IBM Security Symposium 2012

Intelligence | Integration | Expertise

Mobile Security, Everything you NEED to know about Endpoint Security but were afraid to ask !

Matthew Johnson – Senior Technical Staff Member
Mobility Infrastructure, IBM CIO

August 2012

“There are known knowns; there are things we know that we know.

There are known unknowns; that is to say there are things that, we now know we don't know.

But there are also unknown unknowns – there are things we do not know, we don't know.”

—United States Secretary of Defense,
Donald Rumsfeld
February 12, 2002

Mobile devices are different from the standard enterprise laptop & desktop in many ways . . .

Mobile Devices are Shared More Often

Smartphones and tablets are multi-purpose personal devices. Therefore, users share them with friends, and family more often than traditional computing devices – laptops and desktops. Social norms on privacy are different when accessing file-systems vs. mobile apps

Mobile Devices are Used in More Locations

Smartphones and tablets are frequently used in challenging wireless situations that contrast with laptop friendly remote access centers. Laptops are used in a limited number of trusted locations

Mobile Devices prioritize User Experience

Smartphones and tablets place a premium on user experience and any security protocol that diminishes the experiences will not be adopted or will be circumvented. Workstation level security cannot be assumed unless they are dedicated devices

Mobile Devices have multiple personas

Smartphones and tablets may have multiple personas – entertainment device, work tool, etc. Each persona is used in a different context. Users may want to employ a different security model for each persona without affecting another.

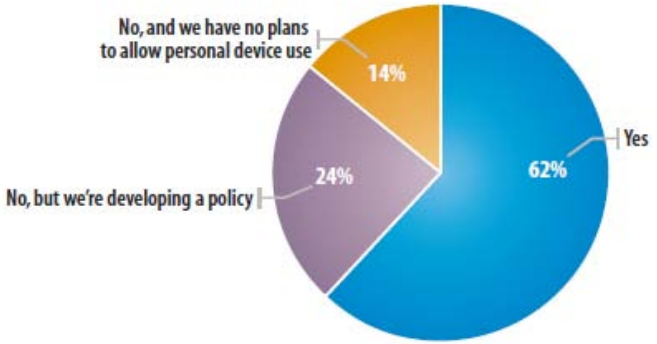
Mobile Devices are Diverse

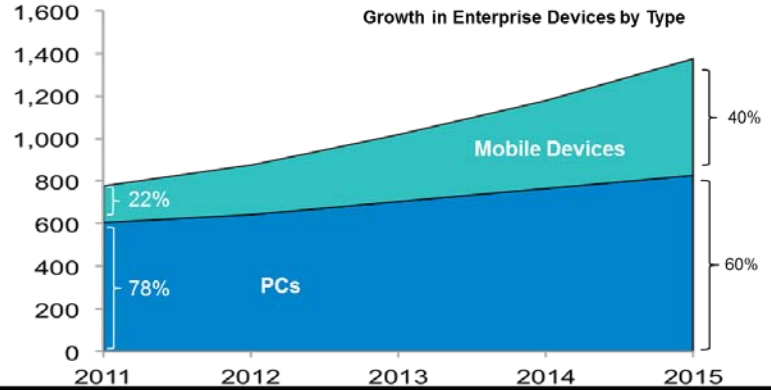
Smartphones and tablets employ a variety of different platforms and have numerous applications aimed at pushing the boundaries of collaboration. The standard interaction paradigms used on laptops and desktops cannot be assumed.

