Estrategia de CiberSeguridad

TM

Abril 2015

Panorama de Amenazas

Ciber Espionaje

Fuente: Reporte de Investigación de Amenazas de Verizon en el 2014

Ataques de espionaje cibernéticos seguirán aumentando en frecuencia. Jugadores a largo plazo se convertirán en sigilosos información recolectores mientras que los recién llegados buscarán maneras de robar dinero e interrumpir sus adversarios.

En 2013, hubo 511 incidentes totales de espionaje cibernético, incluyendo 306 con la divulgación de datos confirmada.

Figure 58.
Variety of external actors within Cyber-espionage (n=437)

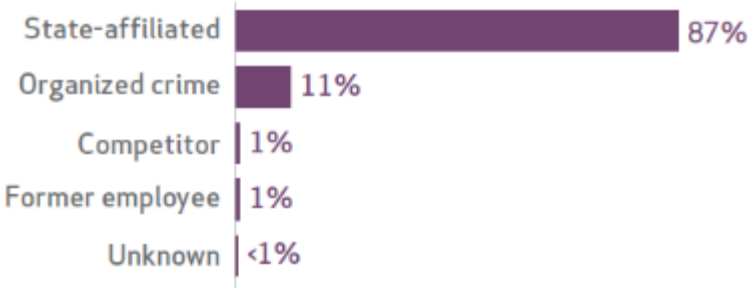
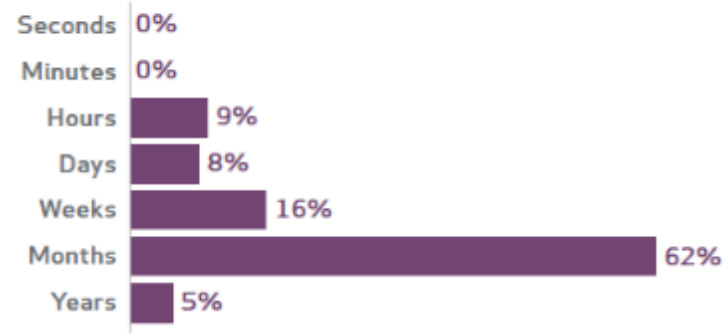


Figure 64.
Discovery timeline within Cyber-espionage (n=101)



Source: Verizon 2014 Data Breach Investigations Report

Panorama de Amenazas

Internet de las Cosas (IoT)

Ataques a los dispositivos del Internet de las Cosas aumentarán rápidamente debido a hipercrecimiento en el número de objetos conectados, la falta de higiene de seguridad, y el alto valor de los datos en estos dispositivos.

En un reciente estudio del dispositivos IoT

- 70% Contenían brechas de seguridad
- 25 Agujeros o riesgos de comprometer la red de casa, en promedio, encontraron para cada dispositivo
- 80% No requerían contraseñas complejas
- 90% recolecto al menos una pieza de información personal
- 70% Permite a un atacante identificar una cuenta válida través de la cuenta de enumeración

Source : McAfee, based on research by BI Intelligence, IDC, and Intel

Fuente : HP

Panorama de Amenazas

Privacidad de Datos

Protección de datos seguirá siendo objeto de ataques al igual que los gobiernos y las empresas continúan luchando con la definición de "información personal".

Cerca de 110 millones de EstadoUnidenses - equivalente a alrededor del 50% de los adultos estadounidenses - han tenido sus datos personales expuestos de alguna forma en el último año.

Fuente: Financial Services Roundtable

91% piensan que los consumidores han perdido el control sobre cómo la información personal es recopilada y utilizada por las empresas.

80% utilizando los sitios de redes sociales están preocupados por los anunciantes o empresas el acceso a los datos que comparten en estos sitios.

