



PCTY2011



Pulse Comes to You

Optimising the World's Infrastructure



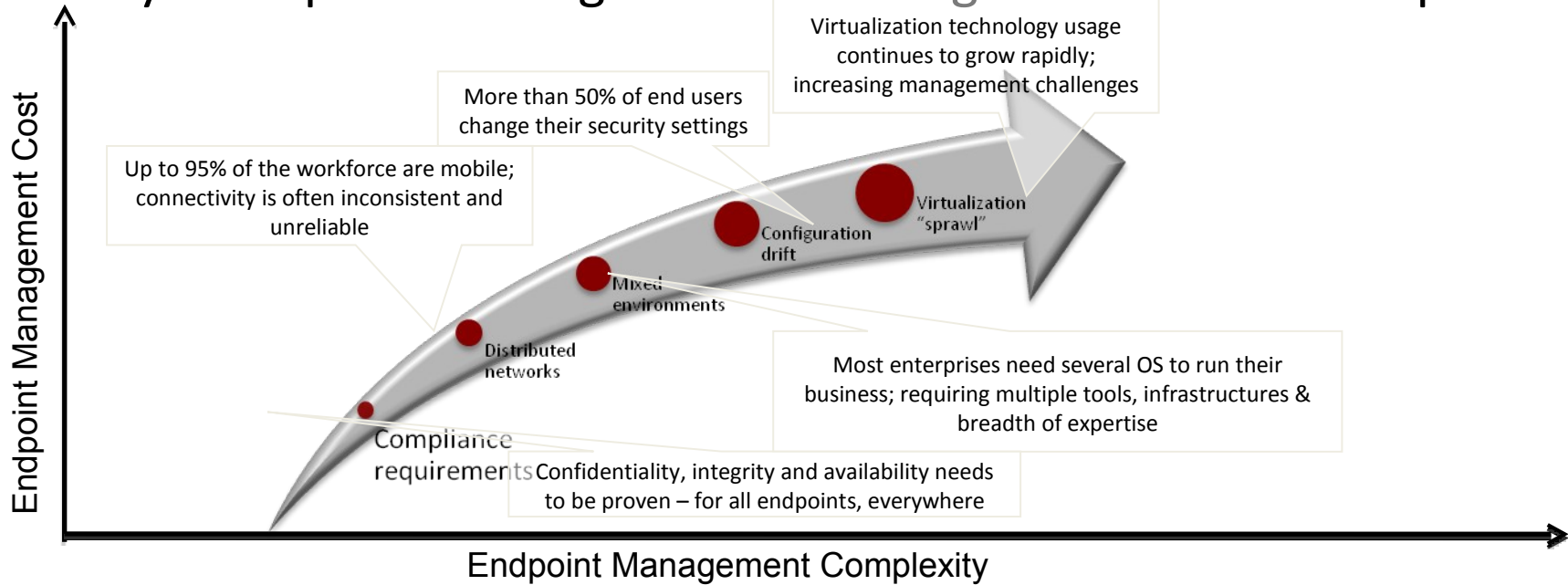
Manage Everything, Everywhere, in Real Time

