Enterprise network security starts here.

Protección contra ataques internos

Malware APT & RAT

Miguel Llerena
Director, Alliances & Channels

PFU
a Fujitsu company

Quien es PFU?, a FUJITSU Company

- **PFU Systems, a Fujitsu company**, con base en Sunnyvale, California, USA y la central en Yokohama, Japón. PFU Systems es una la grandes subsidiarias of Fujitsu, facturando cerca de $1.2B de dólares al año.

- **PFU Systems** tiene mas de 20 años diseñando productos de networking, seguridad, Enterprise software y escáners corporativos para Fujitsu.

- **PFU Systems** comercializa sus productos en Las Américas via distribución y socios certificados. Para mas información visitenos www.inetsec.com

Que buscan los Ciberpiratas?

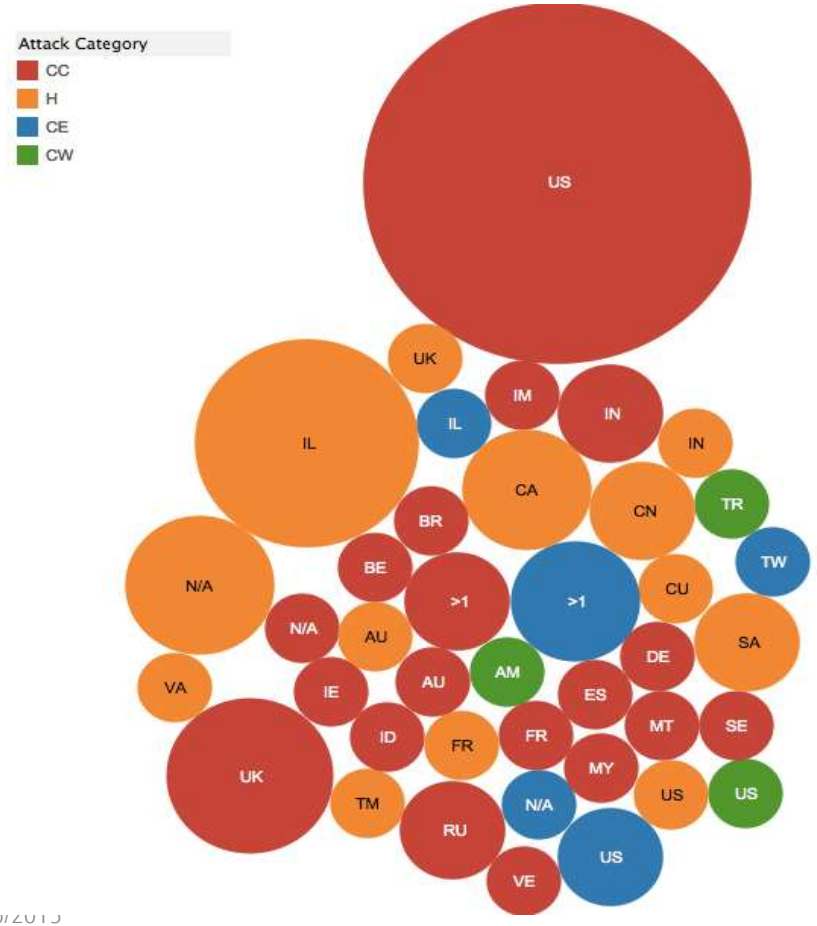
Tarjetas de Crédito, Cuentas Bancarias, Datos Privados del la Organización, Patentes, Formulas de producto, Información Personal, Historiales Médicos, Registros de Estudiantes, Secretos Militares, etc.

