



Innovation
that Matters

**Secure and Manage:
A unified platform for
managing mobile devices together
with your traditional endpoints**

Steven Scheurmann

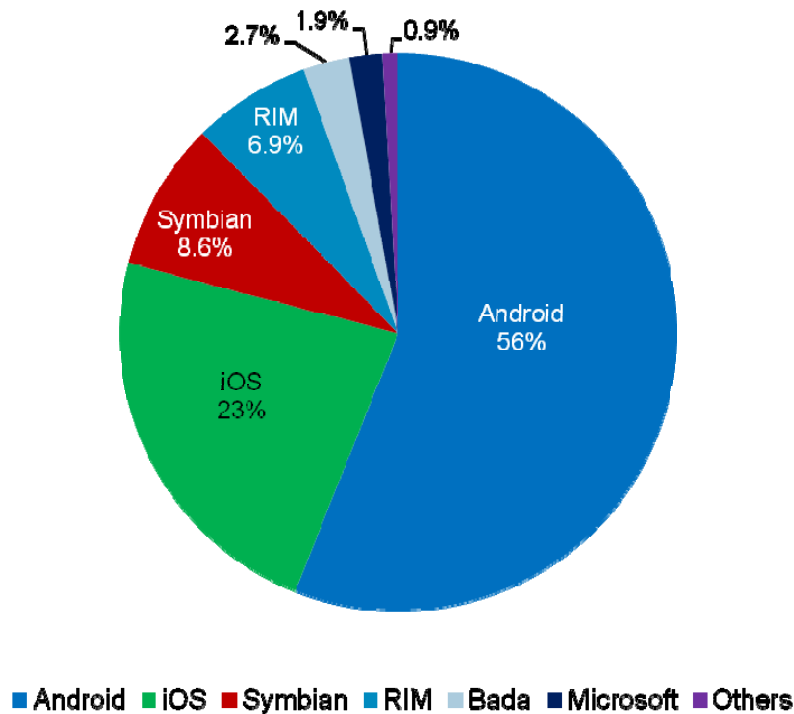
**Vice President of Sales, Tivoli Endpoint Management Products
IBM Asia Pacific & Japan**

Overview

- Mobile Device Trends
- How IBM approaches BYOD
- How IBM Endpoint Manager manages it all (PCs to Phones)
- IBM Worklight (Mobile Enterprise Application Platform or MEAP)
- Li & Fung Case Study
- Summary

Life was so much easier when everyone simply had a Blackberry

Share of global Q1 2012 smartphone sales to end users, by OS



Source: Gartner 2012; does not include media tablets

- Android and iOS accounted for 79% of all smartphone shipments
- Many employees want to use their devices to access work information
- Mobile devices offer significant advantages for companies
- ‘Halo effect’ of Apple Mac’s
- **Before companies can realise the benefits of mobile devices, they need to be able to manage the associated risks**

Managing Devices – Old Philosophy

IT manages risks by maintaining control points

✓ Control the Device

- Enterprises provide all equipment



✓ Control the Complexity

- Small set of supported platforms / models

✓ Control the OS

- Operating systems configured, managed, and updated by IT



✓ Control the Apps

- IT controls which apps are allowed and the configuration



✓ Control the Network

- Network traffic controlled with proxies and web filters



Managing Devices – The New Reality

With BYOD, IT loses control

❌ Control the Device

- Employees bring personal devices (BYOD)



❌ Control the Complexity

- Many different combinations of devices and OSes



❌ Control the OS

- OS version and upgrades managed by carriers, OEMs, users

❌ Control the Apps

- Apps updated automatically by App Stores and users



❌ Control the Network

- Devices connect through 3G/4G, WiFi,

IBM understands the demands of managing a global heterogeneous IT infrastructure with BYOD

- **430,000 IBM employees** in over 120 countries
- Deployment to over **750,000 endpoints**
- A **78 per cent decrease** in endpoint security issues
- IBM is also in the process of deploying IBM Endpoint Manager for Mobile Devices across its entire mobile workforce of over **120,000 staff**
- IBM Endpoint Manager is being deployed across many global outsourced accounts
- BYOD with **200,000+** smartphones projected
- **2099+ Terabytes** of WAN traffic **per month**



How IBM is embracing the growing BYOD trend

w3
News
Search News

News home

Top stories

In the news

MyNews

Archive index

Help

Published on 06 February 2012

[News home](#) > [Top stories](#) >

Working beyond the laptop


IBMers embrace growing mobile trend

IBM creates infrastructure to support "Bring Your Own Device."

IBM and IBMers are embracing "[Bring Your Own Device](#)" — a growing trend in business computing resulting from the explosion of smart phones, tablets and other mobile devices.

[Bill Bodin](#), an IBM Distinguished Engineer and chief technology officer for mobility at IBM, discusses the innovations and infrastructure IBM is putting in place to create an open, secure environment that supports employees using a variety of consumer technologies for business purposes.

In this, the fourth column in the [Digital IBMer](#) series, Bill shares his views on our mobility strategy and the implications for employees.



By Bill Bodin

IBM is on the leading edge when it comes to embracing and enabling "BYOD" — Bring Your Own Device.

As the "consumerization of IT" proliferates, IBM is establishing an open platform approach to enable IBMers to use their own tablets, computers and mobile devices, along with traditional IBM computers to conduct IBM business. Continuing our legacy and leadership in open technologies, we believe our BYOD strategy makes it possible for employees to explore the possibilities of a variety of consumer technologies and work anytime, anywhere, with any device, which has many advantages for IBMers, our company and our clients.

As IBMers increasingly use their own tablets, devices and computers for work, we are taking steps to fortify the infrastructure and device management to allow devices to attach to our network securely. Our strategy is to support personally-owned devices with platforms that work within appropriate management interfaces for secure corporate data access. This is the reason I often refer to BYOD as BYOSD, or "Bring Your Own Securable Device."

