Real Time End Point Management In a Mobile World

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

PCTY2012

Pulse Comes to You

Optimizing the World's Infrastructure

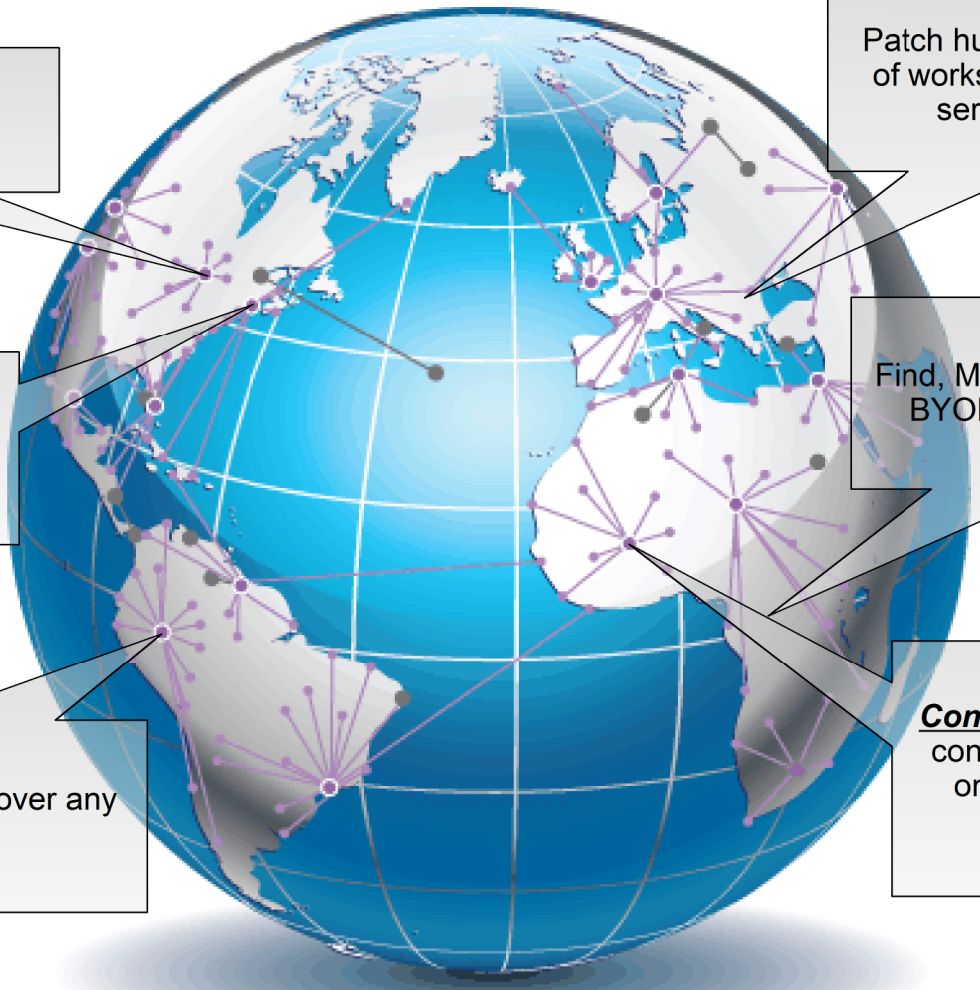
© 2012 IBM Corporation

Visibility is key in a constantly changing, distributed world

Critical systems are globally distributed and in constant flux

Find all assets on your network – NOW!

Patch hundreds of thousands of workstations, laptops and servers in minutes.



Deploy a software application worldwide in days.

Find, Manage and Secure your BYOD and Smart Devices

Patch anywhere, anytime over any network.

Continuously enforce security configuration baselines, even on mobile and off-network devices.

End Point Manager: The Power of One

Faster, Smarter Systems Management

- **See** all endpoints: physical, virtual, fixed, mobile
- **Fix** issues anywhere in minutes regardless of bandwidth or connectivity
- **Deploy** in days: any network size, OS, geography
- **Save** IT time and achieve fast payback

Endpoint management: The Three Cs

Complexity

- Manage Complexity, Simplify and Automate
- Coordination across business processes through the organization
- Heterogeneous endpoints, networks, applications and Os's
- Manage from the datacentre, to the desktop, out to the device.

BigFix Large Enterprise Customers *Sample*	Devices
Fiberlink	800,000
US Department of Veterans Affairs	470,000
Intel Corporation	350,000
Los Angeles Unified School District	276,000
Kaiser Permanente	241,900
Wal-Mart Stores	200,000
Verizon Communications Inc.	186,000
Sinopec	181,200
Merrill Lynch / Bank of America	140,000
Miami-Dade Unified School District	121,000
Deutsche Bank AG	110,000
China Ministry of Rails	103,000
Morgan Stanley and Co Incorporated	100,000
US Federal Bureau of Investigation	100,000

Compliance

- Ensure Compliance, Reduce Risk
- Security vulnerabilities
- Inaccurate inventory
- Industry regulation compliance and auditing (COBIT, SOX, HIPAA, EMA and more)

Cost

- Reduce TCO & Operational Costs
- Remove manual intervention
- Remove unnecessary configuration diversity
- Improve efficiency

PCTY2012

What Does End Point Manager Do?

