



Cisco IronPort Solución Seguridad Correo Electrónico



Gonzalo Madariaga M.

CTO Grupo ISC S.A.

Director de Methodo – Netaccess – DesigNet

gmadariaga@isc.cl



Agenda

- Problemática Actual Seguridad de Correo
- Descripción de la Solución
- Mejores Prácticas de Diseño
- Otras Ventajas
- Beneficios



Problemática Actual Seguridad de Correo



El Reto de Hoy



Globalización



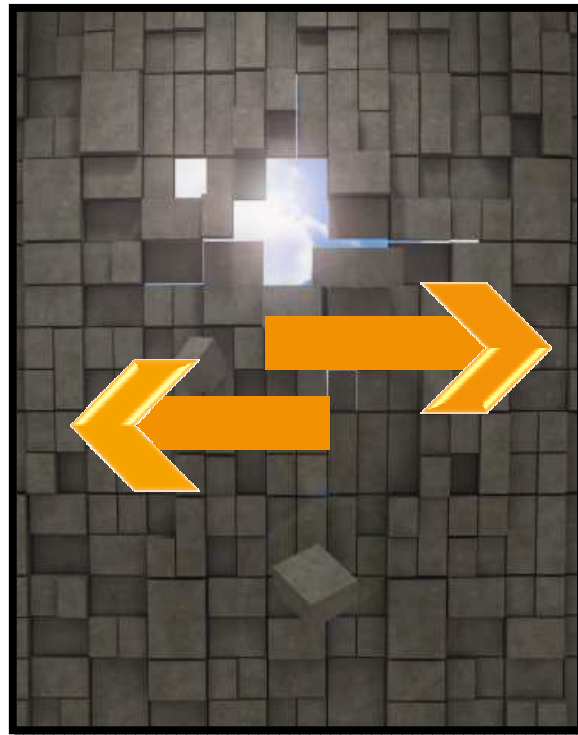
Colaboración



SaaS



Movilidad



Amenazas

Uso Aceptado

Privacy & Security Task Force ADVISORY

October 7, 2008

States Adopting Aggressive New Privacy
and Data Security Laws and Regulations

This advisory summarizes selected state legislative and regulatory developments.

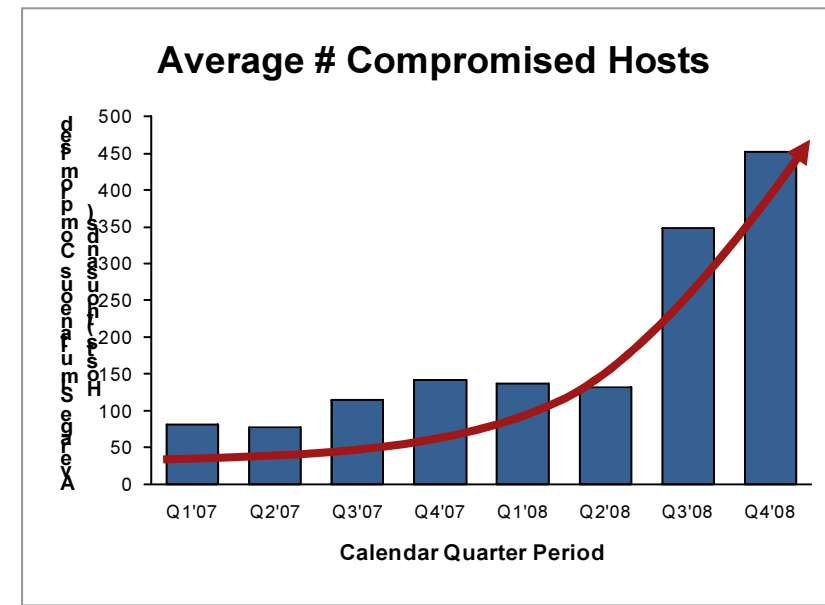
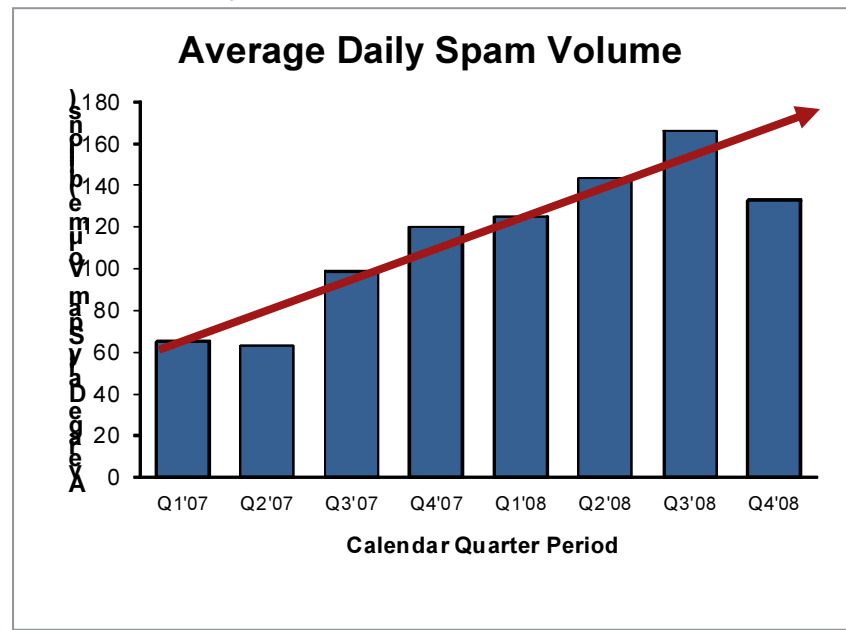
Fuga de
Información

