IBM Global Services

ISS IBM Soluciones de Seguridad Perimetral y DLP

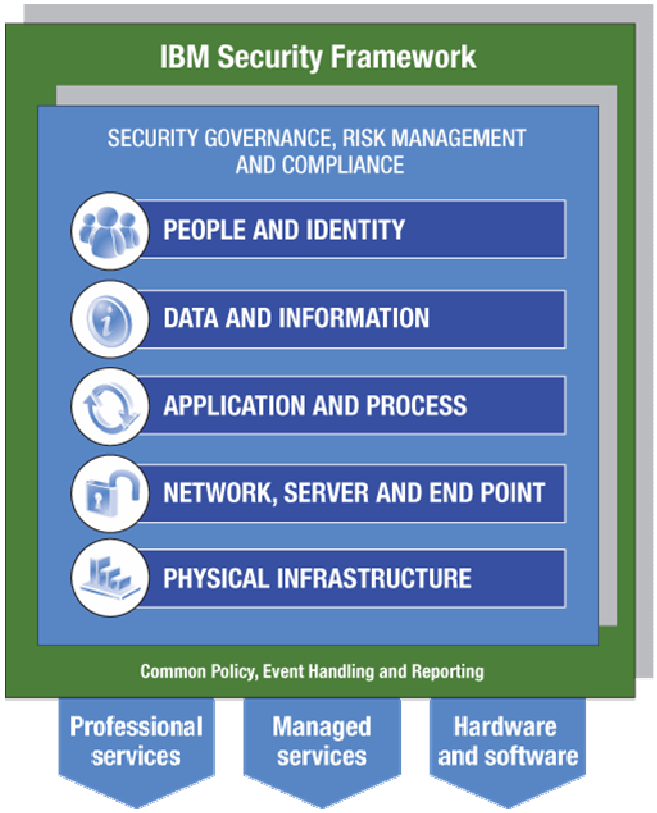
Raúl Pérez García

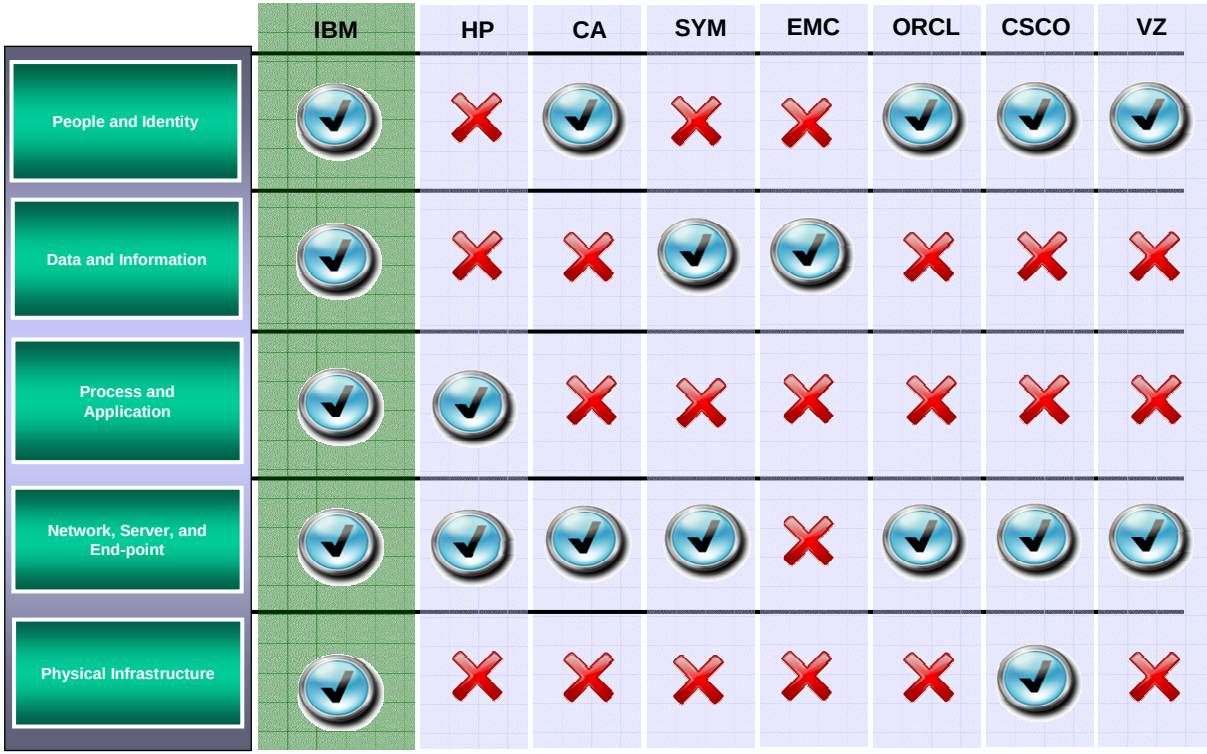
Ahead of the Threat

IBM Internet Security Systems

Ahead of the threat.™

Por que IBM ?

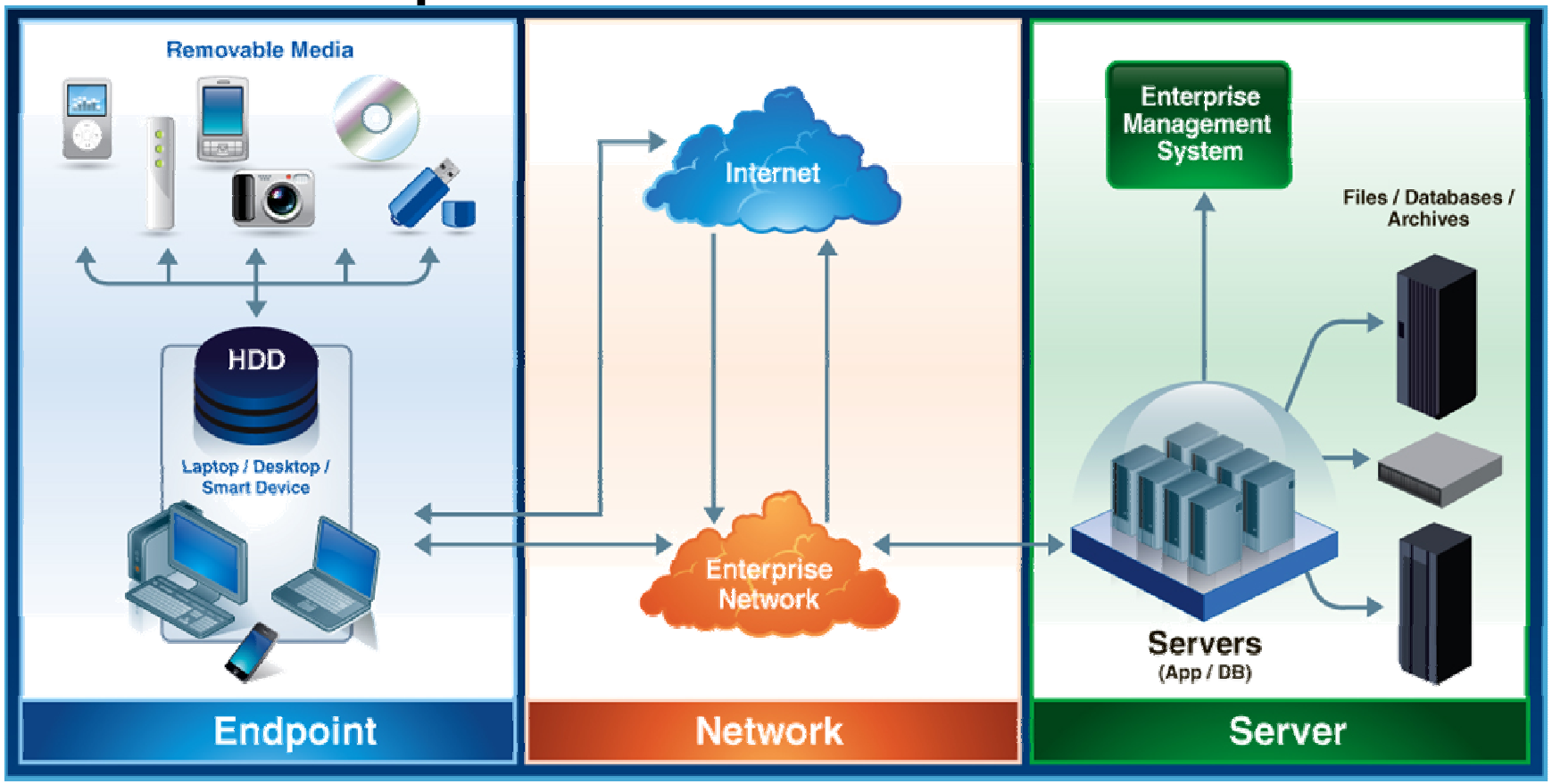




IBM es el único vendedor de seguridad en el mercado que cubre end-to-end de todos los controles de seguridad

Protección de Datos e Infraestructura

- **3 niveles de protección**



Prevención de fugas de información

Seguridad de los datos en tránsito

Protección del CPD

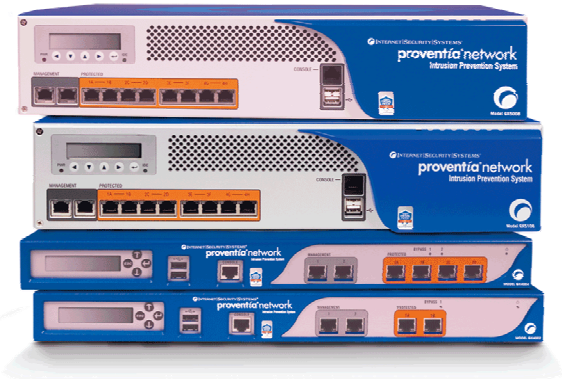
Agenda

Protección del perimetro

Proventia® Network IPS

Proventia® Network IPS **Attack Blocking**

- Que hace…
  - Bloquea múltiples tipos de ataque, mientras que el tráfico legítimo pasa intacto.
- Como funciona…
  - Identifica y analiza más de 198 protocolos y formatos de datos
  - Bloquea ataques con más de 3000 algoritmos de seguridad



- Como ayuda…
  - Recupera ancho de banda y previene de costosos problemas de seguridad
- Por que ISS ..
  - Único vendedor del mercado en recibir constantemente los mejores resultados en efectividad de seguridad

La diferencia...
Investigación = Ahead of the Threat!