Richard Betts

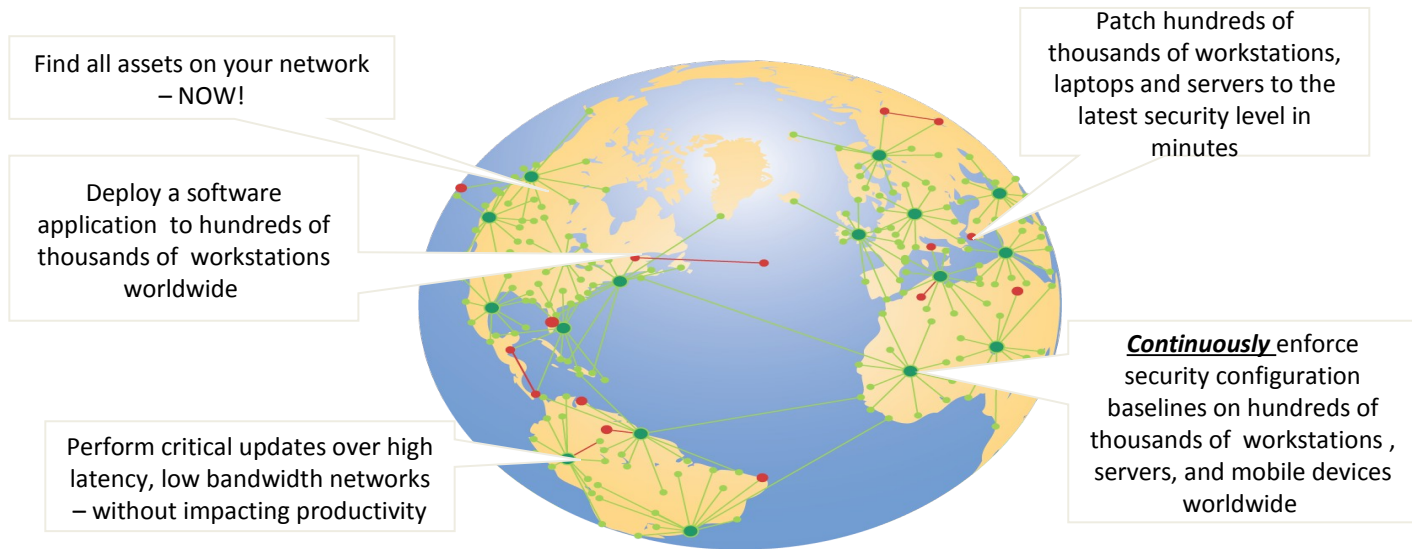
EMEA Technical Director

Tivoli End Point Manager, Built of Big Fix Technology

Today's Endpoint Management Challenges Drive IT Costs Up



Critical Systems are Globally Distributed and in Constant Flux





We believe IT and security operations should be simple.

•Helping to provide...

- Total visibility
- Quality of control
- Speed to remediation
- High scalability
- Versatile framework
- Rapid time to value
- Cost reduction

Through....

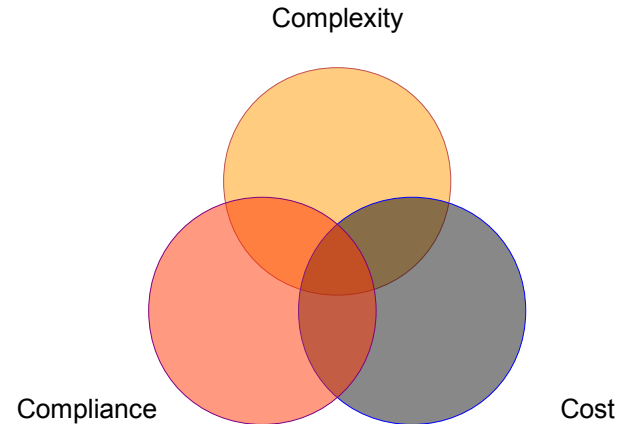
- Security configuration and vulnerability management
- Systems lifecycle management
- Endpoint protection
- Power management

To help..

- Consolidate management of multiple endpoint applications
- Reduce associated endpoint management costs
- Simplify endpoint operations and security to drive business value
- Improve visibility and central control across estate

Endpoint Management: The Three Cs

- Complexity
 - Manage Complexity , Simplify and Automate
 - Coordination across business processes through the organization
 - Heterogeneous endpoints, networks, applications and OSes
- Compliance
 - Ensure Compliance, Reduce Risk
 - Security vulnerabilities
 - Inaccurate inventory
 - Industry regulation compliance and auditing (COBIT, SOX, HIPAA, and more)
- Cost
 - Reduce TCO & Operational Costs
 - Remove manual intervention
 - Remove unnecessary configuration diversity
 - Improve efficiency