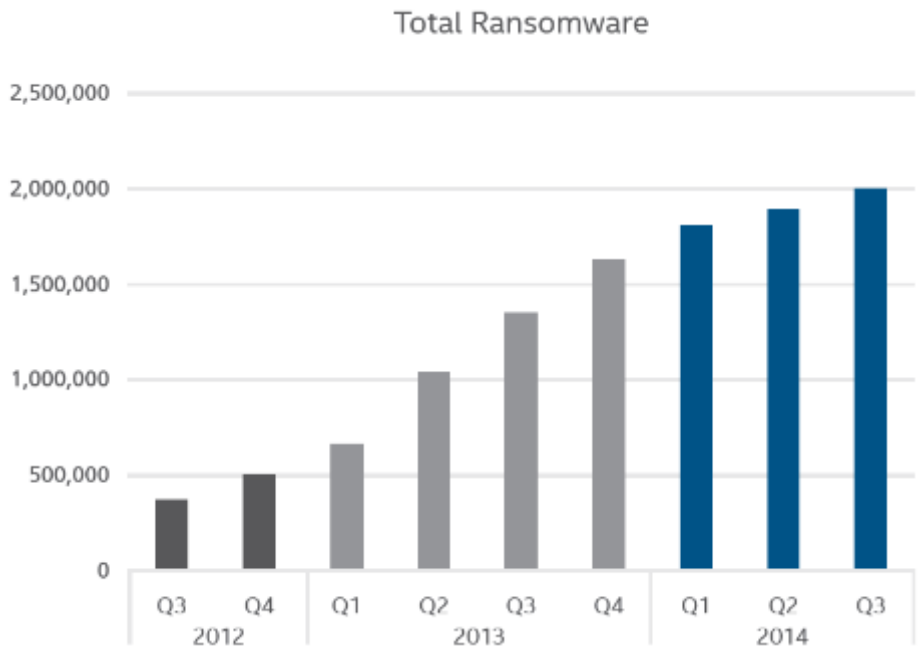
70% usando la red social tienen al menos algo preocupado por la información accediendo gobierno comparten sin su conocimiento.

Fuente: Pew Research Center

Panorama de Amenazas

Ransomware

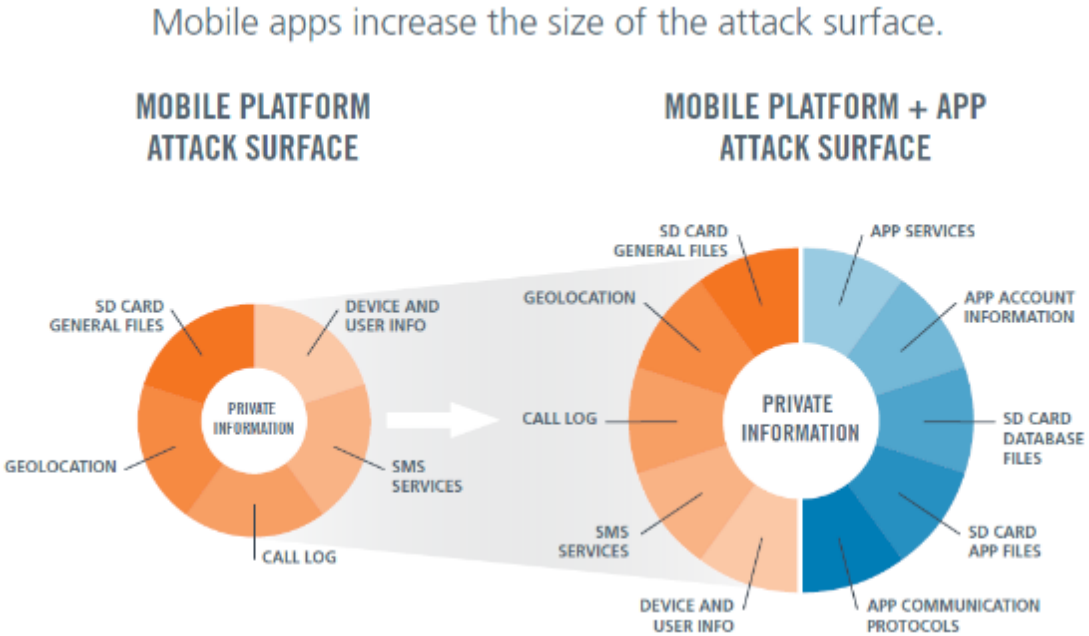
Ransomware evolucionará sus métodos de propagación, el cifrado y los objetivos que pretende. Más dispositivos móviles van a sufrir ataques.