- Que hace…
  - El cliente dispone de un buffer de tiempo para instalar parches cuando una nueva vulnerabilidad es descubierta.
- Como funciona …
  - Virtual Patch protege de la vulnerabilidad en vez del xploit
  - El grupo de investigación X-Force detecta entre el 20 y el 50 % de agujeros de seguridad
- Previene de los ataques Zero-Day

La diferenc
Investigaci

ISS Coverage

Product	Content Version
Proventia Network IDS Proventia Network IPS Proventia Network MFS Proventia Server (Linux) RealSecure Network RealSecure Server Sensor	28.160 29.031
Proventia Desktop Proventia Server IPS (Windows)	2300 2376

Propagation Techniques	ISS Protection	Available
remote exploit	MSRPC_Svcsvc_Re	Aug 8, 2006*
	MSRPC_Pipe_SAMR Windows_Access_Error	
remote exploits (Conficker C)	SMB_System32_FileWritten TCP_Service_Sweep UDP_Service_Sweep	base product
Network scan	ConfickerWorm	Apr 2, 2009

* For additional information related to monitoring and tuning these signatures, contact customer support and ask for KBA 5394.

Highlights:

- Researchers at IBM's Internet Security Systems say they found a way to decode the encryption that masks the data shared by peer-to-peer communications software planted on all systems infected by Conficker.C. As a result, ISS has been able to begin charting the location of infected systems across the globe. - ***Washington Post***
- Separately, I.B.M. said that Mark Yason, a company researcher, had decoded Conficker's internal communication protocol. The company said that will make it easier for security teams to detect and interrupt the program's activities. -- ***New York Times***
- Stewart said X-Force's approach was "completely passive" and didn't require running a scanner. It was not, however, released to the public, but instead was integrated within the IBM Internet Security System's intrusion-prevention appliances.-- ***Computerworld***
- An IBM spokesperson declared in an interview with Forbes Monday that its security team had found a solution the week before and already filtered the bug's latest version in its security products. - ***Forbes***
- IBM identified 1156 instances of the infection in New Zealand as of January 29. Mr Martin suspects this number will have dropped. "A lot of companies will have seriously copped it and will have paid some heed to protecting their systems." - ***The Dominion Post***
- Last Thursday, Big Blue began adjusting intrusion-detection appliances it has in place inside 3,800 corporations in 170 countries. These are subscribers to its Managed Security Services. IBM began to scan for Conficker P2P chatter, and found only a miniscule number of infected PCs inside its customers' networks. -- ***The Last Watchdog.com***
- "[Conficker] really challenges the comprehensive network management practices of an organization," said Tom Cross, manager of X-Force research. "Extremely well-managed networks have not been affected, but if your IT security is deficient in any one of several different domains—inventory management, windows update, intrusion prevention, anti-virus, managed file sharing, strong password policies—you are likely to have problems with Conficker. ".. Cross added, "We are seeing a large number of infections in regions that have seen significant new infrastructure development in the past few years but may not have IT management practices which are as mature, across the board, as they are in the West." -- ***eWeek***

IBM ISS Virtual Patch prote

Security Content – Application Protection **WEB 2.0**

- **Industry Leading NIPS with Targeted Web Application Firewall Protection features (WATCHFIRE) :**
  - SQL (Structured Query Language) Injection
  - LDAP (Lightweight Directory Access Protocol) injection
  - XSS (Cross-site scripting)
  - HTTP (Hypertext Transfer Protocol) response splitting
  - JSON (JavaScript Object Notation) hijacking
  - PHP (Hypertext Preprocessor) file-includes
  - CSRF (Cross-site request forgery)

- **Expanding PCI-DSS Coverage to include:**
  - Payment Card Industry (PCI) Requirement 6.6 which went into effect on June 30, 2008.

  6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

  - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes **(Rational Appscan & PSS)**
  - Inspecting the contents of the application layer of an IP packet, as well as the contents of any other layer that could be used to attack a web application **(PSL & Server Sensor or GX & MX + Websphere Datapower)**

- **Multi-Product Portfolio Impact with the Protocol Analysis Module (PAM)**:
  - The IBM Protocol Analysis Module (PAM) forms the core of network intrusion detection and protection in current IBM Proventia products. **It identifies and analyzes 198 network protocols and data file formats**. As it parses the protocols and monitors the traffic, it employs a variety of techniques to report any of **over 2800** interesting events as they occur.

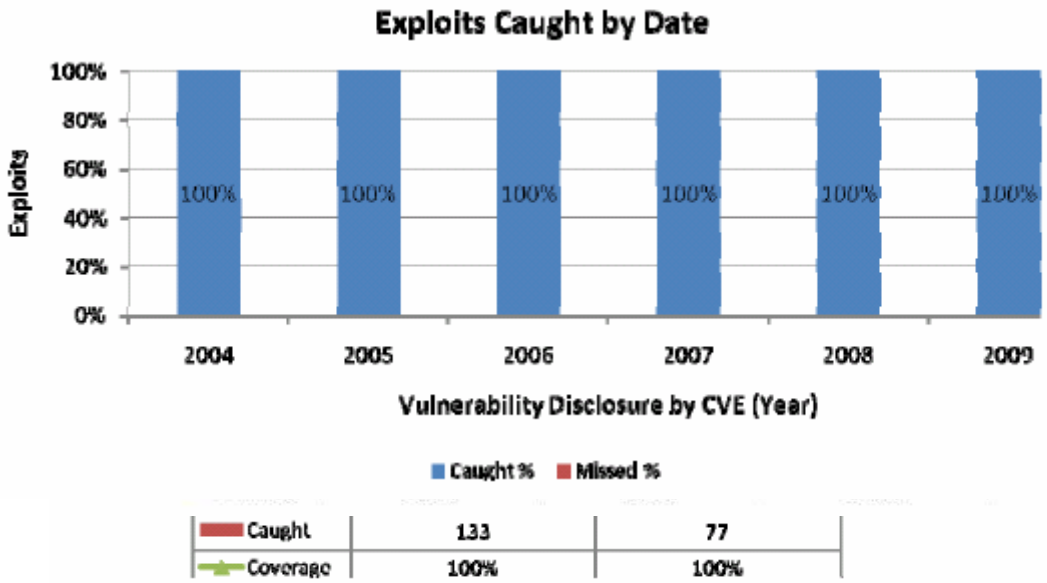
NSS 2009

NSS Labs
Security. Certified.

NSS Labs
Security. Certified.

2.4 COVERAGE BY DATE

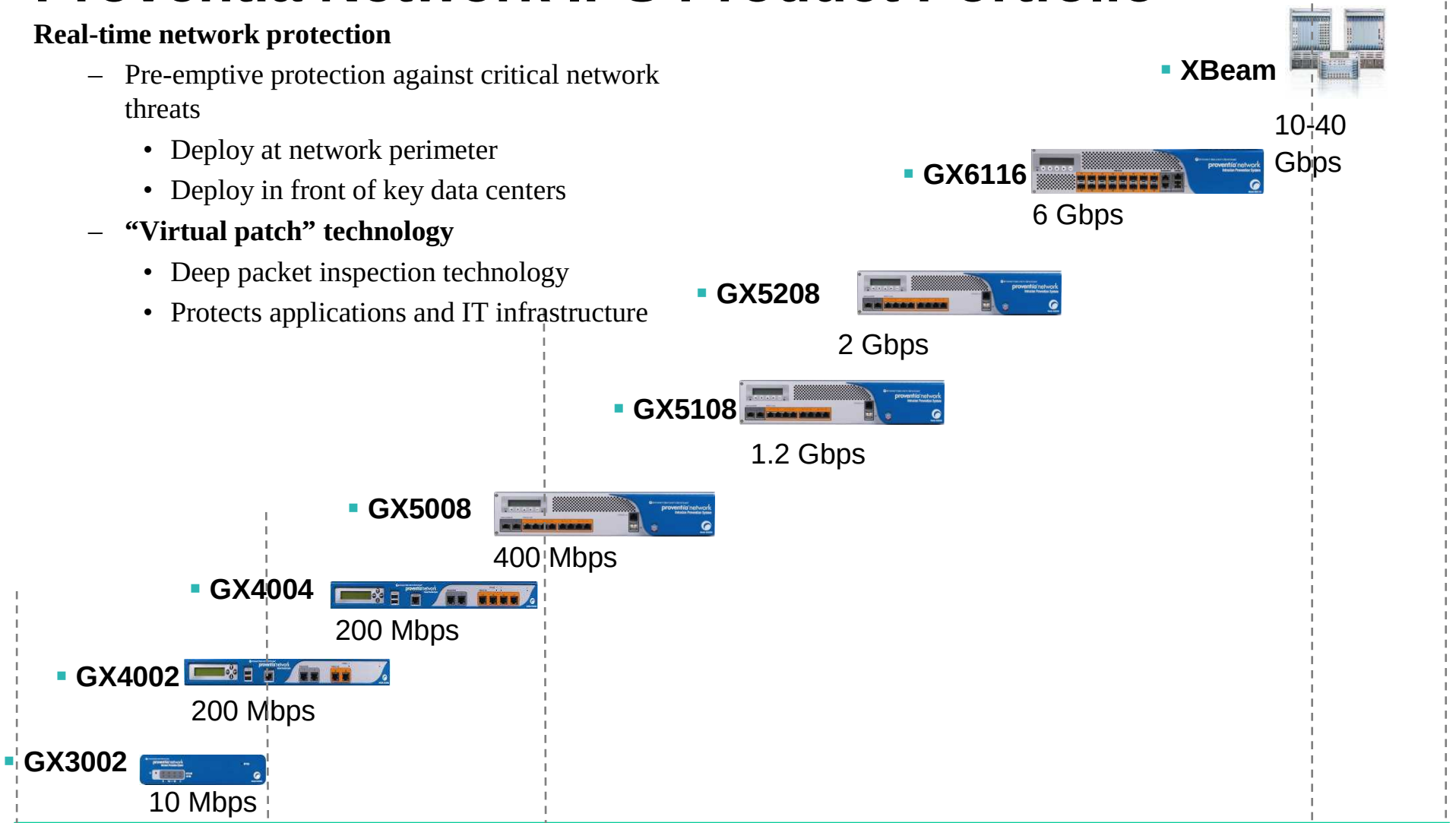
Year	2004	2005	2006	2007	2008	2009
Caught %	100%	100%	100%	100%	100%	100%



