



Pulse Comes To You

PCTY2011



Soluciones de Seguridad, para un planeta más inteligente

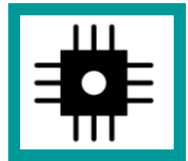
IBM®

¿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.



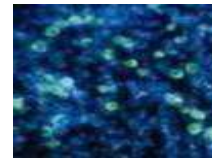
Smart supply chains



Smart countries



Smart retail



Smart water management



Smart weather



Smart energy grids



Intelligent oil field technologies



Smart regions



Smart healthcare



Smart traffic systems

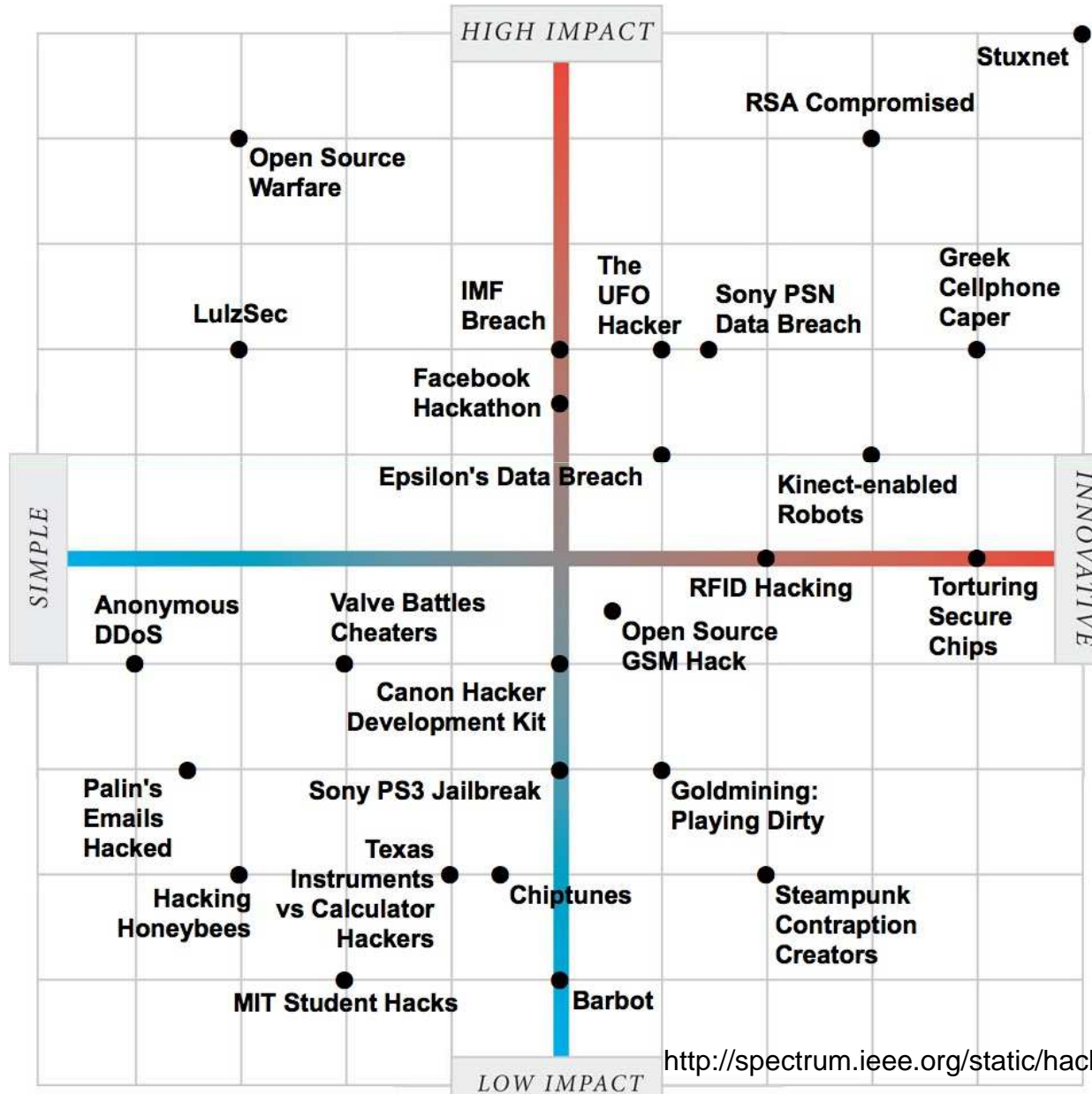


Smart cities



Smart food systems

Características de 25 “eventos”