Tivoli Endpoint Manager: Bringing Sanity To Endpoint Compliance

Traditional compliance



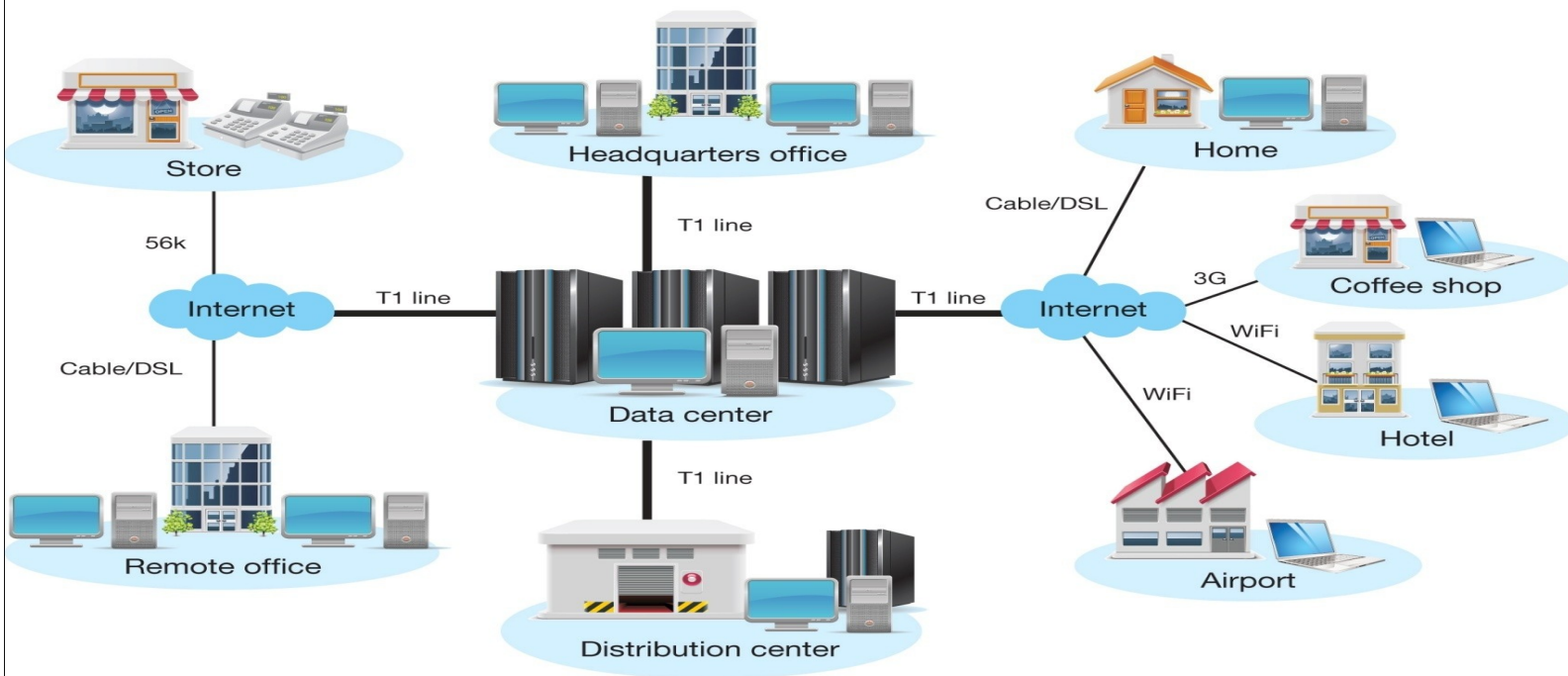
1. The security team develops compliance policies.
2. The security team runs an assessment tool (or tools) against that policy
3. The security team forwards findings to ops
4. Ops makes corrections as workload allows, one item at a time using different tools from security (which generates different answers to questions like “how many endpoints do I have?”)
5. Users make changes causing endpoints to fall out of compliance again
6. Start assessment all over again

Continuous compliance



1. Security and ops work together to formulate policies and service-level agreements (SLAs)
2. Ops implements the baseline (patch, config, AV, etc.) across all endpoints in the organization
3. Policy compliance is continuously monitored and enforced at the endpoint, changes are reported immediately
4. The security team can instantly check on the current state of security and compliance anytime
5. Security and operations teams work together to continually strengthen security and adjust to evolving requirements.