Proventia Network IPS Product Portfolio

Real-time network protection

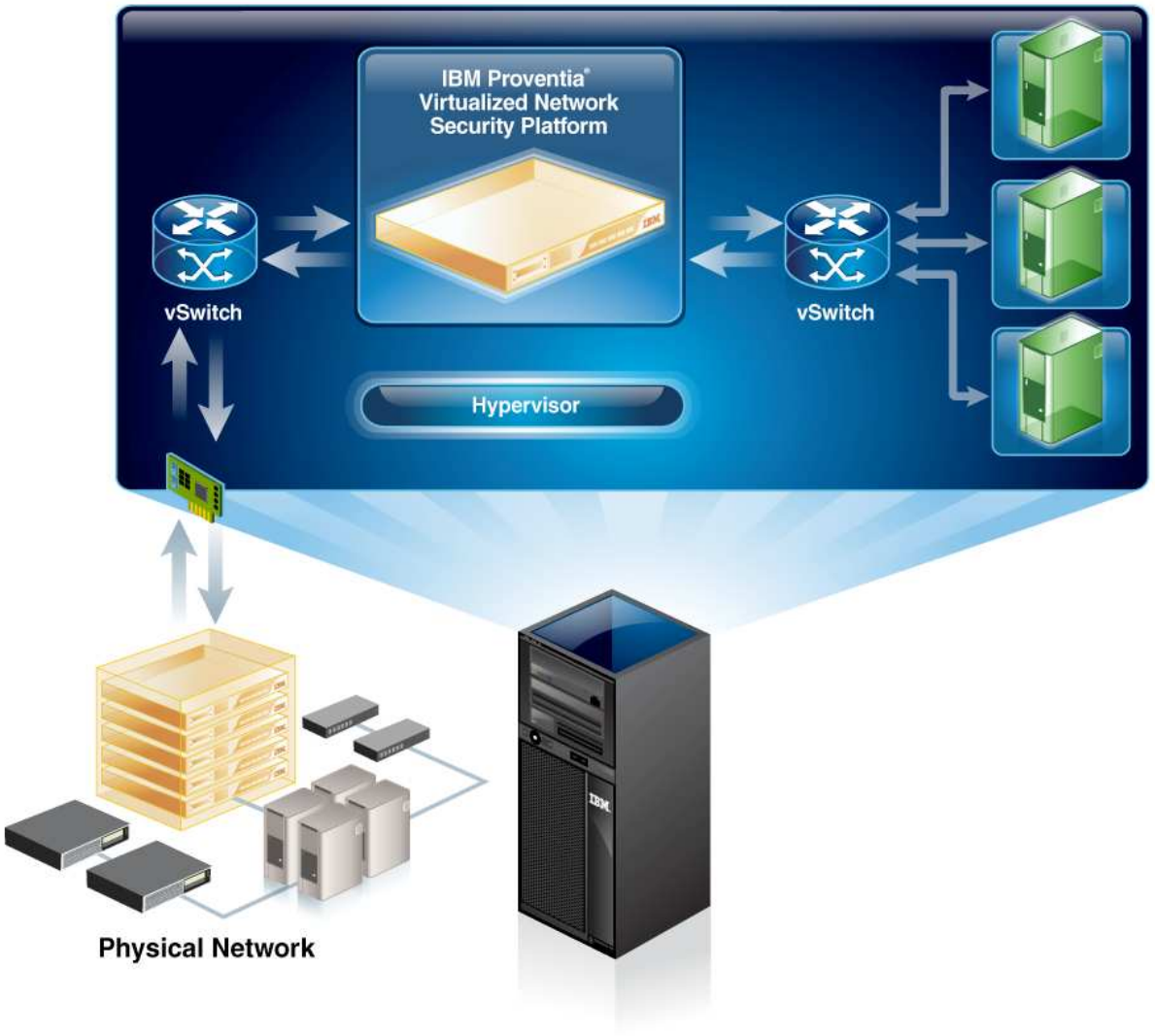
- Pre-emptive protection against critical network threats
  - Deploy at network perimeter
  - Deploy in front of key data centers
- **"Virtual patch" technology**
  - Deep packet inspection technology
  - Protects applications and IT infrastructure



Virtual Security Appliances

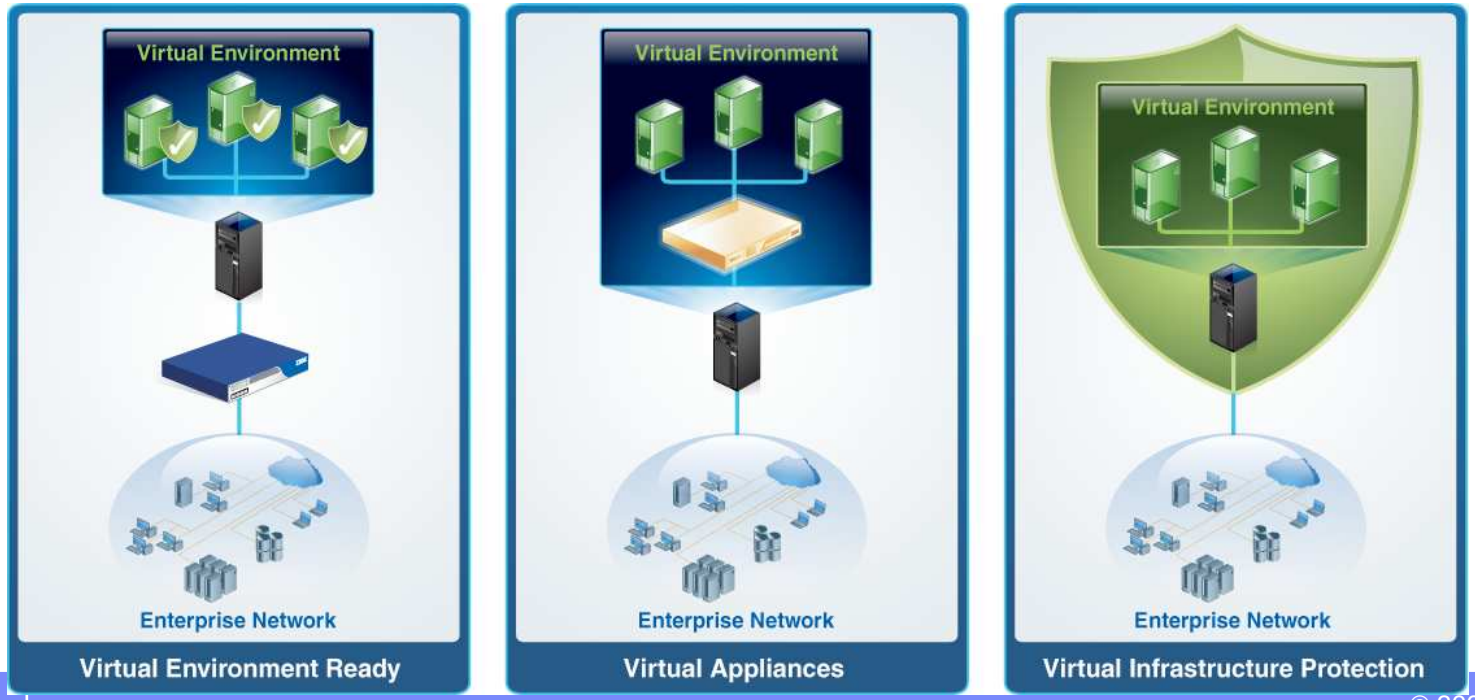
Virtual appliance protege segmentos fisicos de red

Virtual appliance protege segmentos de red virtuales



IBM ISS Reduce el costo y la complejidad en los entornos virtualizados

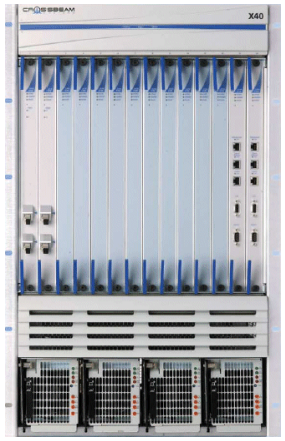
- **Diferentes productos y servicios optimizados para el mundo virtual , de esta forma los clientes podrán beneficiarse de los producttos virtuales de una forma segura**
  - Protección de Host Virtuales
  - Virtual appliances (IPS y Correo)
  - Seguridad para virtualizadoras ESX/ESXi y Vmware server
  - Reducción de costes (ahorro espacio , energetico, refrigeración …)
  - Escalable , consolidado y fácil desarrollo