Amenazas de Seguridad Correo

Más Spam y Spammers

Más Spam

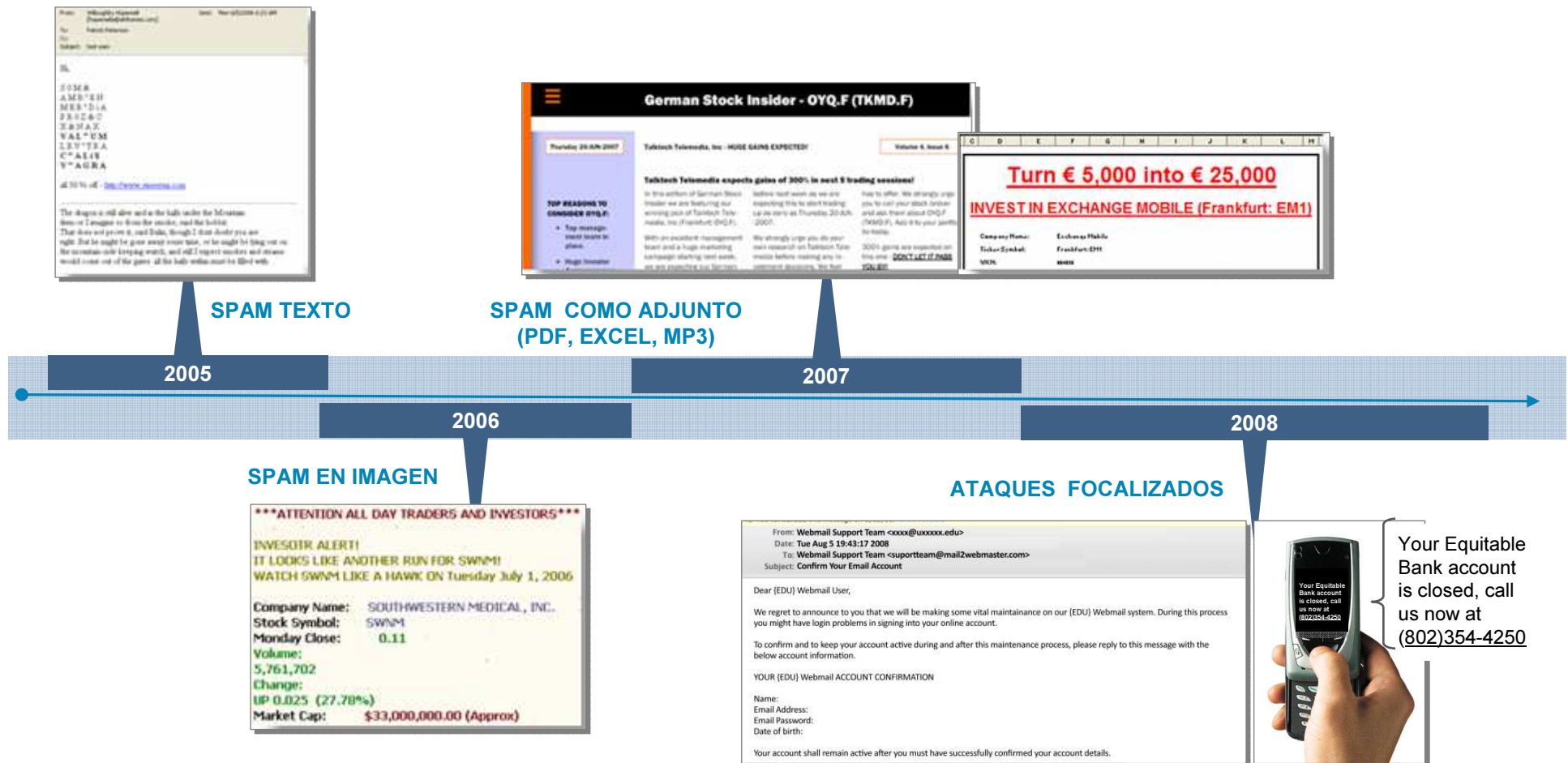
- El volumen del spam diario se duplica anualmente.
- Alcanzando 180 billones de mensajes de spam al día.



