



Soluciones de seguridad Cisco para la Prevención de Fuga de Datos



Daniel Marín Sanuy

Ingeniero de Sistemas

26/02/09

Agenda

Prevención de fuga de datos

Un problema para los negocios

Casos de uso

Tecnología y soluciones Cisco

Resumen



Agenda

Prevención de fuga de datos

Un problema para los negocios

Casos de uso

Tecnología y soluciones
Cisco

Resumen

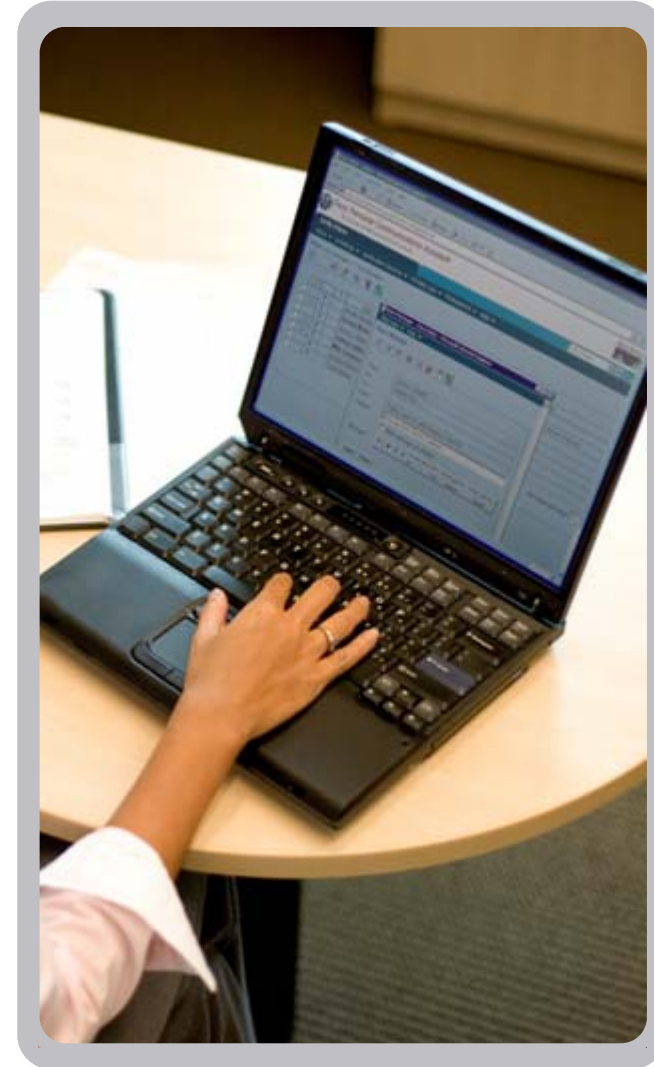


Estadísticas en Prevención de Fuga de Datos

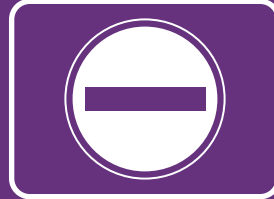
- Los datos de negocio están en continuo crecimiento*
 - El volumen de datos se duplica cada 3 años
 - En 2010: tamaños zettabyte (1 ZB=1021=1 trillón GB)
- Más datos son perdidos/robados**
 - 2006: 50 millones de datos
 - 2007: +160 millones de datos
- Terminales más potentes y con mayor riesgo en contenidos
 - Un portátil con disco de 80MB puede alojar unos 6.000 documentos Word, 720.000 correos, o 360.000 datos personales
- La normativa ISO 27002 contempla dentro de los objetivos de seguridad que cubre la Protección de Fuga de datos

*Fuente: 23 Julio, 2007, Forrester Report "Data, Data Everywhere!"

**Attrition.org: Data Loss Archive and Database



Clasificación actual de amenazas de seguridad desde el punto de vista del Responsable de IT



- 1 Troyanos, Virus, Gusanos y Otros Códigos Maliciosos
- 2 Spyware (código espía)
- 3 Spam (correo basura)
- 4 **Error de Empleado (No intencionado)**
- 5 Piratas informáticos
- 6 Vulnerabilidades en Aplicaciones
- 7 **Robo de datos por empleados o socios de negocio**
- 8 Despliegue de nuevas Tecnologías
- 9 Accesos inalámbricos (WiFi)
- 10 Sabotaje interno

IDC IPC Report 2007, #206750

¿Dónde está mi dispositivo USB?

- Más de la mitad (52%) de los responsables de toma de decisiones corporativas han perdido datos confidenciales a través de dispositivos USB en los últimos 2 años
- La pérdida de datos en dispositivos USB es la mayor preocupación (72%) de seguridad de los Responsables de Seguridad de Datos, seguido de los ataques por Troyanos, spyware y otros virus



64 Gig
de datos

¡más pequeño
que un paquete
de chicles!

Fuente: Forrester Research

Solución Cisco para Prevención de Fuga de datos

¿Qué es la solución Cisco para Prevención de Fuga de datos?

- La solución de Fuga de datos de Cisco provee de una estrategia para prevenir la pérdida de datos incluyendo:
 - Riesgos de acceso: control de acceso a datos, incluyendo personas, procesos, y tecnología
 - Refuerzo en políticas de seguridad de contenidos para prevenir pérdidas de datos de negocio en puntos de alto riesgo (correo electrónico y portátiles)
 - Seguridad perimetral y control de acceso a redes de datos, aplicaciones, servicios de colaboración, y localizaciones físicas; seguridad inalámbrica; encriptación de datos en cintas; refuerzo en las políticas de acceso de usuarios

Agenda

Prevención de fuga de datos

Un problema para los negocios

Casos de uso

Tecnología y soluciones
Cisco

Resumen



Principales Áreas de Riesgo en la Fuga de Datos

CSA
NAC
Ironport

Datos en Movimiento (Control de Acceso)

Correo, MI, Web, FTP, WiFi

- Control información sensible y su uso
- Encriptación
- Bloqueo condicional
- Educación del empleado
- Control de las comunicaciones

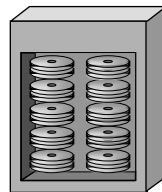


MDS
CSA
NAC

Datos almacenados

Bases de Datos, Cintas

- Encriptación en almacenaje y cintas
- Prevenir accesos no autorizados en sistemas de Centro de Datos



CSA
NAC
WAFS

Datos en Uso

Terminales

- Prevención de uso de información sensible (p.e: USB)
- Protección sin conectividad
- Educación del empleado



CSA
NAC
Ironport

Acuerdos Regulatorios

- PCI – Información tarjetas de crédito
- HIPAA – Información Médica
- GLBA – Información Financiera, etc



VISA



Datos en Movimiento / Control de Acceso

Pérdida de Datos por una red inalámbrica insegura

Protección contra robo de datos por accesos de usuarios no autorizados a la red interna a través de infraestructura inalámbrica insegura

Escenario

Más de 45M de Nos.de tarjetas de crédito fueron robadas y utilizadas para compras por valor superior a \$8M. Los ladrones accedieron a los datos a través de dispositivos portátiles, cajas registradoras y computadoras de las tiendas a través de una red inalámbrica insegura con encriptación obsoleta y sin cortafuegos ni seguridad en los datos guardados en las computadoras.

