

Enterprise Mobile Device Management

Shenandoah Valley Technology Council
March 20, 2014

Presented by:
Michael J. Rozmus
Vice President, Information Services
Sentara RMH Medical Center

Speaker Disclosure

Michael J. Rozmus, VP, Information Services
Sentara RMH Medical Center

I have no financial relationships, affiliation or other relationships with the manufacturer of any commercial product or competing products referenced in this presentation.

Mobile Device Management (MDM)

Def: A **Security Software Solution** used to monitor, manage and secure mobile devices used to access corporate resources across multiple mobile service providers, devices, and operating systems used by the organization.

Source: Webopedia.com

MDM Business Drivers

- Mobile Device Management (MDM) has been driven by a combination of:
 - rapid advancements in mobile technology
 - “consumerization” of mobile technology
 - mobile workforce business advantage
 - compliance, regulatory and data security

Mobile Computing has come a long way...



To Tablets...

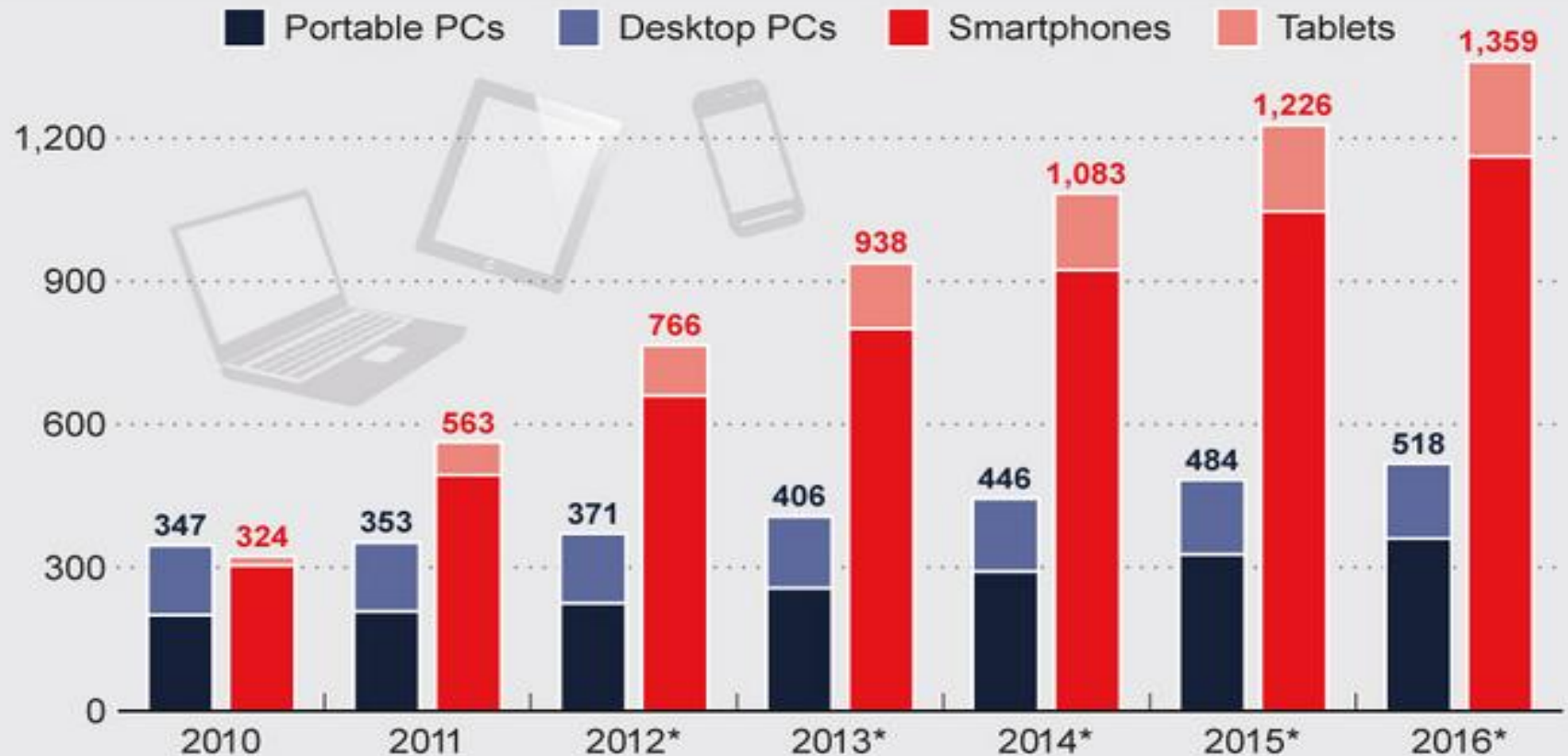


... and Smartphones



The Post-PC Era Has Arrived

Global smartphone, tablet and PC shipments (in millions)



Mobility and the Enterprise User



Source: Airwatch.com



35%
of U.S. adults have
had a mobile device
STOLEN OR LOST

Yet, **2/3** of people **DON'T USE**
MOBILE SECURITY APPLICATIONS
that could help them protect data
when someone else has the device.



Although **73%** of us are aware of the Increased **security**
risk of public WIFI, **66%** still connect to public networks