Beyond the Perimeter



Myriad of Devices to Manage and Secure



Old Solutions - New Challenges

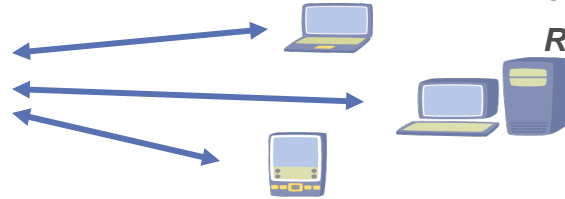
Central Servers

Aggregate Data
Analyze Data
Issue Instructions

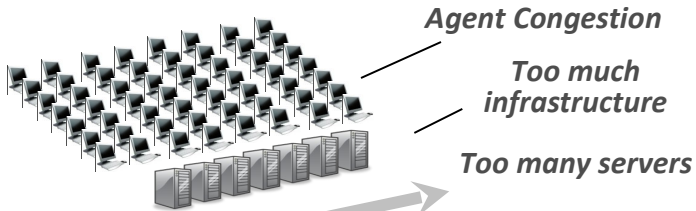


Dumb Clients

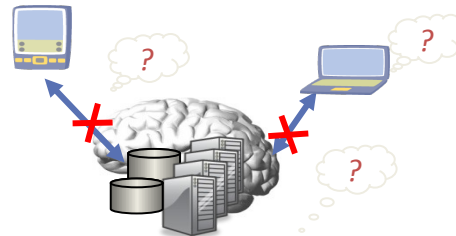
Follow Orders
Report data



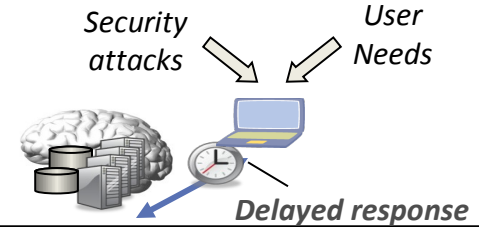
Issue 1: Global Management



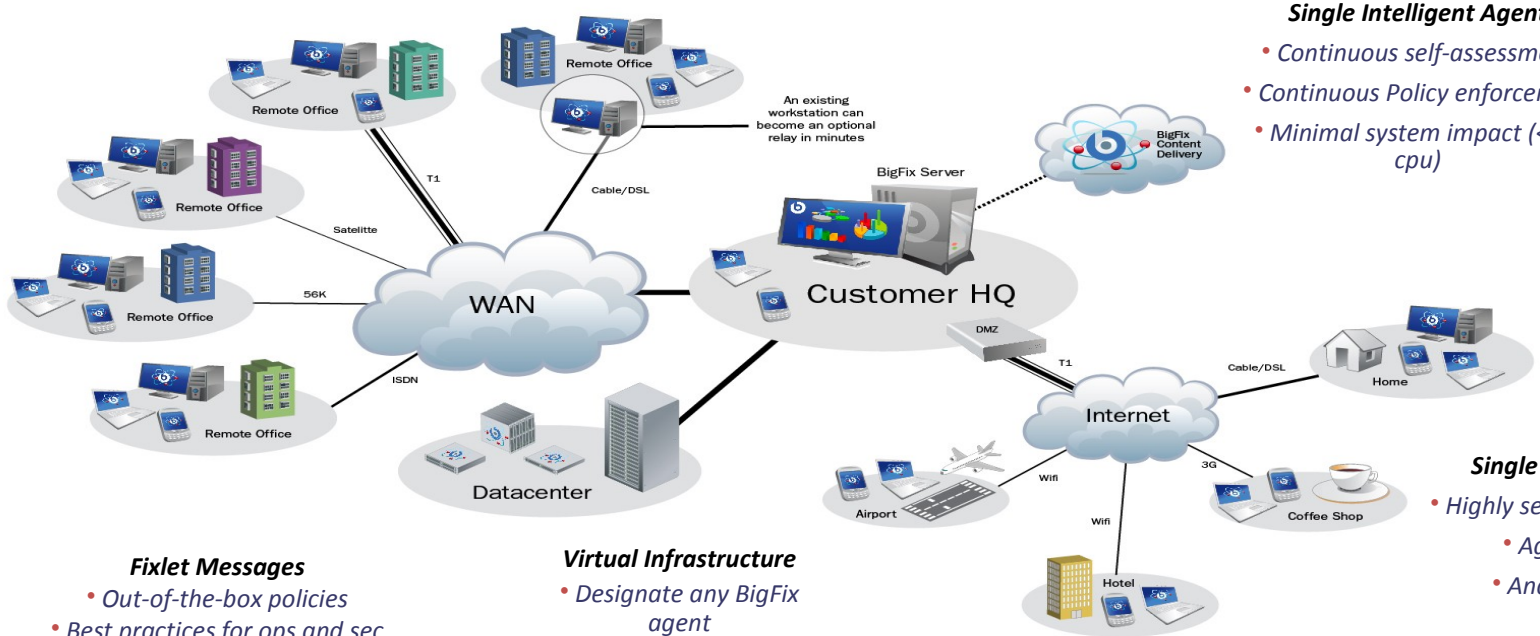
Issue 2: Mobility



Issue 3: Change Velocity



The Power of Distributed Intelligence



Single Intelligent Agent

- Continuous self-assessment
- Continuous Policy enforcement
- Minimal system impact (<2% cpu)

