

Parcheado de Sistemas y Gestión de Políticas de Seguridad con IBM BigFix

Abel Llergo
Rafael Rodríguez

Índice

1. Quiénes somos
2. Identificación de la problemática
3. Definición de la solución IBM BigFix
4. IBM BigFix para Gestión de Parches
5. IBM BigFix para Compliance Security

El Grupo Logicalis



Más de
\$1.500 millones
de facturación



Más de
4.200
empleados



Operaciones en
Europa, Estados Unidos,
Latinoamérica, Asia Pacífico
y África



Cerca de
10.000
Clientes de todos
los sectores

Trabajamos con todos los departamentos para conseguir

resultados tangibles y transformadores en el área digital

IT Híbrida 

- Soluciones Cloud
- Data Center
- Seguridad

Digital Workplace 

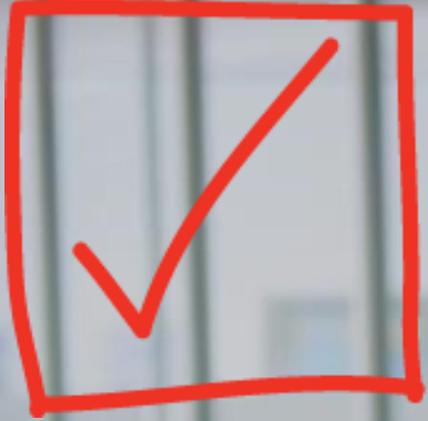
- Comunicaciones y colaboración
- Movilidad
- ITSM