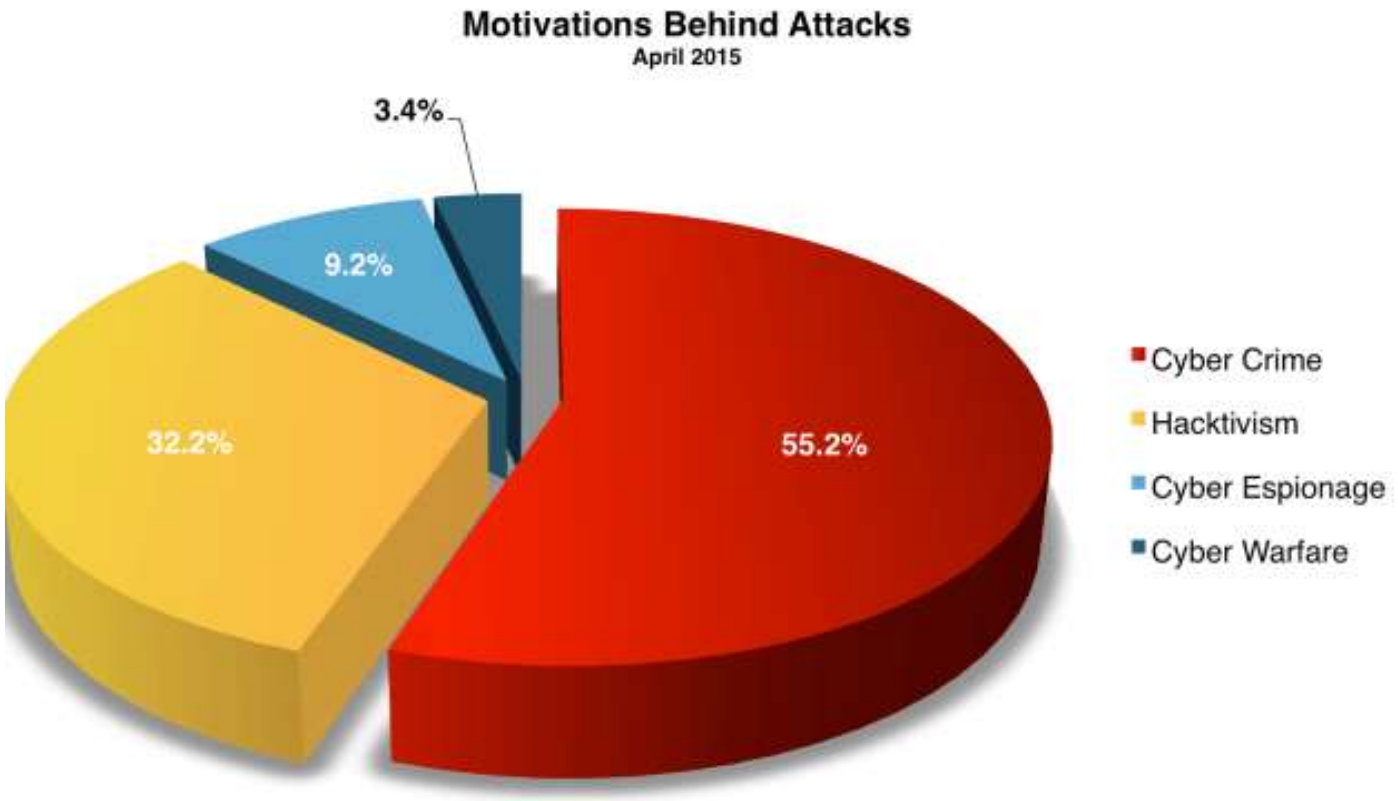
Por ejemplo - Cuanto cuesta un historial medico en el Mercado negro?

El FBI estima que un historial medico de un paciente puede valer 10 veces más que los números de tarjetas de crédito de la misma persona en el mercado negro. Su valor esta estimado entre $ 10 a $ 20 por historial medico.

Cyber Attacks – Donde? Cuantos? De que tipo? Motivación?