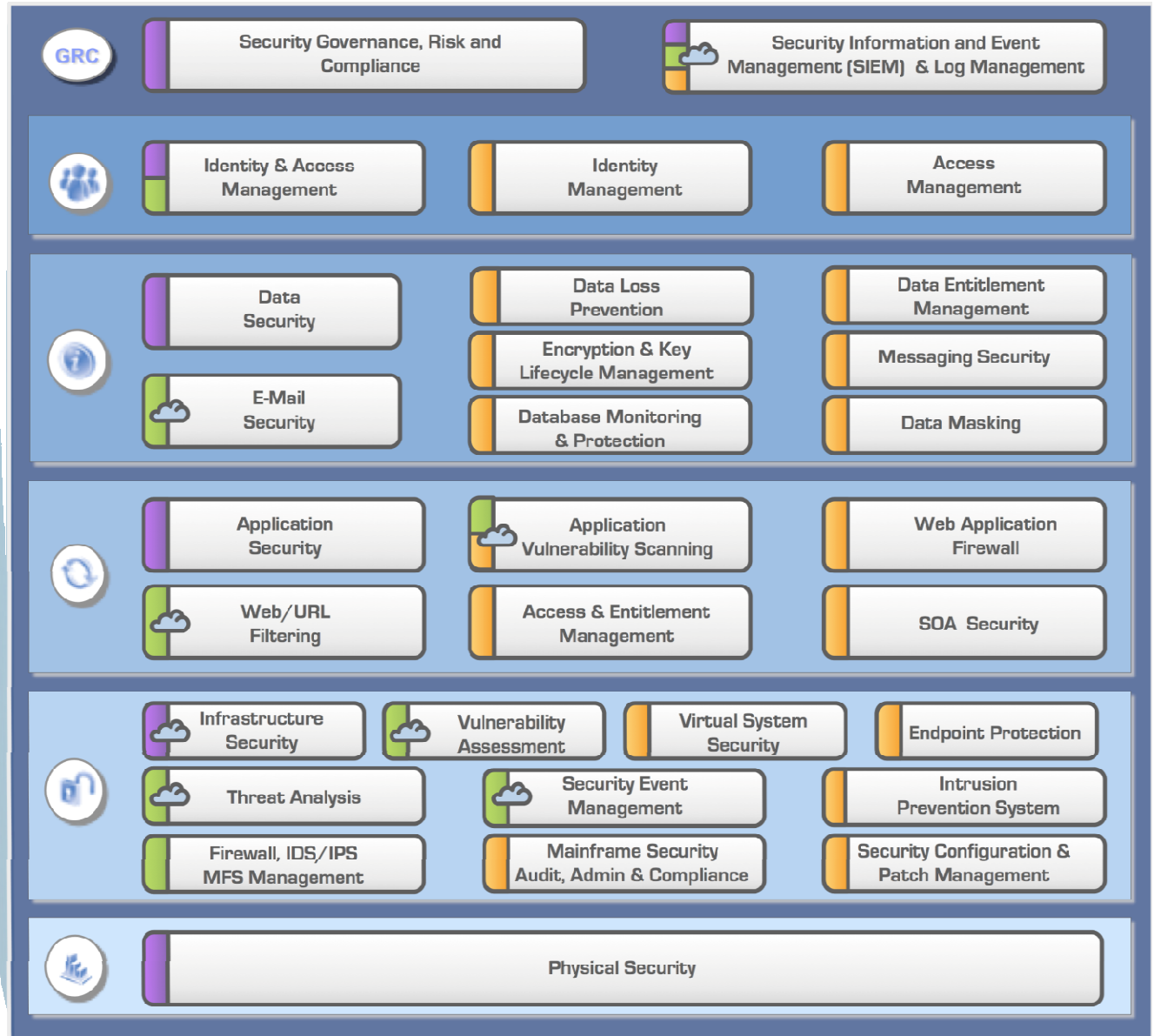
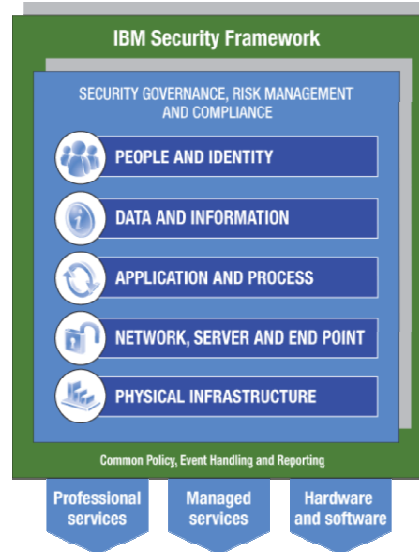