IBM has security standards that address IBM and personally-owned computers and devices: [Read the security policy here.](#)

For IBM, a company based on innovation, providing a robust, open, mobile platform is the right strategy. For IBMers, improving our own digital proficiency is the right approach. Imagine the possibilities: an IBM Researcher participating as a real-time expert and able to access the Watson Q&A system, for example, using a mobile device. Even extending the system to include voice recognition from your mobile device and delivering the response as text-to-speech. What a way for IBM technology, IBMer expertise and agility to come together. That's the vision we're striving to achieve through our BYOD strategy.

© 2012 IBM Corporation

Six steps IBM employees need to follow to keep their devices safe

1. Register your computer, tablet, and mobile devices with IBM
2. Use IBM's tools to secure and encrypt your computer, tablet, mobile device and storage devices
3. Don't mix IBM data with non-IBM clouds
4. Declare public wireless networks untrusted
5. Know if you qualify to use a personally-owned device for specific IBM business purposes
6. Report incidents on personally-owned technologies to IBM

Firms lag on BYOD security

FRAN FOO Australian IT August 17, 2012 9:25AM

ORGANISATIONS that don't take a holistic security approach to bring-your-own-device (BYOD) programs do so at their own peril, an industry expert warned.

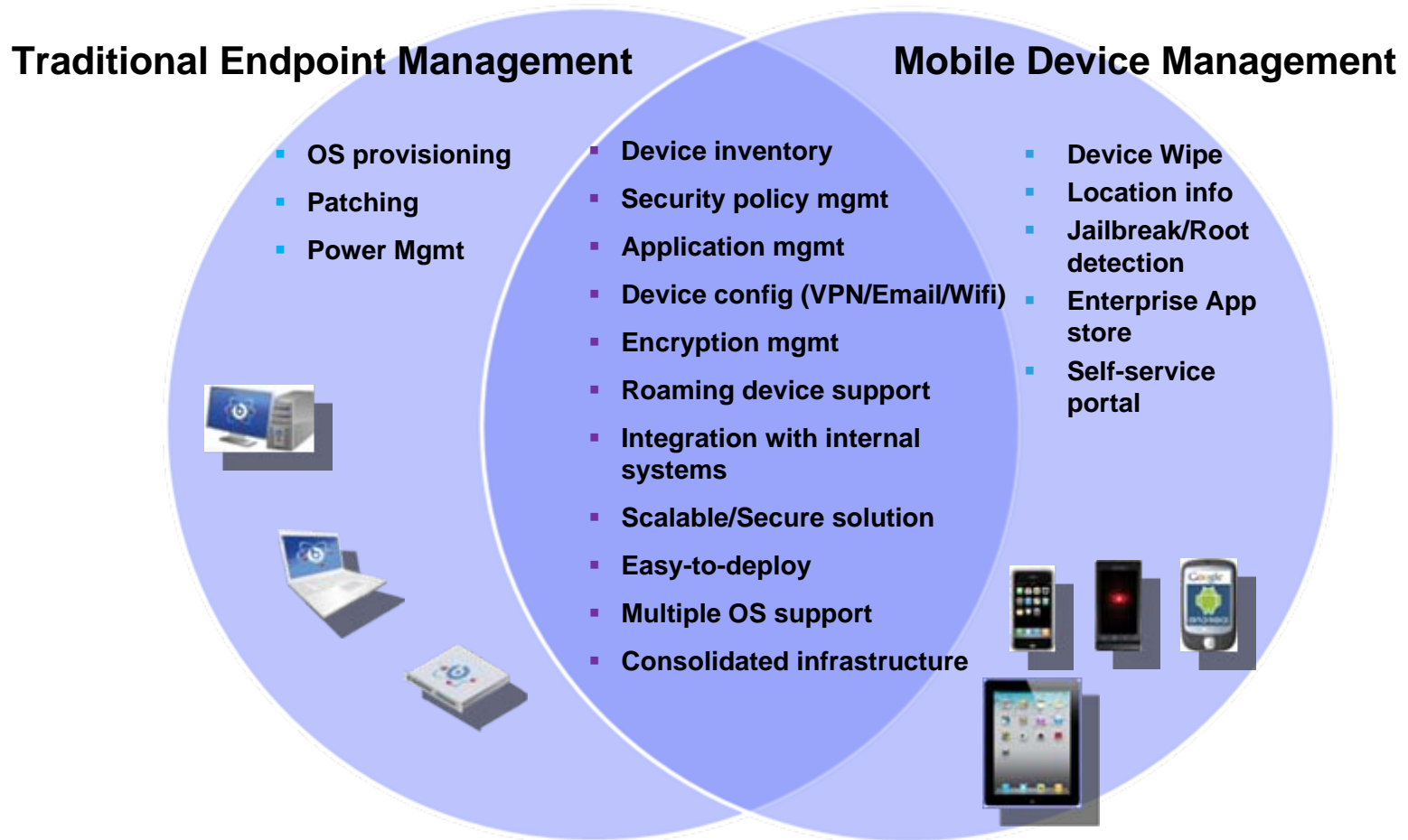
A survey by Forrester Research Australia found that most companies were effectively outsourcing BYOD security to employees.

According to the study, almost 50 per cent of companies viewed user passwords/PIN as the primary method of securing BYOD devices. These smartphones and tablet computers are allowed to connect to corporate networks and access sensitive or commercial information.

Other forms of security such as access control for applications and services, remote locking or wiping of content and data encryption ranked lower.

The research found that organisations were taking a reactive approach to BYOD and had not addressed underlying issues that could help reduce complexity, risk, cost and associated administrative overheads.