Your users are bring these mobile devices to work

Many organizations don't have a plan to allow mobile devices into the workplace

- Information Week





By 2015 40% of Enterprise devices will be mobile devices

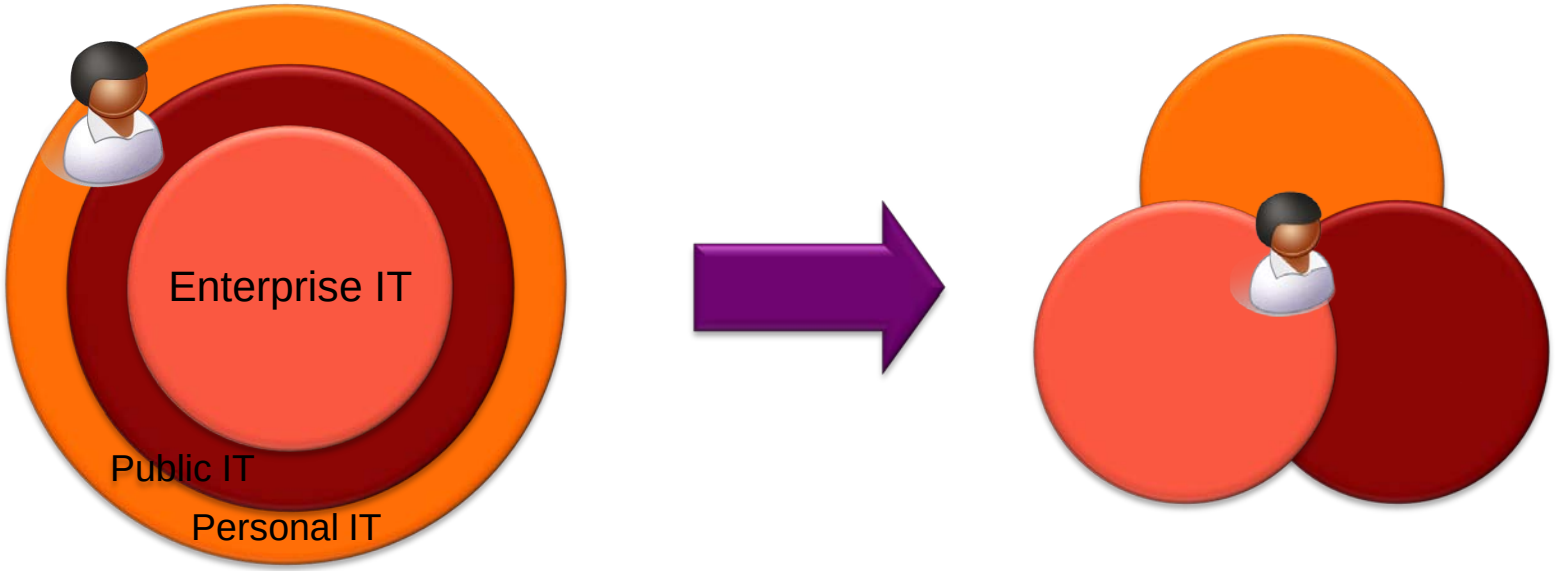
Within a few years, over 50% of all employees will be generation Y

IBM Projection

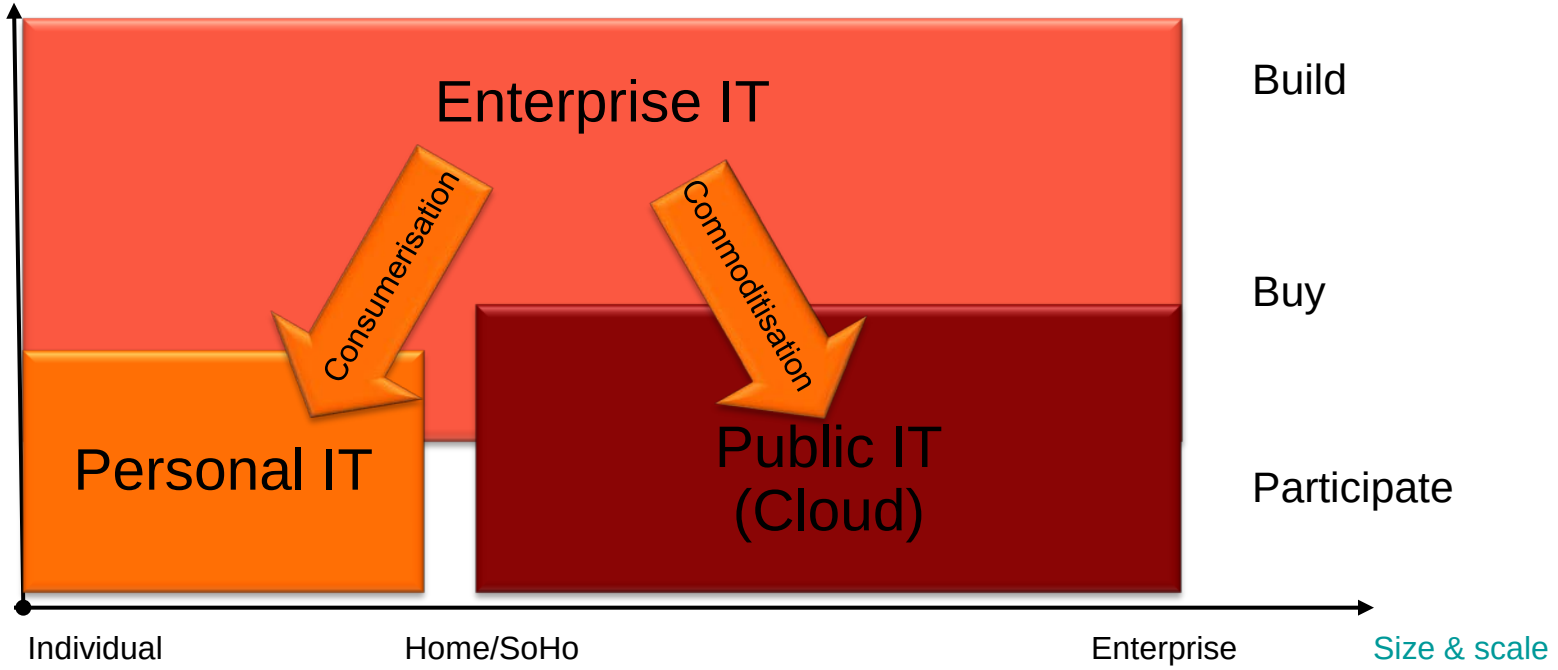
Research from Toyota USA shows gen-Y prefer new devices and gaming consoles purchase over new vehicle purchase

