IBM BusinessConnect
Realise the art of the possible.

Going Mobile: Challenges, limits and impact of new smart devices

Keith Poyser: Sales Leader Europe.
IBM Mobility & End Point

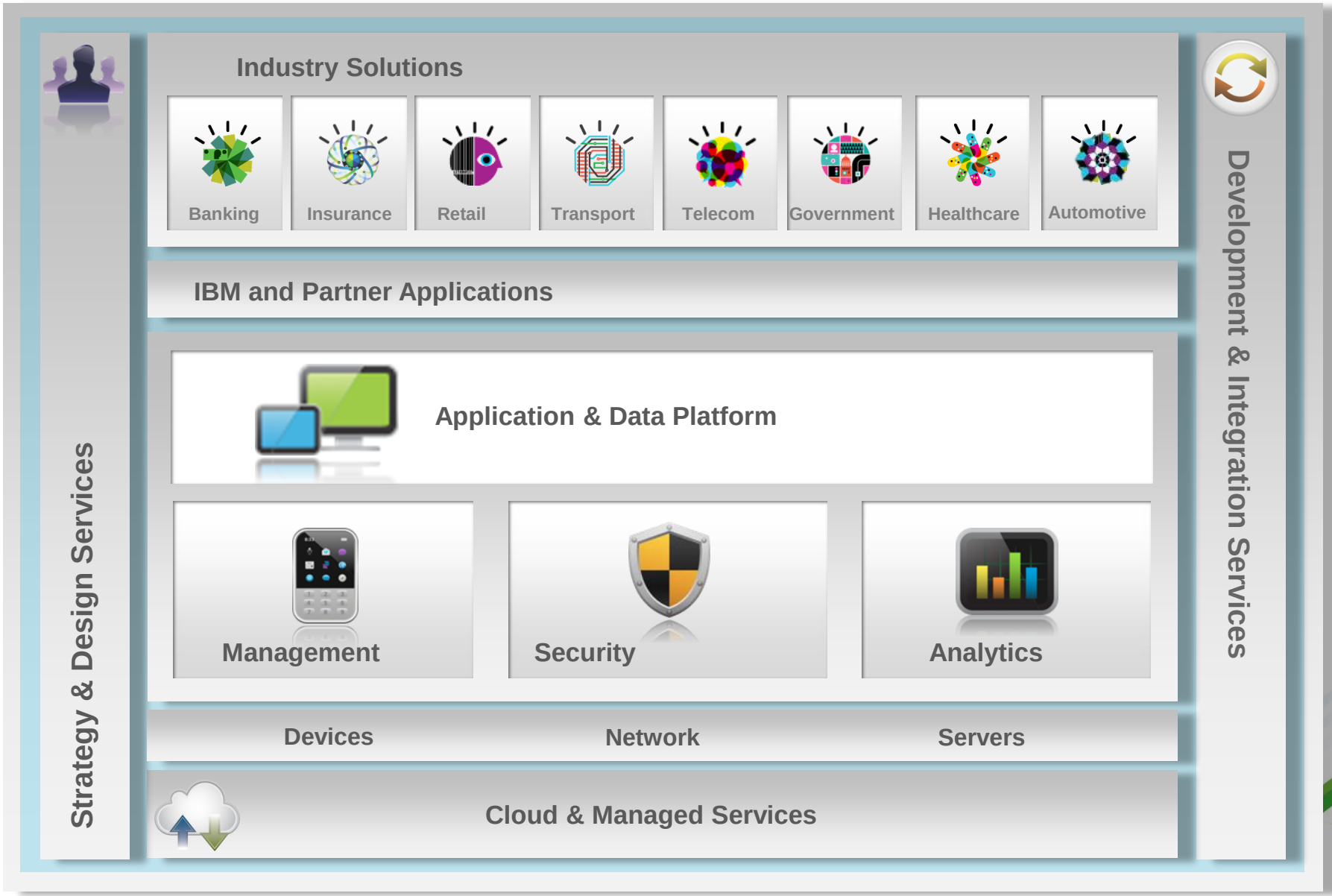
BYOD and Mobile is a mandatory transformation

