

Tivoli Endpoint Manager



Ing. Angel Mouriz
angel.mouriz@infotech.com.uy

Tivoli software

Agenda

- ➔ ■ **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**

Big Fix



Empresa fundada en 1997 y dedicada 100% a la reducción de los costos asociados al manejo y mantenimiento de:

- Redes
- Workstations
- Equipos móviles
- Servidores

Sus productos brindan soluciones en:

- Seguridad y manejo de vulnerabilidades
- Cumplimiento de normativas (Compliance)
- Manejo de actualizaciones y distribución de software

Big Fix: an IBM Company



En julio de 2010, IBM adquiere Big Fix en U\$S 400.000.000



Big Fix – Tivoli Endpoint Manager

En Febrero de 2011 IBM incorpora el portafolio de productos de Big Fix a la brand de software Tivoli



IBM Tivoli Endpoint Manager
built on BigFix technology

Agenda

- ➔ ▪ **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**

Tivoli Endpoint Manager

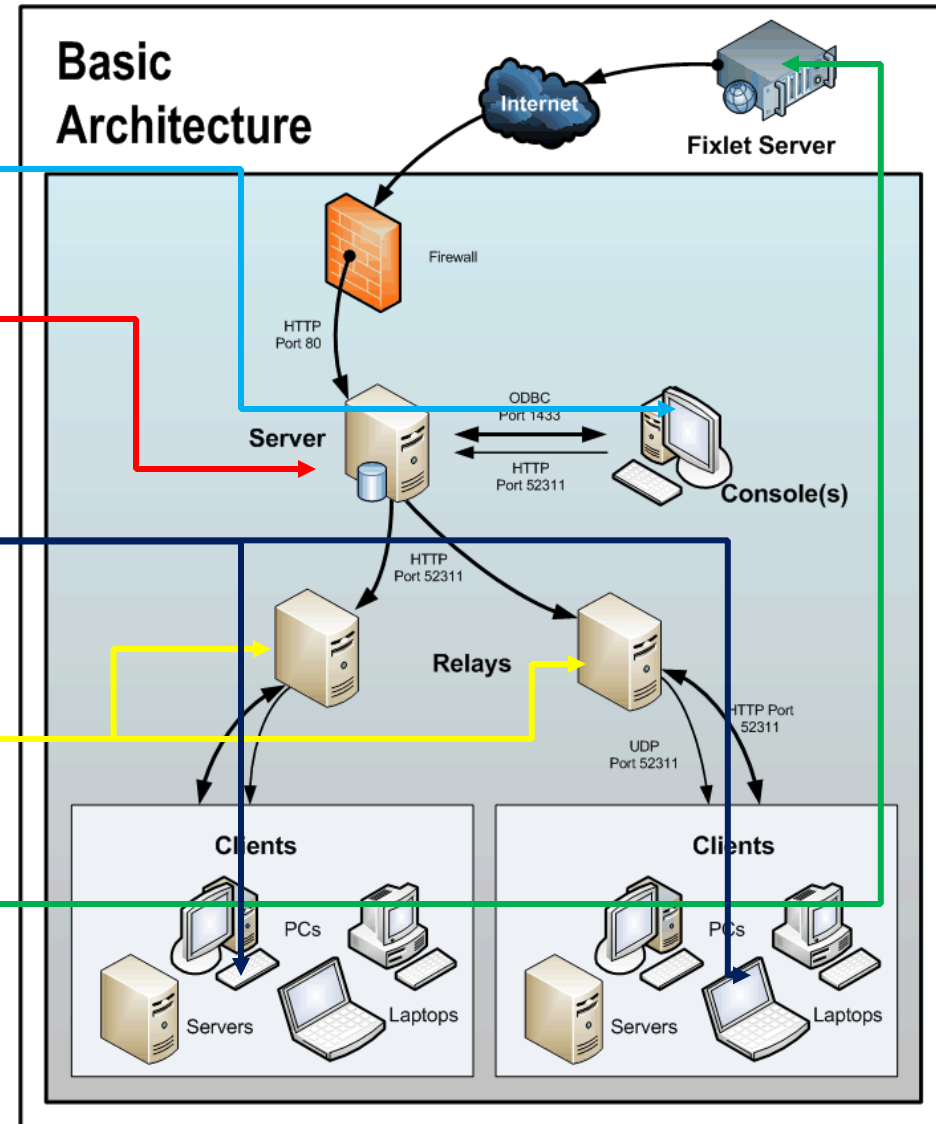
- Basado en la tecnología BigFix®
- Ayuda a alcanzar un manejo inteligente y rápido de los endpoints
- Combina manejo de endpoints y manejo de seguridad en una única solución
- Permite tener visibilidad y manejo de:
 - Servidores físicos o virtuales
 - Equipos de escritorio
 - Laptops
 - Equipamiento especializado (POS, ATMs, Kioscos)
- A medida que las amenazas aparecen, el software permite solucionarlas, proteger los endpoints y realizar reportes en tiempo real de la situación actual
- Automatiza tareas en redes complejas que habitualmente consumen grandes cantidades de tiempo, logrando:
 - Control de los costos
 - Optimizar el uso del tiempo del personal de IT
 - Reducción de riesgo
 - Cumplimiento con regulaciones

