

BYOD & MOBILE SECURITY: EMPOWERING EMPLOYEES WHILE SECURING CORPORATE ASSETS

Damian Bach

AirWatch

Security in
knowledge



Current & Future Mobile Landscape

- ▶ Number of mobile phones will exceed world population by 2014
- ▶ By the end of 2014, the number of global mobile users accessing the Internet is expected to surpass the number of desktop Internet users
- ▶ Today, 90% of U.S. workers are BYODers.
- ▶ 92% of BYODers access their own smartphones for work every week – 62% at least every day and 30 % at least once per week
- ▶ Total smartphone shipments worldwide are expected to reach 1.03 billion by 2015

Key Trends in the Evolution of Mobility

Past

Security infrastructure
Compromised detection
Device lock and wipe
Passcode policy
App distribution
Email management
IT influence

25+ years of one-size-fits-all approach to workplace technology

Present

App SDK
App Wrapping
Content management
BYOD
IT infrastructure integration
Granular privacy policies
Legal influence

82% using personal smartphones/tablets for business purposes

Future

Systems consolidation
Business system integration
Device, laptop, peripherals
Content filtering
Web gateways
Law and regulation influence

56% businesses are looking at mobility to improve productivity

Business Challenges

- ▶ IT Departments are faced with several challenges that come with managing a variety of employee-owned devices and operating systems
 - ▶ Network access
 - ▶ Network security
 - ▶ Data Loss Prevention (DLP)
 - ▶ Lost and stolen devices
 - ▶ Supporting new and unknown equipment

— What is BYOD?

- ▶ According to top analysts, Bring-Your-Own-Device (BYOD) is “an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data.”



Bring Your Own Device (BYOD) Programs



— BYOD Program Benefits

- ▶ **Employee Enablement**
 - ▶ Support all operating systems and latest device models
 - ▶ Enable employees to choose the most productive device
- ▶ **Security and Risk**
 - ▶ Configure security policies based on device ownership
 - ▶ Secure access to enterprise resources, apps and content
- ▶ **Privacy and Transparency**
 - ▶ Configure info collected based on device ownership
 - ▶ Isolate and protect both corporate and personal data
- ▶ **Cost Control**
 - ▶ Reduce procurement and provisioning costs
 - ▶ Focus resources on strategic mobile initiatives

What Does a BYOD Program Mean for IT Support?

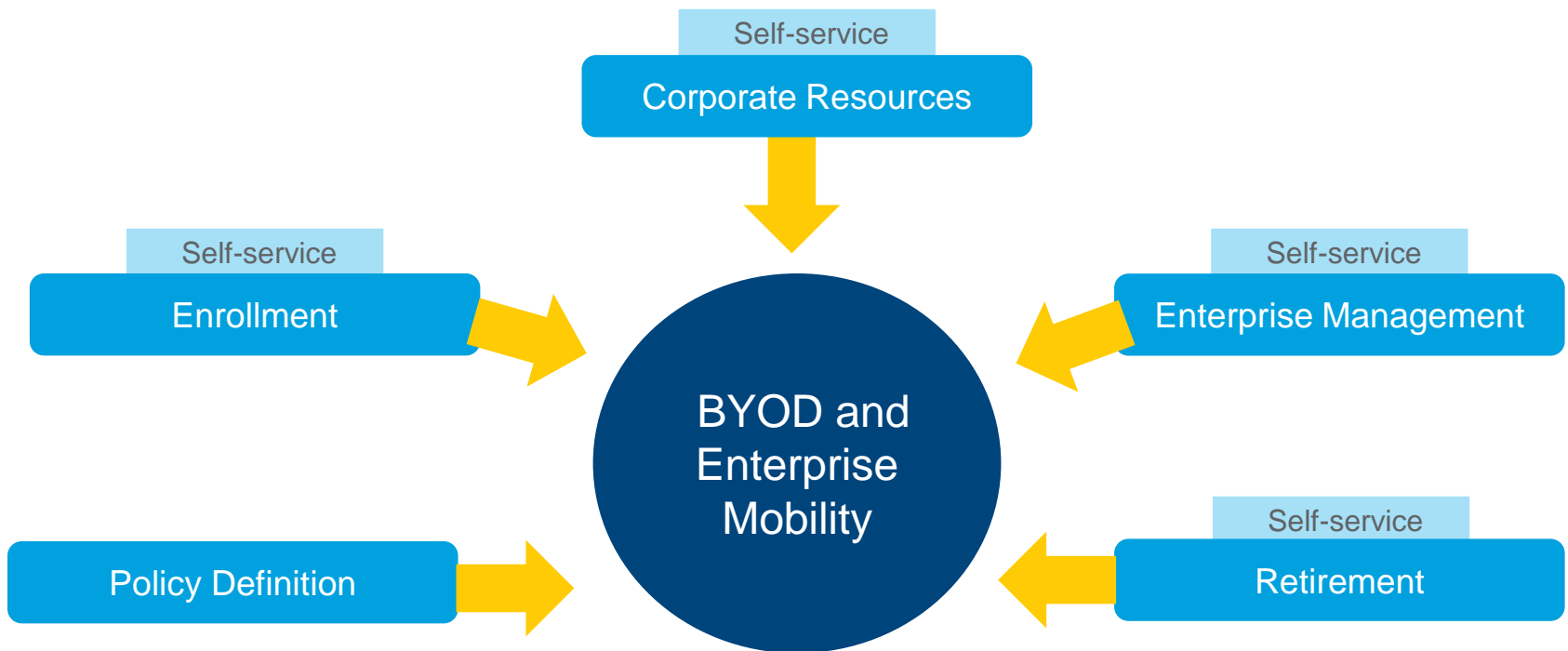
- ▶ The IT department can rid themselves of the costs of mobile devices due to the preference of employees to use their personal devices at work.
- ▶ IT can outsource the cost of some of the company's cost of these devices, employee services, etc.
- ▶ Companies can use the money set aside for purchasing thousands of dollars' worth of devices and data plans to provide support for those devices with maintenance .
- ▶ IT can take more time to focus on issues surrounding financial benefits and operational benefits.