Infraestructura 

- Networking
- Software Defined Networking

Consultoría y Servicios Gestionados 

- Consultoría
- Analytics
- Servicios gestionados

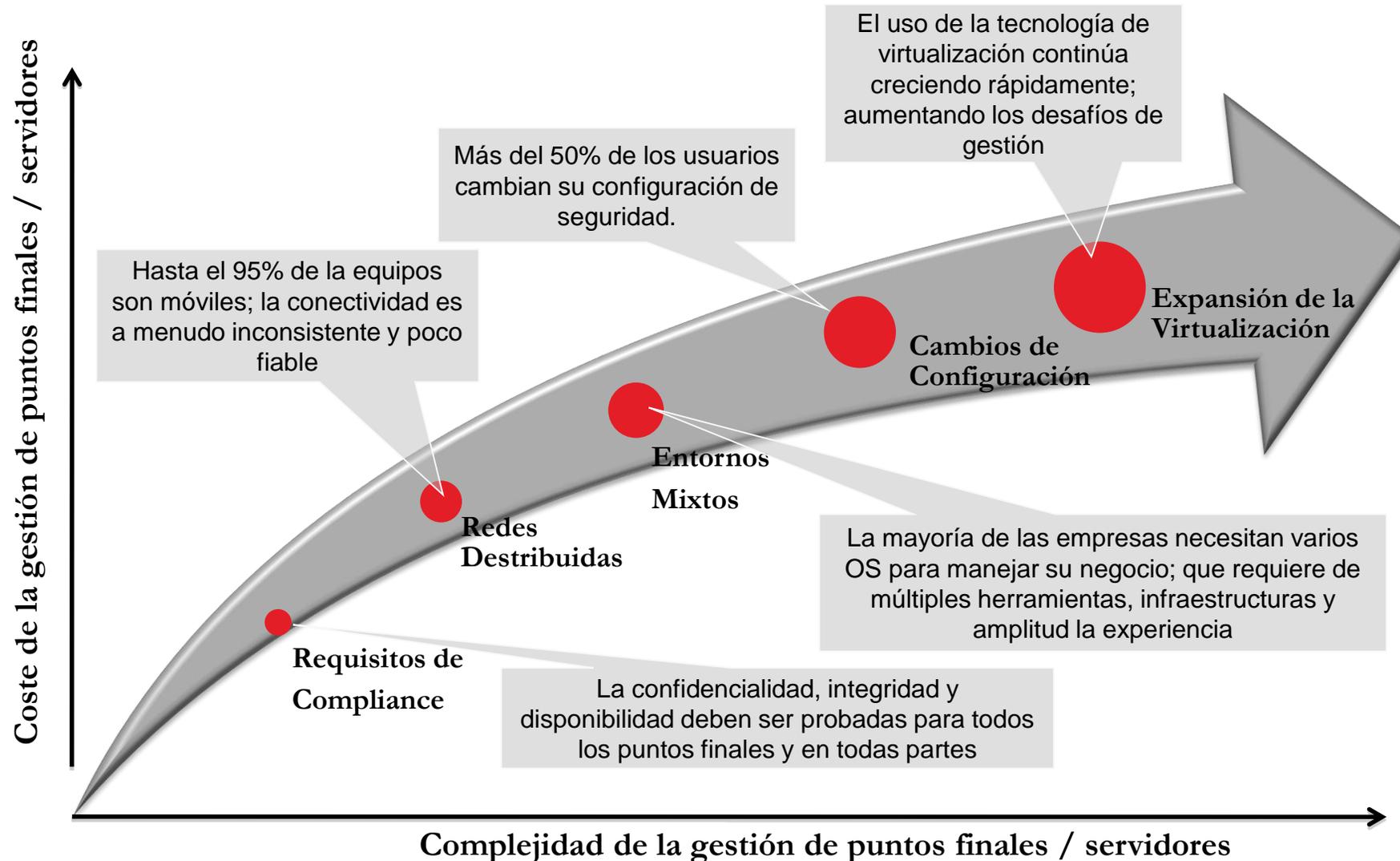


Identificación

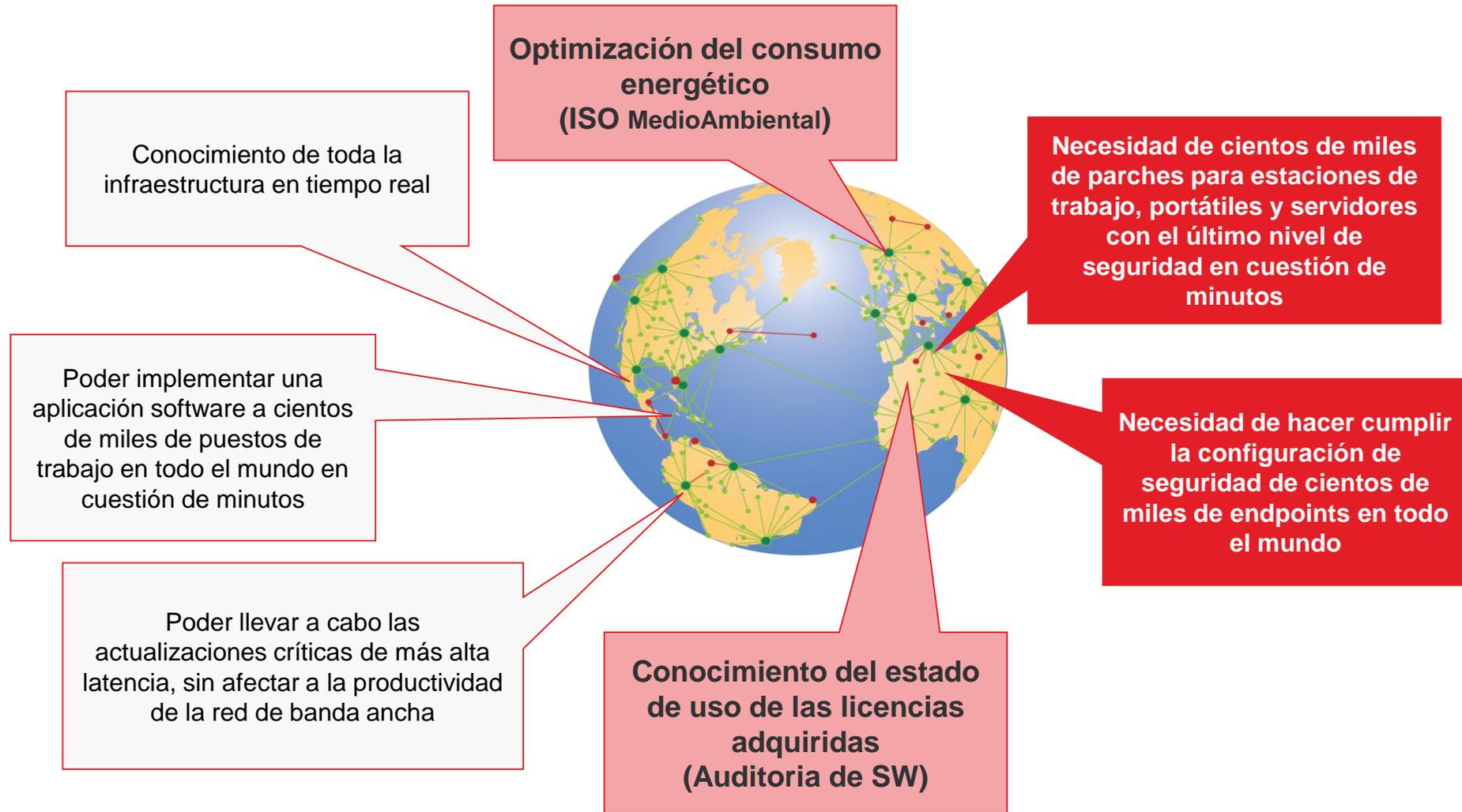
del problema



Identificación de la problemática: Complejidad y coste



Identificación de la problemática





Definición de la solución



¿Qué es IBM BigFix?

IBM BigFix proporciona una solución unificada de gestión de sistemas y seguridad para todos los dispositivos de la empresa.




Lifecycle


Inventory


Patch


Compliance


Detect

¿Qué es IBM BigFix?



IT SECURITY IT OPERATIONS

IBM BigFix
FIND IT. FIX IT. SECURE IT... **FAST**

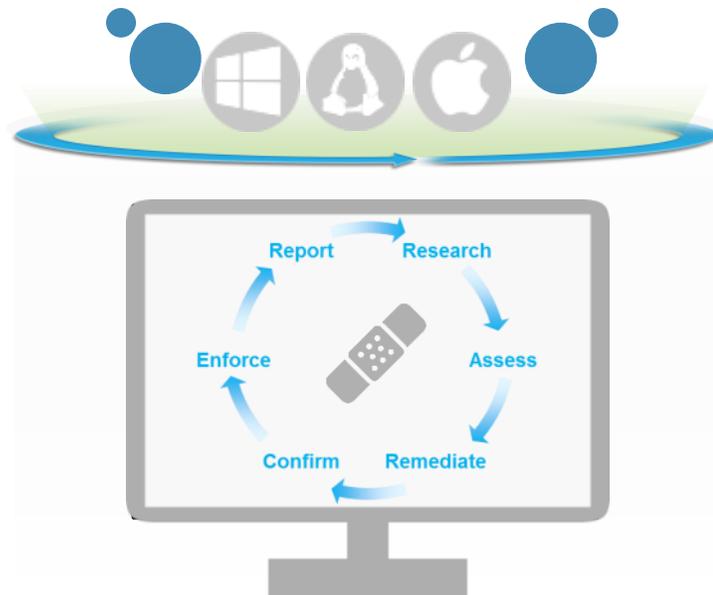
Detect	Compliance	Lifecycle	Inventory	Patch
Detect and respond to malicious activity	Continuous policy enforcement and reporting	Software patching, distribution and provisioning	Audit authorized and unauthorized software	Automated patching with high first pass success
<ul style="list-style-type: none"> • Asset discovery • Detect • Investigate • Response • Query • Patch management • Software distribution 	<ul style="list-style-type: none"> • Query • Patch management • Security configuration management • Vulnerability assessment • Compliance analytics • Third-party anti-virus management • Self quarantine • Add-on: PCI DSS 	<ul style="list-style-type: none"> • Asset discovery • Patch management • Software distribution • Query • Advance patching • Remote control • OS deployment • Power management • Sequenced Task Automation 	<ul style="list-style-type: none"> • Software / hardware inventory • Software usage reporting • Software catalogue correlation • ISO 19770 software tagging 	<ul style="list-style-type: none"> • OS patching • Third-party application patching • Offline patching

IBM BigFix para Gestión de Parches



IBM BigFix Patch: Descubrimiento y Parcheado

Una única consola de gestión para identificar, parchear e informar sobre múltiples dispositivos (con distintos SSOO).

