Software Summit2012

El placer de cautivar y crear nuevos mercados

Haga frente a las amenazas emergentes antes de que impacten su negocio

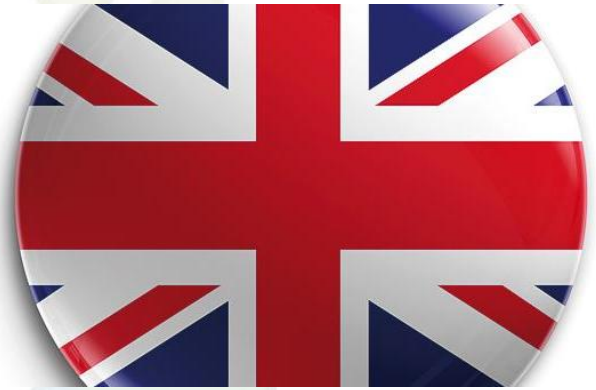
Paul Humberto Rangel Herrera

IBM Security Systems

Technical Professional

IBM

Últimas noticias



Últimas noticias

Anonymous ataca sitios web del gobierno británico en apoyo a Assange

Nota

Europa | Hackers | Julian Assange

Assange, de 41 años de edad, se refugió el pasado 19 de junio en la embajada ecuatoriana en Londres. ARCHIVO

Más información

- Suecia no ve con 'buenos ojos' asilo de Assange
- Asoma el diálogo entre Quito y Londres por el caso Assange
- México pide a Ecuador y Reino Unido retomar diálogo

- Logra inhabilitar temporalmente sitios del Ministerio de Justicia y del primer ministro

El fundador de WikiLeaks, Julian Assange, está refugiado en la embajada de Ecuador en Londres para evitar su extradición a Suecia

LONDRES, **GRAN BRETAÑA (21/AGO/2012).**- El grupo Anonymous atacó sitios web del gobierno británico, en represalia por la forma en que Reino Unido trata el caso del fundador de WikiLeaks, Julian Assange, refugiado en la embajada de Ecuador en Londres para evitar su extradición a Suecia.

Después de que el gobierno británico reiteró la víspera su decisión de extraditar al periodista australiano a Suecia, el grupo de piratas informáticos Anonymous atacó la víspera la web gubernamental, como una acción de apoyo al fundador de WikiLeaks, reportó la cadena brtánica BBC.

Anonymous lanzó la "Operación Liberar a Assange" (#OpFreeAssange), con la que consiguió inhabilitar temporalmente las páginas del Ministerio

de Justicia y del primer ministro, David Cameron

¿Cuál es el sistema más vulnerable?

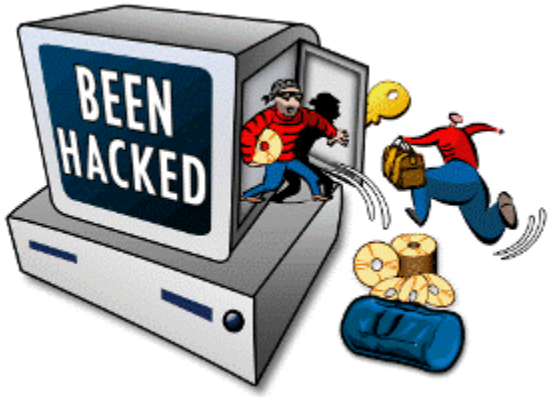
Microsoft Windows

Linux (RedHat, SuSE, CentOS, Ubuntu)

Adobe Acrobat

Apple OS

Piense en el de su preferencia…



¿Cuál es el sistema más vulnerable?

¿Y el factor humano?

Detienen a empleado de IMSS que duplicaba huellas digitales para “checar” asistencias

La aprehensión ocurrió cuando el servidor público presentaba en los lectores biométricos del nosocomio las réplicas de las huellas dactilares, elaboradas con látex, para “checar” la asistencia de sus compañeros ausentes.

Los lectores biométricos fueron instalados en el Hospital General Regional en sustitución del sistema de tarjetas de asistencia, a causa de que se detectó que varios trabajadores adscritos a este centro sanitario “checaban” las tarjetas de otros empleados faltistas, que en ocasiones debían cubrir jornadas de hasta 24 horas.

El sistema 100% seguro

Ayuda!!!Como puedo tener mi **Computadora 100% Segura**??? - Yah...
mx.answers.yahoo.com › ... › Computadoras e Internet › Seguridad
10 respuestas - 21 Jun. 2008
Mejor respuesta: DE TRE MANERAS POSIBLES A SABER 1.- UN BUEN ANTI VIRUS COMO AVAST 4.8. CON ANTI ROCKIT, ANTISPYWARE, EXCELENTE ...

¿que programa para bajar música a mi laptop es **seguro**? - 10 Feb. 2012
¿Qué medidas son recomendables para que mi **computadora** sea ... - 31 Ago. 2011
Más resultados de mx.answers.yahoo.com »

Tu PC **100% segura**-Recopilación de Software anti - Taringa
www.taringa.net/registro-login?private=post...**100**...**segura**...
No se dispone de una descripción de este resultado debido a robots.txt. Más información.

How To **Secure** A **Computer** | **Secure** A **PC** Online |
fasterpc.info/.../how-to-**secure**-a-**computer**-**secur**... - Traducir esta página
9 Jan 2011 – Do you need to know how to **secure** a **computer**? Here we'll cover 10 effective ways to **secure** a **computer** **100**% while online connected to the ...