PCs and mobile devices have many of the same management needs



“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

IBM Endpoint Manager continuously monitors the health and security of all enterprise computers in real-time via a single, policy-driven agent

Endpoints



Desktop / laptop / server endpoint



Mobile



Purpose specific

- Common management agent
- Unified management console
- Common infrastructure
- Single server



Patch Management



Lifecycle Management



Software Use Analysis



Mobile Devices



Power Management



Core Protection



Security and Compliance

Systems Management

Security Management

IBM Endpoint Manager

How it Works

Lightweight, Robust Infrastructure

- Use existing systems as Relays
- Built-in redundancy
- Support/secure roaming endpoints

Cloud-based Content Delivery

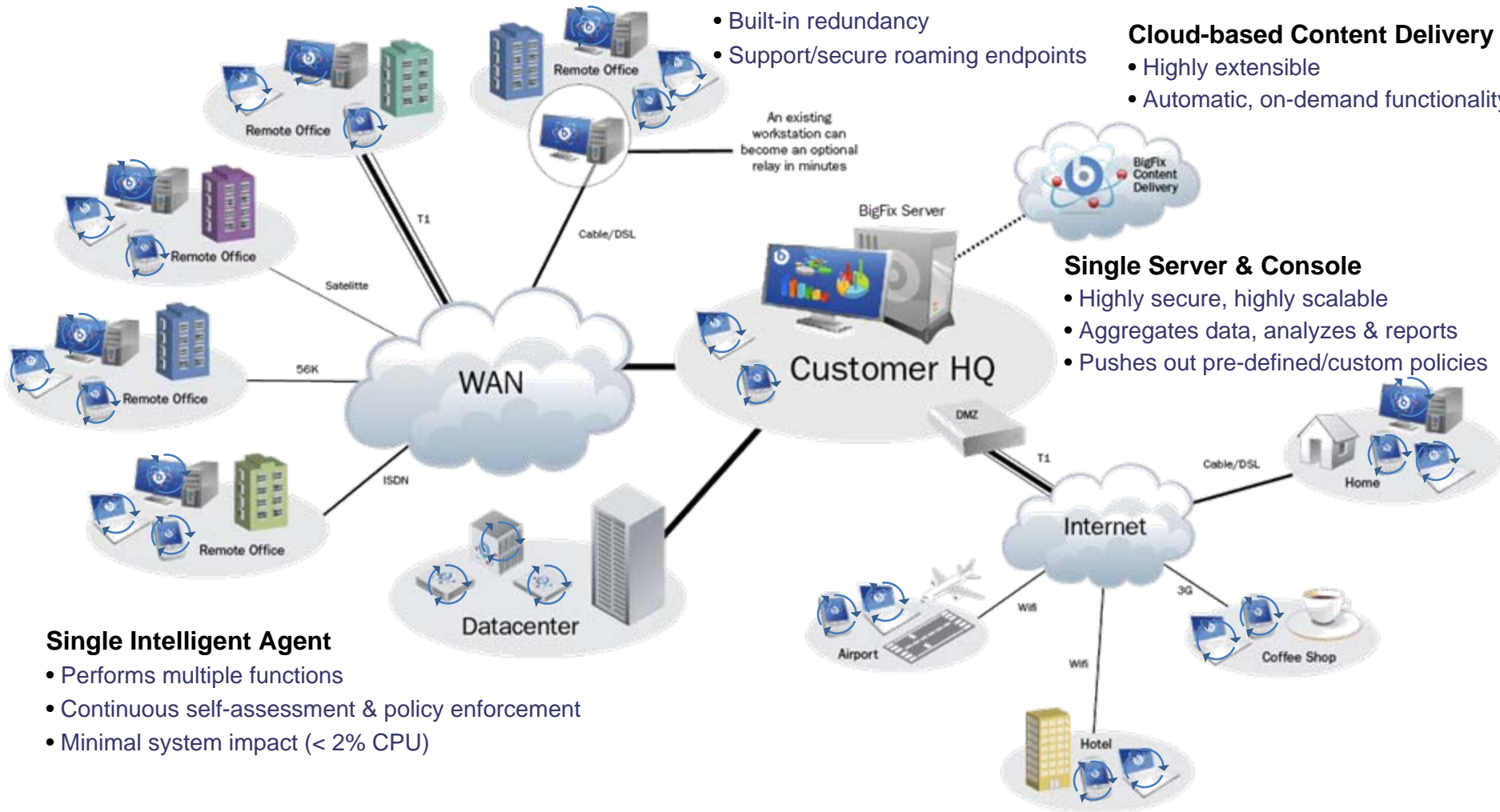
- Highly extensible
- Automatic, on-demand functionality

Single Server & Console

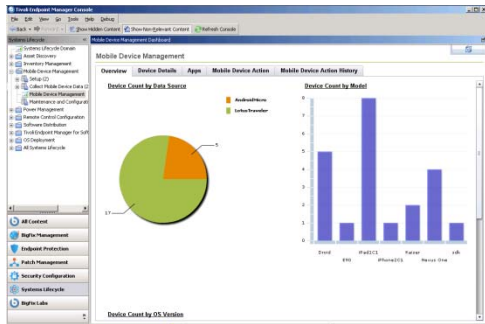
- Highly secure, highly scalable
- Aggregates data, analyzes & reports
- Pushes out pre-defined/custom policies