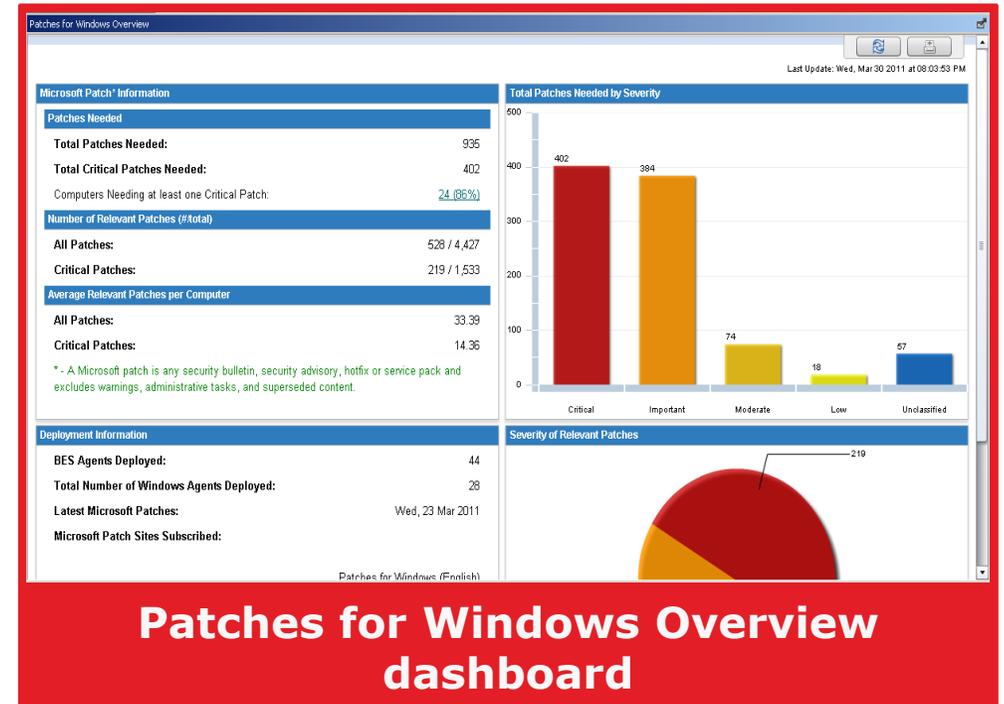


- **Descubre e informa sobre cada endpoint.**
 - Desktops
 - Laptops
 - Servers
 - Purpose-specific endpoints
e.g., ATMs and point-of-sale (POS) devices
- **Permite obtener una visibilidad exacta y actualizada; y la aplicación continua de parches.**
- **Gestión de parches a cientos de miles de endpoints, múltiples SSOO y aplicaciones *de forma automática.***
- ***Más del 98% de éxito* en la primera aplicación del parche.**

IBM BigFix Patch: Status de Parches Críticos de Seguridad

Con cada vez más parches críticos por semana, ¿cómo puedo mantener el ritmo de aplicarlos?

- Aumenta la tasa de éxito de primera aplicación del 60-75% al 95-99%.
- Reduce los tiempos de revisión y aplicación de semanas y días a horas y minutos.
- Reporting en tiempo real.
- Proporciona parches a los endpoints independientemente de su ubicación, tipo de conexión o estado.
- Para SSOO y aplicaciones (Adobe, Mozilla, Apple, Java...)
- Evaluación automatizada, no se requiere de escaneo centralizado o remoto.



IBM BigFix Patch: Principales Características

Más contenido, mayor velocidad de despliegue y cobertura más amplia.

- ✓ Mayor cobertura de parches de productos Microsoft facilitando la confianza del administrador en la solución



- ✓ Mayor cobertura para el soporte de aplicaciones de terceros.