IPS Plataforms

Support for Crossbeam AP 8400/8600 APM cards (up to 10 per chassis)

- **Integrated network switch**
  - Load balancer
  - Traffic routing
- **Robust high availability**
  - Port redundancy
  - Standby blades
  - Box-to-box HA
- **Performance**
  - Up to 1 Gbps throughput per blade



Blade-based IPS

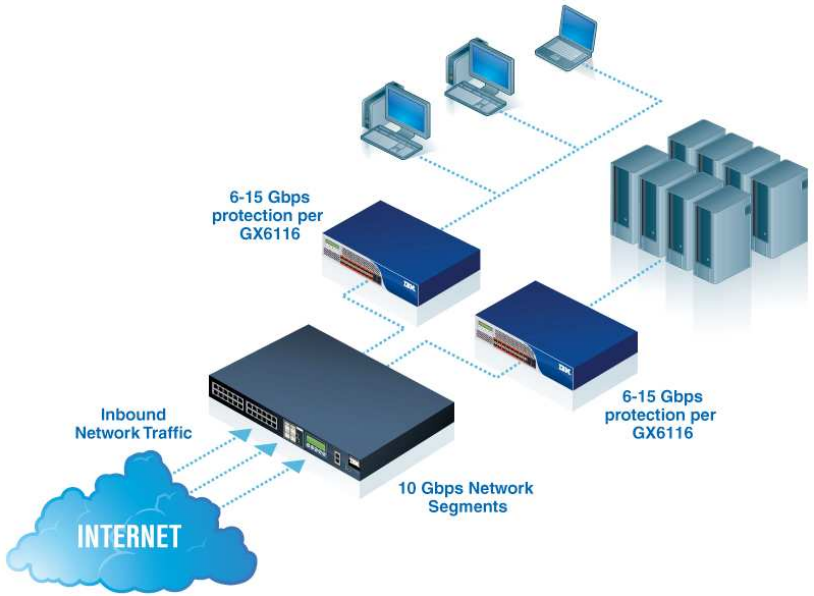
• Network core and carrier focus

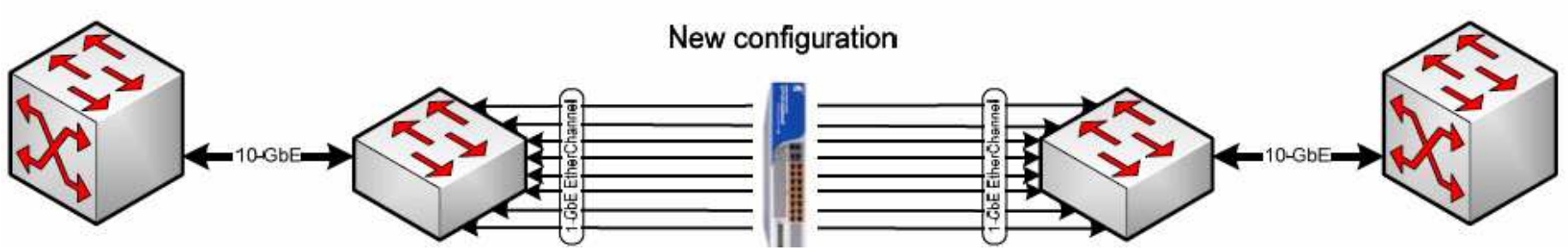
• Crossbeam, IBM BladeCenter

• Virtualization

IBM Proventia Network Security Controller

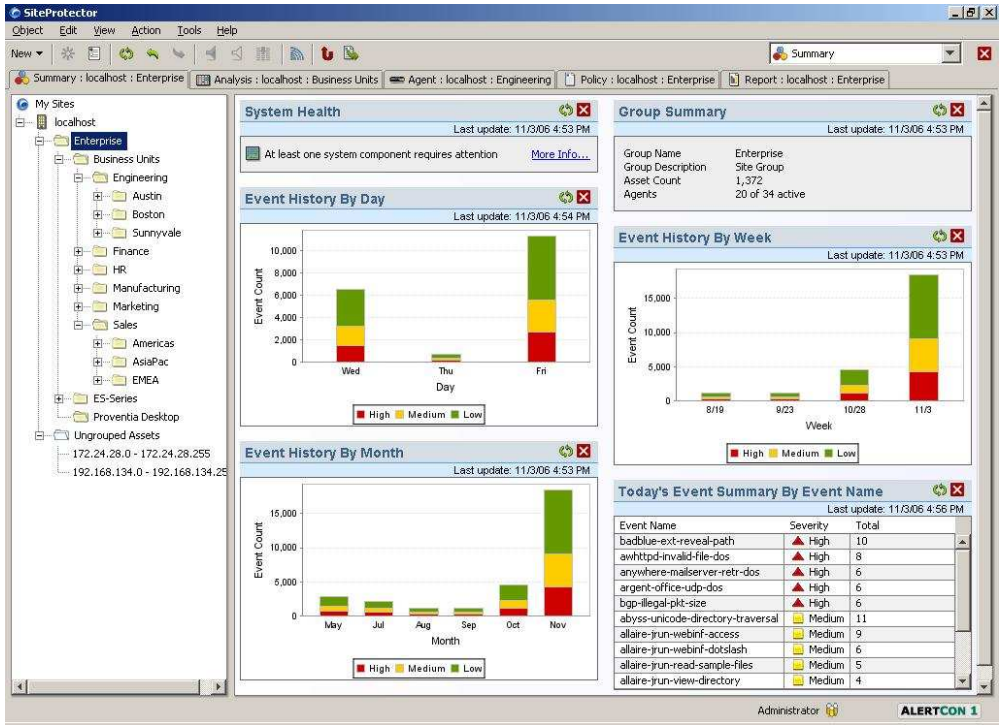
- **IBM Proventia Network Security Controller**
  - 10 Gbps interface to balance 10 Gbps network segments across multiple Proventia Network IPS appliances
  - Extend the life of existing NIPS appliances
  - Full active bypass functionality eliminates the need for additional hardware on the network
  - Plug and play setup and management





Proventia Network IPS Management

- **Browser-based local management interface (LMI)**
- **Central Management through Proventia Management SiteProtector:**
  - Simple, powerful configuration and control
  - Robust reporting, customized event viewing and event correlation
  - Comprehensive alerting and response options
  - Scheduled data retention to be used for compliance efforts
  - Highly scalable to accommodate hundreds of Proventia Network IPS appliances



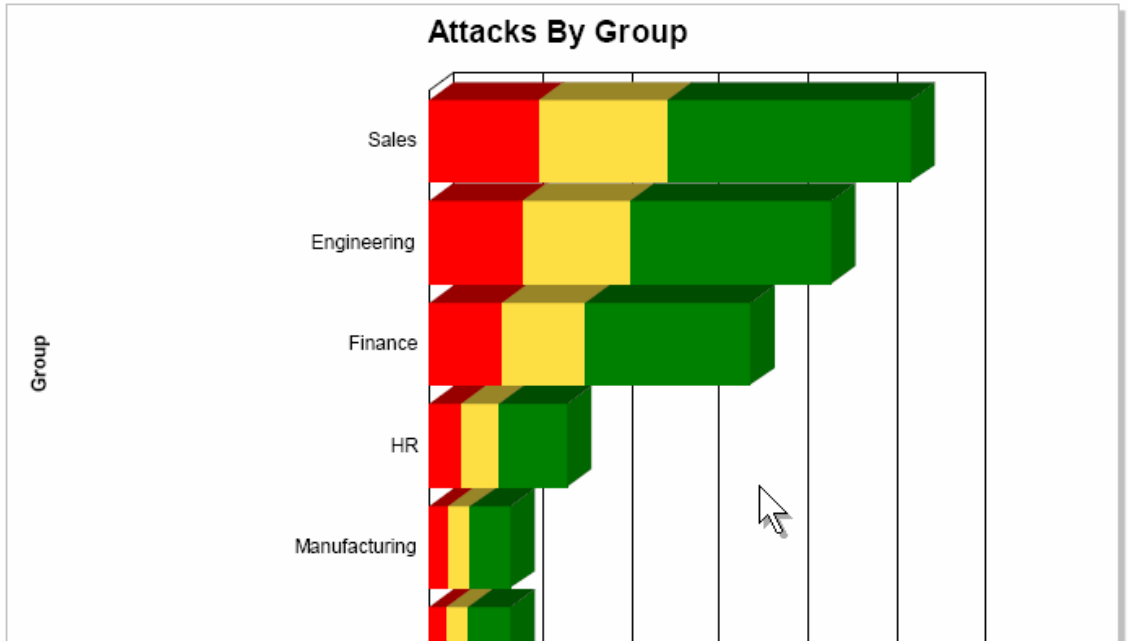
Reports

Attacks By Group

Sorted By Total Attacks

INTERNET SECURITY SYSTEMS

Group Name:	Business Units
Period Start Time:	2006-11-01 18:25:50 GMT
Period End Time:	2006-11-21 18:25:50 GMT
Exceptions:	Excluded
Asset Type:	All Assets
Subgroups:	Included
Comment:	
Includes:	Intrusion Detection, AntiVirus, Firewall, Network Anomaly Detection