- Millones de ataque diarios – algunas instituciones en USA reciben hasta 20M de ataques al mes
- Costos a la economía mundial en el 2014 – estimado en $400 billones de dólares
- Porcentaje de ataques que se originaron internamente – de un 60% a un 80%
- USA lidera la lista de países mas atacados
- Tipo de ataque mas frecuente? #1 - Cyber Crime 55.2%, #2 - Hacktivism



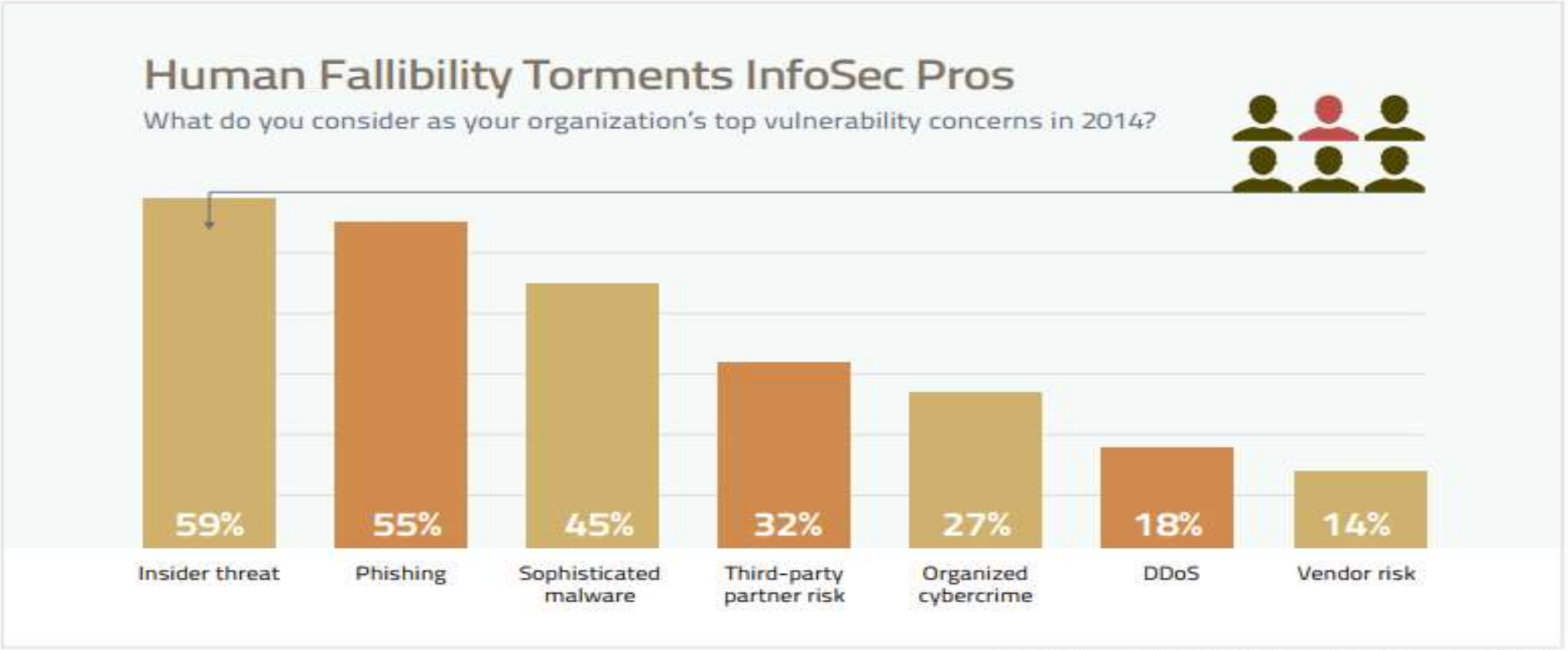


Origen de las amenazas?

INSIDER KILL CHAIN

According to a 2014 Wisegate member survey, insider threats topped the list of organization's vulnerability concerns at 59%, followed by phishing at 55%. Third-party partner risk ranked fourth, at 32% (after malware, at 45%). The senior IT and security professionals who were surveyed also reported concern about finding the staff to fight these threats.