- ✓ Repositorio personalizado para descargas de Java que ayuda a proteger un área común de vulnerabilidad

- ✓ Desplegar actualizaciones en las imágenes de disco existentes para un fácil rollback.



- ✓ Vista previa de implementaciones de paquetes TL y SP que permite reducir errores de parcheo durante las ventanas de mantenimiento

- ✓ El asistente de AIX Deployment soporta NFS que minimiza los requisitos de espacio en disco

- ✓ Parches para múltiples distribuciones de Linux con una sola herramienta



- ✓ Soporte de Native Tools que garantiza flexibilidad y fiabilidad en la implementación de parches

- ✓ Capacidad de rollback de parches, disminuyendo de esta forma el esfuerzo manual

- ✓ Compatibilidad con NFS para parches de Solaris que permite minimizar los requisitos de espacio en disco



- ✓ Patch cluster fixlets for Solaris Live Upgrade to support cluster patching of alternate boot environment

- ✓ Tareas de instalación de paquetes para Solaris 11 consiguiendo una administración remota mejorada y reduciendo los costes de soporte in situ

IBM BigFix Patch: Diferenciadores clave

■ Compliance Continuo

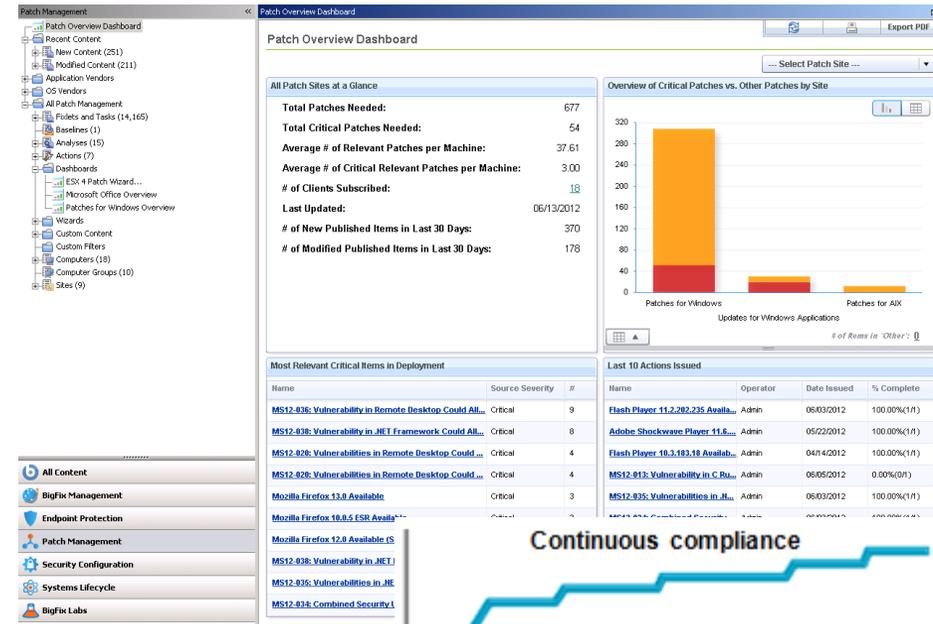
- El agente inteligente evalúa el sistema para identificar parches necesarios a aplicar o corruptos
- Evaluación automática del estado de parcheado una vez es implementado
- Distribución de parches y actualizaciones de software a endpoints en cualquier lugar
- Aplicación de políticas de parcheado para lograr un cumplimiento continuo

■ Visibilidad

- Informes centralizados de todos los activos
- Proporciona un proceso de parcheo automatizado y simple que se administra desde una única consola