100% Secure Server - Free Hosts R Us
freehosts.r-us.biz/h**secure**.htm - Traducir esta página
100% Secure? The final part of the ordering process (when entering your cards details) will take place via our **100% secure server** (operated by WorldPay).

¿Entonces qué hacemos?

Establecimiento de controles de seguridad:

- Nivel físico (candados, gafetes, biométricos, etc.)
- Nivel lógico (identidades, accesos, tráfico legítimo, etc.)

Estrategias de protección:

- Evitación (equipos aislados)
- **Prevención**
- Detección
- Recuperación

¿Sigue siendo la seguridad perimetral una realidad?

Antes:

- Protección en el perímetro:

  Switches, Routers, Firewalls

- Usuarios en la oficina
- Redes cableadas

Ahora:

- Protección en el perímetro:

  Switches, Routers, Firewalls, IDS, IPS,

  monitores de red, VPN, entre otros

- Usuarios fuera de la oficina
- Redes cableadas, wireless, dispositivos móbiles

Hablando de Seguridad

- **Centros de operaciones de seguridad**
- **Centros de investigación de seguridad**
- **Centros de desarrollo de soluciones de seguridad**
- **Instituto de sucursales de seguridad avanzada**

Investigación de IBM

IBM Institute for Advanced Security

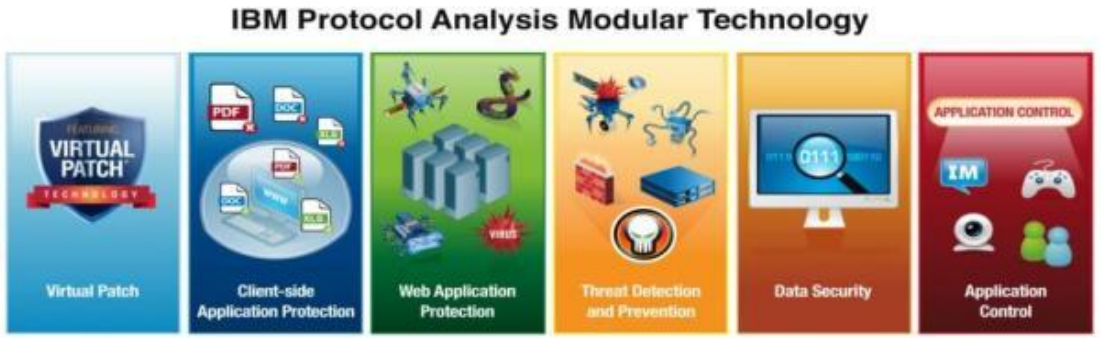
Enabling cybersecurity innovation and collaboration

10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
46K documented vulnerabilities
Millions of unique malware samples

X FORCE

- Más de 20.000 dispositivos en contrato
- Más de 3.700 clientes de MSS en el mundo
- Más de 9.000 millones administrados por día
- Más de 1.000 patentes de seguridad
- 133 países monitoreados (MSS)

Protocol Analysis Module

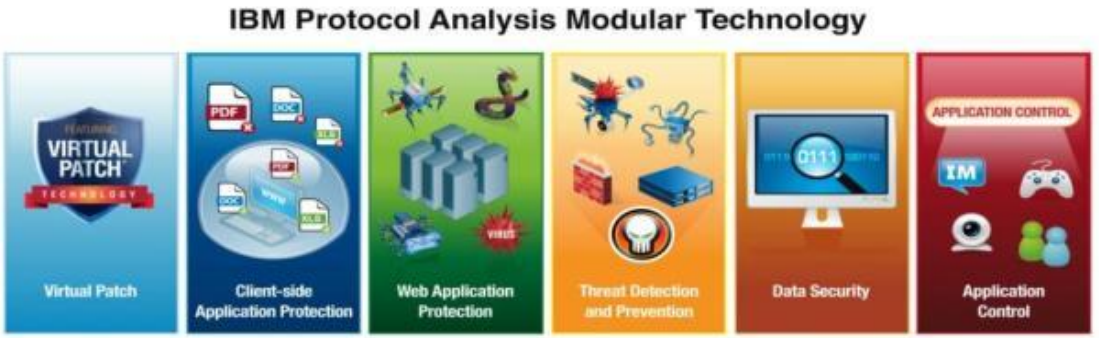


Virtual Patch

Qué hace:
Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada.

Por qué es importante:
A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante

Protocol Analysis Module



Virtual Patch

Qué hace:
Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada.

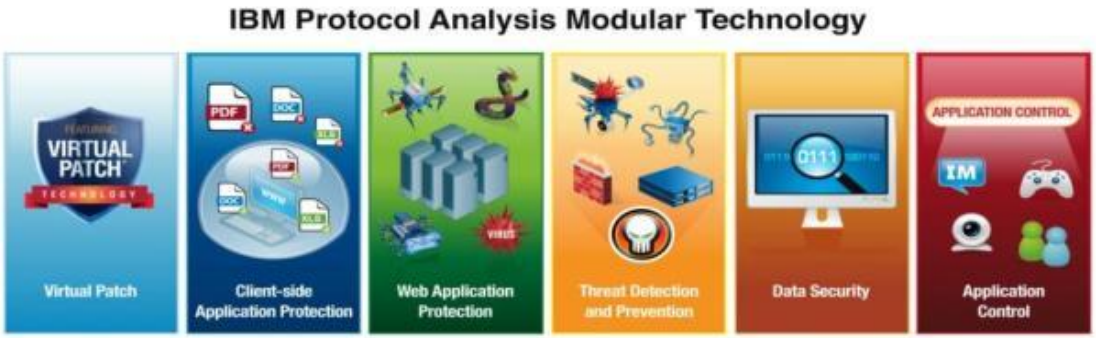
Por qué es importante:
A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante

Client-side Application Protection

Qué hace:
Protégé a los usuarios finales de archivos malicosos dentro de Microsoft Office, Adobe PDF, archivos multimedias y Web browsers.

