Pulse Comes To You

PCTY2011

Soluciones de Seguridad, para un planeta más inteligente

http://www.ibm.com/security

Juan Paulo Cabezas
Arquitecto de Seguridad para Sudamérica
jcabezas@cl.ibm.com

IBM®

¿Hacia donde va la seguridad en un planeta más inteligente?

Nuestro mundo esta cada vez más

Instrumentado

Nuestro mundo esta más

Interconectado

Nuestro mundo es cada vez más

Inteligente

Nuevas posibilidades.

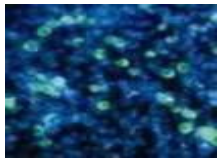
Nuevas complejidades.

Nuevos Riesgos.


Smart supply chains


Smart countries


Smart retail


Smart water management


Smart weather


Smart energy grids


Intelligent oil field technologies


Smart regions

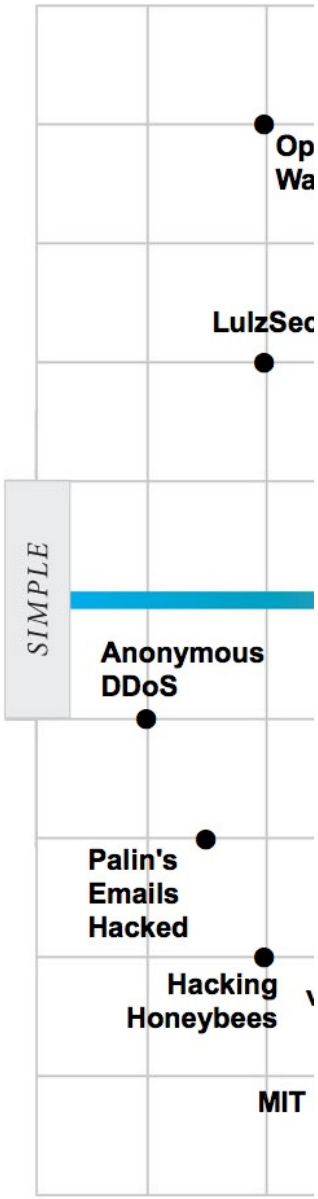

Smart healthcare


Smart traffic systems


Smart cities


Smart food systems

Características de 25 “eventos”



An
pe
Aye
grup
ellos
crec

Es a
atac
com

Lo r
San
resp
más

Los
por
un g
cola

La s
un c
en s
cont

Lunes 20 de junio del 2011 | 11:55

Política

Web de la Presidencia de Ecuador sufrió ataque informático

AFP | QUITO

La página web de la **Presidencia de Ecuador** y su **portal informativo** fueron objeto de ataques informáticos el pasado fin de semana que no afectaron sus bases de datos, reportó este lunes el gobierno.

"Estamos investigando el origen (de los bloqueos), hemos restablecido las páginas y será cuestión de seguir trabajando en eso", dijo a la prensa el subsecretario de Innovación y Nuevos Medios, Marco Antonio Bravo.

Los ataques ocurrieron el domingo y dejaron fuera de servicio el sitio de la Presidencia durante dos horas. La página **elciudadano.com** -periódico electrónico del ente gubernamental- fue restablecida una hora después del hecho.

Fotos

Ampliar imagen

El sitio www.presidencia.gov.ec permaneció durante dos horas el pasado domingo fuera del aire por ataques informáticos.

Bravo señaló, basado en un primer informe técnico, que **no hubo daño a la información ni a las bases de datos** de ambos sitios, y que el caso está siendo analizado con el área de seguridad y sistemas de la Presidencia.

Las intromisiones fueron reivindicadas por un grupo que se identificó como "Latin hack team", que dejó un mensaje en la web presidencial: **"¡Contra la hipocresía y la corrupción de los gobiernos, por la libertad de expresión!**

Es el segundo ataque de piratas informáticos que sufre el sitio de la Presidencia, luego del ocurrido en febrero de 2008.

Características del nuevo escenario y cambio de paradigma

- En el informe anual de X-Force del 2010 se indica: ".. En vez de enfocarse en un único punto de entrada, las nuevas amenazas tienen como objetivo múltiples recursos en la compañía. No sólo lo expuesto al público esta en riesgo, sino que, cada empleado y endpoint se ha convertido en un potencial punto de entrada".

- El "adversario" externo es altamente entrenado e inteligente, por lo que se requiere una postura más activa ante el riesgo.

- Algunos mensajes de nos avisan el cambio:
  - "Las agencias deben ser capaces de monitorear continuamente la información de seguridad a través de la organización, de una manera gestionable y procesable"
  - Alan Paller, *Director de investigación del instituto SANS*, indicó ante el Congreso: ".. Las Agencias deben dejar de gastar dinero en reportes anticuados, en vez deben enfocar su gasto en el monitoreo continuo y reducción del riesgo"

1. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
2. http://www.thenewnewinternet.com/2010/06/16/alan-paller-our-cyber-defense-must-be-near-perfect/

Framework de Soluciones de Seguridad IBM

GRC

GOBIERNO DE SEGURIDAD, GESTIÓN DE RIESGO Y CUMPLIMIENTO

Asegurar gestión integral de actividades de seguridad y conformidad con todos los mandatos de seguridad

PERSONAS E IDENTIDAD

Mitigar los riesgos asociados con el acceso de usuarios a recursos corporativos

DATOS E INFORMACIÓN

Comprender, desplegar, y probar correctamente controles para el acceso y uso de datos sensitivos

APLICACIONES Y PROCESOS

Mantener a las aplicaciones seguras, protegidas de uso malicioso o fraudulento, y más robustas contra fallas

