MobileIron®

BYOD, MDM and MAM (2nd Generation)

MobileIron

March 2012

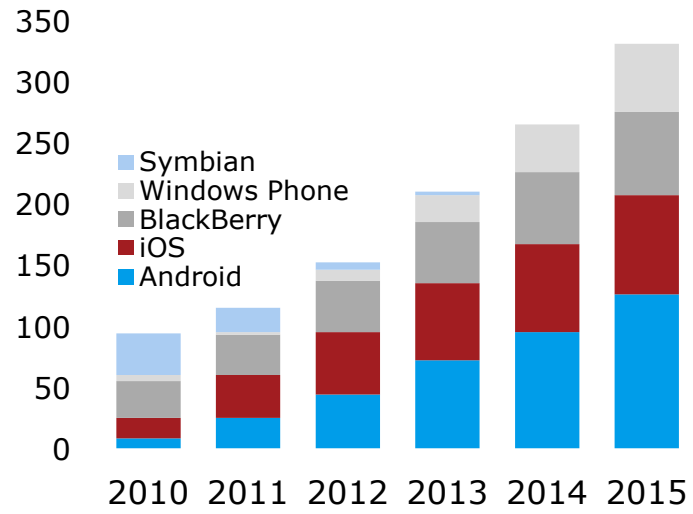
Agenda

- **Mobile challenge**
- **MobileIron solution**
- **Best practices**
- **Product updates**

Massive adoption, constant uncertainty

Devices everywhere

New Business Use Smartphone Shipments
(000,000)



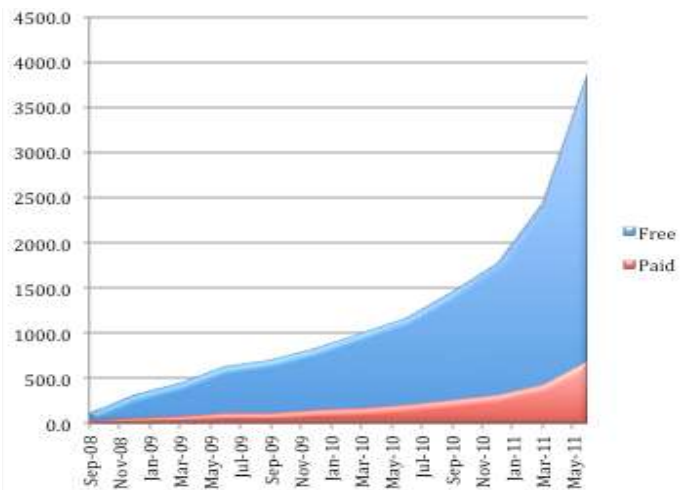
Source: IDC (Sept 2011)

BYOD >50% starting 2012

&

Apps everywhere

New App Store Downloads
(000,000)



Source: Piper Jaffrey, Fortune (July 2011)

47 apps per device and growing

Post-PC enterprise hits 50-50-50 tipping point in 2013

Context: Consumer preference #1 driver

50	More than 50% of employees go mobile
50	More than 50% of devices owned by employees
50	More than 50% of apps built outside IT

Impact: Complexity and constant migration

Tipping point is now

Mobile device is primary endpoint

Mobile app is preferred method of work

Mobile IT drives business transformation

Mobile First enterprise

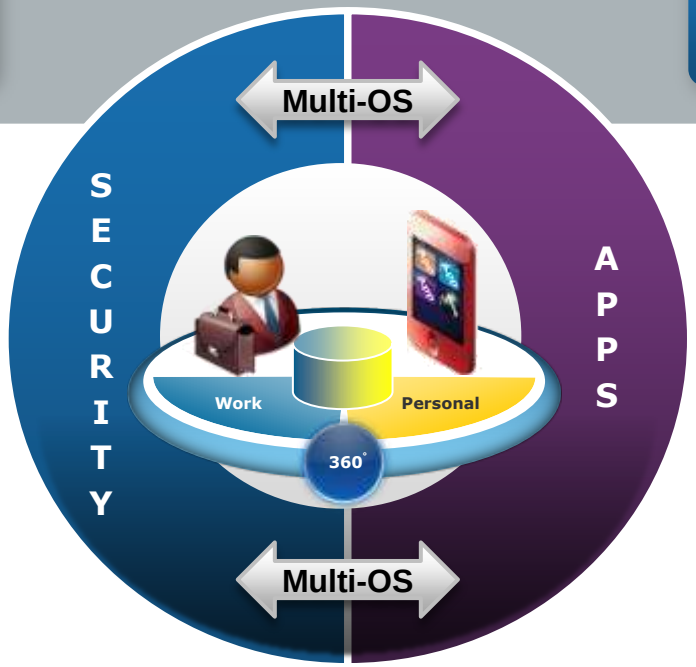
Forrester: "Corporate app stores become the intranet of the future"

Trusted Mobility

TRUSTED USERS

TRUSTED DEVICES

TRUSTED APPS



Business transformation for company and users

Today's Mobile IT objectives

- Support multi-OS
- Leverage BYOD
- Prevent data loss
- Go global cost-effectively
- Transform business through apps

Agenda

- Mobile challenge
- **MobileIron solution**
- Best practices
- Product updates

Analyst perspective on MobileIron

MobileIron ratings for Mobile Device Management

"[MobileIron] was built from the ground up with the dynamics of today's mobility market in mind and therefore does not have legacy issues that others face in terms of re-architecting their solutions."
IDC November 2011

MobileIron was the only vendor with top ratings in all four Gartner MDM Magic Quadrant and Critical Capabilities categories (execution, vision, viability, capability)

Customer success: Key item on CIO agenda

"MobileIron's strength is its ease of use for iPad owners." **Ashwin Ballal, CIO KLA-Tencor** (CIO, June 30, 2011)

"His team uses MobileIron to secure and lock down devices, push out specific apps, and offer users an app store." Interview with **Steve Phillpott, CIO Amylin Pharmaceuticals** (InformationWeek Sept 13, 2011)

"To provide better security controls on those mobile devices, we're using a tool called MobileIron." **Tina Rourk, CIO Wyndham Vacation Ownership** (Network World, Aug 30, 2011)

"These guys were the closest to having support for Apple. They almost had everything we needed, and they jumped on the opportunity --10,000 devices deployed nationwide! -- and did what it took to really hammer this thing out." **Dick Escue, CIO RehabCare** (SearchCIO, March 2011)

Click for video

Customer success is our focus

MobileIron®

- Founded in 2007
- Multi-OS architecture
- Security / apps leadership
- Global operations
- Mobile IT best practices