10 Billion devices by 2020

61% of CIOs put mobile as priority

45% increased productivity with mobile apps

IBM MobileFirst: Breadth and Depth beyond Device



BYOD can help realise broader business objectives, with five in particular being targeted by interviewees

IT cost savings

67% believe BYOD will actually increase total costs

Need to consider: stipend, tax implications, infrastructure upgrades, support costs, security solutions, multi-device costs

~80% decision-makers of 500+ employee organisations based BYOD business case on productivity gains

Need to consider: work/life balance, potential inefficiencies, productivity cost of self support

Productivity gains

Employee satisfaction

40% of CIOs consider 'allowing employee choice of device' as key driver of BYOD

Need to consider: graduates and low basic wage targets, broader employee device schemes, device funding

Source: 2012 BYOD Survey, Liberman Software; Key Strategies to Capture and Measure the Value of Consumerization of IT, Forrester

BYOD can help realise broader business objectives, with five in particular being targeted by interviewees contd…

Understanding the consumer

- Consumers use a range of different devices so BYOD can help employees understand their customers
- Useful test-bed for customer-facing applications

Operational flexibility

- Frequently overlooked as a BYOD benefit
- Particularly relevant for the following scenarios:
  - **High growth phases** (e.g. technology start-ups)
  - **M&A is business as usual** (e.g. oil and gas majors)
  - **Workforce is highly contractor-based** (e.g. broadcast media
  - **Improving flexible working and business continuity**

Bring-Your-Own-Device represents a broad spectrum of devices, capabilities and responses

Devices



Capabilities

Wi-Fi access and webmail ⟷ Full functionality

‘Flavours’

	Enterprise	Employee (BYOD)
As-a-complement		+ 
As-an-addition	*not eligible*	
As-a-replacement		

The CIO has three options: Tolerate, clamp down or provide a managed BYOD programme

1 **Tolerate unmanaged BYOD**

~ 50% of respondents reported that their employers did not know about BYOD or **turned a blind eye to it**

2 **Attempt a clampdown**

Over 50% of “20-something” workers believe that mobile device BYOD was a right not a privilege. 1 in 3 would break anti-BYOD rules

3 **Provide a managed BYOD programme**

The only workable option for most organisations and often intertwined with other programmes aimed at broader business objectives

Source: Ovum reveals firms face huge security risks as 80% of BYOD goes unmanaged, Ovum; Young employees say BYOD a 'right' not 'privilege', Network World

Security a Prime Concern…Mobile Widens the attack surface

Top 7 Most ATTACKED Industries

1. Health & Social Services
2. Transportation
3. Hospitality
4. Finance & Insurance
5. Manufacturing
6. Real Estate
7. Mining, Oil & Gas

Security Attacks

The Average Company Faces Per Week

2,641,350

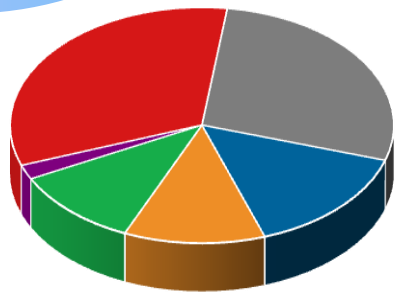
Top 5 reasons WHY attacks were possible

1. End user didn't think before clicking
2. Weak password / default password in use
3. Insecure configuration
4. Use of legacy hardware or software
5. Lack of basic network security protection or segmentation

62

Security Incidents
The Average Company Experiences Per Week

What IBM Sees



Categories of Attack

- Malicious Code
- Sustained Probe or Scan
- Unauthorized Access
- Low-and-Slow Attack
- Access/Credentials Abuse
- Denial of Service

BYOD challenges: IBM faces the same as our Clients

How do I support applications on multiple devices and secure data?

How do I provide secure access to the network?

How do I provide support for a variety of different devices?

