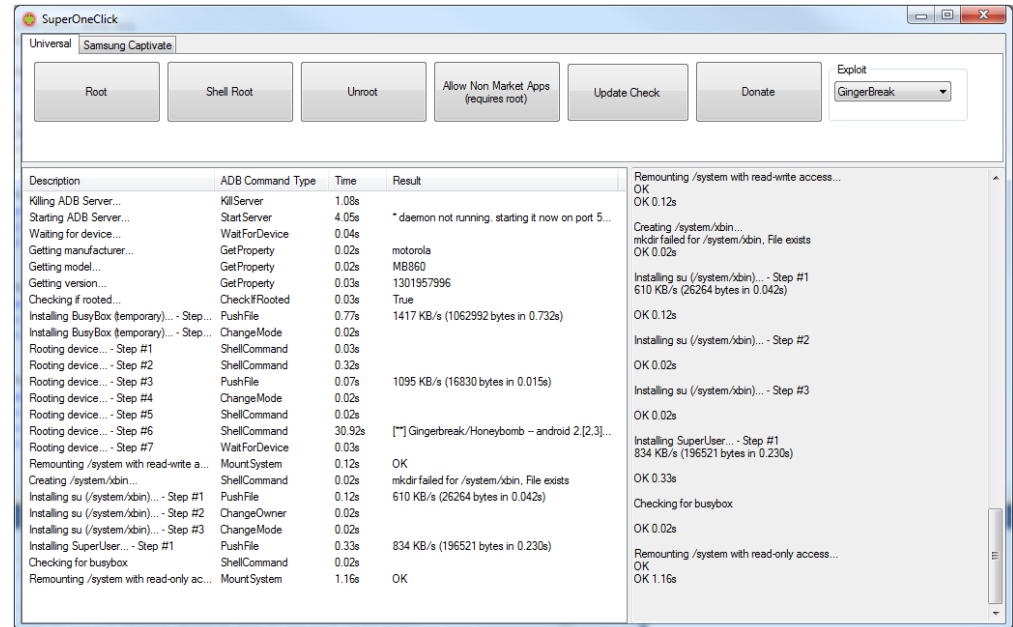
■ Android – Root

- Why Root?
 - Full OS control
 - Control manufacturer ‘bloatware’
 - Apply security patches
 - Free apps
 - Tethering

got root?

■ Common Roots

- SuperOneClick
- Unlock Root
- One Click Root
- Nexus Root Toolkit
- Various others..



Mobile Trends

Apple iOS (7)

- AirDrop
 - Ability to transfer files w/out email
- Control Center
 - Quick Access to Enable Airplane Mode
- Notification Center
 - Improved lock screen access
- Multitasking
 - Automatic scheduled syncing/refresh
- AppStore
 - Apps Auto-Update

Management Updates

- Prevent Apps Using Cellular Data
- Single Sign-On
- Silent Install
- Lost Mode



Mobile Trends



- iOS Security Updates

- Touch ID
 - Also raises additional concerns
- Data Protection for 3rd Party Applications
 - Accessible after first unlock
- Activation Lock
 - Require Credentials to Reset/Activate Device
- Managed Open-In
- Per-App VPN

- iCloud



- **Photo Sharing** – Share photos with people with shared photo streams.
- **Keychain** – Works with Safari to remember account names, passwords and credit card numbers. Can synchronize across supported devices. Secured with AES-256 bit encryption but resident in the cloud.



Mobile Trends

- Evasi0n
 - iOS 7.1
 - Others?





Enterprise Challenges

Enterprise Challenges



Enterprise Challenges



- Requirements
- What devices to support?
- Security challenges
 - Policies
 - Accessing corporate content
 - Loss/theft
- Human Resources – Privacy Concerns



Enterprise Challenges

- Data loss due to lost/stolen devices
- Data transmission to third parties
- Loss of data during employee separation / termination
- Regulatory / compliance requirements



Enterprise Challenges

- What are organizations doing?
 - Corporate Liable
 - Personal Liable (BYOD)
 - Hybrid
- Why BYOD?
 - Costs
 - Executive adoption
 - Work/Life Balance
 - Productivity



Enterprise Challenges

■ Additional Concerns

- Data stored in the cloud
 - Dropbox/Box.com/iCloud/Google Drive
- Differentiate personal and business data
- Copy/paste, Open-in, and Print control
- Single Sign-on