Características del nuevo escenario y cambio de paradigma

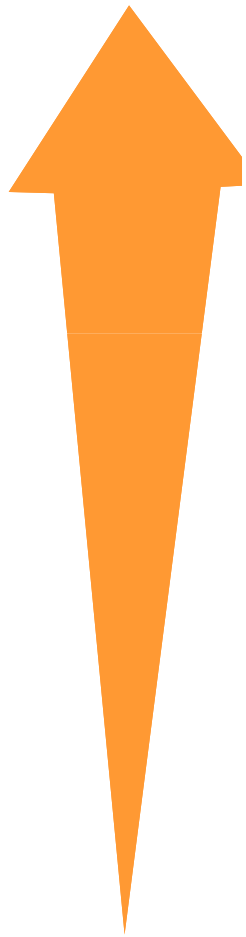
- En el informe de X-Force del 2010 se indica: “.. En vez de enfocarse en un único punto de entrada, las nuevas amenazas tienen como objetivo múltiples recursos en la compañía. No sólo lo expuesto al público esta en riesgo, sino que, cada empleado y endpoint se ha convertido en un potencial punto de entrada”.
- El “adversario” externo es altamente entrenado e inteligente, por lo que se requiere una postura más activa ante el riesgo.
- Un memo de la Casa Blanca en el 2010 sobre FISMA (Federal Information Security Management Act) indica:
 - “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”

IBM Security Solutions Portafolio

-  **Professional Services**
-  **Managed Services**
-  **Products**
-  **Cloud Delivered**