REDES, SERVIDORES Y END POINT

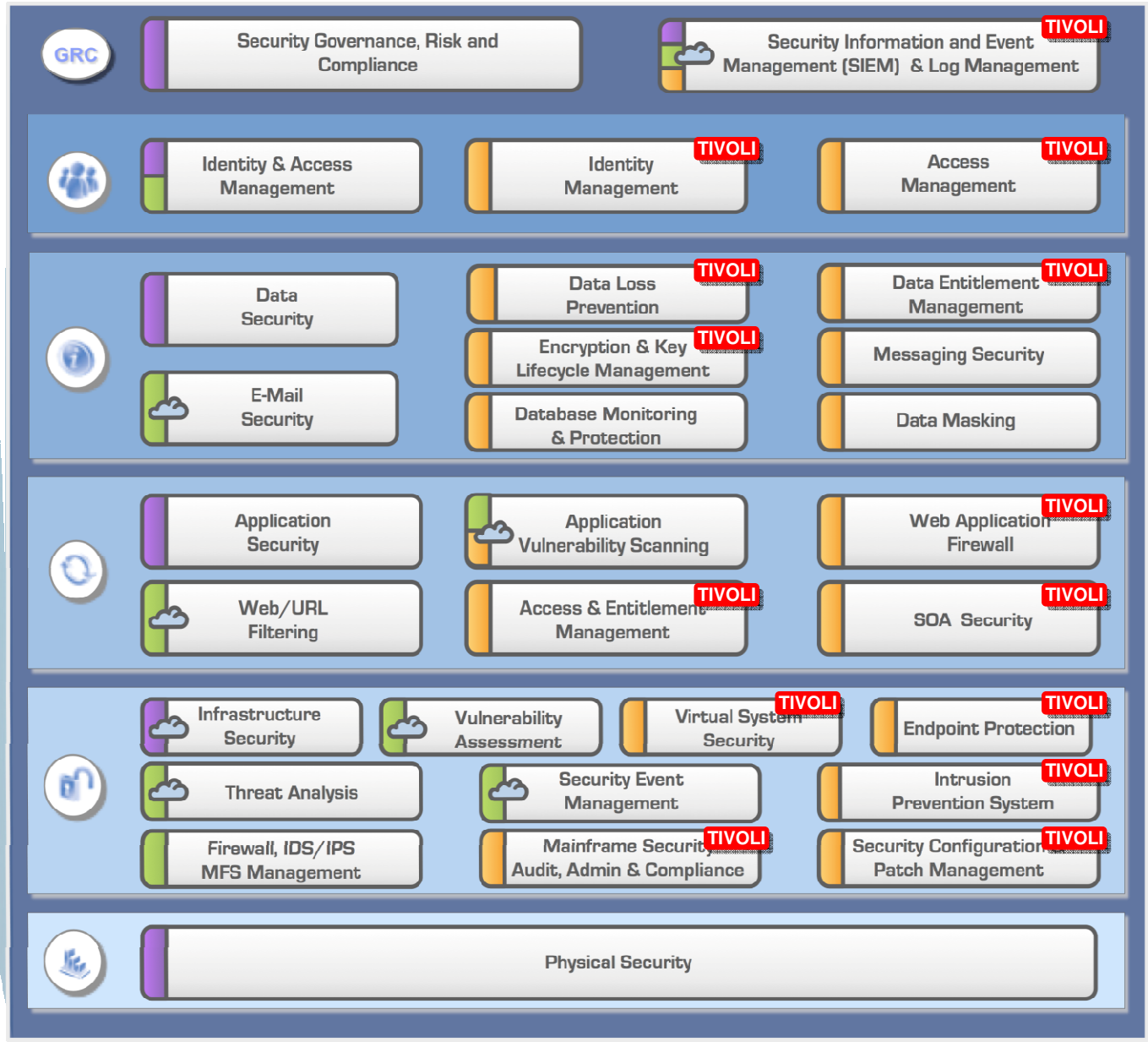
Optimizar la disponibilidad de servicio al mitigar riesgos para componentes de red

INFRASTRUCTURA FÍSICA

Proporcionar inteligencia practicable en el estado deseado de seguridad de infraestructura física y realizar mejoras

IBM Security Solutions Portafolio

- Professional Services
- Managed Services
- Products
- Cloud Delivered



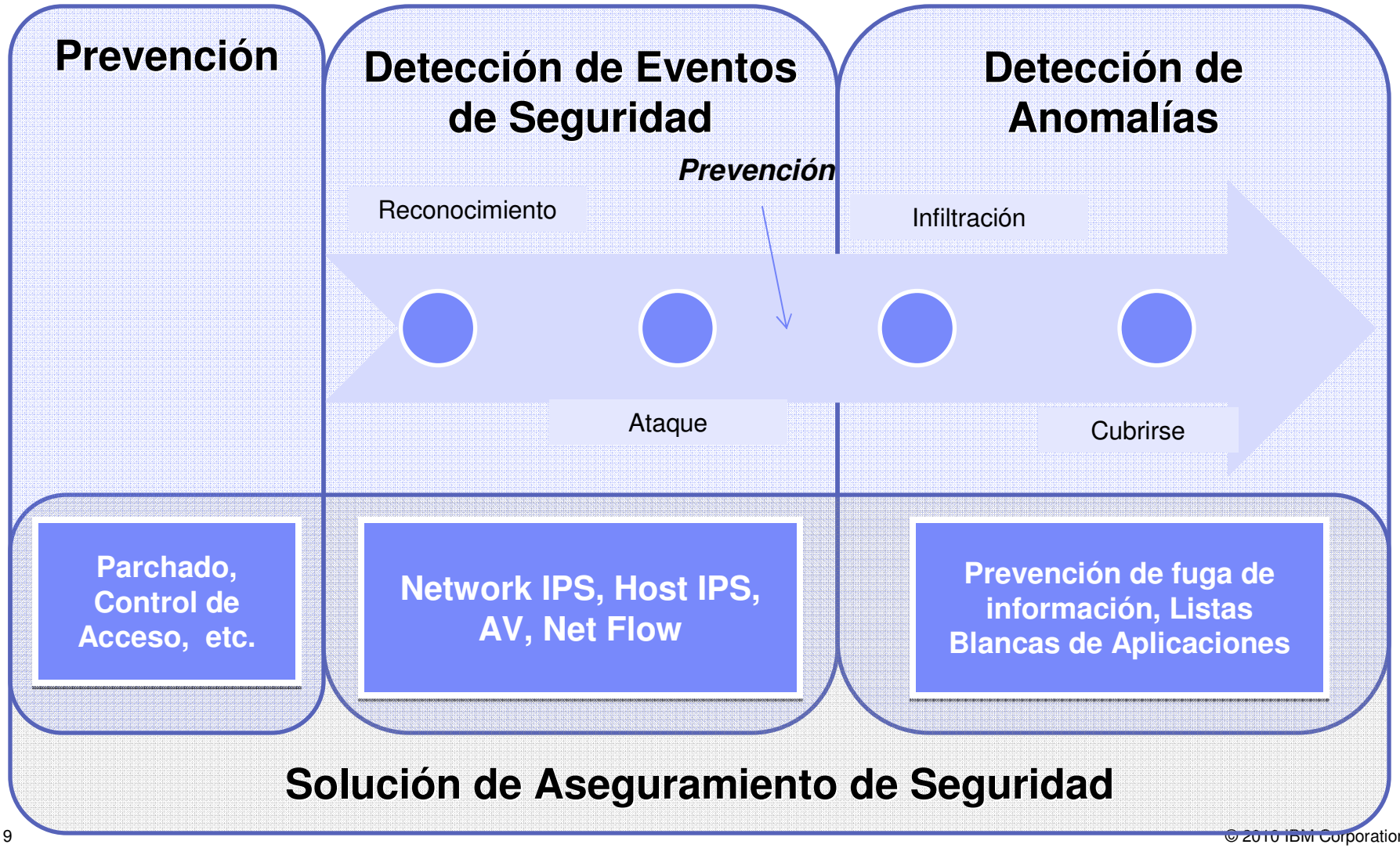
TOP 20 Controles Críticos de Seguridad, según Instituto SANS