Tivoli Endpoint Manager

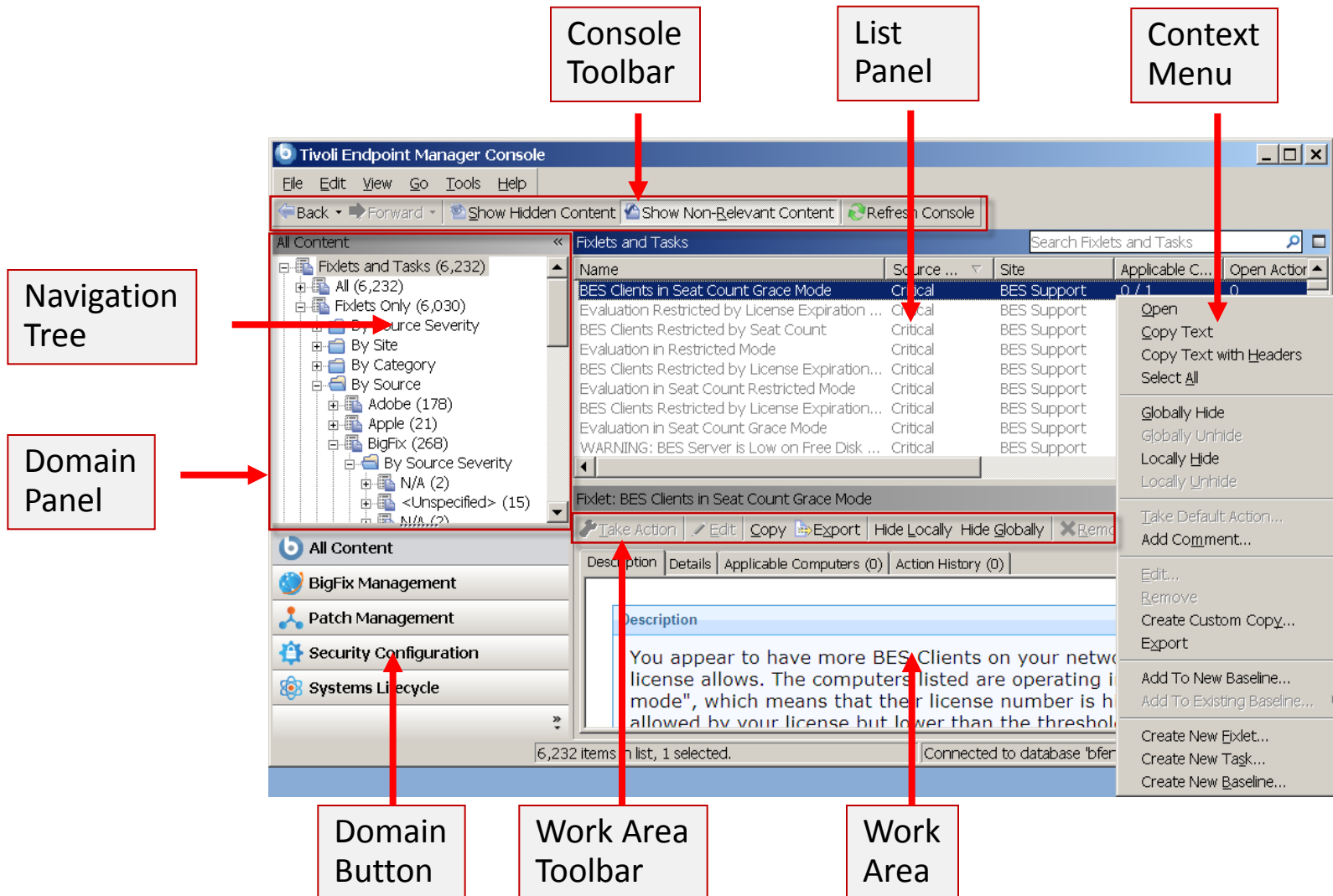
- Puede ser implementado en pocos días en una red de cualquier tamaño
- Un único agente instalado en los endpoints brinda todas la funcionalidades del producto
- Visibilidad y control en tiempo real desde una única consola de administración
- Manejo de decenas de miles de endpoints, sin importar:
 - Ubicación
 - Tipo de conexión
 - Estado
- Personalización de las acciones a realizar según el endpoint destino
- Reduce la complejidad de administración, aumenta la eficacia y maximiza la productividad
- Soporte para plataformas heterogéneas:
 - Microsoft® Windows®
 - UNIX®
 - Linux®
 - Mac

Componentes de TEM

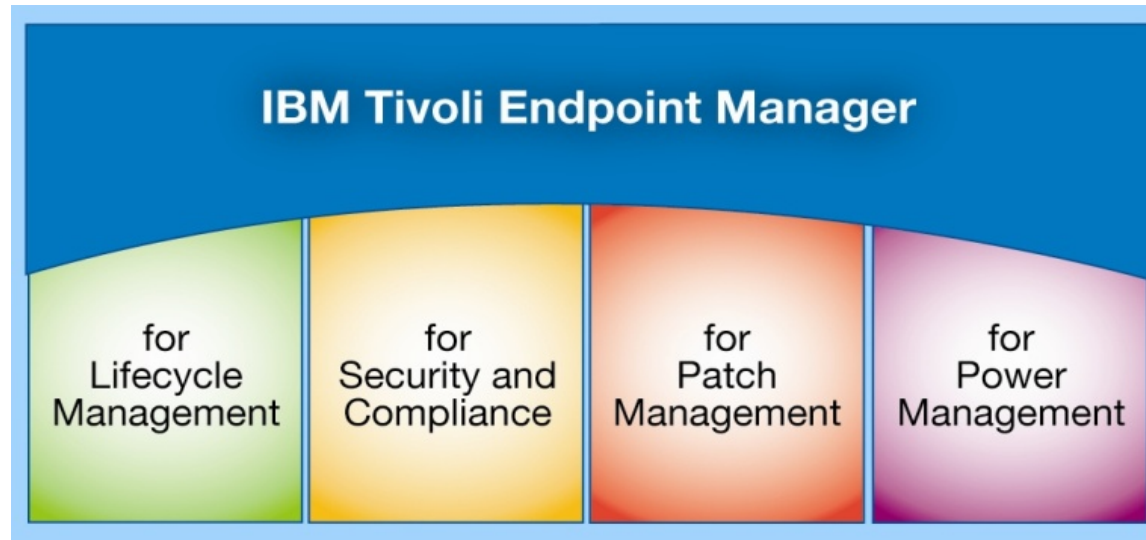
- **Consola:** Interfaz unificada de administración del sistema
- **Servidor:** Sistema central de manejo y generación de reportes
- **Agentes:** Componente que se instala en todos los equipos manejados
- **Relay:** Componente opcional entre los clientes y los agentes
- **Soluciones:** Contenido empaquetado que contiene “Fixlets”, parches, actualizaciones, gráficos, reportes, etc.



