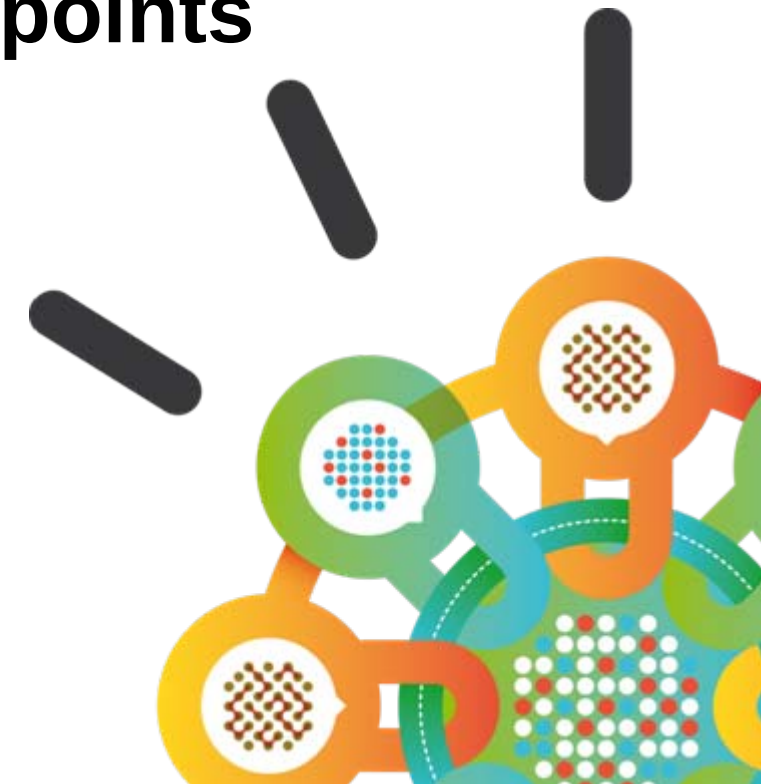
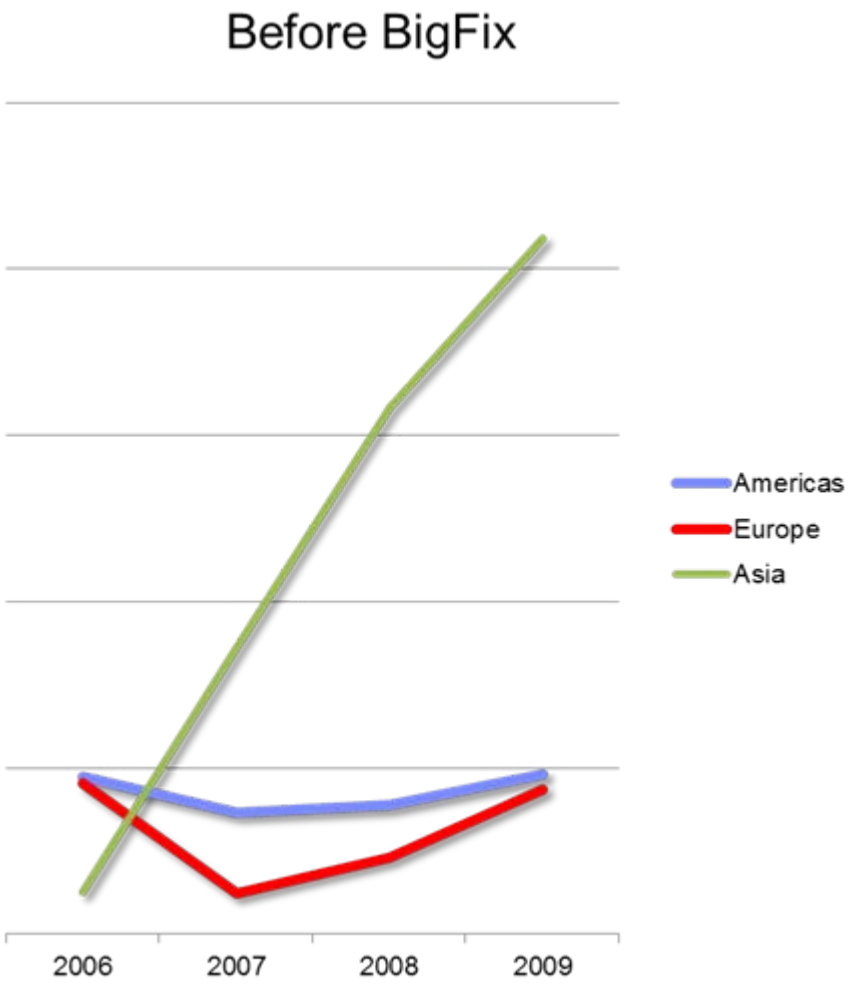
David Merrill, Matthew Johnson
Senior Technical Staff Members
IBM Security Division/IBM CIO