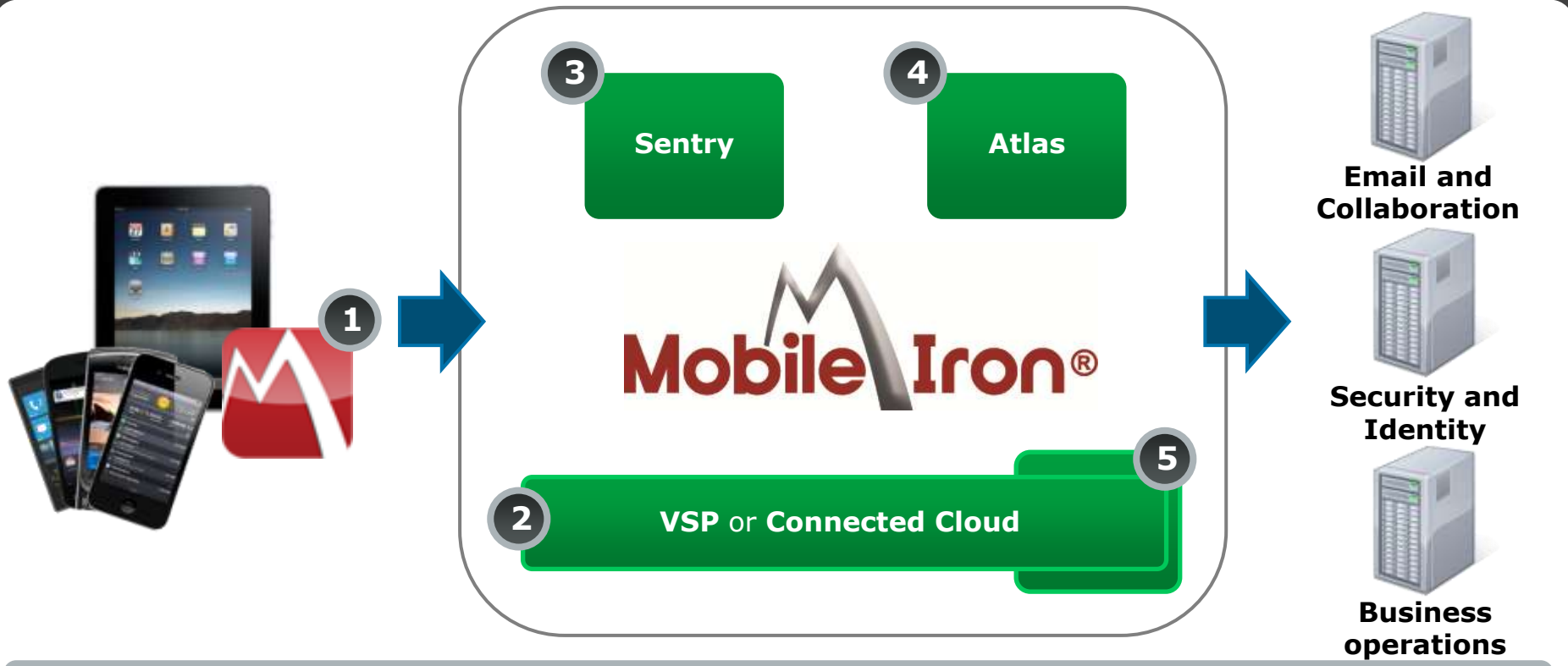
1500+ customers in two years

200+ of Fortune 1000/Global 2000

200+ using apps through MobileIron

99% renewal rate

MobileIron platform components



1 Client
Secure app storefront
Posture monitor (jailbreak)
Enforcement

2 Multi-OS core (premise/cloud)
Inventory
Policy
Security and privacy
Apps
Events and workflow

3 Access control
Allow/block email
Allow/block apps (coming)
Automated workflow
ActiveSync visibility

4 Central console
Monitoring and reporting
Troubleshooting
Scale to 100,000+ devices

5 Enterprise integration
Email
AD/LDAP
Certificates
BES
Archival
Custom (Passport API)

MobileIron: Comprehensive platform for Mobile IT

1 Configure securely

Email and apps
Security and identity
Wi-Fi and VPN
… by group, individual, or ownership