Mayo 2007 www.wallstreetjournal.com



Solución Cisco

- Cisco Wireless LAN Controller ofrece conectividad segura para evitar grietas en la infraestructura inalámbrica
- Cisco Wireless Control System detecta puntos de acceso y usuarios inalámbricos no autorizados para proteger la red ante el acceso de dispositivos no reconocidos
- Cisco NAC refuerza la seguridad de los sistemas conectados a la red para que accedan sólo donde estén autorizados según la política de seguridad en red

Datos en Movimiento / Control de Acceso

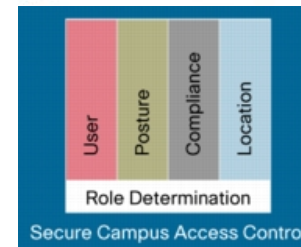
Fuga de Datos por compartición de ficheros

Prevenir Fuga de Datos por accesos no autorizados a dispositivos de compartición de ficheros

Escenario

Datos de empleados de una compañía de impresión fueron eexpuestos inadvertidamente, incluyendo Nos.de la Seguridad Social, fechas de nacimiento, nombres y direcciones, cuando fueron accedidas desde dos dispositivos con direcciones IP desconocidas. Los datos de empleados fueron cargados en un servidor de ficheros utilizado para compartición de ficheros entre socios de negocio.

Febrero 2008 <http://www.privacyrights.org>



Solución Cisco

- Cisco TrustSec, integrado en todos los conmutadores Cisco Catalyst, provee protección de fuga de datos en base al control de Identidad para el acceso y el control de aplicaciones y recursos sensibles de red, incluyendo servidores de ficheros
- El cortafuegos y terminador de VPN Cisco ASA puede restringir el acceso a bases de datos internas a socios y empleados autorizados

Datos en Movimiento / Control de Acceso

Fuga de datos desde Accesos a red Remotos

**Prevenir la Fuga de Datos desde Accesos remotos
No autorizados o No encriptados**

Escenario

Un análisis de vulnerabilidad en un hospital del sur de California reveló que algunos doctores eran capaces de conectarse a sus computadoras desde su casa vía Internet por RDP (no VPN) y eran capaces de ver datos de pacientes por un canal inseguro y sin encriptación.

Octubre 2005 (Private Communication with Author)



Solución Cisco

- Cisco ASA soporta VPNs SSL e IPsec para autenticar y encriptar las comunicaciones de usuarios de accesos remotos
- Cisco Secure Desktop está disponible con Cisco SSL VPN para prevenir fuga de datos en:
 - Comprobando la localización/seguridad del terminal antes de establecer la conexión remota
 - Encriptando las descargas de ficheros durante una sesión
 - Realizando limpieza una vez finalizada la sesión. P.e: borrando ficheros temporales, historia de accesos a internet y facilidad de recordatorio de contraseñas
- Cisco NAC refuerza las políticas de seguridad controlando que todos los terminales conectados a la red vía VPN son equipos admitidos y controlados por la compañía y cumplen con las políticas de seguridad y actualizaciones

Datos en Movimiento / Control de Acceso

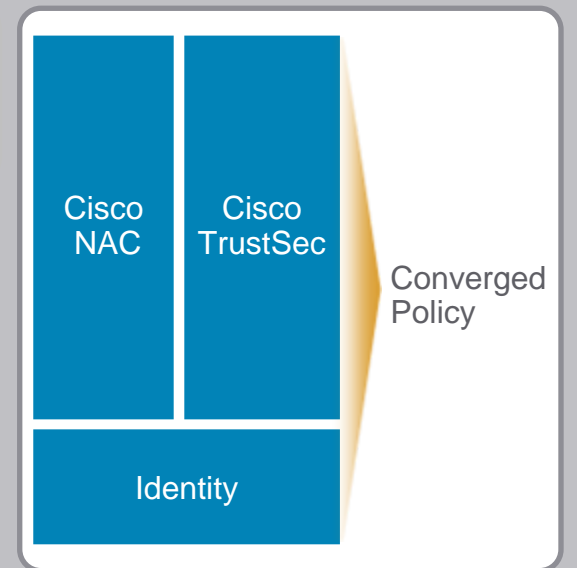
Accesos No autorizados a Bases de datos y servidores

Prevenir accesos a Bases de datos y servidores del Centro de datos por usuarios No autorizados, que puede resultar en robo de datos privados o confidenciales

Escenario

La habilidad del pirata informático Jérôme Kerviel para acceder a sistemas y servidores de empresas resultó en unas pérdidas valoradas en \$8B en accesos de un importante banco francés. Esto además tuvo consecuencias a nivel mundial por la desconfianza creada en los mercados de valores ante ataques de este tipo.

Enero 2008 (Multiple Reports)



Solución Cisco

- Cisco NAC controla y autoriza el acceso a redes que contienen datos sensibles
- Cisco TrustSec controla y autoriza el acceso a sistemas que contienen datos sensibles, desde servidores hasta portátiles
- Cisco Security Agent (CSA) previene el acceso a ficheros sensibles localizados en Bases de datos restringidas

Seguridad y Control de Acceso

Fuga de datos a través de aplicaciones Web

Prevenir la Fuga de datos por accesos No autorizados a aplicaciones Web

Escenario

Una compañía de realidad virtual descubrió que un pirata informático accedió a su base de datos de clientes a través de sus servidores web. Los datos afectados incluían nombres, datos de contacto, contraseñas e información de pagos que no estaban encriptados.

Septiembre 2006 <http://www.privacyrights.org>



Solución Cisco

Cisco ACE Web Application Firewall

- Protege contra ataques basados en aplicaciones/servidores Web, como ataques de diccionario, (XSS) ataques/SQL e inyección de comandos, que habitualmente son diseñados para interceptar o robar información de tarjetas de crédito vía aplicaciones Web
- Protege de la pérdida de datos sensibles, como Nos. de tarjetas, pasaportes, seguridad social, monitorizando y filtrando todo el tráfico de salida de los servidores

Datos Almacenados

Fuga de datos a través de dispositivos de almacenamiento

Prevenir la Fuga o Robo de Datos de dispositivos de almacenamiento encriptando los datos almacenados y controlando el acceso físico

Una gran compañía de almacenamiento perdió una cinta con datos perteneciente a GE Money que contenía información de tarjetas de crédito de aproximadamente 650.000 clientes. La cinta SIN encriptar además contenía los datos de Seguridad Social de unos 150.000 clientes. Ubo más de 230 empresas afectadas.