1. Inventario de Dispositivos autorizados y no autorizados: Tivoli Endpoint Mgr
2. Inventario de Software autorizado y no autorizado: Tivoli Endpoint Mgr
3. Asegurar la configuración de Hardware y Software para Laptops, estaciones de trabajo y servidores: Tivoli Endpoint Mgr y IBM Security Server Protection
4. Asegurar la configuración de dispositivos de redes como Firewalls, Routers, y Switches: Tivoli Netcool Configuration Manager
5. Defensa perimetral: IBM Security Network IPS
6. Almacenamiento, Monitoreo y Análisis de registros de auditoría de seguridad: Tivoli Security Information & Event Mgr
7. Seguridad de Software Aplicativo: IBM Security Network IPS + Rational Appscan
8. Control del uso de Privilegios Administrativos: Tivoli Identity Mgr+Tivoli Access Mgr ESSO = Privileged Identity Manager

TOP 20 Controles Críticos de Seguridad, según Instituto SANS

9. Controlar el acceso basado en lo que se necesita saber: IBM Security Server Protection y Tivoli Endpoint Mgr
10. Revisión y Remediación continua de vulnerabilidades: Tivoli Endpoint Mgr y IBM Security Network IPS
11. Control y Monitoreo de Cuentas: Tivoli Identity Mgr+Tivoli Security Information & Event Mgr
12. Defensas de Malware: Tivoli Endpoint Mgr for Core Protection, IBM Security Network IPS y IBM Security Server Protection
13. Limite y Control de Puertos, Protocolos y Servicios: Tivoli Endpoint Mgr, IBM Security Network IPS, IBM Security Virtual Server Protection, IBM Security Server Protection
14. Control de Dispositivos Inalámbricos
15. Prevención de Fuga de Información: IBM Security Network IPS, IBM Security Virtual Server Protection, IBM Security Server Protection

Protección de Amenazas en profundidad

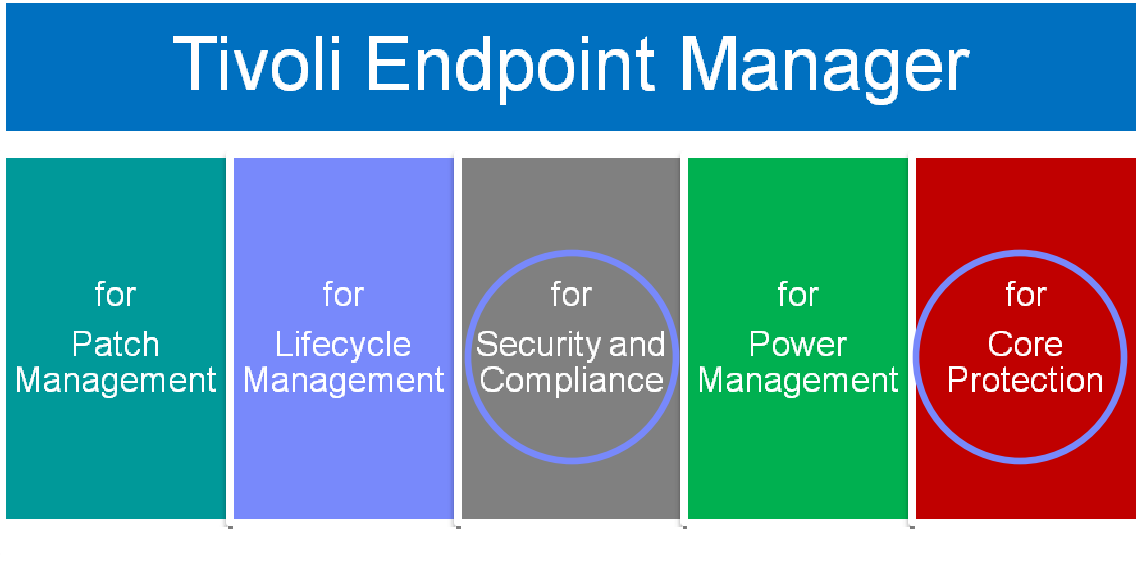


Tivoli Endpoint Manager permite a los clientes consolidar sus operaciones de TI y funciones de seguridad en una sola vista

Comentarios de clientes:

- "Se reemplazó el antivirus existente en 4300 estaciones de trabajo en 2 semanas, sin problemas"
- "Se pasó de un 60% al 95%+ de A/V actualizados a la última firma"
- "No se necesitó hardware adicional para su funcionamiento"