■ Escalabilidad

- Escalable de 1 a 250.000 endpoints con un solo servidor



IBM BigFix para

Compliance de Security

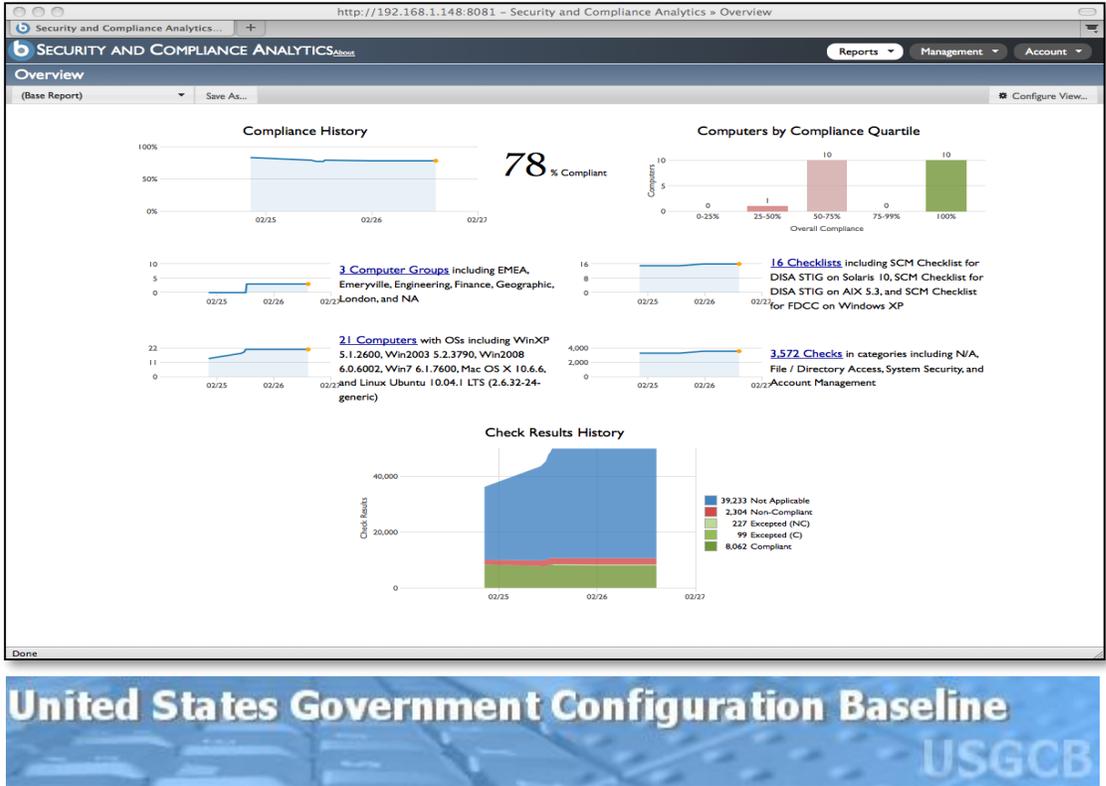




BigFix Compliance

BigFix Compliance proporciona un cuadro de mando para análisis y reporting de cara a cumplir con las normativas internas y externas y la seguridad de TI.

Permite determinar el progreso y muestra las tendencias a través de las configuraciones continuas de las políticas de seguridad y permite identificar las exposiciones y los riesgos de seguridad de los puntos finales

