Pulse

IBM SolutionsConnect 2013

Building the Education Mobility Revolution

Michael Knauth

IT Systems Engineer

St. Joseph's College

12/06/2013

IBM

Plan of attack

- Who is ‘Terrace’
- What were the challenges
- What is the solution
- OS Deployment
- Patch Management
- Power Management
- Mobile Devices

Who is ‘Terrace’?

- Catholic boys school for years 5 – 12, founded in 1875
- Located on the fringe of Brisbane’s CBD
- 4 campuses, 5 sites
- 1300 students
- 200 teaching and management staff
- 1600+ end user devices – thin terminals, laptops, netbooks, iMacs, MacBooks, mobile devices
- 4 IT support personnel

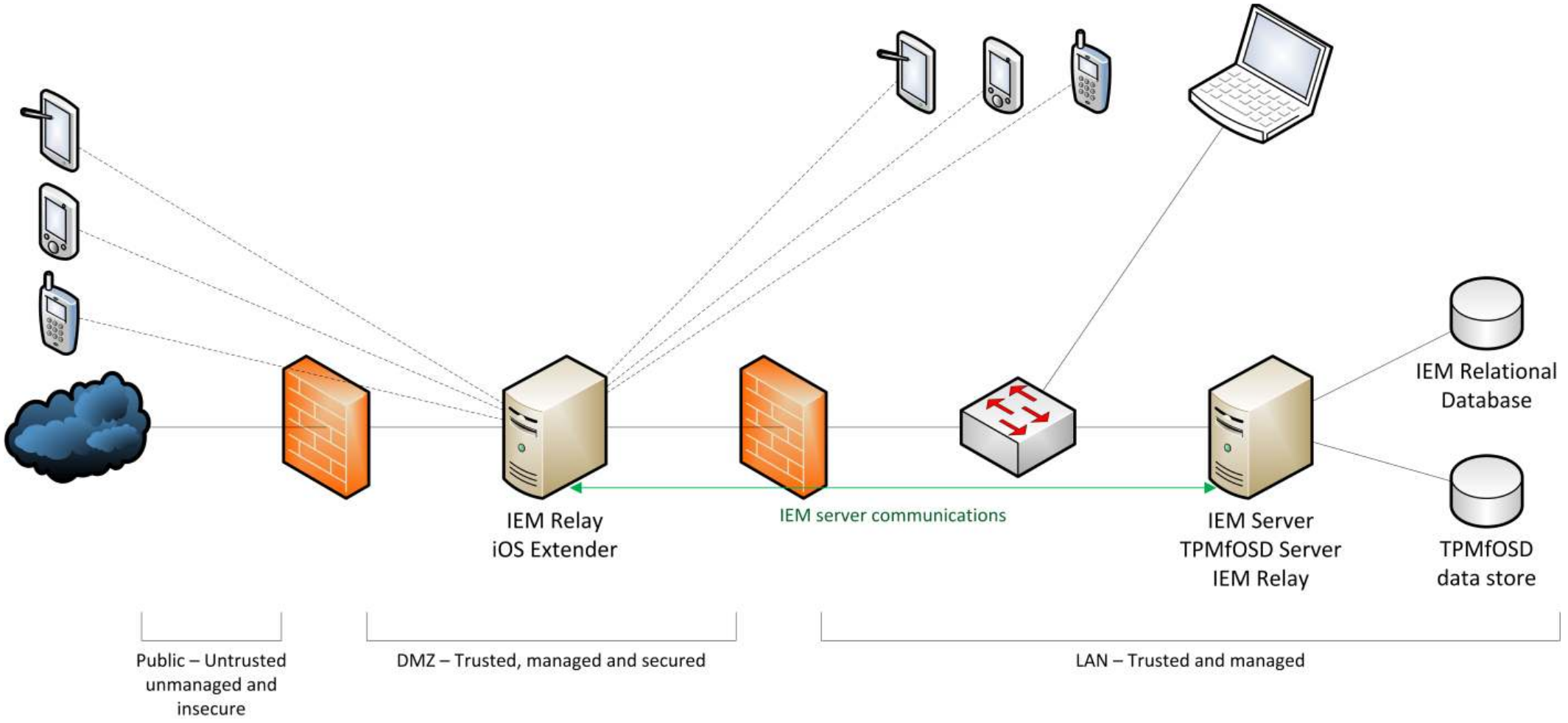
The problem

- Multiple images to cater for:
  - Difference in hardware platforms;
  - Variance in software requirements.
- Multiple tools
  - Hard drive imaging software;
  - ‘Home grown’ post imaging tools.
- Growing network
- Excessive time to patch and manage
- Consistent requests for additional applications
- Patches for some software unmanageable
  - Adobe, Google, Mozilla, Oracle, Apple, Curriculum specific titles;
  - WSUS can only patch 35% of vulnerabilities;
  - 13 or more updating systems required to patch remaining 65%.
- Limited resources
- Introduction of mobile devices and the associated impacts

Addressing the problem

- Introduced:
  - Tivoli Provisioning Manager for OS Deployment, and;
  - IBM Endpoint Manager.
- Complete deployment and management solution of end points
- Single server
- Two days to install and configure
- Extremely flexible and extensible

IEM Architecture



OS deployment

- TPMfOSD
- Bare metal deployment
- Consolidated OS images from 10 down to 2
- Hardware independent
- Includes deployment of a hardened OS baseline and additional software modules
- Deployments are managed centrally, distributed remotely
- Image development time significantly reduced – between 50% and 75%

Patch management

- Central patch management
- Patches (fixlets) created by IBM Content Delivery Team
- Supporting all major OS vendors and versions
- Updates, fixes and patches for major software vendors
- Eliminates the need to constantly maintain OS images
- Minimises the need for users to bring devices to IT support staff
- Cuts down costs associated with support
