



Pulse Comes To You 2012

Business Without **LIMITS**



Security

IBM Security

Intelligence, Integration, Expertise

Pulse Comes to You 2012

Business without **LIMITS**

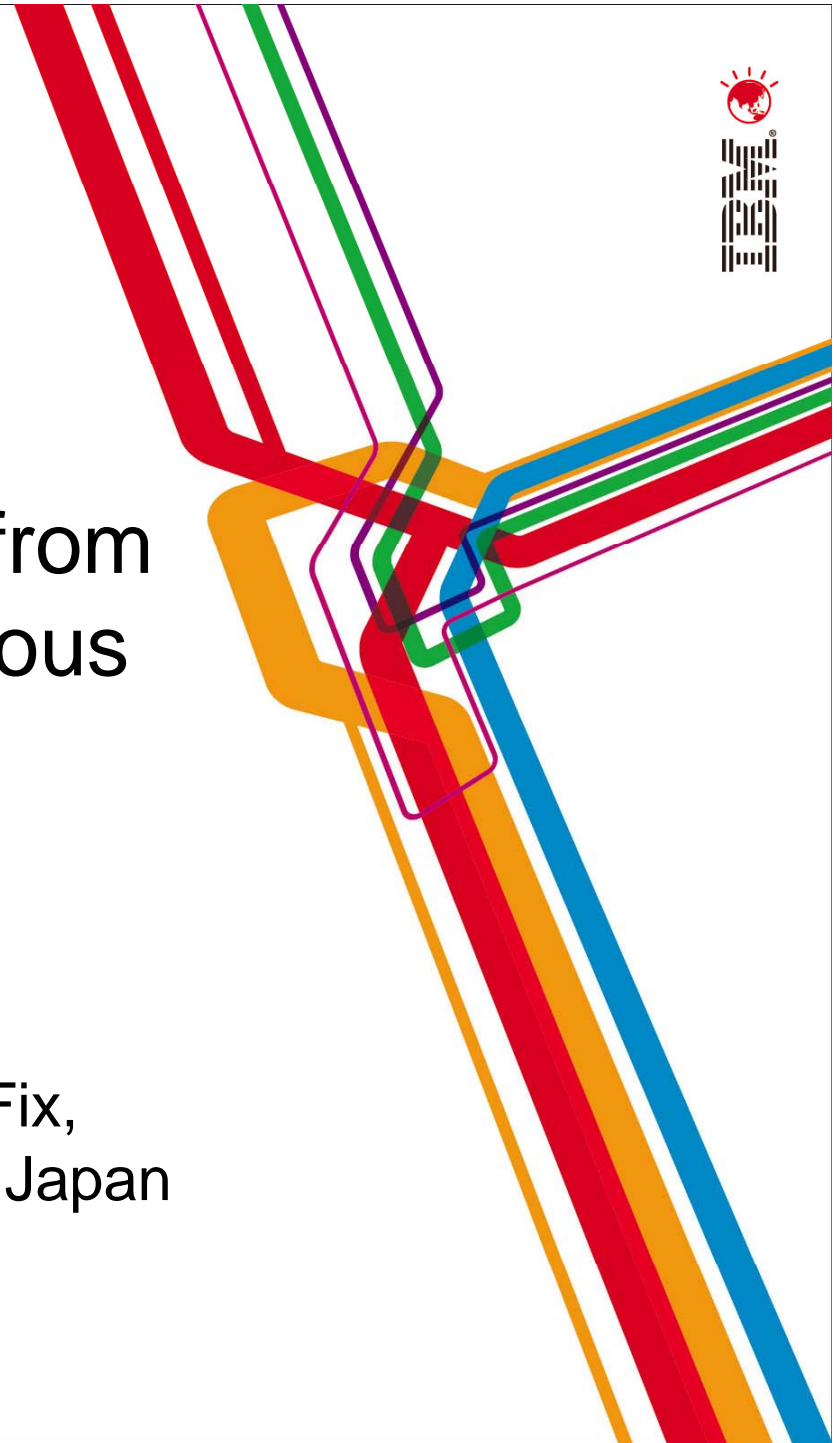
21 August | Thailand



Securing Your Endpoints from Malware and Other Malicious Threats

Steven Scheurmann

Sales Leader, Tivoli Endpoint
Management Products, built on BigFix,
IBM Software Group, Asia Pacific & Japan



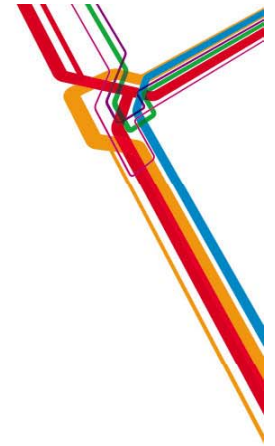
Key Drivers of Data Protection

Protection of **intellectual property**
(designs, source code, strategic plans)

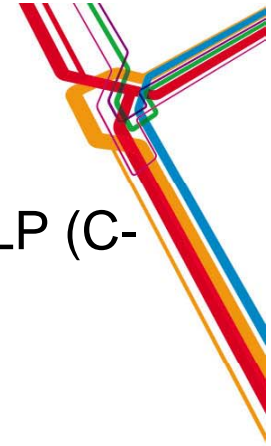
Compliance to public and private **regulations**
(PCI-DSS, HIPAA, SOX, GLBA, SB1386)

Risk Mitigation – Threats to brand and customer retention when breaches occur

Financial consequences of handling data breaches can be high due to lawsuits, communication with affected parties, credit monitoring services, loss of brand equity



Market Overview



Two market segments – Enterprise-DLP (E-DLP) and Channel-DLP (C-DLP)

E-DLP solutions cover multiple channels (network, endpoint, discovery), but are costly and difficult to implement

C-DLP and “DLP-lite” solutions cover a single channel, are simpler to implement, are less expensive, and address basic data protection requirements

Data Protection Add-on to TEM-CP is a C-DLP, or “DLP-lite” solution

What does Gartner say?

“As channel DLP and DLP-lite solutions evolve, more organizations are seeing value in these offerings”¹

“Gartner has seen a significant increase in channel DLP and DLP-lite deployments in large and small organizations.”²

¹ 2011 Buyer’s Guide to Content-Aware DLP, Gartner, August 2011

² Magic Quadrant for Content-Aware DLP, Gartner, August 2011

Key Benefits & Features of Data Protection Add-on



- **Real-time content scanning** of sensitive data
- **Out-of-the-box compliance templates** to detect credit card numbers, social security numbers, among other sensitive data
- **Monitoring and enforcement** of multiple egress points (email, browser, USB, etc)
- **Low TCO** – Addresses baseline data protection requirements with minimal cost and investment; scales to 250,000 endpoints on a single server

Tivoli Endpoint Manager, built on BigFix Technology



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

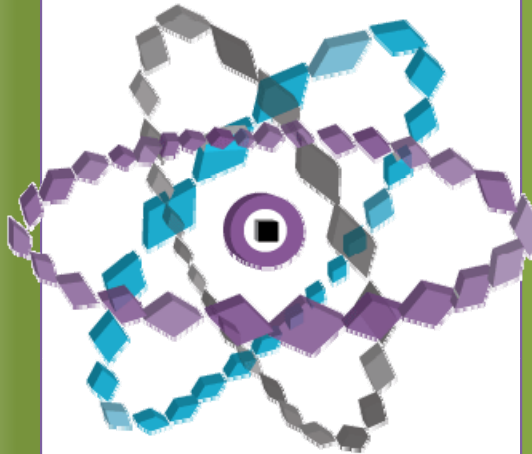


Tivoli Endpoint Manager for Power Management



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

Real Infrastructure Consolidation; True systems & security management convergence



Before IBM's Endpoint Manager

With IBM's Endpoint Manager

Software Distribution	e.g., Microsoft SMS/SCCM	
Patch Mgmt	e.g., LANDesk, Microsoft SMS/SCCM	
Security Configuration Mgt	e.g., Symantec, NetIQ, CA	
Asset & License Mgt	e.g., Altiris - Asset Manager	
Endpoint Data Protection	e.g., McAfee, Symantec, etc	