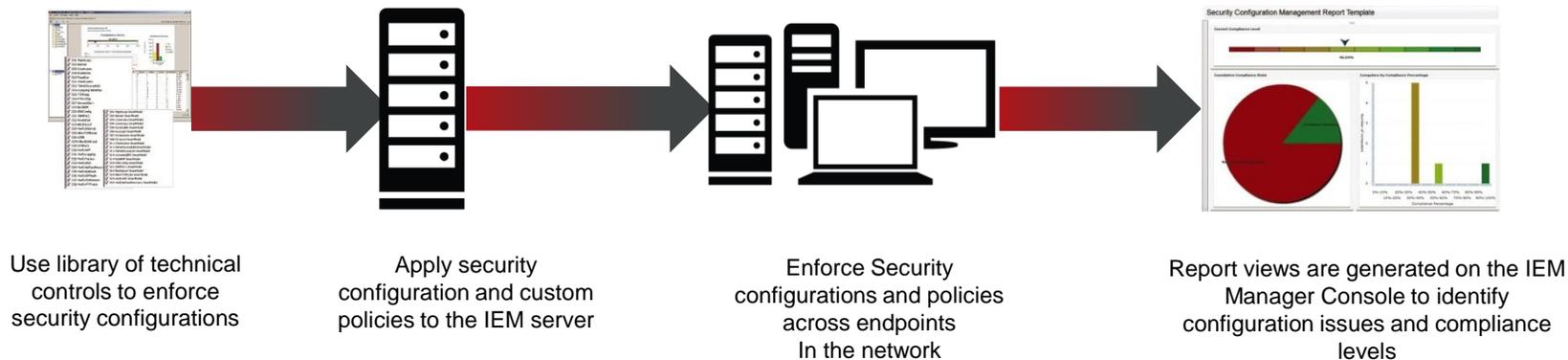


IBM BigFix Compliance – Bastionado

Gestión de la configuración y del cumplimiento

Reto:

- Protección de los activos TI en un entorno de amenazas en constante escalada y en evolución
- Cumplimiento de las exigencias reglamentarias y demostrar el cumplimiento en tiempo real



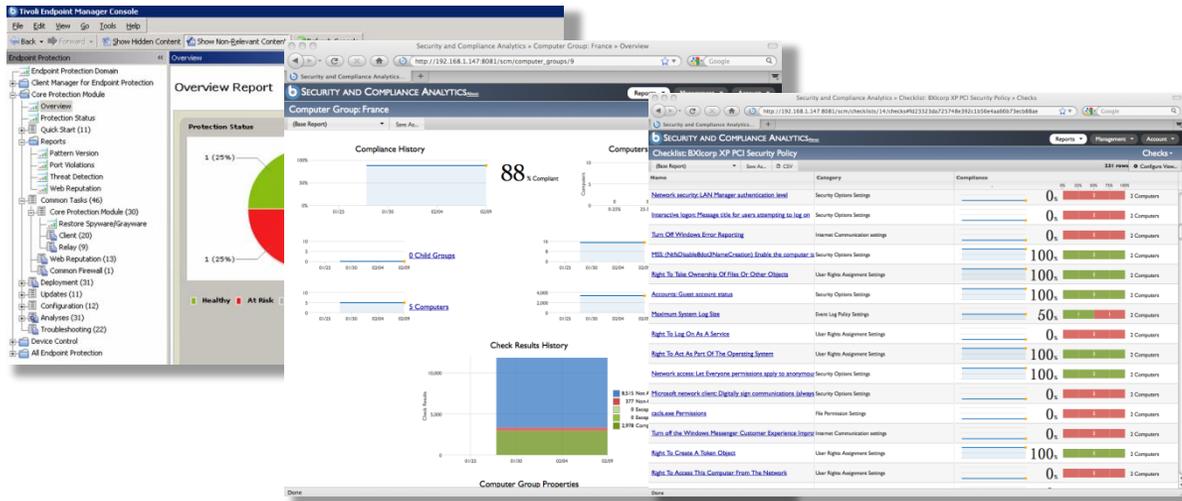
BigFix Compliance permite una configuración continua de cumplimiento para cualquier tipo de activos Servidores, puestos de trabajo y portátiles

IBM BigFix Compliance – Bastionado

- Asset Discovery
- Compliance Analytics
- Patch Management
- Security Configuration Management
- Vulnerability Management
- Multi-Vendor Endpoint Protection Management

Librería con más 15,000 ajustes de cumplimiento, incluyendo soporte de las normativas FDCC, USGCB, DISA STIG, CIS, PCI-DSS