69%
of those surveyed
DO NOT BACK UP
THEIR PHONE DATA



64%
of those surveyed
DO NOT USE A
SCREEN LOCK OR
PASSWORD TO
ACCESS THEIR DEVICE

Source: Bluecoat.com

Regulatory and Compliance increasing across all industries



Source: [google.com/images/bccampus.ca](https://www.google.com/images/bccampus.ca)

Business Need vs. Mobility



Primary MDM Features

- Enforce data encryption
- Require a device passcode with timeout
- Remotely reset the passcode
- Remotely lock the device
- Enforce device restrictions (applications, etc.)
- Track the device's location
- Perform enterprise or device-level wipe
- Send push notifications

Deployment Options

- **Premise Based** (Corporate Network)
- **Software as a Service (SaaS)** – managed by local administrators, cloud based deployment
- **Managed Service** – 100% outsourced administration and management of platform.

MDM Primary Use Cases

- Corporate Owned Devices
 - 100% managed, dedicated to corporate use
- BYOD (Bring your Own Device)
 - Enterprise “container” on personal device
 - BYOD Policy imperative to define corporate data use and monitoring practices

The MDM Landscape

Gartner Magic Quadrant – May 2013

- 51 MDM Companies Represented
- 18 made the Chart



Source: Gartner

Gartner MDM “Leaders” Quadrant



Source: Gartner.com

20

Key Elements of a Successful MDM Deployment

STRATEGY

- Technology
- Policy
- Education
- Support

Key Elements of MDM Deployment



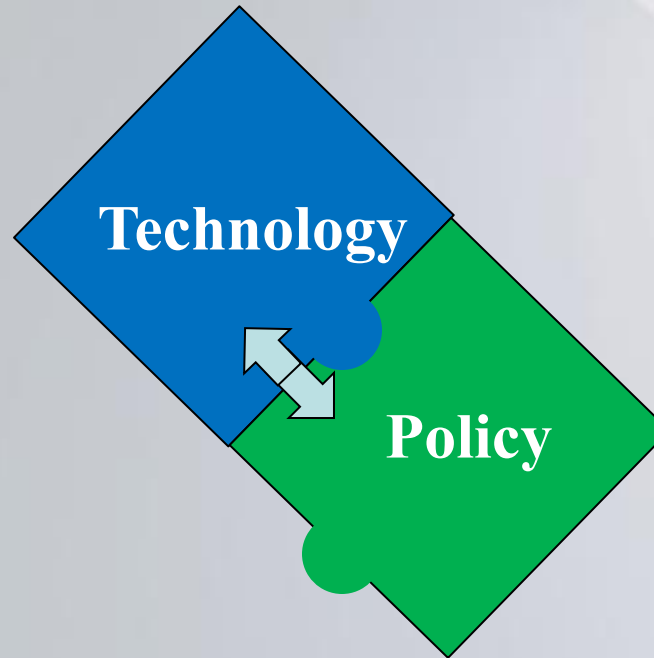
The Technology implements, monitors and enforces the corporate policy