- 1 server
- 1 agent on end point
- 1 console
- Implemented in weeks

100 - 125 servers/5 different consoles/10 different agents on client, implemented over months and years

Pulse Comes to You 2012

Business without **LIMITS**

Pain Points with Existing Endpoint Data Protection (AV)



IT Operations

- **Bloated AV consumes too much CPU, network bandwidth, too many servers**
- **Too many tools, too much complexity**
- **Impacts virtualization costs, limits consolidation of VMs**
- **Can't validate compliance, visibility**

Compliance

- Lack of Evidence:**
- **need proof of compliance across multiple endpoints**
 - **Want single dashboard/view**

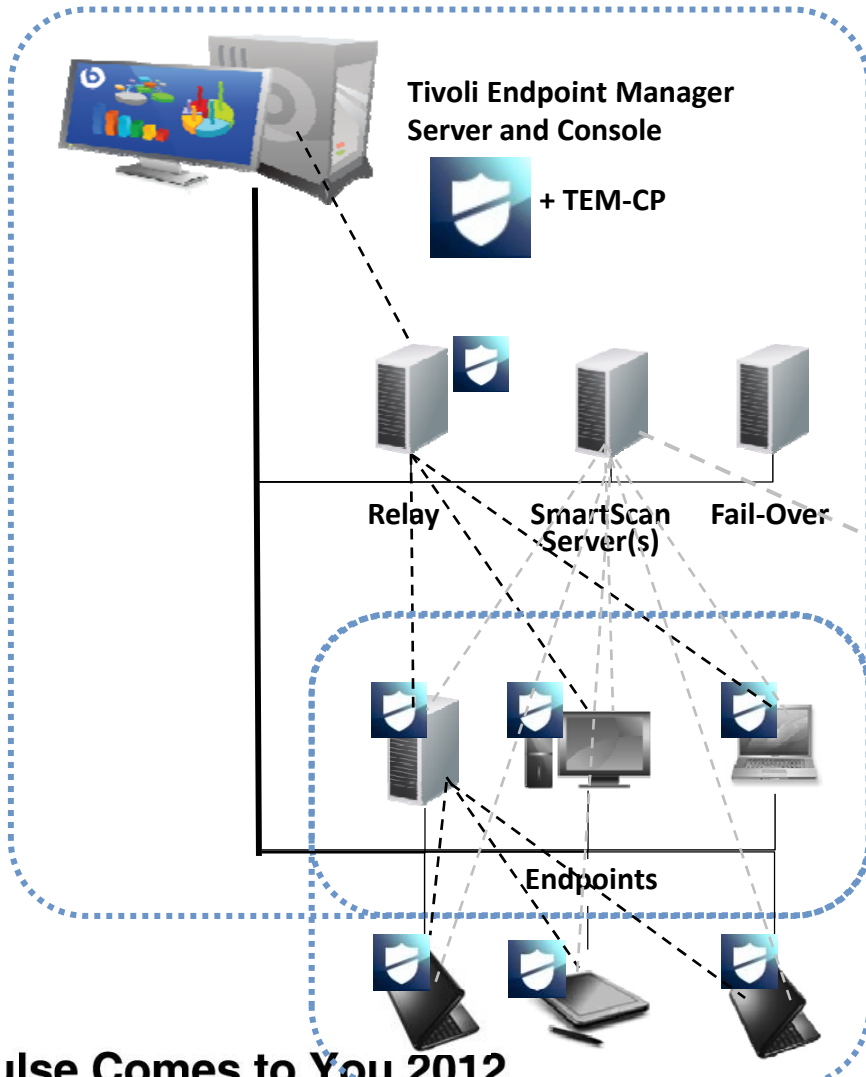
IT Security

- Security ineffective:**
- **Too slow to deploy, missing endpoints**
 - **Not effective in detecting new threats**
 - **Turned off by users due to performance issues**

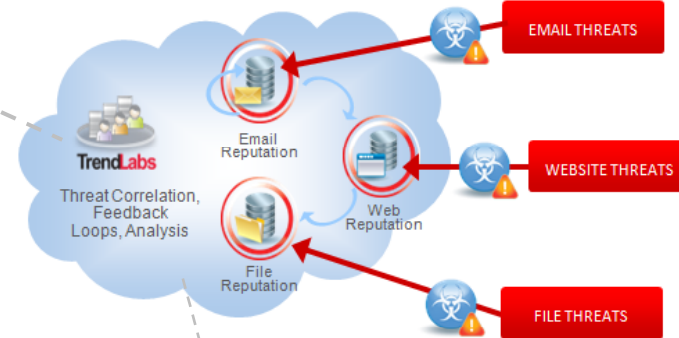
What is TEM-CP? IBM's Anti-virus / Anti Malware & Data Protection



Tivoli Endpoint Manager for Core Protection

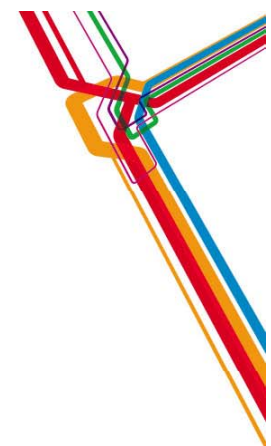


- **Anti-virus / Anti-malware** featuring:
 - Smart Protection Network
 - Web Reputation
 - File Reputation
 - Behavior Monitoring
- **Data Protection Add On**
 - Data Loss Prevention (DLP)
 - Device Control



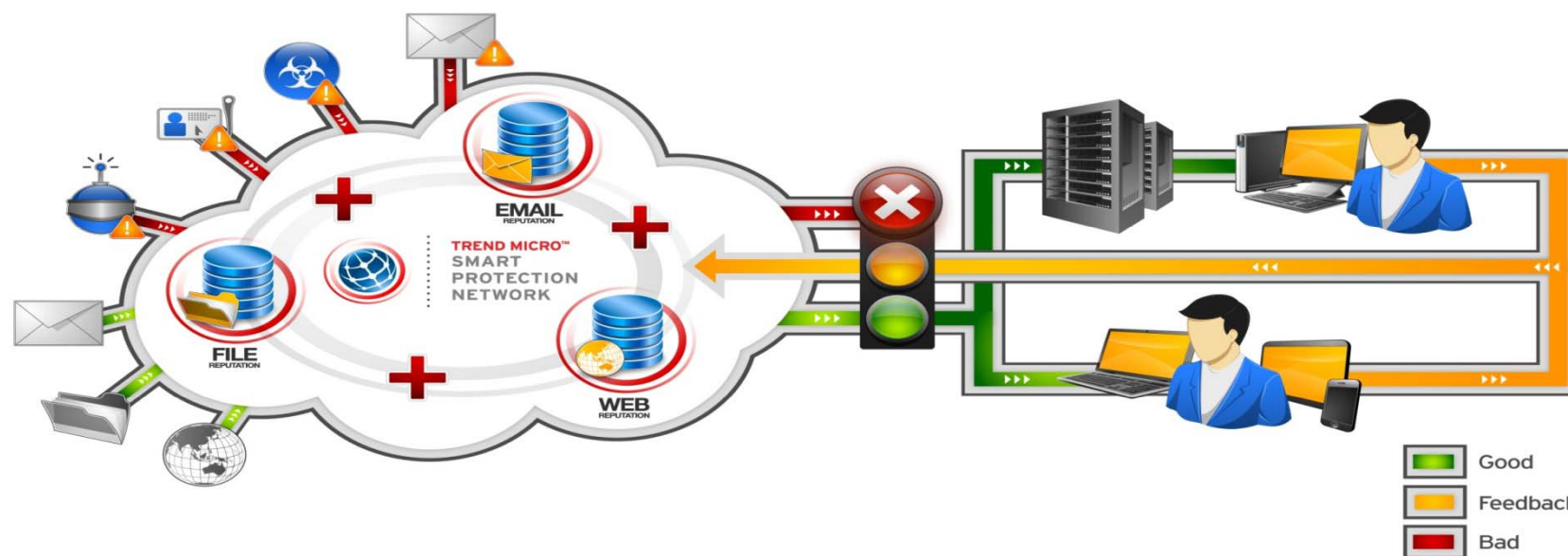
Business without **LIMITS**

Pulse Comes to You 2012

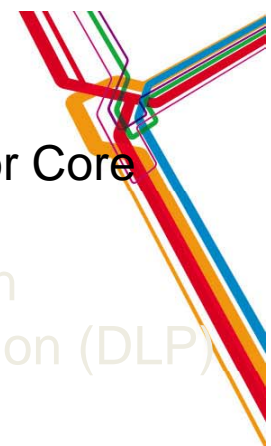


The Smart Protection Network infrastructure stops threats in the cloud, before they reach you