Enero 2008 www.informationweek.com



Escenario

Solución
Cisco

MDS 9000: Cisco Storage Media Encryption

- Provee de una solución segura para encriptar los datos en almacenamientos heterogéneos (discos, cintas...), dispositivos de almacenamiento SAN y librerías de cintas virtuales (secure AES-256)

Cisco Physical Security

- El control de acceso físico de Cisco provee de políticas de acceso basadas en políticas que utilizan la red IP. Si se detecta algún evento, Cisco Physical Access Control puede ser usado coordinadamente con el sistema de VideoVigilancia de Cisco para realizar y ver grabaciones de vídeo.

Datos en Uso

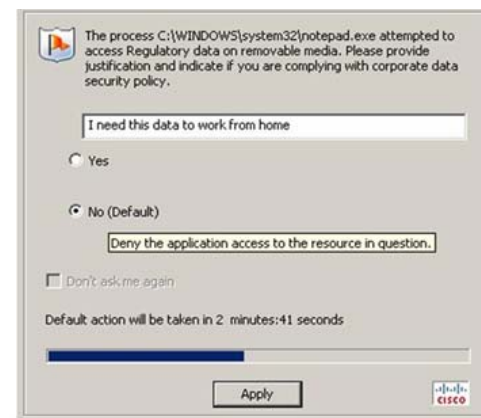
Fuga de Datos a través de dispositivos portátiles

Prevenir la transferencia de datos sensibles a través de dispositivos portátiles/removibles como discos externos, lápices USB, o CD/DVDs

Escenario

Una organización de salud británica reportó una pérdida de una memoria USB por un empleado con información confidencial médica y personal de 4.000 pacientes.

Diciembre 2007 <http://news.bbc.co.uk>



Solución Cisco

- Cisco Security Agent previene que ficheros que contienen datos sensibles o palabras claves puedan ser copiados a dispositivos removibles como memorias USB, CD/DVDs, discos externos...
- Cisco NAC previene el acceso no autorizado a la red que contiene datos sensibles
- Cisco TrustSec previene el acceso no autorizado a servidores que contienen datos sensibles

Datos en Uso

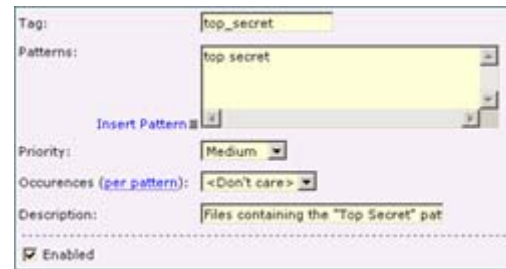
Fuga de Datos por mal uso de la copia del portadocumentos del escritorio

Previene la copia de datos sensibles a aplicaciones externas como Blogs, Redes Sociales o Mensajería Instantánea

Escenario

Una organización de salud norteamericana informó a 140 de sus asegurados que un empleado había publicado muchos de sus datos confidenciales en su blog. Esta organización fue una de las primeras multadas por violar la norma regulatoria en seguridad de datos HIPAA por el departamento de salud de california (DMHC).

Marzo 2005 www.computerworld.com



Solución Cisco

- Cisco Security Agent protege contra el abuso de copias del portadocumentos del escritorio, ya sea de manera intencionada o accidental, cuando algún dato sensible es copiado y pegado en una aplicación externa (como blogs o Facebook) o de Mensajería Instantánea

Agenda

Prevención de fuga de datos

Un problema para los negocios

Casos de uso

**Tecnología y soluciones
Cisco**

Resumen



Cisco ACE Web Application Firewall

Cisco ACE WAFS protege ante la Fuga de datos con:

- **Encubrimiento/mapeo de excepciones**

Previene trazas de stack u otras aplicaciones de datos internas para alcanzar a clientes a través de códigos de error sustituyendo un error de aplicación web por un error genérico

- **Respuesta ante re-escritura de contenido**

Filtra datos sensibles encontrados en respuestas, como Nos. de tarjetas de crédito, Nos. de Seguridad Social, etc. proveyendo de un “parche” virtual a las aplicaciones que publican los datos a través de respuestas erróneas, SQL Injections, u otros tipos de ataques.

- **Extenso listado de firmas validadas por Cisco para patrones conocidos de ataques maliciosos HTTP y XML**

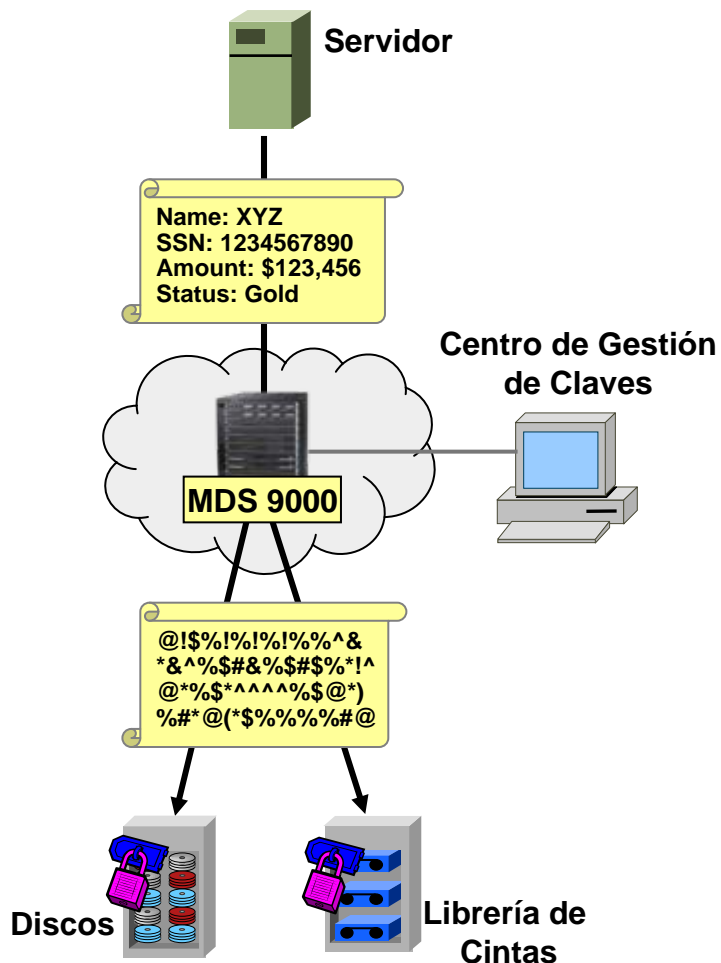
SQL Injection, buffer overflow, cross-site scripting, cooking & session poisoning, etc.