- Gives IT the visibility, speed, adaptability, control, and precision to do more with less
- Packaged Specific Solution Areas:
  - Systems Lifecycle Management
  - Core Protection & DLP & DC
  - Security & Compliance Management
  - Patch Management (s/alone)
  - Power Management (s/alone)
  - Mobile Device Management
  - Software Use Analysis
- As well as solving unforeseen problems such as…….

DISCOVER IN MINUTES:

- How many machines are hardware-compatible with Win7?
- Which laptops are affected by a manufacturer's battery recall?
- What software are we paying for vs. what we're using?

RESULTS IN MINUTES:

- Automatically target machines for migration that are hardware-ready
- Precisely manage battery/hw replacements
- Reduce software spend based on accurate usage patterns

End Point Manager : How it Works

Lightweight, Robust Infrastructure

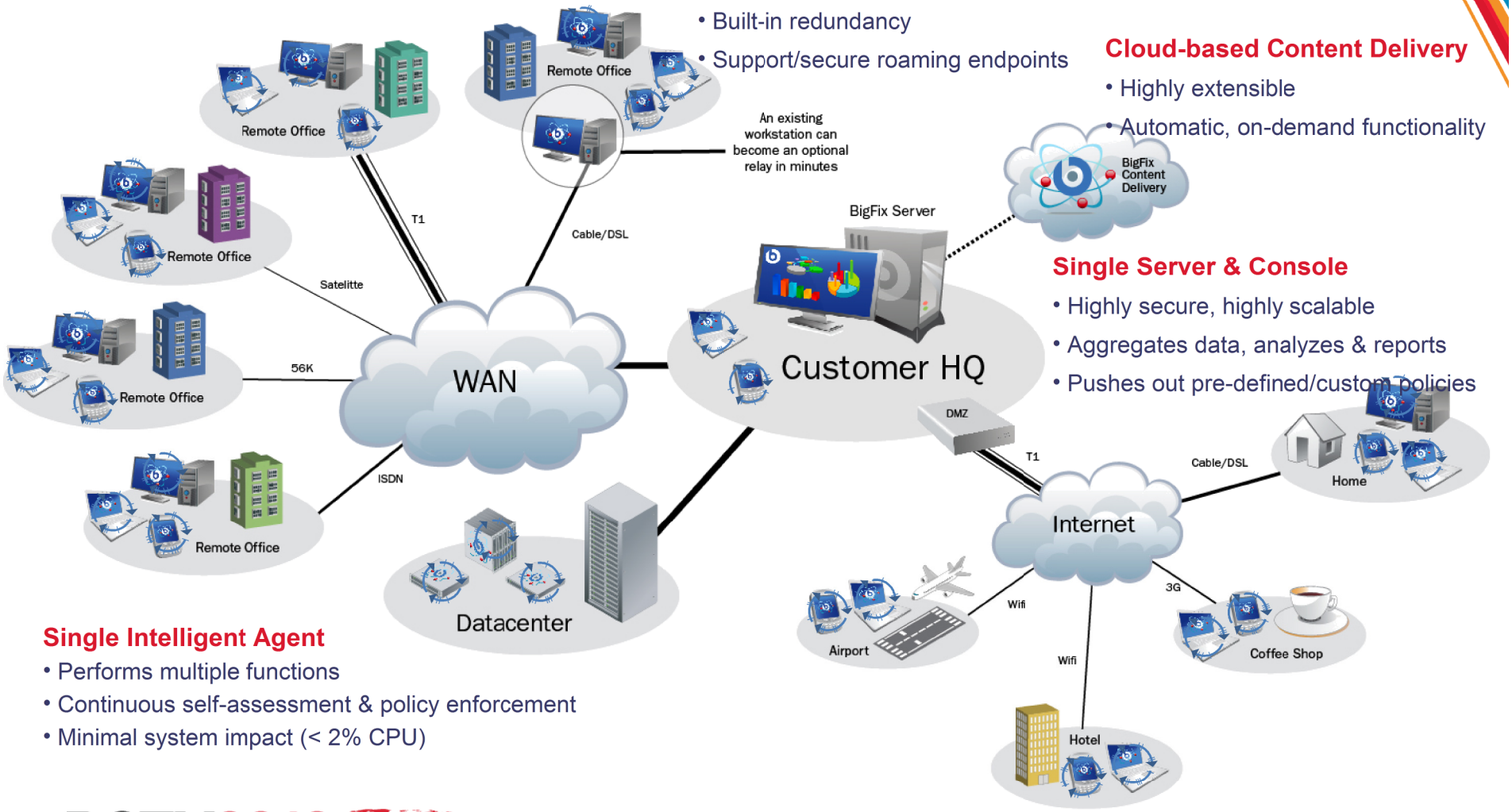
- Use existing systems as Relays
- Built-in redundancy
- Support/secure roaming endpoints