Security Made Smarter :
Cloud Based Security Private Cloud Real Time Visibility

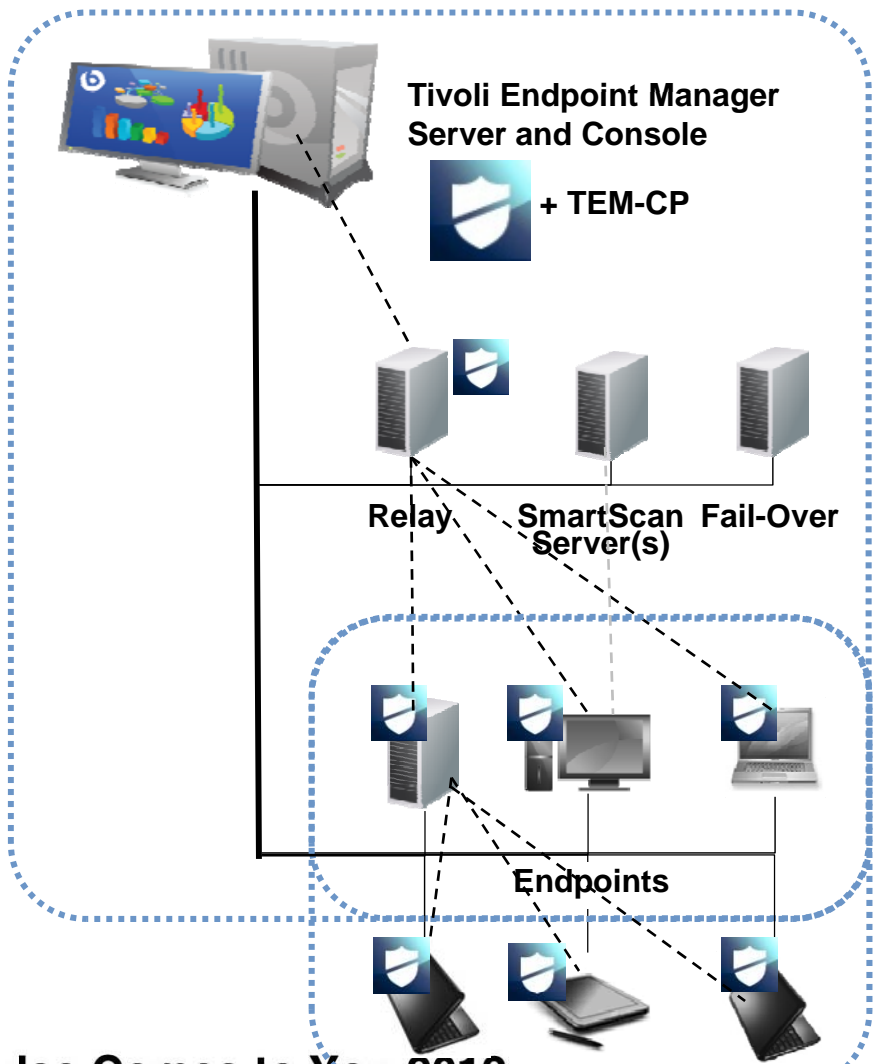


What is TEM-CP's "Data Protection Add-On"?



Tivoli Endpoint Manager for Core Protection

- Data Protection Add On
 - Data Loss Prevention (DLP)
 - Device Control

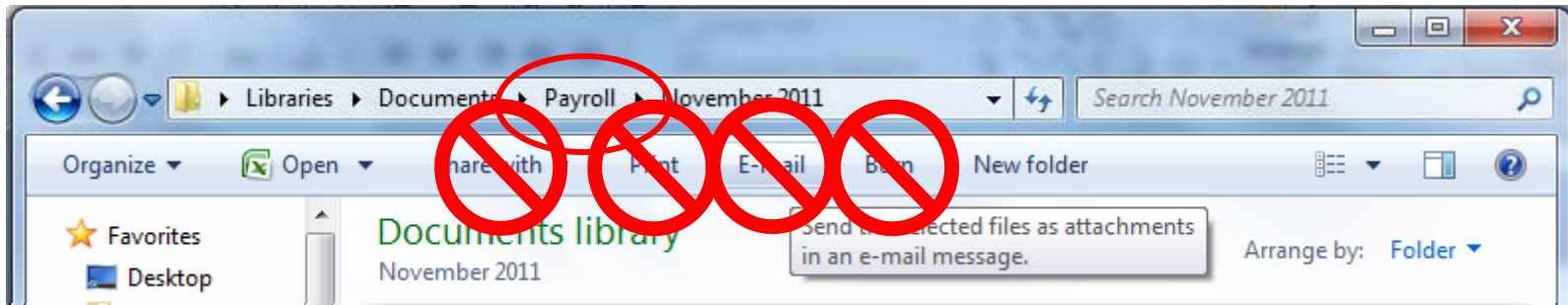


- Real-time content scanning of sensitive data
- Robust features:
 - Advanced device control with granular rules
 - Protection of structured data
 - Compliance templates
 - Multi-channel monitoring and enforcement
 - Minimal incremental impact on client performance
- Integrated with TEM-CP Console and management framework

Pulse Comes to You 2012

Business without **LIMITS**

Example: Protecting Confidential Data

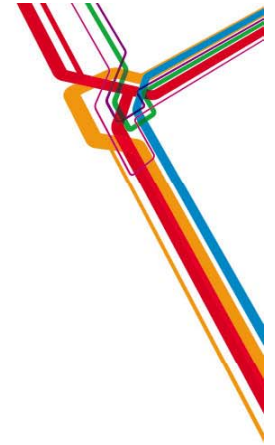


Protect confidential data by enforcing acceptable use practices, content-aware scanning, device control