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

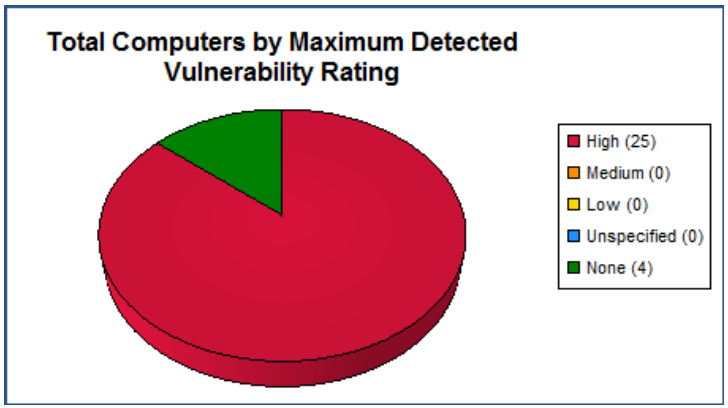


10

Tivoli Endpoint Manager for S&C, Visualizando el estado de las vulnerabilidades

Detección y Gestión de vulnerabilidades basadas en:

- OVAL Open Vulnerability and Assessment Language
- CVE Common Vulnerabilities and Exposures
- CVSS Common Vulnerability Scoring System



Vulnerabilities to Windows Summary

Total Unique Detected Vulnerabilities

Total Unique Detected Vulnerabilities:	2,129
Total Unique Detected Vulnerabilities Rated High:	1478

Total Unique Vulnerabilities:

Total Unique Vulnerabilities:	2,885
Total Unique Detected Vulnerabilities Rated High:	1,984

Description

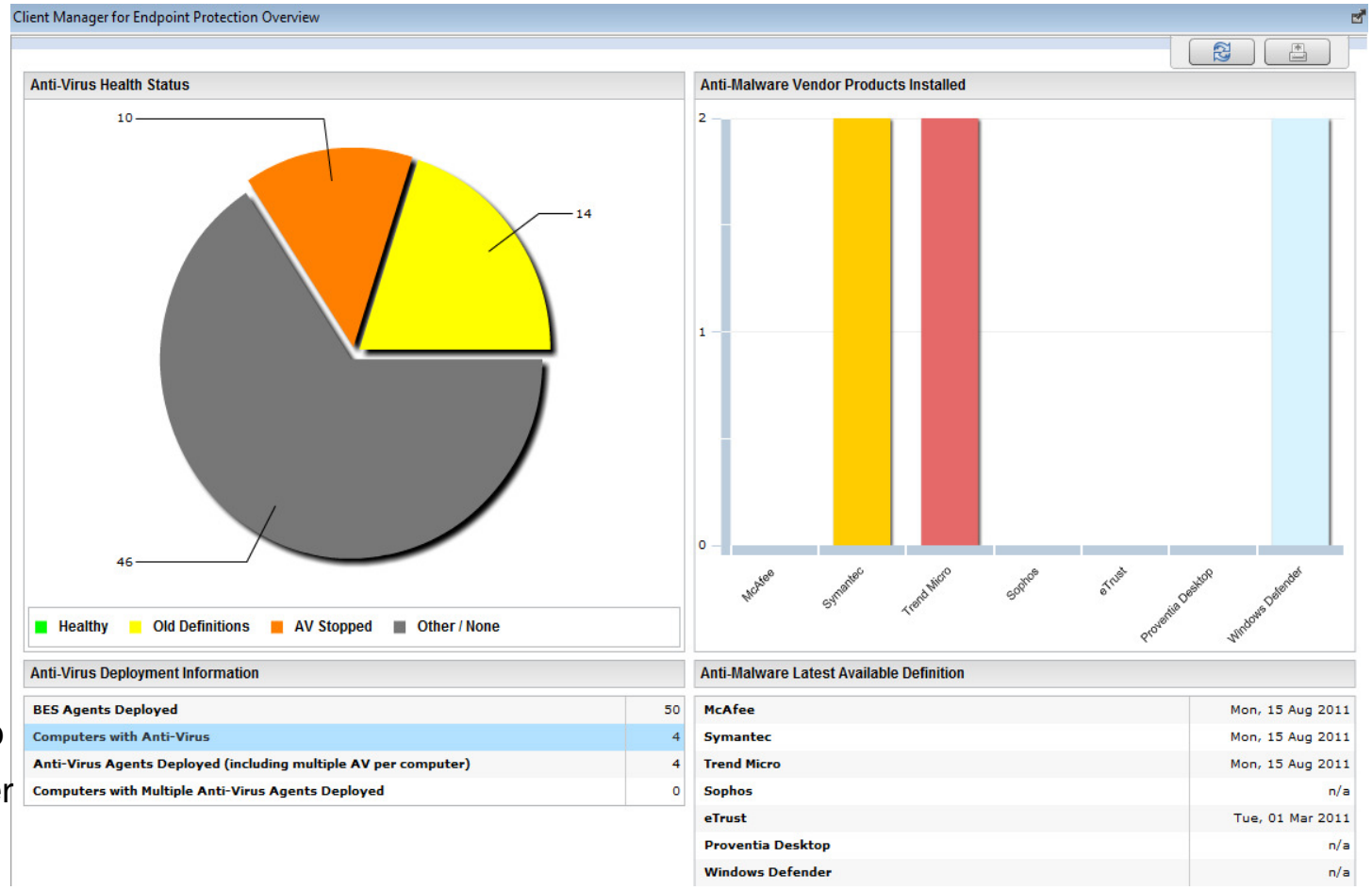
Multiple buffer overflows in the Resolution Service for Microsoft SQL Server 2000 and Microsoft Desktop Engine 2000 (MSDE) allow remote attackers to cause a denial of service or execute arbitrary code via UDP packets to port 1434 in which (1) a 0x04 byte that causes the SQL Monitor thread to generate a long registry key name, or (2) a 0x08 byte with a long string causes heap corruption, as exploited by the Slammer/Sapphire worm.

CVE: CVE-2002-0649
OVAL: OVAL1077
OVAL Status: ACCEPTED
CVSS Base Score: 7.5 (HIGH)
CVSS Base Score Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Vulnerability assessment definition from MITRE OVAL repository at oval.mitre.org (schema version 5.0). BigFix Enterprise Suite has met the Mitre OVAL/OVAL-ID Compatibility Requirements.