Single Intelligent Agent

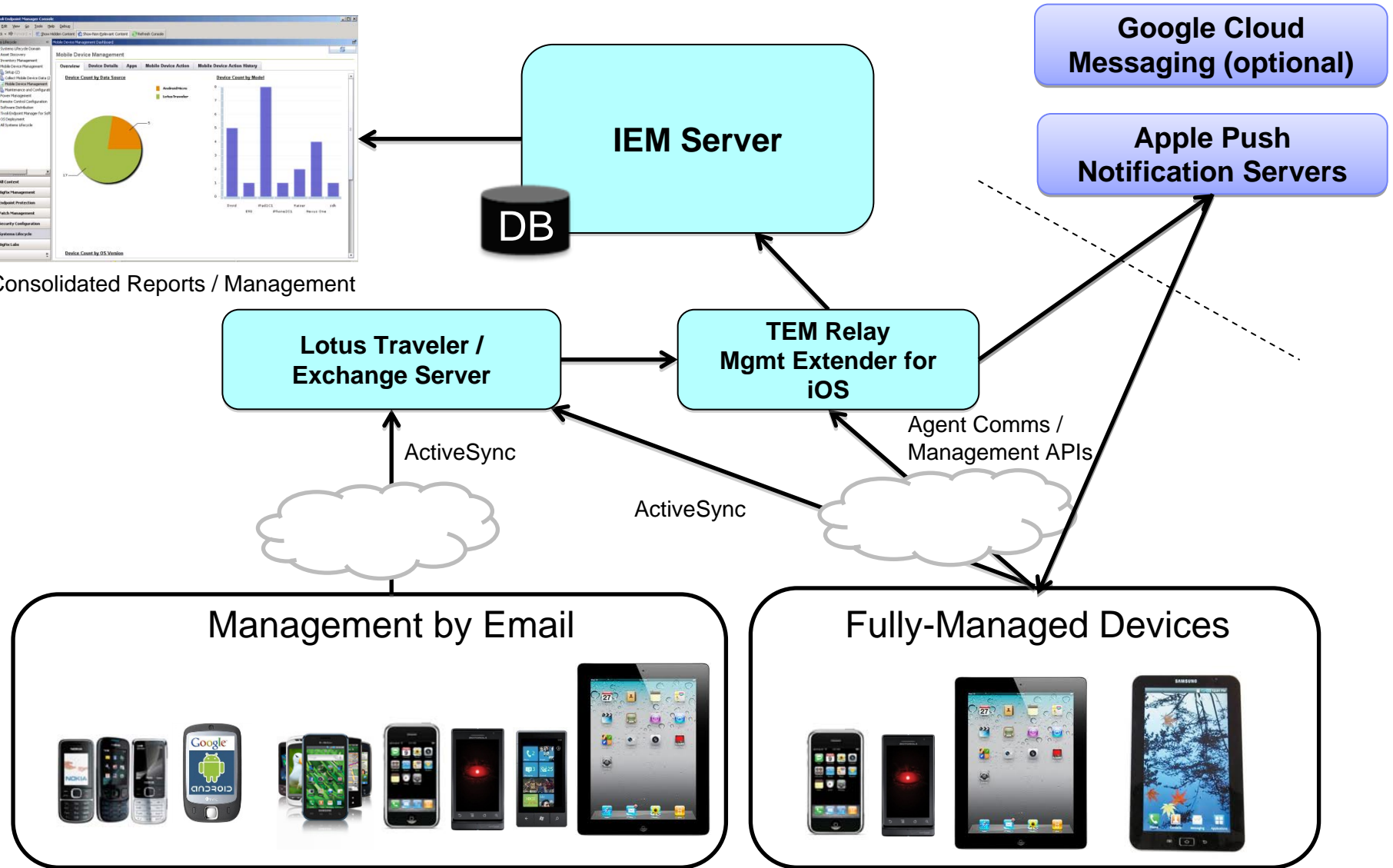
- Performs multiple functions
- Continuous self-assessment & policy enforcement
- Minimal system impact (< 2% CPU)



IBM Endpoint Manager for Mobile Devices Architecture



Consolidated Reports / Management



IEM approach for Mobile Device Management

- Advanced management on iOS through Apple's MDM APIs



- Advanced management on Android through a BigFix agent



- Email-based management through Exchange (ActiveSync) and Lotus Traveler (IBMSync)
 - iOS
 - Android
 - Windows Phone
 - Windows Mobile
 - Symbian

