

# Enterprise Mobile Management

*e* FOCUS

---



# Enterprise Mobile Management

Ben Santing, HP



# Changing Face of Enterprise Mobility

- **Consumerisation** has transformed mobility
- Line between **corporate and private** blurring
- Cloud computing
- Pace of technology change
- Growing mobile workforce
- Requirement for **multi-platform** support
- Rising **cost** of providing corporate devices
- Multiplied attack vectors for **cyber-criminals**
- More **vulnerable** corporate data

# Enterprise Mobile Management

*e* FOCUS



# Top 5 Mobile Security Threats 2012

---

- Viruses, Trojans
- Mobile malware is big business
- Browser based apps
- You can't block the browser
- One Cloud to rule them All
- Employees sharing corporate data
- Lost, stolen and traded phones
- Poor Planning
- Source: InformationWeek reports

# Enterprise Mobility Management

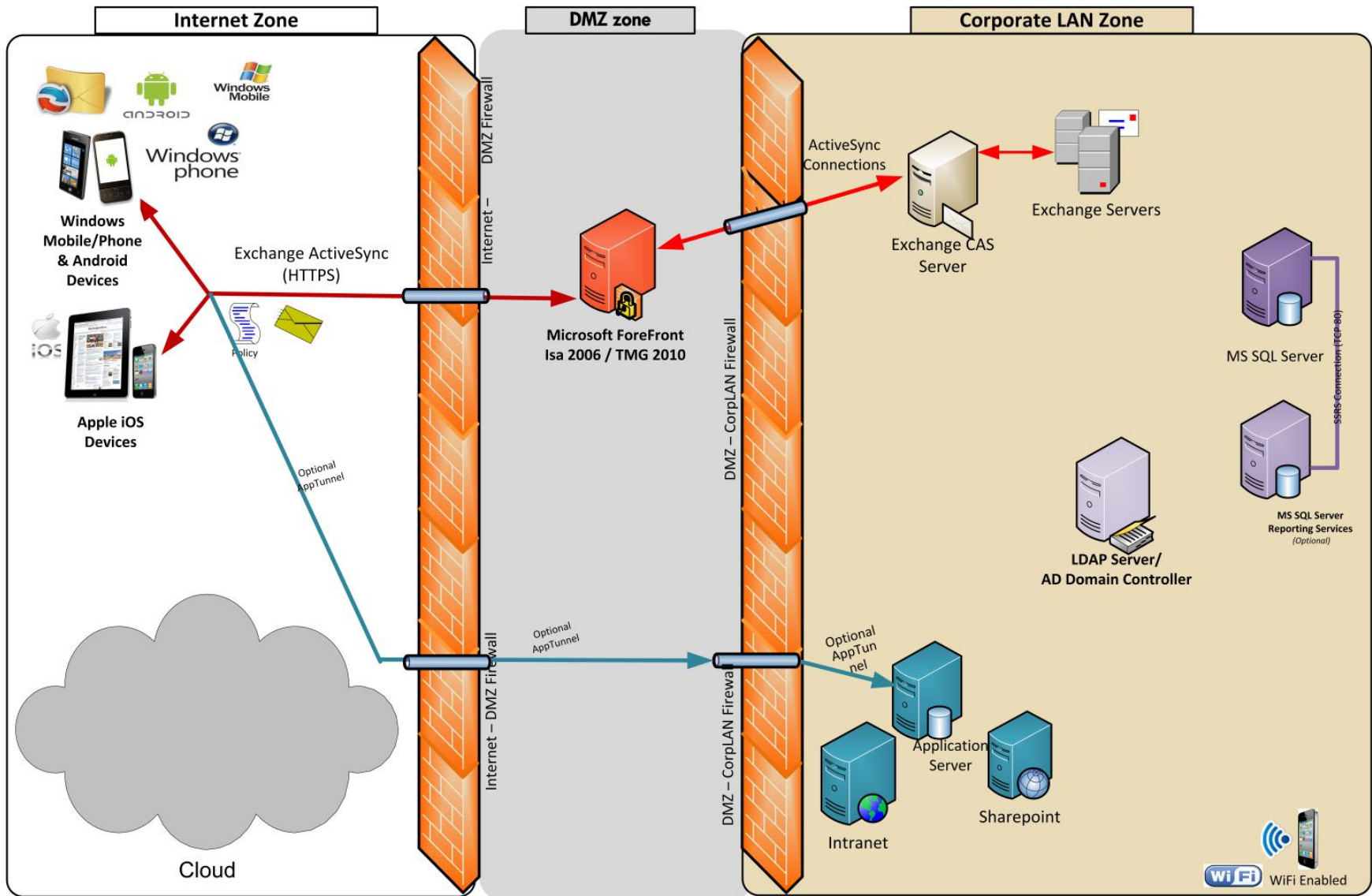
## • Traditional MDM

- Engineered for corporate owned devices
- Securing devices against malicious or casual access
- Through policies and commands, such as PIN enforcement and OTA wipes
- No choice: “Any color as long as it is black” (H. Ford)

## • Enterprise Mobility Management

- Also incorporate BYOD (for both trusted & non-managed)
- Also securing data against leakage to un-monitored/non-corporate environments
- MDM, MAM, MSM, MUM etc.
- Evolve at Consumers pace
- Mobility Lifecycle Management

# Example of Traditional MDM - EAS



# Traditional MDM - EAS

---

- Exchange ActiveSync (EAS) Policies
- EAS Remote Wipe
- No Application Support
- Cumbersome Certificate Management
- No Device Inventory
- Devices have known to lie ...
- No answer on “Where is my Data”
- What about retired devices? Rogue devices?
- WiFi