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

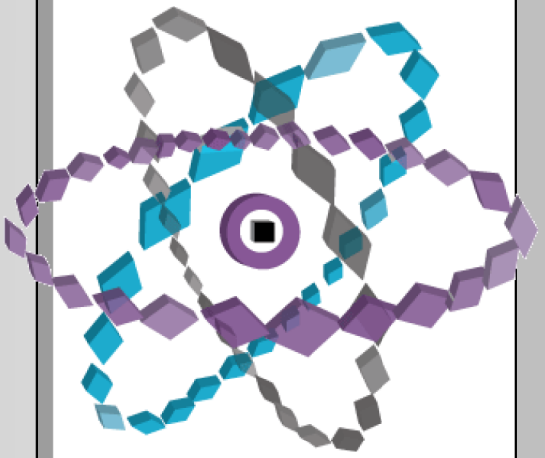
- Performs multiple functions
- Continuous self-assessment & policy enforcement
- Minimal system impact (< 2% CPU)

Tivoli Endpoint Manager, built on BigFix technology: Converged Capability.

Tivoli Endpoint Manager IT Operations Solutions

- Tivoli Endpoint Manager for Lifecycle Management
- Tivoli Endpoint Manager for Mobile Device Management
- Tivoli Endpoint Manager for Patch Management
- Tivoli Endpoint Manager for Power Management
- Tivoli Endpoint Manager for Software Use Analysis

Unifying IT operations and security



Tivoli Endpoint Manager IT Security Solutions

- Tivoli Endpoint Manager for Security and Compliance
- Tivoli Endpoint Manager for Core Protection
- Tivoli Endpoint Manager for Mobile Device Management
- Tivoli Endpoint Manager for Patch Management

Endpoint Manager Value Across the Enterprise: Relevance

Unified Endpoint Management

Microsoft Windows • Mac OSX • IBM AIX • HP-UX • Solaris • VMWare ESX Server •
7 versions of Linux • iOS • Android • Symbian • Windows Mobile

Mobile Workforce

- Enable password policies & 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

IT Operations

- Compress patch cycles to minutes-hours with 98-99% first pass success
- Patch 80+ OS variations and popular 3rd Party Windows applications
- Software distribution
- OS deployment
- Remote control
- Server management

IT Security and Compliance

- Ensure continuous compliance across all endpoints, regardless of location of network connectivity
- Security configuration baselines
- Vulnerability assessment
- Network self-quarantine
- Personal firewall
- Multi-vendor anti-malware management
- Endpoint protection

Facilities

- Reduce annual electricity costs by $20-$50 per PC/Mac
- Wake-on-LAN
- Current power usage baselines and savings models

IT Asset Management

- Attain real-time visibility and control
- Network discovery
- Managed endpoint hardware inventory
- Managed endpoint software inventory
- Software use Analysis to reclaim under used applications
- PC software license compliance analysis

1 console, 1 agent, 1 server, many OSs

AND.....

One billion consumers will have smart phones by 2016.

By 2016, 350 million employees will use their smart phones – 200 million will bring their own

Mobile spend will reach $1.3 trillion as the mobile apps market reaches $55 billion in 2012

Table and smart phone apps, average price of $2.43 USD, will grow to $56 billion in 2012

Business spending on mobile projects will grow 100% by 2015

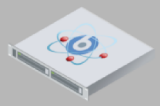
IT professionals will respond to the onslaught by diverting IT budgets to mobile technology

35% of the technology economy

We are Not New to this…..!

Traditional Endpoint Management

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



Mobile Device Management

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

- 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

IBM & Business Partner Confidential

Benefits of an Endpoint Manager based Approach to Mobile Device Management

- "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	Fast Time-to-Value
• "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	• 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

Mobile Devices Create New IT Challenges

Mobile devices magnify existing challenges and also pose unique ones that significantly disrupt traditional management paradigms.

Traditional Mgmt Model	New Device Mgmt Paradigm
Enterprises provide all equipment	Employees bring personal devices (BYOD)
Small set of supported platforms / models	Many different manufacturers / models
IT initiates and manages upgrades	OS/app upgrades managed by carriers, OEMs, users
IT tightly controls apps and security	Users control their own devices