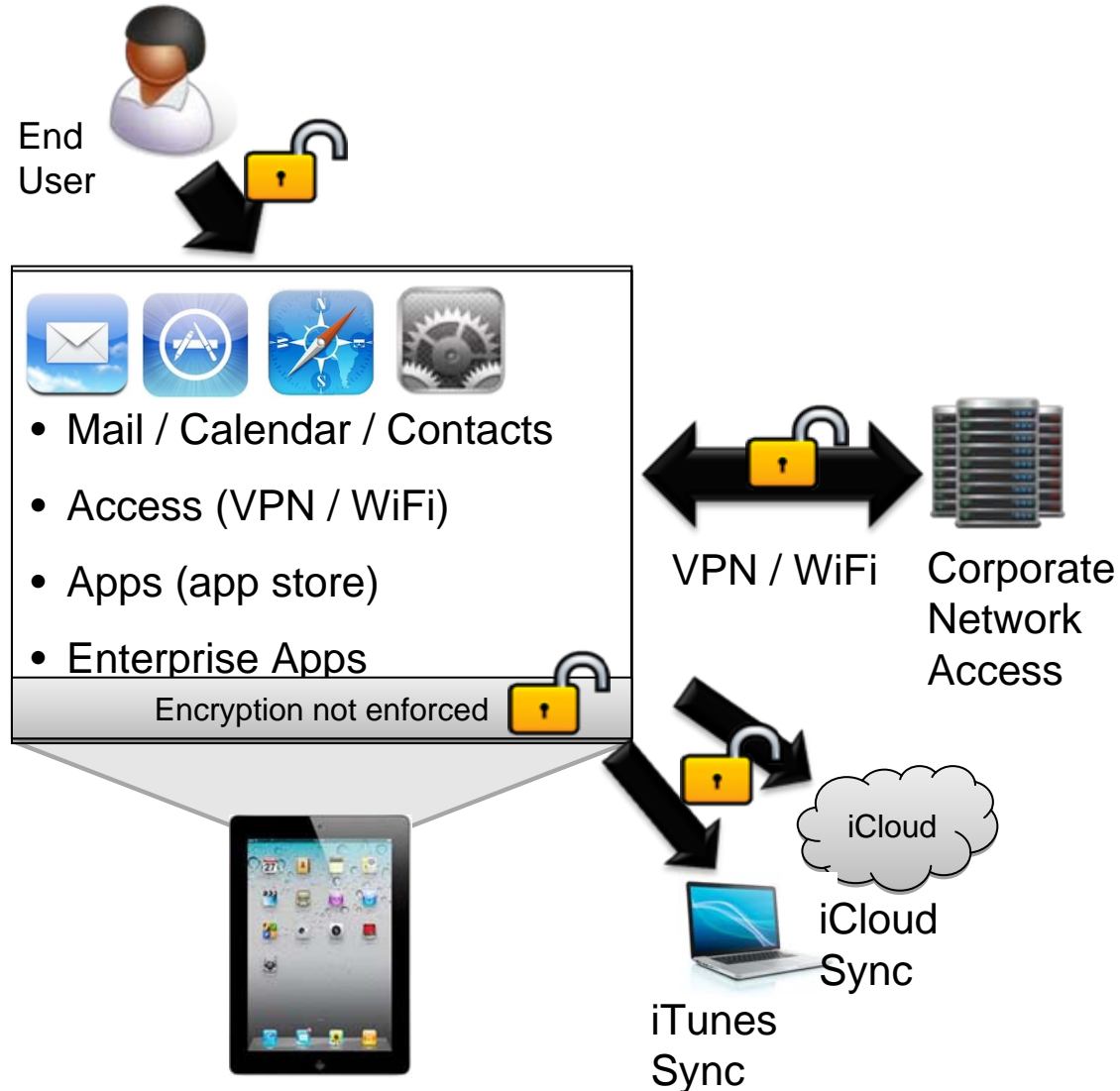
Apple iOS
Google Android

Nokia Symbian
Windows Phone
and Windows
Mobile

Managing Mobile Devices – The Problem

Security & Management Challenges

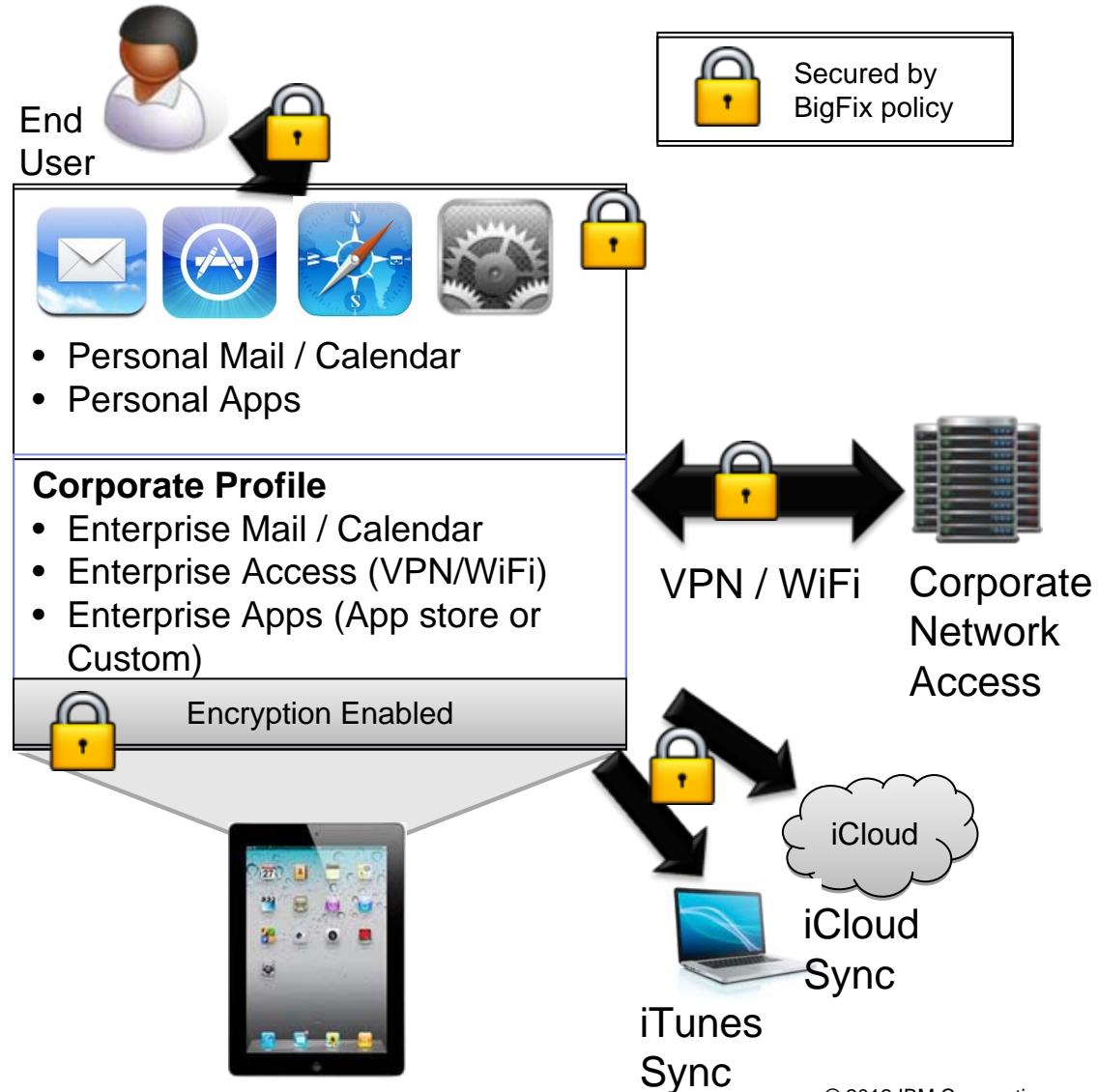
- Potential unauthorized access (lost, stolen)
- Disabled encryption
- Insecure devices connecting to network
- Corporate data leakage