Mobile Risks & Threats



Mobile Risks & Threats

Las Vegas - estimated 5,000 cabs

- average of 2 phones per week
- 10,000 phones per week

United Kingdom – London


- Estimated 19,000 cabs (black cabs only)
- 10,000 phones per week



Average 113 phones lost every minute

\$50 average price for lost/stolen device

Mobile Risks & Threats

- **Phishing**
 - Fraudulent imitation of a site to obtain credentials or cc
- **Clickjacking**
 - Malicious technique to trick users into clicking a malformed link
- **Likejacking**
 - Uses Facebook  like button
- **MitM**
 - Spoof public/private WiFi
- **Prevention**
 - Device security settings
 - Don't click on links
 - Type the address
 - User Awareness Training



Mobile Risks & Threats

- **iOS Passcodes (Security vs. Usability)**
 - Simple Passcode (4 numeric digits)
 - Less than 30 minutes
 - Longer Passcode (6 numeric digits)
 - Less than 3.15 days
 - Complex Passcode (7 alphanumeric, at least 1 uppercase and 1 numeric)
 - Less than 44,667 YEARS.



Mobile Risks & Threats

Android

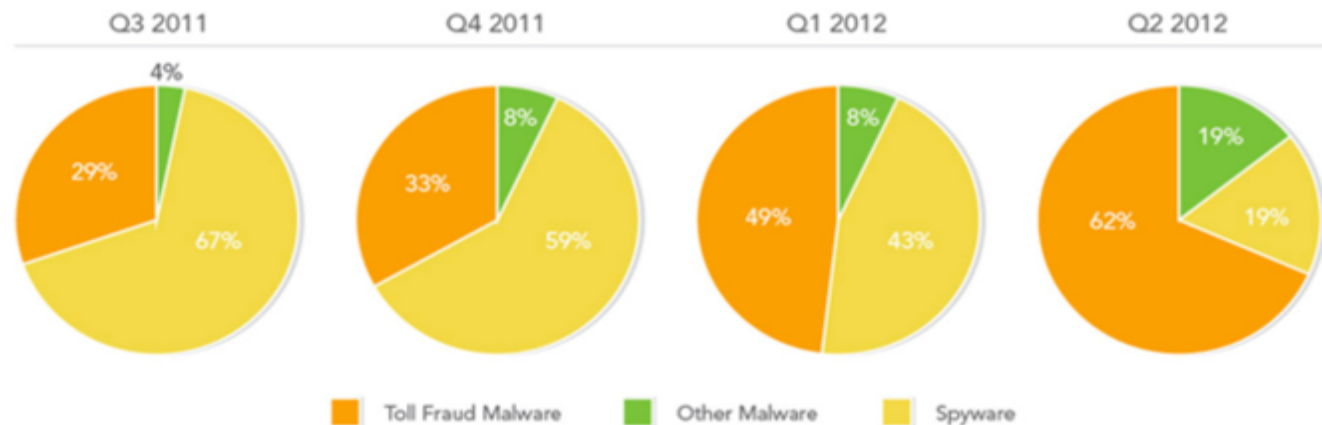
- Marketpay.A
- DroidDream
- Geinimi
- HongTouTou (aka ADRD)
- Zitmo
- MasterKey
- OpFake
- Obad