ZDNet

Which is causing a fundamental shift from Enterprise to Personal as the **Primary IT** that an person experiences



As personal IT grows, enterprises will “participate” in IT eco systems that are controlled by vendors & carriers.



As such we need to look at Mobility from a different point of view

Old Mobility

Mobility is focused on connecting an **enterprise employee**, using a standard **enterprise asset** managed in compliance with enterprise IT standards

New Mobility

Mobility is now about **securely projecting** the enterprises capability (applications) onto almost **any device, anywhere** that connectivity can be found

An enterprise needs to address the opportunities & challenges that mobile devices & BYOD offers across the organisation, it cannot be addressed by IT alone.

- ***Human Resources***: What are the policies, guidelines and programs for mobile users and bring-your-own devices? (BYOD)
- ***Legal***: What are the legal requirements in different geographies?
- ***Security***: How do you ensure intellectual property is secure on a variety of mobile devices?
- ***Learning***: How do you educate your workforce about mobility options available to them?
- ***Communications***: How do you make sure your workforce hears key messages? How do you make sure you hear your workforce?
- ***Governance***: How do you align IT strategy with business strategy and ensure that the business is on track to achieve its goals? Are mobile solutions delivering business value?
- ***Information Technology***: What tools and technologies are needed to enable various personas to effectively do their jobs and drive innovation?

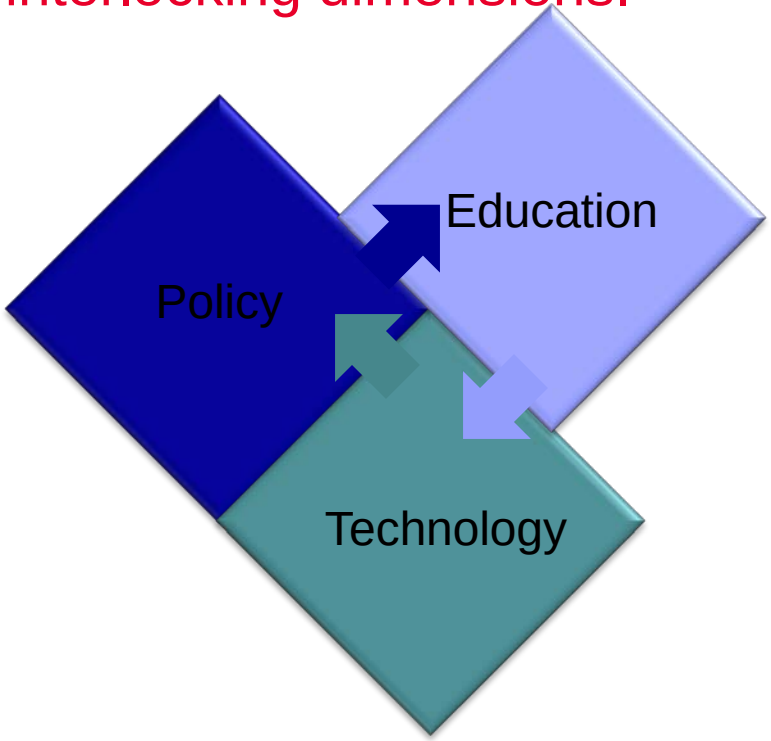
You can reduce this down to a key set of items that you “need to know”.