Beneficios para el Negocio:

- Protege contra fuga de datos privados o de propiedad intelectual que pueden ocurrir a través de aplicaciones web.
- Ayuda a las organizaciones a proteger la información sensible con seguridad PCI y políticas para datos privados

Cisco MDS 9000: Funcionalidad SME



- Provee la funcionalidad SME (storage media encryption) de encriptación para el almacenamiento de datos (AES-256) como un servicio de red (fabric) SAN
 - Ofrece un performance altamente escalable
 - Crypto-engine integrada en el módulo del conmutador: MSM
- Encripta los datos sobre sistemas de almacenamiento heterogéneos
- Simplifica la provisión y gestión de los volúmenes encriptados
- Securitiza y centraliza la gestión de claves SME
- Certificación FIPS nivel-3

Cisco Network Admission Control (NAC)



Funcionalidades

- Control de Acceso basado en reglas y políticas de seguridad en red con obligación de cumplimiento
- Ciclo completo: descubrimiento, valoración, refuerzo y obligación de cumplimiento, y remedio

Beneficios

- Securiza ambos dispositivos: gestionados (con usuario) y no gestionados
- Provee acceso a invitados y previene accesos no autorizados
- Reduce vulnerabilidades-basado en explotaciones

Despliegue Flexible

Layer 2, Layer 3
In-band, Out-of-band
Centralizado, Distribuido
SNMP, RADIUS

Servicios NAC Innovadores

Valoración de estado
Remedio
Perfiles
Invitados

Pero...¿Qué es Cisco NAC?

Network
Admission
Control

Mayor
criterio para
el control de
acceso que
un simple
“¿Quién
es?”