Managing Mobile Devices – The Solution

Endpoint Manager for Mobile Devices

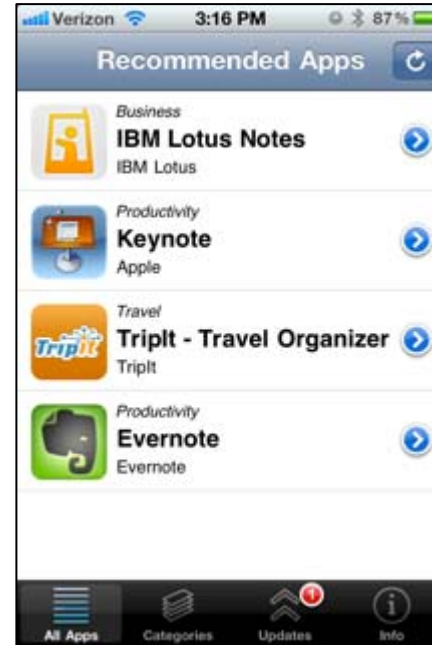
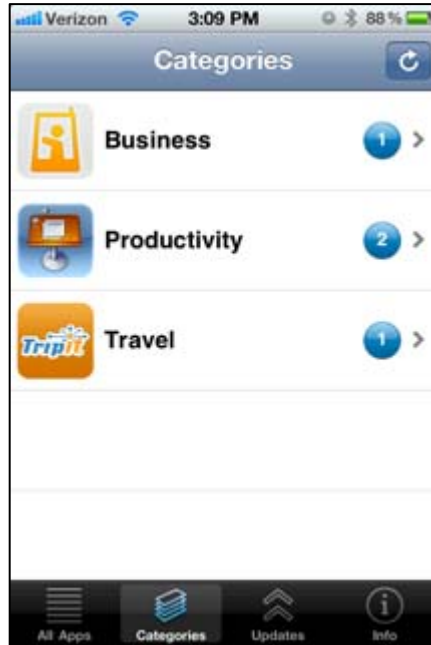
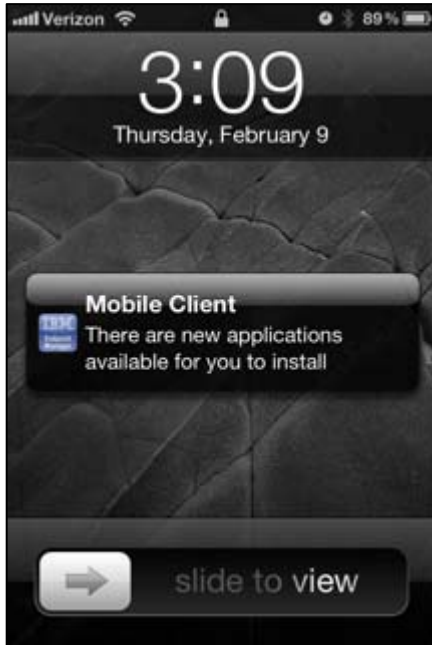
- Enable password policies
- Enable device encryption
- Force encrypted backup
- Disable iCloud sync
- Access to corporate email, apps, VPN, WiFi contingent on policy compliance!
- Selectively wipe corporate data if employee leaves company
- Fully wipe if lost or stolen



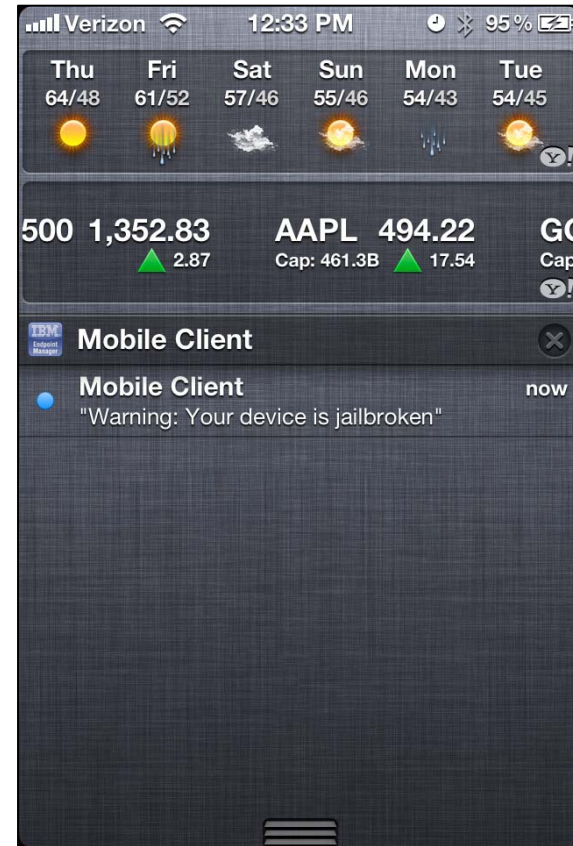
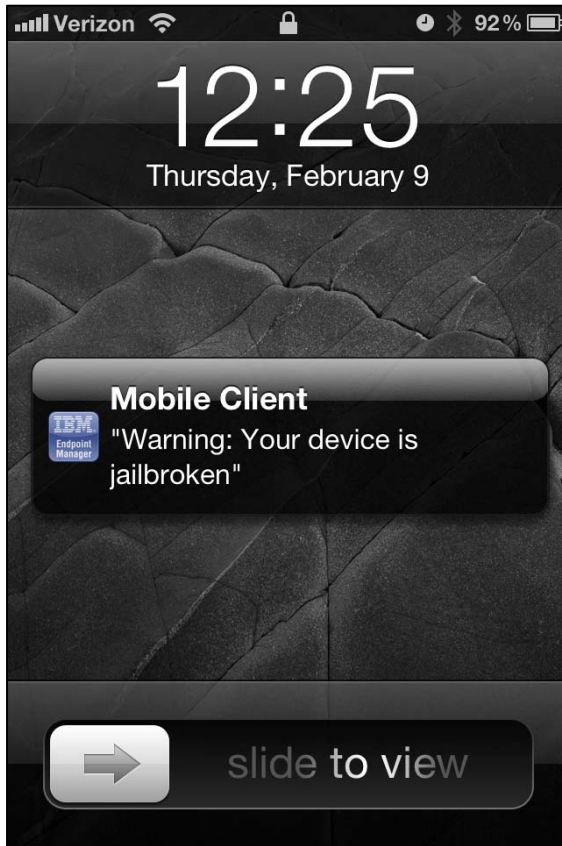
MDM Functionality Overview