2 Integrate tightly

Email
AD/LDAP
Certificates
BES
Archival

3 Protect privacy

BYOD programs
Regional regulations

4 Roll out at scale

By group or policy

MobileIron®

5 Manage all devices

Multi-OS console for employee- and company-owned mobile devices

TRUST

6 Monitor posture/risk
7 Control access *(Sentry)*
8 Enforce identity *(certs)*
9 Automate workflow

APPS

10 Keep out rogue apps
11 Distribute apps *(IT)*
12 Discover apps *(user)*
13 Secure app data

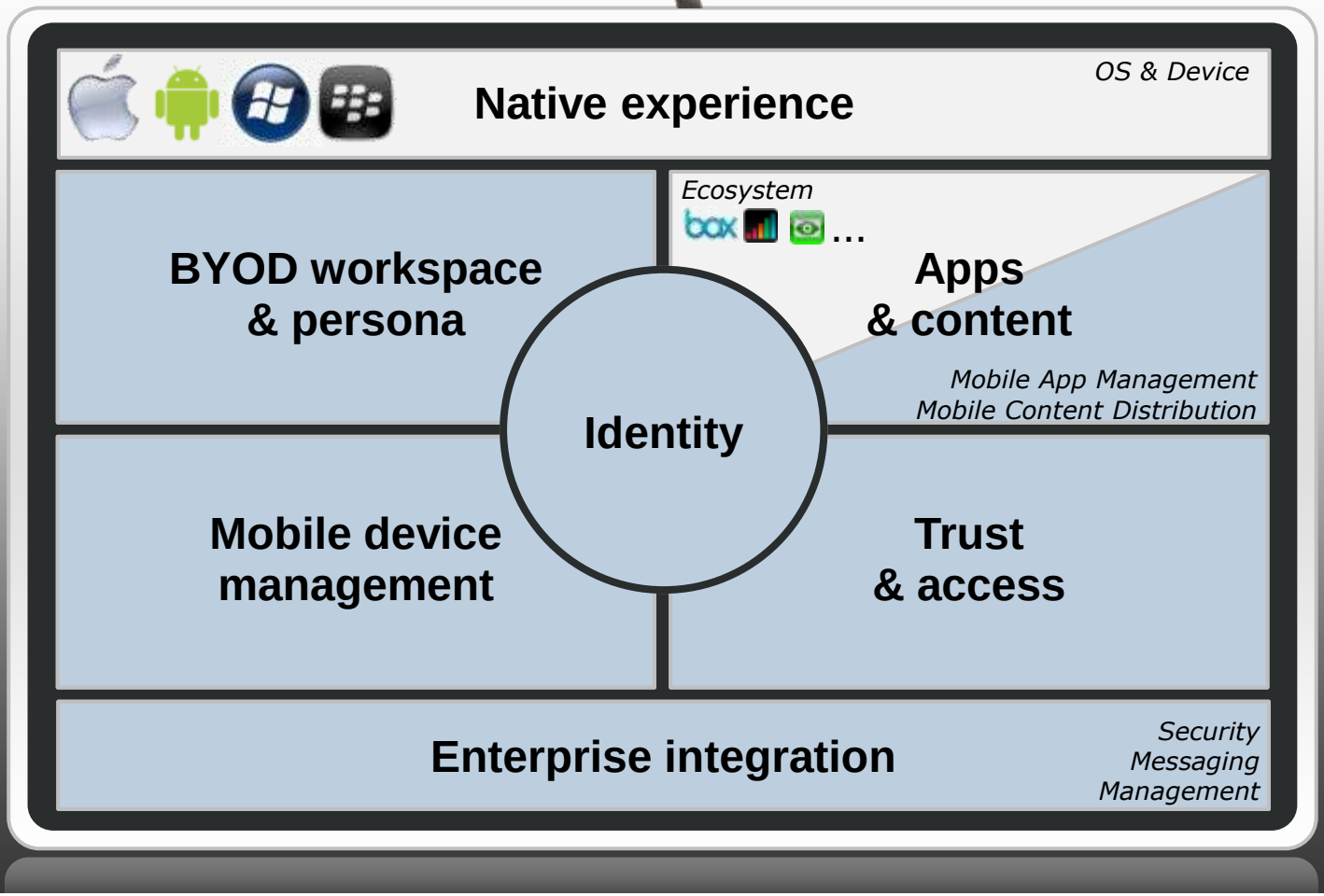
COST

14 Limit usage costs

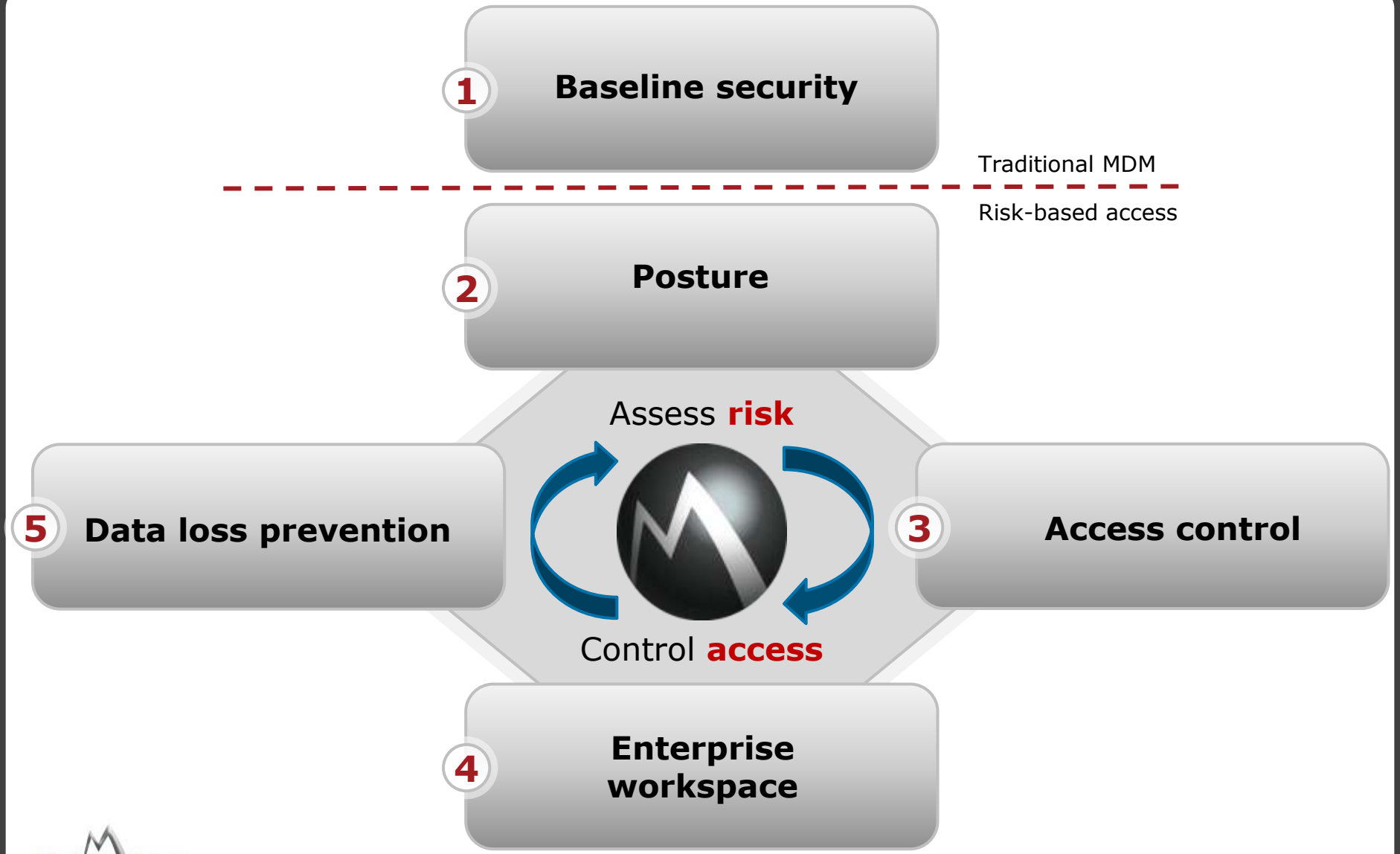
15 Wipe corporate data

Building the Mobile IT stack

PREMISE MobileIron® **CLOUD**



MobileIron security model



MobileIron apps model

1

App Control

For IT to keep out rogue apps

- **Track inventory**
- **Monitor permissions**
- **Create app policies** (Required, Allowed, Disallowed)
- **Alert/block on violations**

2

Enterprise App Storefront

For users to get apps

- **Discover (user)**
- **Download (user)**
- **Distribute in-house apps**
- **Recommend public apps**
- **Delete managed apps**

3

AppConnect*

For developers to secure apps

- **Authenticate**
- **Configure**
- **Authorize**
- **Control access (tunnel)**
- **Remove**