iOS

- Ikee
- iPhone.A
- Dutch 5€ Ransom
- Code signing exploit

Blackberry

- Zitmo



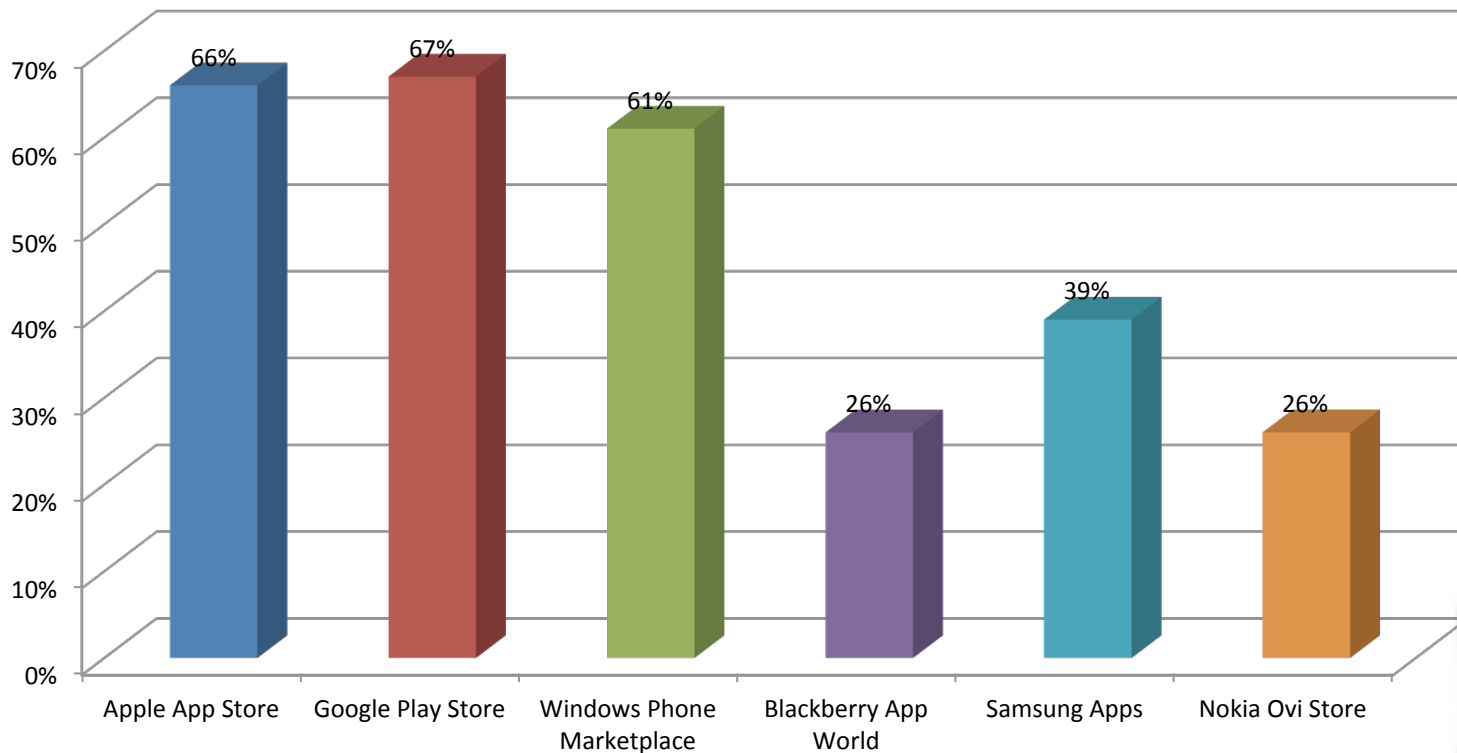


Mobile Application Awareness

Breakdown of Free Apps

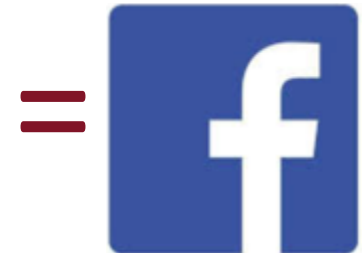
■ What's the risk?

Percentage of Free Apps available in various App Stores



Mobile Awareness

Storage Modify or delete the content on your device's storage	Audio Settings Change your audio settings	Your location Approximate location (network-based), precise location (GPS and network-based)
Other Application Permissions Draw over other apps	Sync Settings Read sync settings, toggle sync	Camera Take pictures and videos
System tools Read battery statistics	System tools Install shortcuts, read Home screen shortcuts, test access to power	Your applications information Retrieve running apps
Microphone Record audio	Affects Battery Control vibration, prevent auto-rotation	Your accounts Add or remove accounts, create accounts and set passwords
Your location Approximate location (network-based), precise location (GPS and network-based)	Your applications information Reorder running apps, run background services	Phone calls Directly call phone numbers, read phone status and identity
Camera Take pictures and videos	Network communication Download files without network access, view network connections	Network communication Full network access
Your applications information Retrieve running apps	Your accounts Find accounts on the device	Your social information Modify your contacts, read call log, read your contacts, write call log
Your accounts Find accounts on the device		