Un modelo de seguridad enfocado en madurez

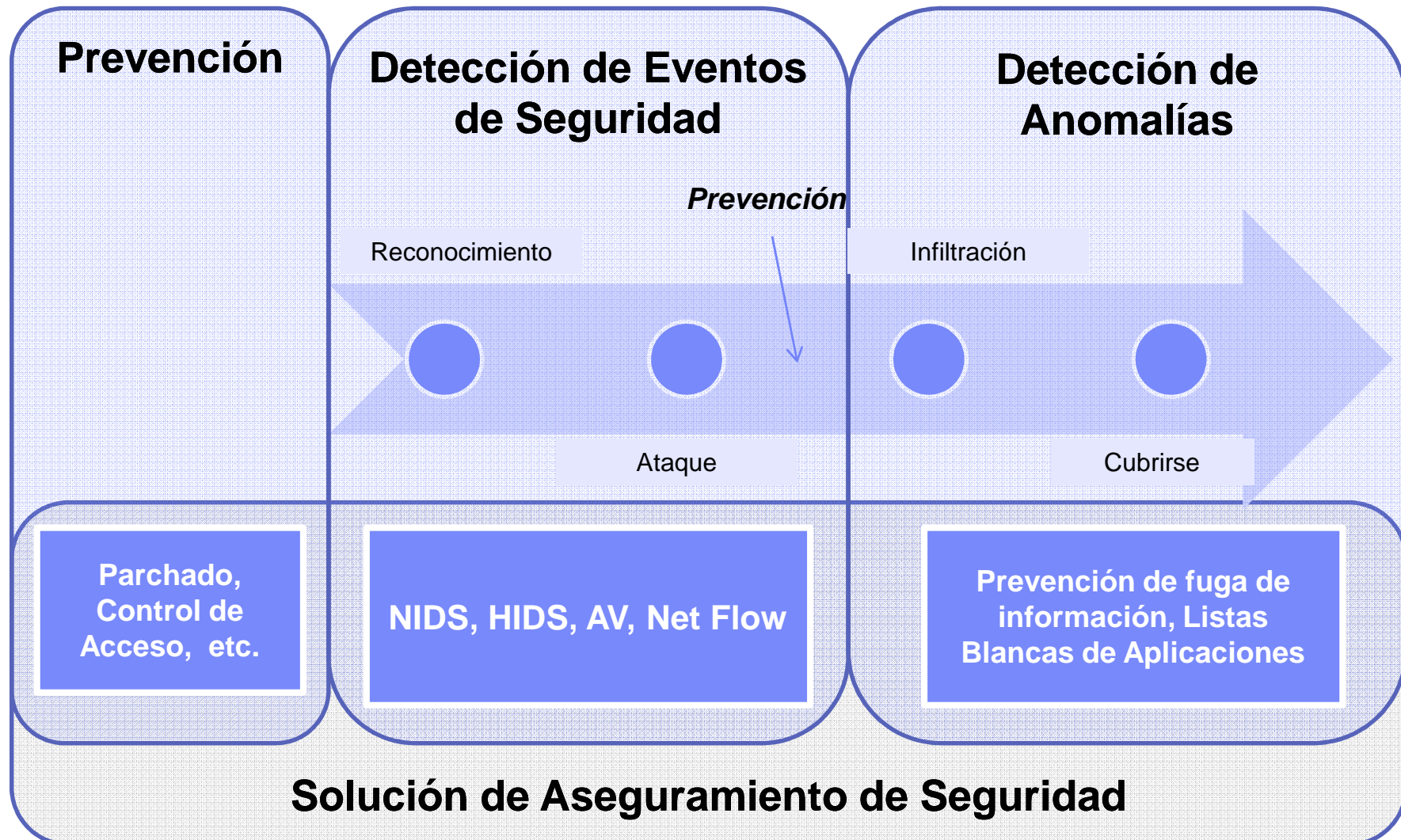


	People	Data	Applications	Infrastructure
Optimized	Governance, risk and compliance		Advanced correlation and deep analytics	
	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure application development Fraud detection	Advanced network monitoring / forensics Secure systems
Proficient	Identity management Strong authentication	Activity monitoring Data loss prevention	Application firewall Source code scanning	Asset management Endpoint / network security management
Basic	Passwords and user identities	Encryption Access control	Vulnerability scanning	Perimeter security Anti-virus

TOP 20 Controles Críticos de Seguridad, según SANS Institute

1. Inventory of Authorized and Unauthorized Devices: **Tivoli Endpoint Mgr**
2. Inventory of Authorized and Unauthorized Software: **Tivoli Endpoint Mgr**
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers: **Tivoli Endpoint Mgr y IBM Security Server Protection**
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches: **Tivoli Netcool Configuration Manager**
5. Boundary Defense: **IBM Security Network IPS**
6. Maintenance, Monitoring, and Analysis of Security Audit Logs: **Tivoli Security Information & Event Mgr**
7. Application Software Security: **IBM Security Network IPS + Rational Appscan**
8. Controlled Use of Administrative Privileges: **Tivoli Identity Mgr+Tivoli Access Mgr ESSO = Privileged Identity Manager**
9. Controlled Access Based on the Need to Know: **IBM Security Server Protection y Tivoli Endpoint Mgr**
10. Continuous Vulnerability Assessment and Remediation: **Tivoli Endpoint Mgr y IBM Security Network IPS**
11. Account Monitoring and Control: **Tivoli Identity Mgr+Tivoli Security Information & Event Mgr**
12. Malware Defenses: **Tivoli Endpoint Mgr for Core Protection, IBM Security Network IPS y IBM Security Server Protection**
13. Limitation and Control of Network Ports, Protocols, and Services: **Tivoli Endpoint Mgr, IBM Security Network IPS, IBM Security Virtual Server Protection, IBM Security Server Protection**
14. Wireless Device Control
15. Data Loss Prevention: **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

Ayuda a proveer

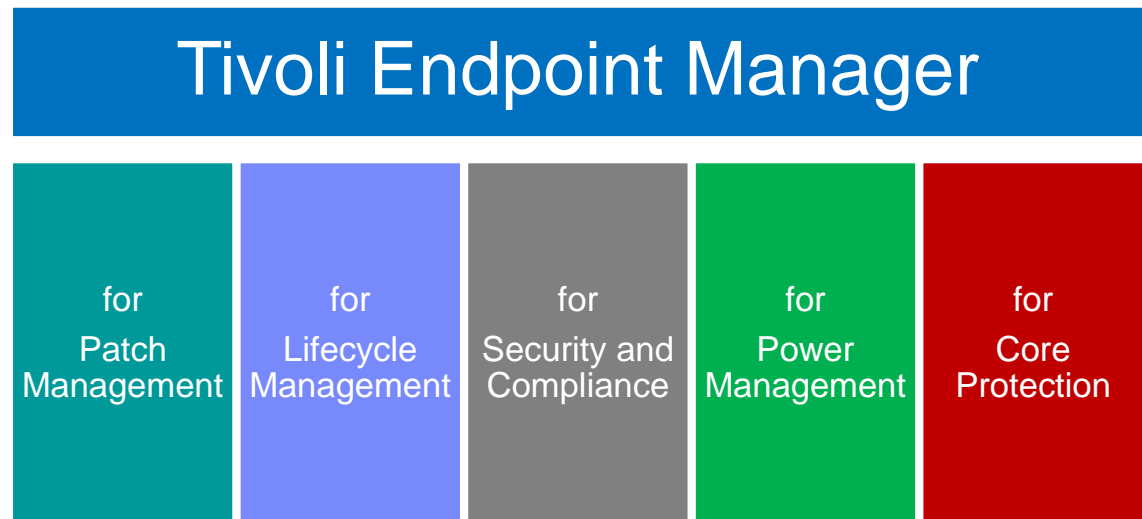
- Visibilidad total
- Control de calidad
- Rapidez en remediación
- Gran escalabilidad
- Framework versátil
- Reducción de costos

Mediante

- Gestión de configuración de seguridad y vulnerabilidades
- Gestión del ciclo de vida de los sistemas
- Protección contra Malware y firewall a través de tecnologías *Trend Micro™*
- Conocimiento de ambientes virtuales
- Gestión de consumo energético