Single Server & Console

- Highly secure, highly available
- Aggregates data
- Analyzes & reports

Fixlet Messages

- Out-of-the-box policies
- Best practices for ops and sec
- Simple custom policy authoring

Virtual Infrastructure

- Designate any BigFix agent
- Built-in redundancy
- Leverage existing systems

Tivoli TEM Platform and Endpoint Manager Modules





TEM Components. Understand the Platform

- TEM Platform
 - TEM Server
 - Central management and reporting system
 - TEM Agent
 - Client component installed on all managed computers
 - TEM Relay
 - Multi-tier relay infrastructure between server and clients
 - TEM Console
 - Administration interface to system
- TEM Solutions
 - Pre-packaged content



TEM Server

- Scalability
 - Single server deployment over 250,000 endpoints
 - HA and cluster configurable
- Real-time
 - Visibility of endpoint statuses
- Open APIs
 - For inbound and outbound integrations
- Security
 - PKI 2 factor authentication



TEM Agent

- Intelligent and continuous
 - Enforces policies on or off network
- Transparent
 - Low resource utilization <1% CPU
- Multiplatform
 - All Windows, UNIX, Linux, Mac OSX, Windows Mobile, IOS* Blackberry*, Android*
- Patented Fixlet[®] technology
 - Programmable clients
 - *Coming Q4 2011



TEM Relay

- Existing infrastructure
 - No additional hardware/software required
- Lightweight and automatic
 - Easy production admin and configuration
- Centrally managed
 - As a client component
- Bandwidth management
 - Policy based and dynamic configuration



TEM Console

- Dashboard and reporting
 - Customizable reports and alerts
- Delegated administration
 - Assignment rights
- Real-time security posture and asset state
 - Point in time visibility and accuracy



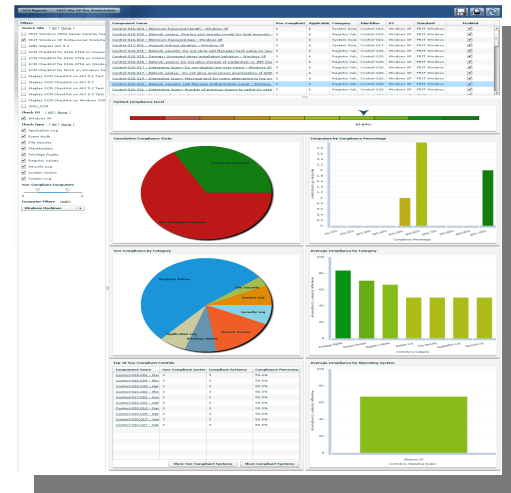
Key Platform Benefits

- Designed and proven for distributed and massively mobile estates
- Near Real Time Visibility and control of Assets, Fixed, Mobile, LAN or Internet
- Private Cloud for managing Laptops, Home Workers, Handheld, Smart Phones*
- Few Moving Parts, 99.9% uptime
- Consistent method to delivery solution
- Distributed intelligence, what is posture now
- Single Server, virtualized relays
- Lightweight, deployment in weeks

TEM for Security and Compliance

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

- 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
- Heterogeneous platform support: Windows, UNI X, Linux, and Mac OS X



TEM for Patch Management

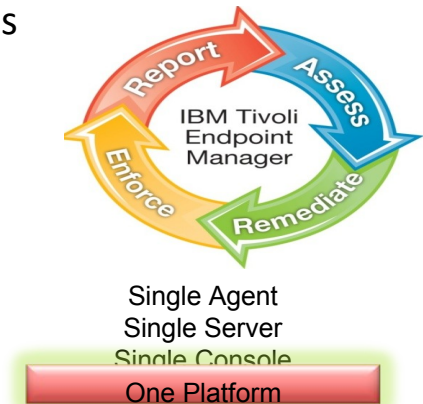
- Reduction in patch and update times from weeks and days to hours and minutes
- Increase first-pass success rates from 60-75% to 95-99+%
- System administrator workload reductions of 75% or more
- Assured compliance with internal and external standards/requirements
- Lightweight agent (<2% of CPU on average)



TEM for Lifecycle Management

Comprehensive solution for end-to-end systems management which includes:

- Dramatically reduced patch cycles and increased first-pass success rates
- Closed loop validation in real-time
- Massive scalability and support for remote and intermittently connected devices
- Detection and resolution of corrupted patches
- Multi-platform support (Unix, Linux, Windows, Mac OS X)



TEM for Power Management

- Cost savings (up to \$50 per year per TEM managed device) through reduction in energy usage and utility rebates where applicable
- Obtain max power savings while avoiding disruption to IT system management
- Project potential savings using “what-if” scenario calculator
- Single tool to identify misconfiguration and automatic remediation



Case Study: Financial Customer

Before TEM:

- Incumbent tool deployed on only 40,000 of 120,000 devices
- 15 configuration management software tools to manage entire IT environment
- Experienced a low 80% success rate with limited reporting capabilities

With TEM:

- TEM deployed on 120,000 devices
- Consolidated 15 configuration management tools into 7
- TEM is delivering 95% success rate with real-time reporting

Key Matrix	Before TEM	TEM
# of Managed Endpoints	40,000 out of 120,000	120,000
# of Locations	100+	800
Time to Install	8+ months for all infrastructure	1 week for all infrastructure
# of Required Administrators	20	4
# of Dedicated Servers	25	1
Time to complete an enterprise wide full discovery, remediation and reporting cycle	~7 days	~5 minutes

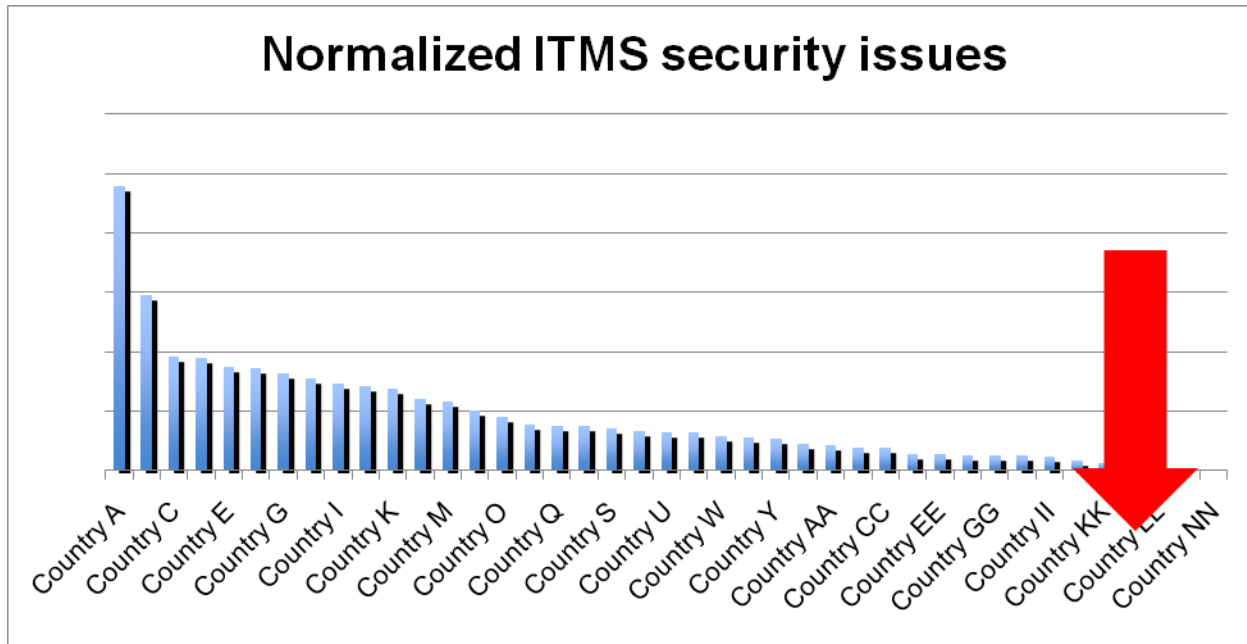


What the Analyst Say!

- "Time to protection with Tivoli End Point Manager is your biggest value add."
-Dan Blum, **Gartner (from RSA)**
- Gartner recognizes IBM TEM innovation, our strong presence in highly distributed, large enterprises and our ability to scale and as such considers us a Visionary in this market.
- Gartner also see IBM TEM as one of the few vendors with the vision to satisfy and support security and operational convergence as well as broad platform support.

IBM CIO Office Pilot of TEM

Normalized ITMS security issues



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