<u>Options for IT departments</u>

Don’t allow mobile devices because they are too hard to manage ✖

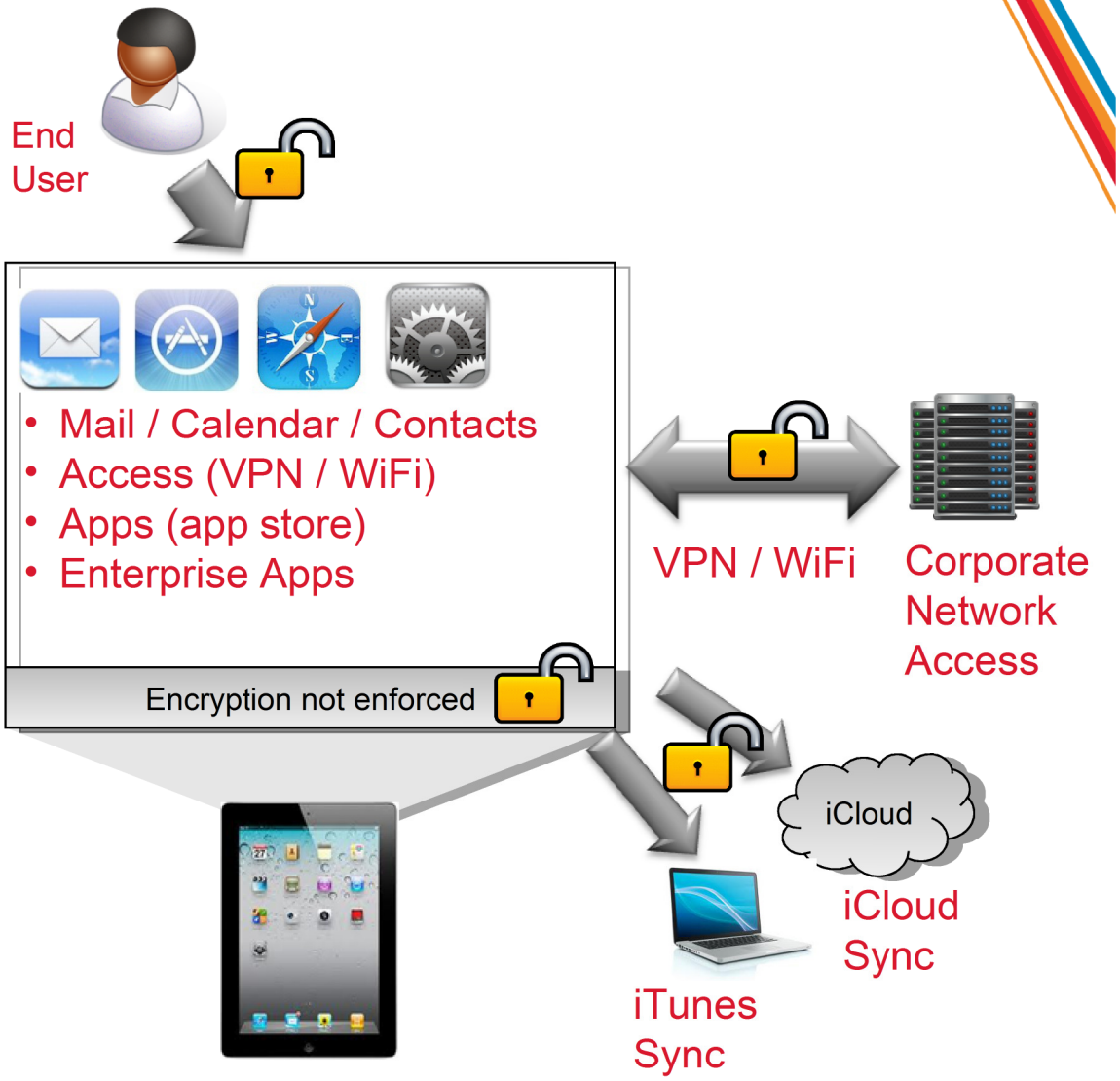
Allow unmanaged and insecure mobile devices ✖

Invest in tools to secure and manage devices ✔

Managing Mobile Devices – The Problem

Security & Management Challenges

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



End Point Manager:
MDM Functionality: Same Tech

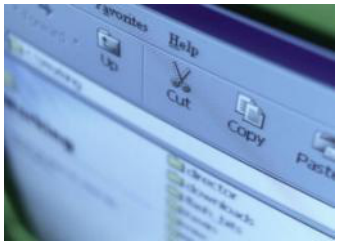
Category	Endpoint Manager Capabilities
Platform Support	Apple iOS, Google Android, Nokia Symbian, Windows Phone, Windows Mobile
Management Actions	Selective wipe, full wipe, deny email access, remote lock, user notification, clear passcode
Application Management	Application inventory, enterprise app store, whitelisting, blacklisting, Apple Volume Purchase Program (VPP)
Policy & Security Management	Password policies, device encryption, jailbreak & root detection
Location Services	Track devices and locate on map
Enterprise Access Management	Configuration of Email, VPN, Wi-fi
Expense Management	Enable/disable voice and data roaming

End Point Manager Patch Management

TEM Patch Management is a comprehensive solution for delivering Microsoft, UNIX, Linux, and Mac patches, as well as third-party application patches, through a single console.

Features and Benefits

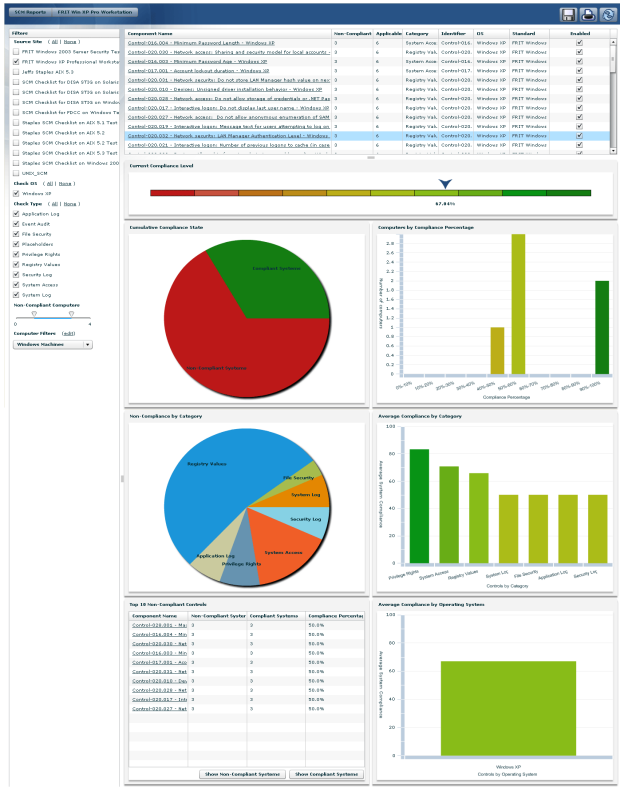
- Patch capabilities for multiple platforms: Windows, Linux, UNIX, Mac
- Coverage for a variety of software vendors, such as Adobe, Mozilla, RealNetworks, Apple, and Java
- Real-time reporting that provides information on which patches were deployed, when they were deployed, who deployed them, and to which endpoints
- Scalability—manage more than 250,000 endpoints from a single server
- No loss of functionality over low-bandwidth or globally distributed networks. Compression of patch cycle!