Insider threats range from current and former employees to contractors and business partners with authorized access to networks and critical data systems. They



SOURCE: WISEGATE, APRIL 2014; RESPONDENTS COULD SELECT MULTIPLE CONCERNS

Nadie se salva de los ataques APT

- El costo de los ataques internos sobrepasa a los ataques externos.[2]

"What companies do is look for attacks at the perimeter, but the adversaries are inside the perimeter" said NSA Deputy Director. Sources: [1],[2] CSI San Francisco

- Soluciones de seguridad perimetral y protección de dispositivos (AVs) no son suficientes para proteger la red corporativa contra ataques APT

"The bad news is that we discovered an advanced attack on our own internal networks. It was complex, stealthy, it exploited several zero-day vulnerabilities, and we're quite confident that there's a nation state behind it."
Source - Kaspersky's website

ABC NEWS: OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected For More Than A Year, Sources Say
Jun 11, 2015, 4:59 PM ET, By MIKE LEVINE

The **hack of U.S. government employee records (aka the OPM hack)** was actuallydiscovered in a product demo. Attackers stole personnel data and Social Security numbers for every federal employee, a government worker union said Thursday, asserting that the cyber theft of U.S. employee information was more damaging than the Obama administration has acknowledged

Datos Interesantes sobre Malware APT

SURVEY DEMOGRAPHICS

1,500 Professionals worldwide participated in the survey. From tech service consultants, to people in the banking industry.

- **32%** From North America
- **19%** From Asia
- **38%** From Europe & Africa
- **8%** From Latin America
- **3%** From Oceania

AWARENESS

- **25%** Very Familiar
- **42%** Familiar
- **29%** Somewhat Familiar
- **4%** Not At All Familiar

93.6% OF RESPONDENTS UNDERSTOOD APTs ARE A VERY SERIOUS THREAT

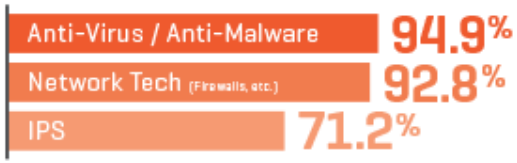
47% Respondents believed that APTs were a new and unique threat.

53% Respondents believed APTs are similar to what they've dealt with in the past.

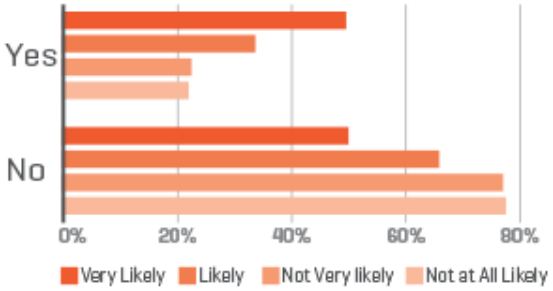
87% BELIEVE THAT JAILBREAKS, ROOTING & BYOD GREATLY INCREASE THE CHANCES OF AN APT OCCURRING.

63% BELIEVE IT'S ONLY A MATTER OF TIME BEFORE THEIR BUSINESS IS TARGETED.

How are people handling the threats?



Has your enterprise increased security training as a result of APTs?



Anatomía de un ataque APT

Vectores mas usados para ataques APT

1. **Los dispositivos no autorizados** en la red, tanto por cable e inalámbricos: computadores portátiles, tabletas, teléfonos inteligentes, puntos de acceso, seguridad física, computadoras de escritorio, ruteadores, servidores virtuales, NAS, juegos y otros

2. **El uso de aplicaciones peligrosas** en ambos dispositivos corporativos y personales en la red. intercambio de archivos p2p, streaming de medios de comunicación, juegos, intercambio de audio-video, redes sociales y otros

3. **APT (Ataques Persistentes Avanzados):** "avanzados" = técnicas sofisticadas que utilizan el malware (RAT) para explotar vulnerabilidades en los sistemas. "persistente" = un sistema de C & C externa está monitoreando y extrae datos de un objetivo específico de forma continua. "amenaza" = proceso con la participación humana en la orquestación de la attack.[1]

   Ataques APT disfrazan de comunicaciones rutinarias que son indetectables por las soluciones de seguridad en el mercado (por ejemplo, antivirus, protección contra intrusiones sólo firma, cortafuegos, etc.).