IBM in a snapshot

435,000 + employees (+ contractors)

50% of employees are “mobile”

600,000 managed laptops/desktops (5% personally owned)

120,000 managed mobile devices (80% personally owned)

BYOD @IBM

BYOD = Bring Your Own Device
(*IAPD = IBM Authorized Personal Device*)

IBM has been supporting “BYOD” for many years

Mobile and consumerization of IT is simply accelerating

Key lesson : today’s employees simply expect it
…you can not stop it
…if you don’t enable it, employees will self enable

Role Studies helped show security and capability gaps

Employment Status: Full-time IBM

Country: USA

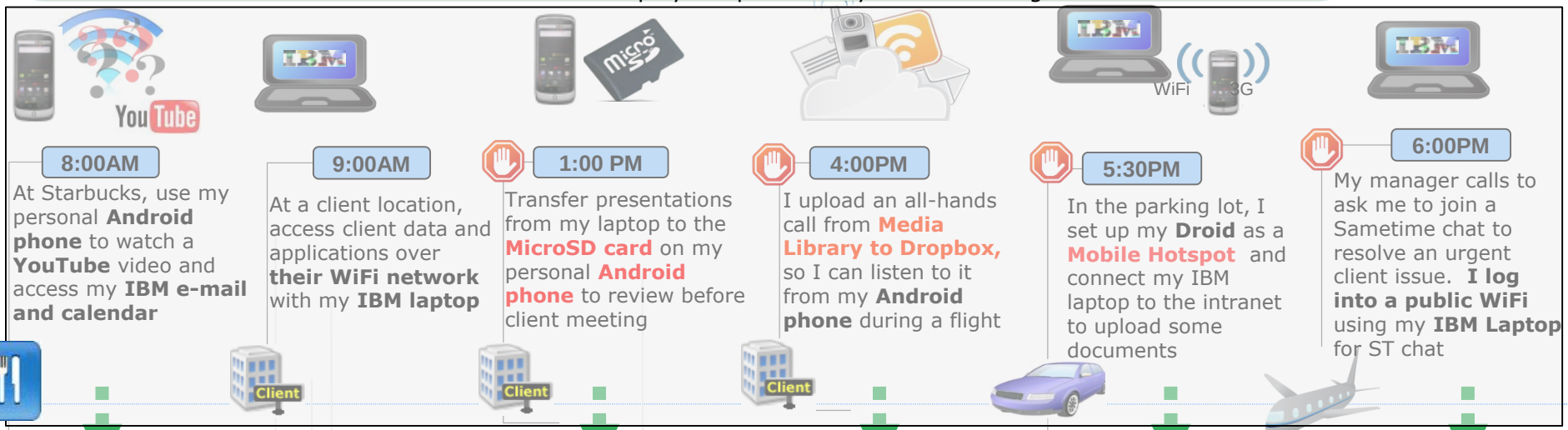
Equipment used: IBM laptop, personal Android phone

Environment: IBM, Client, Home, Public

SOLUTION

- ✓Malware protection and TEM enforcement allow Android devices to securely access IBM data and reduce malware threat
- ✓Encrypted MicroSD cards provide secure storage for IBM and client data
- ✓Tools such as My Mobile Hub provide secure solutions for cloud storage
- ✓Education on proper configuration of devices helps users keep their devices secure
- ✓Open access to key collaboration tools such as Sametime increase employees' productivity when traveling

Today (from user interviews)



8:00AM
At Starbucks, use my personal **Android phone** to watch a **YouTube** video and access my **IBM e-mail and calendar**

9:00AM
At a client location, access client data and applications over **their WiFi network** with my **IBM laptop**

1:00 PM
Transfer presentations from my laptop to the **MicroSD card** on my personal **Android phone** to review before client meeting

4:00PM
I upload an all-hands call from **Media Library to Dropbox,** so I can listen to it from my **Android phone** during a flight

5:30PM
In the parking lot, I set up my **Droid** as a **Mobile Hotspot** and connect my IBM laptop to the intranet to upload some documents

6:00PM
My manager calls to ask me to join a Sametime chat to resolve an urgent client issue. **I log into a public WiFi** using my **IBM Laptop** for ST chat

8:00 AM
I use my personal **Android** phone for **IBM e-mail and calendar**

1:00 PM
Transfer presentations from my laptop to the **IBM encrypted container on the MicroSD card** on the **Android** phone