	A1	Date												
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Date	Employee ID	Name	Hourly Wage	Hours	Gross Pay	Federal Allow.	State Tax	Federal Income Tax	Social Security 6.2%	Medicare 1.45%	Total Tax Withheld	Insurance Deduction	Net Pay
2	11/4/2011	56	Kane, John	\$13.25	36.00	\$477.00	0	\$34.33	\$57.10	\$29.57	\$6.92	\$127.92	\$26.00	\$323.08
3	11/4/2011	57	Kane, Lori	\$25.00	40.00	\$1,000.00	2	\$74.86	\$146.54	\$62.00	\$14.50	\$297.90	\$35.00	\$667.10
4	11/4/2011	58	Kastner, Steven H.	\$31.00	39.00	\$1,209.00	1	\$96.49	\$213.70	\$74.96	\$17.53	\$402.68	\$35.00	\$771.32
5	11/4/2011	59	Katyal, Sandeep	\$13.00	20.00	\$260.00	0	\$17.73	\$24.55	\$16.12	\$3.77	\$62.17	\$26.00	\$171.83
6	11/4/2011	60	Kawai, Masato	\$7.50	30.00	\$225.00	1	\$13.03	\$10.36	\$13.95	\$3.26	\$40.60	\$26.00	\$158.40
7	11/4/2011	61	Kearney, Bonnie	\$8.22	36.00	\$295.92	0	\$20.48	\$29.94	\$18.35	\$4.29	\$73.05	\$26.00	\$196.87
8	11/11/2011	56	Kane, John	\$13.25	40.00	\$530.00	0	\$38.39	\$65.05	\$32.86	\$7.69	\$143.98	\$26.00	\$360.02
9	11/11/2011	57	Kane, Lori	\$25.00	33.00	\$825.00	2	\$59.11	\$102.79	\$51.15	\$11.96	\$225.01	\$35.00	\$564.99
10	11/11/2011	58	Kastner, Steven H.	\$31.00	28.00	\$868.00	1	\$65.80	\$128.45	\$53.82	\$12.59	\$260.65	\$35.00	\$572.35
11	11/11/2011	59	Katyal, Sandeep	\$13.00	39.00	\$507.00	0	\$36.63	\$61.60	\$31.43	\$7.35	\$137.01	\$26.00	\$343.99
12	11/11/2011	60	Kawai, Masato	\$7.50	30.00	\$225.00	1	\$13.03	\$10.36	\$13.95	\$3.26	\$40.60	\$26.00	\$158.40
13	11/11/2011	61	Kearney, Bonnie	\$8.22	36.00	\$295.92	0	\$20.48	\$29.94	\$18.35	\$4.29	\$73.05	\$26.00	\$196.87
14	11/18/2011	56	Kane, John	\$13.25	33.00	\$437.25	0	\$31.29	\$51.14	\$27.11	\$6.34	\$115.88	\$26.00	\$295.37
15	11/18/2011	57	Kane, Lori	\$25.00	40.00	\$1,000.00	2	\$74.86	\$146.54	\$62.00	\$14.50	\$297.90	\$35.00	\$667.10
16	11/18/2011	58	Kastner, Steven H.	\$31.00	39.00	\$1,209.00	1	\$96.49	\$213.70	\$74.96	\$17.53	\$402.68	\$35.00	\$771.32
17	11/18/2011	59	Katyal, Sandeep	\$13.00	20.00	\$260.00	0	\$17.73	\$24.55	\$16.12	\$3.77	\$62.17	\$26.00	\$171.83
18	11/18/2011	60	Kawai, Masato	\$7.50	28.00	\$210.00	1	\$11.88	\$8.11	\$13.02	\$3.05	\$36.06	\$26.00	\$147.94

Pulse Comes to You 2012

Multiple Tools for Protecting Your Digital Assets Controlled



Patterns - Regular Expressions
(credit card, social insurance, account numbers)



Keywords – Lists of terms
(confidential, internal, project/product names...)



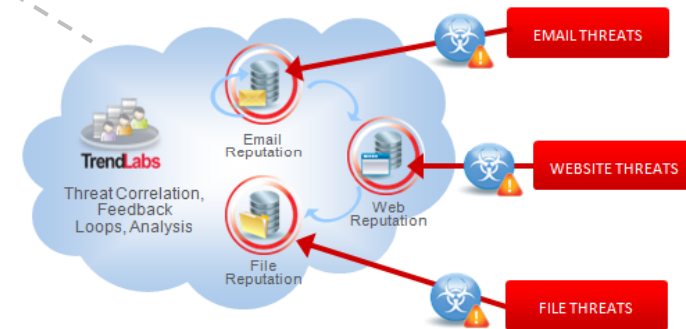
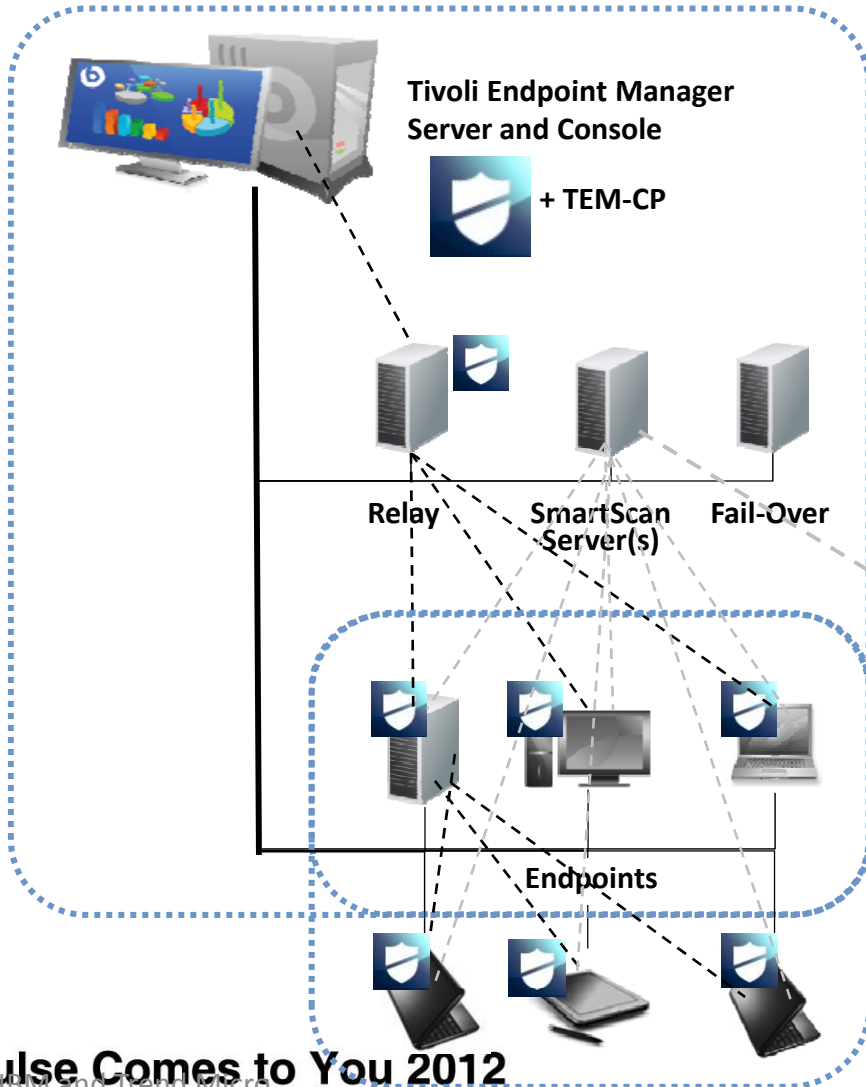
File Attributes – File Name, File Size, File Type
(threshold of acceptable use)

Data Protection Add On Scenario

Tivoli Endpoint Manager for Data Protection



- Data Protection
- Device Control



Business without **LIMITS**

Pulse Comes to You 2012

IBM and Trend Micro
Confidential



Example: Device Control Access Restrictions



Pulse Comes to You 2012

IBM and Trend Micro
Confidential

Business without **LIMITS**

Device Control Capabilities



	TEM-CP 10.6 with Data Protection Add- on
<p>Basic Device Access Control (no access/read/write/execute for USB, optical disks, mapped drives, floppy disks)</p>	✓
<p>Expanded Device Control Device Types (on/off by device type for CD/DVD, IEEE1394, Modems, Com Port, Print Port, Imaging Device, PCMCIA, Floppy, Infrared Device)</p>	✓
<p>Granular Device Control (on/off by device type*) & (restrict access by vendor, model, serial number for USB removeable storage device)</p>	✓
<p>Granular Device Control + Data Protection (on/off by device type*) & (restrict access by vendor, model, serial number for USB removable storage device) & (content-aware scanning)</p>	✓