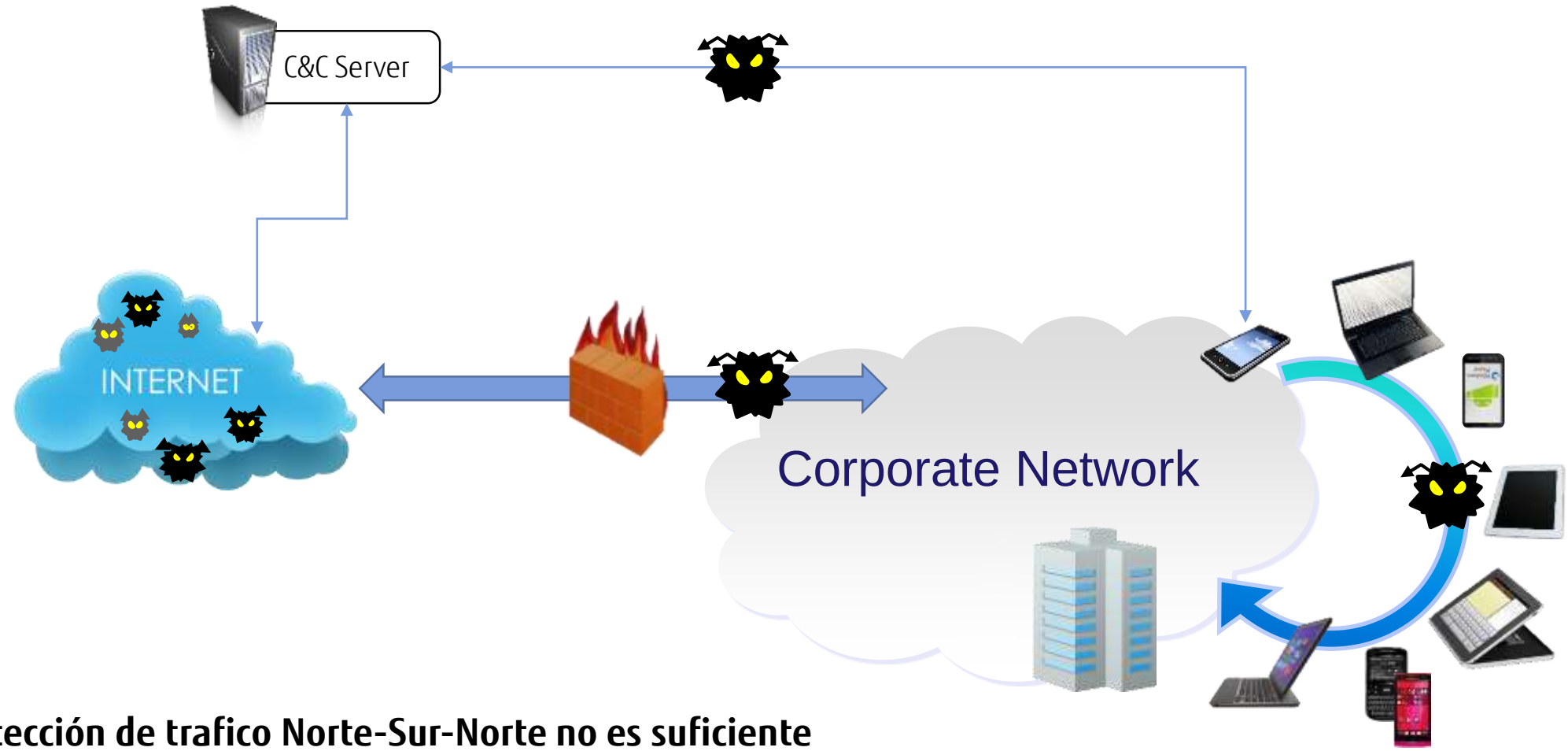
Sources: [1]Wikipedia

BYOD : Oportunidades y Riesgos

- Cerca de un 1 billón de dispositivos móviles fueron vendidos en 2013. En 2017 se espera que se lleguen a los 3 billones de dispositivos.[1]
- Los empleados están utilizando sus dispositivos tanto para fines personales y de trabajo. 4 de cada 5 empresas con políticas BYOD en su lugar han experimentado beneficios.[2]
- Escuelas, Universidades y Centros públicos (hoteles, hospitales, aeropuertos) han sido los primeros en adoptar BYOD (Bring Your Own Device)
- BYOD viene acompañado de BYOA (Bring Your Own Application) Presentando nuevos puntos vulnerables