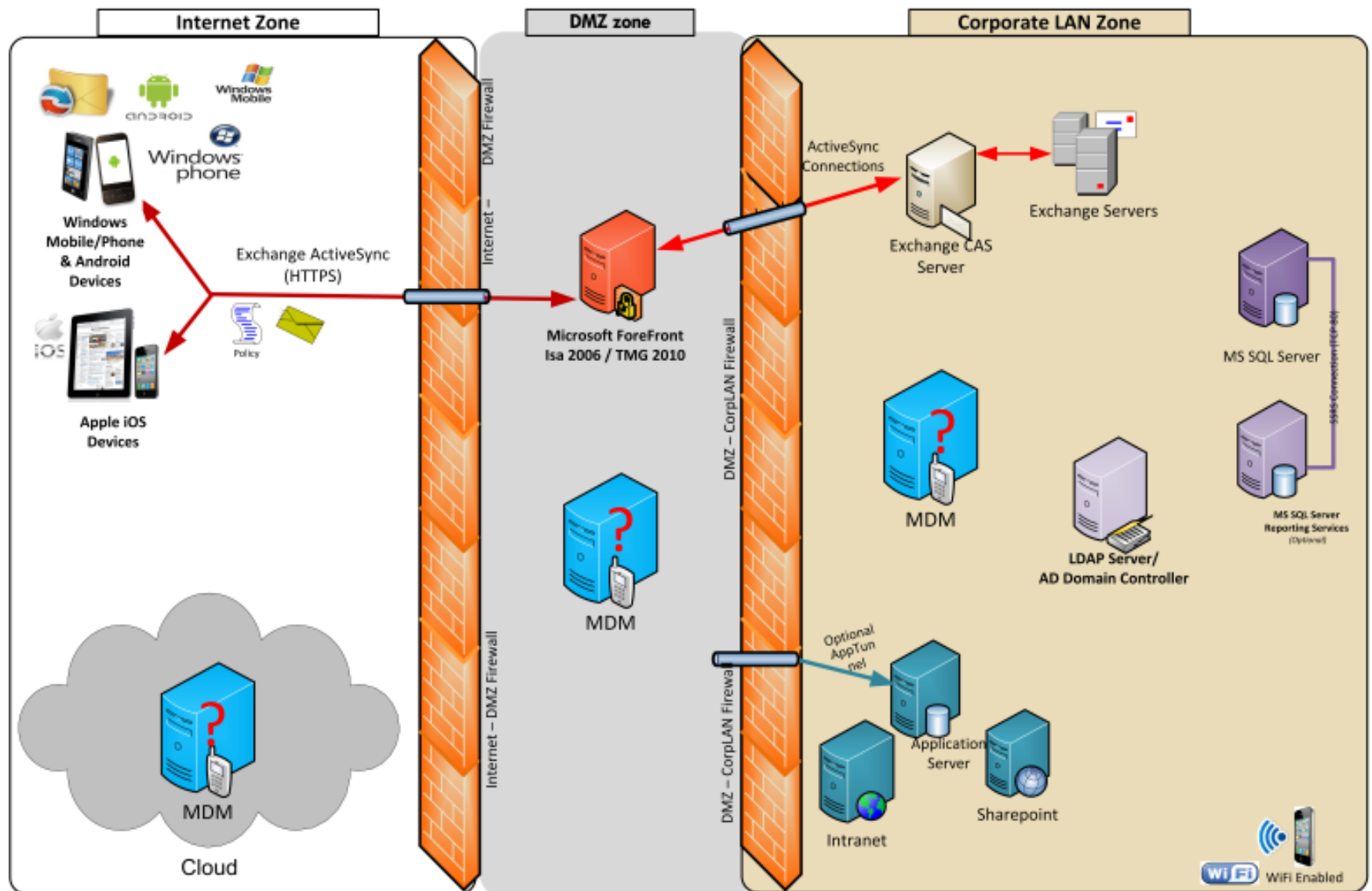


# Where is my Data? Future Trend

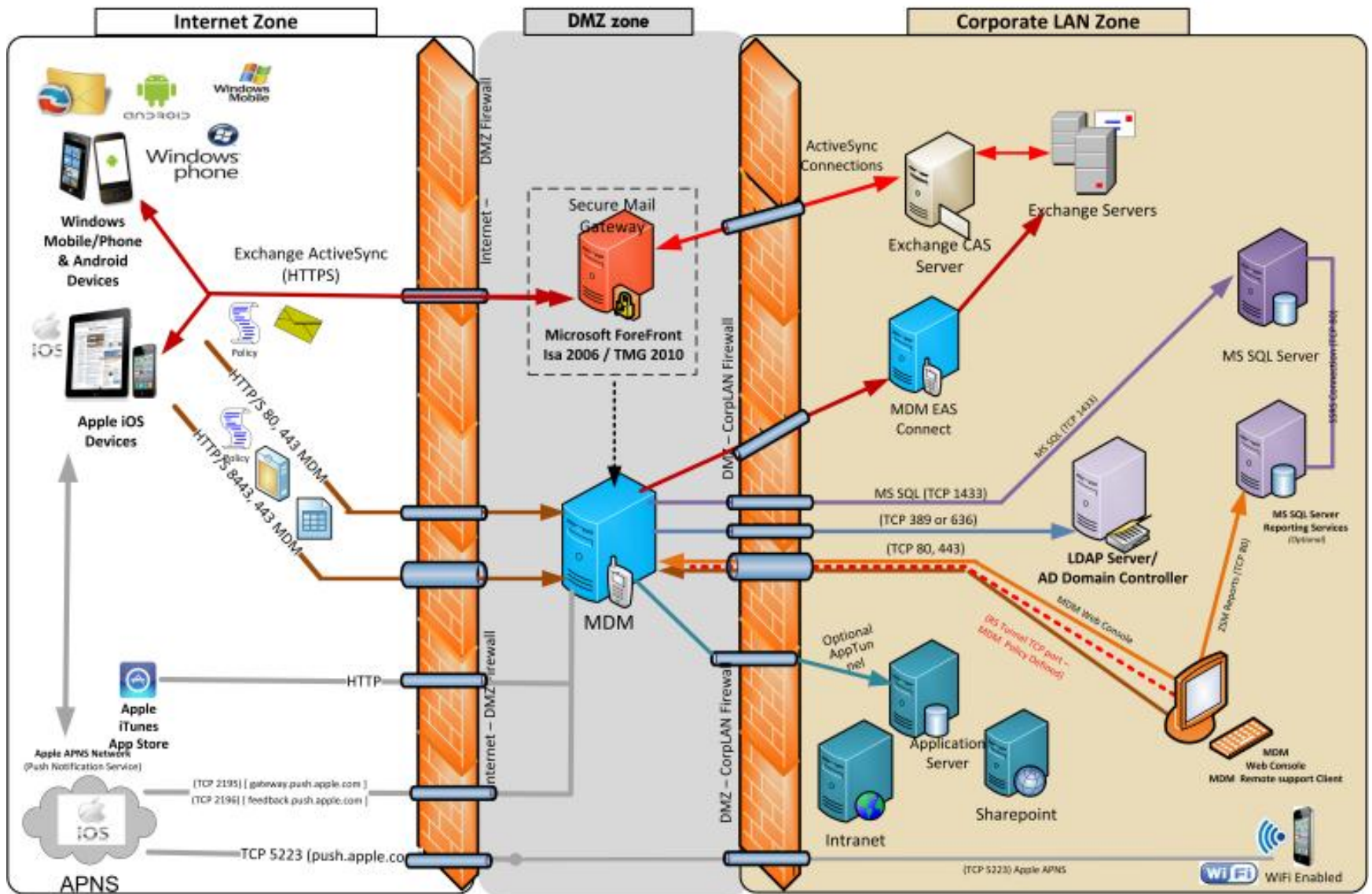
---

- Diverse devices chosen based on role and work mode at that moment
- Local device storage is authoritative for nothing
- Data may optionally be cached on any device
- Seamless secure access to all data from any device
- PC Backup as we know it does no longer exist
- Data is discoverable, available, compliant
- Trust model **shall be** in place