From Servers to Smartphones: Global Management and Security of All Your Distributed Endpoints



© 2012 IBM Corporation

Endpoint security issues by GEO

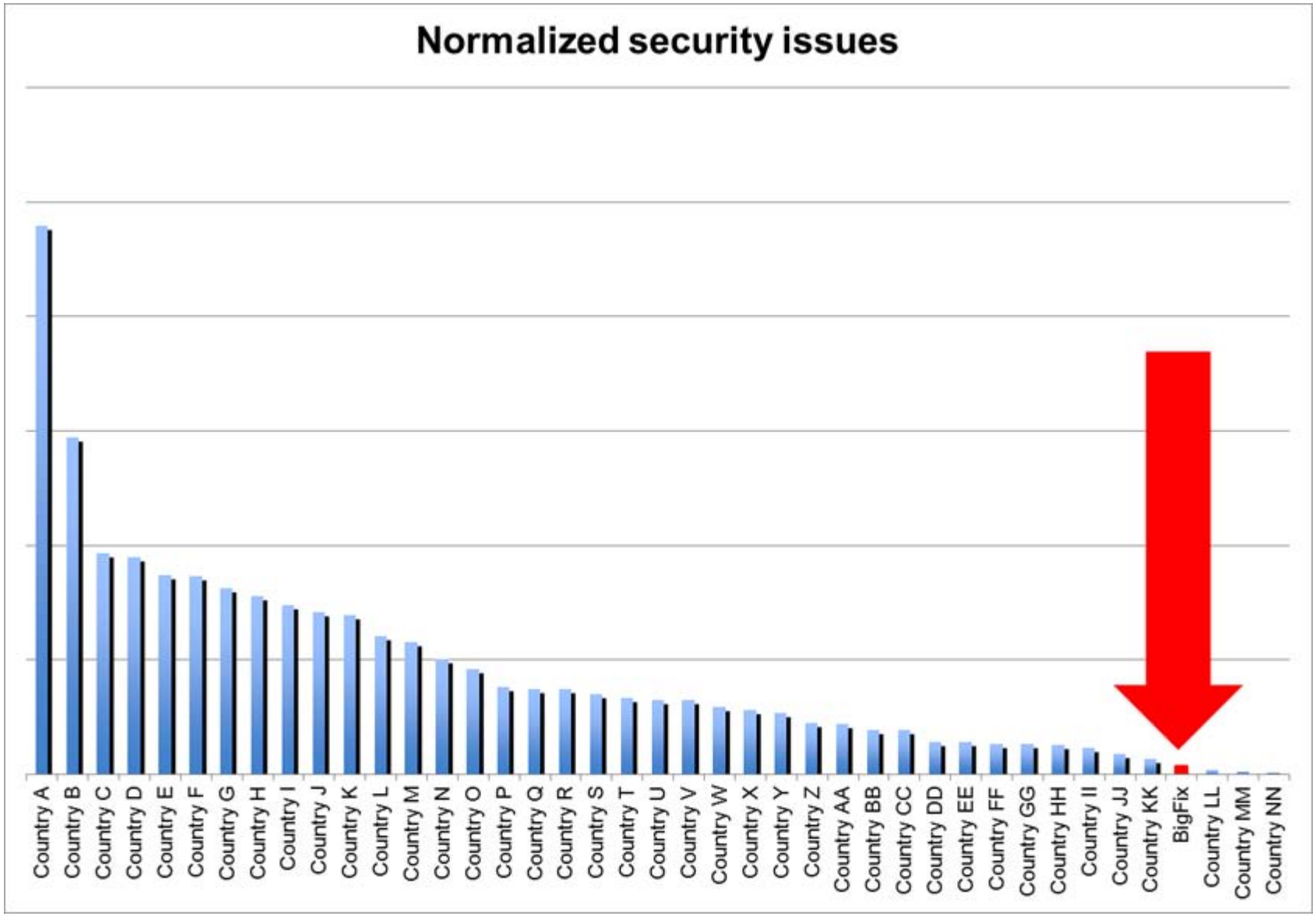


© 2011 IBM Corporation

It’s all about reducing business risk – initial BigFix challenges

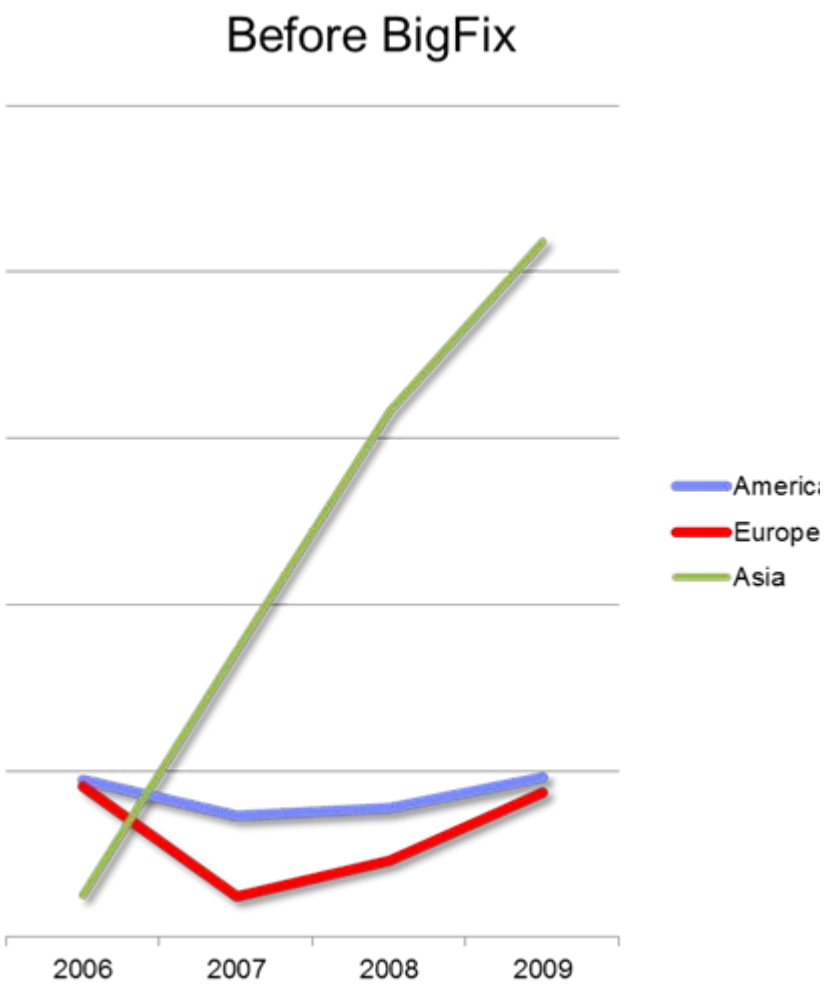
- Evolving IT business models have increased risk to clients and infrastructure
  - Partnering with other companies for Joint Development projects
  - Outsourcing of internal network
  - Increased pace of Acquisitions and Divestitures
  - Increased mobility / more employees working from unprotected environments
- Continual increase in risk and sophistication of malware attacks
- Need to secure more platforms (beyond Windows)
- Migrate from compliance-based endpoint program to automated enforcement program