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”



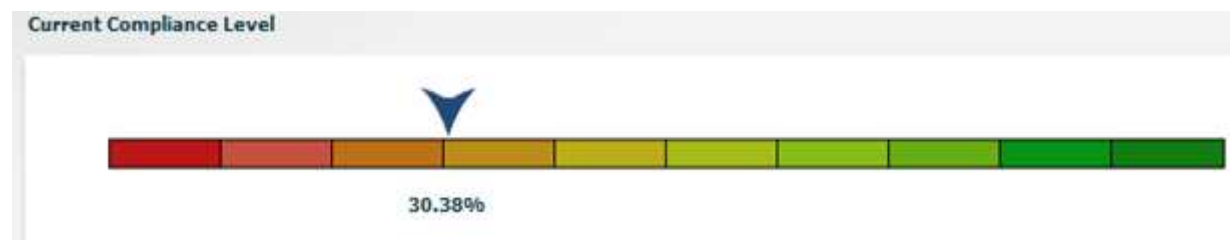
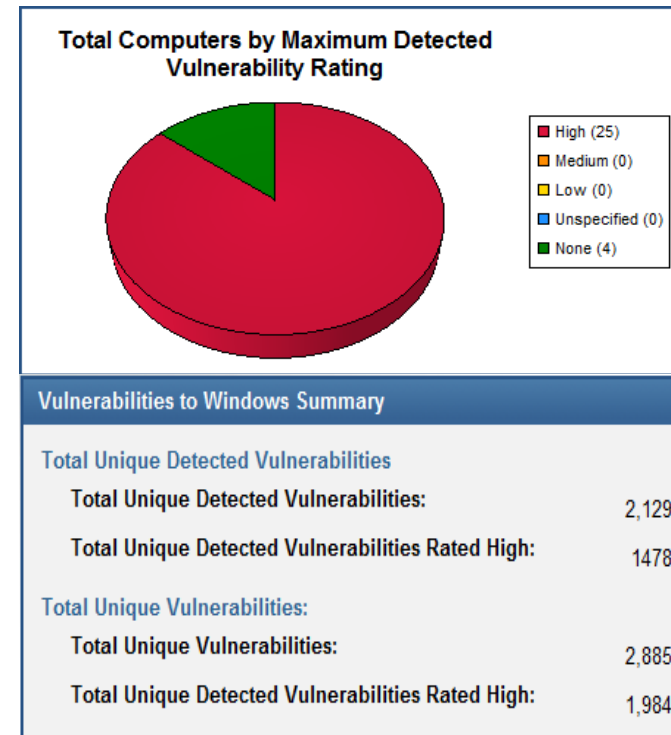
Tivoli Endpoint Manager apoyando la gestión de vulnerabilidades y configuración de seguridad

Detección y Gestión de vulnerabilidades basadas en:

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

Mejores prácticas y plantillas basadas en:

- 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
 - Windows 7



Nuevo IBM Security Network IPS GX7800

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
- Capacidades de protección a nivel de red de Core

IBM Security Network Intrusion Prevention GX7800



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

Rendimiento Incomparable provee capacidad de inspección de tráfico de mayor a 20Gbps de throughput, con conectividad 10GbE sin comprometer la profundidad y amplitud de protección

• Evolución de la protección impulsado por la investigación de X-Force para estar “delante de la amenaza“