Agenda

Protección del perimetro

Proventia® MX UTM

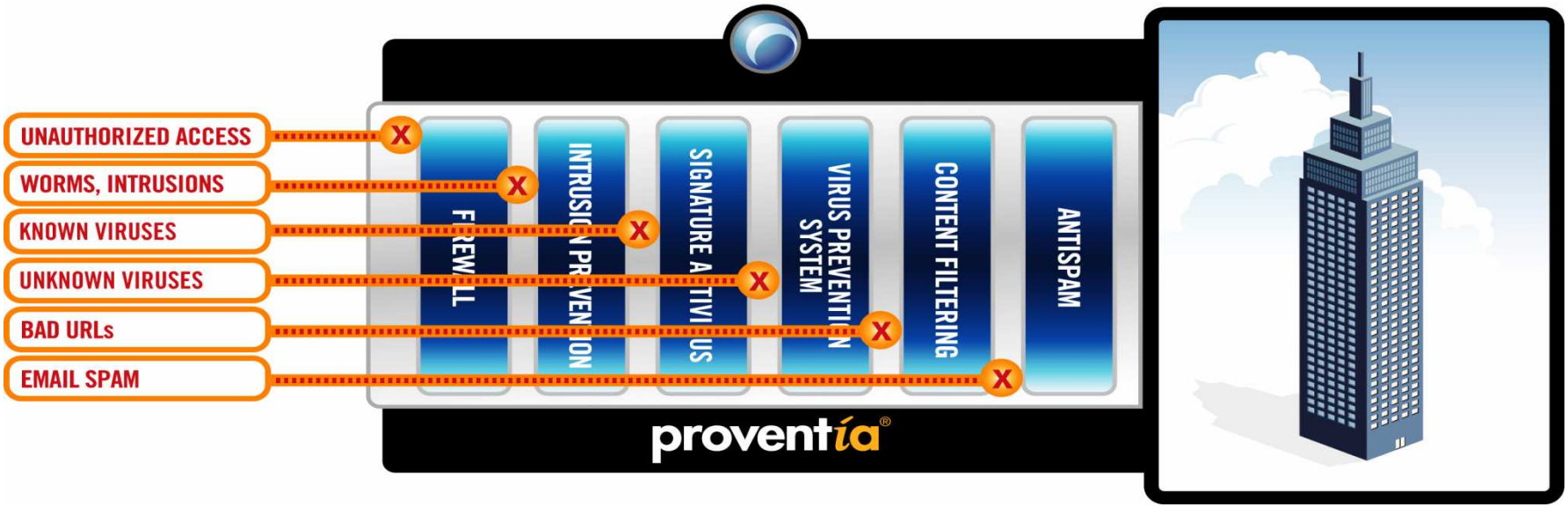
Proventia® Network MFS Attack Blocking

- Que hace…
  - –Bloquea múltiples tipos de ataque, mientras que el tráfico legítimo pasa intacto.
- Como Funciona …
  - –Incluye la última tecnología IPS, AV,VPS, AntiSpam, WebFiltering, NLB, QOS, FW+VPN & VPN SSL en un solo appliance

- Por que ISS ?
  - –Fabricante reconocido mundialmente con gran capacidad de I+D (X-Force)

Descripción General

proventía® network
Multi-Function Security



La diferencia...
Investigación = Ahead of the Threat!

- **Últimas tecnologías en Seguridad**
- **Más de 7400 vulnerabilidades bloqueadas por defecto**
- **340 Mil Virus Bloqueados (sophos)**
- **93% de los nuevos virus bloqueados por el VPS**
- **90 Mil millones de URL's registradas**
- **4 Mil millones de imagenes registradas**
- **95% del Spam Filtrado**
  - 1 de cada 10,000 Falso positivo
- **Protección Spyware Multicapa**
- **Servicios gestionados OPCIONAL**

RENDIMIENTO AL MEJOR COSTE!

Mx0804

Mx1004

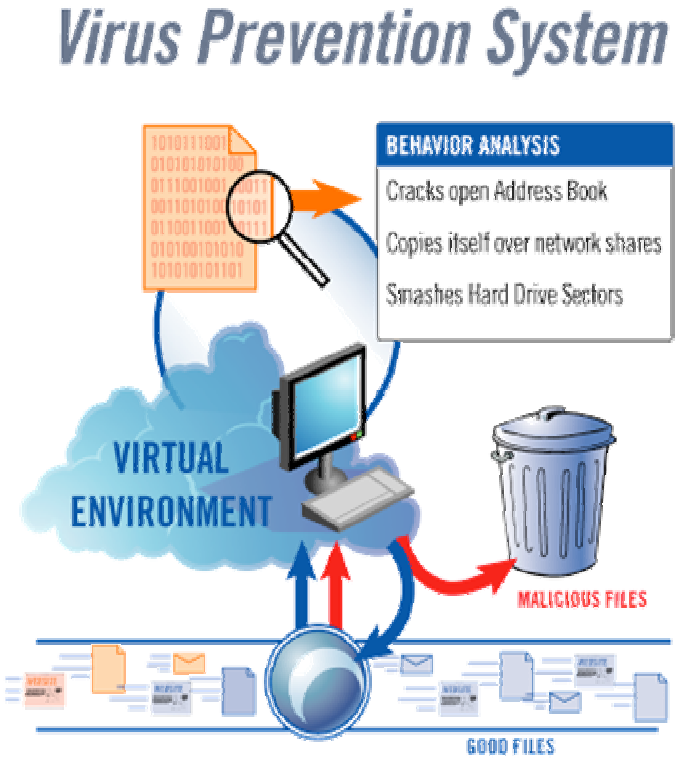
Mx3006

Mx4006

Mx5008

Mx5110

La diferencia...
Investigación = Ahead of the Threat!



- **Los programas maliciosos son detenidos antes de ejecutarlos**
  - Virtualiza en un entorno seguro
  - El entorno replica una API Windows , CPU, memoria, etc.
  - Se analiza el programa en busca de comportamientos anómalos
- **Se complementa con un antivirus tradicional**
- **93% de efectividad sin actualizaciones**

Rendimiento

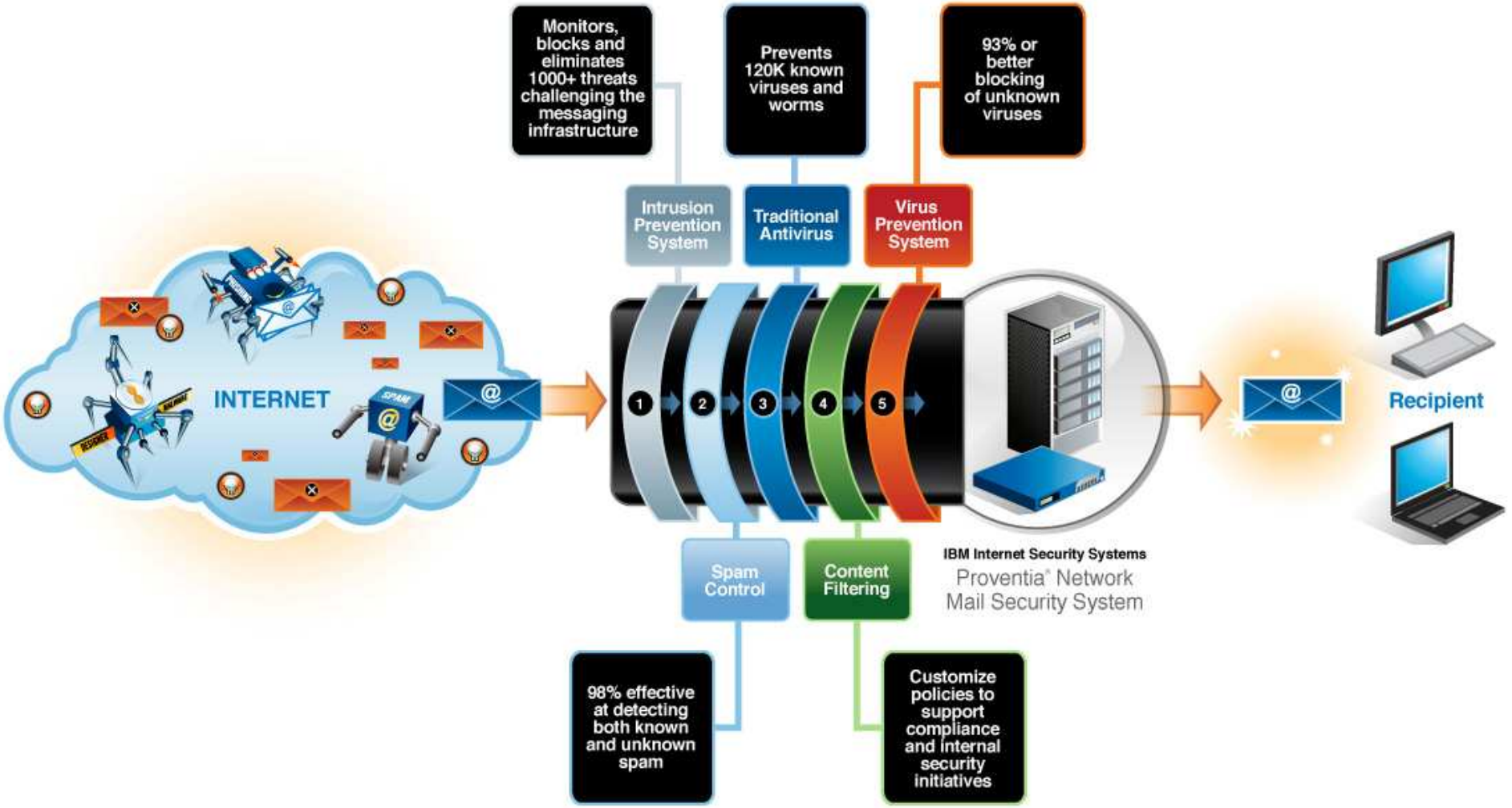
	MX0804	MX1004	MX3006	MX4006	MX5008	MX5110
						