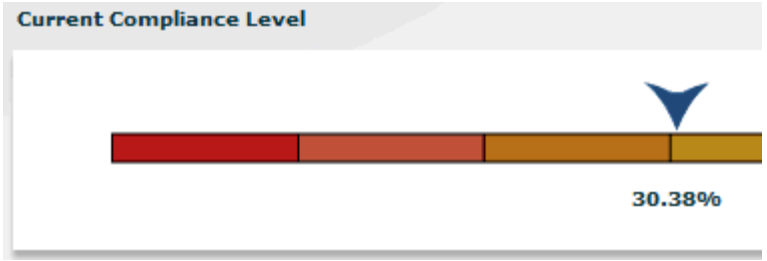
Tivoli Endpoint Manager for S&C, mejorando la gestión de antivirus de terceros

- Seguimiento
  - Instalado
  - Actualizado
  - Corriendo
  - Patrón al día
- Antivirus:
  - McAfee
  - Symantec
  - Trend Micro
  - Sophos
  - CA eTrust
  - Proventia Desktop
  - Windows Defender



Tivoli Endpoint Manager for S&C, revisando continuamente el estado cumplimiento de configuraciones de seguridad

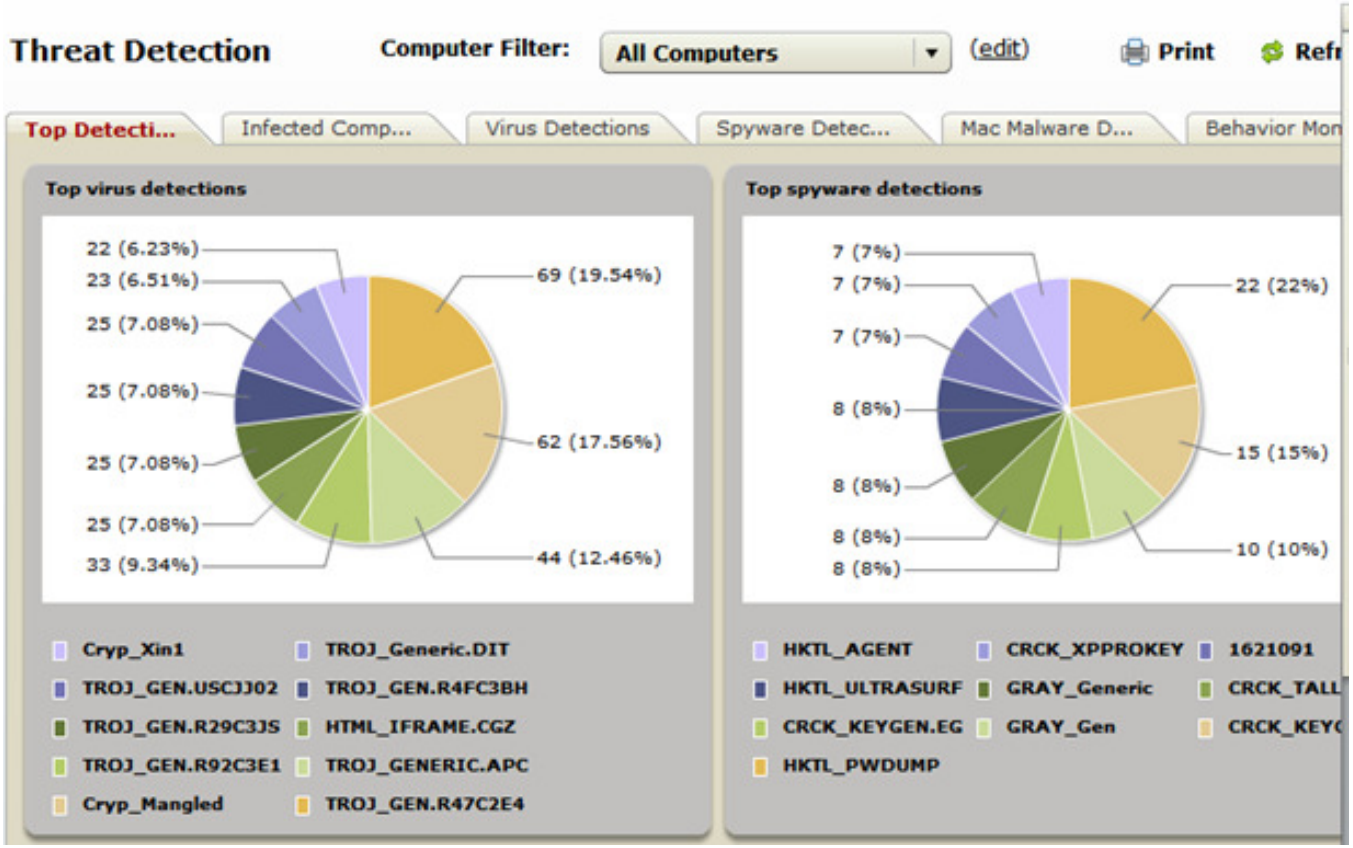
- SANS Top Vulnerabilities
- Defense Information Systems Agency, Security Technical Implementation Guide, para Unix y Windows
- Federal Desktop Core Configuration
  - Win XP/Vista
  - Win 2003
- United States Government Configuration Baseline