Sources: [1]Frost&Sullivan, [2]Citrix

Corporate Network Security – New directions

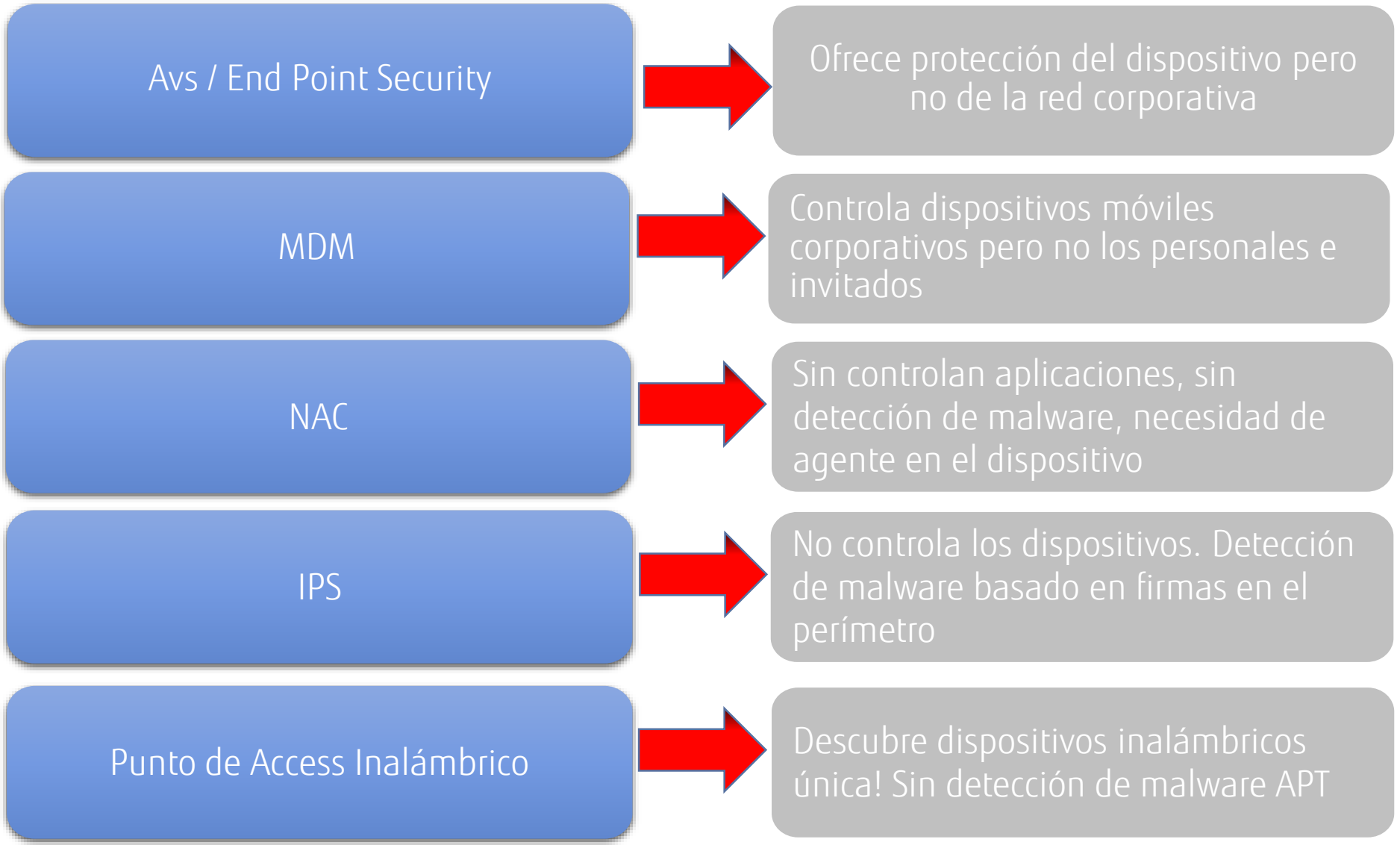


Protección de trafico Norte-Sur-Norte no es suficiente

Soluciones perimetrales no pueden proteger contra trafico este-oeste.

Contaminación en la red corporativa.

Posibles Technologias de Proteccion



Cual es la solución ideal?

Hacer frente a las amenazas internas de seguridad y movilidad se requiere un sistemas sofisticado que ofrezca visibilidad total quien y que esta presente en la red y su comportamiento.

- Un sistema que permita ver y gestionar todos los dispositivos de la red y hacer cumplir las políticas de seguridad de TI de la empresa y reaccione inmediatamente contra comportamientos extraños de los dispositivos.