Public apps
In-house apps

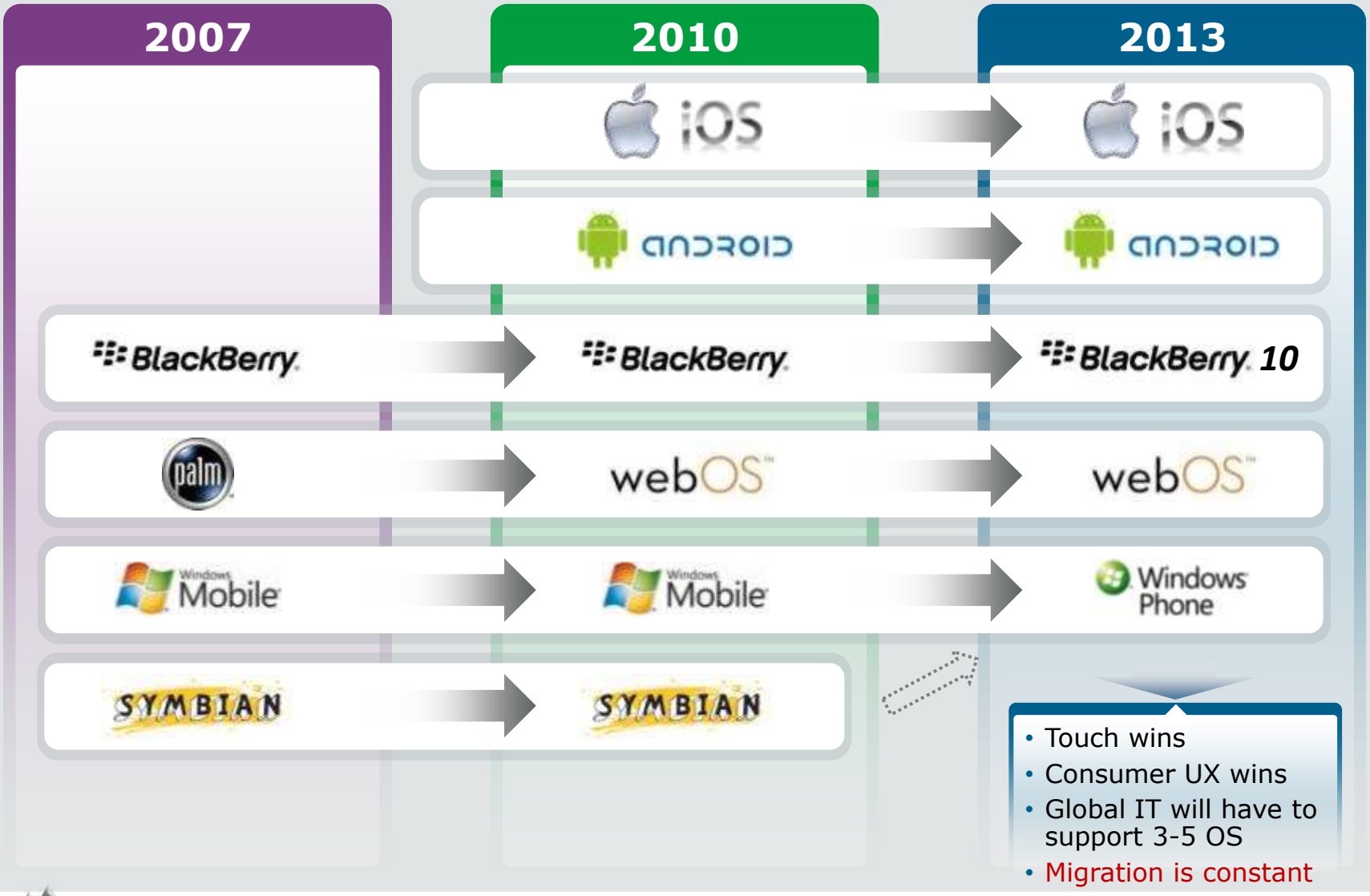
* In development

MobileIron across the app lifecycle

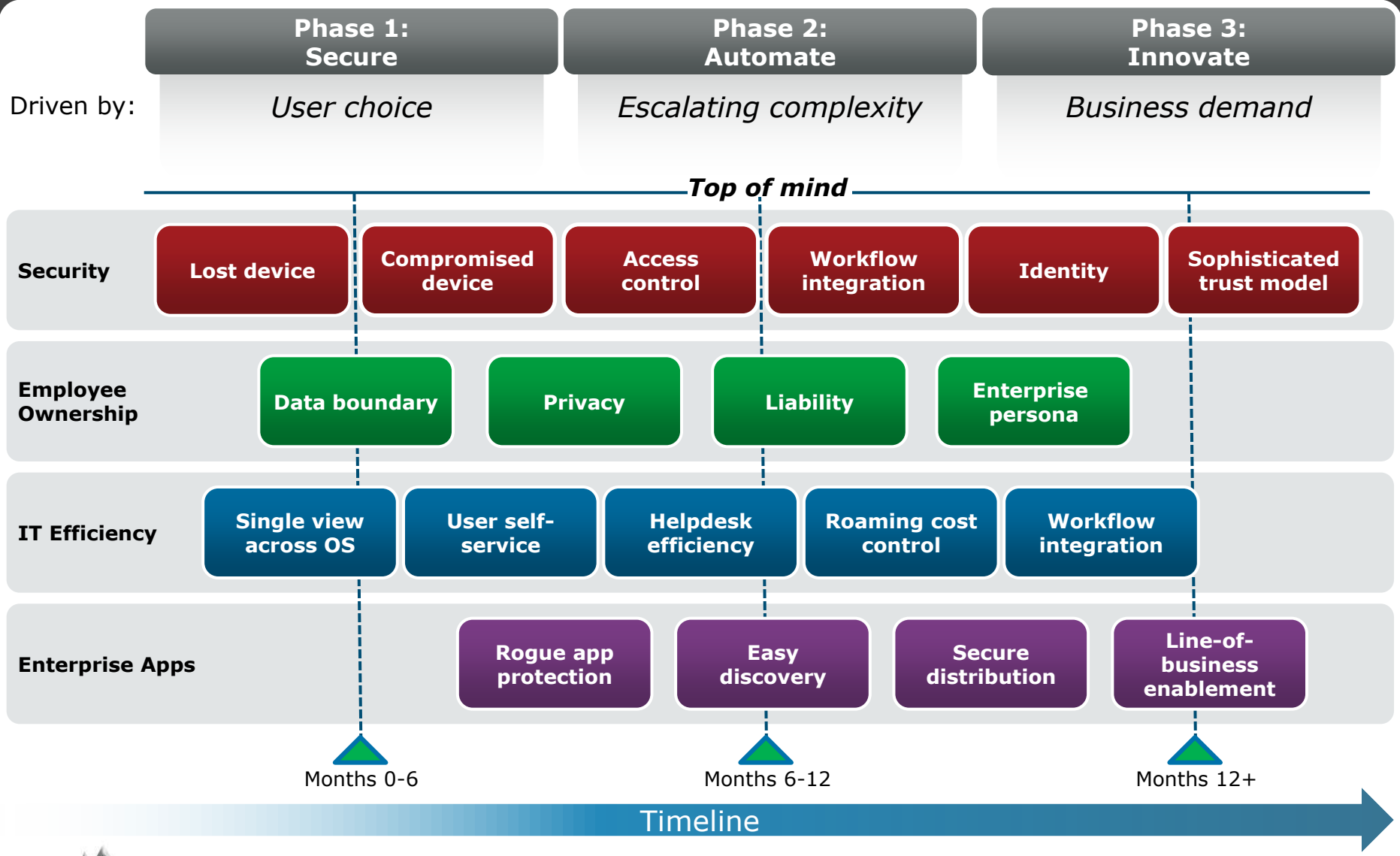
Agenda

- Mobile challenge
- MobileIron solution
- **Best practices**
- Product updates

Mobile operating system evolution continues



Enterprises requirements evolve over time …



Several best practices emerging