Consola



Tivoli Endpoint Manager



Compuesto por 4 módulos independientes para cubrir las necesidades de cada organización:

- TEM for Lifecycle Management
- TEM for Security and Compliance
- TEM for Patch Management
- TEM for Power Management

Tivoli Endpoint Manager



Manejo del Ciclo de Vida

Descubrir Activos

Manejo de Parches

Administración de Energía

OS deployment

Control remoto de equipos

Análisis de uso de Software (add-on)

Seguridad y cumplimiento

Descubrir Activos

Manejo de Parches

Manejo de seguridad

Manejo de Vulnerabilidades

Multiple-vendor endpoint protection management

Manejo de Parches

Manejo de Parches

Reportes en tiempo real

Personalización de la aplicación de parches

Administración de Energía

Manejo de ahorro de energía

Reportes sencillos

Programación de Wake-on-LAN

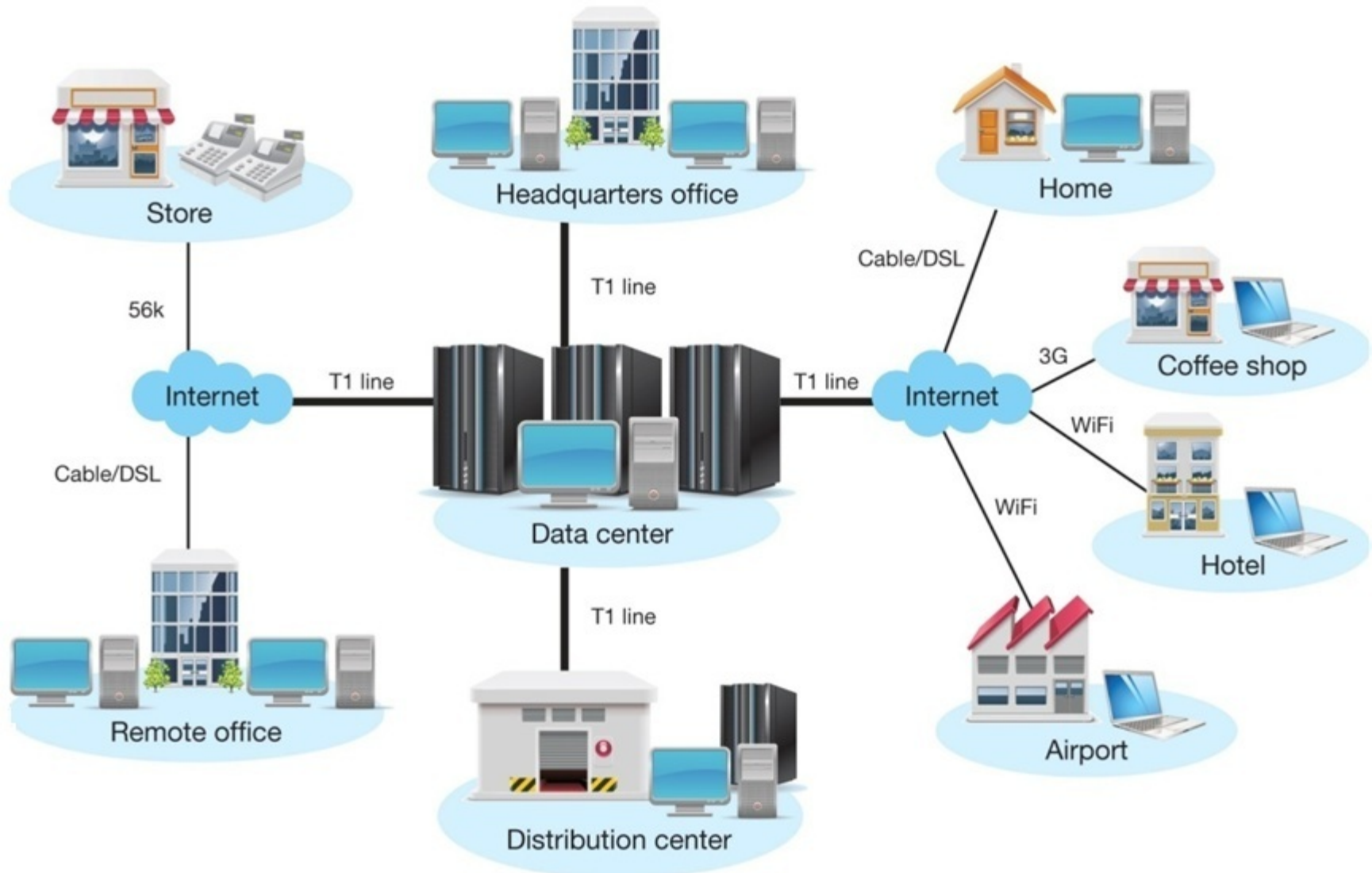
Definición de wake-up-points

Grabado automático de archivos abiertos

IBM Tivoli Endpoint Manager



TEM – Cobertura total



Agenda

- **Big Fix**

- Soluciones para Endpoints
- Big Fix: An IBM Company

- **Tivoli Endpoint Manager**



- Visión General
- Patch Management
- Lifecycle Management
- Security and Compliance
- Power Management
- Core Protection

- **Conclusiones**

Tivoli Endpoint Manager



Manejo de Parches

- Gran aumento en la distribución de software malicioso
 - Explotan vulnerabilidades ya conocidas
 - Rápidamente explotan nuevas vulnerabilidades
- Vulnerabilidades en varios niveles
 - Sistemas Operativos
 - Software aplicativo
- TEM brinda una plataforma unificada para el manejo de todos los parches

Tivoli Endpoint Manager



Manejo de Parches (cont.)

- Sistemas Operativos

- Windows
- Linux
- UNIX
- Mac



- Aplicaciones

- Adobe
- Mozilla
- Microsoft
- Java
- Google
- VMWare
- RealNetworks
- Apple
- Skype
- Y muchos más...



Tivoli Endpoint Manager



Manejo de Parches (cont.)