End Point Manager Security & Compliance Management

Comprehensive solution for end-to-end security and compliance management which includes:

- Asset Discovery
- Patch Management
- Security Configuration Management
- Vulnerability Management



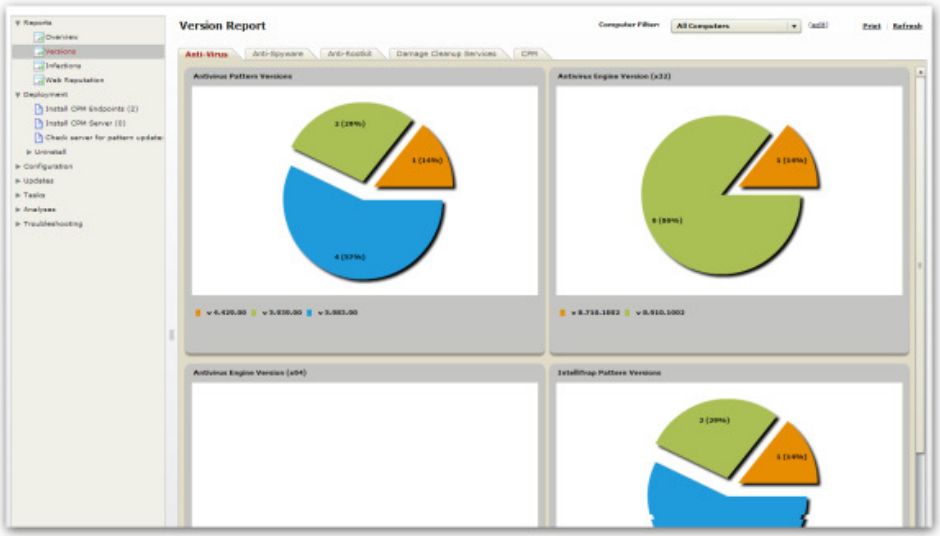
Features and Benefits

- Continuous enforcement of security policies, regardless of network connection status
- Host-based vulnerability assessment with severity scoring and a 99.9% accuracy rate
- Define and assess client compliance to security configuration baselines
- SCAP certified for FDCC, EAL-3 and more.
- Heterogeneous platform support: Windows, UNIX, Linux, and Macintosh