Panorama de Amenazas

Dispositivos Moviles

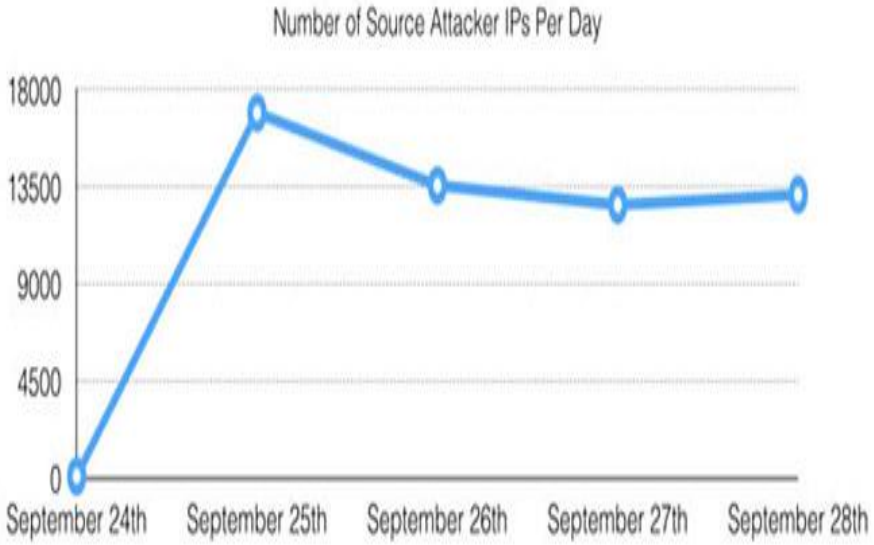
Ataques móviles seguirán creciendo rápidamente a medida que las nuevas tecnologías móviles amplían la superficie de ataque y poco se hace para detener el abuso tienda de aplicaciones.



Panorama de Amenazas

Malware más allá de Windows

Los ataques de malware que no sean Windows explotarán, alimentada por la vulnerabilidad Shellshock.



Source: Akamai

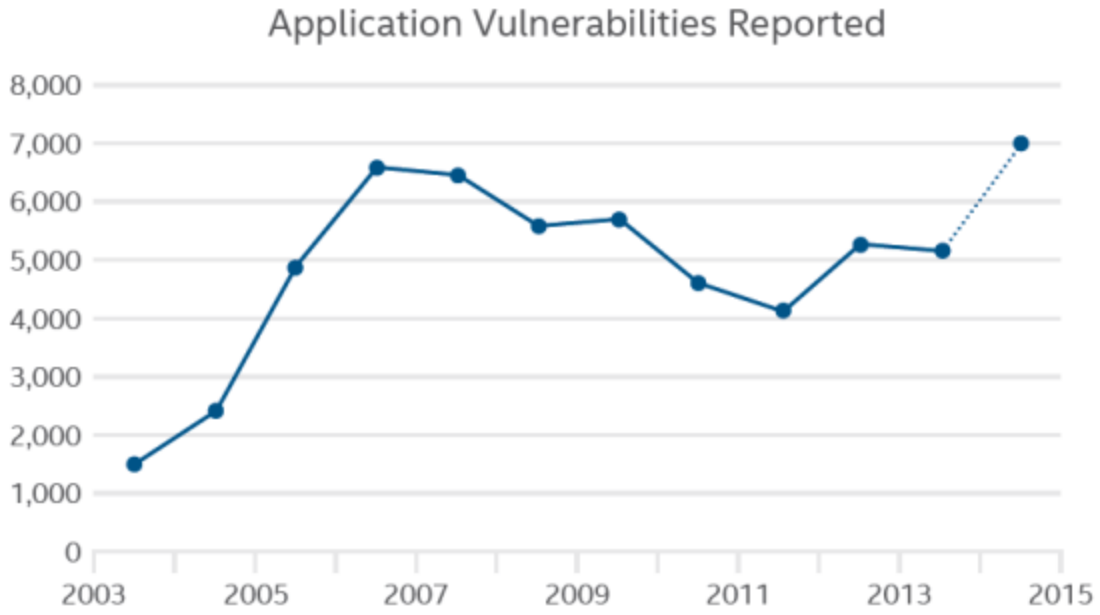
Partial list of device types that may contain Shellshock vulnerability:

- Servidores corriendo UNIX, Linux, y Mac OS X
- Apple Mac
- Routes (Con y sin Cable)
- Electrónicos como los TVs
- Controladores Industriales
- Sistemas de Vuelo
- Dispositivos que conforman las IC

Panorama de Amenazas

Vulnerabilidades

Las vulnerabilidades aumentarán a medida que el número de defectos en el software mas usado siguen creciendo.



Source: National Institute of Standards and Technology—National Vulnerability Database.

Tendencias Claves

“

Entre 5 y 9 nuevas amenazas cada segundo, o más de 500 por minuto.

”

Source: McAfee Labs

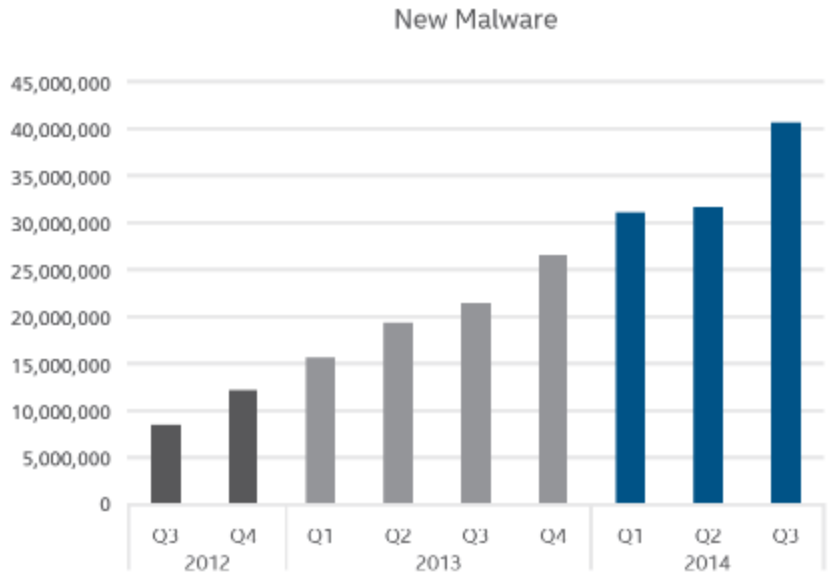
intel Security

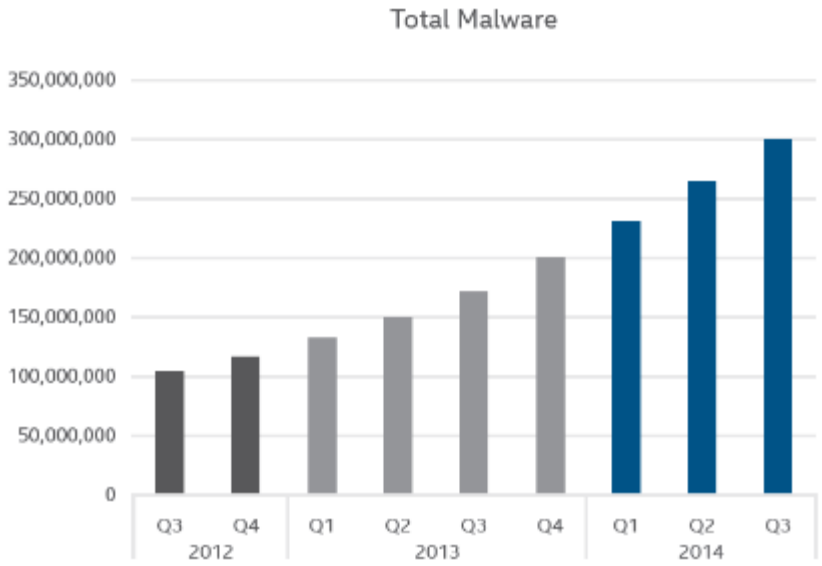
Tendencias

Malware

Hay más de 500 nuevas amenazas cada minuto, o más de 7 de cada segundo.

El Zoo de malware de McAfee Labs rompió la barrera de los 300 millones de la muestra en la Q3 de 2014, un crecimiento del 76% en el último año.