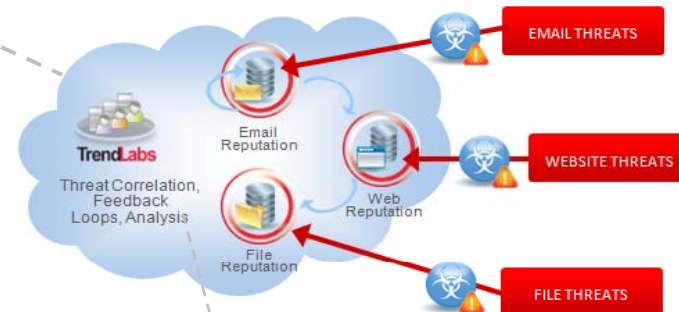
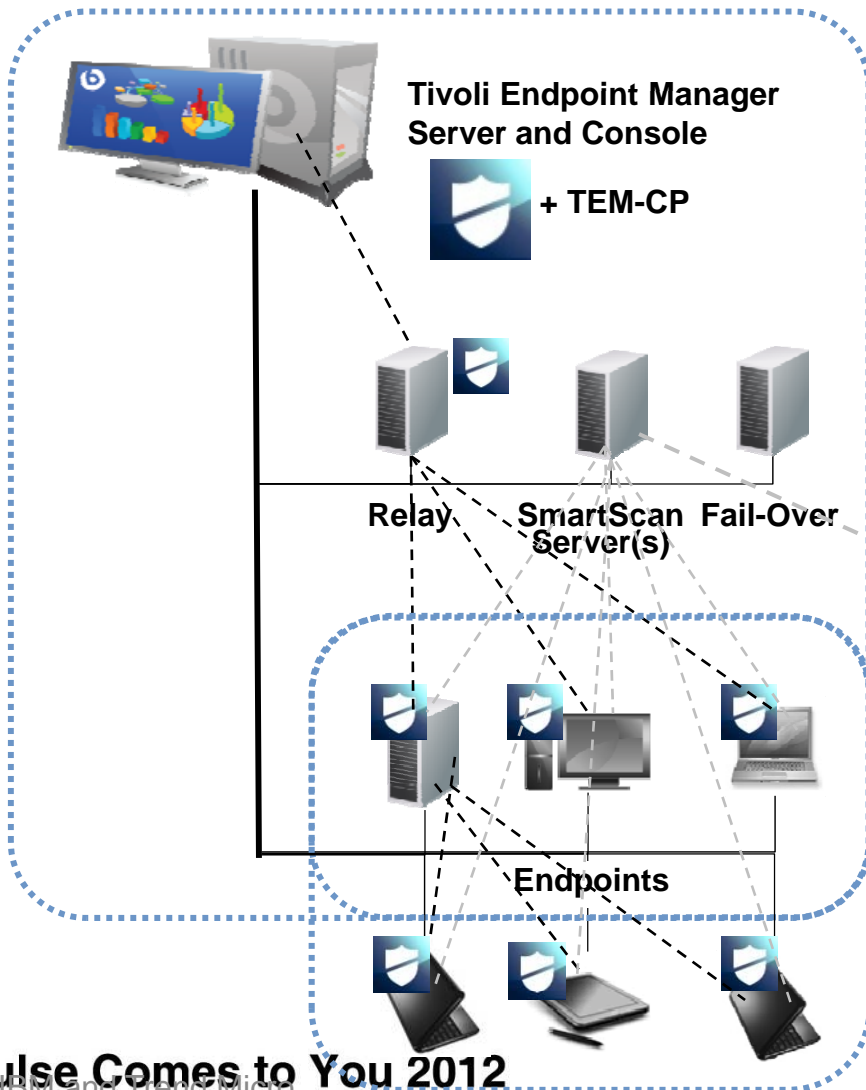
TEM-CPM's Data Protection Add On Summary



Tivoli Endpoint Manager for Data Protection Add On

- Data Protection
 - Data Loss Prevention(DLP)
 - Device Control

- **Secure all data**
- **Enforce security policies**
- **Comply with data privacy laws**



Business without **LIMITS**

Pulse Comes to You 2012

IBM and Trend Micro
Confidential

TEM Endpoint Protection



Integrated Endpoint Protection modules include:

Anti-Virus

Anti-Malware

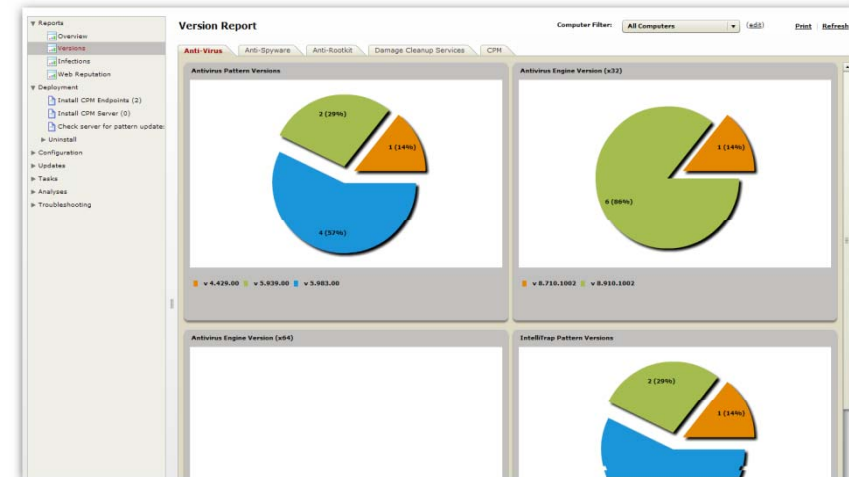
Endpoint Firewall

Web Protection

Smart Protection Network (Cloud)

Client Manager for
Endpoint Protection

Device Control and DLP



Features and Benefits

Prevent infection, identity theft,
data loss, network downtime, lost productivity, and compliance
violations

Eliminate security gap with real-time threat intelligence

Achieve unparalleled visibility into complete enterprise protection

Combine endpoint protection, security configuration, patch
management, and systems lifecycle management tools

Tivoli Endpoint Manager for Core Protection

Protecting endpoints from malware and other malicious threats

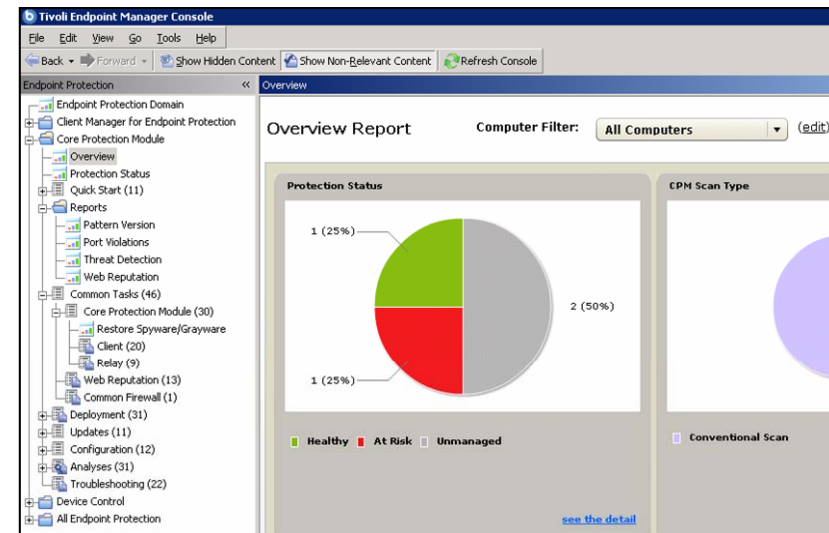


Overview

Delivers **single-console, integrated cloud-based protection** from **malware** and other malicious threats via capabilities such as file and web reputation, personal firewall, and behavior monitoring