Firewall Only	100 Mbps Unlim. users	100 Mbps Unlim. users	200 Mbps Unlim. users	600 Mbps Unlim. users	1.6 Gbps Unlim. users	1.8 Gbps Unlim. users
Firewall ▪7400+ vulnerabilities blocked by IPS	100 Mbps Unlim. users	100 Mbps Unlim. users	200 Mbps Unlim. users	450 Mbps Unlim. users	730 Mbps Unlim. users	800 Mbps Unlim. users
Firewall ▪7400+ vulnerabilities blocked by IPS ▪Antivirus on Mail protocols ▪URL filtering for over 9B web objects	25 Mbps Less than 50 users	43 Mbps Less than 100 users	200 Mbps Less than 500 users	360 Mbps Less than 1000 users	496 Mbps Less than 2000 users	566 Mbps Less than 3000 users
Firewall ▪7400+ vulnerabilities blocked by IPS ▪Antivirus on all protocols ▪95%+ of spam blocked ▪URL filtering for over 9B web objects	15 Mbps Less than 50 users	34 Mbps Less than 100 users	94 Mbps Less than 500 users	120 Mbps Less than 1000 users	135 Mbps Less than 3000 users	150 Mbps Less than 3000 users
VPN Max Speed (AES 192)	30 Mbps	50 Mbps	143 Mbps	170 Mbps	230 Mbps MX5008A: 298 Mbps	247 Mbps MX5008A: 313 Mbps
						

Agenda

Protección del perimetro

Proventia® Network MAIL

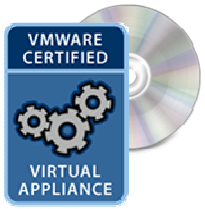
Proventia Network Mail - Multi-layered Email Protection



Mail Security

Proventia Network Mail protege el correo de forma preventiva y controla el spam de forma segura

Proventia Network Mail Security System MS3004N



Proventia Network Mail Security System Virtual Appliance – MS1002-VM

Product Features

- Easy to install appliances
  - Physical or virtual
  - Proventia set-up assistant
- Dynamic host reputation
  - 300 mail/second
- Gateway-to-gateway encryption
- Directory integration objects
- 40+ foreign languages supported
- Flexible and granular rule set

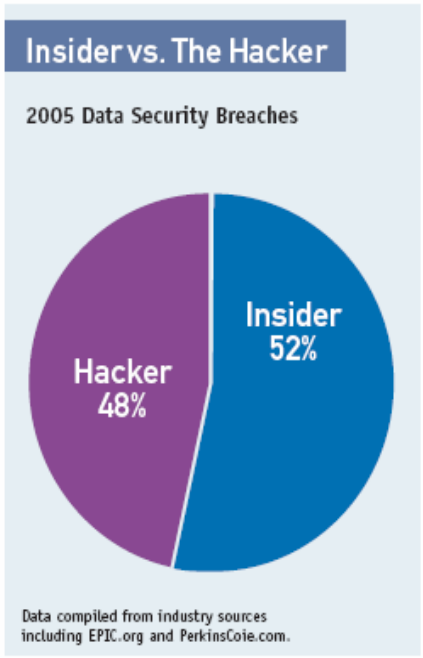
Agenda

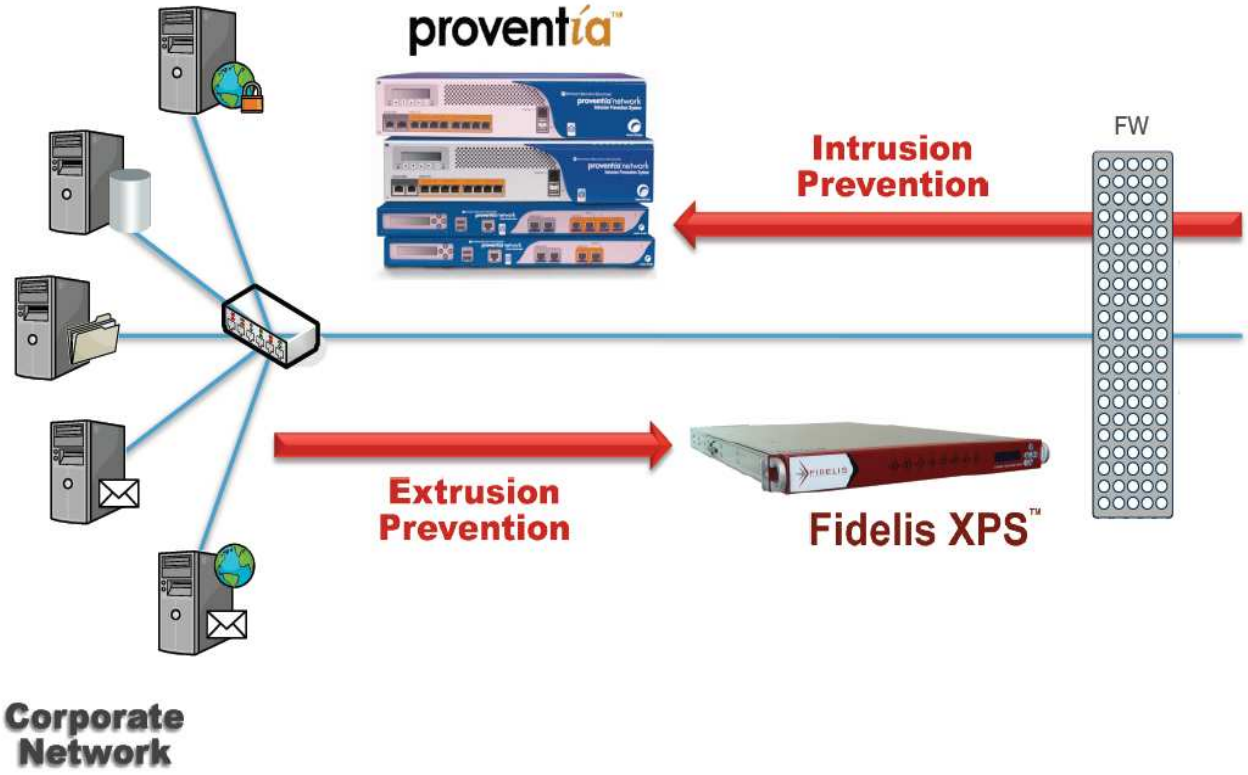
DLP

Data loss prevention

RED

Plataforma de Protección de Fuga de la Información en Redes: Evolución desde la protección del perímetro a la protección de los datos



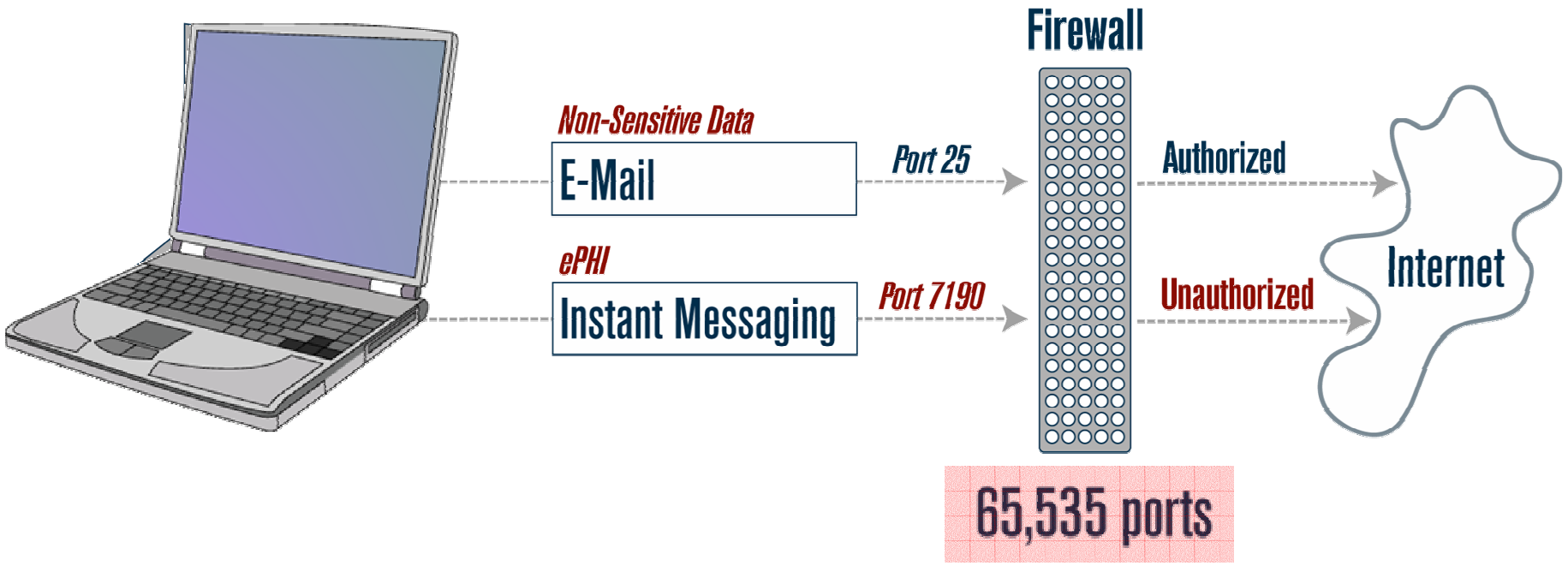


"…según Gartner, los riesgos que provienen del interior de las organizaciones son responsables del 70% de los fallos de seguridad"