BYOD

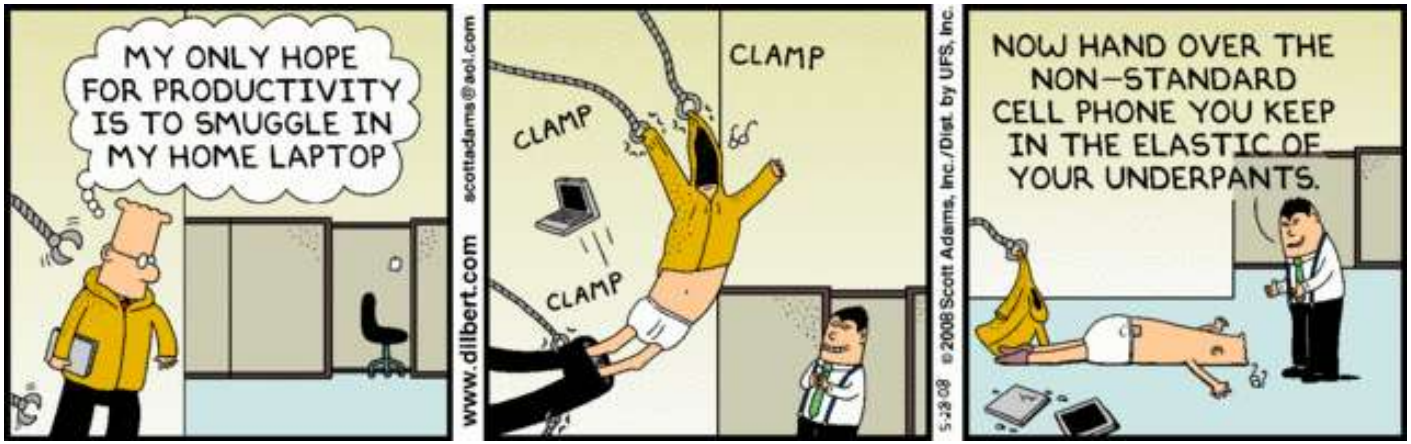
Apps

Data loss prevention

Android

Malware

The BYOD police

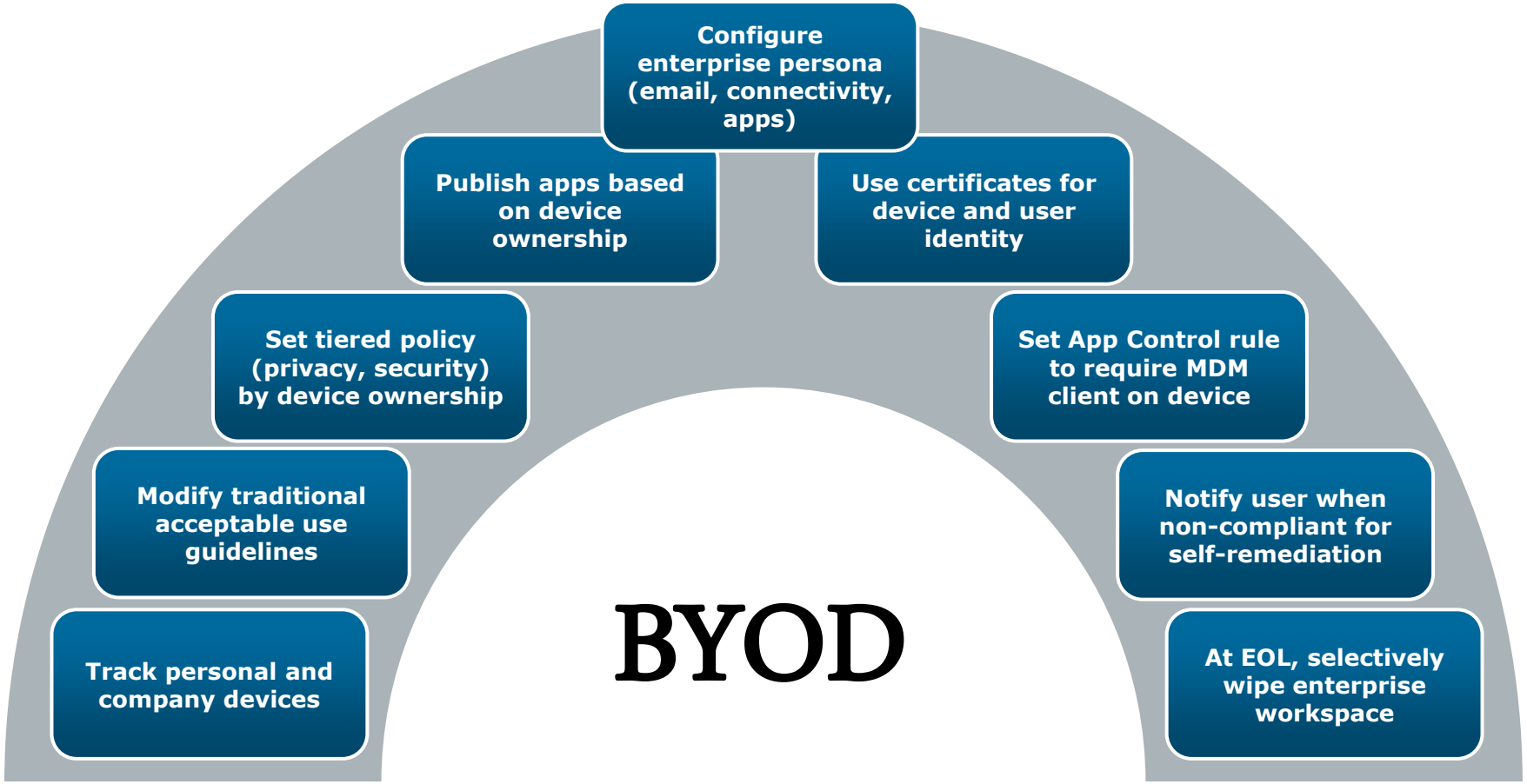


BYOD programs that damage the user experience

- Diminish value to the enterprise
- Limit user adoption

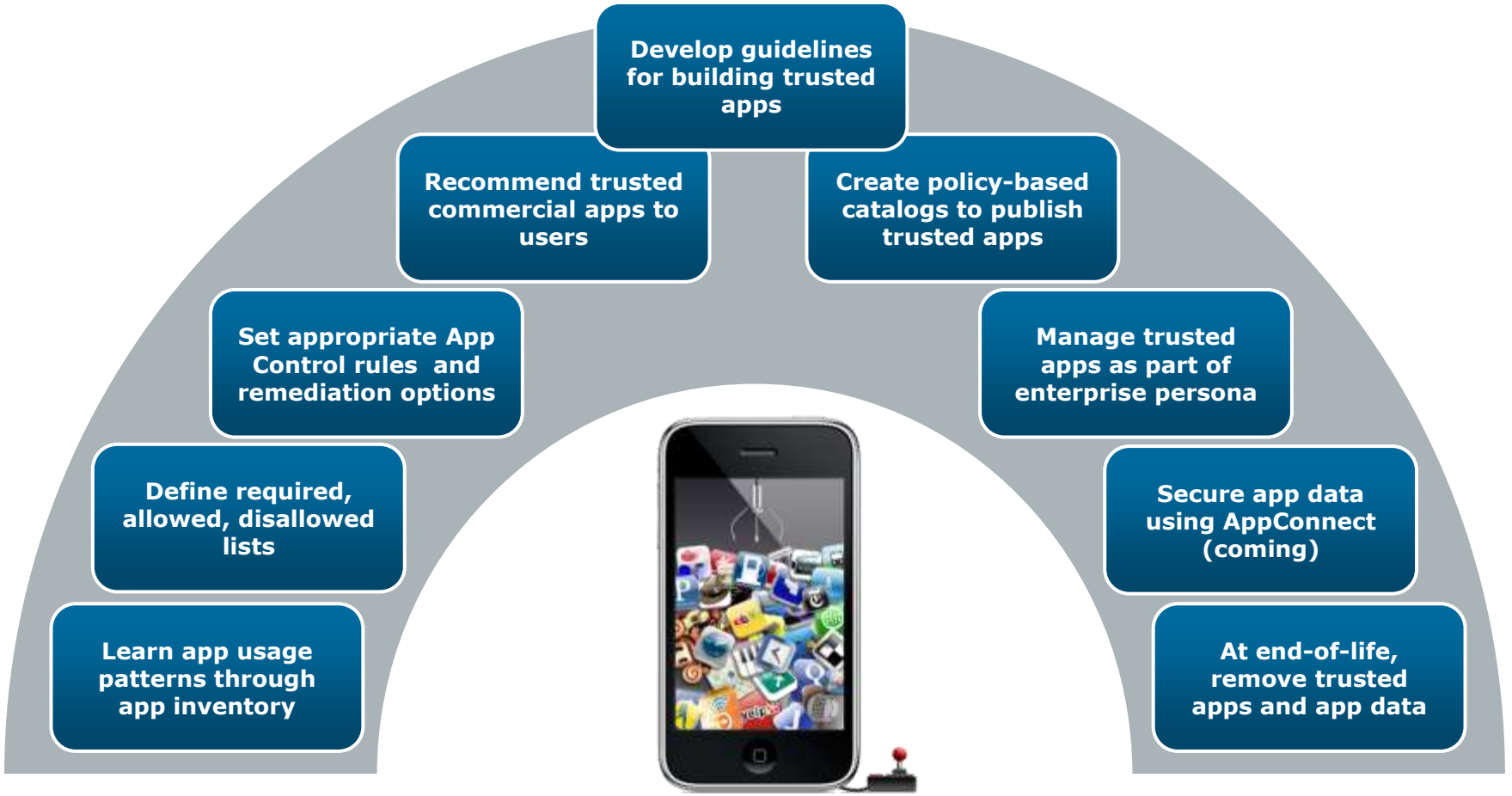
Best practices for Bring Your Own Device programs