4:00 PM
I upload the all-hands call file to **My Mobile Hub** and use my **Android** phone to listen during a flight

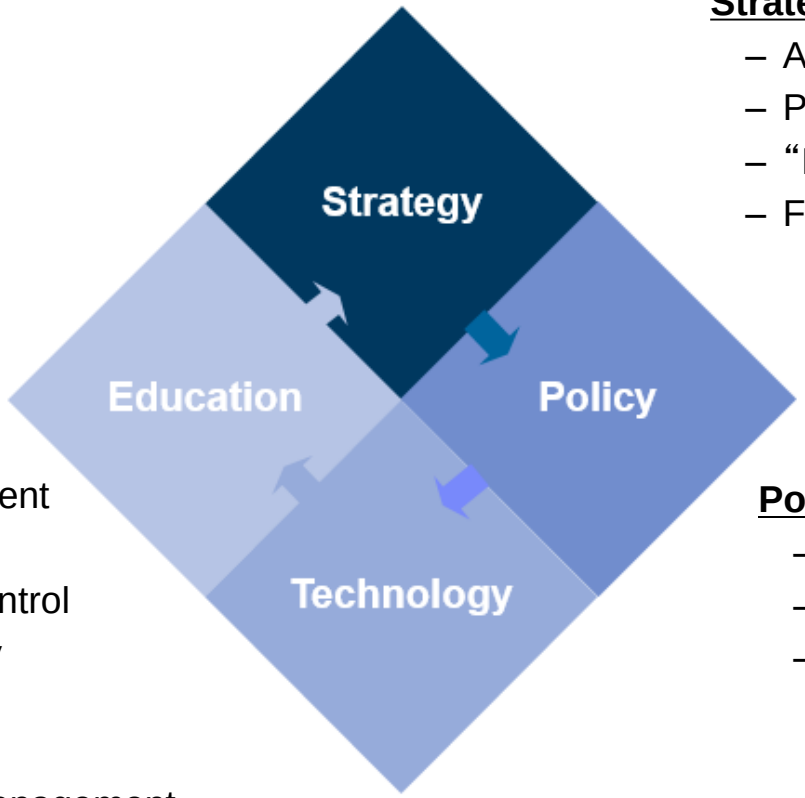
5:30 PM
I configure my **phone's hotspot** based on **IBM security guidelines** and then connect my IBM Thinkpad to it

6:00 PM
My manager calls to ask me to join a **ST chat**. I log-in to **ST using my Android device**

Technology is only 1 part of the Mobility Issue:

Education
- Formal
- Casual
- Social
- Developer

Strategy
- Acceptance
- Personas
- “Day In The Life”
- Funding Models

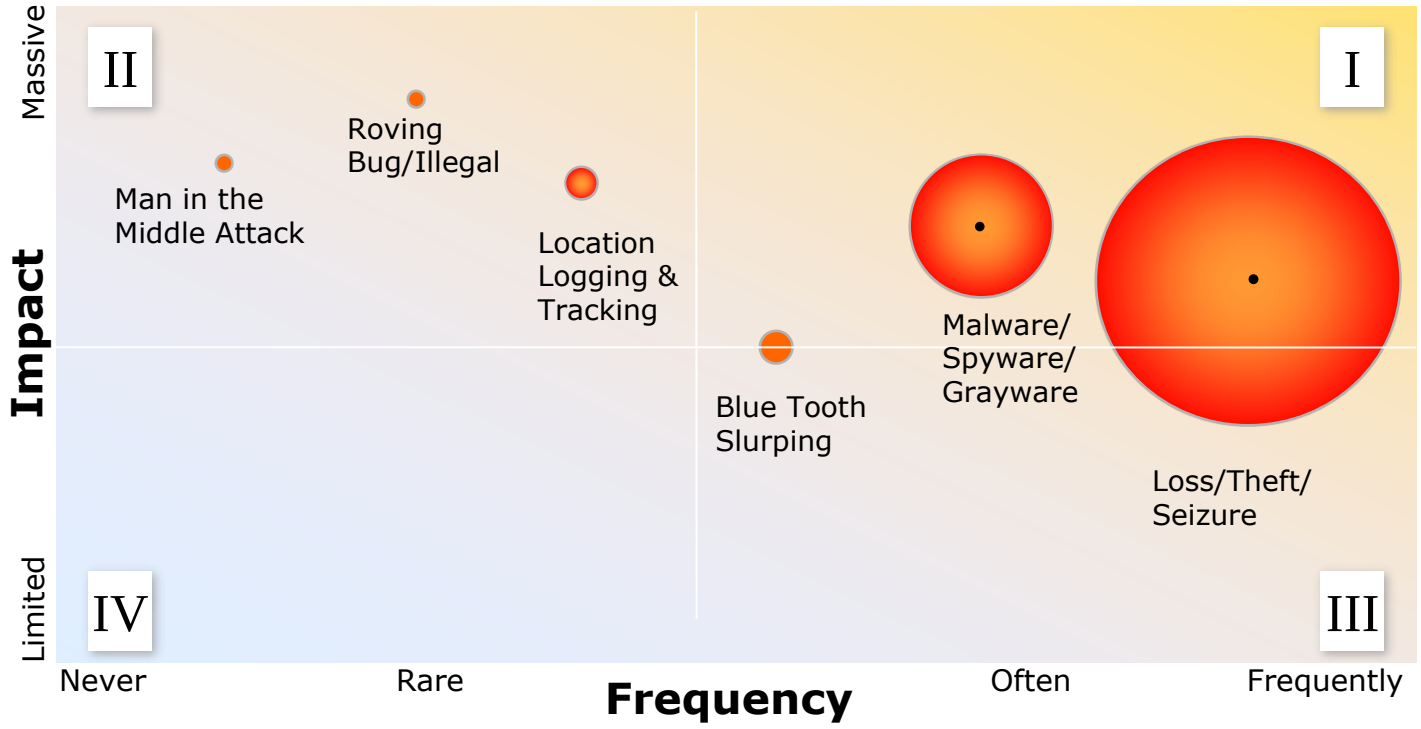


Technology
- Endpoint Management
- Anti-Malware
- Network Access Control
- Application Security
- Containterization / Virtualization
- UNIFIED Device Management

Policy
- Legal
- HR
- Technical Controls

The Device Layer: Why Manage…..

Based on Gartner, Mobile Security Risks, interviews with members of IBM ISS, IBM xForce, and Corporate Executive Board. e.g. Industry (not IBM only) view



Control Category I: Focus on risks for all mobile devices used by IBMers for IBM business purposes
Control Category II: Focus on risks for targeted populations of IBMers (ex. SVPs)

Solution Relevance: Broad, Multi Purpose, Single Solution.

IBM Endpoint Manager: *UNIFIED* Device Mngt..!

Network Discovery, Global Properties Inventory, Custom Fixlets, Wake-on-LAN, n-Tier Relay Architecture, Dynamic Bandwidth Throttling
SOAP APIs for integration with Service Desk, CMDB, SIEM, GRC, and other IT management, security, and compliance solutions

Lifecycle Management

- Endpoint HW, SW Inventory
- OS Deployment
- Asset Discovery
- Patch Management
- Software Distribution
- Remote Desktop Control

Software Use Analysis

- Endpoint HW, SW Inventory
- Software Usage Metering
- Software usage counting
- Basic license management

Power Management

- Power Policy management
- Power usage and cost reporting
- Automated shutdown and Wake-on-LAN

Patch Management

- Patch Management:
  - Windows
  - Mac
  - Linux
  - Unix

Server Automation

Mobile Device Management

- Apple iOS and Android Device Management
- Lotus Traveler and MS Exchange management
- Mobile Profile Management
- MDM HW, SW Inventory
- Remote Lock and Wipe
- Application Deployment
- Mobile Profile Management

Security and Compliance

- Security Configuration Management
- Vulnerability Management
- Asset Discovery
- Patch Management
- Network Self Quarantine
- Multi-Vendor Endpoint Protection Management
- Security and Compliance Analytics