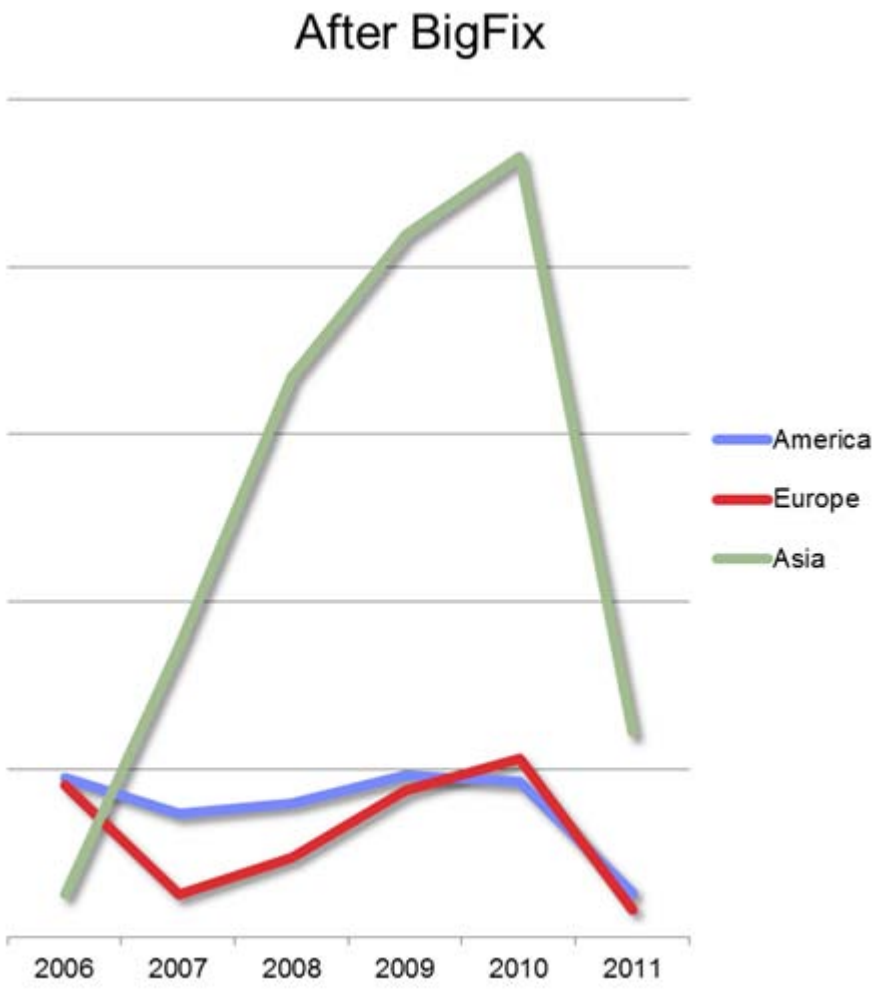
© 2011 IBM Corporation



© 2011 IBM Corporation

Endpoint security issues by GEO





© 2011 IBM Corporation

IBM experience using BigFix

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 Windows requirements can be automatically remediated*
Exceptions at machine level	*Exceptions at setting level*

© 2011 IBM Corporation

Mobile is a major driver in the evolution of computing

Mobile/Wireless/Cloud

Web/Desktop

Client/Server

Host/Mainframe

Employees

34%

employees in 2012 are mobile
(Source: IDC*)