Key Elements of MDM Deployment

People Policy:

Company EULA

- Corporate Data Management
- Compliance/HR
- Personal Device Use Policy



Device Policy:

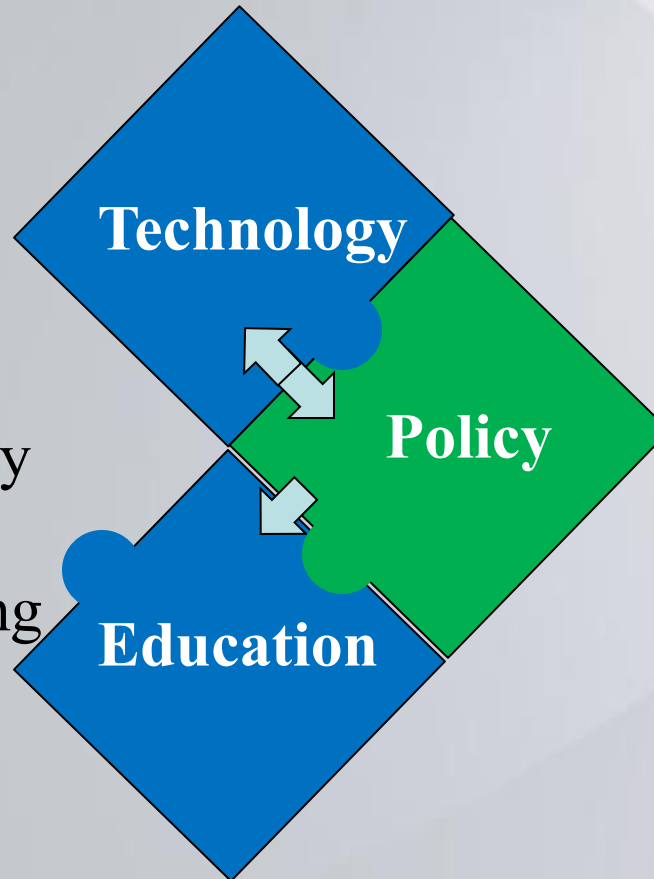
- PIN capable
- Auto Lockout
- Encryption
- Remote Wipe
- Patch Mgmt.

A written, management supported mobile policy is essential to success

Key Elements of MDM Deployment

Education:

- Safeguarding Devices
- Corporate and personal data protection
- Timely data and security incident reporting
- Basic user understanding of cybersecurity threats