BigFix / TEM Core Protection

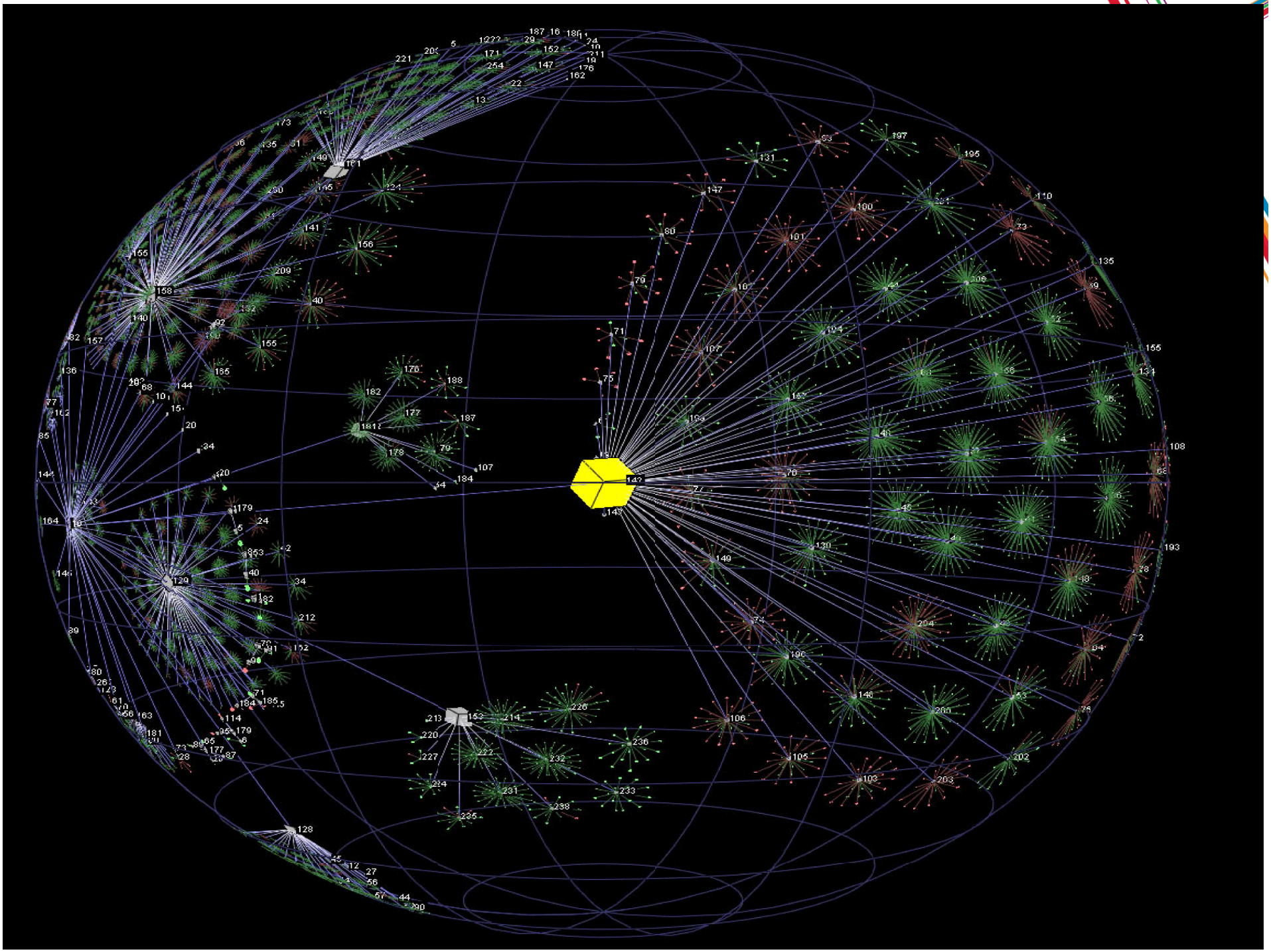
IntegratedCore Protection modules include:

- Anti-Virus
- Anti-Malware
- Endpoint Firewall
- Web Protection
- Client Manager for Endpoint Protection
- Network Access Control (NAC)



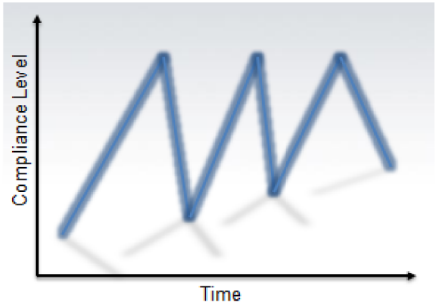
Features and Benefits

- Prevent infection, identity theft, data loss, network downtime, lost productivity, and compliance violations
- Eliminate security gaps with real-time threat intelligence
- Achieve unparalleled visibility into complete enterprise protection
- Combine endpoint protection, security configuration, compliance, patch, DLP, DC….etc.

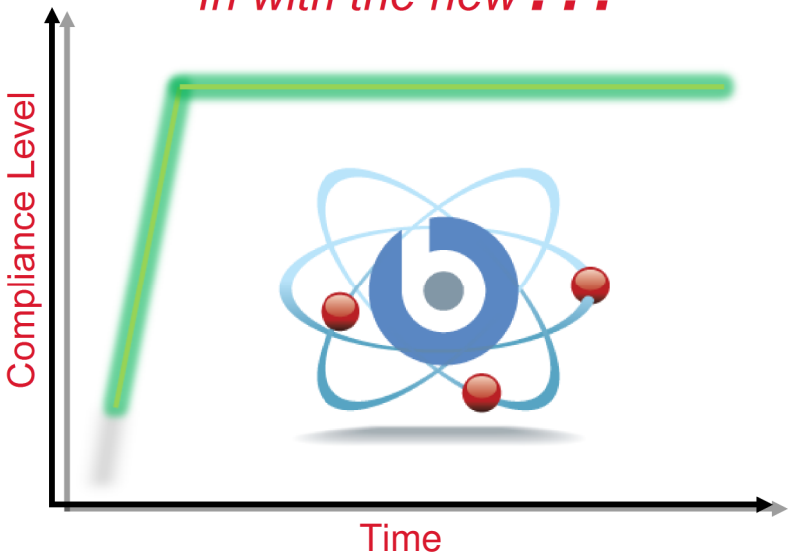


Compliance:DataCenter to Desktop to Device
Raise the bar and manage the right way!

Out with the old…



In with the new . . .



Continuous Compliance with BigFix

- Initial low-cost hit to get compliant
- Continuous assessment, identify non-compliance within minutes
- Enforce compliance with minimal effort
- Overall reduced cost to maintain compliance and security.