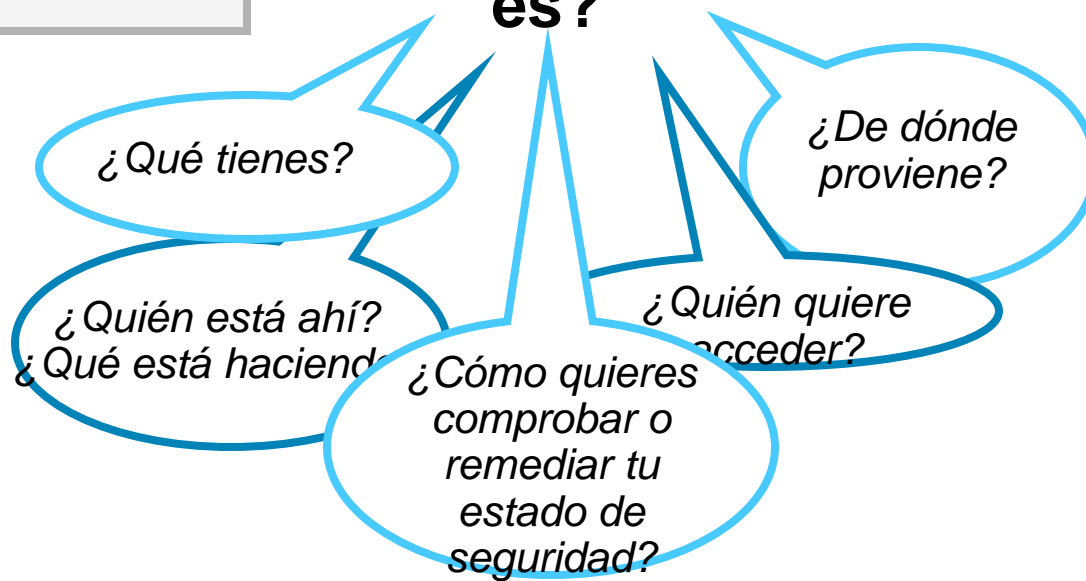
4 Funciones Principales

Autenticar
y Autorizar

Comprobar y
Evaluar

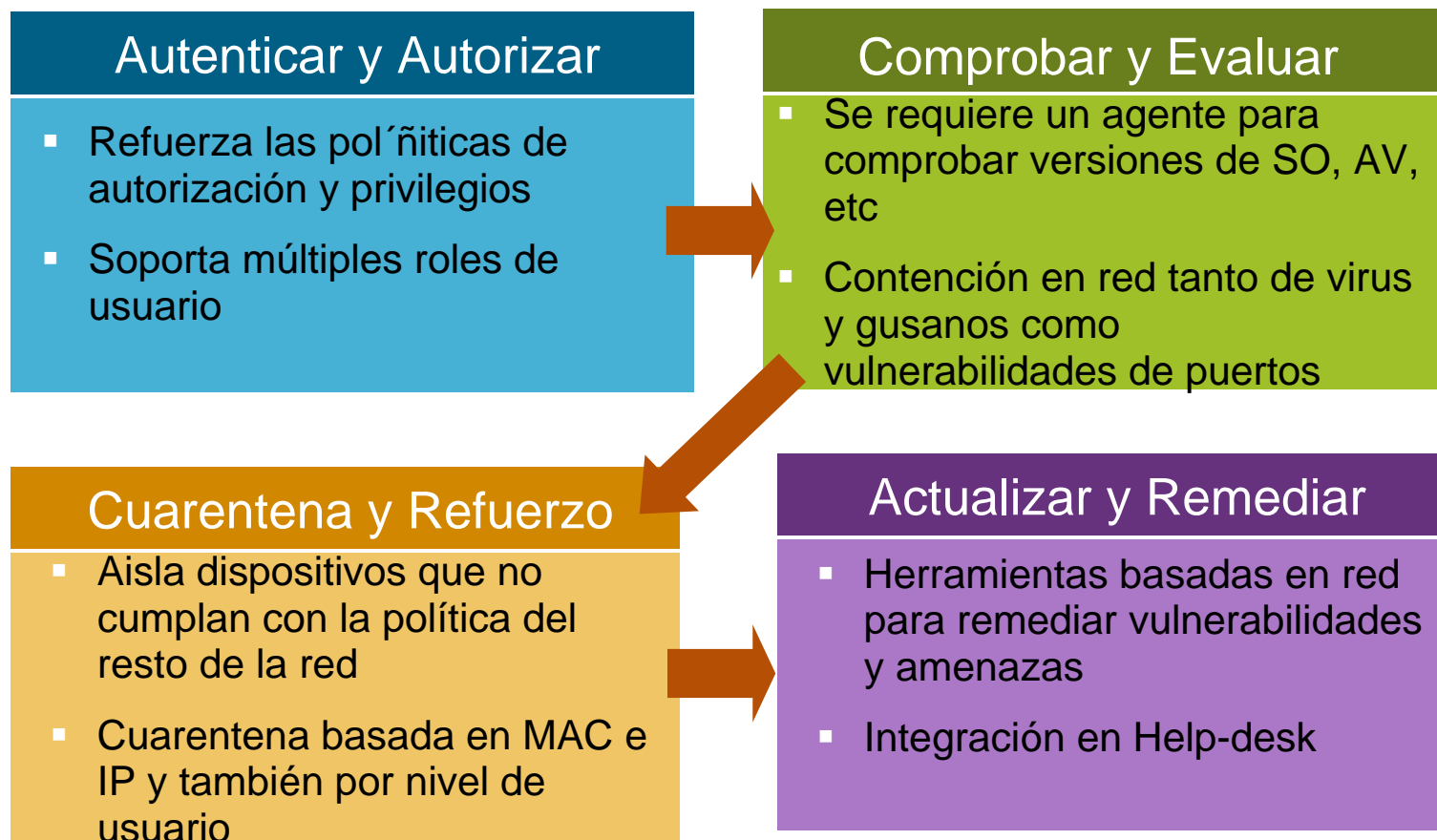
Cuarentena
y Refuerzo

Actualizar y
Remediar

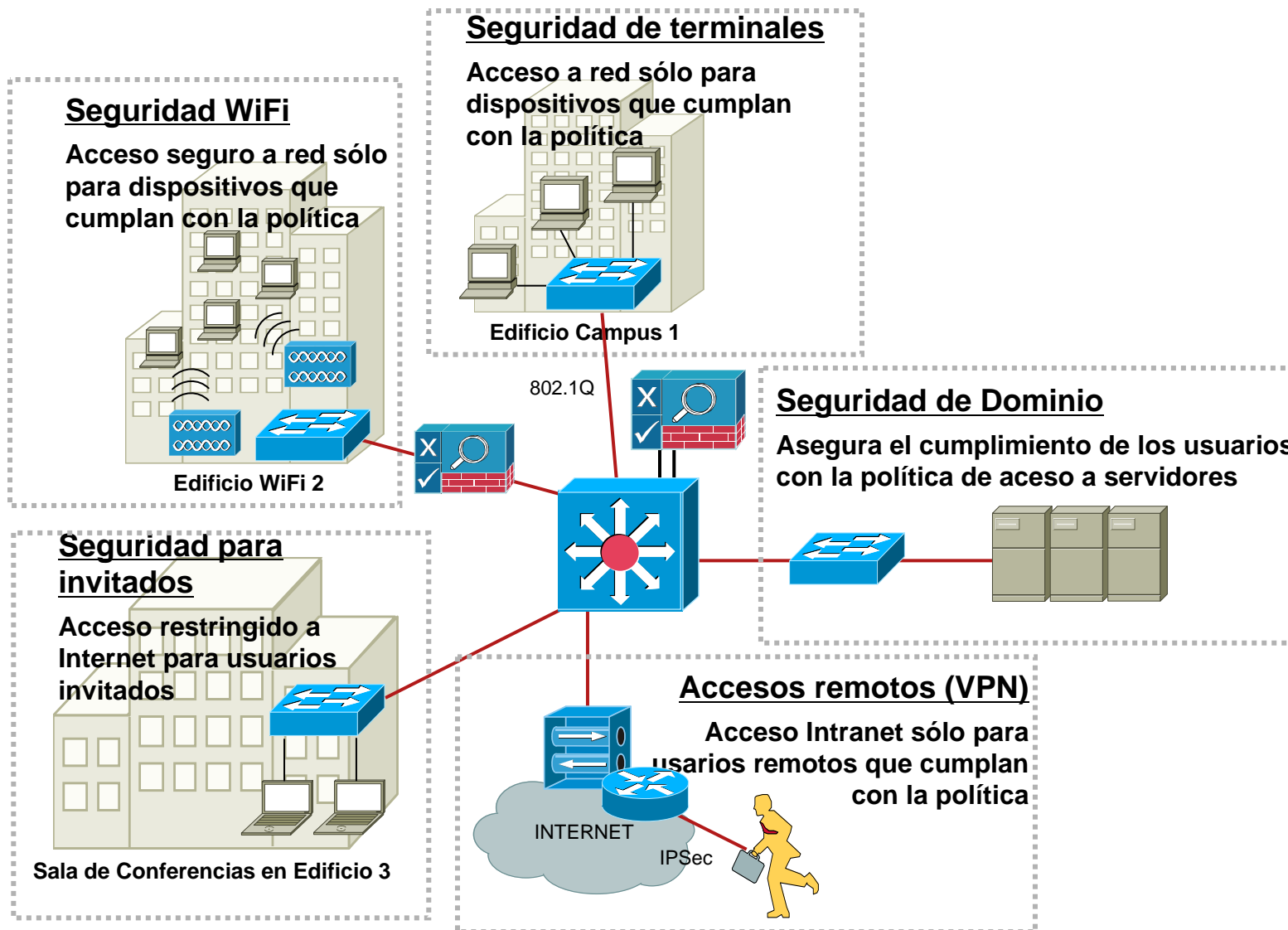


Definición de Cisco NAC: 4 Funciones

Usar la red como plataforma para reforzar la seguridad asegura que cualquier dispositivo que quiera acceder cumple con la política requerida.



Cisco NAC cubre la mayoría de casos de uso



Control de Acceso basado en Identidad (Dispositivo) Cisco NAC Profiler: Automatización



PCs	No-PCs			
	UPS	Tfns	Impres	WiFi

Es capaz de localizar y aplicar la política adecuada a cualquier tipo de dispositivo en la red