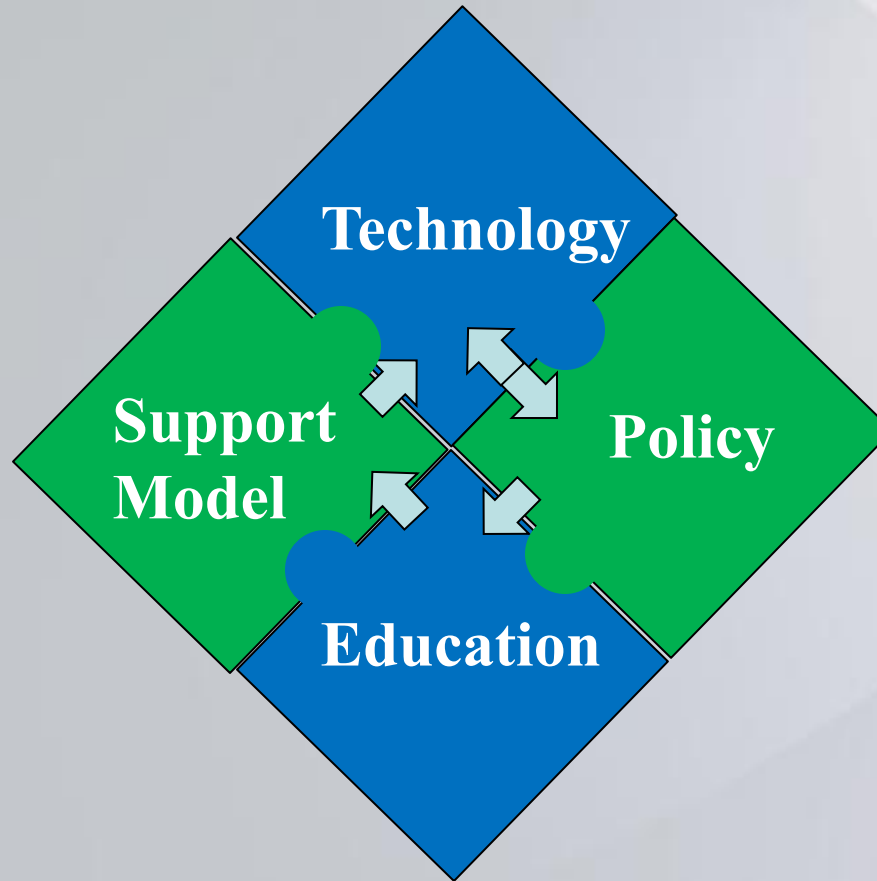


*End User
Education is key!
The weakest link
in the MDM
program is often
end user
compliance*

Key Elements of MDM Deployment

Support Model:

- Device Support (Corporate)
- SLA for Personal Devices



The support model needs to place a high responsibility for self service for customer owned devices.

The Sentara MDM Pilot

- Scope: 370 Corporate Owned Devices
(mostly iPhone and iPads)
- Several MDM solutions evaluated
- Technical Issues:
 - Shared Devices
 - Some non iDevices failed with native mail client
 - Profiles created for unique application/device combinations – increased administration
- NonTechnical: License renewals

The ongoing challenge of mobile, an adolescent technology

MDM Limitations

Mail+ for Outlook

By iKonic Apps LLC

Open iTunes to buy and download apps.

[View More by This Developer](#)



[View In iTunes](#)

+ This app is designed for both iPhone and iPad

\$5.99

Category: [Business](#)

Updated: Dec 30, 2013

Version: 3.4.8

Size: 26.5 MB

Languages: English, Chinese, Dutch, French, German, Italian, Japanese, Korean, Portuguese, Spanish, Traditional Chinese, Turkish

Seller: iKonic Apps LLC

© iKonic Apps LLC

[Rated 4+](#)

Compatibility: Requires iOS 6.1 or later. Compatible with iPhone, iPad, and iPod touch. This app is optimized for iPhone 5.

Description

#####

- Securely access Outlook Email and Calendar
- TOP 5 business apps for last 12 months

[iKonic Apps LLC Web Site](#) > [Mail+ for Outlook Support](#) >

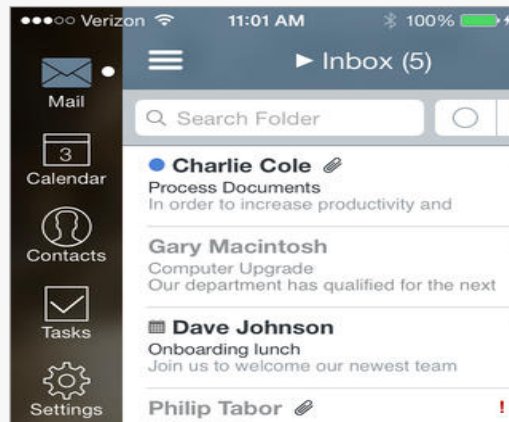
[...More](#)

What's New in Version 3.4.8

- Connection fixes

Screenshots

iPhone | iPad



Source: Apple Store

Enterprise Mobility Challenges

Business / IT Change

- Consumerization of IT – with or without BYOD Policy
- Anytime, anywhere, business mobility expectation
- Personal and business interactions intersect

Security and Compliance

- Data Loss Prevention and Regulatory Compliance
- Policy for corporate and employee owned devices
- Security Administration of Mobile policies

IT Lifecycles

- Complexity of devices, OS, platforms (tablets/phones)
- Consistent Application Delivery to mobile devices
- Asset /License Management / Decommissioning

In Summary

- Mobile device technology and consumerization are driving corporate IT toward Mobile Device Management
- MDM niche is immature with lots of players
- A company with a defined strategy for MDM which addresses the non technical elements will be most successful

Thank You

8/31/08

31