Secure enterprise workspace while preserving user experience



Best practices for mobile enterprise apps

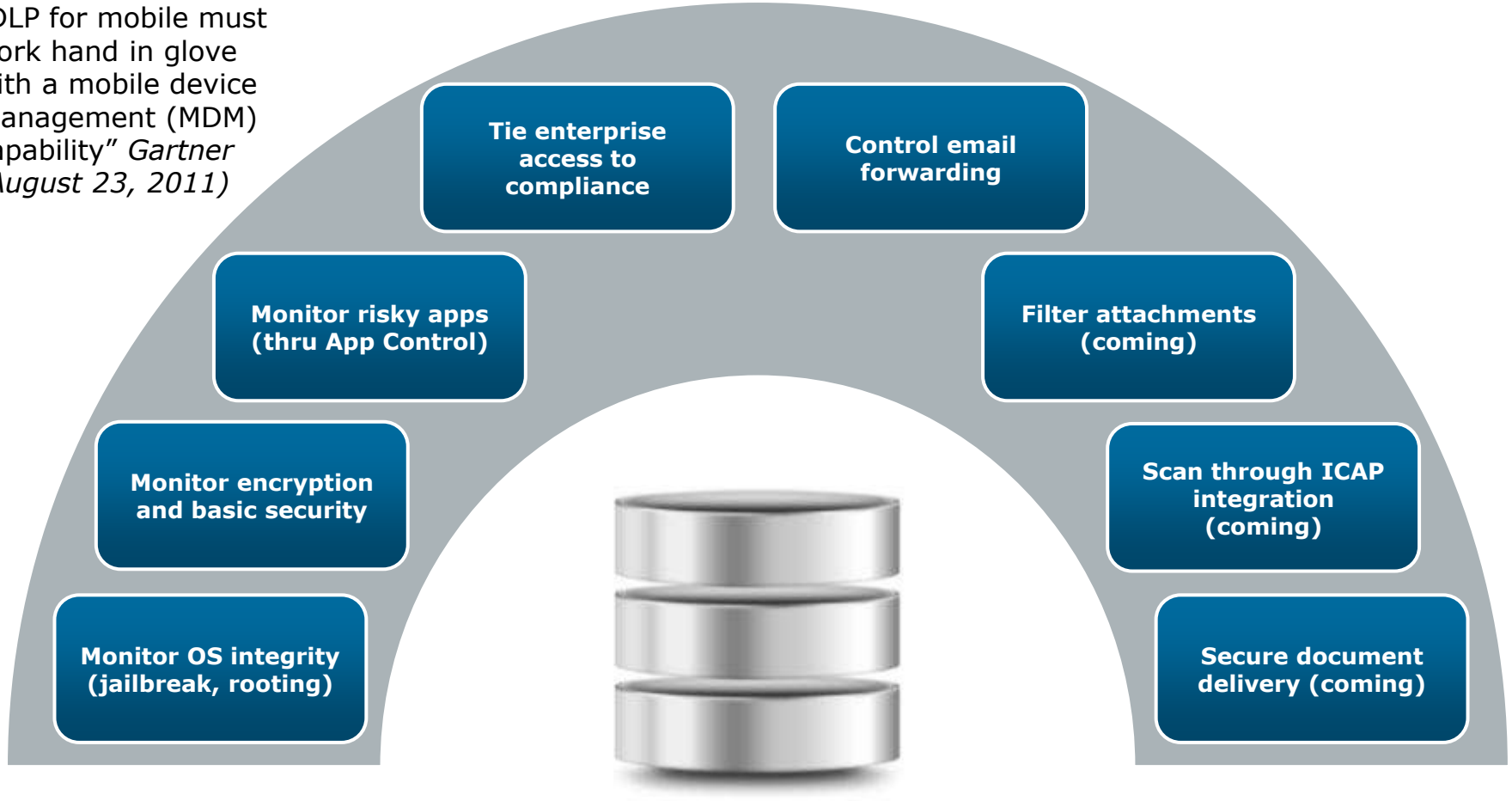
Remove obstacles blocking enterprise app deployment



Best practices for mobile data loss prevention

Reduce risk of data loss without damaging user experience

"DLP for mobile must work hand in glove with a mobile device management (MDM) capability" *Gartner (August 23, 2011)*

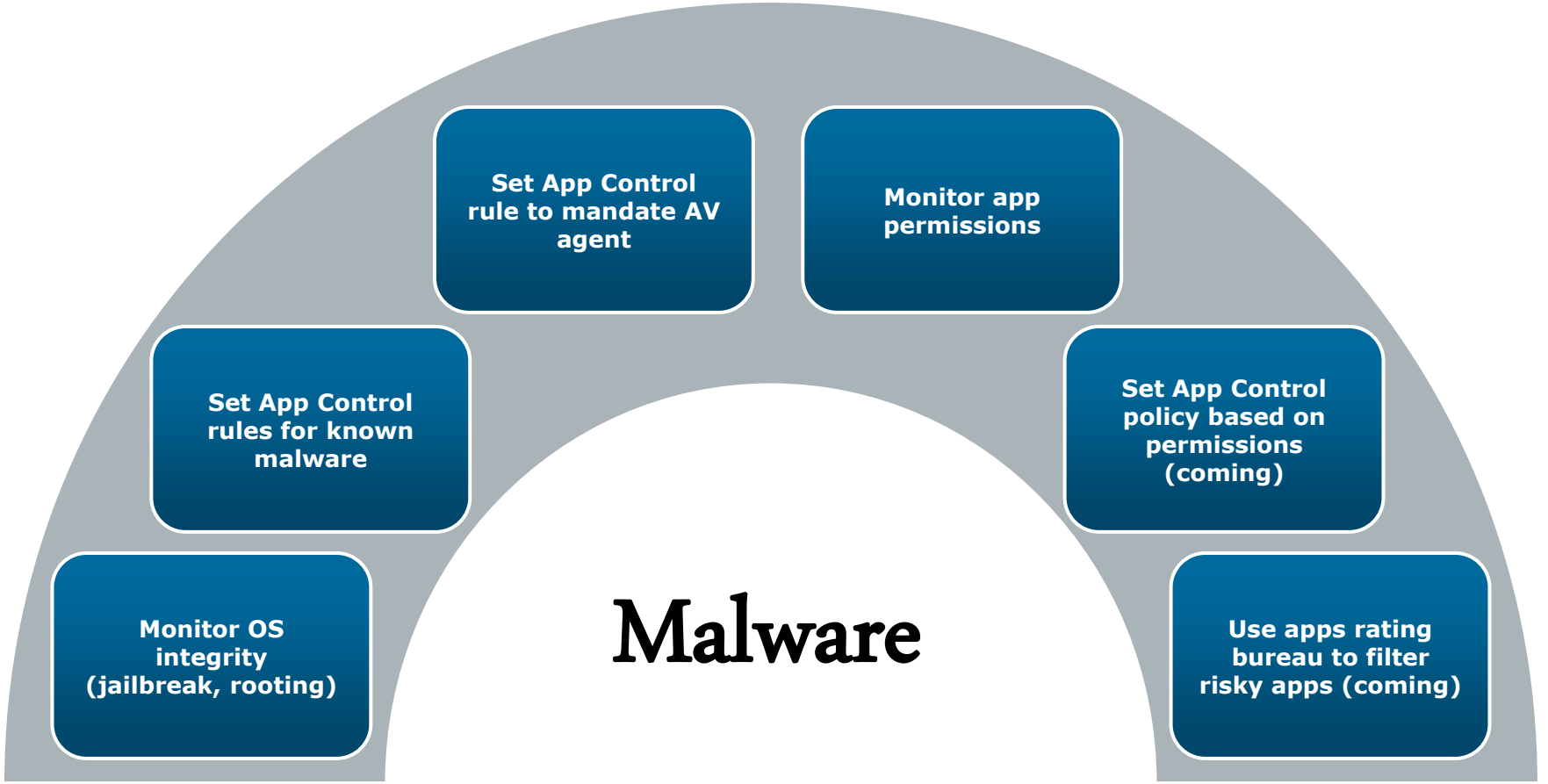


Best practices for Android

Prepare now for the complexity to come

Best practices for protecting against malware

Structure around visibility and action, beyond just AV

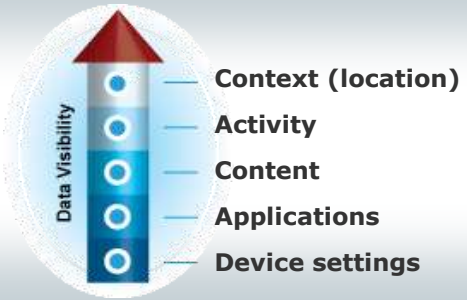


Agenda

- Mobile challenge
- MobileIron solution
- Best practices
- **Product updates**

MobileIron product investments

Data architecture



Area of focus

1. **Core services**
2. **Mobile platforms**
3. **Large deployments**

Core features

Core services	Mobile platforms	Large deployments
Security	**Android**	**Global scale**
App management	**BlackBerry**-> QNX/BBX/10	**Speed of deployment**
Device management	**iOS**	**Reporting**
Activity intelligence	**Symbian** -> Win Phone	**Hostability**
Troubleshooting	**webOS** -> open source	**Enterprise integration**
Content distribution (coming)	**WinMo** -> Win Phone	**Internationalisation**
	Win Phone	

2012 themes – next set of mobile enterprise challenges

"Appstorm" data security

BYOD security & privacy

Android unification and enterprise viability

MobileIron unified security for Android

Google

App Vendors

TouchDown by NitroDesk, Inc.