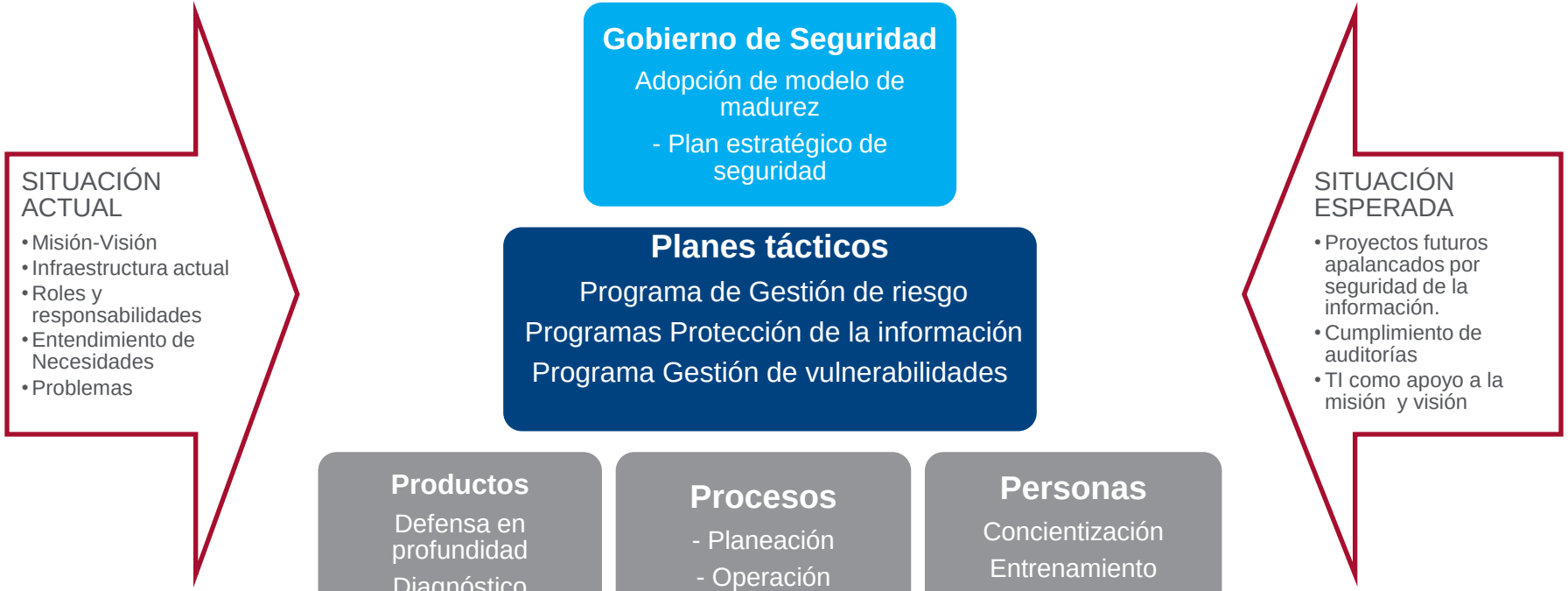




Source: McAfee Labs

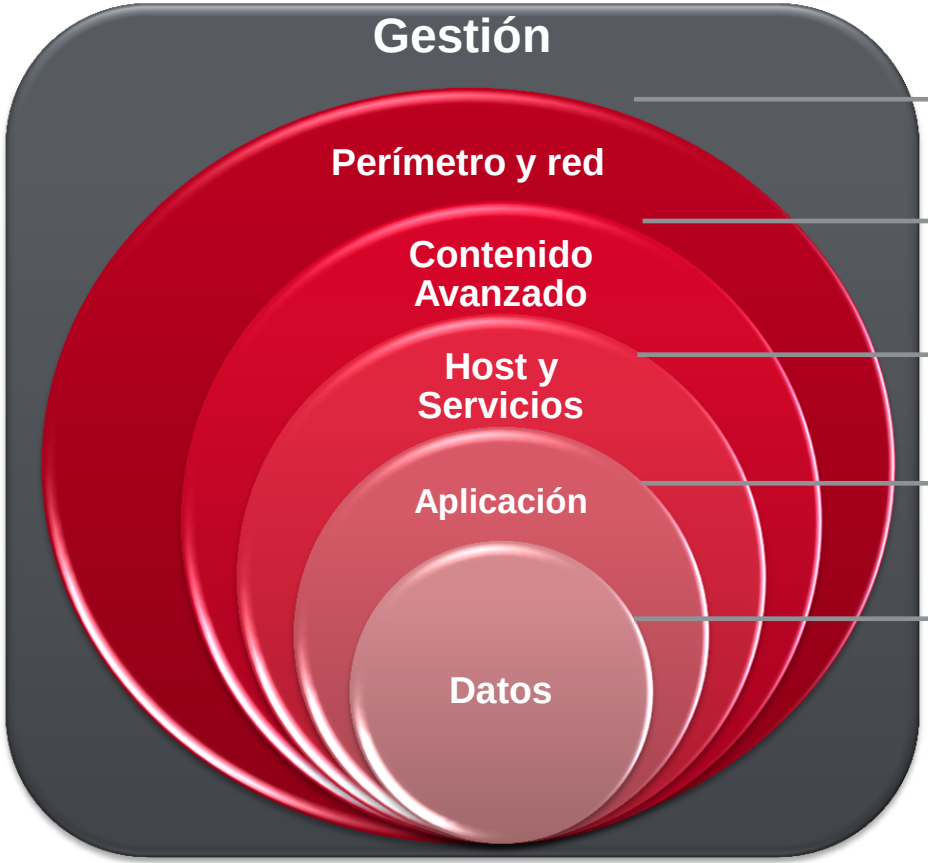
¿QUE BUSCAN LAS ORGANIZACIONES?

Alcance


SITUACIÓN ACTUAL
• Misión-Visión
• Infraestructura actual
• Roles y responsabilidades
• Entendimiento de Necesidades
• Problemas
Gobierno de Seguridad
Adopción de modelo de madurez
- Plan estratégico de seguridad
Planes tácticos
Programa de Gestión de riesgo
Programas Protección de la información
Programa Gestión de vulnerabilidades
Productos
Defensa en profundidad
Diagnóstico
Gestión
Procesos
- Planeación
- Operación
- Soporte
Personas
Concientización
Entrenamiento
Transferencia de conocimiento
SITUACIÓN ESPERADA
• Proyectos futuros apalancados por seguridad de la información.
• Cumplimiento de auditorías
• TI como apoyo a la misión y visión