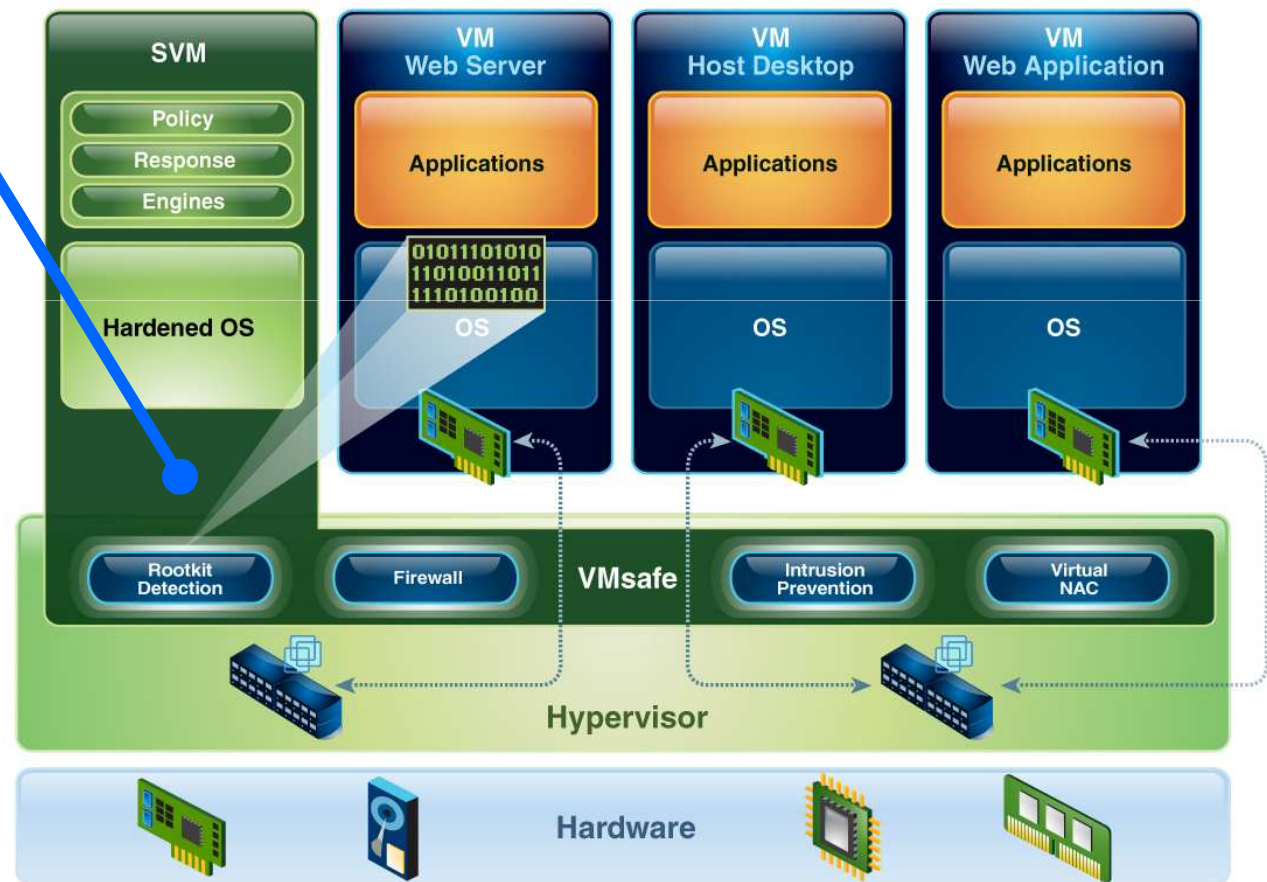
Ubicación	Remoto	Perímetro			Core		
Modelo	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
Tráfico Inspeccionado	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	8 Gbps	20 Gbps+
Segmentos	2	2	4	4	4	8	4

