Mobile Security
Market Trends and Best Practices
24 May 2013
Agenda

- Mobile Market Trends
  - Mobile Security Challenges
  - Mobile Security Options
  - Mobile Security Best Practices
BYOD Growing Rapidly

Personal mobile device use in the workplace

47 percent of respondents say that more than half of their employees are BYOD

Source: Ponemon Institute, 2013 State of the Endpoint study, December 2012
Mobile Trends

By 2015, smart device shipments to exceed 1 billion units

76% of organizations support BYOD

By 2015, mobile app projects outnumber PC app projects by 4:1

50% of employees take business data onto personal devices

Security implications of supporting smart devices concern 43% of IT executives
Mobile Apps Have Taken Off

Worldwide Mobile App Store Total Revenue ($M)

Source: Gartner, Market Trends: Mobile App Stores, Worldwide, August 2012
Agenda

- Mobile Market Trends
- Mobile Security Concerns
- Mobile Security Options
- Mobile Security Best Practices
Data loss & lack of data segregation are top concerns

1. The lack of segregation between corporate data/content and consumer data/content: 58%
2. Enforcing acceptable usage policies on mobile devices: 53%
3. The lack of data protection or DLP capabilities on mobile devices: 72%
4. Data loss due to device loss or device theft: 75%
5. Mobile malware: 53%

Base: 859 IT security decision makers. Source: Forrsights Security Survey, Q2 2012
No Separation of Personal & Work

Email, contacts, appointments – includes personal and corporate data
Deployed Protection Measures Not Mature

- MDM: 21%
- Application sandboxing: 10%
- VDI for mobile: 13%
- Device security functions (pwd, lock, wipe), very little else: 38%
- No data protection on mobile devices: 23%
- Other technology: 2%
- Don't know: 3%

Base: 1103 IT security decision makers. Source: Forrsights Security Survey, Q2 2012
Agenda

- Mobile Market Trends
- Mobile Security Concerns
- **Mobile Security Options**
- Mobile Security Best Practices
Mobile Device Management (MDM)

- Initially the only tool available
- Appropriate for specific situations
  - Corporate-liable devices
  - Kiosk / retail devices
- Often inappropriate for growing classes of devices
  - Devices you don’t own – i.e., employee-owned (BYOD), extended enterprise (distributors, business partners)
- Potential privacy implications

**Misses the point.**
It’s about the **data**, not the **device**.
Mobile Management Market is Evolving...

Visionary

Strategic

Mobile Management (EMM) – B2B, B2C

Extended Enterprise MAM (B2B)

Enterprise MAM (B2E)

Tactical

…and so is the customer

- IT/Security began by solving tactical security problems with MDM

- LOBs now creating apps for non-employees & need distribution (no MDM)

- Wrapping technology shifts buyers and users
Collaboration is Critical

**Table Stakes**
- Email
- Calendar
- Contacts

**Competitive Advantage**
- Forecasts
- Rh Analyzer
- Productivity
- Approval
- Shuttle
- Inventory

... and much more.
MAM gets a lot of mindshare

What are your firm's plans to adopt the following mobile technologies?

- Enterprise app store: 24% Interested but no plans, 12% Planning to implement, 8% Already invested
- Mobile application management: 26% Interested but no plans, 25% Planning to implement, 17% Already invested
- Mobile device management software: 25% Interested but no plans, 27% Planning to implement, 23% Already invested

Base: 1282; Source: Forrester's Forrsights Hardware Survey, Q3 2012
Mobile Application Lifecycle

- Procure
- Provision
- Distribute
- Track (license, entitlement)
- Rate & Review
- Analyze (usage)
- Update
- Decommission
Agenda

- Mobile Market Trends
- Mobile Security Concerns
- Mobile Security Options
- Mobile Security Best Practices
Recommended Mobile Security Best Practices

1. Understand use cases
   - What do people need to be successful in their role?

2. Secure application data

3. Enable secure workflows

4. Automate management to reduce risk and cost
Understand Use Cases

Executive
BYOD
Personal tablet
Board docs

Sales
BYOD
Personal tablet
Customer deck

Nurse
Corporate liable
Share tablet
Patient records
Secure Apps and Data

Containerize App!

- Separates personal from corporate
- Controls at the app level
- Application password

The right Container

- Minimizes data loss even if the device is compromised
- Lets IT say “yes” to users!
- Enables secure workflows
Enterprise App Store

- Moral equivalent of disk image for mobile devices
  - Employees know what’s approved
- Private, brandable, enterprise app store
  - It’s your enterprise’s face on the mobile device
- Consumer-like experience
  - Ratings & reviews, search/browse, categories
- Employees and beyond
- IT management of user device not required
Enable Secure Workflows
Industrial Manufacturer Workflow

1. Connect measuring apparatus to iPhone
2. Launch custom measuring app
3. Record various thicknesses of a component
4. Capture defects with custom camera app
5. Markup image and describe defects with iAnnotate
6. Email image and measurements to next production station to fix

- Increased employee productivity
- Lowered equipment costs
- Constant information protection
- Higher production yields
Automate Management

Exponential Cost, Complexity & Risk

Secure Mobile User Enablement with Reliability, Economies of Scale, & Risk Reduction

Devices x Users x Apps

Endpoints

Security + Support + Operations

Time

REAL-TIME VISIBILITY

AUTOMATION

© 2013 Good Technology, Inc. All Rights Reserved.
Summary

1. BYOD is here – it’s all about the apps
2. Embrace and transform
3. Mobile security is an enabler
4. Security and user satisfaction are not mutually exclusive
Company Mobile Maturity Journey

Value of Mobility

Collaborative Apps, Existing Business Processes
Deliver, secure, & manage apps

Business Transformation through Workflows
(B2E, B2B, B2C), New Opportunities

Email, PIM, Intranet
Manage Device

Run
Grow
Transform

Mobile Maturity
Thank you