Keeping Data Secure on Your Mobile Device

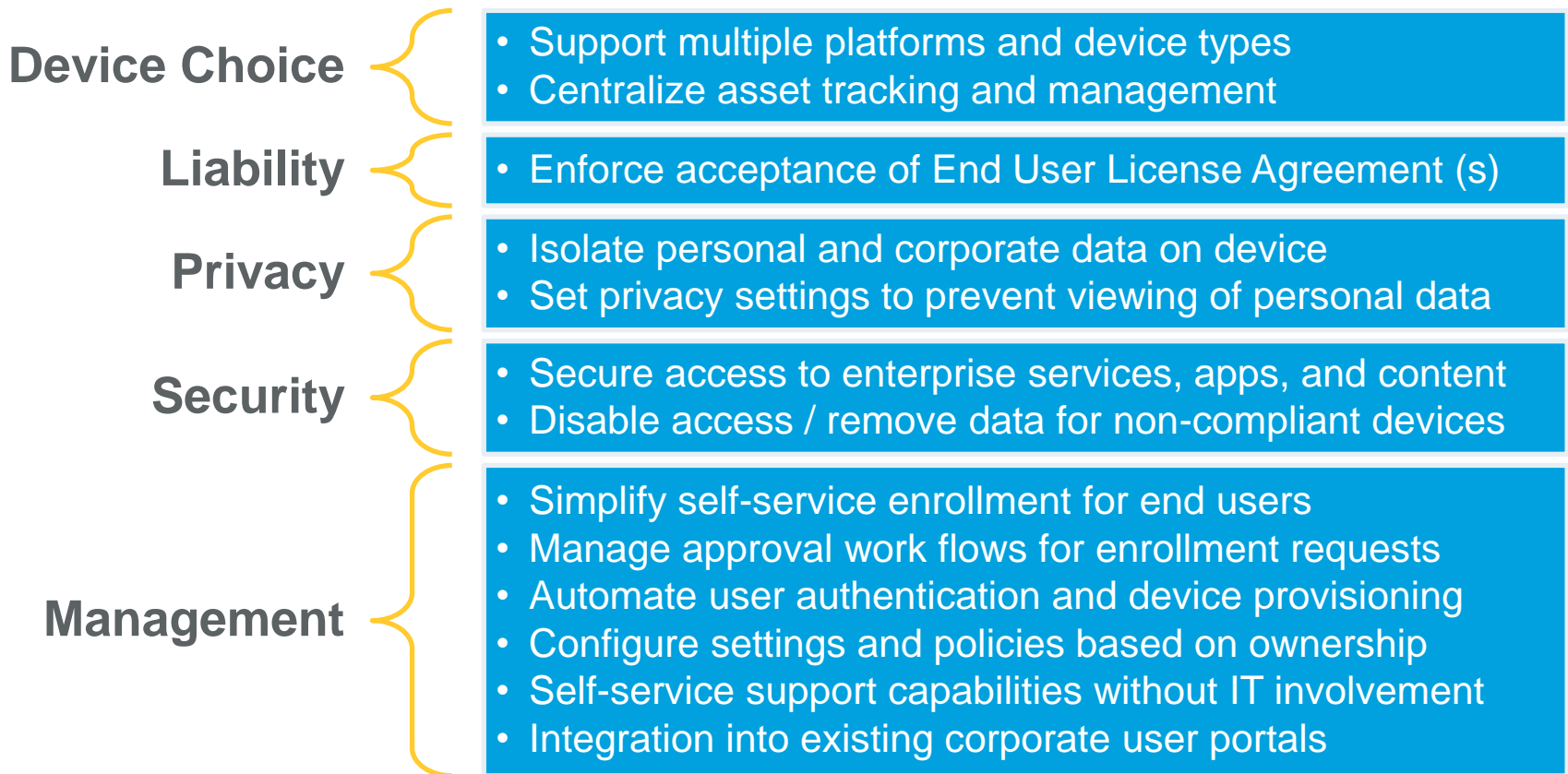
- ▶ Device ownership
- ▶ Terms of Use agreements
- ▶ Device and user authentication
- ▶ Data encryption
- ▶ Compromised device detection
- ▶ Remote data wipe