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

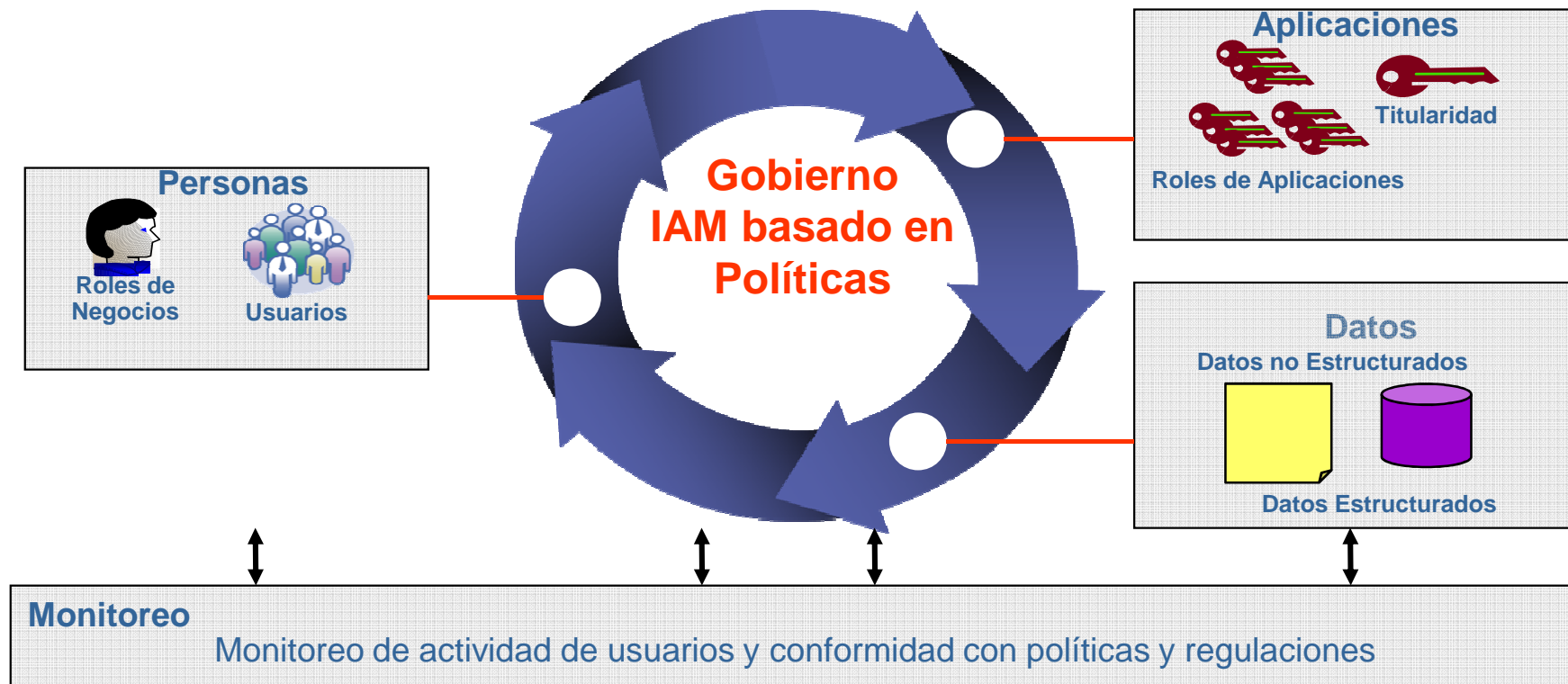


Gobierno de Identidades, Tivoli Identity & Access Assurance

- IBM líder tecnológico y del mercado.
- Gestión segura, automatizada y basada en políticas de las cuentas y permisos de usuarios.
- Soluciones de Single Sign-On para ambientes Web, Federaciones y estaciones de trabajo.
- Integración con sistemas de autenticación robusta
- Monitoreo automatizado de actividad de usuarios



La estrategia de IBM para gestión de identidades y accesos provee las bases para establecer gobierno de la Identidad



Visibilidad de identidades de usuarios, sus roles y derechos a aplicaciones y a datos

Control de definición de roles y asignación de usuarios a roles y derechos – gobernanza y cumplimiento

Automatización de suministro de usuario, rectificación de acceso y distribución de políticas