Mas Spammers

- Más Spammers con más host comprometidos con Botnet para envío de spam.
- La sofisticación del Malware está continuamente en aumento.

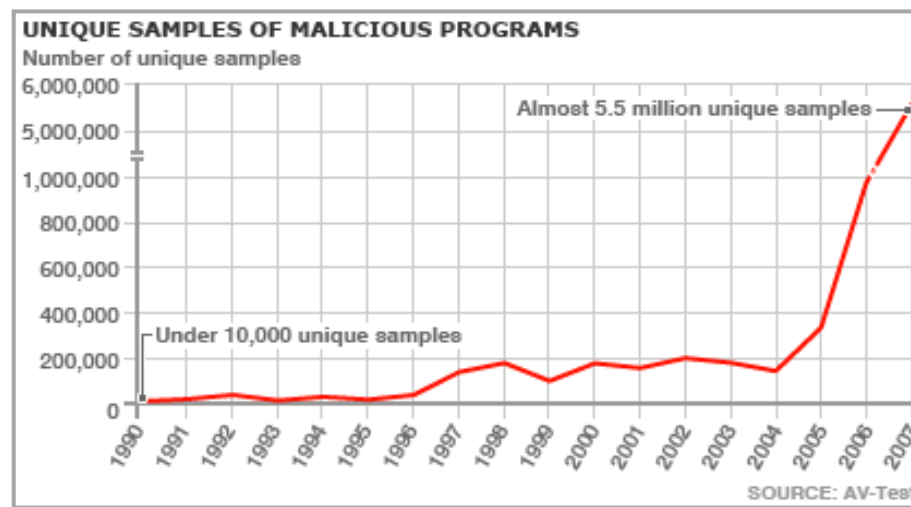
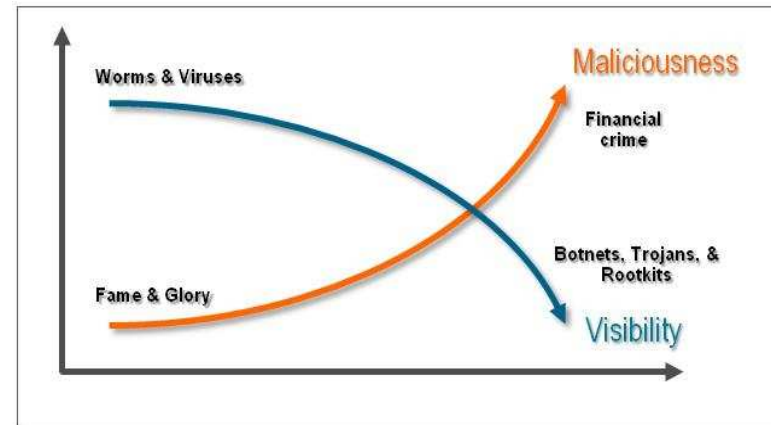
La Innovación en el Spam está en Aumento



“El Spam ha experimentado una evolución significativa durante el 2008... Criminales sofisticados están usando pequeñas campañas de phishing dirigidas a un grupo identificado de destinatarios – con gran resultado”

Malware en Alza

Correo es el principal medio



DLP Las Presiones Continuan Creciendo

Aumentan Reportes de Fuga de Información

Viernes 14 de febrero de 2003

El ex gerente de Inverlink encarcelado por la fuga de noticias del Banco Central de Chile

El ex gerente de la corredora de bolsa Inverlink, Enzo Bertinelli, fue encarcelado tras ser interrogado durante más de tres horas por la jueza del 2° Juzgado del Crimen de Santiago, Elizabeth Reinoso, quien investiga el hurto de información confidencial del Banco Central de Chile (BC).

Fuga por Correo es el Medio Dominante

many different vectors of DLP leakage but not all equal.

Order	Leakage Concern	Percent
1	Email	56%
2	Lost Laptop	51%
3	Web	37%
4	IM	33%
5	USB	19%

Table1: IT Concerns for Leakage (IDC)

Nuevas Normativas Derivan en Nuevos Requerimientos

13/10/2008

Embeber Link Enviar Imprimir

Senadores presentaron proyecto de ley que sanciona el envío de spam

- La iniciativa también contempla castigo a la publicidad en otros medios.
- Parlamentarios propusieron multas de hasta 36 millones de pesos.