Security

8X

increase in security risk driven by proliferation of mobile data and devices

Mobile Applications

85 billion

mobile applications will be downloaded in 2012

(Source: IDC)

Unified Communications (UC)

78%

of multinational corporations plan to adopt mobile UC by 2015, including mobile video streaming and conferencing

"Consumerisation of IT"

62%

individual–liable (BYOD*) devices used for business, compared to 38% corporate-liable in 2012

(Source: IDC*)

© 2011 IBM Corporation

Getting started with Enterprise Mobile Security – the four questions to ask

- ✓eMail
- ✓Contacts
- ✓Calendar
- ✓Intranet Access
- ✓Sensitive Personal Information
- ✓Other?

What mobile apps and data are required?

What are associated required security controls?

- ✓Security Policy
- ✓Password
- ✓Device Timeout
- ✓Disk Encryption
- ✓Malware Protection
- ✓Other?

Data

What platforms are desired?

- Blackberry
- Windows Mobile
- Symbian
- iOS
- Android

What additional mobile controls?

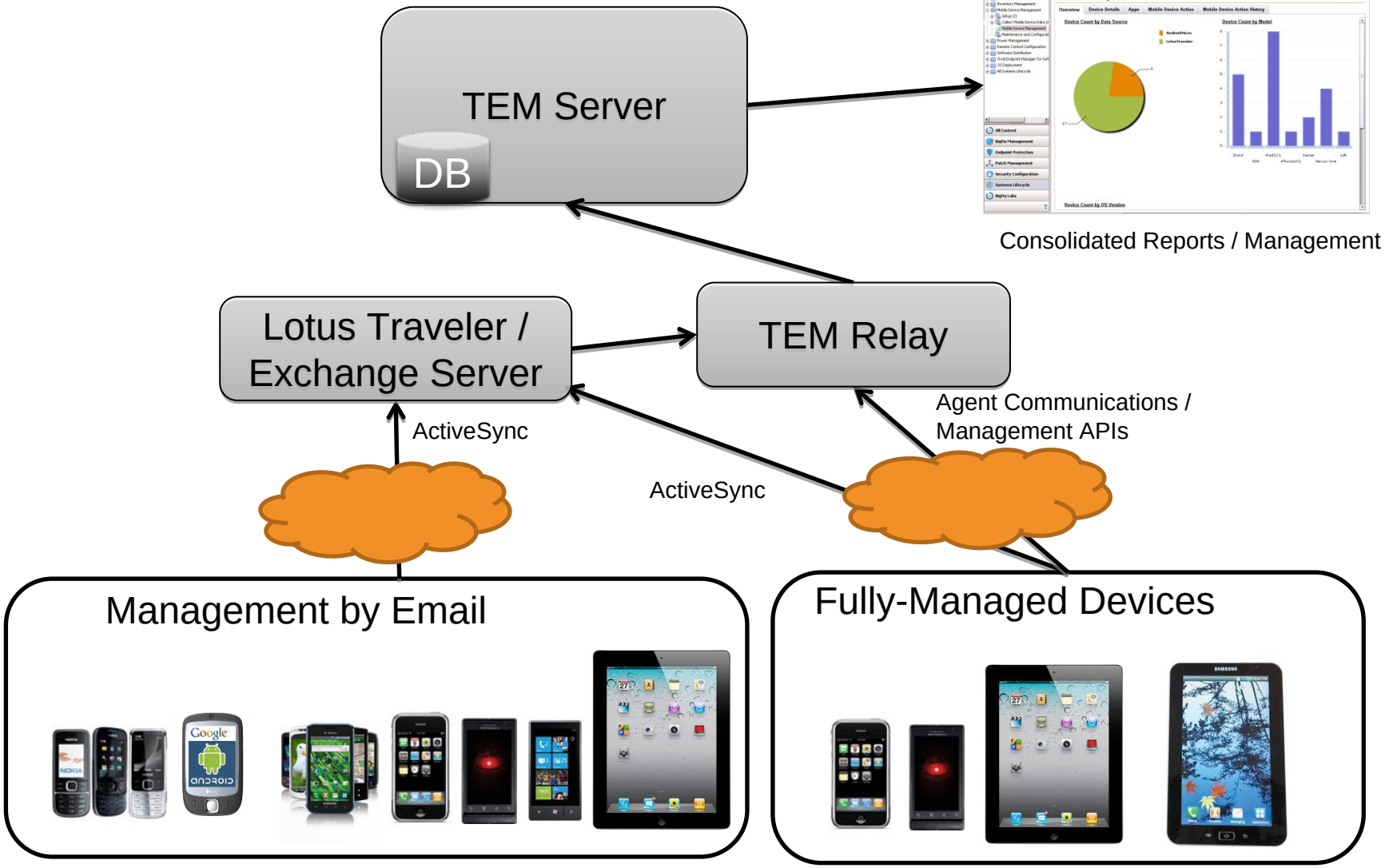
- ✓Data Wipe
- ✓Device Kill
- ✓Other?