- Detección automática de vulnerabilidades y de software desactualizado
- Distribución automatizada de parches y actualizaciones
- Sin pérdida de funcionalidad en distintos tipos de redes:
 - Redes de poco ancho de banda
 - Redes distribuidas geográficamente
- Definición de ventanas de mantenimiento
 - qué parches
 - a qué ubicaciones
 - en qué momento
- Rollback Wizards para desinstalar parches
- Reportes en tiempo real del proceso de distribución e instalación

Tivoli Endpoint Manager

Patch Management Domain

Patch Management Domain

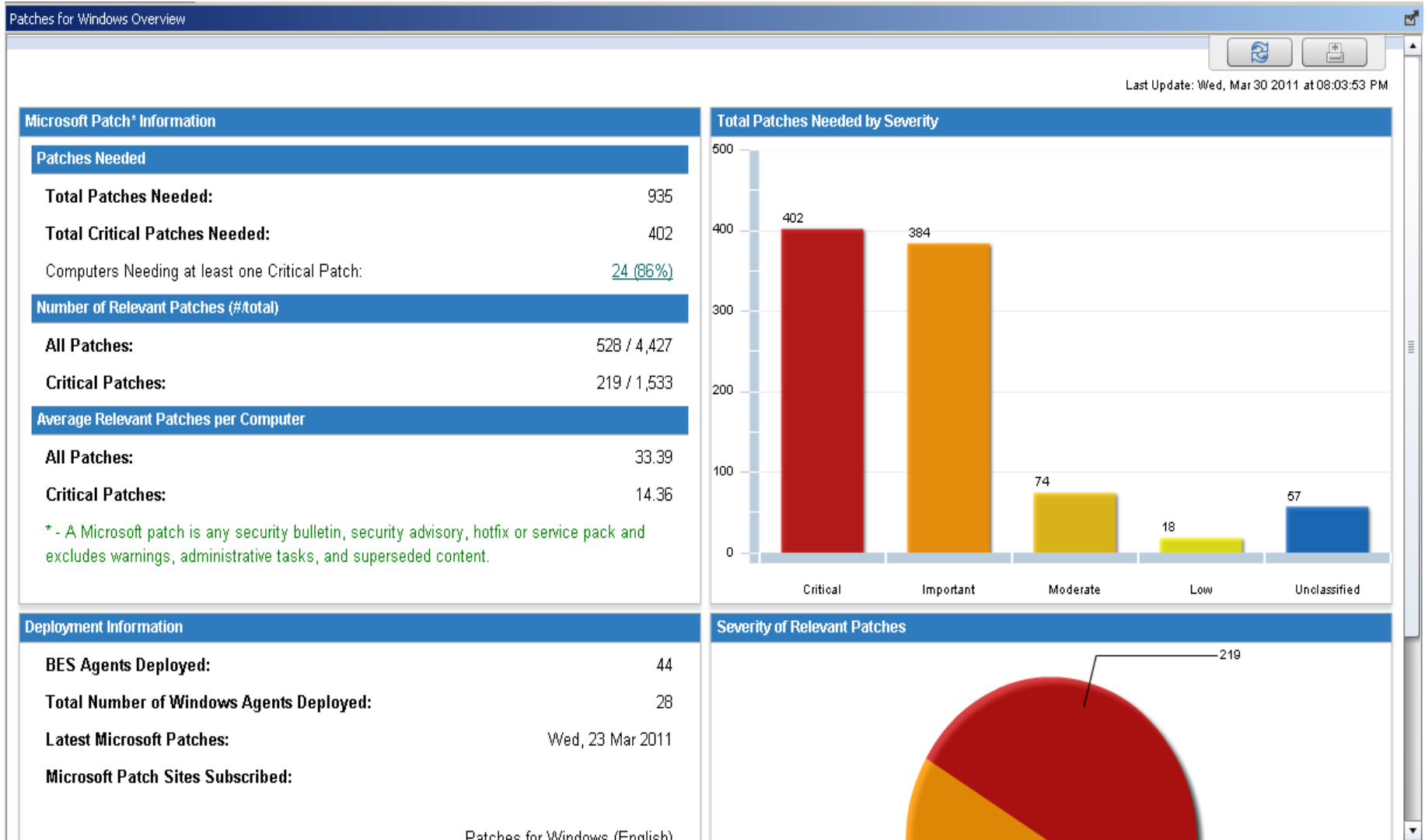
The Patch Management domain provides patching capabilities across a variety of operating systems and applications. A list of recent additions to the domain is available below with specific controls and views available to the left.

Content released or modified in the last 30 days:

Name	Type	Site	Modified/New	Date	Applicable Computers ▼
Flash Player 10.2.153.1 Available - Internet Explorer	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	5
WinZip 15.0 Available (French)	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	4
Flash Player 10.2.153.1 Available - Firefox/Mozilla	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	3
Flash Player 7 Available - Internet Explorer (Windows NT/95)	Fixlet	Updates for Windows Applications	Modified	Tue, 01 Mar 2011	3
Windows Security: Microsoft Windows Malicious Software Removal Tool - Deploy	Task	Patches for Windows (English)	Modified	Wed, 09 Mar 2011	3
Adobe Reader 9.1 Available - Adobe Reader 9 (French)	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	3
Adobe Reader 9.1 Available - Adobe Reader 9	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	3
Apple iTunes 7.3.2 Available - Windows 2000	Fixlet	Updates for Windows Applications	Modified	Tue, 01 Mar 2011	3
Apple iTunes 10.1.2.17 Available - Windows XP/2003/Vista/2008/Win7, Vista/Win7 x64 (Superseded)	Fixlet	Updates for Windows Applications	Modified	Thu, 03 Mar 2011	3
Adobe Reader 8.2.1 Available - Adobe Reader 8.2 (French)	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	3
Java Runtime Environment 6 update 24 Available (JRE 5 & 6 Installed) (x64)	Fixlet	Updates for Windows Applications	Modified	Tue, 22 Mar 2011	3
Apple QuickTime 7.1.6 Security Update Available	Fixlet	Updates for Windows Applications	Modified	Tue, 01 Mar 2011	3
Update Available for Potential Vulnerabilities in Adobe Reader 7	Fixlet	Updates for Windows Applications	Modified	Tue, 01 Mar 2011	3

Connected to database 'bfenterprise' as user 'itemMaster'

Tivoli Endpoint Manager



Agenda

- **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**



Tivoli Endpoint Manager



Manejo del Ciclo de Vida

- Descubrimiento de activos e inventario
 - Visibilidad de los endpoints
 - Descubrimiento de cualquier dispositivo con IP
- Reportes de inventario
 - Reportes de hardware y software
- Manejo de parches
 - Minimiza los tiempos de actualización
 - Reduce la carga de trabajo del personal
- Administración y del control remoto de los equipos
 - Microsoft Windows Remote Desktop & Remote Assistance
 - Tivoli Remote Control Components (*Peer to Peer*)