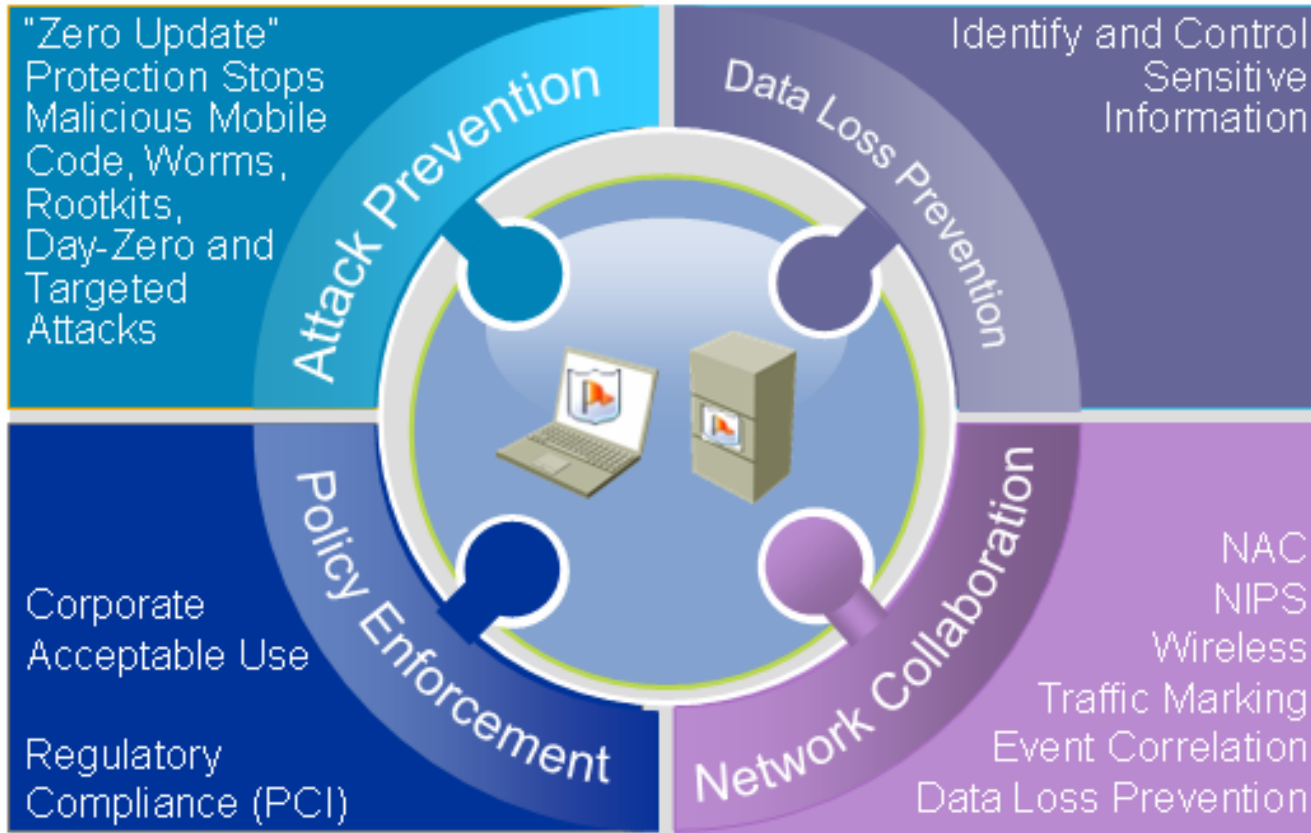
Descubre
Perfil de terminales
 Describe todos los terminales en la red por tipo y localización
 Mantiene un contexto en tiempo real e histórico de todos los terminales

Monitoriza
Monitorización de comportamiento
 Monitoriza el estado de los terminales en red
 Detecta eventos como MAC spoofing, port swapping, etc.

El proceso automático localiza y guarda la lista de dispositivos en el NAC Manager; y subsecuentemente, dentro de la política NAC adecuada

Cisco Security Agent

Seguridad "Siempre Vigilante" para terminales



Protección para Portátiles – PCs



Protección de servidores



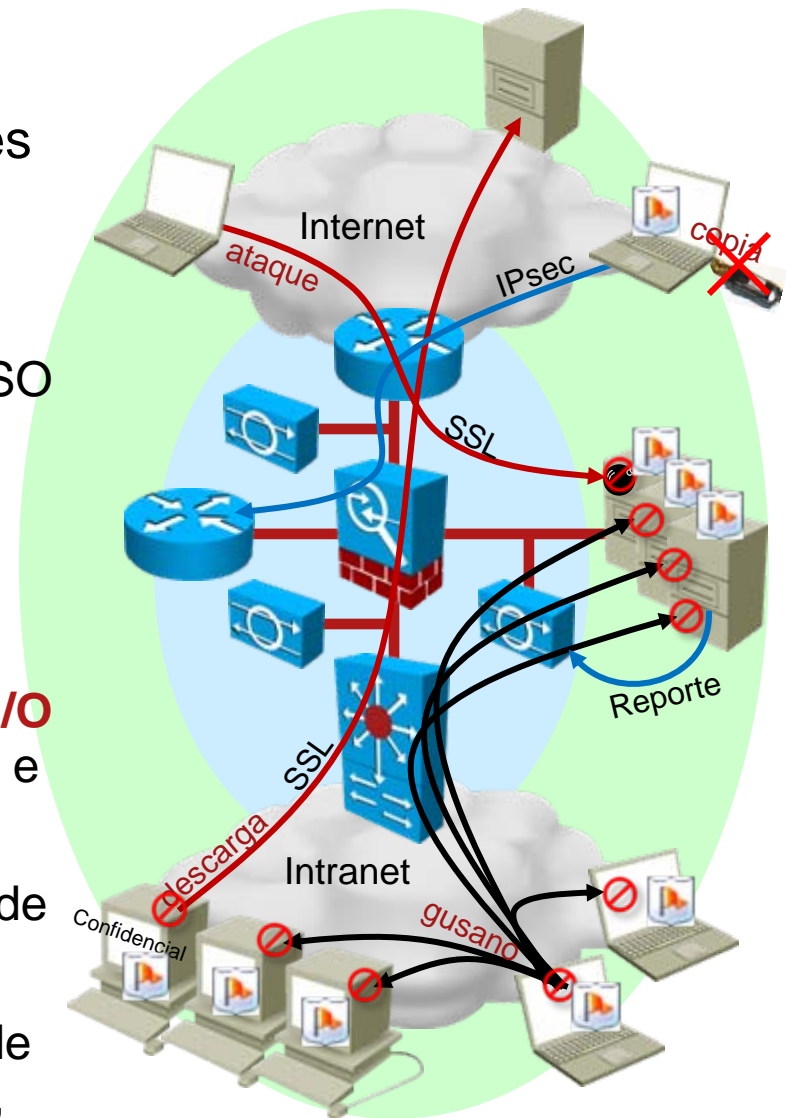
Protección POS

SINGLE INTEGRATED AGENT AND MANAGEMENT

Seguridad Avanzada de Terminales

con Cisco Security Agent

- CSA extiende las soluciones de seguridad de red hasta los terminales
- Cisco Security Agent mejora la seguridad con:
 - **Protección “Zero Update”** basada en SO y comportamiento de aplicaciones
 - **Control de contenidos** después de descifrar o antes de encriptar (p.e: SSL, IPsec)
 - **Control de Acceso para dispositivos I/O** basado en procesos, localización de red e incluso contenido de ficheros
 - **Gestión Centralizada** y monitorización de eventos
 - **Interacción SDN** con otras soluciones de red como NAC, IPS, QoS, MARS, VOIP, etc



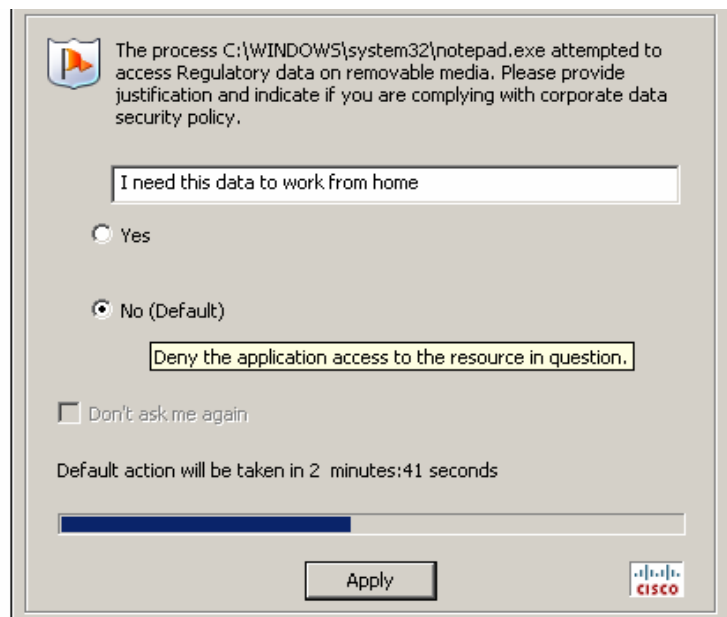
Tendencias recientes...