Cooperativa.cl

Privacidad de los mensajes

El correo electrónico es hoy en día, ampliamente usado para **enviar y recibir información “sensible” e importante.**

Es por esto que se ha hecho cada vez más importante la protección de dicha información, las soluciones actuales tienen las siguientes debilidades:

- **No son multiplataforma.**
- **Los usuarios necesitan tener certificados digitales.**
- **Se requiere instalar Software especial o Plug-Ins.**



Frustración de los Administradores

- Aumento en las Amenazas incrementa la carga de trabajo y demanda mayor experiencia.
- Los pocos recursos con que cuentan los administradores, son cada vez, más demandados dado las restricciones presupuestarias.



Resumen de Problemas y Solución

Nuevas Amenazas	• Solución flexible e innovadora. • Líder en el mercado.
Crecimiento del spam	• Alta performance • Red de Muestreo
Fuga de información	• DLP • Filtros de contenidos
Malware	• Antivirus • Web Reputation
Propagación de virus	• Filtro anti Epidemias • Variedad de Antivirus
Manejo de Información Sensible	• Cifrado. • DLP • Filtro Contenido
Demanda de Administración	• Red de Muestreo • Centro de Análisis y Generación de Reglas
Satisfacer las necesidades de conectividad y uso.	• Solución flexible. • Administración Amigable. • Trackeo de Correo
Complejidad del problema	• Solución especializada, integrada y escalable.