Cisco AnyConnect

Device Manufacturers

SAMSUNG

htc quietly brilliant

3LM Three Laws of Mobility

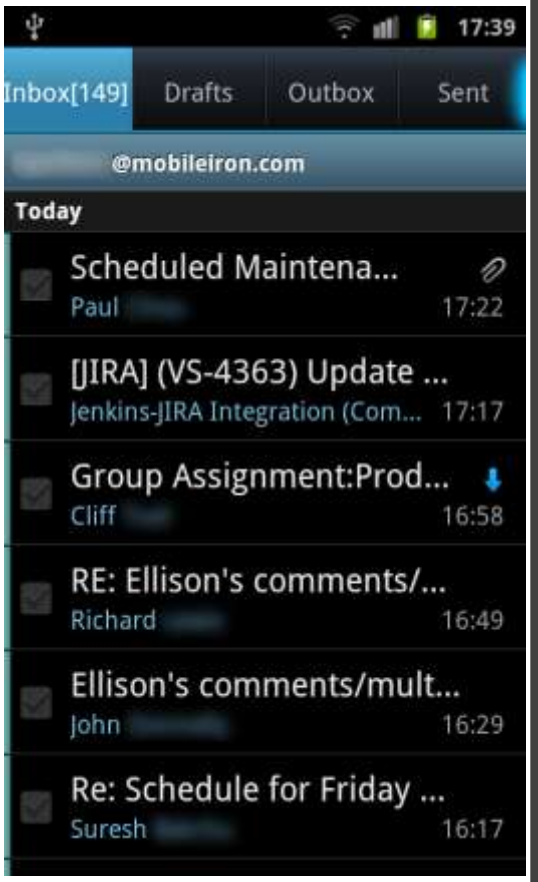
LG Life's Good

Leverage native Android capabilities when possible

Leverage device specific capabilities when necessary

Samsung integration

- **Features**
  - Encryption Policy
  - Native E-mail Client Configuration (with certs)
  - Lockdown: Camera, Wi-Fi, Bluetooth
- **Devices**
  - Galaxy S.A.F.E.-certified devices only
  - Legal issues may affect availability – Europe, Australia, others?



Cisco AnyConnect integration

- **Features**
  - Configuration settings
  - Certificates
    - Provisioned directly to the AnyConnect App
  - Configuration removed upon retire
- **Devices**
  - Samsung Galaxy S.A.F.E.-certified devices only
  - HTC (coming soon)

What can you do?

- **Identify baseline set of management capabilities**
  - Encryption, password policy, lock, wipe, etc.
- **Identify devices which meet minimum requirements**
  - Corporate-owned: Single device
  - Employee-owned: “Choose” Your Own Device (CYOD)
- **Communicate your Android enterprise requirements**
  - Google, carriers, manufacturers
- **Create a Mobile IT Team**
  - Appoint an Android expert
  - Investigate Android app development

MobileIron enterprise app storefront for iOS

Most broadly deployed Mobile Application Management (MAM) solution:

ACROSS ALL APPS	Publish in-house and App Store apps Manage Volume Purchase Program (VPP)
EASY DISTRIBUTION AND DISCOVERY	Distribute through policy to user or group and only to authorized devices
DELETION	Delete app and app data for managed apps
CUSTOM BRANDING	Brand app storefront launch icon
SECURE CATALOG	Provide most complete security for app distribution (next page)

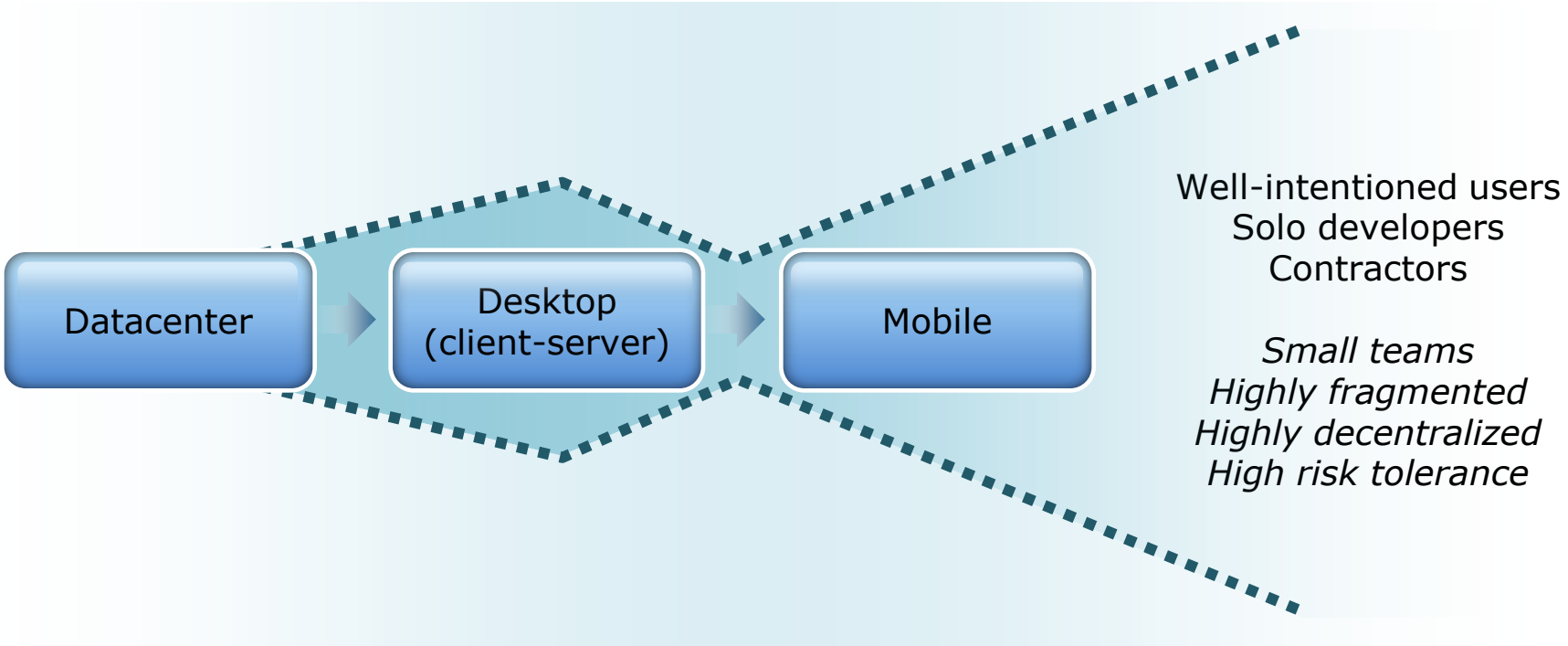
Complete security for app catalog and distribution