- Un sistema que permita visualizar y controlar todas las aplicaciones y el uso de ancho de banda por dispositivo para prevenir el abuso de ancho de banda y la ejecución de aplicaciones de algo riesgo.
- Un sistema que sea capaz de analizar el comportamiento del tráfico de red creado por los dispositivos internos para detectar ataques APT y malware y correlación de tráfico norte-sur y oeste-este. Esta solución debe operar bajo tecnologías de algoritmos que analizan comportamientos.
- Una sistema que no afecte la productividad de la empresa implementado un rediseño de la red interna y la instalación de agentes en los dispositivos que creen conflictos en la red y los dispositivos.

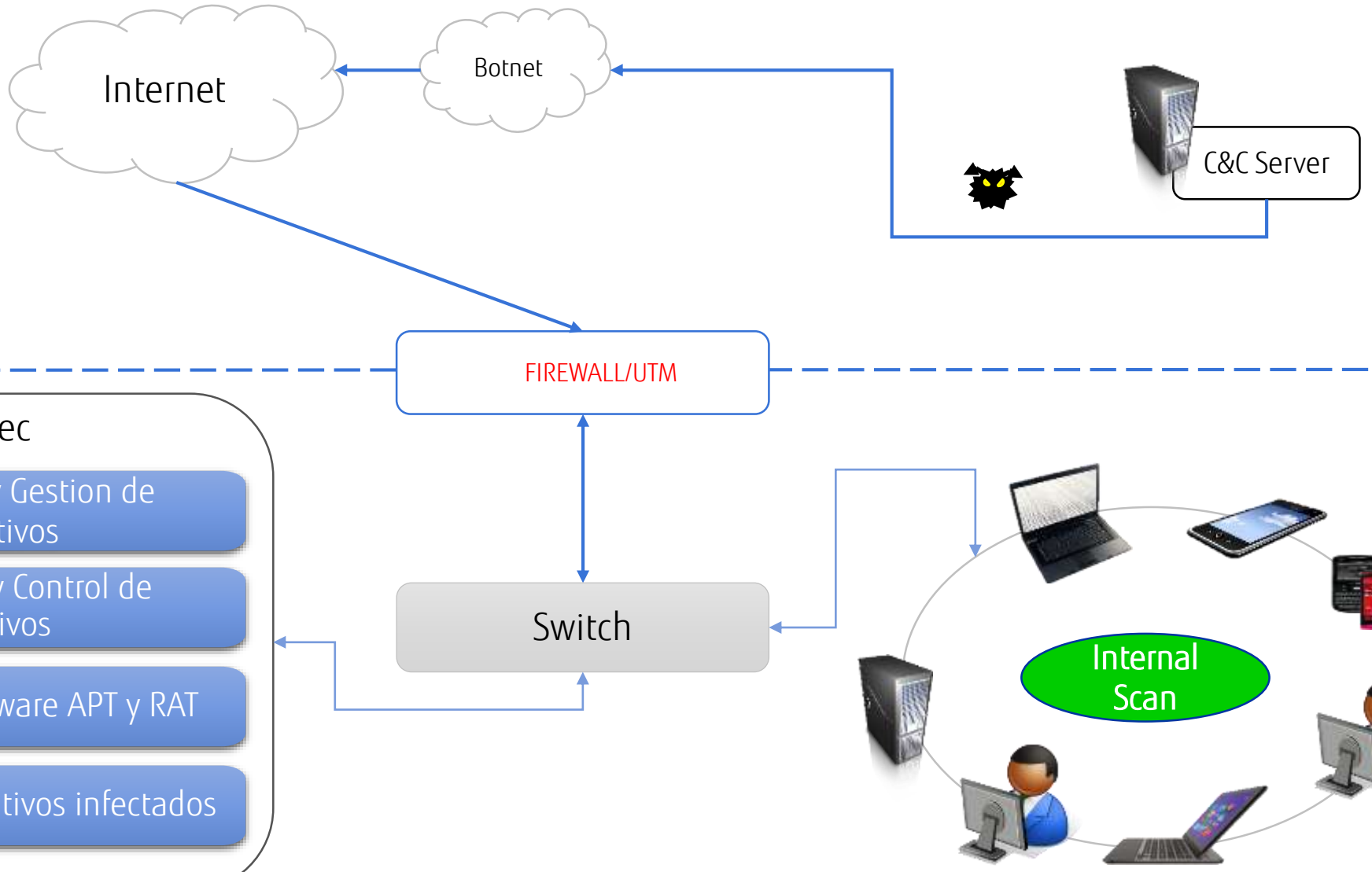
Las empresas están buscando una solución simple pero eficaz para resolver estos problemas, sobre todo para las empresas sensibles a los costes y, sin embargo sensibles a la seguridad.