Endpoint Management Convergence Matters….

- Why does this matter?
  - Cost
  - Compliance and reporting
  - Enablement of role-based security management
- Proliferation of tactical mobile security tools and point products
  - Served purpose
  - Ultimately inefficient and complex
- Consistency across all endpoints
  - Tablets and smartphones are really just computers
  - Same data at risk
  - Extend security standards ➔ Roles ➔ Configuration policies

© 2011 IBM Corporation

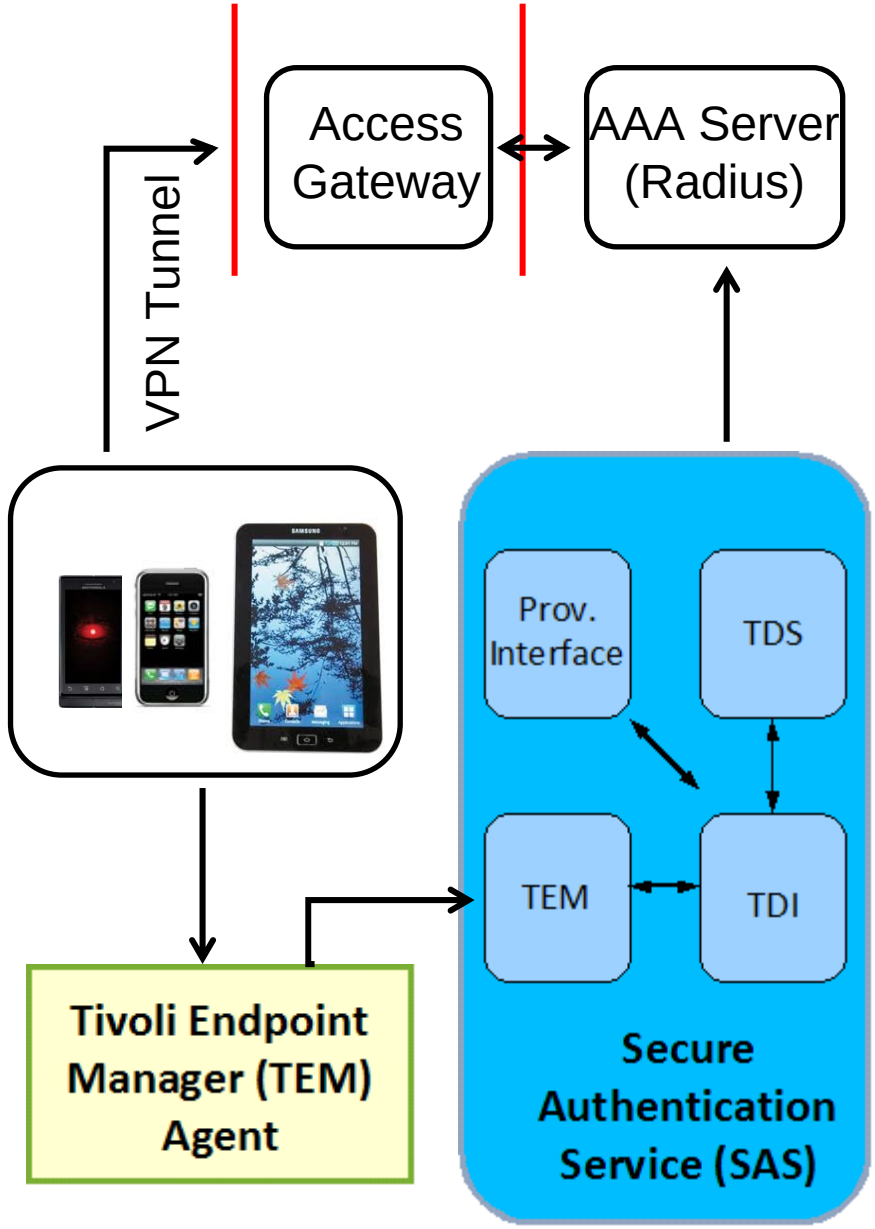
TEM MDM Architecture



© 2011 IBM Corporation

Secure Enterprise Remote Access

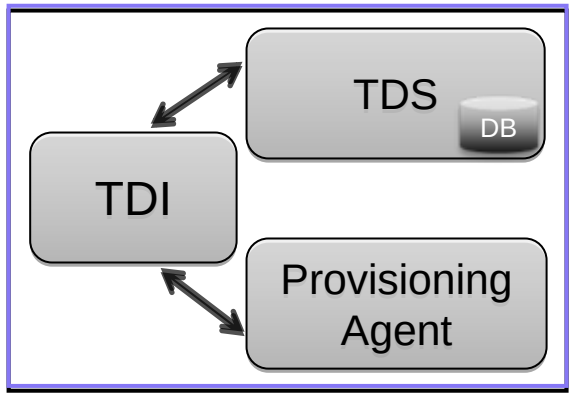
- Challenges
  - Current tools are application or infrastructure specific
  - Device posture validation can be circumvented
- Research Innovation
  - Provide an extensible architecture and access methodology applicable across any device
  - Ensures only compliant devices can access corporate internal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