Tivoli Endpoint Manager

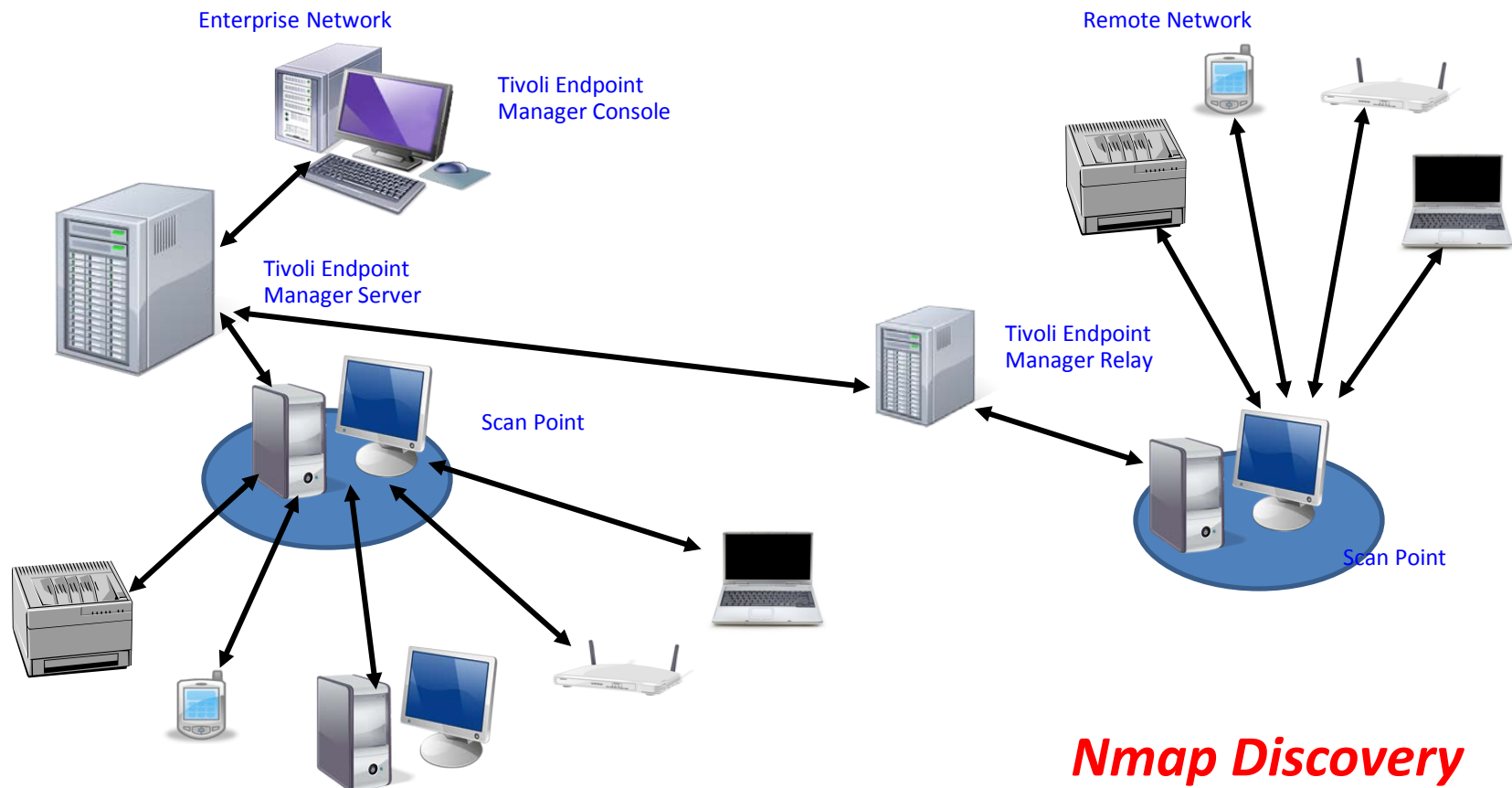


Manejo del Ciclo de Vida (cont).

- Distribución de software
 - Basado en políticas definidas por el administrador
- Despliegue de Sistema Operativo (OS Deployment)
 - Bare Metal imaging
 - OS Provisioning (*Incluye TPM for OS Deployment*)
- Análisis de uso de Software
 - Módulo opcional con costo adicional
 - Analiza el uso de los aplicativos para lograr un licenciamiento eficiente

Tivoli Endpoint Manager – Lifecycle Mgmt.

Asset Discovery



Tivoli Endpoint Manager – Lifecycle Mgmt.

Asset Discovery

Unmanaged Assets

Search Unmanaged Assets

Hostname	IP Address	MAC Address	OS	OS A
fsm9234b-rtp-b510-4th-a50...	9.42.12.198	00:15:17:9F:F8:94	Linux 2.6.13 - 2.6.28	100%
apca13.tivlab.raleigh.ibm.com	9.42.12.2	00:C0:B7:6D:CE:66	Schweitzer Engineering SEL-2701 Ethernet processor	100%
cto-tuam.tivlab.raleigh.ibm.com	9.42.12.200	00:50:56:AD:2E:2E	Linux 2.6.9 - 2.6.28	100%
apca59.tivlab.raleigh.ibm.com	9.42.12.202	00:C0:B7:6D:CF:13	APC AP9319 Environmental Monitoring Unit or Smart-UPS ...	100%
apca59-1.tivlab.raleigh.ibm.c...	9.42.12.203	00:C0:B7:6D:CE:73	APC AP9319 Environmental Monitoring Unit or Smart-UPS ...	100%
beneth01.tivlab.raleigh.ibm...	9.42.12.204	00:0D:60:4E:13:A2	Microsoft Windows Server 2003 SP1 or SP2	100%
tsbla113.tivlab.raleigh.ibm.com	9.42.12.209	00:0D:60:4E:32:2C	Linux 2.6.9 - 2.6.28	100%
mc-esxi2.tivlab.raleigh.ibm.com	9.42.12.210	00:21:5E:6E:28:EC	FreeBSD 7.0-BETA4 - 7.0 or FreeNAS 0.69.1 (FreeBSD 6....	91%
tsblasvr2.tivlab.raleigh.ibm.c...	9.42.12.211	00:09:6B:CA:B8:C0	IBM BladeCenter management module (firmware BRET8SL...	100%
cto-pxe.tivlab.raleigh.ibm.com	9.42.12.212	00:50:56:AD:73:05	Linux 2.6.9 - 2.6.28	100%
linfiber01.tivlab.raleigh.ibm.c...	9.42.12.213	00:14:5E:38:66:92	Linux 2.4.9 - 2.4.18 (likely embedded)	100%
candleaix1.tivlab.raleigh.ibm...	9.42.12.216	00:09:6B:6B:33:18	IBM AIX 5.3 - 6.1	100%
prfr3s34.tivlab.raleigh.ibm.com	9.42.12.217	00:11:25:3E:9E:34	Linux 2.6.9 - 2.6.28	100%
itsmaix8.tivlab.raleigh.ibm.com	9.42.12.219	00:11:25:7E:1E:6A	IBM AIX 5.3 - 6.1 or IBM AIX 5.3 or FreeBSD 4.3-RELEAS...	92%
zpmun6.tivlab.raleigh.ibm.com	9.42.12.221	00:03:BA:2F:9F:80	Sun Solaris 9 or 10, or OpenSolaris 2009.06	100%
bvtwin01.tivlab.raleigh.ibm...	9.42.12.222	00:0D:60:4E:01:9E	Microsoft Windows Server 2003 SP1 or SP2	100%