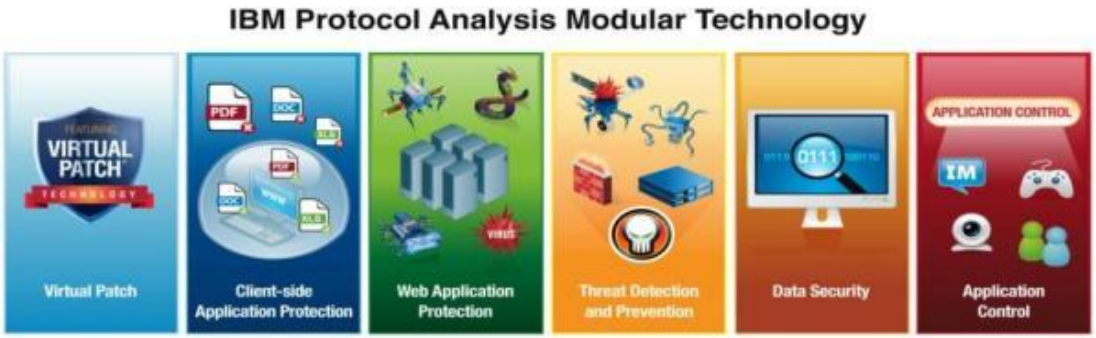
Por qué es importante:
Durante el 2011 el 49% de las vulnerabilidades descubiertas fueron sobre aplicaciones Web.

Protocol Analysis Module



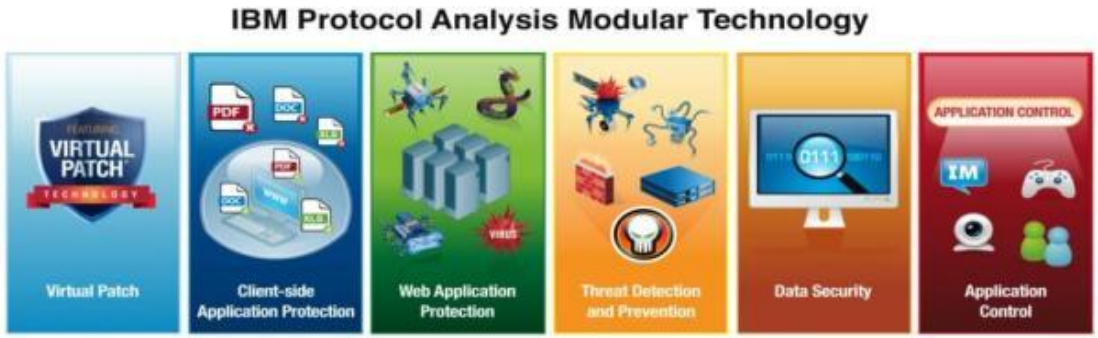
Virtual Patch	Client-side Application Protection	Web Application Protection
Qué hace: Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada. **Por qué es importante:** A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante	**Qué hace:** Protégé a los usuarios finales de archivos malicosos dentro de Microsoft Office, Adobe PDF, archivos multimedias y Web browsers. **Por qué es importante:** Durante el 2011 el 49% de las vulnerabilidades descubiertas fueron sobre aplicaciones Web.	**Qué hace:** Protégé las aplicaciones Web contra ataques del tipo SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery). **Por qué es importante:** Protección de las aplicaciones Web mientras se busca la remediación

Protocol Analysis Module



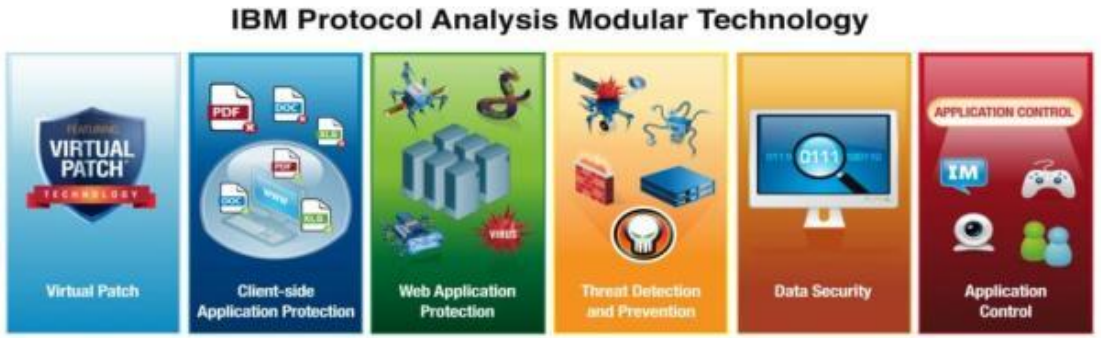
Virtual Patch	Client-side Application Protection	Web Application Protection	Threat Detection and Prevention
Qué hace: Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada. **Por qué es importante:** A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante	**Qué hace:** Protégé a los usuarios finales de archivos malicosos dentro de Microsoft Office, Adobe PDF, archivos multimedias y Web browsers. **Por qué es importante:** Durante el 2011 el 49% de las vulnerabilidades descubiertas fueron sobre aplicaciones Web.	**Qué hace:** Protégé las aplicaciones Web contra ataques del tipo SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery). **Por qué es importante:** Protección de las aplicaciones Web mientras se busca la remediación	**Qué hace:** Detecta y previene tipos de amenazas en grupos en vez de algún exploit en particular (Shellcode Heuristics) **Por qué es importante:** Elimina la necesidad de constantes actualizaciones, protegiendo contra ataques de día cero