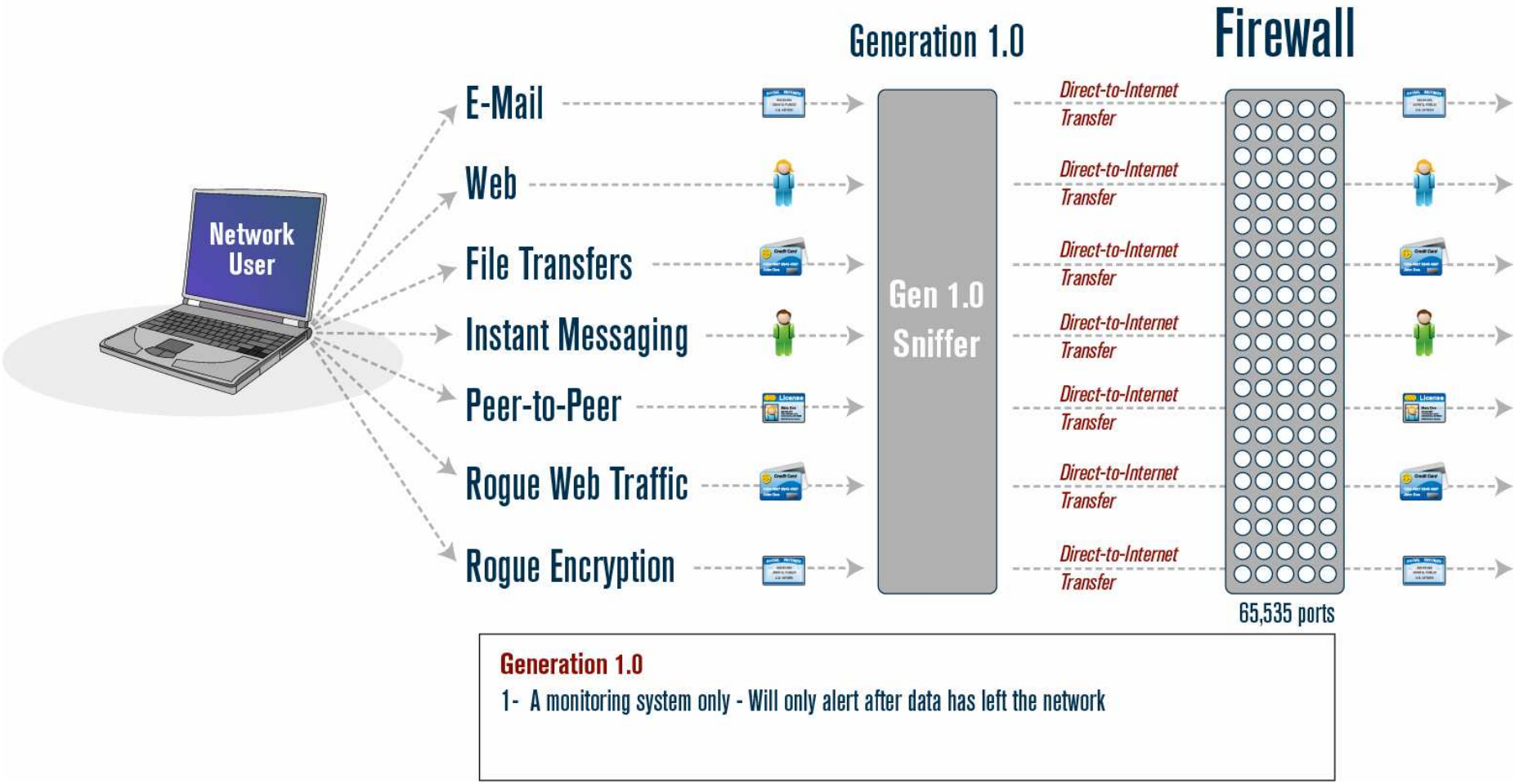
Pervasive Security in a Connected World, Wachovia, April 2007

XPS : Controlar el 100% del tráfico

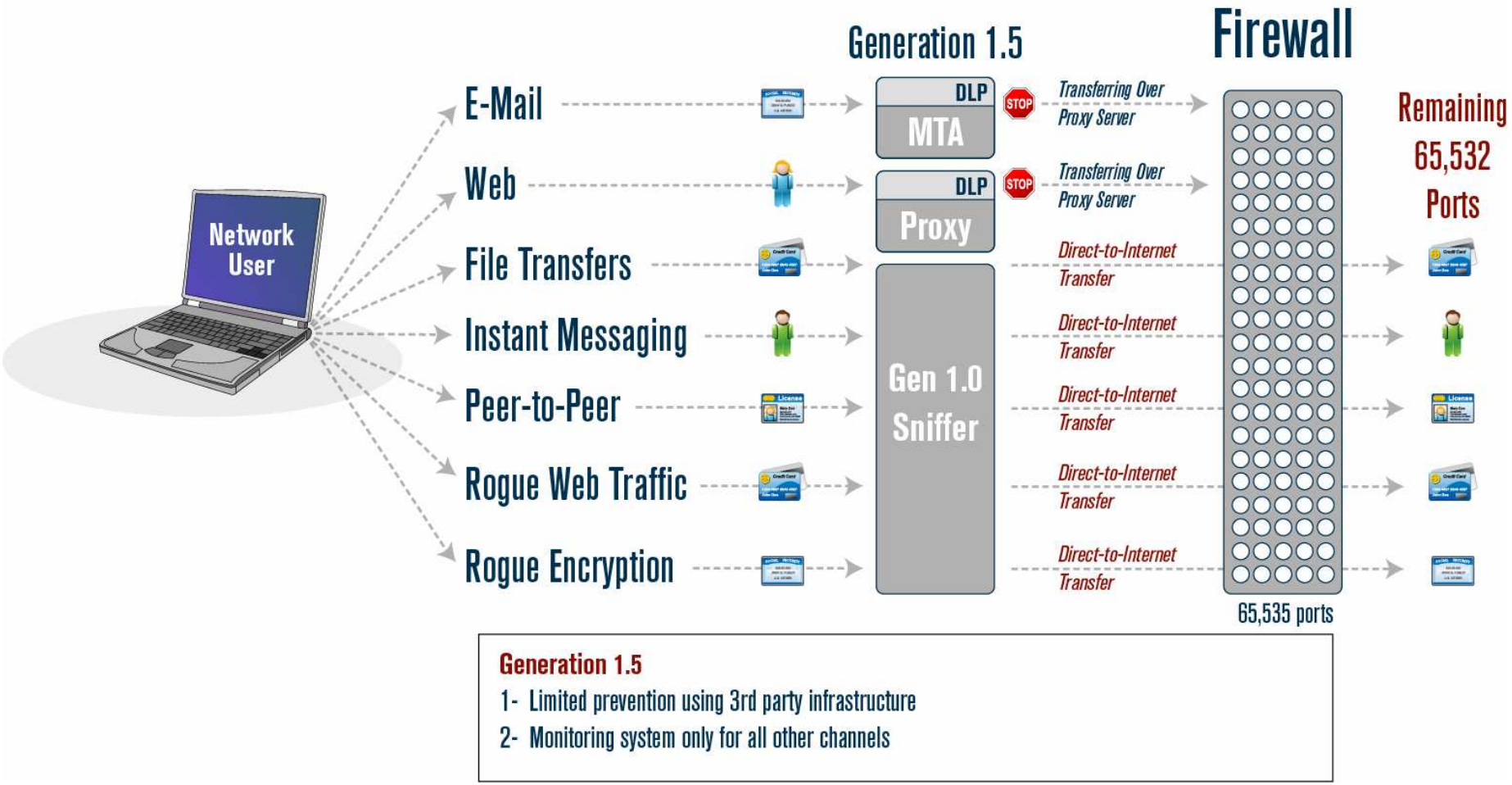
Los analistas estiman que el 90% de las organizaciones no controlan adecuadamente la salida a internet