Mobile Security Technology

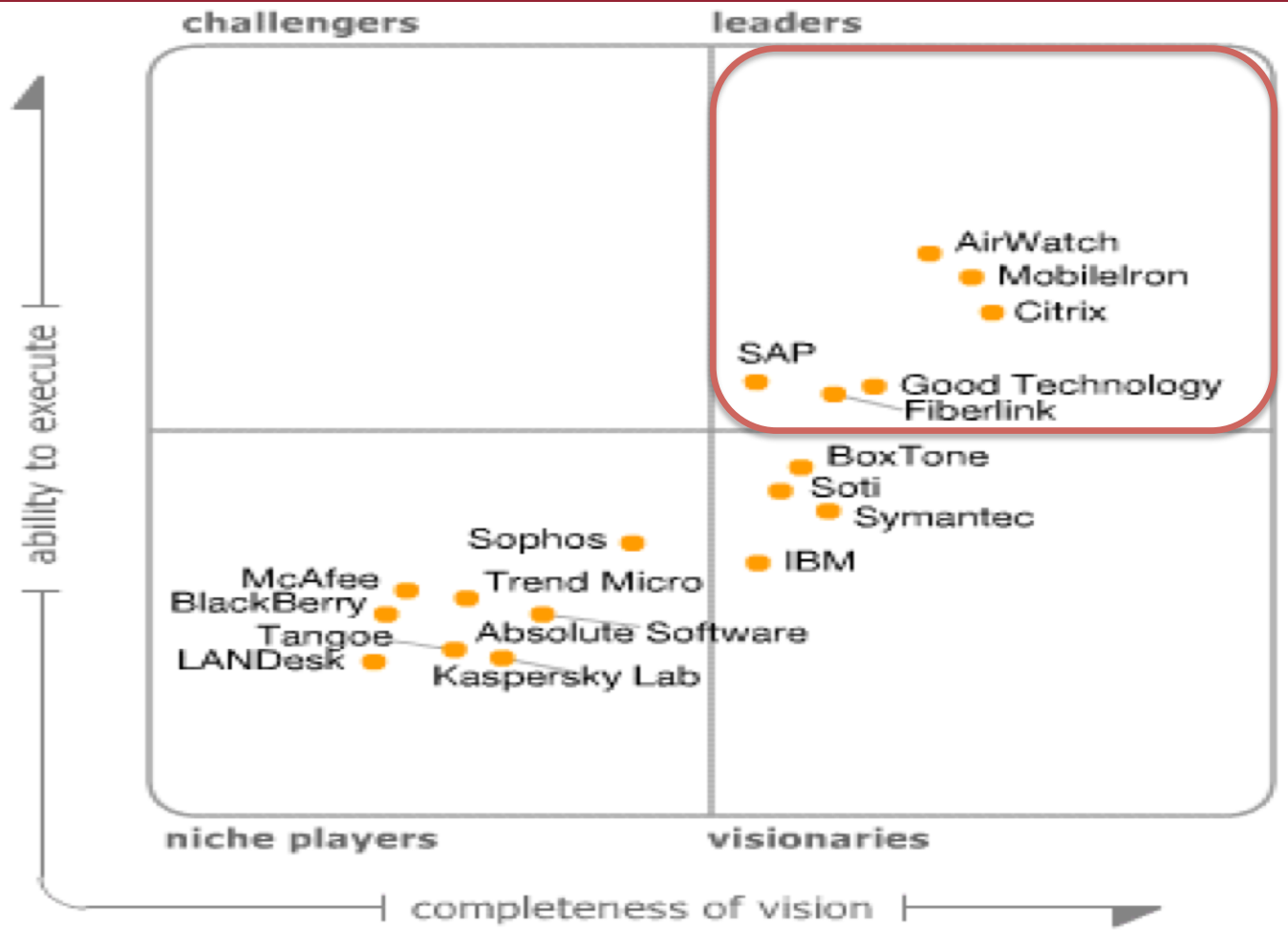


Mobile Security Technology

	IPCU	EAS	Third-Party MDM
Enforce passcode, length/complexity, history	X	X	X
Lock after timeout or retry limit	X	X	X
Remote lock and wipe over the air (OTA)		X	X
Selectively disable the camera	X	X	X
Selectively disable the browser	X		X
Control clipboard	X		X
Retrieve console logs, inventory	X		X
Manage VPN, Wi-Fi certificates	X		X
Manage ActiveSync email certificates		X	X
Remove enterprise-distributed apps	X		X
Jailbreak detection/action			X
Manage enterprise App Store			X
Restrict data access to encrypted container			X
Manage devices remotely/OTA		X	X
Lock on enterprise configuration violation			X
Comprehensive management for multiple platforms			X

Note: EAS functions described are based on Apple's implementation of EAS; only a partial comparison of features is shown.