Les invito a conocer “iNetSec Smart Finder”

PFU
a Fujitsu company

Internal Network Security
Appliance + Manager + Chart

Visualizar - Administrar - Descubrir - Reaccionar



Leaderes en Seguridad

Info Security Products Guide 2015 GLOBAL EXCELLENCE GOLD

Best 2015
Security Products and Solutions
for Healthcare, Education, Canada

Info Security Products Guide 2014 GLOBAL EXCELLENCE GOLD

Best 2014
Security Products and Solutions for
Education, Bring Your Own Device (BYOD)
Security, Intrusion Detection and Prevention

CTR Computer Technology REVIEW MVP AWARDS MOST VALUABLE PRODUCTS 2015

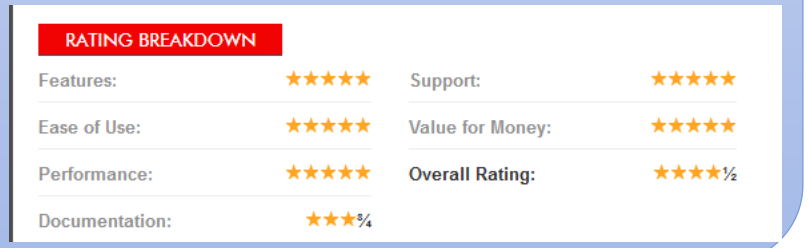
2015 Most Valuable
Networking Products


SC MAGAZINE NEWS PRODUCTS

PRODUCT INFORMATION

PFU Systems iNetSec Smart Finder

SC Magazine, 2014
"Strengths: Powerful features, excellent price."


RATING BREAKDOWN

Features:	★★★★★	Support:	★★★★★
Ease of Use:	★★★★★	Value for Money:	★★★★★
Performance:	★★★★★	Overall Rating:	★★★★½
Documentation:	★★★¾		

Best of Show at InterOp Japan.
"June 20135 Best Security Solution"

INTEROP BEST OF SHOW AWARD 2015 Grand Prize

!Gracias!

Visitenos @ www.inetsec.com

PFU
a Fujitsu company