Highlights

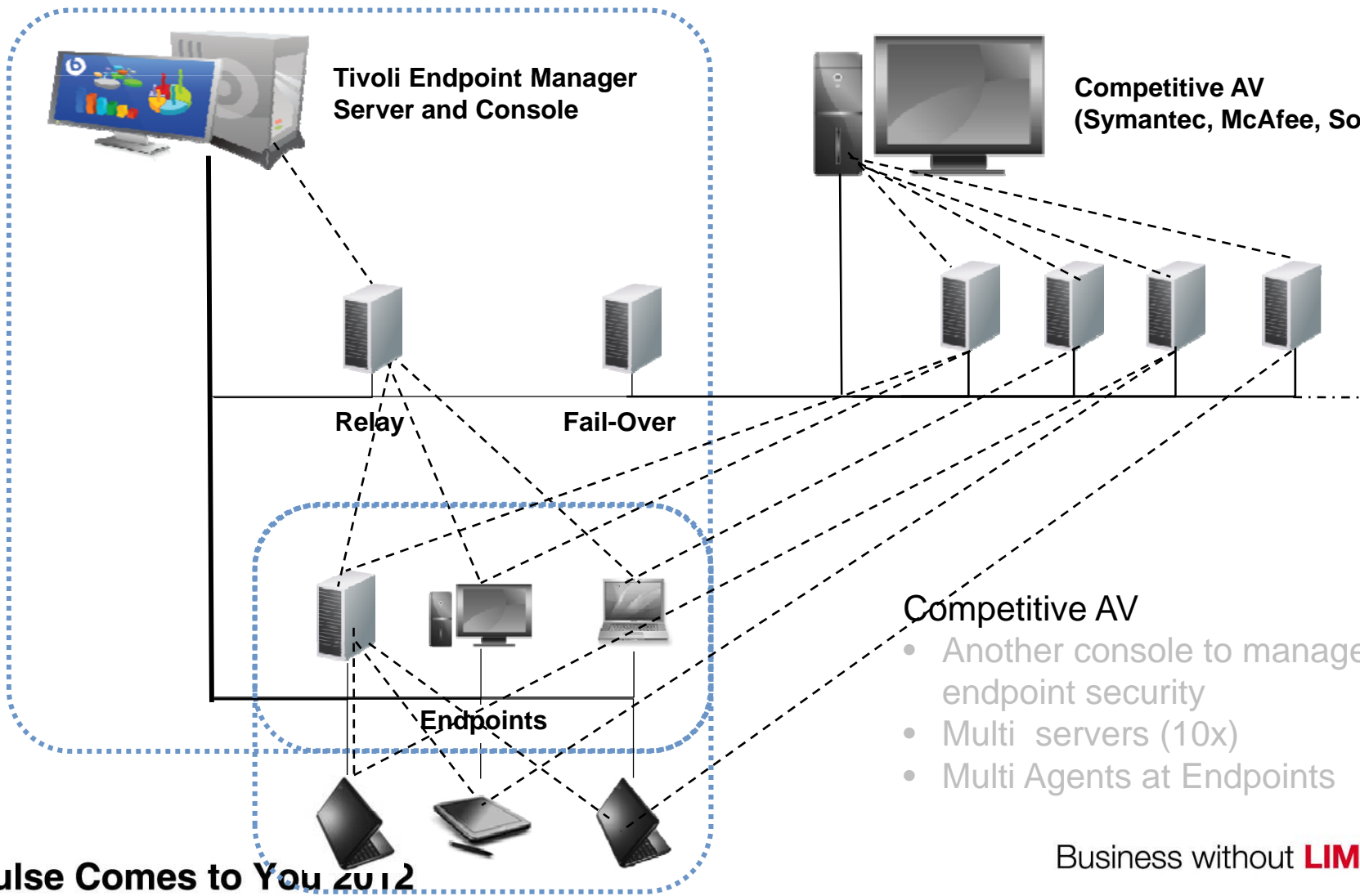
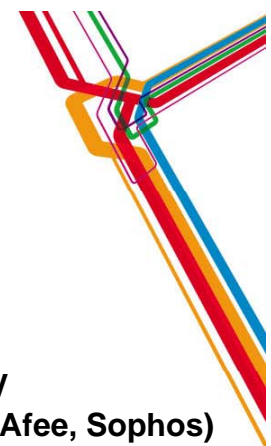
- Delivers real-time **endpoint protection** against viruses, Trojan horses, spyware, rootkits and other malware
- Protects through **cloud-based file and web reputation**, behavior monitoring and **personal firewall**
- Provides **virtualization awareness** to reduce resource contention issues on virtual infrastructures
- Leverages **industry-leading IBM® and Trend Micro™ technologies** with a single-console management infrastructure
Pulse Comes to You 2012



Tivoli. software

Business without **LIMITS**

Life Without TEM-CP

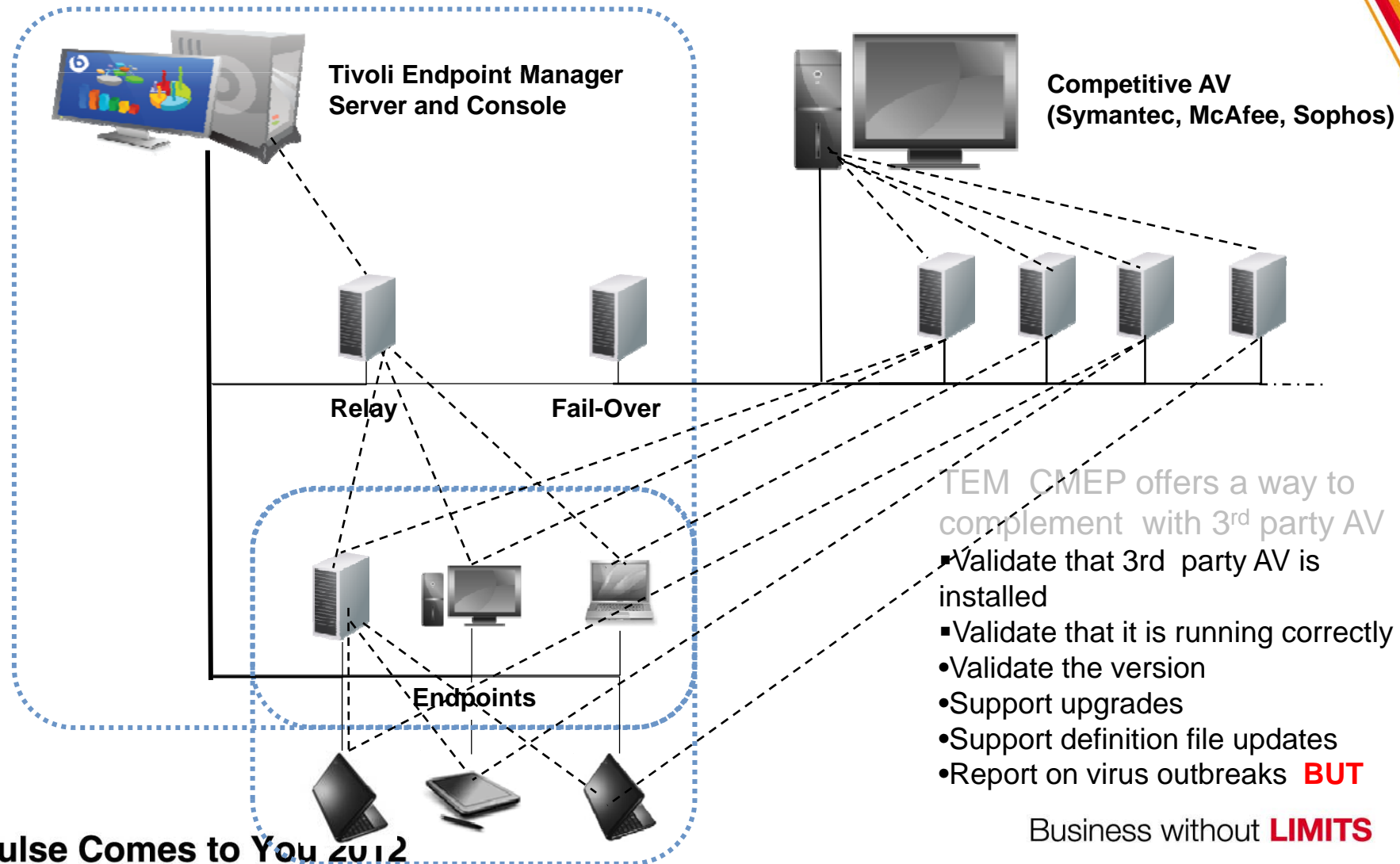
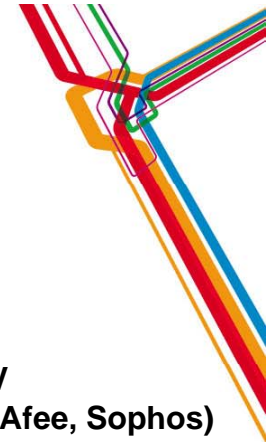