Protocol Analysis Module



Virtual Patch	Client-side Application Protection	Web Application Protection	Threat Detection and Prevention	Data Security
Qué hace: Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada. **Por qué es importante:** A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante	**Qué hace:** Protégé a los usuarios finales de archivos malicosos dentro de Microsoft Office, Adobe PDF, archivos multimedias y Web browsers. **Por qué es importante:** Durante el 2011 el 49% de las vulnerabilidades descubiertas fueron sobre aplicaciones Web.	**Qué hace:** Protégé las aplicaciones Web contra ataques del tipo SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery). **Por qué es importante:** Protección de las aplicaciones Web mientras se busca la remediación	**Qué hace:** Detecta y previene tipos de amenazas en grupos en vez de algún exploit en particular (Shellcode Heuristics) **Por qué es importante:** Elimina la necesidad de constantes actualizaciones, protegiendo contra ataques de día cero	**Qué hace:** Monitorea e identifica Información Identificable Personal (PII) y otro tipo de información confidencial. **Por qué es importante:** Es un complemento a data security, como soluciones de DLP

Protocol Analysis Module



Virtual Patch	Client-side Application Protection	Web Application Protection	Threat Detection and Prevention	Data Security	Application Control
Qué hace: Protege las vulnerabilidades que no tienen parche del fabricante, permitiendo una administración de parchado adecuada. **Por qué es importante:** A finales de 2011, 36% de las vulnerabilidades no tenían un parche liberado por parte del fabricante	**Qué hace:** Protégé a los usuarios finales de archivos malicosos dentro de Microsoft Office, Adobe PDF, archivos multimedias y Web browsers. **Por qué es importante:** Durante el 2011 el 49% de las vulnerabilidades descubiertas fueron sobre aplicaciones Web.	**Qué hace:** Protégé las aplicaciones Web contra ataques del tipo SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery). **Por qué es importante:** Protección de las aplicaciones Web mientras se busca la remediación	**Qué hace:** Detecta y previene tipos de amenazas en grupos en vez de algún exploit en particular (Shellcode Heuristics) **Por qué es importante:** Elimina la necesidad de constantes actualizaciones, protegiendo contra ataques de día cero	**Qué hace:** Monitorea e identifica Información Identificable Personal (PII) y otro tipo de información confidencial. **Por qué es importante:** Es un complemento a data security, como soluciones de DLP	**Qué hace:** Administra el control a la red de aplicaciones no deseadas, tales como ActiveX fingerprinting, P2P, Mensajería instantánea y tuneling. **Por qué es importante:** Cumplimiento de políticas de uso de la red de la compañía

Data Security

FIRMAS
Número de TC
Nombres
Fecha
Cantidades ($)
Dirección e-mail
Número de seguridad social
Números de teléfono
Código Postal
8 + Definidos por el usuario

PROTOCOLOS
AOL IM
Microsoft Messenger
Yahoo Messenger
IRC
HTTP
FTP
SMB
SMTP
IMAP
POP3

CONTENIDO
Microsoft Office
*Microsoft Messenger
PDF
Texto
RFT
XML
HTML
GZIP

IBM Apuesta a la Seguridad

April, 2000 – Network ICE releases BlackICE Guard, first commercial IPS

June, 2001 – Network ICE acquired by Internet Security Systems

October, 2003 – BlackICE Guard and RealSecure Network Sensor unified in first ISS IPS appliances. Proventia G100 and G200 (maximum throughput **200Mb/sec**)

1st half 2004 – ISS releases G1000 and G1200 appliances (maximum throughput **1200Mb/sec**)

February, 2005 – ISS releases G2000 and revamps policy editor (maximum throughput **2000Mb/sec**

1st half 2006 – ISS releases GX appliance line (1st hardware refresh). Shellcode Heuristics engine added to PAM.

October 2006 – ISS acquired by IBM

May 2007 – IBM releases GX6116 (maximum throughput **6Gb/sec**, later increased to **8Gb/sec**)

2nd half, 2007 – Injection Logic engine added to PAM

December, 2007 – Content Analysis Engine added to PAM

2008 – Web Protection Content begins being added to PAM

April, 2009 – IBM releases Proventia Network Security Controller, providing connectivity for 10GbE networks

Q1, 2010 – IBM releases GX-version 2 appliances (2nd hardware refresh) 2X-4X performance increase at same price points

Q2, 2010 – IBM firmware 4.1: New LMI and web application protection wizard, IPv6, Rational AppScan integration

Q4, 2010 – IBM firmware 4.3: SNMPv3

March, 2011 – IBM releases GX7800 (secured throughput **23Gb/sec**) with 64-bit PAM 2.0 and native 10GbE interfaces

IBM certifies Netronome SSL Inspector “Ready for Tivoli”

Q3, 2011, IBM to release GX7412s (**5Gb/sec, 10Gb/sec and 23Gb/sec**) with 64-bit PAM 2.0

IBM Security
Network Intrusion Prevention System

IBM Security Network IPS Models									
	Remote	Perimeter			Core				
Model	GX4004-200	GX4004	GX5008	GX5108	GX5208	GX7412-5	GX7412-10	GX7412	GX7800
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

Últimas novedades

GX7800

RSA Conference 2011, se realizó el anuncio del equipo **GX7800**

- 20 Gbps+ de througput
- Interfaces nativas de 10GbE
- Respaldo del equipo de Desarrollo e Investigación (X-Force Team).