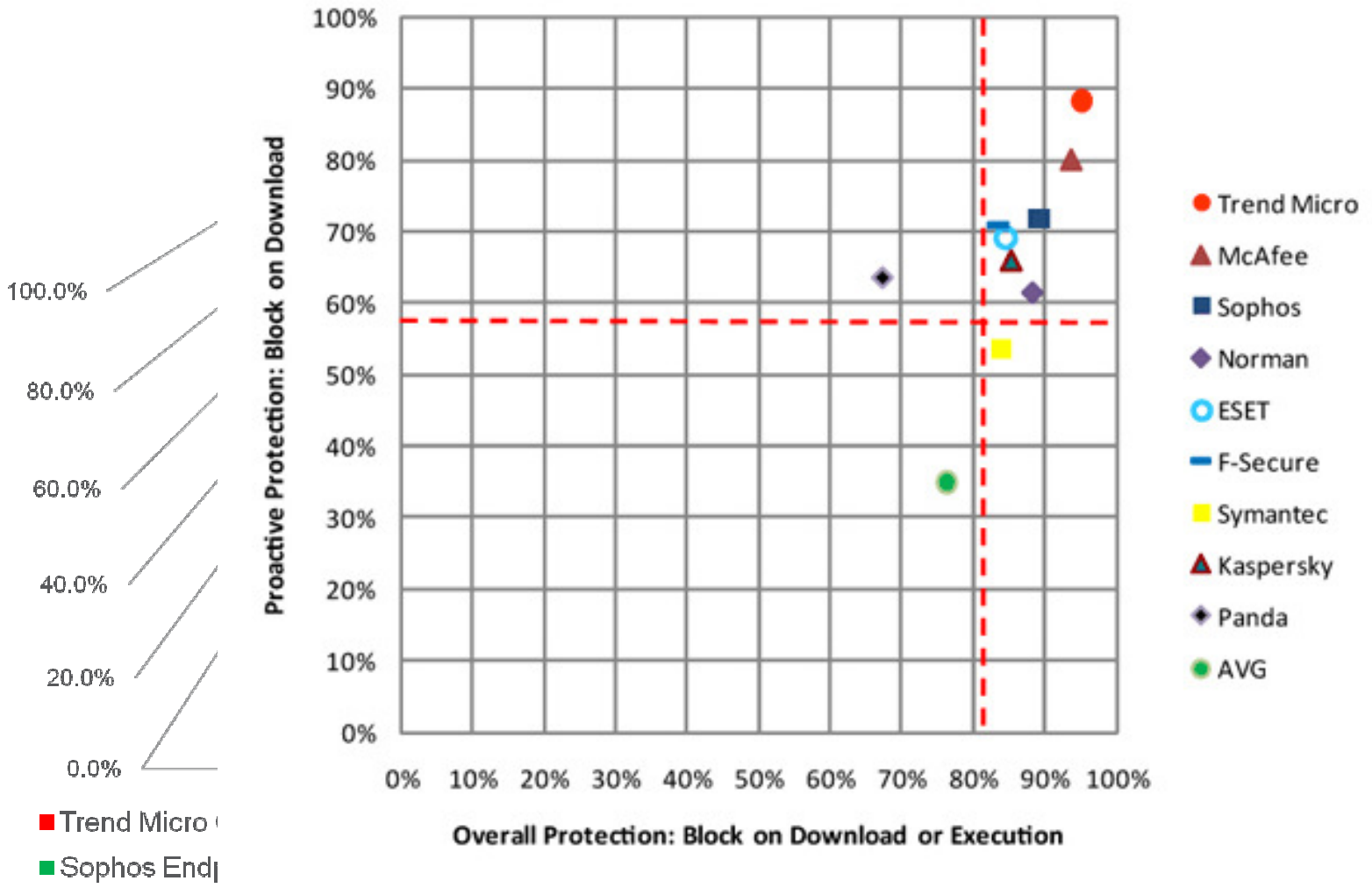
Component Name	Non-Compliant	Subsci	Category	Iden	Type	Standard	Exclus	Enabled
Turn off shell protocol protected mode	1	1	Windows Explorer Settings	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Turn off printing over HTTP	1	1	Internet Communication se	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Network security: Minimum session security for NTLM SSP b	1	1	Security Options Settings	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Accounts: Rename guest account	1	1	Security Options Settings	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Teredo State	1	1	IPv6 Transition Technologie	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Network access: Shares that can be accessed anonymously	1	1	Security Options Settings	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Enable user control over installs	1	1	Windows Installer Settings	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Turn off Internet connection wizard if URL connection is ref	1	1	Internet Communication se	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Computer Account Management	1	1	Account Management Settir	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Turn off Internet file association service	1	1	Internet Communication se	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Network security: Allow LocalSystem NULL session fallback	1	1	MSS Security Options Settir	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑
Turn off downloading of print drivers over HTTP	1	1	Internet Communication se	CCE-	Micrc	USGCB Checklist for Windows 7	Includ	☑

Tivoli Endpoint Manager for Core Protection

- Basado en tecnología de Trend Micro
- Protección en tiempo real para virus, troyanos, spyware, rootkits
- Firewall personal
- Reputación de archivos y Web
- Consiente de ambientes virtualizados
- Consola única administrativa
- Bajo consumo de recursos



TEM for Core Protection, utiliza tecnología líder



Source: ***Real World Corporate Endpoint Test Report*****, January 2011**
http://us.trendmicro.com/imperia/md/content/us/pdf/trendwatch/av-test_january_2011_enterprise_endpoint_comparative_report_final.pdf
http://us.trendmicro.com/us/trendwatch/core-technologies/competitive-benchmarks/nss-labs/

IBM Security Intrusion Prevention Systems

Funcionalidades Claves

•Equilibrio entre seguridad y rendimiento de las aplicaciones críticas de negocio
•Enfocado a gestionar amenazas cambiantes en un ambiente con pocos recursos y baja especialización
•Reducir el costo y la complejidad de la infraestructura de seguridad
•Tres modos de funcionamiento:
- PASSIVE MONITORING
- INLINE SIMULATION
- INLINE PREVENTION

Capacidades básicas

Protección más allá de los IPS de red tradicionales:

• Protección de aplicaciones Web
• Protección de ataques a nivel cliente
• Funcionalidades de Data Loss Prevention (DLP)
• Control Aplicativo
• Tecnología de Virtual Patch

IBM Protocol Analysis Modular Technology

Nueva Línea GX7000, mejor relación precio/Mb

Capacidades	GX7412	GX7800
Latencia	**<150µSec**	**<150µSec**
Conexiones/Seg	**647,481**	**703,788**
Conexiones abiertas	**12,500,000**	**12,500,000**