- You have a *published policy* on Mobility, BYOD & Workstation Security
- The *practice in your enterprise* matches the policy that is published
- Your *users understand their responsibilities* in a Mobile/BYOD environment
- You have the *technology in place* to ensure that the devices connecting into the enterprise Intranet are, indeed, compliant to the policy.

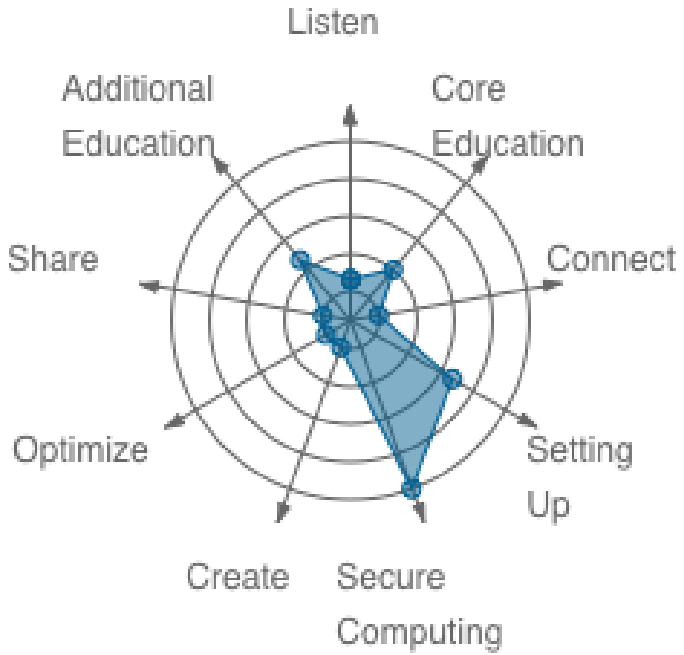
Mobility @ IBM today

- Security and safeguarding IBM data is paramount
  - Very conservative approach
  - Constantly evaluating devices, operating systems and applications for suitability
- IBM supports BYOD for employees
  - Work is no longer a “place you go to”
  - Potential to drive productivity
- Internal Appstore called WhirlWind
  - > 500 apps
  - More than 40k downloads
  - E.g. MyMobileHub delivers file sharing
- Lotus Traveller
  - Application allowing mobile access to email, calendar, contacts
  - 30% of employees currently enabled, 20% active
  - 120,000 mobile devices, 80,000 personally owned, supported in months
    2/3rds BYOD, 1/3rd IBM-supplied
  - Best practices from pilot now available as a client service via

In IBM we approach workstation security from 3 overlapping and interlocking dimensions.