Nuevas características

Soporte para firmas basadas en Snort

- Combinación de Protocol Analysis Module (PAM) con la facilidad de crear e importar reglas SNORT.

- Provee protección más allá de los IPS tradicionales tales como ataques a los navegadores, robo de información, y aplicaciones Web maliciosas diseñadas para evadir la seguridad.

Últimas novedades

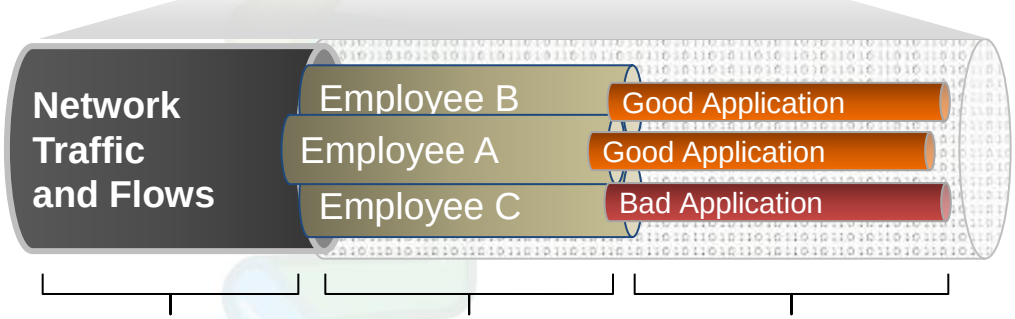
XGS 5000

	NEW WITH XGS	NEW WITH XGS
SEGURIDAD PROBADA	**VISIBILIDAD**	**CONTROL**
Extensible, Protección del PAM, proveída por el X-Force Team	**Comprender Quién, Qué y Cuándo sobre la actividad en la red**	**Uso apropidado de la red**

IBM Security Network Protection XGS 5000
contruido en la seguridad ya probada de IBM además de agregar la visibilidad y el control para cumplir los requerimientos de seguridad y del negocio

Últimas novedades

- **Descubre inmediatamente** qué aplicaciones están siendo utilizadas.
- **Identifica mal uso** sobre aplicación, sitio Web, grupos y usuarios.
- **Comprender** el uso de ancho de banda
- Integración con **QRadar** para el análisis de tráfico anómalo.



Network Flow Data provee visibilidad del tráfico anómalo mediante la integración con QRadar

Complete Identity Awareness asocia los grupos y usuarios con la actividad de la red, para verificar el uso de la misma.

Application Awareness clasifica el tráfico de la red independientemente de la dirección, el puerto, el protocolo, la aplicación, y el evento de seguridad

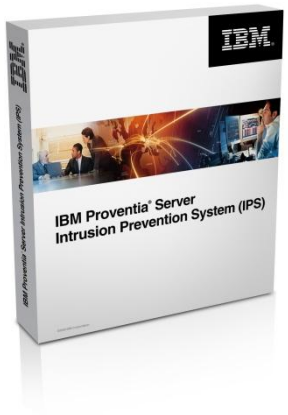
Increase Security ● Reduce Costs ● Enable Innovation

IBM Security
Network Active Bypass

- **10 GbE Active Network Bypass (8 puertos)**
- **Soporte de hasta 4 segmentos de red independientes**
- **Puertos de red TAP**
- **Fuentes de poder redundantes**
- **Disminución en el tiempo de respuesta**
- **Envío de traps SNMP**

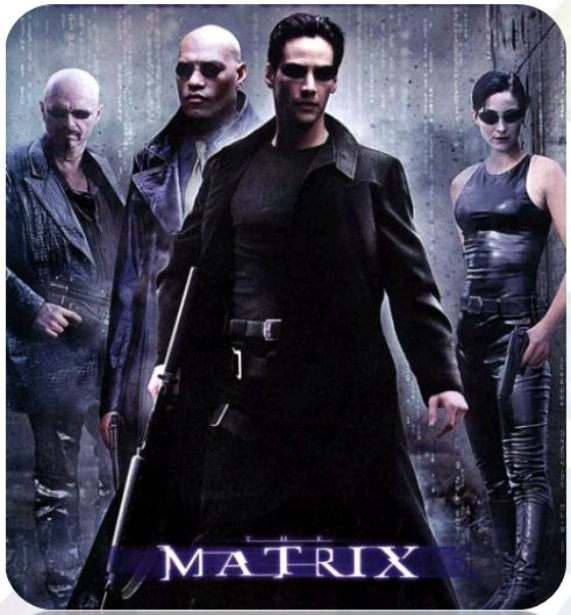
IBM Security
Host Intrusion Prevention System

- **Tecnología de Prevención *(respaldo por X-Force)***
  - Firewall
  - Intrusion Prevention & Detection
  - Buffer Overflow Protection
  - Application Black & White Listing
  - SSL Inspection