- Cisco define la Prevención de Intrusión basada en Host como **la habilidad de parar código malicioso en Día Cero sin reconfiguración (SO) ni actualización (AV).**
- CSA tiene un histórico probado de éxitos en parada de ataques de Día Cero, gusanos y virus durante los pasados 7 años:
 - 2001 – Code Red, Nimda (con sus 5 variantes), Pentagono (Gonner)
 - 2002 – Sircam, Debplot, SQL Snake, Bugbear,
 - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
 - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
 - 2005 – Internet Explorer Command Execution Vulnerability, Zotob
 - 2006 – USB Hacksaw, IE VML exploit, WMF, IE Textrange, RDS Dataspace
 - 2007 – Rinbot, Storm Trojan, Big Yellow, Word (MS07-014)

Sin firmas, ni reconfiguraciones, ni actualizaciones

Cisco Security Agent

Prevención de Fuga de datos



- Un único agente, única consola, solución para protección de terminales para Prevención de Fuga de datos. CSA puede monitorizar ficheros con datos sensibles y definidos por el usuario, y prevenir o auditar la actividad de dicha información.
- Basado en la política de seguridad, CSA-PFD puede:
 - Prevenir el abuso del uso del portadocumentos (p.e: copiar información sensible en aplicaciones tipo MI, blogs, etc.)
 - Prevenir la copia de información sensible en dispositivos USB/removibles, y el acceso desde la red (TCP/UDP)
 - Permite sólo a las aplicaciones autorizadas acceder a la información sensible (p.e: no permite permite enviar ficheros sensibles via Outlook)
 - Impone restricciones para usuarios remotos o WiFi (p.e: no permite copiar información sensible a dispositivos USB cuando se está desconectado de la red corporativa)

CSA: Prevención de Fuga de datos

Gestión del Proceso

Localización y Control de Información Sensible

■ Clasificación

- Tarjetas de Crédito, Seguridad Social...
- Definiciones de Propiedad Intelectual

Descubre

Monitoriza

■ Informes

- Seguimiento de localización y uso de datos sensibles

Educa

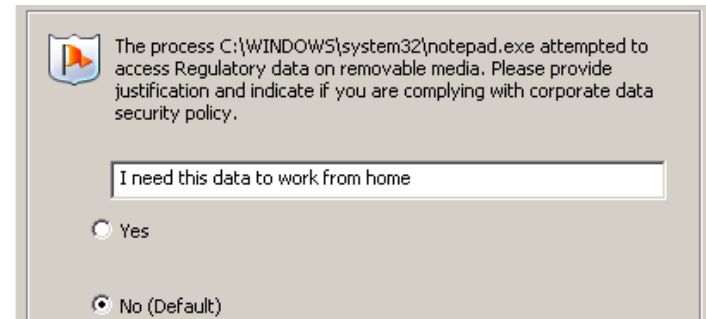
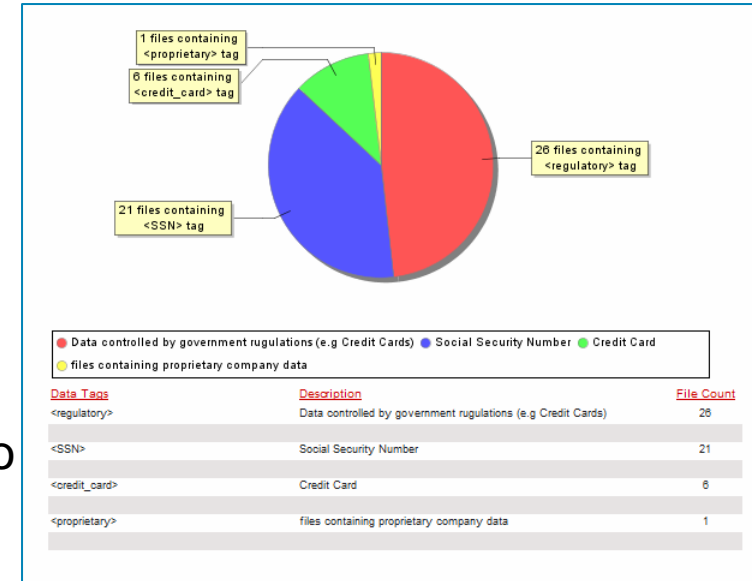
■ Mejora la utilización del usuario

- Audita y pregunta al usuario

Fuerza

■ Nuevos controles actualizados

- Bloqueo de impresión
- Control flexible de portadocumentos
- Cuarentena con NAC

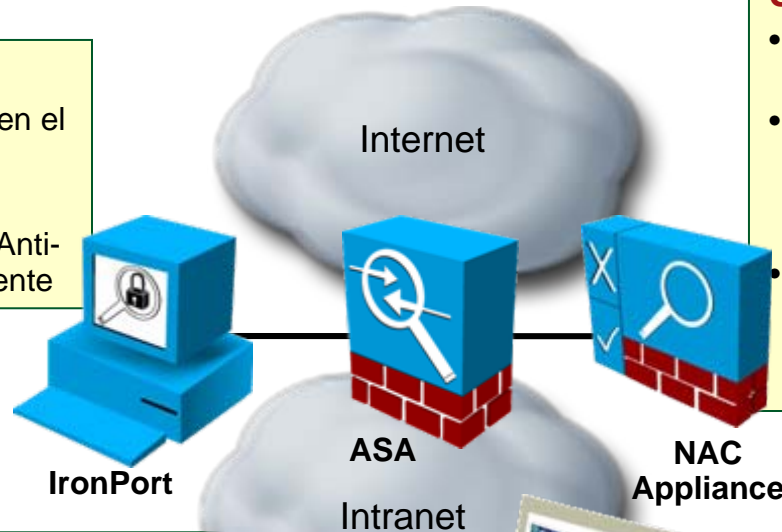


Soluciones Cisco de Seguridad para Prevención de Fuga de datos integradas en la red

CSA con NAC, DLP y IronPort

IronPort

- Previene la Fuga de Datos en el perímetro de red
- Exploración Multi-Protocolo
- Refuerza la infraestructura Anti-Spam y Anti-Spyware existente