Security Requirements

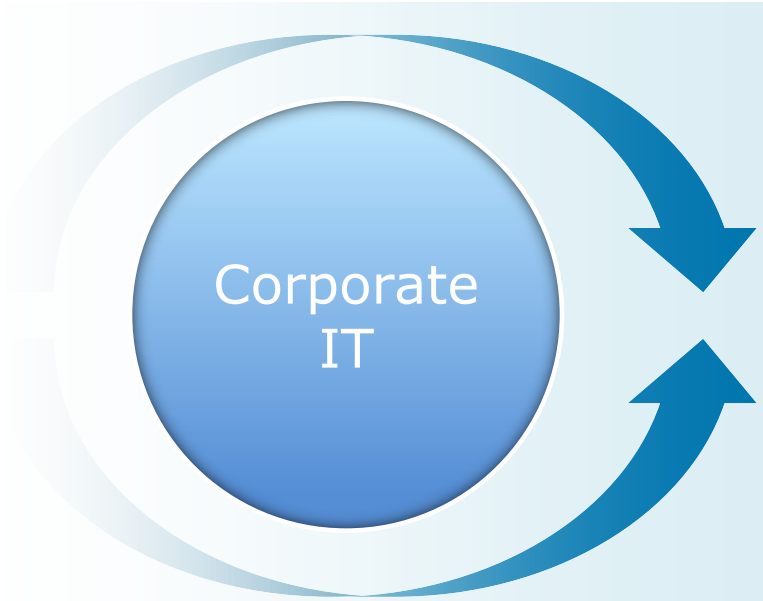
- Only **authorized users** can access app catalog
- Only **authorized devices** can access app catalog
- **App installation files** cannot be misappropriated
- **VPP tokens** cannot be misappropriated

Secured Using MobileIron Certificate Architecture

Mobile apps will create Shadow IT 2.0



IT bypass is risky and inevitable



"**IT bypass**" catalyzed by:

- Strong user demand for mobile apps
- Increasingly technical user base
- Easy (initial) app development
- Corporate policies lagging technology

"The more the CIO says 'no', the less secure the organization becomes."

Vivek Kundra, U.S. Federal CIO, Jan 2011

Role shift for IT

New services mindset to harness apps innovation

- Consumer-grade user discovery experience
- Company-wide, policy-based distribution
- Plug `n play security
- Best practices knowledge base and advocacy
- Marketing and communications
- ***Mobile First!***

MobileIron across the app lifecycle

AppConnect basics

Extend MobileIron's security framework to apps

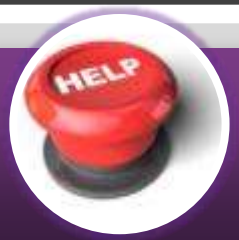
- **Authentication**
  - Verify authorized users can get access to the app
- **Configuration**
  - Get the app up and running properly
- **Authorization**
  - Verify device is in compliance before allowing app to run
- **Tunneling**
  - Allow only trusted app traffic onto the corporate network
- **Removal**
  - Wipe app data

Initial partners

MobileIron: Innovation leader for Mobile IT

- Multi-OS architecture
- Enterprise app stores
- Selective wipe
- Jailbreak detection
- E-mail access control
- Certificate-based identity
- Privacy policy
- BYOD groups
- Real-time roaming detection

Ongoing programs for education, training, and support



World-class global technical support and services

Domain expertise around mobility best practices

MobileIron University

Best Practice Toolkits

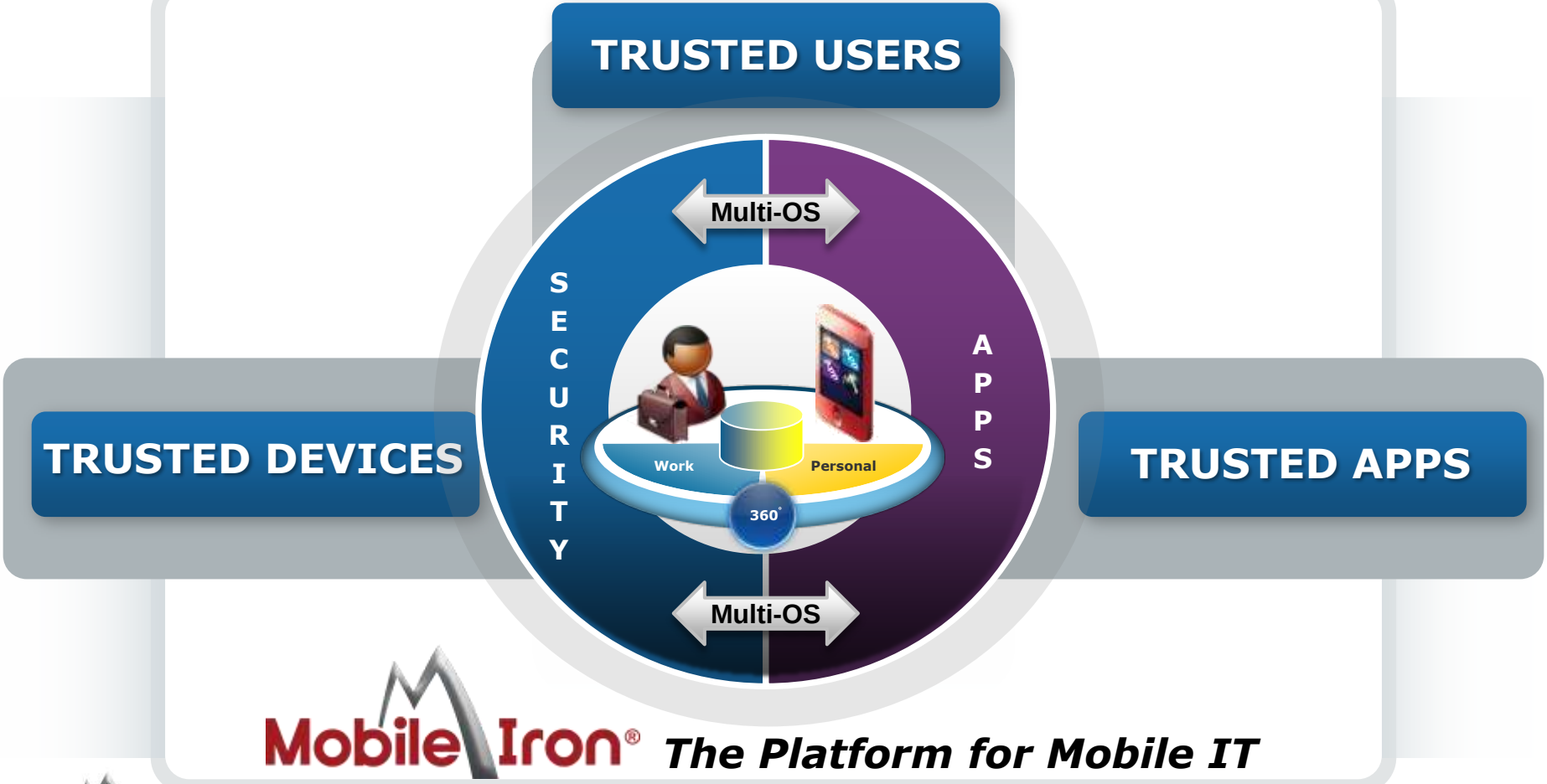
Sample: BYOD

1. Risk assessment
2. Security policy
3. User agreement
4. FAQ template
5. Self-service guidelines

Peer community

Setting up Mobile IT for success

"The more the CIO says no, the less secure the enterprise becomes" Vivek Kundra, CIO of the United States, Jan 2011



MobileIron®

Thank you