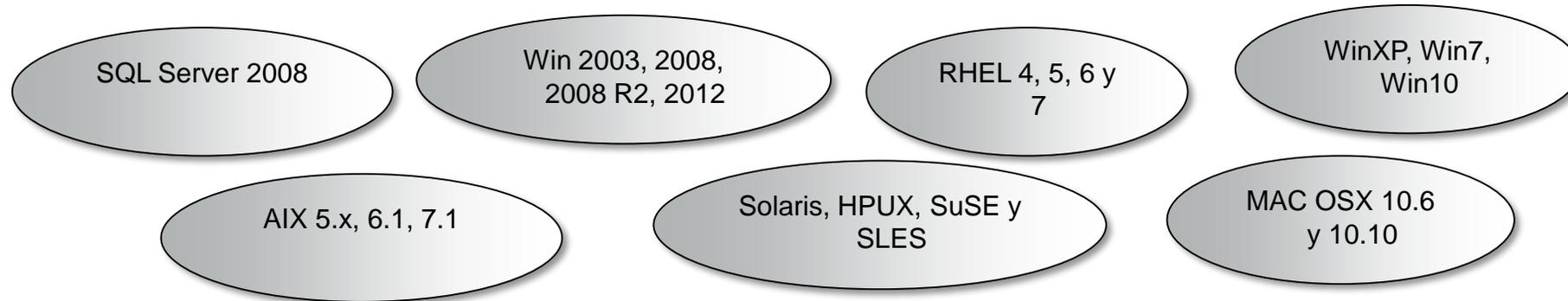
Cumplimientos de las políticas de forma automática y continua en los dispositivos.



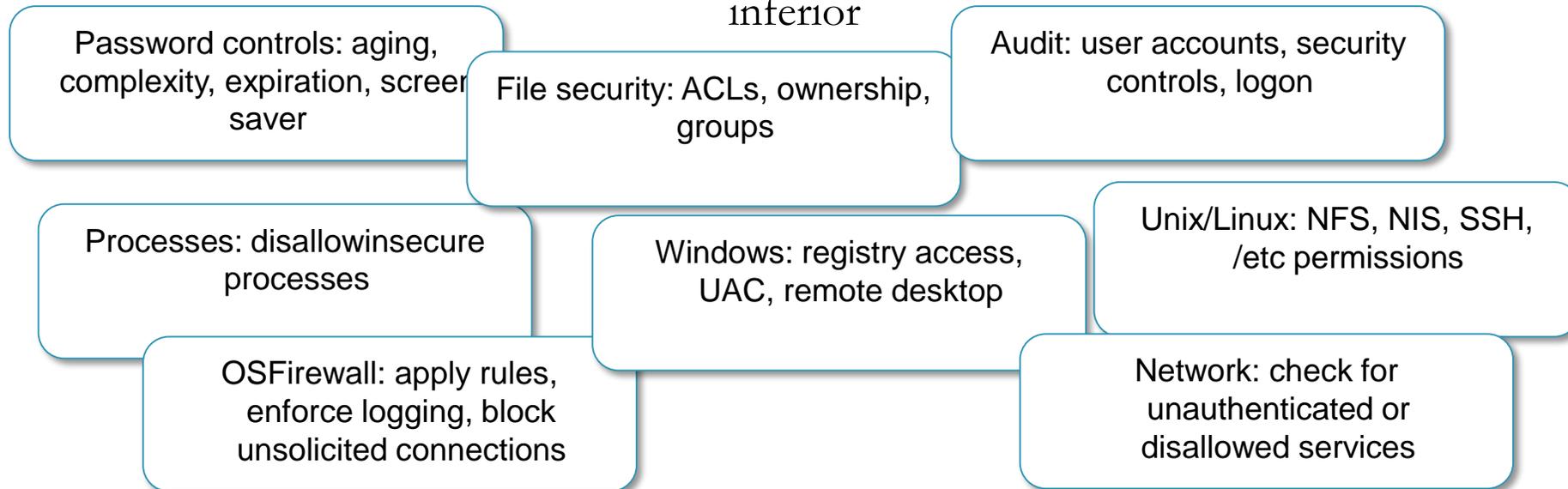
- Automatiza y gestiona de forma **continua la configuración de seguridad y las políticas de cumplimiento**.
- De forma fácil y rápida evalúa **la postura de seguridad** del dispositivo gestionado.
- Automáticamente **parchea y remedia** los sistemas que no cumplen con las políticas de seguridad.
- Despliega, actualiza y muestra el estado de salud de las soluciones de **Antivirus** de diferentes proveedores
- Identifica, gestiona e informa de las **excepciones y desviaciones de las políticas**.

Descripción de IBM BigFix Compliance

+30 Sistemas Operativos + Internet Explorer y Windows Firewalls



Mejores prácticas de controles de seguridad: De la parte superior a la amplia cobertura inferior





Business and technology working as one

Gracias