Solución NAC

- Verifica la versión de CSA y si está funcionando
- Comprueba el estado de los sistemas como “arranque inseguro detectado” y si los datos sensibles existen
- Comprueba la identidad del usuario si CSA reporta información sensible en el sistema

Cisco Security Agent

- Previene la pérdida de datos sensibles:
 - Explora los ficheros para localizar datos sensibles
 - Previene la copia a dispositivos externos (USB flash y discos, dispositivos IR/Bluetooth)
 - Previene el uso con aplicaciones de red (e-mail, MI, navegador)
- Previene evitar la protección de red de IronPort

CSA

Agenda

Prevención de fuga de datos

Un problema para los negocios

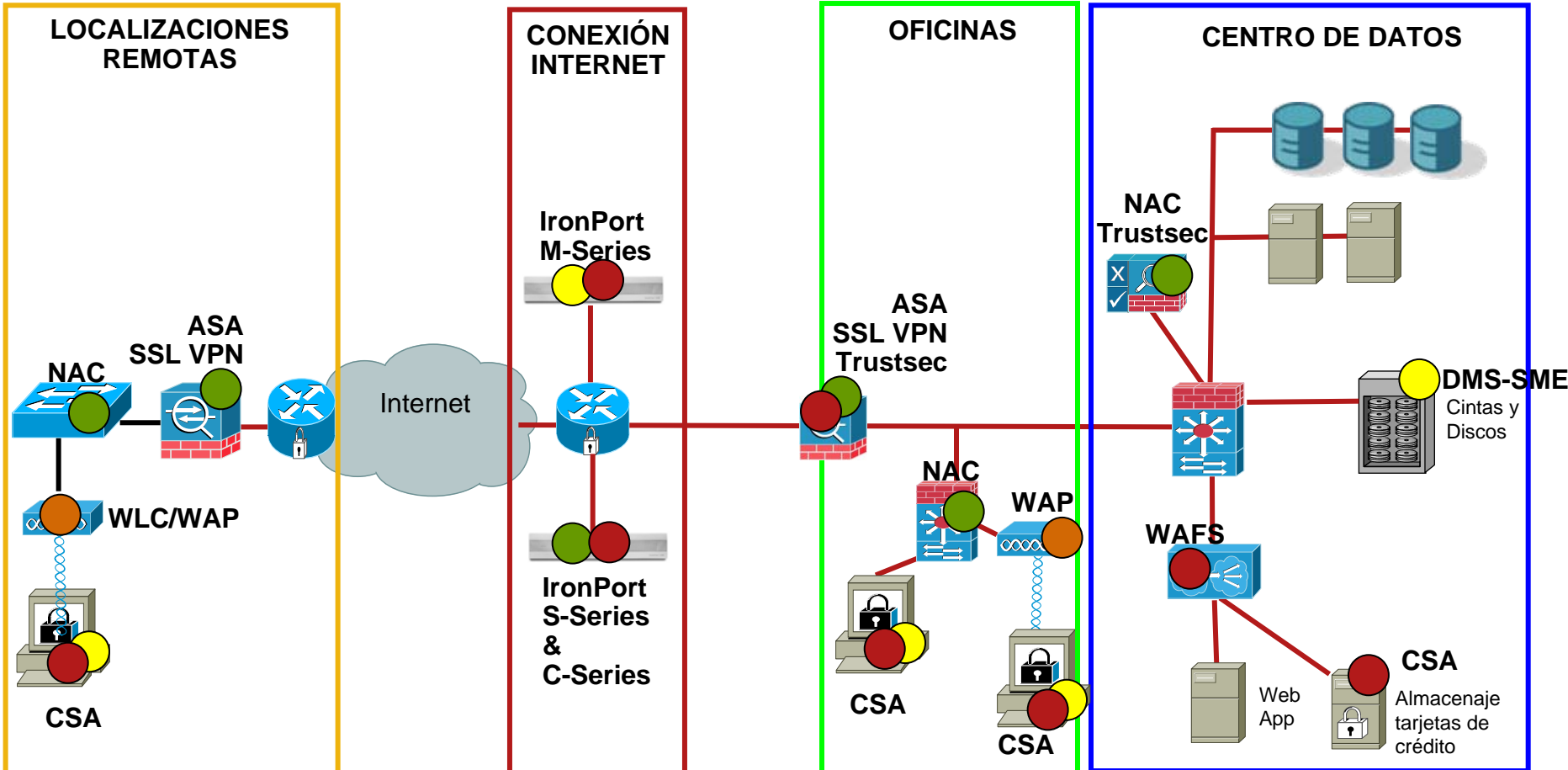
Casos de uso

Tecnología y soluciones
Cisco

Resumen



Arquitectura Cisco de Seguridad en Red para la Protección de Fuga de Datos



	Control de Acceso
	Conectividad Segura
	Aumenta Seguridad de Datos
	Control de Contenidos para filtración de datos

Prevención de fuga de datos

Resumen

Cisco provee de un portfolio completo de soluciones de Seguridad, incluyendo la Prevención en Fuga de Datos

Con una red de datos auto-defensiva de Cisco como plataforma con servicios de Prevención de Fuga de Datos integrados en los dispositivos de seguridad de red, las organizaciones pueden mejorar en:

- Prevenir la Fuga de Datos, incluyendo propiedad intelectual y datos privados de empleados y clientes
- Reforzar el cumplimiento regulatorio en seguridad con políticas de uso aceptables
- Incrementar la visibilidad dentro del uso de datos sensibles
- Decrementar el coste y complejidad de despliegues para prevención de Fuga de Datos



Prevención de fuga de datos

Resumen

Los switches de Cisco protegen de las pérdidas y robos de datos e identidad en la red – con facilidades como DHCP Snooping, Dynamic Address Resolution, IP Source Guard e Identity 4.0 (IBNS)

Con Cisco Network Admission Control, se puede proteger a la red controlando la admisión de usuarios no autorizados así como de dispositivos que no cumplan con las políticas de seguridad

Con Cisco Security Agent se puede prevenir el envío accidental de datos confidenciales por correo electrónico

Monitoriza los ficheros y datos sensibles en la computadora y previene que los ficheros sean adjuntados al correo electrónico

Con Cisco Security Agent se puede prevenir la Fuga de datos vía navegador WEB

La protección por comportamiento sospechoso de CSA defiende a los terminales ante ataques tipo Malware, Códigos maliciosos, Rootkits, virus y ataques objetivos



Más Información sobre Soluciones de Seguridad de Cisco:

- Cisco.com Data Loss Prevention site:

www.cisco.com/go/dlp

- Cisco CSA:

<http://www.cisco.com/go/csa>

- Cisco NAC:

<http://www.cisco.com/go/nac>

- Cisco Self-Defending Network:

http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/self_defending_network/index.html

- Information on global data breaches:

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<http://attrition.org/dataloss/>