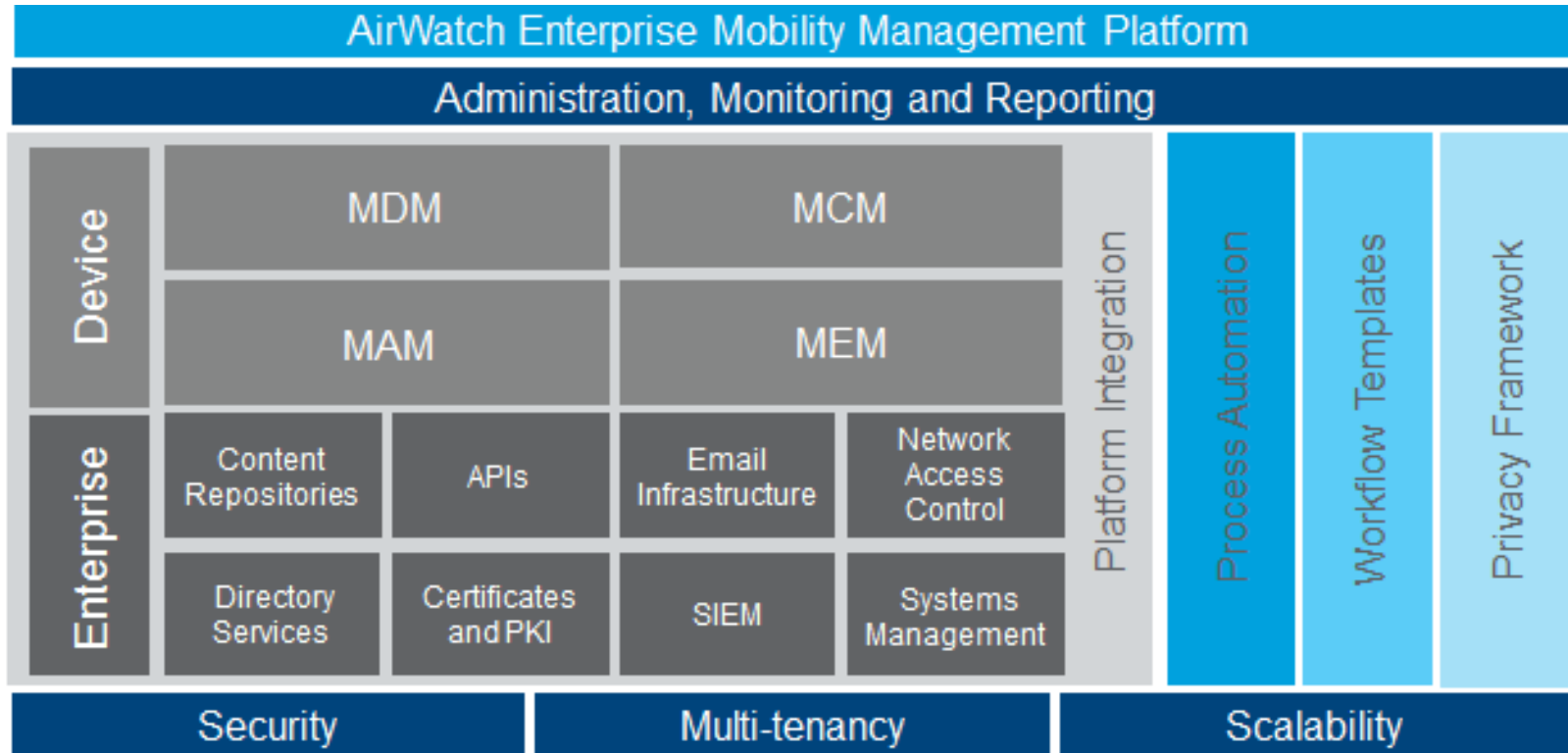
BYOD Lifecycle



EMM is Key Enabler for BYOD Programs



Technology Platform



RSA[®] CONFERENCE ASIA PACIFIC 2013