GX7412

GX7800

Modelos de IBM Security Network IPS

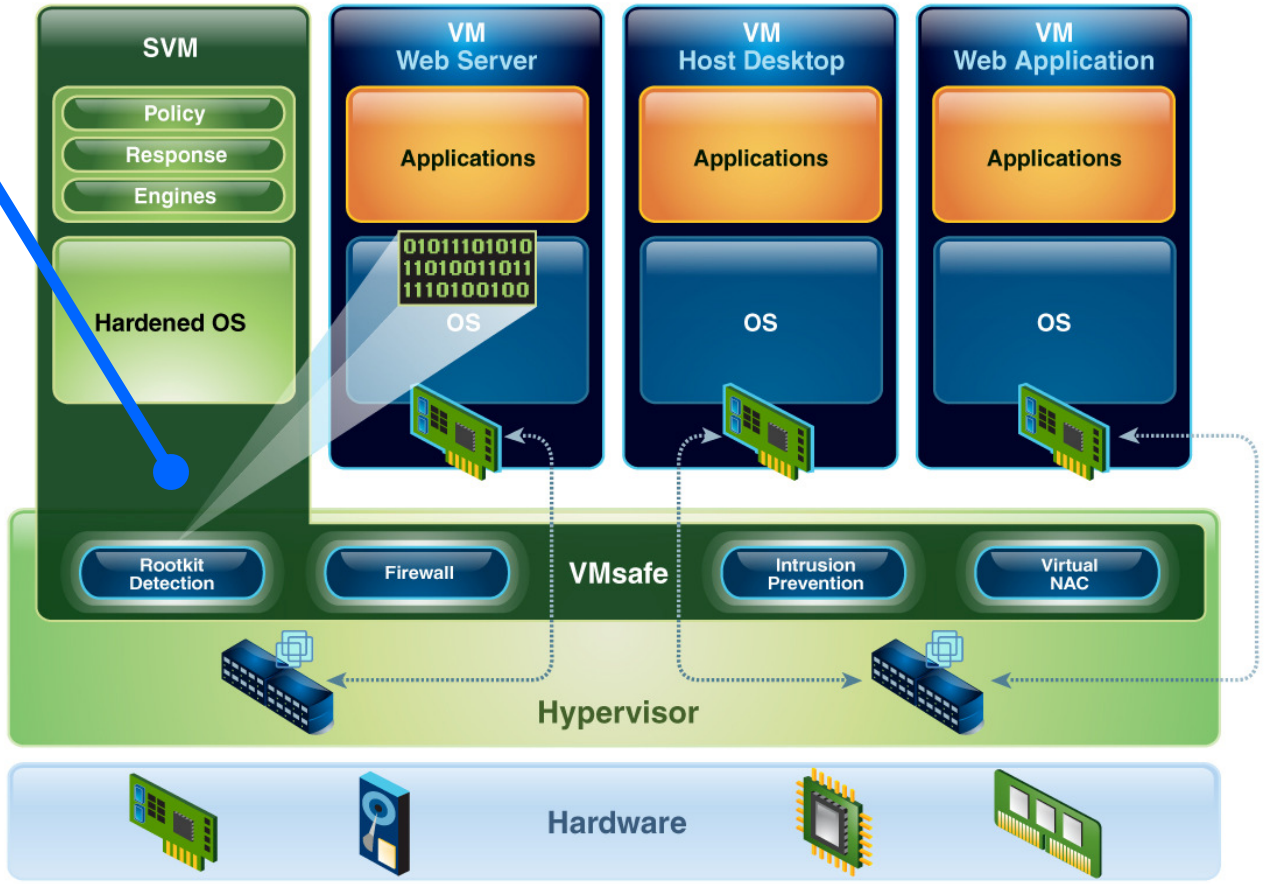
	Remoto	Perimetro			Core				
						NEW	NEW	NEW	
Modelo	GX4004-200	GX4004	GX5008	GX5108	GX5208	GX7412-5	GX7412-10	GX7412	GX7800
Tráfico Inspeccionado	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Segmentos protegidos	2	2	4	4	4	8	8	8	4

IBM Virtual Server Protection for VMware

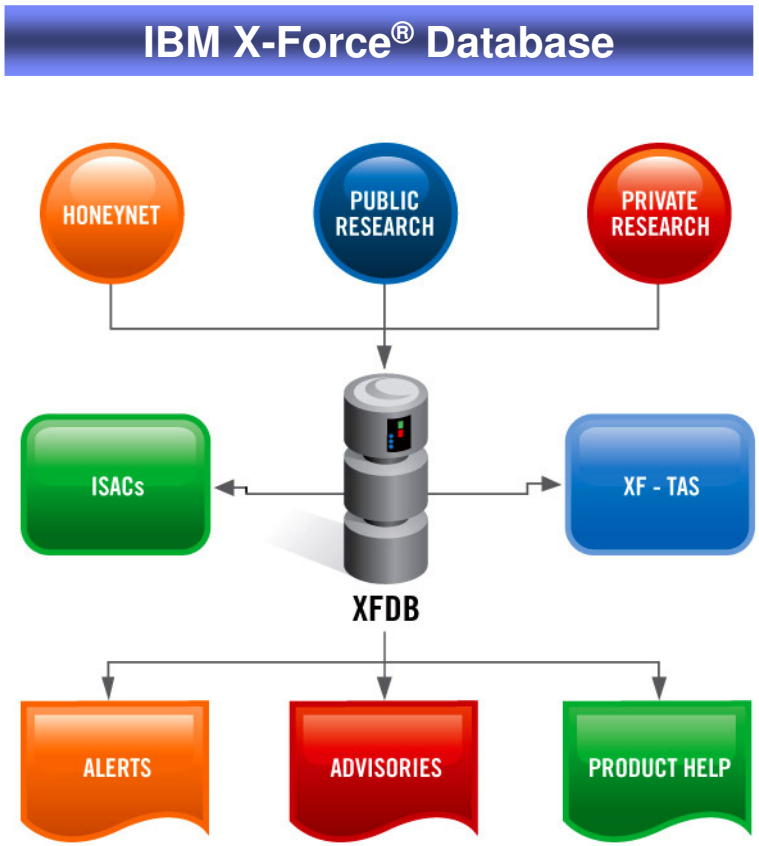
Protección de amenazas Integrales para VMware vSphere 4

Ofrece la más amplia, integrada y profunda protección para ambientes virtualizados con un solo producto

- Firewall
- Integración con VMsafe
- Detección de Rootkit
- Intrusion Detection & Prevention
- Análisis de tráfico entre VMs
- Gestión separada de VMs
- Aplicación de política de red
- Protección integrada con VMotion
- Auto descubrimiento de VMs
- Auditoría de Infraestructura Virtual (Monitoreo de usuarios privilegiados)
- Protección de segmentos virtuales
- Virtual Network-Level Protection
- Virtual NAC
- Gestión Centralizada
- Protección de Web Application
- Virtual Patch



¿Qué es IBM X-Force?