Category	Endpoint Manager Capabilities
Platform Support	Apple iOS, Google Android , Nokia Symbian, Windows Phone, Windows Mobile
Management Actions	Selective/full wipe, deny email access, remote lock, user notification, clear passcode
Application Management	Application inventory, enterprise app store, iOS WebClips, whitelisting/blacklisting
Policy and Security Management	Password policies , device encryption, jailbreak/root detection, disable iCloud
Location Services	Track devices and locate on map
Enterprise Access Management	Configuration of Email, VPN, Wi-Fi, Authenticated Enrollment, Self Service Portal
Expense Management	Enable/disable voice and data roaming
Cloud Email Device Management	Office 365 support
Containerisation	Nitrodesk Touchdown for Android

App Management



Jailbreak / Root Detection – Warn Users, Notify Administrators, Take Action



A “Single Device View” enables administrators and helpdesk personnel to easily view device details and take required action

The screenshot shows a Windows Internet Explorer browser window displaying Google Maps. The address bar contains the URL `http://maps.google.com/maps?q=44.801100,-68.777800`. The search bar contains the text `44.801100, -68.777800 (Location of device Harrison's DROIDX as of Wed Jun 6 15:41:47 GMT+1000 2012)`. The map shows a location in Bangor, Maine, with a red location pin labeled 'A'. A pop-up information window is open over the pin, displaying the following text:

Location of device Harrison's DROIDX as of Wed Jun 6 15:41:47 GMT+1000 2012 [more info](#) ☆
 44.801100, -68.777800

Below the text is a small street view image and a [Street view](#) link. At the bottom of the pop-up are links for [Directions](#), [Search nearby](#), [Save to map](#), and [more](#).

The map interface includes standard Google Maps controls: a search bar, a 'Get directions' button, a 'My places' button, and a 'Sign in' button. The map shows streets such as Hammond St, Union St, and Kenduskeag Stream Park. A satellite view inset is visible in the top right corner.

Delivering for multiple mobile platforms

IBM Worklight

Fast and cost-effective development, integration and management of rich, cross-platform mobile applications



Client Challenge

Using standards-based technologies and tools and delivering an enterprise-grade services layer that meets the needs of mobile employees and customers

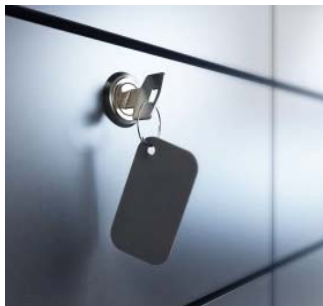
Key Capabilities

Mobile optimised middleware

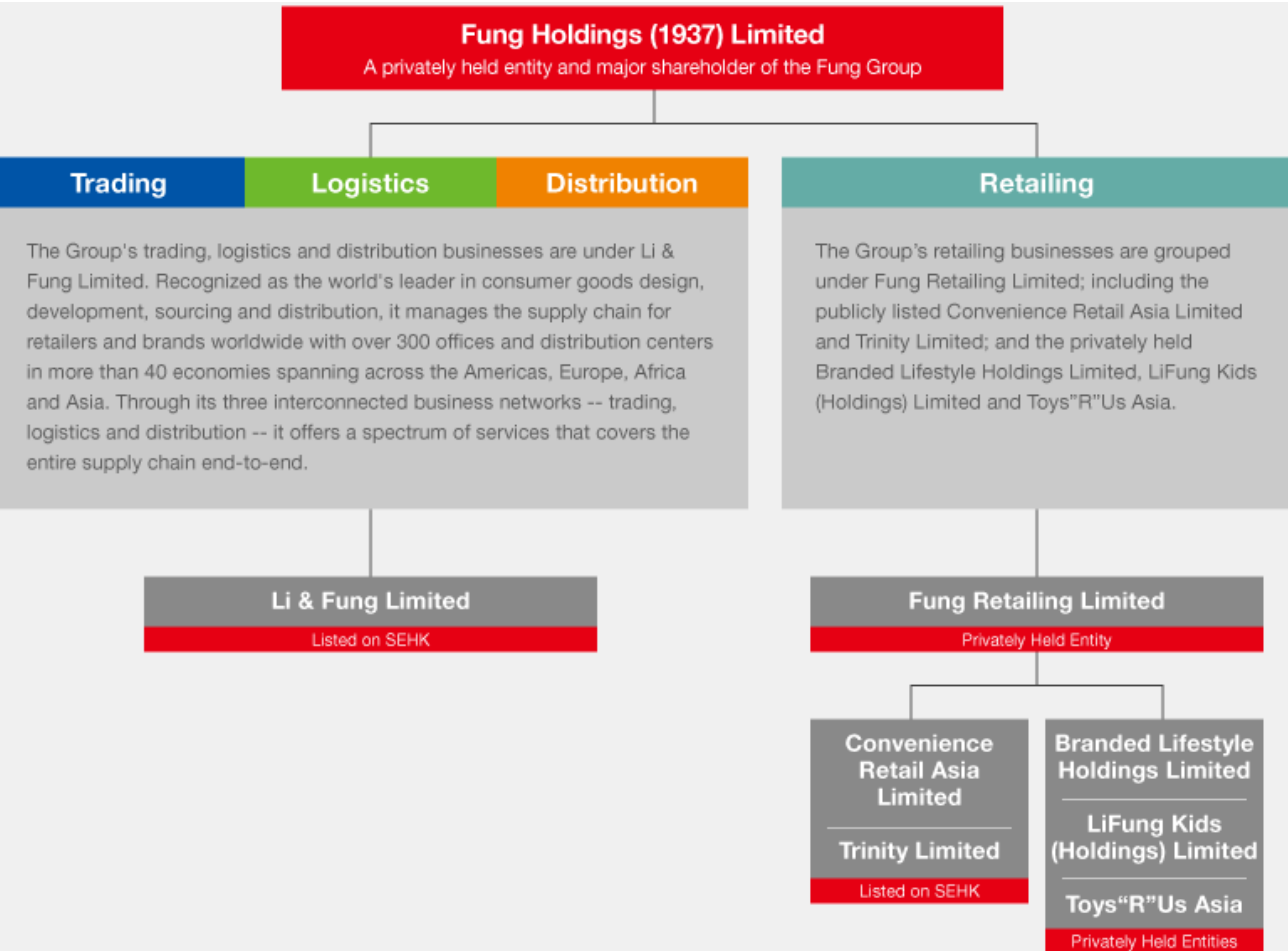
- Open approach to 3rd-party integration
- Mix native and HTML
- Strong authentication framework
- Encrypted offline availability
- Enterprise back-end connectivity
- Unified push notifications
- Data collection for analytics
- Direct updates and remote disablement
- Packaged runtime skins