- Competitive AV
- Another console to manage endpoint security
 - Multi servers (10x)
 - Multi Agents at Endpoints

Pulse Comes to You 2012
IBM and Trend Micro Confidential

Business without **LIMITS**

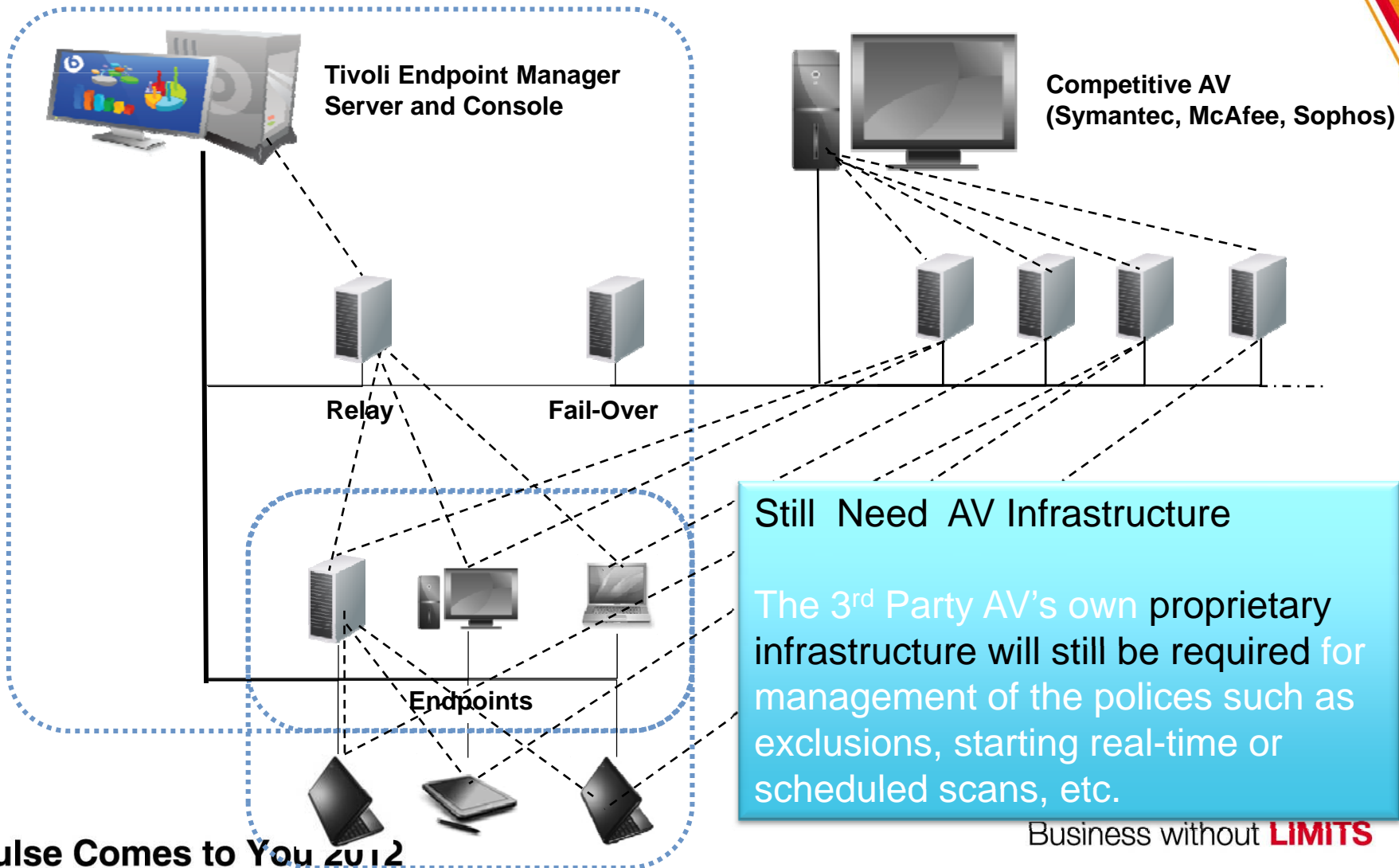
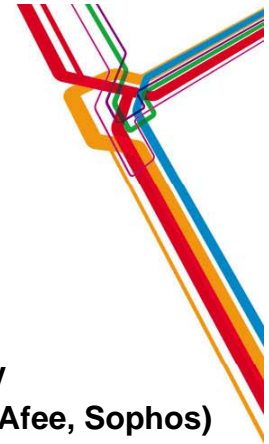
Life Without TEM-CP but How about CMEP ?



Pulse Comes to You 2012

IBM and Trend Micro Confidential

Life Without TEM-CP but How about CMEP ?



Still Need AV Infrastructure

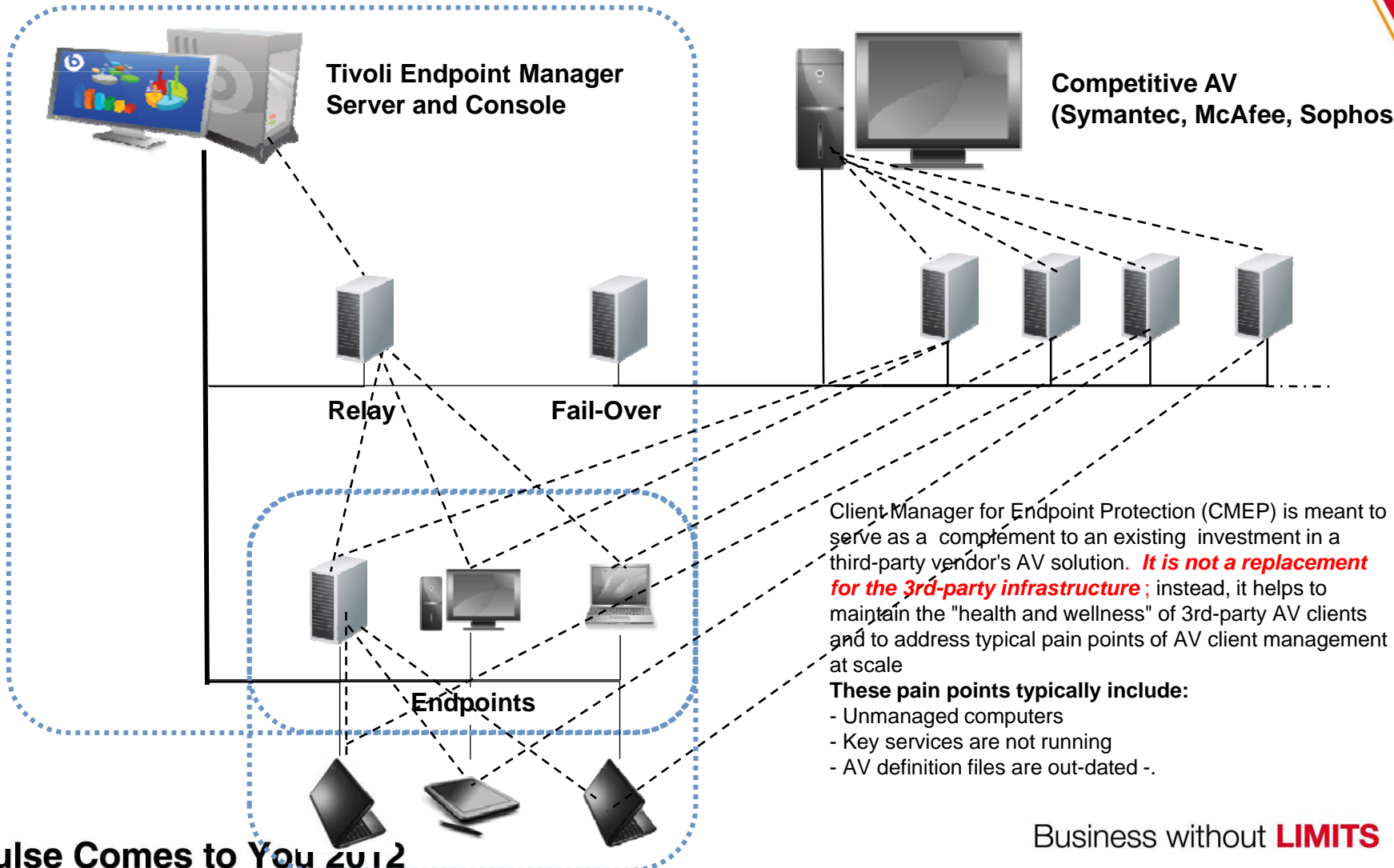
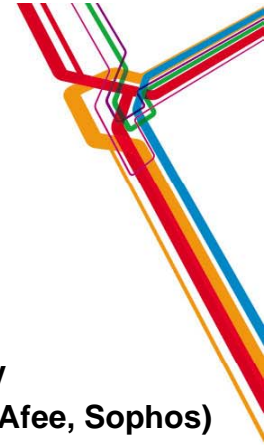
The 3rd Party AV's own proprietary infrastructure will still be required for management of the policies such as exclusions, starting real-time or scheduled scans, etc.