Endpoint Manager Value : Drives Down Cost and Complexity

istributed architecture matches today's enterprise

andwidth Throttling for low bandwidth networks

ffective mobile and remote computer management

lazing Speed

00x faster than competing solutions

Massive Scalability

- Manage thousands to hundreds of thousands

Extreme Productivity

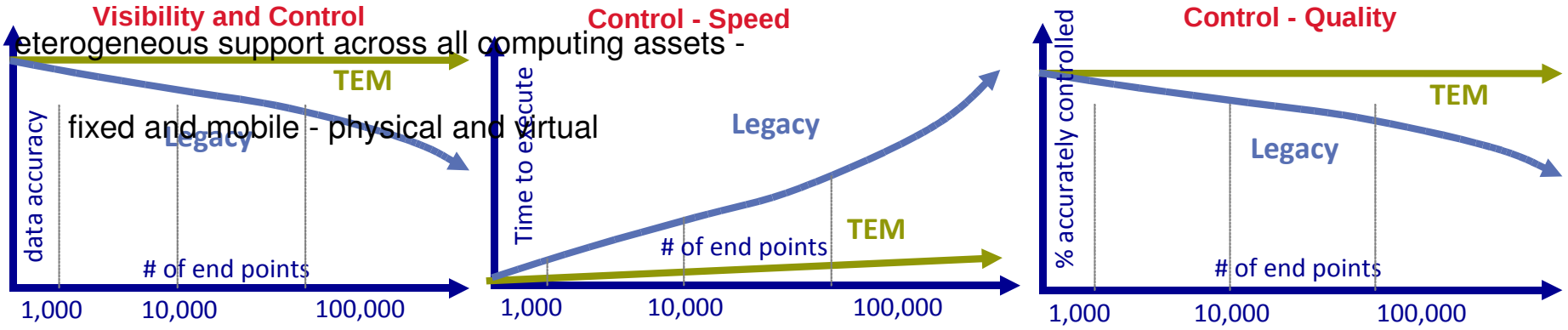
- 1 FTE performing the task of a dozen

Revolutionary Economics

- Proven ROI and the Lowest TCO

ervasive Visibility and Control

eterogeneous support across all computing assets - fixed and mobile - physical and virtual

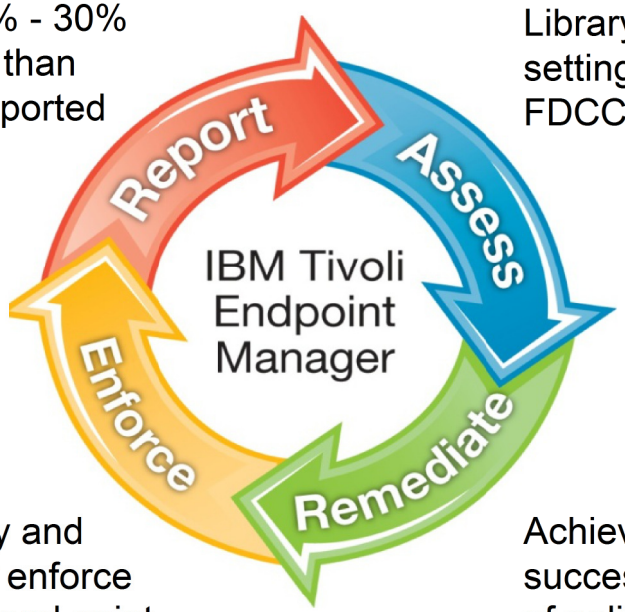


Tivoli Endpoint Manager: Security and Compliance across all Devices

See More, Secure More; Real Time Value. DC, to Desk, to Device

- Patch Management
- Security Config Mgmt
- Vulnerability Mgmt
- Asset Mgmt
- Network Self-Quarantine
- Multi-Vendor Endpoint Protection Mgmt
- Anti-Malware & Web Reputation Service, D.C and DLP.
- Software Distribution
- O.S Distribution
- Mobile Device Management

Discover 10% - 30% more assets than previously reported



Library of 5,000+ compliance settings, including support for FDCC SCAP, DISA STIG

Automatically and continuously enforce policy at the end point

Achieve 95%+ first-pass success rates within hours of policy or patch deployment

Common Criteria Certified EAL3

oval.mitre.org

cve.mitre.org

FIPS VALIDATED 140-2 FIPS 140-2 Inside

- Customer since 2007
- Protecting 240,000 WW endpoints
- Deal size - $2.65M

Business Problem

- Lacked automation and real-time analysis of compliance findings resulting in weeks of manual, labor - intensive procedures to collect and correlate scan data.
- Lacked the ability to automatically remediate and validate issues Identified during vulnerability assessments.
- Lacked ability to protect “non-connected” endpoints heightened by new & potential acquisitions in emerging markets.

Competition:

- Microsoft, HP, BMC

What they bought: - **IBM Tivoli Endpoint Manager for Lifecycle Management**

Why they bought it:

- Our rapid deployment and no additional infrastructure elements required.
- Flexibility and coverage on multiple operating systems and 3rd party applications.
- We could implement a solution in one week across 240,000 endpoints.
- Achieve automated, continuous compliance by leveraging common security checklists DISA STIG, FDCC, SANS Top 20, etc.
- Audit procedures have improved dramatically with hourly reporting verses weekly or monthly.
- Issues are identified in real-time and remediation tasks are executed automatically increasing efficiency and quickly closing critical gaps of exposure

Customer: US Department of Veterans Affairs

- Customer since 2006
- Protecting 420,000 endpoints
- Deal size $9.3M

Business Problem:

- Could not reach all of their enterprise machines within the acceptable time frame to maintain required security levels.