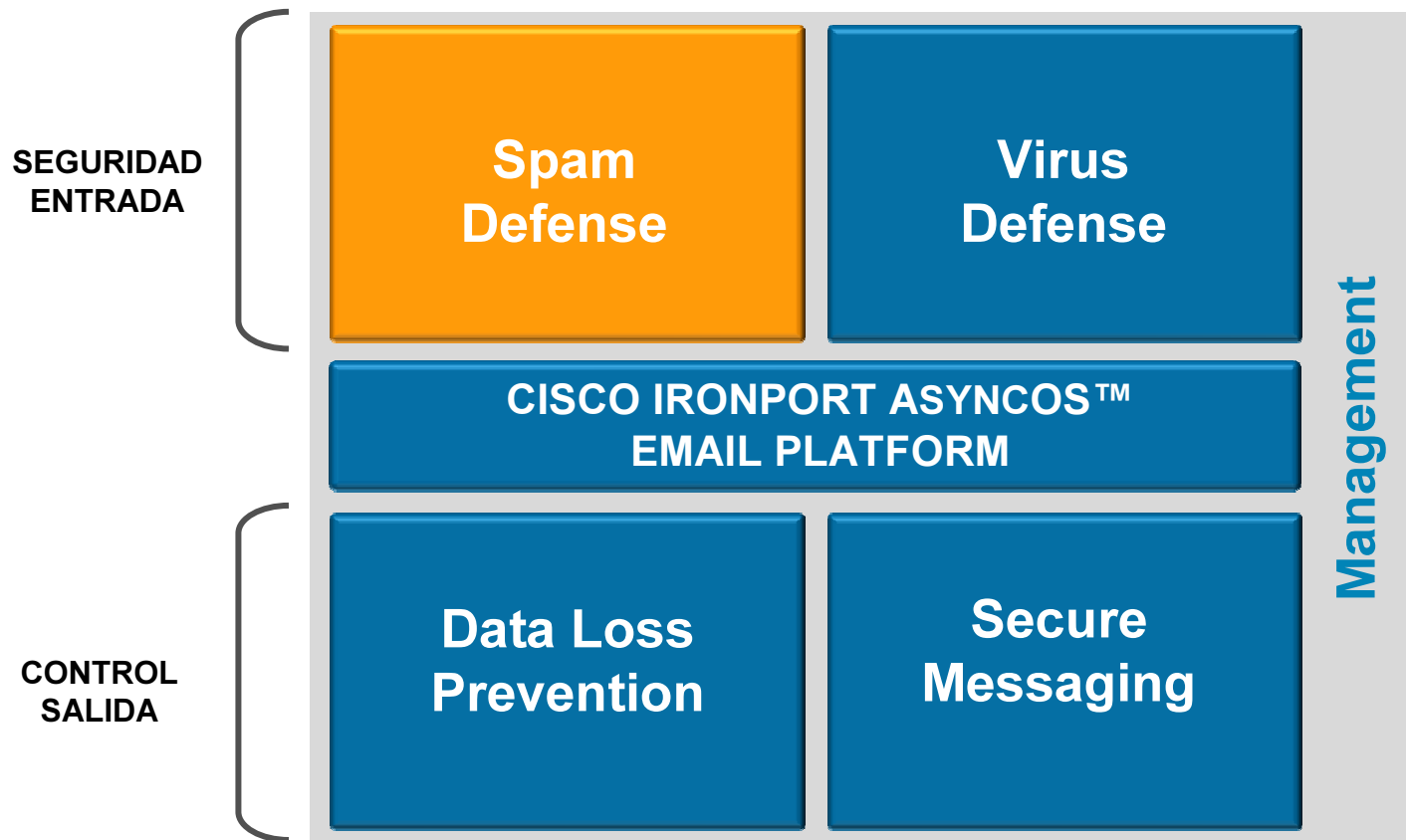


Descripción de la Solución

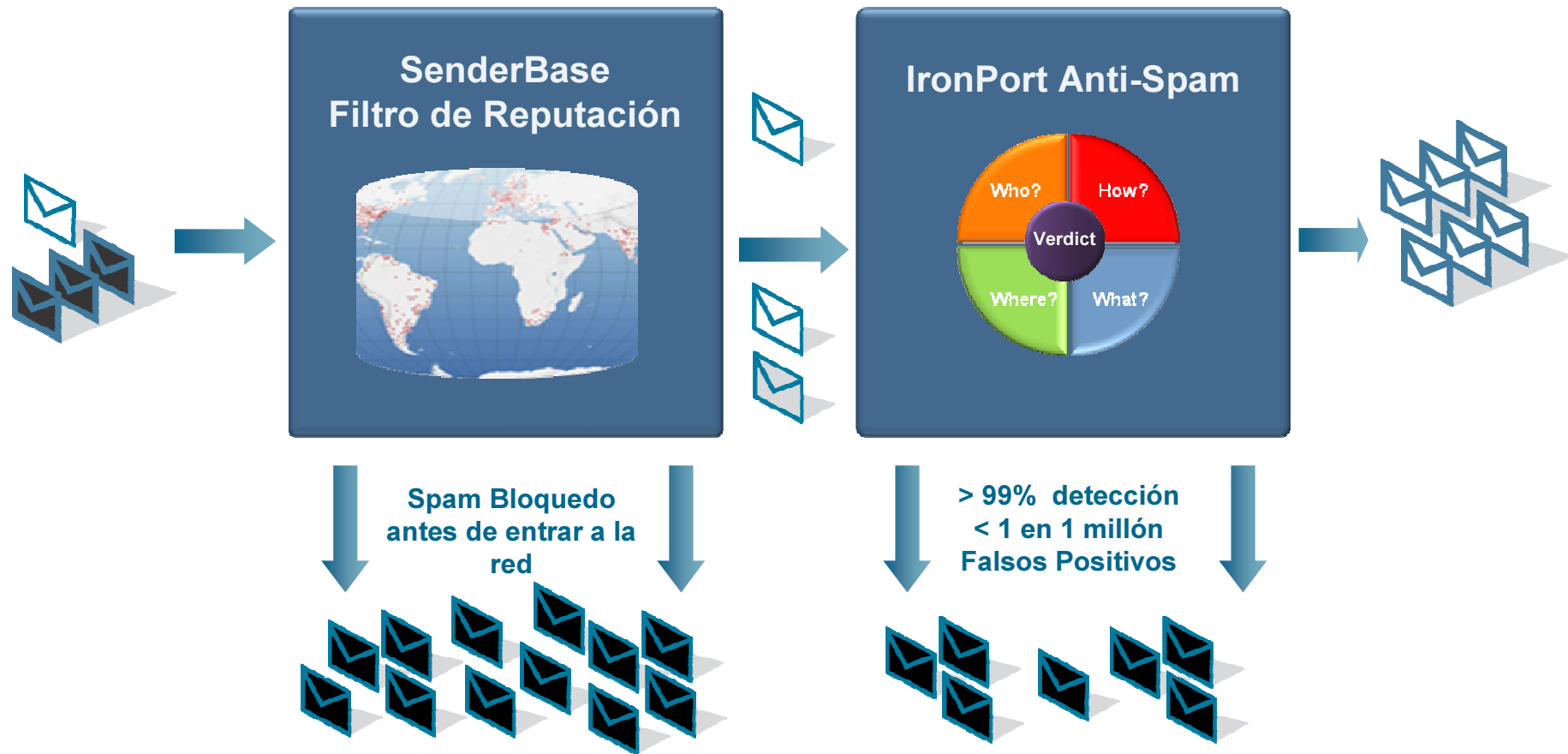


Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida

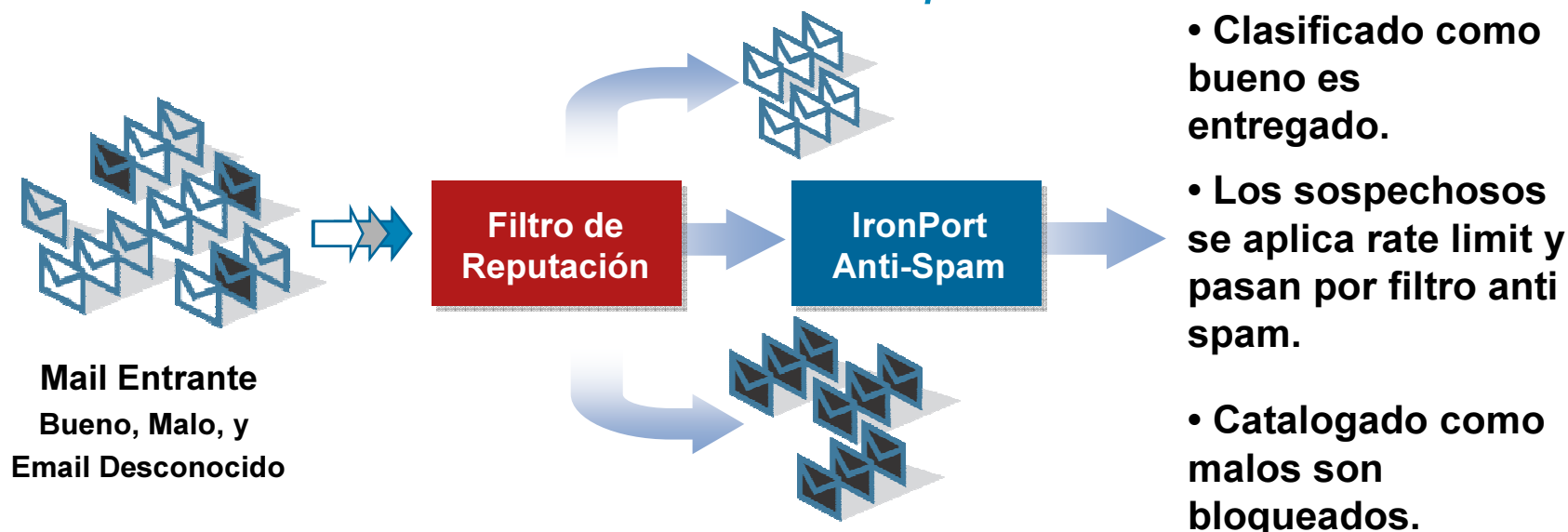