- Results in a consistent state of computing devices

Patch management

- Adobe (336)
- Apple (425)
- Bigfix (7)
- BigFix (31)
- Google (2)
- IBM (1)
- Microsoft (8,849)
- Mozilla (87)
- Nullsoft (8)
- Oracle (292)
- Real Networks (14)
- Skype (22)
- Summit Software (1)
- Sun (10)
- VMware (51)
- VMware, Inc. (82)
- Winzip (13)

List of applicable fixlet sources

- All (106)
- Fixlets Only (40)
- Tasks Only (66)

Name	Source Severity	Site	Applicable Computer
Adobe Reader 11.0 Available	<Unspecified>	Updates for Win...	107 / 129
BES Clients using Main BES Server instead of BES Relay - Manual...	Important	BES Support	123 / 364
Enable Encryption for Clients	<Unspecified>	BES Support	126 / 364
Mozilla Firefox 17.0.6 ESR Available	Critical	Updates for Win...	32 / 129
Mozilla Firefox 21.0 Available	Critical	Updates for Win...	36 / 129
MS11-002: Vulnerabilities in Microsoft Data Access Components...	Critical	Patches for Win...	2 / 129
MS11-006: Vulnerability in Windows Shell Graphics Processing C...	Critical	Patches for Win...	1 / 129
MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of P...	Important	Patches for Win...	2 / 129
MS11-020: Vulnerability in SMB Server Could Allow Remote Cod...	Critical	Patches for Win...	3 / 129
MS11-024: Vulnerability in Windows Fax Cover Page Editor Coul...	Important	Patches for Win...	3 / 129
MS11-030: Vulnerability in DNS Resolution Could Allow Remote ...	Important	Patches for Win...	3 / 129
MS11-031: Vulnerability in JScript and VBScript Scripting Engine...	Critical	Patches for Win...	1 / 129
MS11-056: Vulnerabilities in Windows Client/Server Run-time Su...	Important	Patches for Win...	2 / 129
MS12-048: Vulnerability in Windows Shell Could Allow Remote ...	Important	Patches for Win...	1 / 129
MS12-057: Vulnerability in Microsoft Office Could Allow Remot...	Important	Patches for Win...	79 / 129
MS12-057: Vulnerability in Microsoft Office Could Allow Remot...	Important	Patches for Win...	79 / 129
MS13-022: Vulnerability in Silverlight Could Allow Remote Code...	Critical	Patches for Win...	46 / 129
MS13-023: Vulnerability in Microsoft Visio Viewer 2010 Could All...	<Unspecified>	Patches for Win...	80 / 129
MS13-023: Vulnerability in Microsoft Visio Viewer 2010 Could All...	Critical	Patches for Win...	80 / 129