Unmanaged Asset: 00-37 (M)

Open
Copy Text
Copy Text with Headers
Select All
Edit Keywords...
Delete Unmanaged Asset...
Install Tivoli Endpoint Manager Client...

Filterable Properties

Last Scan Time (Server Time) 2/22/2011 9:08:37 PM

Hostname bvtwin01.tivlab.raleigh.ibm.com

MAC Address 00:0D:60:4E:01:9E

First Scan Time (Server Time) 2/22/2011 9:08:37 PM

OS Accuracy 100%

Device Type general purpose

Import Time (Server Time) 2/22/2011 9:11:34 PM

Newly Discovered

Tivoli Endpoint Manager – Lifecycle Mgmt.

Inventory Management

- Brinda visibilidad de los activos
- Recopila información de:
 - Sistema Operativo
 - RAM
 - CPU
 - Espacio disponible en disco
 - Dispositivos USB
 - Aplicaciones instaladas
- Soporte para:
 - Windows
 - Linux
 - UNIX
 - Mac
 - Ambientes Virtuales

Tivoli Endpoint Manager – Lifecycle Mgmt.

Otras funcionalidades

- Análisis de uso de aplicaciones
 - Permite controlar el uso de aplicaciones específicas en los endpoints.
 - Facilita el inventario y manejo de licencias de software
 - Análisis de actividad de cada aplicación
 - Análisis de actividad por usuario
- Manejo de parches
 - Este módulo también es parte de “Lifecycle Management”
- Administración de Energía
 - Este módulo también es parte de “Lifecycle Management”

Tivoli Endpoint Manager – Lifecycle Mgmt.

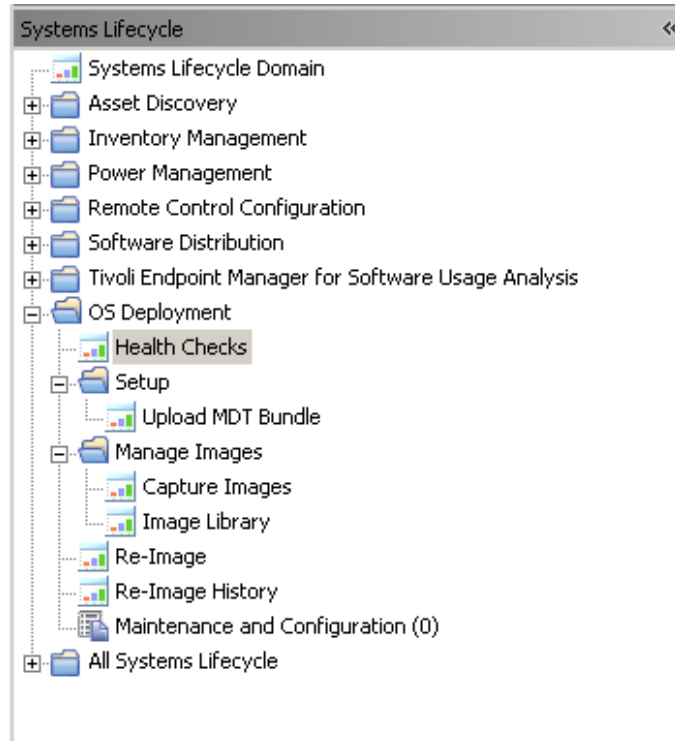
Otras funcionalidades (cont.)

- Configuración de Control Remoto
 - Manejo y administración de soluciones de acceso remoto.
 - Remote Desktop (Windows)
 - Remote Assistance (Windows)
 - Tivoli Remote Access (otras plataformas)
- Distribución de Software:
 - Permite distribuir e instalar paquetes de software.
 - TEM se transforma en una biblioteca de aplicaciones
 - Centro de distribución unificado
 - Fácil administración
 - Control de ancho de banda para el proceso de distribución
 - Instalación de paquetes existentes
 - Creación de nuevos paquetes y capacidad de generar “Fixlets” para ellos

Tivoli Endpoint Manager – Lifecycle Mgmt.

Otras funcionalidades (cont.)

- Despliegue de Sistemas Operativos
 - Solución centralizada y consolidada.
 - Captura, prepara y almacena imágenes
 - Permite realizar la distribución de las imágenes a través de la red

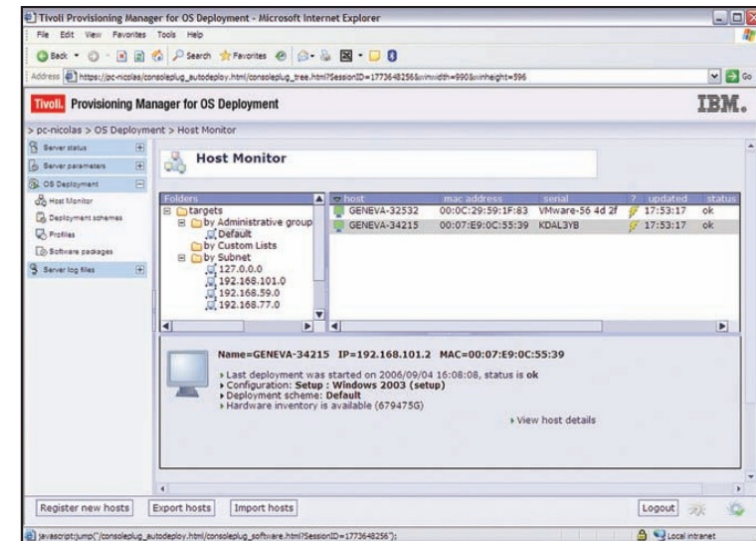


Soporte para todas las plataformas
Windows

Tivoli Endpoint Manager – Lifecycle Mgmt.