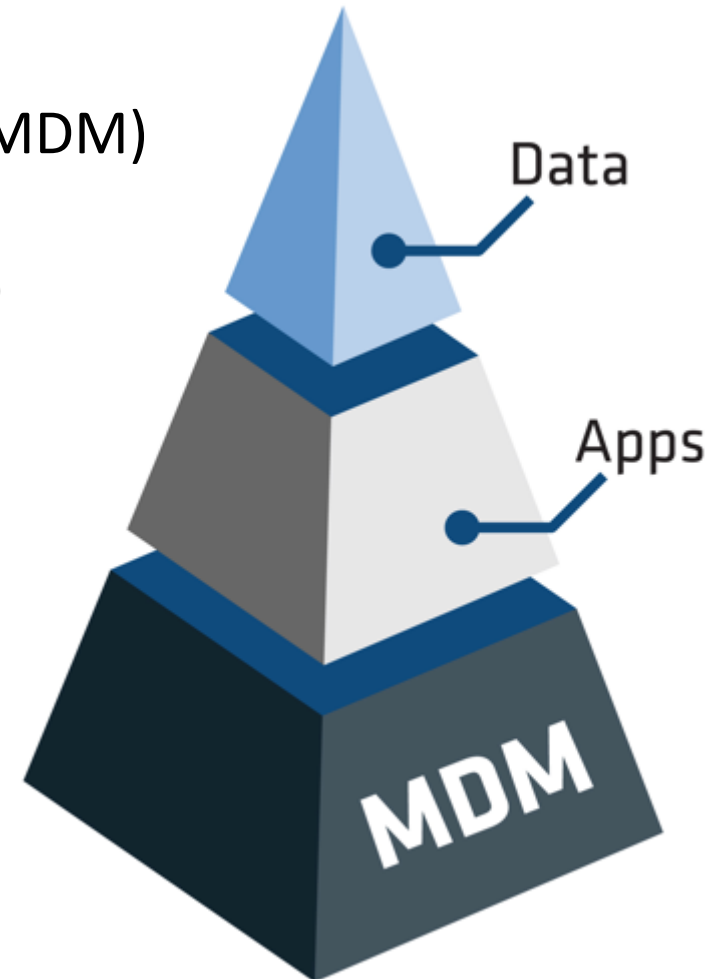
Mobile Security Technology



As of May 2013

Mobile Solutions

- Container Based
- Pure-Play Mobile Device Management (MDM)
- Mobile Application Management (MAM)
 - Not an Enterprise App Store
 - Next-Generation
- Mobile Content Management (MCM)



Mobile Management

- **Containerized**
 - Separation of personal & corporate data
 - Simple BYOD deployment
 - Personal Information Manager (PIM)
- **Verticals**
 - Healthcare
 - Financial



Mobile Management



- **Non-Containerized**
 - Device restrictions
 - Use of native applications
 - Simple architecture
- **Verticals**
 - Technology
 - Entertainment
 - Transportation

Mobile Security Technology

Containerize or not to containerize?

Pros	Cons
<ul style="list-style-type: none">• High degree of data security	<ul style="list-style-type: none">• Can increase your carrier costs¹
<ul style="list-style-type: none">• Control access to e-mail application via PIN	<ul style="list-style-type: none">• Reliance on 3rd party NOC
<ul style="list-style-type: none">• Data Leak Prevention	<ul style="list-style-type: none">• Non-native experience
<ul style="list-style-type: none">• Regulatory compliance (e.g. FIPS 140-2, SOX, HIPAA, etc.)	<ul style="list-style-type: none">• Only available as On Premise Solution

¹ Contact your wireless carrier(s) for details on required plan changes and associated costs

Mobile Security Technology

- MDM
 - Vmware AirWatch
 - MobileIron
 - Citrix XenMobile
 - Symantec App Center
 - IBM MaaS 360

- Container
 - Good Technology
 - Fixmo
 - AirWatch Workspace
 - Citrix WorxMail



Mobile Security Technology

- MAM (Mobile Application Management)
 - Personal and corporate application segmentation
 - Policy based application access
 - Application and data encrypted container
 - Wipe only corporate data and applications
 - IAM application access



Mobile Security Technology

- MCM (Mobile Content Management)
 - Secure access to internal resources
 - Sharepoint
 - Network Drives
 - Document control
 - Strong Authentication



Mobile Security Technology

- MBM (Mobile Browser Management)
 - Secure access to internal sites
 - Sharepoint
 - Intranet Sites
 - Content Filtering
 - Strong Authentication



Mobile Security Technology

Now that devices are under control, what's next?

- 2014 will bring
 - Mobile Application Management
 - Mobile Content Management
 - Further consolidation?
 - Expect innovation from leaders
 - Expect new, more complex devices



Thank You