Anillos de seguridad tecnológica

Defensa en profundidad



Visibilidad, monitoreo y correlación
Alertas tempranas y nivel de riesgo

Control de acceso y anomalías
Segmentación y filtros de tráfico de red

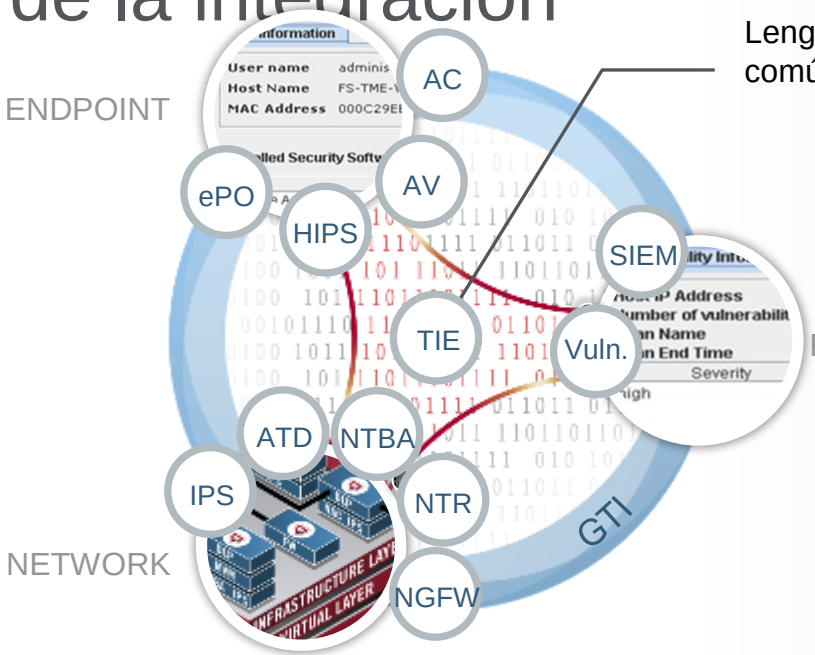
Detección de amenazas avanzadas persistentes e inteligencia adaptativa

Protección de estaciones finales y servidores (contexto local)

Protección de aplicaciones (Aplicaciones claves)

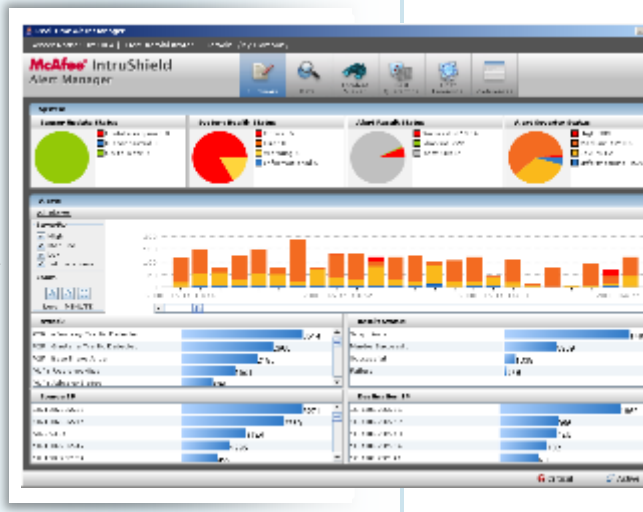
Autenticación y acceso seguro
Clasificación y control de información sensible