IBM Tivoli Identity Manager

Automatización

**Administrators
Create Accounts**

User Change

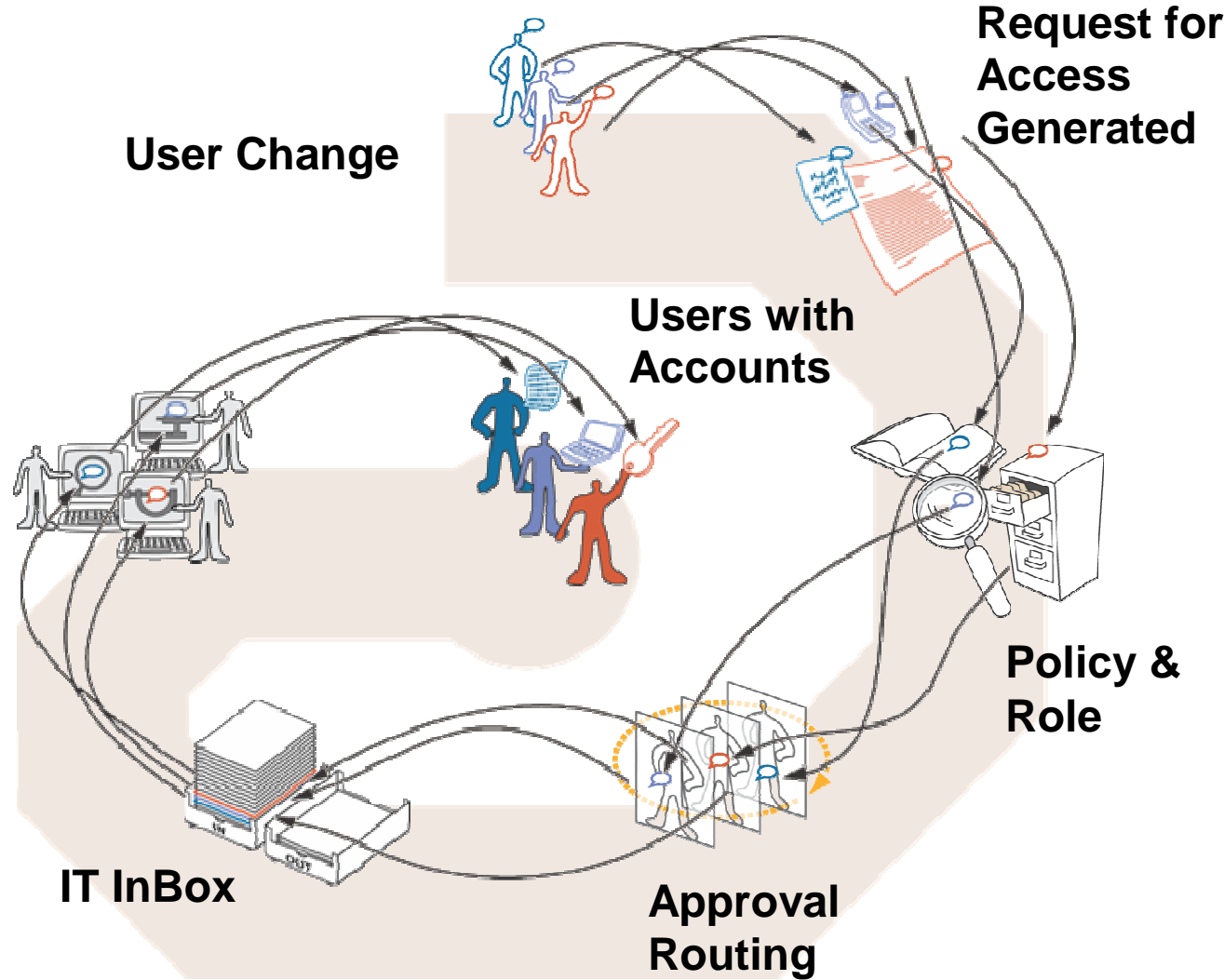
**Request for
Access
Generated**

**Users with
Accounts**

**Policy &
Role**

IT InBox

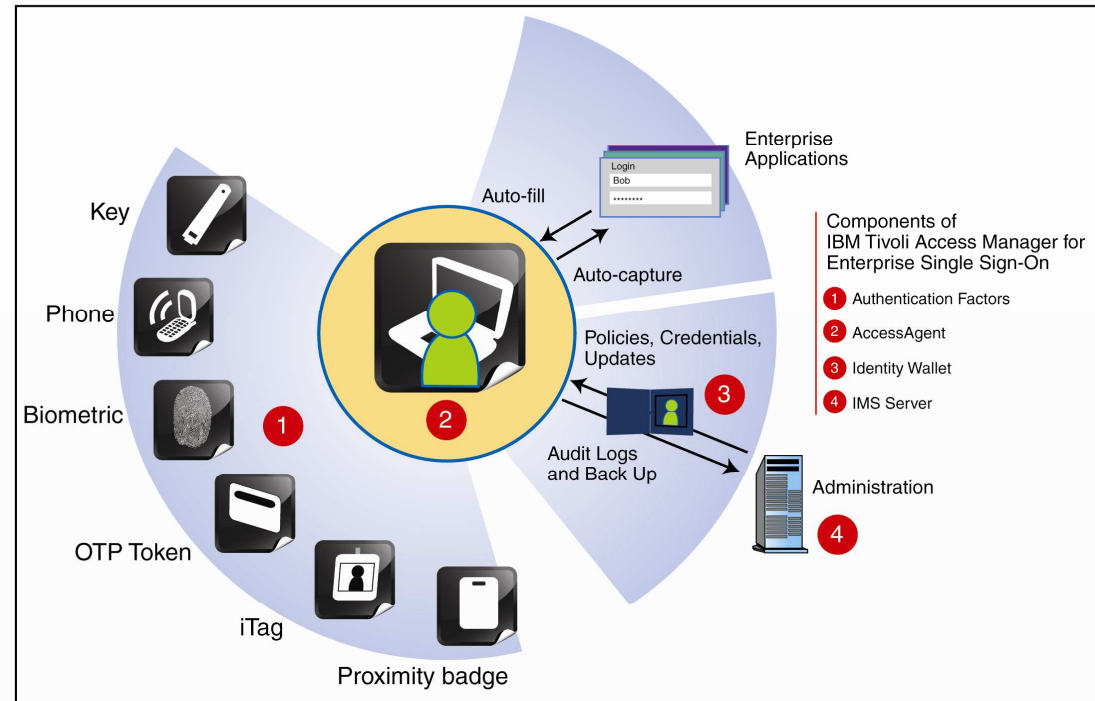
**Approval
Routing**



Tivoli Access Manager for Enterprise Single Sign-On

TAM E-SSO provee:

- Enterprise SSO
 - Autenticación de Doble Factor
 - Workflows Automatizados para Seguridad y Acceso
 - Estaciones de trabajo compartidas
 - Auditoria y seguimiento de uso de aplicaciones por usuario
 - Gestión centralizada
- Sin ningún cambio en la organización



TAM E-SSO provee *visibilidad* de la actividad de los usuarios, *control* sobre los accesos a los recursos, y *automatización* en el proceso de SSO para entregar un valor significativo hacia nuestros clientes.

¿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



» 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)



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



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

Thank
YOU



Por Un Mundo Más Inteligente
La Gente Lo Quiere
Nosotros Lo Hacemos