Core Protection

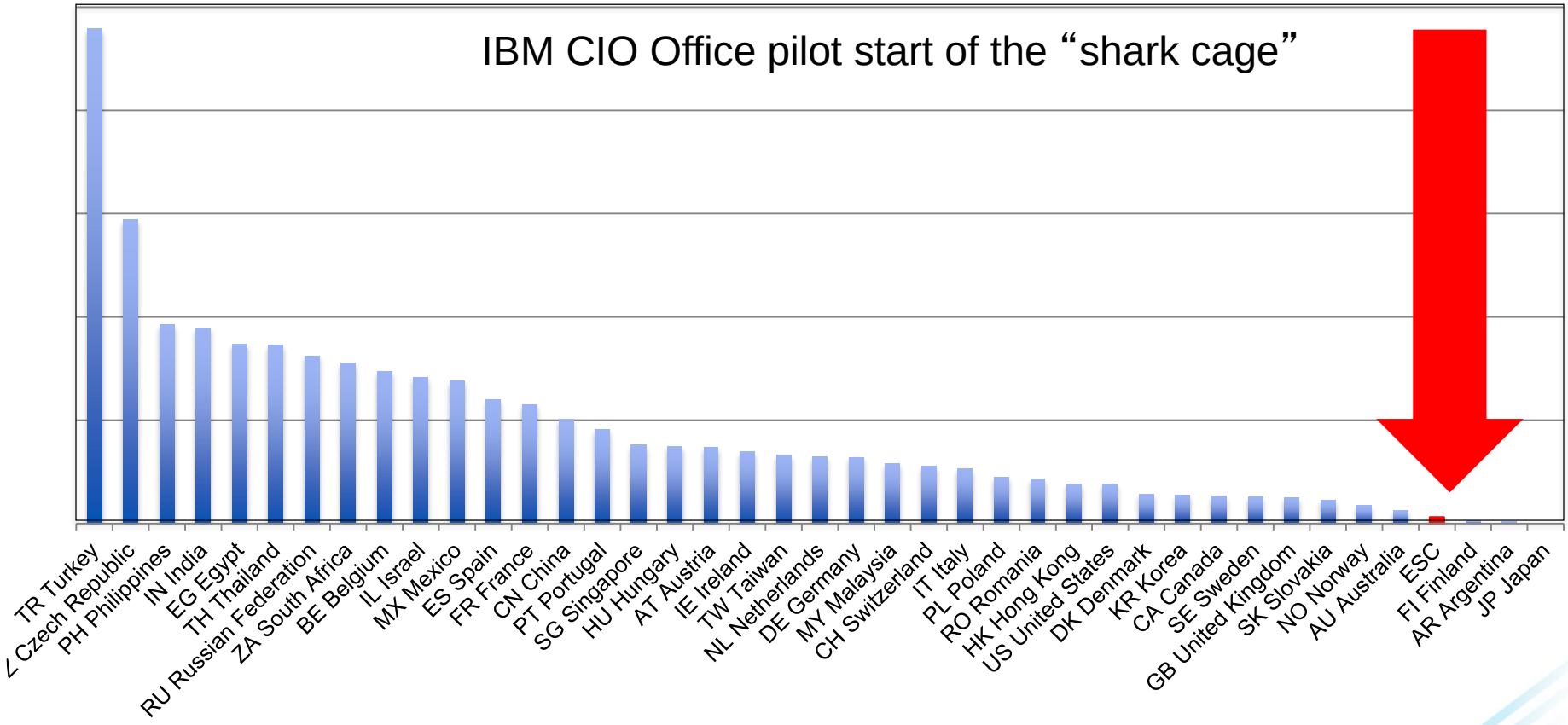
- Anti-Virus
- Personal Firewall
- File and web reputation
- DLP**
- Device Control**

** Data Protection Add-on

1 console, 1 agent, 1 server: 250,000 endpoints, 90+ OS versions

IBM Endpoint Manager Piloted in IBM Globally

Pilot Normalized ITMS infections



Normalized: ITMS detected malware per country divided by number of employees per country

IBM Pilot: Desktop “Shark Cage” Results:

BAU	BigFix
Patch availability typically 3-14+ days	*Patch availability within 24 hours*
92% compliance within 5 days (ACPM only)	*98% within 24 hours*
EZUpdate sometimes misses application of patches on required machines	Detected about 35% of participants missing at least one previous patch
Compliance model, completely reliant on user	*90% of Windows requirements can be automatically remediated*
Exceptions at machine level	*Exceptions at setting level*

Traditional Endpoint Management

- OS provisioning
- Patching
- Power Mgmt
- Anti-Virus Mgmt

Mobile Device Management

- Device inventory
- Security policy mgmt
- Application mgmt
- Device config (VPN/Email/Wifi)
- Encryption mgmt
- Roaming device support
- Integration with internal systems
- Scalable/Secure solution
- Easy-to-deploy
- Multiple OS support
- Consolidated infrastructure

- Device Wipe
- Location info
- Jailbreak/Root detection
- Enterprise App store
- Self-service portal

IBM's internal Endpoint management convergence: EXTENDING SHARK CAGE TO DEVICES

- Convergence = one management solution to rule them all

- Why does this matter?
  - Cost/Efficiency
  - Compliance and reporting
  - Role-based management

- Central control of mobile security proliferation
  - Mobile management market still immature.
  - Many tactical and point products still needed
  - Ultimately inefficient and complex

- Consistency across all endpoints
  - Tablets and smartphones are really just computers
  - Easily extend security standards to new devices
  - Single View e.g Blacklisted Application from Server to Desktop to Smart Phone

Ensuring you Secure Sensitive Data, Regardless of the Device

How do I ensure the security of mobile devices as they access more and more sensitive systems?

Unified compliance reporting across all devices, including CIS Benchmarks

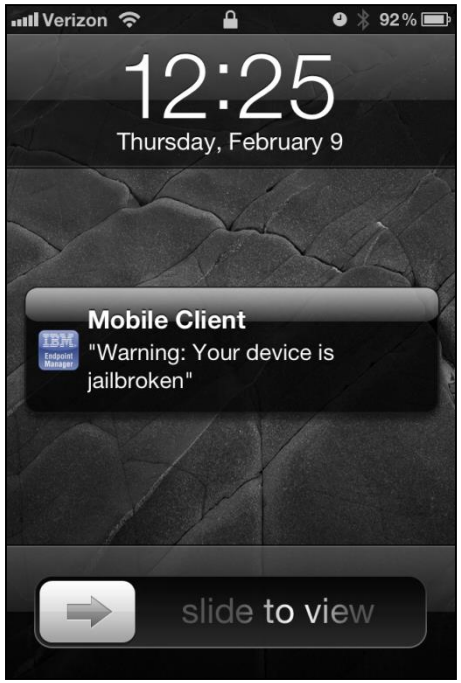
Configure security settings such as password policy, encryption, WiFi, iCloud sync

Full wipe, remote lock, map device location, and clear passcode options if device is lost or stolen

Blacklist apps and automate alerts, policy response

Detect jailbroken / rooted devices to notify users, disable access

Integrate with mobile VPN and access management tools to ensure only compliant devices are authorized



Multiple user communication and alert methods, including Google Cloud Messaging (GCM), enables users to be part of the security solution.

Benefits of an Endpoint Manager based Approach to Mobile Device Management …The analysts agree.

- "Organizations…would prefer to **use the same tools across PCs, tablets and smartphones**, because it's increasingly the same people who support those device types"

  – Gartner, PCCLM Magic Quadrant, January 2011

- Although at some level mobile is unique, **the devices are just another form of endpoints in your infrastructure**. This means whichever technologies you procure should have a road map for integration into your broader endpoint protection strategy.

  – Forrester, Market Overview: Mobile Security, Q4, 2011

Reduces Hardware & Administration Costs

- "Single pane" for mobile devices, laptops, desktops, and servers
- Single Endpoint Manager Server scales to 250,000+ devices
- Unified infrastructure/administration model reduces FTE requirements

Fast Time-to-Value

- Enterprise-grade APIs enable integration with service desks, CMDBs, etc (Integrated Service Management)
- Cloud-based content delivery model allows for rapid updates with no software upgrade or installation required

Now in IBM BYOD, policy starts with legal & HR, then Technology.