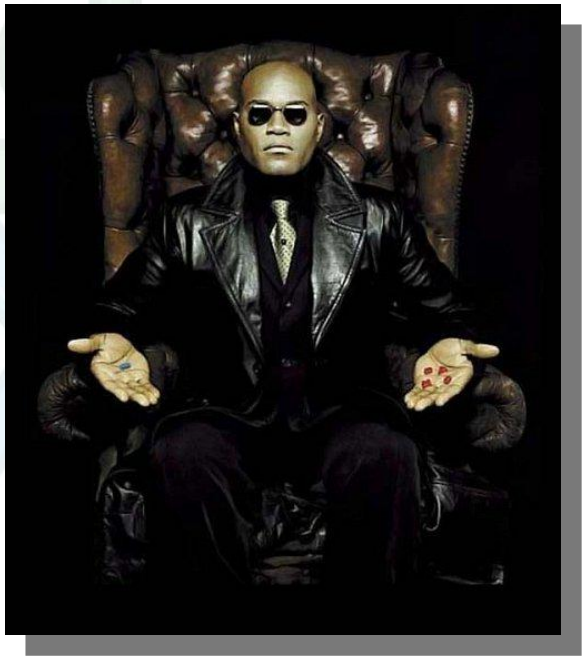


- **Tecnología de Cumplimiento:**
  - Registro Quién, Qué, Cuándo y Dónde de la actividad de los usuarios
  - File Integrity Monitoring (FIM)
  - OS Auditing
  - Registry Integrity Monitoring
  - Anti-Virus Compliance
  - Third Party Log Monitoring

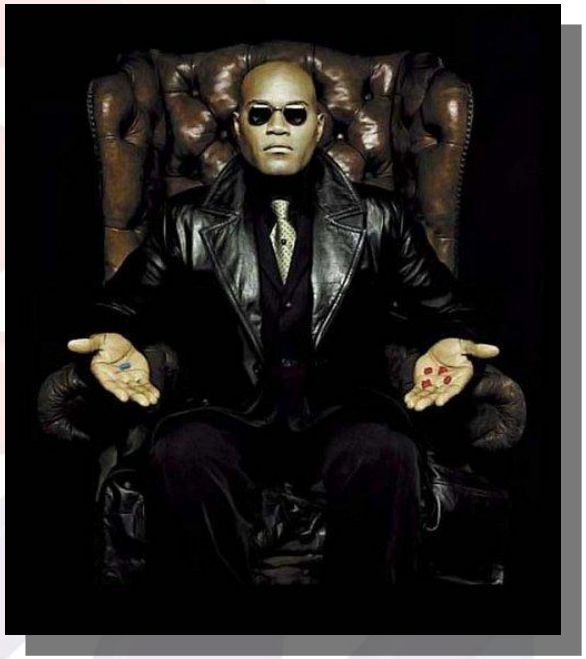
IBM Security
Virtual Server Protection for VMware

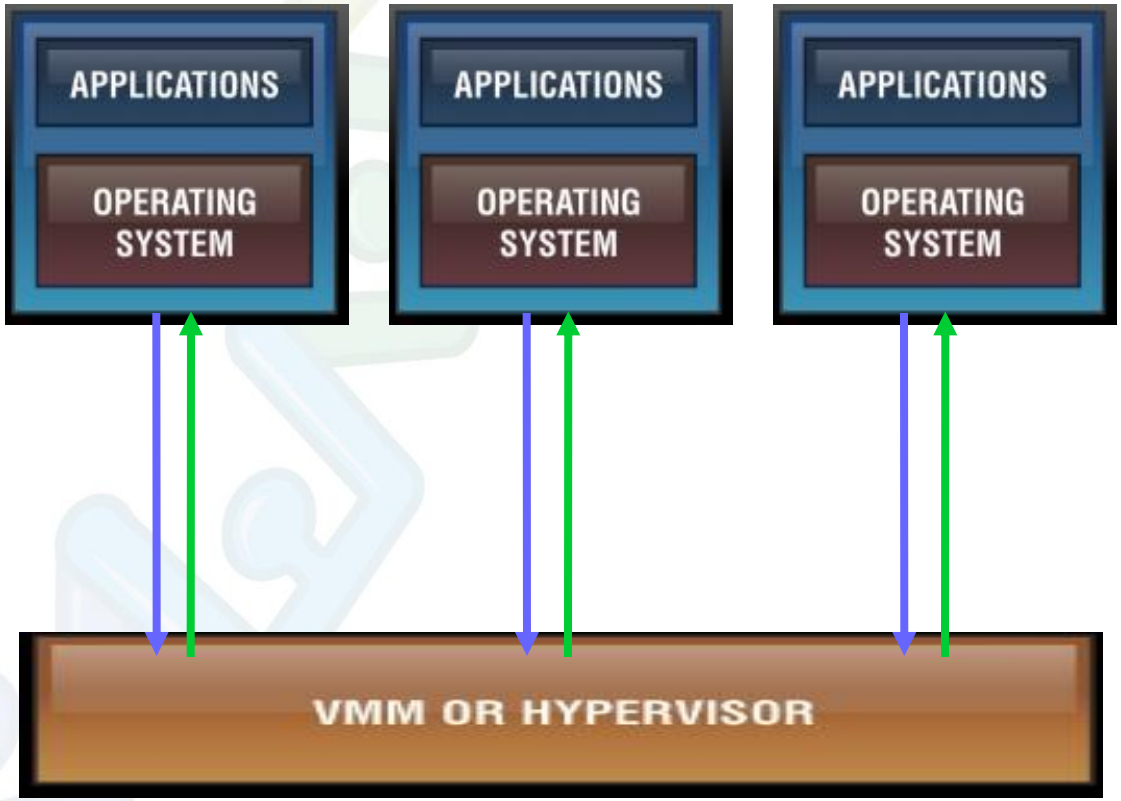


¿Blue Pill o Red Pill?