- **¿Qué es lo que hace?**
  - Investiga y evalúa las vulnerabilidades y problemas de seguridad
  - Desarrolla la evaluación y la tecnología de contramedidas para las ofertas de seguridad de IBM
  - Educa al público sobre las nuevas amenazas de Internet
- **¿En qué se diferencia?**
  - Uno de los equipos comerciales de investigación en seguridad más reconocidos en el mundo
  - La tecnología desarrollada por X-Force en promedio protege 341 días antes que existan las amenazas.
- **IBM Xforce Database** se actualiza diariamente por un grupo dedicado de investigación que revisa sobre:
  - **7,600 Proveedores**
  - **17,000 Productos**
  - **40,000 Versiones**
- **IBM X-Force Database** mantiene la más amplia información de vulnerabilidades del mundo, más de 51.000, conteniendo información desde 1990

Como investiga IBM X-Force

- MSS Telemetry Data
  - IBM automatiza la alimentación de más de 8.000 millones de eventos a PAM por día, para asegurar que los **falsos positivos sean lo más cercano a 0**, como sea posible
  - 4,000 Clientes de GTS con más de 20,000 sensores IPS
  - Sitios y clientes de pruebas para nuevos códigos e ideas
  - **Ninguno de nuestros competidores maneja esta cantidad de información**
- La precisión de la seguridad provista por PAM es evaluada cada hora, si se encuentran inconvenientes estos son identificados y corregidos.
- Darknet y Honeynets
  - X-Force opera una red clase B para recibir ataques y detectar tráfico anómalo en Internet.
- X-Force mantiene investigación en la red de manera continua
- Al día de hoy 260 protocolos decodificados, se adicionan un promedio de 3 x mes durante el último año
- .

¿Cuál es el valor de X-Force para mi?

- El motor de los IBM IPS ha detenido los ataques a gran escala de zero-day SQL injection o Cross Site Scripting (XSS)

- De las 48 Vulnerabilidades más importantes del 2010:
  - 35% se encontraban protegidas con **más de un año de anticipación**
  - 54% el mismo día que se dieron a conocer
  - Sólo 11% dentro de los 15 días que se dieron a conocer

  En resumen estuve protegido de un **89% dentro de las primeras 24 horas**

- 14 Vulnerabilidades y exploit reportados en 2011, se encontraban **protegidos desde el 2007**

¿Por que IBM ? Opinión de los analistas

Gartner

- **Liderazgo en Gartner Magic Quadrant**
  - User Provisioning (Nov 2010)
  - Web Access Management (November 2008)
  - Static Application Security Testing (Dic 2010)
  - Enterprise Governance, Risk and Compliance Platforms (Oct 2010)
  - Security Information and Event Management (May 2009)

- **Gartner en Marketscope**
  - Enterprise Single Sign-On - Strong Positive (Sept 2010)
  - Web Access Management - Positive (Nov 2010)
  - Network Intrusion Prevention System Appliances Magic Quadrant

IDC Analyze the Future

- **e Leadership**
  - #1 Identity & Access Management (2009)
  - #1 Identity Management Provider (2007)
  - #1 Security & Vulnerability Management Software Worldwide (2007)
  - #1 Vulnerability Assessment Software Worldwide (2007)
  - #1 Application Vulnerability Assessment Software Worldwide (2007)

FORRESTER®

- **Liderazgo en Forrester Wave**
  - Database Auditing and Real-Time Protection (May 2011)
  - Managed Security Services Wave (Ago 2010)
  - Information Security And Risk Consulting Services (Ago 2010)

SC MAGAZINE AWARDS

- **SC Magazine**
  - Identity Access & Assurance, Best Identity Management Application 2011
  - IBM, Best Security Company, 2010

EMA™

- **ENTERPRISE MANAGEMENT ASSOCIATES**
  - Leadership in Intrusion Prevention (Ene 2010)

¿ Consultas ?

Pulse Comes To You
PCTY2011

Por Un Mundo Más Inteligente

La Gente Lo Quiere

Nosotros Lo Hacemos

IBM

Anexos

- Zero-day SQL injection o Cross Site ScriXSS.
  - Asprox – reportado 12/11/2008 – bloqueado 6/7/2007
  - Lizamoon – reportado 3/29/2011 – bloqueado 6/7/2007
  - SONY (publicado) – reportado May/Jun/2011 – bloqueado 6/7/2007
  - Apple Dev Network – reportado Jul/2011 – bloqueado 6/7/2007

Nueva Vulnerabilidad o Exploit	Fecha Reportada	Protegido desde
Nagios expand cross-site scripting	5/1/2011	6/7/2007
Easy Media Script go parameter XSS	5/26/2011	6/7/2007
N-13 News XSS	5/25/2011	6/7/2007
I GiveTest 2.1.0 SQL Injection	6/21/2011	6/7/2007
RG Board SDQL Injection Published:	6/28/2011	6/7/2007
BlogiT PHP Injection	6/28/2011	6/7/2007
IdevSpot SQL Injection (iSupport)	5/23/2011	6/7/2007
2Point Solutions SQL Injection	6/24/2011	6/7/2007
PHPFusion SQL Injection	1/17/2011	6/7/2007
ToursManager PhP Script Blind SQli	7/2011	6/7/2007
Oracle Database SQL Injection	7/2011	6/7/2007
LuxCal Web Calendar	7/2011	6/7/2007
Apple Web Developer Website SQL	7/2011	6/7/2007
MySQLDriverCS Cross-Param SQLi	6/27/2011	6/7/2007