Valor de la integración



Lenguaje común

RIESGO



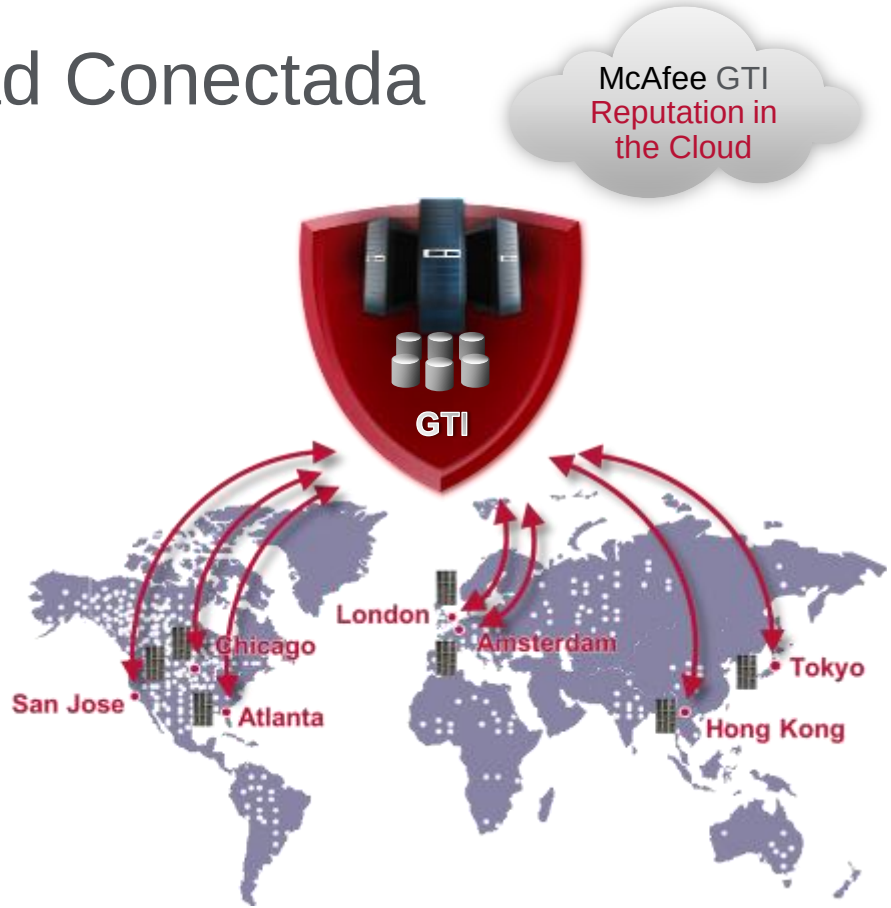
Tecnologías de seguridad interconectadas	Inteligencia en las soluciones	Respuesta y entendimiento en tiempo real

Ecosistema de Seguridad Conectada

McAfee GTI Integration

Responder a la información de amenazas globales en tiempo real, incluyendo la información de McAfee Labs

- Reputación de Archivos
- Reputación de URLs
- Categorización Web
- Reputación de Mensajes
- Reputación de Ips
- Reputación de la Certification



El Portafolio

Construyendo Seguridad por Silos

El proceso de adquisición de Tecnología ha generado caos en la seguridad.

McAfee – Vistazo Completo de la Seguridad

Socios de Negocios – McAfee (SIA)

McAfee Security Innovation Alliance

SIA Associate Partner
SIA Technology Partner
(McAfee Compatible)

Seguridad “Adentro”

Clientes Alrededor del Mundo en todas las Industrias

Lo que el mercado dice acerca de McAfee

“

Es bueno ver a McAfee enfocandose en **el empoderamiento de las empresas**, no solo en seguridad.

- Stephanie Balaouras
Forrester

”

La Solución al problema por Segmento

Soluciones para Salud

- Detección y prevención de acceso no autorizado
  - Administración de riesgos en el sector salud
- Seguridad a dispositivos móviles
  - Protección para mantener la integridad en el flujo del proceso de los datos
- Seguridad de los dispositivos médicos
  - Desde la integración directa con el fabricante de estos hasta la protección de los dispositivos ya adquiridos.

Entendiendo al Sector SALUD en materia de TIC

Hospitales Públicos	• Protección de Datos (Pacientes y Plantilla laboral) • Cumpliento de Regulaciones (NOMS, LFDP) • Asegurar dispositivos médicos y aprovisionar un acceso seguro a los mismos
Oficinas Administrativas	• Protección de Información (Planes estratégicos, iniciativas, tratados internacionales, etc.,) • Expediente Clínico electrónico
Hospitales Privados	• Protección de Datos • Cumplimiento Regulaciones (PCI, LFDP) • Expediente Clínico Electrónico
Laboratorios	• Propiedad Intelectual • Protección de Información • Cumplimiento Regulaciones

¿Cuál es la necesidad?

Diferentes organizaciones, necesidades similares

Protección de la Información

Cumplimiento de Regulaciones

Seguridad Conectada

Seguridad flexible y adaptable


intel
Security