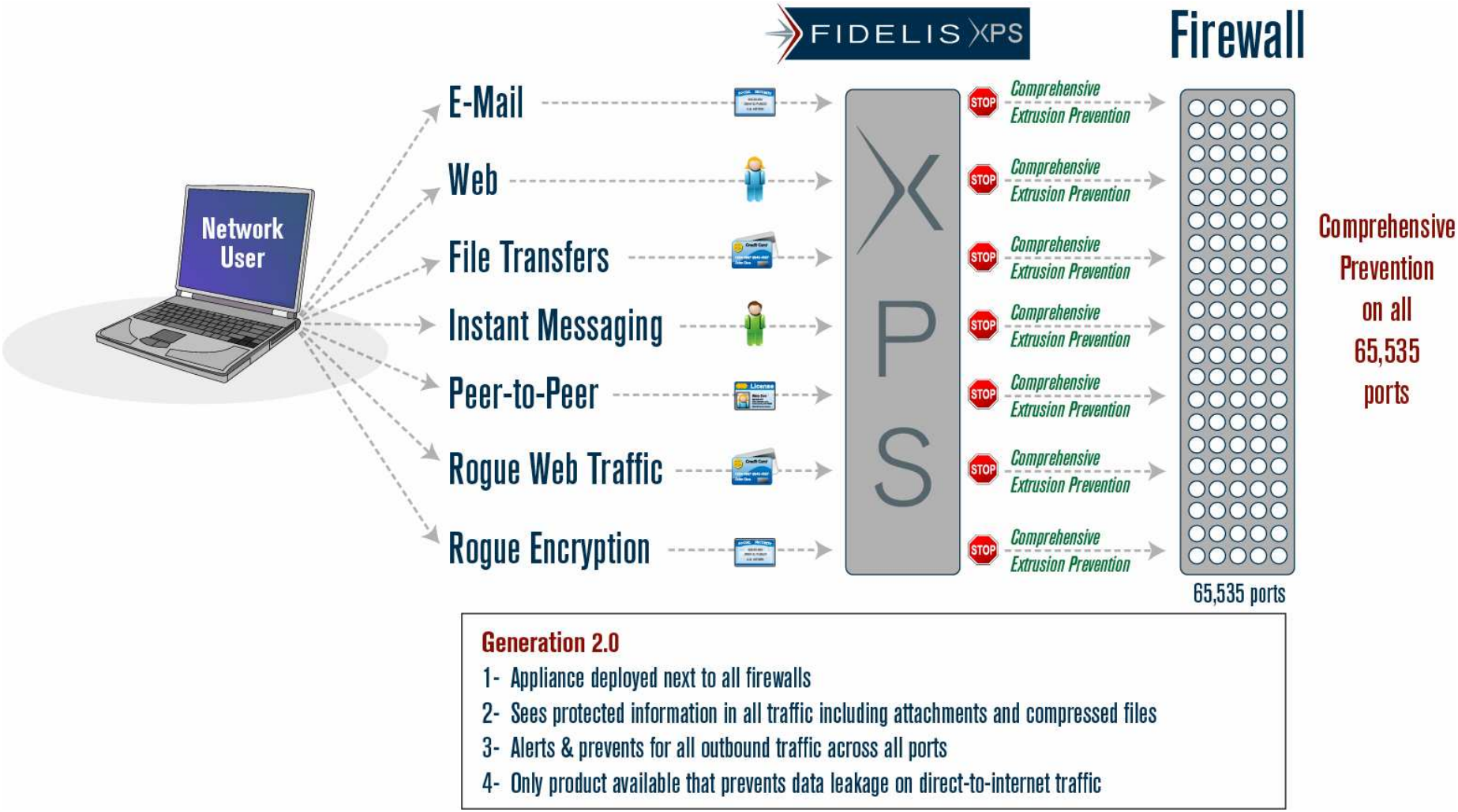
Gen 1 Extrusion: Solo Detección



Gen 1.5 Extrusion: Prevención Límitada



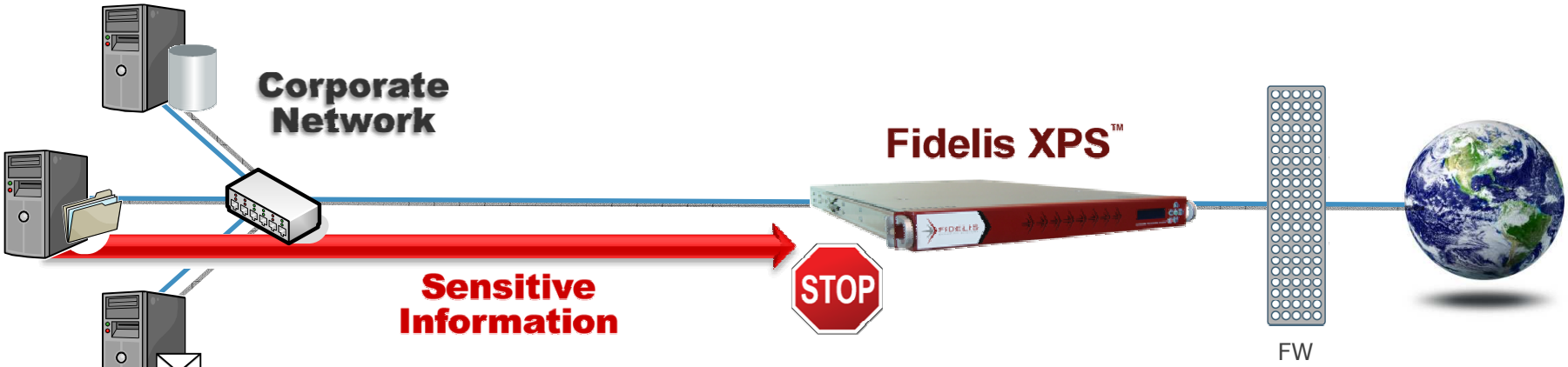
Gen 2.0 DLP: Prevención Global



Generation 2.0

1- Appliance deployed next to all firewalls
2- Sees protected information in all traffic including attachments and compressed files
3- Alerts & prevents for all outbound traffic across all ports
4- Only product available that prevents data leakage on direct-to-internet traffic

DLP en redes - Extrusion Prevention System (XPS)



Trigger > Content

Sensitive information defined in content analyzers

1. Smart Identity Profiling
2. Keyword
3. Keyword Sequence
4. Regular Expressions
5. Binary Signatures
6. Encrypted Files
7. File Names
8. Exact File Matching
9. Partial Document Matching
10. Embedded Images

Trigger > Location

Sender and recipient information

1. source IP address
2. destination IP address
3. Geographical Data–the country in which the IP address is registered
4. Username
5. LDAP directory attributes

Trigger > Channel

Details about the information flow

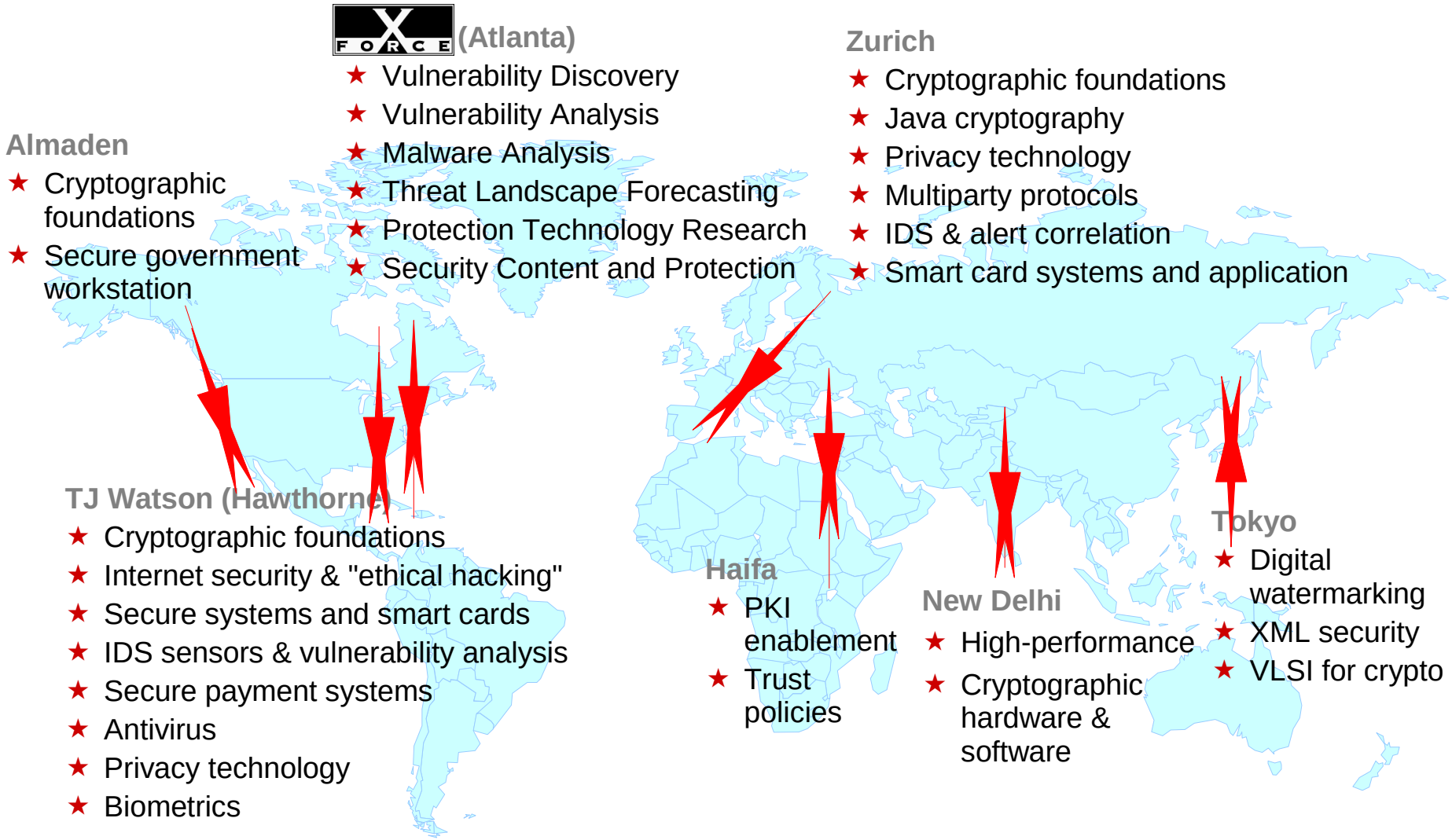
1. Application / protocol (port -independent)
2. Application-specific Attributes (e.g., user, e-mail address, subject, filename, URL, encrypted, cipher, and many more)
3. Port (Source / Destination)
4. Session length / size
5. Day of week / Time of day
6. Session duration
7. Decoding path

Servicios Gestionados

IBM Global Security Reach

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

IBM maintains worldwide Security and Privacy Research and Development capabilities



Almaden
- Cryptographic foundations
- Secure government workstation

X-FORCE (Atlanta)
- Vulnerability Discovery
- Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research
- Security Content and Protection

Zurich
- Cryptographic foundations
- Java cryptography
- Privacy technology
- Multiparty protocols
- IDS & alert correlation
- Smart card systems and application

TJ Watson (Hawthorne)
- Cryptographic foundations
- Internet security & "ethical hacking"
- Secure systems and smart cards
- IDS sensors & vulnerability analysis
- Secure payment systems
- Antivirus
- Privacy technology
- Biometrics

Haifa
- PKI enablement
- Trust policies

New Delhi
- High-performance
- Cryptographic hardware & software

Tokyo
- Digital watermarking
- XML security
- VLSI for crypto

IBM Global Services

Gracias

Raúl Pérez García

IBM Internet Security Systems

Ahead of the threat.™