Defensa Anti-Spam en profundidad



SenderBase Filtro de Reputación

Prevención de amenazas en Tiempo Real

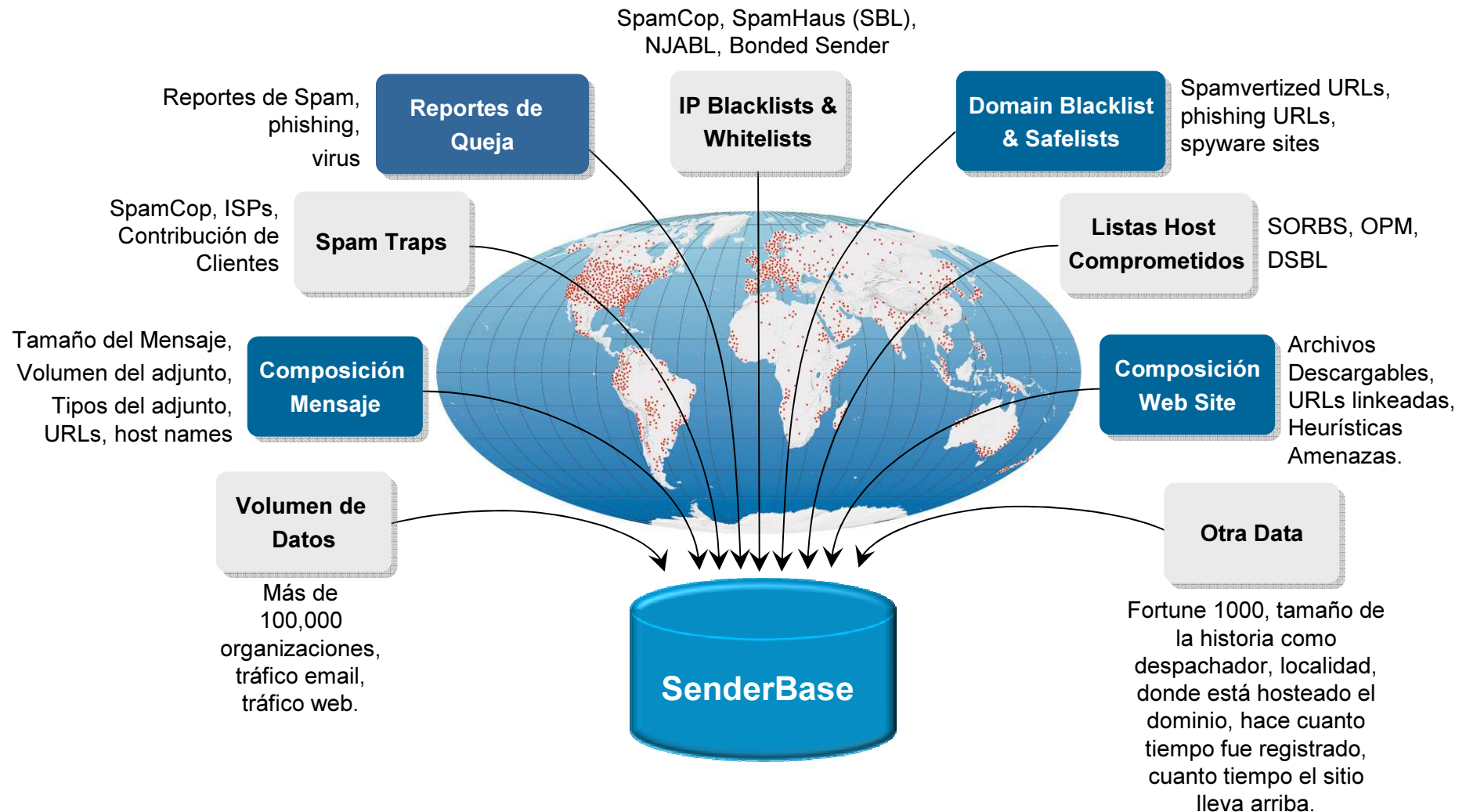


Cisco en Cisco
Nuestra experiencia
Corporativa de Correo

Message Category	%	Messages
Stopped by Reputation Filtering	93.1%	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	96.8%	728,797,126
Clean Messages	3.2%	24,102,874
Total Attempted Messages:		752,900,000