Encrypted cache on-device

- A mechanism for storing sensitive data on the client side
- Encrypted - like a security deposit box



Case Study: Li & Fung Group



Endpoints: 30,000 +

Geography: 40+

Over 240 Offices & DC's
Over 3,000 retail outlets

OS:
XP, Win7, 2003 server, 2008 server, Windows Mobile 6.x, Mac (10.x), Red Hat ES 5.5

3 Global Data Centers

Overview of endpoint management challenges

- Complex nature of legacy endpoint management platform
Limitations, support, performance, accuracy, consolidation.
- Large number of endpoints and growth
Acquisitions and integration strategies
- Geographic distribution of endpoints
Office based, mobile, retail, factory and warehouse
- Asia & Global Complications/Challenge
Network bandwidths, latencies, blocking and stability
- Pace of change
Rollout of updates, security management and patches

How Tivoli End Point Manager has helped

It does what they says on the box!

Was told: *“Fast and Easy Rollout”*

>15,000 rollout out within 15 working.

Was told: *“Less Complex, Lower TCO”*

Before: 79 dedicated servers and 42 Database licenses

Now: 1 TEM, 1 Report, 1 Remote Control, 2 Databases licenses.
Leveraged Existing local servers as relay servers

Was told: *“Endpoint resources < 2% and controllable”*

Before 12 local processes, >8% CPU and >40MB

IBM 5 local processes < 2% CPU and < 30MB

Was told: *“Near real-time and flexible reporting”*

Before Next day, batch based, limited adhoc reporting

IBM Near real-time, flexible and highlighted legacy report was on 70% accurate!

Our Approach and Next Steps

Fast POC converted to Production environment

- Dedicated and specific scope, no more no less, keep it simple.
- No workarounds, use the product how it works
- Committed to the outcome.

What did we get?

- A lot more than we expected!
- More business decisions based accurate data
- Examples: Licenses, Performance (EUE), Security, Patch Management, Budgets, Antivirus

Next Steps

- Not Just EPM now!
- Inventory scanning, reporting, Software/Configuration deployment, Remote Control, Software usage report, Patch Management, Core Protection including Anti-Virus and Device Control, Security, Power Management

Summary

- **Android and iOS devices have quickly penetrated the enterprise**, bringing productivity gains, along with increased risk and cost
- IBM Endpoint Manager for Mobile Devices delivers strong MDM capabilities in an infrastructure that enables **unified management of all enterprise devices** – desktops, laptops, servers, smartphones, and tablets
- IBM is uniquely positioned to deliver **end-to-end app and mobile device lifecycle management** with Mobile Enterprise Application Platform (MEAP) and Mobile Device Management (MDM)
- Start developing your own BYOD policy by using IBM's six step policy as an example



ibm.com

Legal Disclaimer

- © IBM Corporation 2012 All Rights Reserved.
- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- If the text contains performance statistics or references to benchmarks, insert the following language; otherwise delete:
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 many factors, including 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 results similar to those stated here.
- If the text includes any customer examples, please confirm we have prior written approval from such customer and insert the following language; otherwise delete:
All 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.
- Please review text for proper trademark attribution of IBM products. At first use, each product name must be the full name and include appropriate trademark symbols (e.g., IBM Lotus® Sametime® Unyte™). Subsequent references can drop "IBM" but should include the proper branding (e.g., Lotus Sametime Gateway, or WebSphere Application Server). Please refer to <http://www.ibm.com/legal/copytrade.shtml> for guidance on which trademarks require the ® or ™ symbol. Do not use abbreviations for IBM product names in your presentation. All product names must be used as adjectives rather than nouns. Please list all of the trademarks that you use in your presentation as follows; delete any not included in your presentation. IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.
- If you reference Adobe® in the text, please mark the first use and include the following; otherwise delete:
Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- If you reference Java™ in the text, please mark the first use and include the following; otherwise delete:
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- If you reference Microsoft® and/or Windows® in the text, please mark the first use and include the following, as applicable; otherwise delete:
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- If you reference Intel® and/or any of the following Intel products in the text, please mark the first use and include those that you use as follows; otherwise delete:
Intel, Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- If you reference UNIX® in the text, please mark the first use and include the following; otherwise delete:
UNIX is a registered trademark of The Open Group in the United States and other countries.
- If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.