# MDM Server or Service?



# Network Architecture – MDM

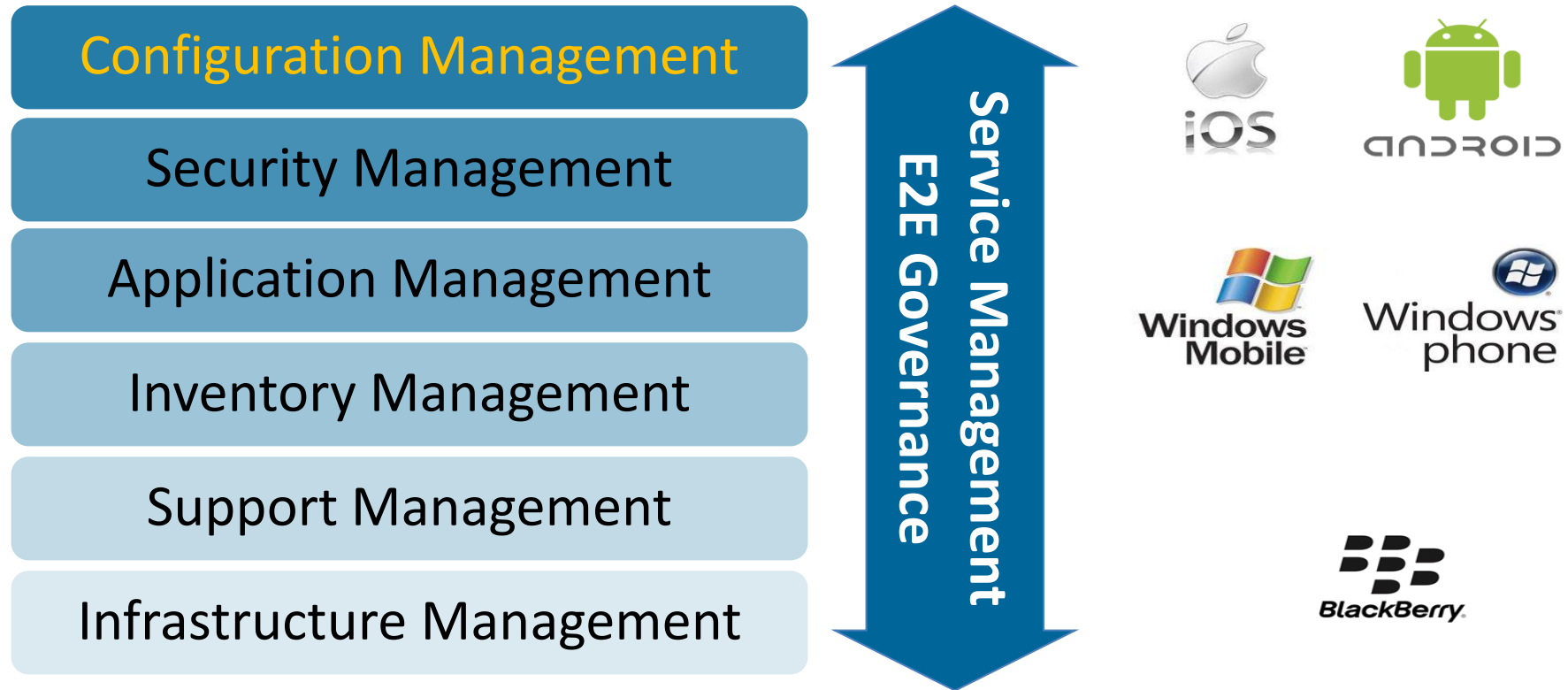


# Steps towards Enterprise Mobility

---

1. Leverage HP Mobility Services
2. Integrate with EAS
3. Add Secure Gateway
4. Add advanced security / configuration
5. Build Enterprise App Store
6. Start building X-Platform Apps
7. Add DLP functionality
8. Add Advanced App Security

# HP MMS – Service Scope



- Cloud, Hosted or On Premise
- Multi-Platform End-to-end Service
- Smartphones, Tablets and Ruggedized devices

# HP Mobile Workplace Services



- Holistic Service Integration
- “**anywhere at any time**” access to information

# Recent Success Stories & Benefits

---

- **KoneCranes**
  - 3000 ruggedized devices, end-to-end service, On-site Service
- **Trucking Company**
  - 2000 Enterprise SmartPhones, Support, Dedicated Cloud Service
- **Hospital**
  - 1000 devices (Clinical, Company owned & BYO) On-Site Install
- **Bearing Manufacturer**
  - 8000 Devices, 24x7 support, Application Mngmt, Procurement, Hybrid Cloud Service
- **Brewery**
  - 2000 x-platform devices, 24x7 Support, Cloud Service

# HP leader in mobility services

- **2M+** mobile handheld subscribers
- **237K** devices encrypted
- Global carrier relationships
- Mobile messaging supported in **50** countries
- **10+** years providing Mobile Application Services
- Key alliances Microsoft, RIM, SAP, Boxtone etc.
- Proven, global delivery methodology and tools based on best practices





# Thank you for your attention



# Why MMS - Enterprise

- Consumerization: BYOD
- Data protection and compliance practices
- Track, monitor and authorize data access
- Enterprise app stores
  - only approved apps can be downloaded
  - only devices with approved apps installed can access corporate resources
- Implement security solutions to remove problems that have already infected devices
- Data security is main driver, device management required layer

# 10 Steps to a multi-device Future 1

- Charter a **Mobility Council** to drive Management and Security Strategy
- Segment users based on **mobile requirements** and associated security risks
- Employees, Partners, Consultants, Customers and VIPs
- Tier devices, implement an Enterprise Mobility Solution
- No “One-Size-Fits-All” approach
- Your business is mobile – deliver your **business applications** multiplatform
- Prioritize and stage mobile app portfolio, build Enterprise app store

# 10 Steps to a multi-device Future 2

---

- Master multi-platform development
- Native app, HTML5, cross-platform, desktop virtualization
- **(Re)Fund** mobile network, access, and security infrastructure
- Adopt reimbursement policies that **align costs** with business benefits
- **Educate**, inform, build consensus
- Fast-track, **partner** with HP