© 2011 IBM Corporation

Secure Authentication Service Components

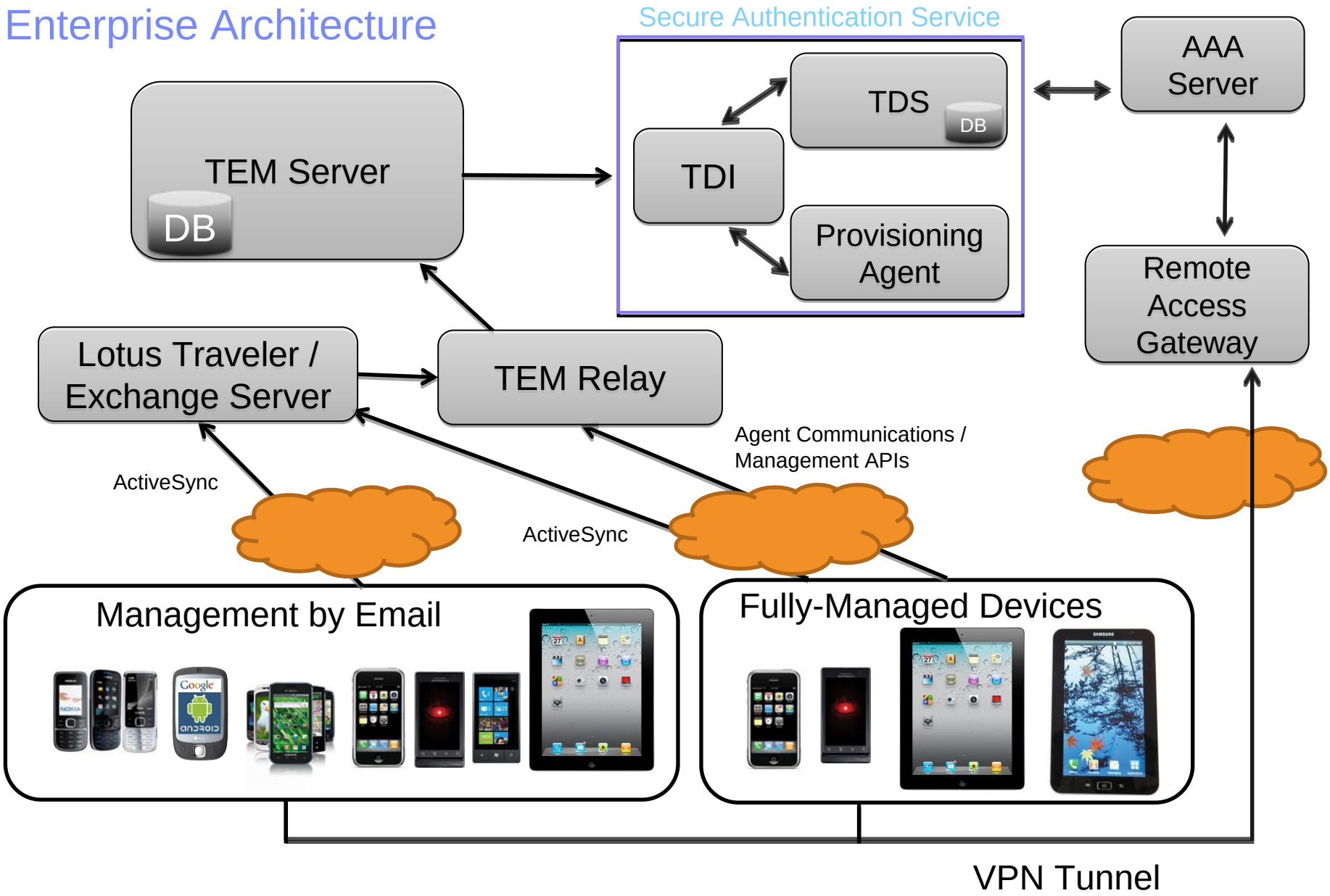
- Tivoli Endpoint Manager (TEM)
  - Agent on client device
  - Set of fixlets to perform ITCS300 compliance testing
  - Fixlet generates device unique Remote Access credentials



- Tivoli Directory Integrator (TDI)
  - Integrates TEM, TDS, Bluepages and provisioning service
- Tivoli Directory Server (TDS)
  - Authoritative Remote Access authentication and authorization database
- Provisioning Agent
  - End-user, helpdesk support and administrator management interface to Remote Access user and device records

© 2011 IBM Corporation

Enterprise Architecture



© 2011 IBM Corporation

Read my thoughts

- Follow me at the Institute of Advanced Security Mobile Security expertblog
  - http://instituteforadvancedsecurity.com/ias-blogs/community-blogs/b/weblog12/default.aspx
- LinkedIn: Dave_merrill@us.ibm.com
- Twitter: @davidpmerrill
- Read IBM's ISS XFORCE trend report
  - Mobile security update in 2012 edition available now
  - http://www-935.ibm.com/services/us/iss/xforce/trendreports/

© 2011 IBM Corporation

© 2011 IBM Corporation

Trademarks and disclaimers

© Copyright IBM Australia Limited 2012 ABN 79 000 024 733 © Copyright IBM Corporation 2012 All Rights Reserved. TRADEMARKS: IBM, the IBM logos, ibm.com, Smarter Planet and the planet icon are trademarks of IBM Corp registered in many jurisdictions worldwide. Other company, product and services marks may be trademarks or services marks of others. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© 2011 IBM Corporation