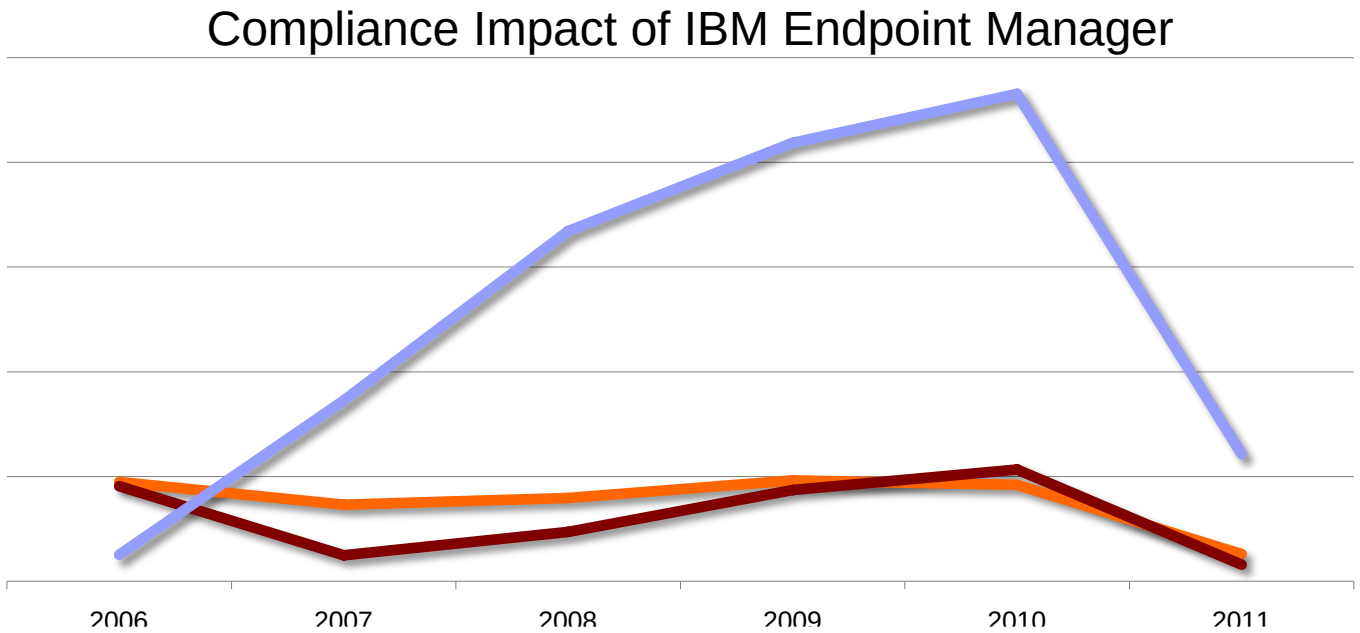


Every IBMer must complete relevant, online, self paced education



IBM has as part of the annual standards update revised our security standards to include BYOD etc.

IBM is in the process of extending IBM Endpoint Manager to all of the mobile devices connecting into IBM

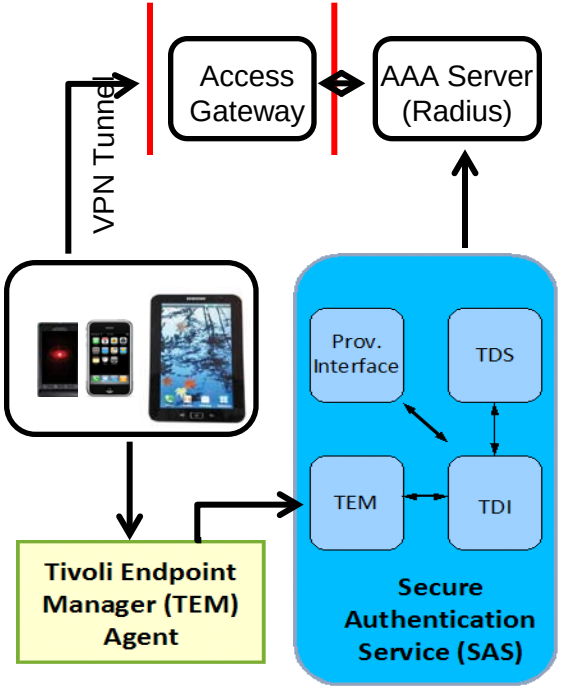


IBM experience using IBM Endpoint Manager

Before	After
Patch availability typically 3-14+ days	*Patch availability within 24 hours*
92% compliance within 5 days (ACPM only)	*98% within 48 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 Device requirements can be automatically remediated*
Exceptions at machine level	*Exceptions at setting level*

This is only the start of the transformation – use the information gathered to make “smart” decisions – IBM’s VPN as an example

- Challenges
  - Current tools are application or infrastructure specific
  - Device posture validation can be circumvented
- The Innovation
  - Provide an extensible architecture and access methodology applicable across any device
  - Ensures only compliant devices can access corporate internal networks
    - User identity
    - Device posture
- End-user simplicity
  - Automated device registration
  - Records based on user and respective devices



In Summary.

- Have a *published policy* on Mobility, BYOD & Workstation Security
- Ensure the *practice in your enterprise* matches the policy that is published
- Ensure your *users understand their responsibilities* in a Mobile/BYOD environment
- Have the *technology in place* to ensure that the devices connecting into the enterprise Intranet are, indeed, compliant to the policy.
- Use the information that you gather to *make decisions on access* to business capability based on your unique set of circumstances.

IBM Security Symposium 2012

Intelligence | Integration | Expertise

Thank You

Matthew Johnson – Senior Technical Staff Member
Mobility Infrastructure, IBM CIO

August 2012

Twitter : @mjohnson
Blog : http://matthewjohnson.id.au