Otras funcionalidades (cont.)

- Incluye licencias de **Tivoli Provisioning Manager for OS Deployment**
 - Cada endpoint manejado por TEM puede usarse con TPM for OSD
 - Captura, almacena y permite editar imágenes
 - Permite generar una base de datos de drivers y aplicaciones que se seleccionan e instalan automáticamente en el momento de la distribución
 - Único repositorio de imágenes para todos los modelos de hardware
 - Instalación completamente automática
- Manejo de ambientes virtualizados
 - P2V
 - V2P
 - V2V
- Distribución de las imágenes a través de la red
 - Booteo remoto mediante PXE
 - Optimización de uso del ancho de banda
 - Instalación de decenas de equipos en paralelo



Soporte para las principales plataformas del mercado:
AIX, Linux, Solaris, Windows

Agenda

- **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - ➔ ■ Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**

Tivoli Endpoint Manager



Seguridad y cumplimiento

- Uno de los puntos críticos en el manejo de endpoints
- Eliminación de vulnerabilidades
- Control sobre los parches de seguridad aplicados
- Respuesta casi inmediata frente a nuevas vulnerabilidades
- Estandariza el proceso de instalación de parches de seguridad
- Simplifica el cumplimiento con regulaciones
 - COBIT
 - SOX
 - HIPAA
 - muchas más...



Tivoli Endpoint Manager



Seguridad y cumplimiento (cont.)

- Descubrimiento de activos
- Visibilidad global del nivel de aplicación de parches de seguridad
- Control sobre los parches de seguridad distribuidos y aplicados
- Opción de Anti-malware y Web Reputation Service
- Manejo automatizado de vulnerabilidades
- Reportes detallados de cumplimiento que facilitan las auditorías
- Interacción con software antivirus y antispysware
 - Detección de definiciones desactualizadas de la base de virus y malware
 - Detección de equipos donde el antivirus está inactivo o no funcional
 - Actualización automática de las definiciones de virus y malware

Tivoli Endpoint Manager



Seguridad y cumplimiento (cont.)

- Manejo de configuración de seguridad
 - Primer producto certificado por NIST (National Institute of Standards and Technology) para detección y corrección de vulnerabilidades
 - Amplia biblioteca de 'checklists' para detectar fallas de configuración
 - Posibilidad de definir 'checklists' personalizadas
- Soporte para nuevas definiciones SCAP (Security Content Automation Protocol)
- Soporte para análisis de vulnerabilidades mediante el uso de definiciones OVAL (Open Vulnerability and Assessment Language)
- Manejo de vulnerabilidades publicadas por el SANS Institute (SysAdmin, Audit, Network, Security Institute)
- Manejo de parches
 - Este módulo también es parte de "Seguridad y cumplimiento"

Tivoli Endpoint Manager



Seguridad y cumplimiento (cont.)

- Administración de acceso a dispositivos
 - CD, DVD, Floppy
 - USB devices, PCMCIA devices, Parallel port devices
 - Activación/Desactivación del uso de estos dispositivos
 - Reportes históricos de dispositivos conectados en cada endpoint
- Network Access Control
 - Verifica el cumplimiento de ciertos atributos, incluyendo parches de seguridad, antivirus, vulnerabilidades, etc.
 - Si el endpoint no cumple las definiciones de la política, no se le permite el acceso a la red hasta que se solucionen los problemas detectados (Self Quarantine / Network Enforced Quarantine)

Agenda

- **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - ▪ Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**

Tivoli Endpoint Manager



Administración de Energía

- Creciente presión para reducir los costos de funcionamiento
- Uno de los mayores costos de funcionamiento de los departamentos de IT es el consumo eléctrico
- Los endpoints disponen de funcionalidades para el ahorro de energía eléctrica, pero habitualmente no son utilizadas adecuadamente
- Problema difícil de enfrentar, ya que no se tiene noción del consumo de todos los equipos informáticos
- TEM permite hacer una administración completa y permanente del consumo de energía e implementar medidas de ahorro de forma automatizada

Tivoli Endpoint Manager



Administración de Energía (cont.)

- Estadísticas de consumo
- Reportes de opciones de configuración disponible en cada endpoint
- Monitoreo permanente del consumo de energía de todos los endpoints
- Solución de problemas de configuración de energía
- Apagado proactivo de equipos que no están en uso
 - Permite grabar los archivos abiertos antes de apagar el equipo
- Programación de tareas “Wake-On-LAN”
 - Los dispositivos de red son configurados automáticamente
 - Definición de un LMS (Last Man Standing) por sub-red
- Definición de “Perfiles de Energía” con opciones de ahorro que se aplicarán a los endpoints

Tivoli Endpoint Manager

Power Consumption Summary

Aggregate Power Usage

Yearly ▼

Current Power Usage
(11%)

Full Power Consumption ?

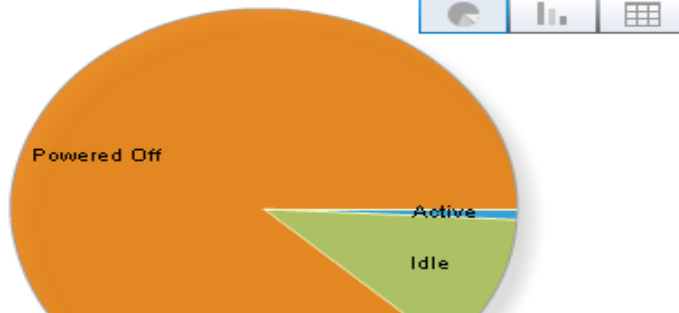


Power	23 kWh	326 kWh	2,716 kWh
Cost	\$2	\$26	\$217
Carbon	32 lb	456 lb	3,802 lb

Yearly Possible Savings: 303 kWh / \$24 / 424 lb

Potential Ecological Impact: 0.0 cars removed or 0.0 acres of trees planted

Average Day Breakdown



Total Tracked Computers

Type	Systems
Laptops	0 (0 %)
Desktops	1 (50 %)
Servers	1 (50 %)
Totals	2 (100 %)
Removed due to errors	0