Pulse Comes to You 2012

IBM and Trend Micro Confidential

Business without **LIMITS**

Life Without TEM-CP but How About CMEP ?



Pulse Comes to You 2012

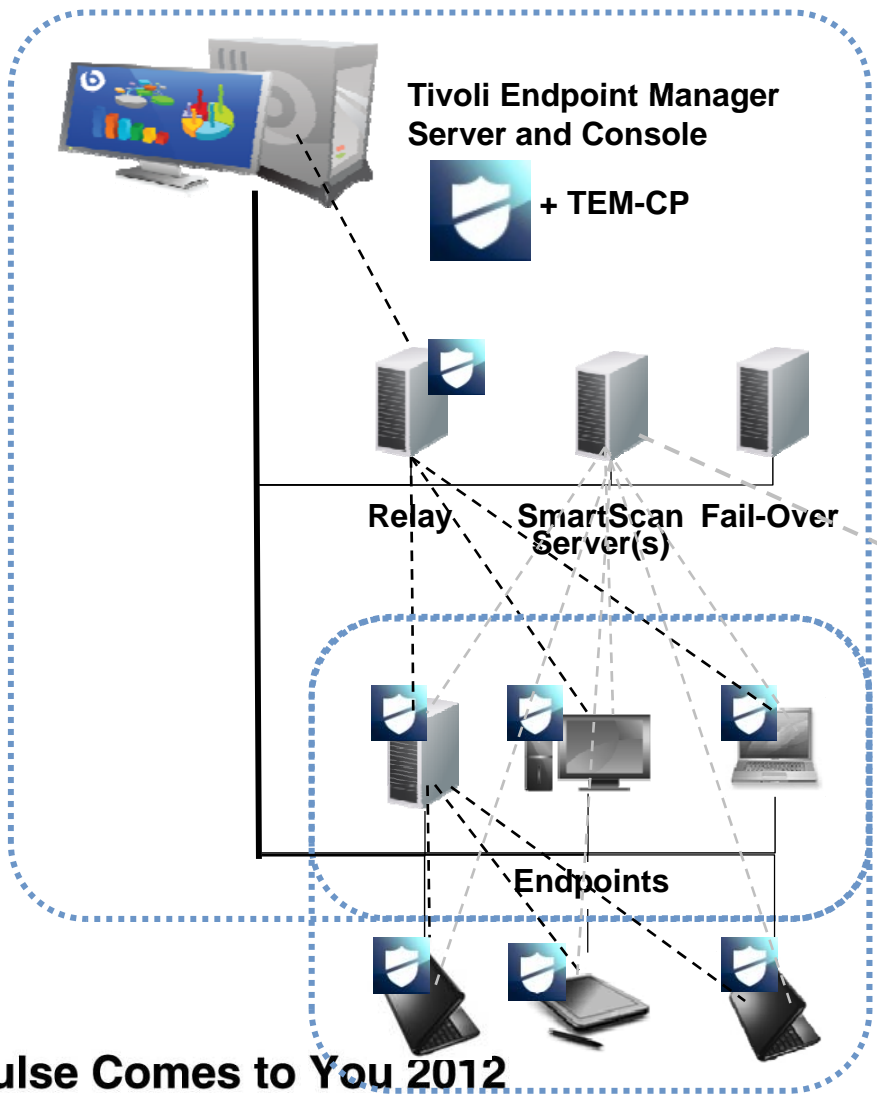
IBM and Trend Micro Confidential

Business without **LIMITS**

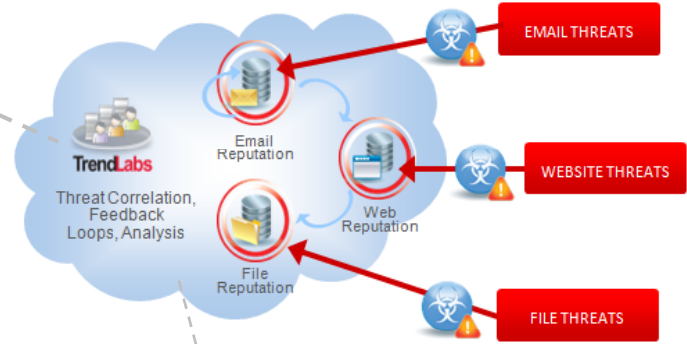
TEM with TEM-CP – A Better Way



Tivoli Endpoint Manager for Core Protection

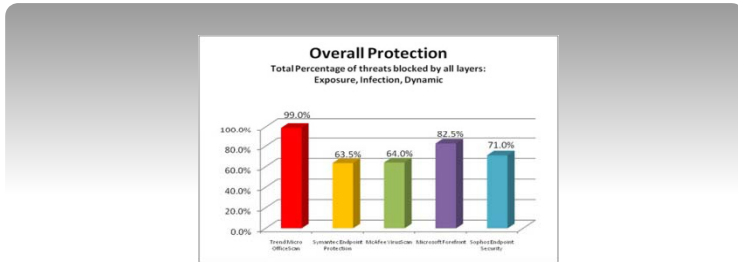


- Single Management Server
- Integrated Reporting
- Lightweight Footprint
- Real-time Policy Enforcement



Business without **LIMITS**

Why TEM Core Protection & DLP?



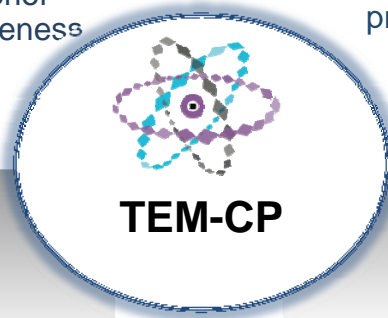
Effectiveness and Performance

TEM Core Protection Solutions is proven by independent testing agencies to be superior endpoint performance and security effectiveness



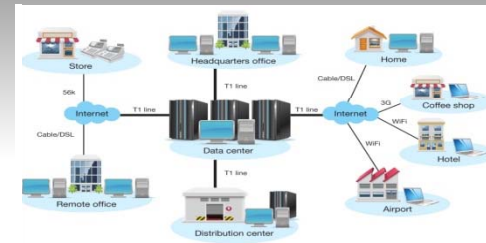
Power of the Cloud

TEM-CP uses the Smart Protection Network providing immediate protection from the latest threats and lowers administrative burden



Focused on Security Innovation

IBM's Security Systems Brand has a single-minded focus on security – a focus that has enabled our 20+ years of security innovation



TEM-CP runs on Big Fix Platform

Whether it's a Mac connecting from hotel WiFi, or a Windows laptop at 30K feet, Tivoli Endpoint Manager has it covered. In real time, at any scale.

Business without **LIMITS**

Pulse Comes to You 2012

Business without **LIMITS**



Thank You





Pulse Comes To You 2012

Business Without **LIMITS**



Security

IBM Security

Intelligence, Integration, Expertise