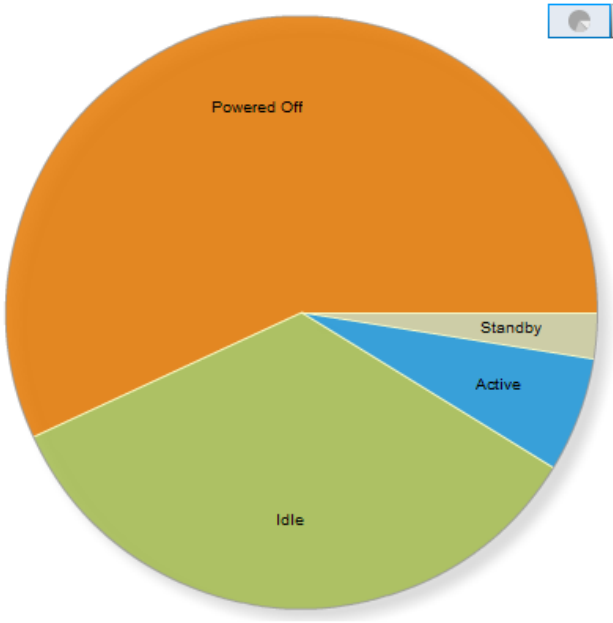
Applicable fixlets for a selected device

Power management

- Devices are:
  - left on;
  - suffering insomnia;
  - experiencing damage as a result.
- Systems Lifecycle component provides Power Management
- Configure and deploy OS power profiles/schemes
- Metrics show power usage in contrast to device utilisation
- Scheduled shutdown of devices
- Wake on LAN

Power management

Average Day Breakdown



Power State	Hours
Powered Off	13.6 (56.9 %)
Idle	8.2 (34.3 %)
Active	1.5 (6.3 %)
Standby	.6 (2.5 %)

Idle Time Breakdown for Last Week

	Office Hours	Outside Office Hours		Full Week
		Weekends	Workdays	
Idle Time (hours)	19.41	13.23	3.04	**35.68**
Total Hours/Week	45	63	59.1	**168**
Idle Time (%)	**43.13 %**	**21 %**	**5.14 %**	**21.24 %**

Total Tracked Computers

Type	Systems
Notebooks	108 (33 %)
Desktops	216 (66 %)
Servers	1 (0 %)
Totals	325 (100 %)
Removed due to errors	1
Removed due to insufficient data	3

Power Profile Settings

Computers with System Standby Enabled: 213 of 325 - 65%

Computers with Monitor Standby Enabled: 304 of 325 - 93%

Computers with Hard Drive Spindown Enabled: 300 of 325 - 92%

Average Statistics

Average Cost per kWh: $0.08

Daily Usage per Computer:

Power: 0.86 kWh

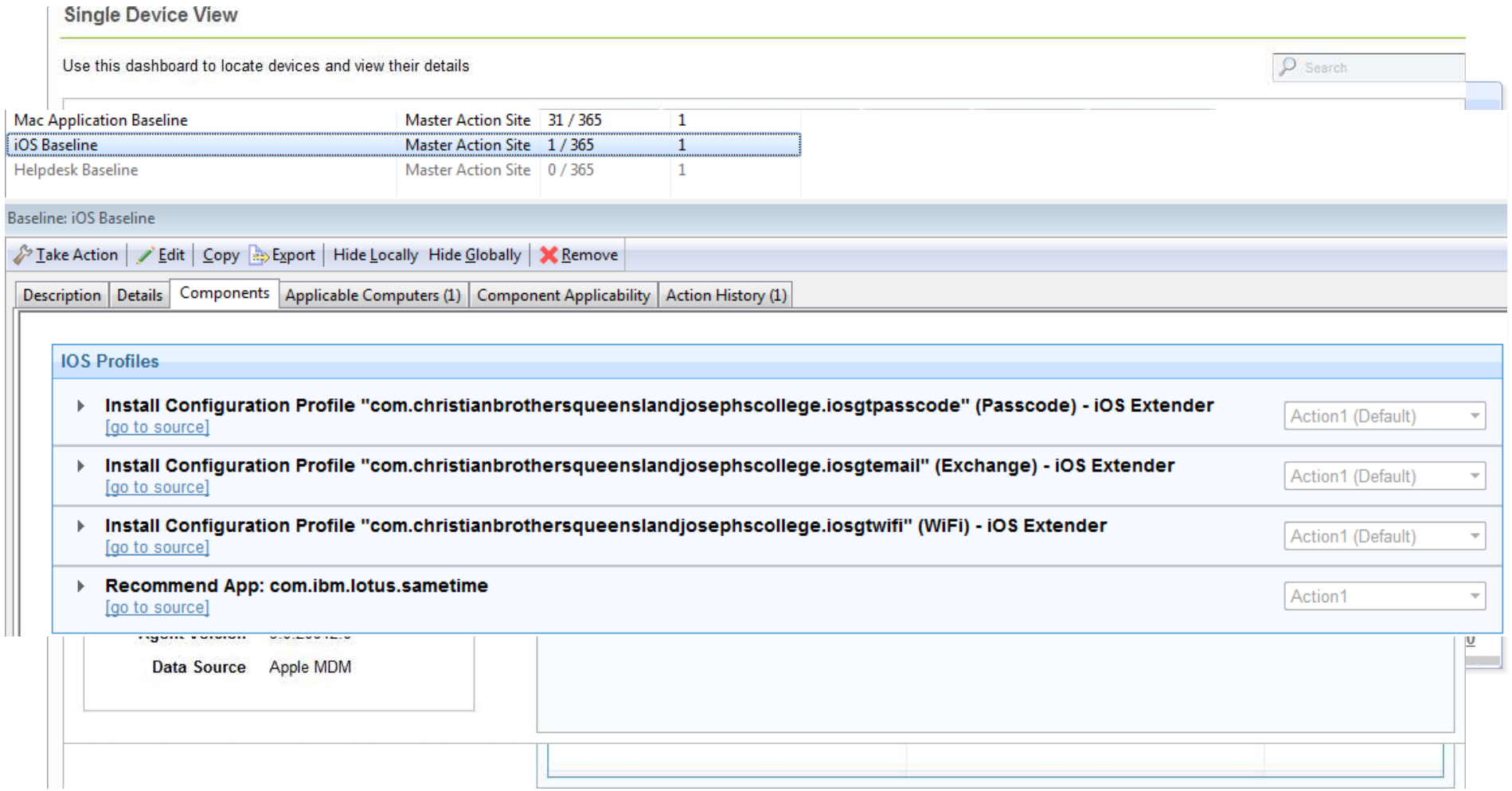
Cost: $0.07

Carbon: 1.20 lb

Mobile device management

- Requirement for staff to fully leverage mobile devices on-site
- Deploy profiles for:
  - Security
  - WiFi
  - Email
  - Apps
- Interaction with RADIUS and directory server to satisfy access requirement policies
- Distribute apps to devices
- Offer paid apps under volume purchase agreements
- Device security management options

Mobile device management



Back to the future

- Core protection
- Deploying ‘on the fly’
- BYO_
- OS Deployment through IEM
- Remote control

Q&A

- Questions:\>_