Power Profile Settings

Computers with System

Agenda

- **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**



Tivoli Endpoint Manager



Core Protection

- Protección de los endpoints en tiempo real:
 - Virus
 - Malware
 - Troyanos
 - Spyware
 - Rootkits
- Protección mediante diversos métodos:
 - File reputation
 - Web reputation
 - Behavior monitoring
 - Personal Firewall
- Detección automática de desktops virtuales para ajustar el uso de recursos
- Basada en tecnologías líderes de Trend-Micro e IBM



TREND
M I C R O™



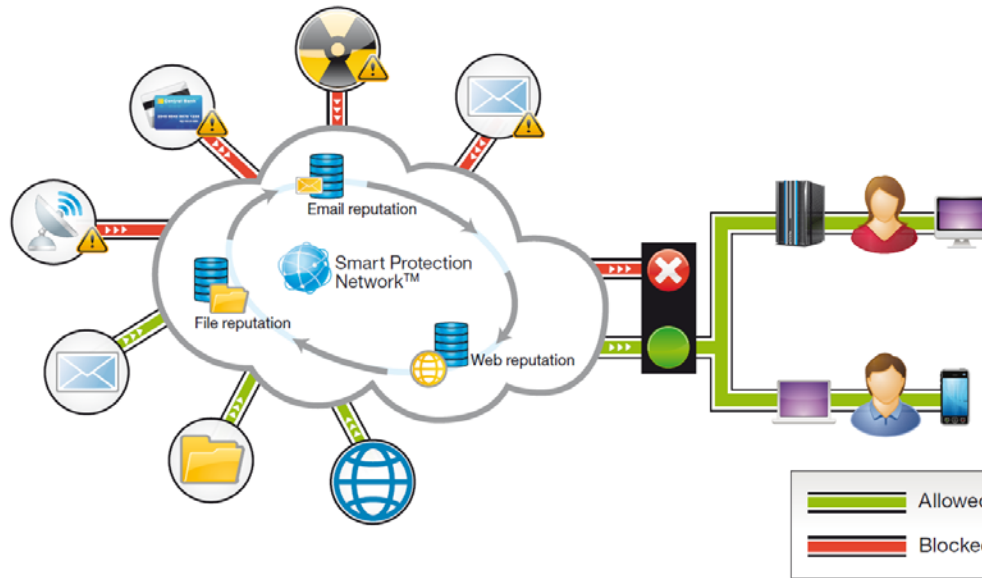
Tivoli Endpoint Manager



Core Protection (cont.)

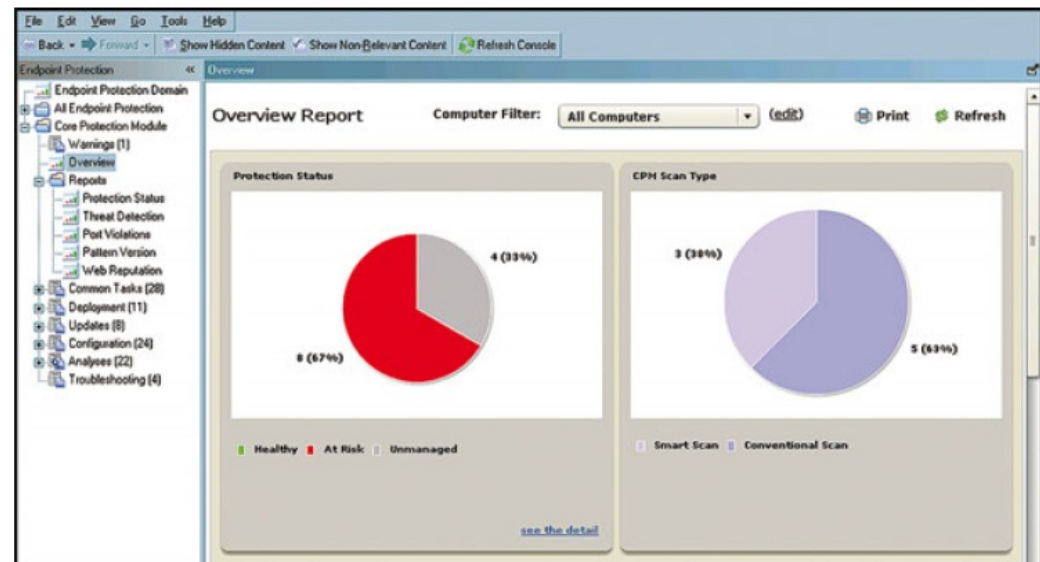
- Solución automatizada y fácil de usar
- Detecta y remueve software malintencionado
- Control centralizado desde una única consola
- Actualización de definiciones automatizada
- Cruzado de referencias con la base de datos “Cloud” de Trend Micro para detección segura de amenazas
- Limpieza de los endpoints, incluyendo procesos y entradas en el registro de Windows que estén ocultas o lockeadas
- Soporte completo para las plataformas:
 - Microsoft Windows Family
 - Mac OS X

Tivoli Endpoint Manager



Utilización de Smart Protection Network de Trend Micro para detección de amenazas

Consola Centralizada de Administración



Agenda

- **Big Fix**
 - Soluciones para Endpoints
 - Big Fix: An IBM Company
- **Tivoli Endpoint Manager**
 - Visión General
 - Patch Management
 - Lifecycle Management
 - Security and Compliance
 - Power Management
 - Core Protection
- **Conclusiones**



Conclusiones

- TEM es una solución completa para el manejo de los endpoints, ya sean:
 - Estaciones de Trabajo
 - Servidores
 - Equipos móviles
 - Hardware dedicado
- Permite realizar el manejo integral de:
 - Distribución de parches
 - Distribución de software
 - Despliegue de sistemas operativos
 - Mantenimiento de inventario de software y hardware
 - Configuraciones de seguridad
 - Manejo de Energía
 - Detección y remoción de virus y software malintencionado
- Un solo servidor TEM permite manejar fácilmente decenas de miles de endpoints
- Diseñado para acceder a endpoints a través de cualquier medio de comunicación disponible, sin importar:
 - Ancho de banda
 - Ubicación geográfica

¿ Preguntas ?

Muchas Gracias !!!