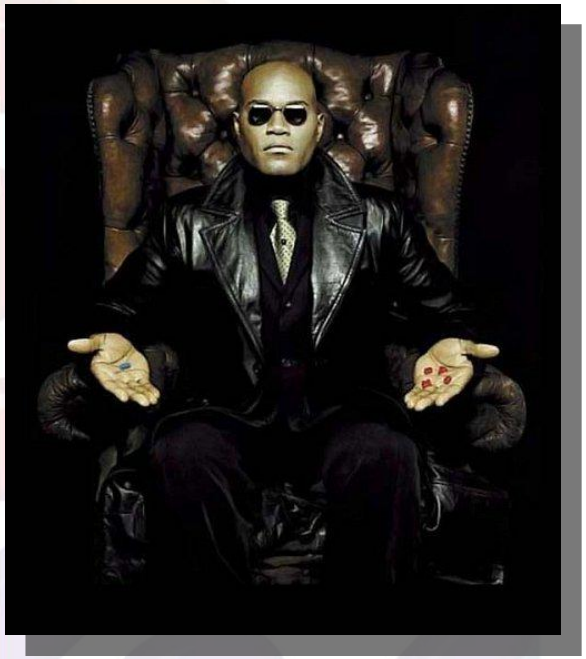


IBM Security
Virtual Server Protection for VMware

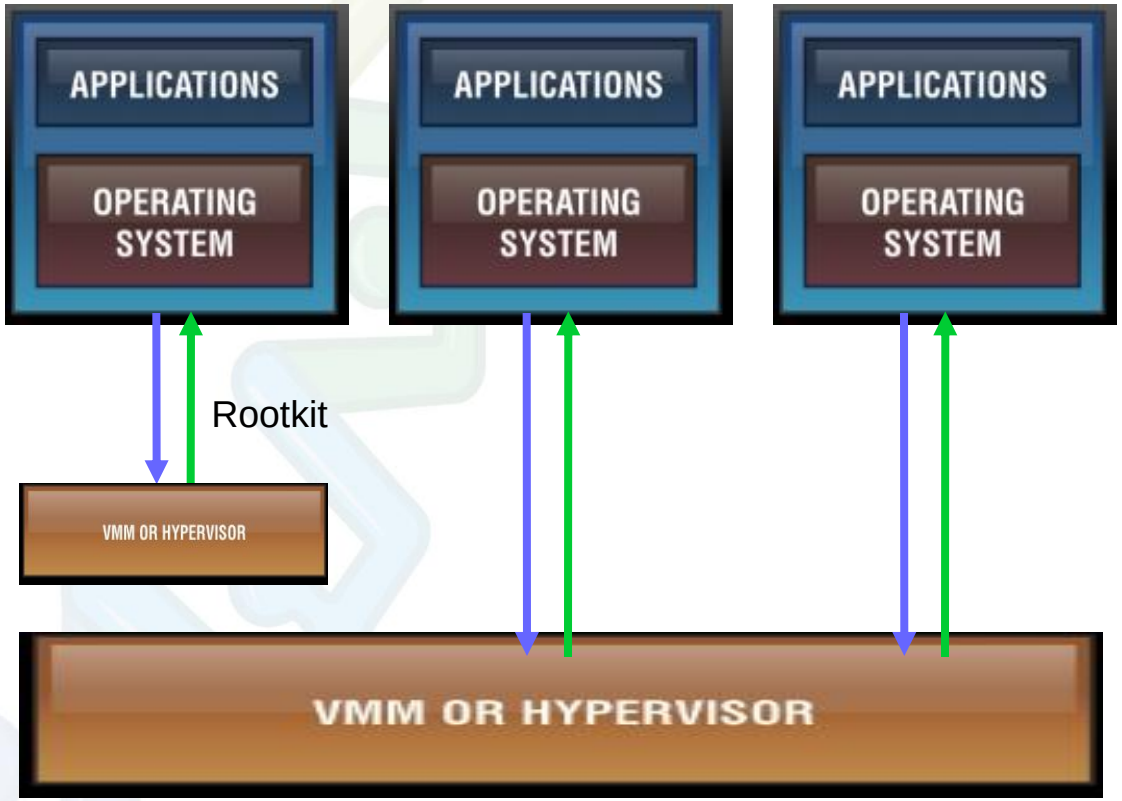




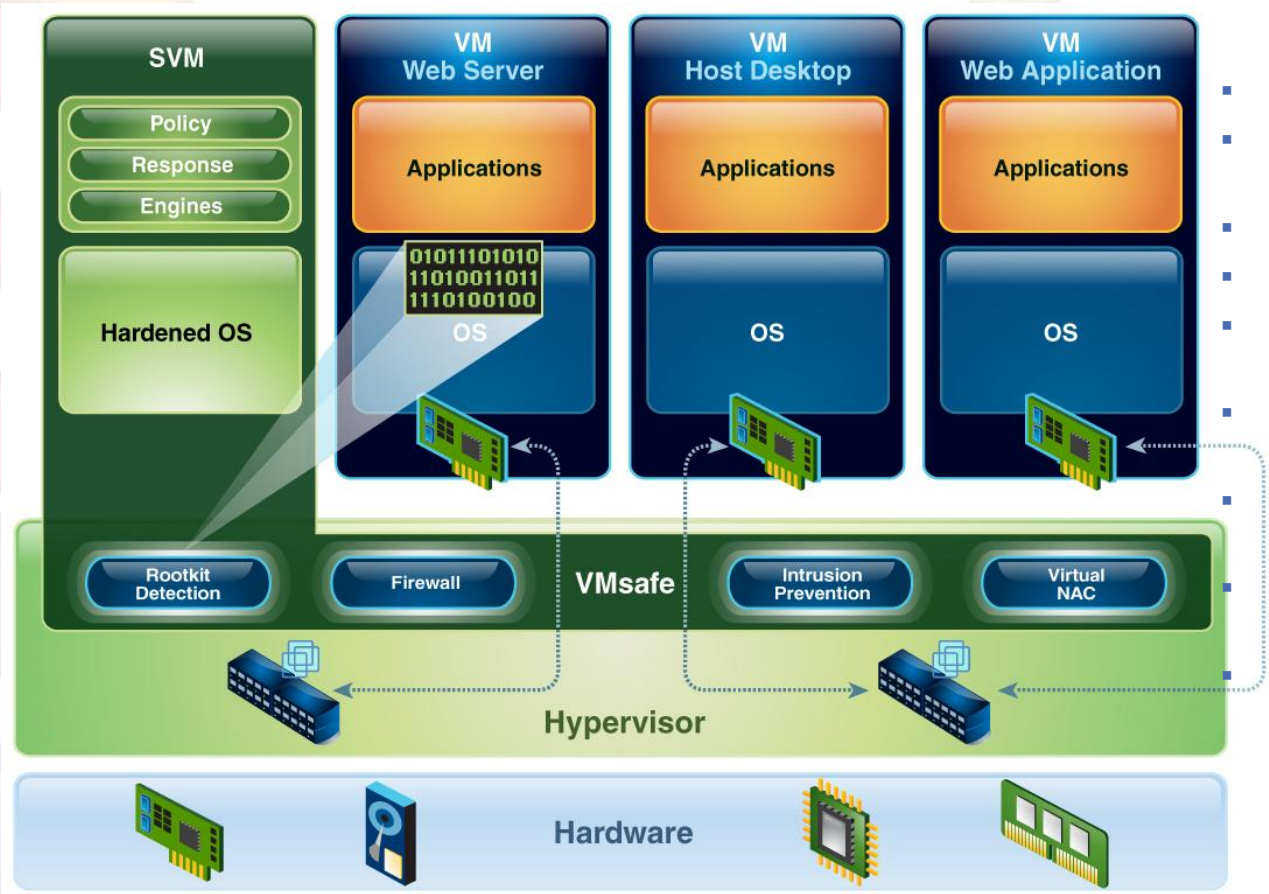
IBM Security
Virtual Server Protection for VMware



Blue Pill



IBM Security
Virtual Server Protection for VMware



- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network Access Control

IBM Security SiteProtector System

Asset Management
- Discovery
- Clarification
- Inventory
- Ownership

Broad Agent Support
- All ISS agents and appliances

Command and Control
- Policy Management
- Product, Content Updates
- Content Updates
- Central, Agent Responses

Track Improvements to Operational Security

Enforce Segregation of Duties
- Default, Custom Roles
- Granular Permissions
- Multiple Consoles

SiteProtector™

Reporting
- Asset, Audit, Attack Activity, Management, Permissions, and Ticketing Categories and more

Workflow and Ticketing
- Track Vulnerability Remediation
- Facilitate & Document Incident Response

Event Analysis
- Real-time Monitoring
- Convert Data into Actionable Steps

IBM Security
Six in a box

Proteja sistemas y datos críticos de su negocio

Seguridad y protección

$ 8,054.9 USD

Configuración