IBM Terms & conditions for personal devices include topics such as:

Employee will:

- Understand use of the device is governed by enterprise rules (conduct guidelines)
- Allow installation of enterprise management agents (and freedom of their operation)
- If requested, allow inspection/possession of device by enterprise (or 3rd party delegate)
- Understand enterprise can wipe all work data/property off device (at any time)
- Ensure all software on device is fully licensed (including personal software)
- If device is lost/stolen, call in as enterprise security incident
- Not share the device with non employees (unless controls exist to secure work data)
- Must understand enterprise can revoke right to use device at any time (without warning)

Company will:

- Honor data privacy laws
- Not wipe full device without asking permission
- Not track users geo-location without permission
- etc

IBM needs both general policy & detailed controls. IEM Enforces.

Overall endpoint policy includes includes:

- minimum acceptable devices locks
  (password policies, autolock settings, etc)
- required malware protection
  (antimalware software, firewall, intrusion protection, system currency, etc)
- required data protection
  (minimum acceptable encryption, data loss prevention, url filtering, etc)
- required endpoint management
  (to enforce the above & enable enterprise to respond to change)

definitions of acceptable use

Remote Wipe and Selective Remote Wipe

Technical controls per platform include:

Details of how to meet general policy, on a platform by platform config basis

Some mobile platform examples @ IBM:
- 8 char, alphanumeric passcode, 30 minute max auto lock, wipe after 10 attempts
- required antimalware software on android, no jailbroken iOS devices
- itunes backups encrypted, siri prevented from bypassing passcode
- device encryption on Android 4.0+ devices to enable full network access
- minimum acceptable OS versions

Where do we see it Going….
Workspace Aggregation – User Centric Management

Evolving from device centric management to user centric: allows consistent policy based management across heterogeneous environment.

- **BYOD** is driving device proliferation in the enterprise increasing the importance of the “user”
- End-users expect services and data will **”follow the user” across devices**, regardless of form factor or ownership
- Managing the device is no longer sufficient, **mobile management converges previously separate domains** like file sharing, backup, and VPN with device management
- Requires additional partnerships and/or technology development

Gartner early view of Workspace Aggregators

Borrowing the Gartner terminology, “workspace aggregators” provide:

- A presentation of the end user’s computing environment across services
- Unify security and management of the various services and devices

Some key functions:

- Aggregation of SaaS, Server-Based Computing, Virtualized, Local Apps
- Single Sign-On
- Provisioning / de-provisioning of applications
- Self Service Interface
- Meter usage, compliance reporting
- Context Aware Security

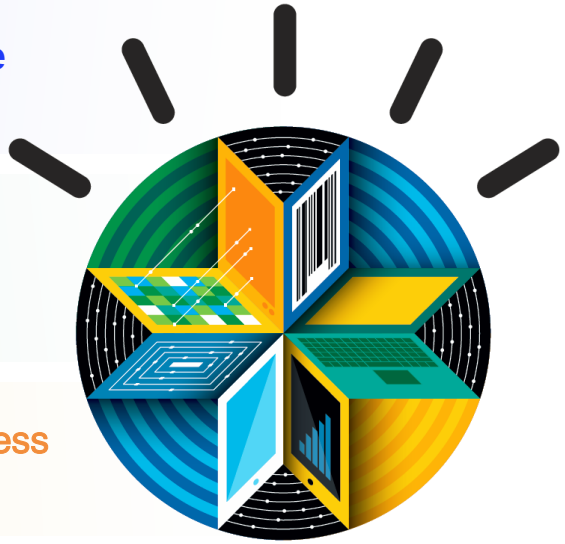
Source: Gartner (August 2012)

Three ways to get started with IBM MobileFirst

1. **Download the IBM Endpoint Manager for Mobile Devices 30 day trial** ibm.co/EndpointMgrTrial

2. **Learn more:**
   ibm.com/mobilefirst
   twitter.com/IBMMobileFirst (#IBMMobileFirst)
   facebook.com/IBMMobileFirst

3. Talk with me, or your IBM representative or Business Partner to find the right next step for you



Thank You!