Competition:

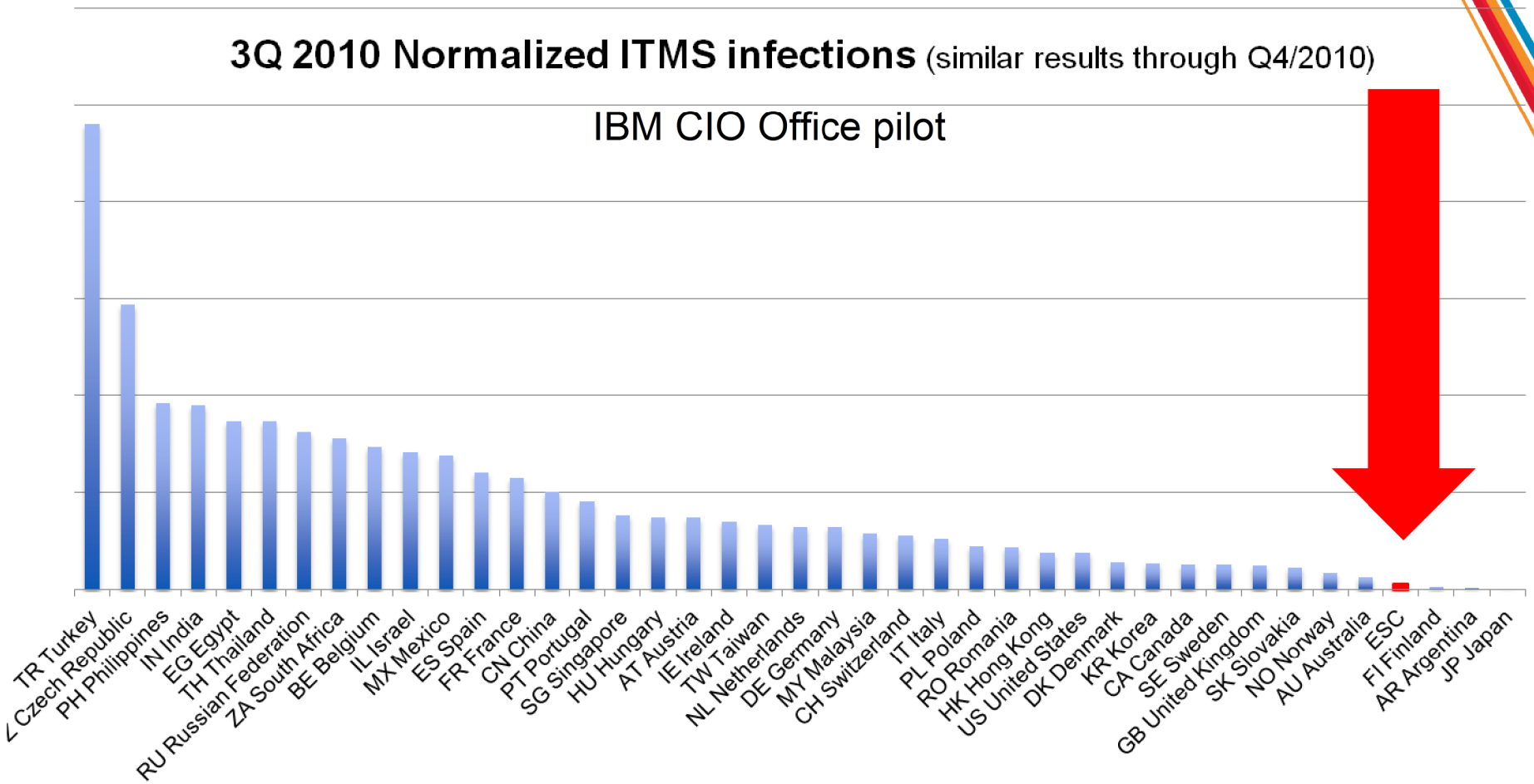
- Microsoft SCCM & Patchlink

What they bought: **IBM Tivoli Endpoint Manager for Security and Compliance**

Why they bought it:

- Demonstrated ability to rapidly identify, isolate and mitigate malware attacks.
- Patched 7,000 “un-reachable” machines in less then 1 hour.
- Confirmed in testing to be the only solution that could be deployed in one week ensuring the VA was protected.

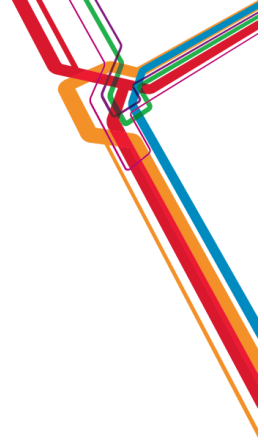
Tivoli Endpoint Manager in IBM Globally



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

IBM Pilot
Production 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*



Thank You !

keith.poyser@uk.ibm.com
+44 7711773878

Acknowledgements, disclaimers and trademarks

© Copyright 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 publication to IBM products, programs or services do not imply that they will be made 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, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. 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.

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.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

PCTY2012

Pulse Comes to You

© 2012 IBM Corporation