#	Brand	Tipo / Modelo	Descripcion	Cantidad	Total
1	SW	SPSW-STD-1-P	SiteProtector Standard SW Package - management for IBM Security Protection	1	$0.00
2	SW	SPSW-STD-1-P-M	SiteProtector Software Maintenance (36 Months)	1	$0.00
3	SW	D0JWTLL	IBM TIVOLI SECURITY SERVER PROTECTION FOR WINDOWS INSTALL LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTHS	1	$0.00
4	SW	E0C9CLL	IBM TIVOLI SECURITY SERVER PROTECTION FOR WINDOWS INSTALL ANNUAL SW SUBSCRIPTION & SUPPORT RENEWAL	2	$0.00
4	xSeries	258262U	X3100m4, xeon E3-1220 3.10 GHz 4C 80W	1	$0.00
5	xSeries	39M4514	500GB 7200 rpm 3.5" Simple-Swap SATA II	1	$0.00
6	xSeries	94Y6161	IBM Pref. Pro Keyboard USB-LA Spanish 171 RoHS	1	$0.00
7	xSeries	40K9200	IBM 2 Button Optical Wwheel Mouse-Black-USB	1	$0.00
8	xSeries	44T1570	2GB (1x2GB Single Rankx8) PC3-10600CL9 CC DDR3 1333MHz LP UDIMM	3	$0.00
9	xSeries	39M4514	IBM 500GB 3.5in 7.2K SS SATA HDD	1	$0.00
			Precio Cliente		$8,054.90

Financiamiento 36 Pagos fijos de 243.07 USD mensuales*

IBM Security

IBM Security Network Intrusion Prevention System

IBM Security Server Protection for Windows

IBM Proventia Intrusion Prevention System for Linux

IBM Security Virtual Server Protection for VMware

IBM Security SiteProtector System

Six-in-a-box

Software Summit2012