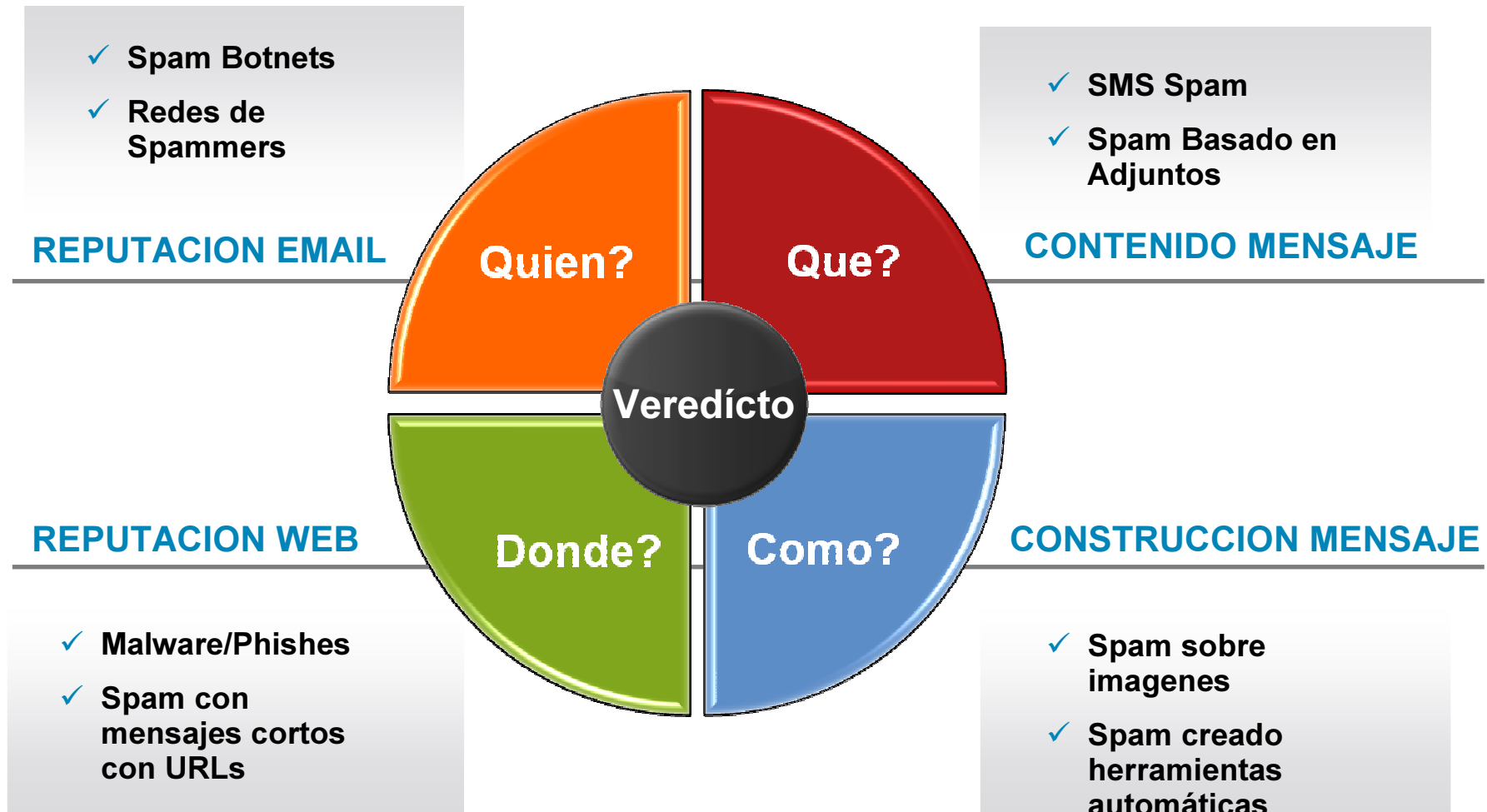
Cisco IronPort SenderBase

Cantidad y Calidad de la Información hace la Diferencia



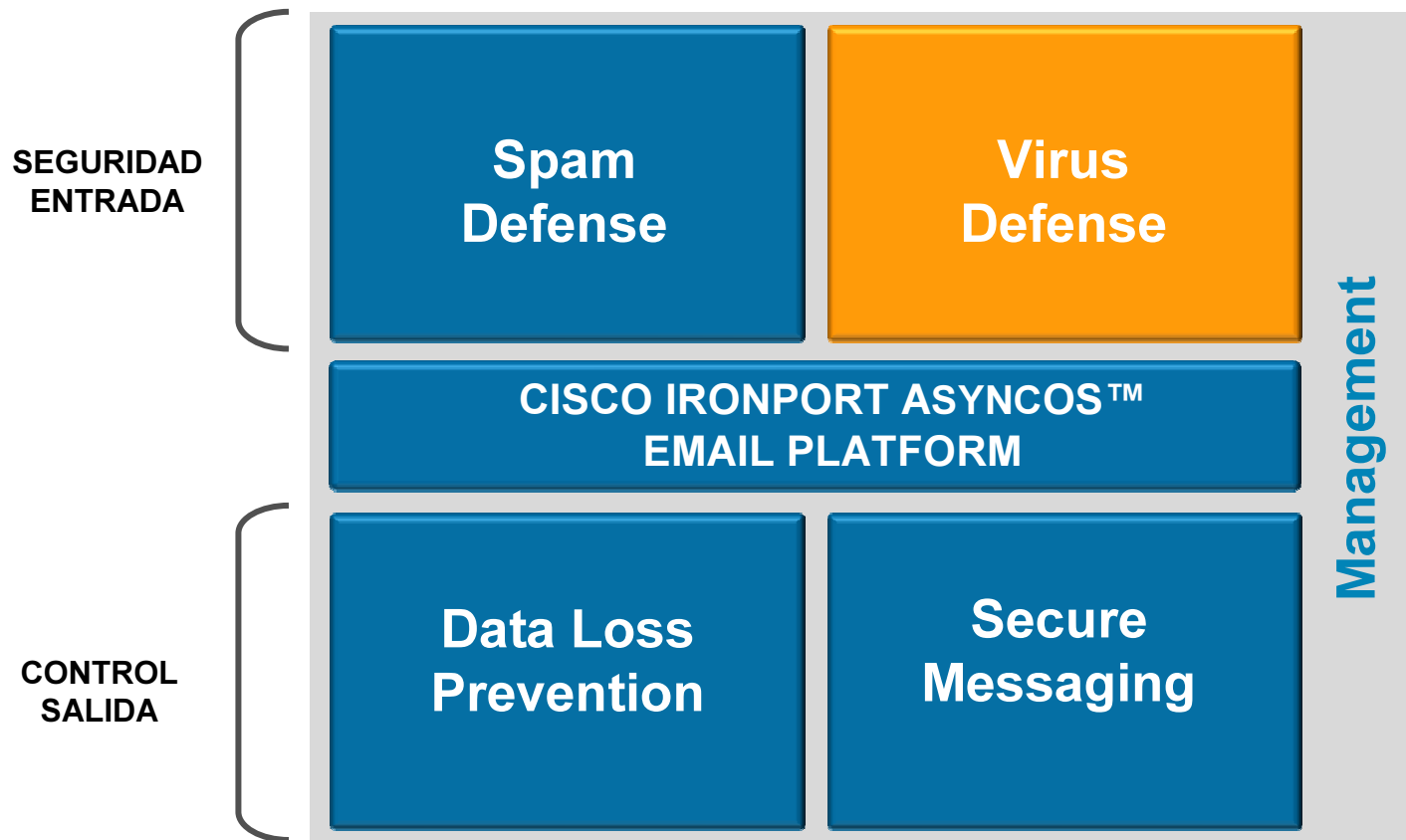
Cisco IronPort Anti-Spam

C.A.S.E. (Context Adaptive Scanning Engine)

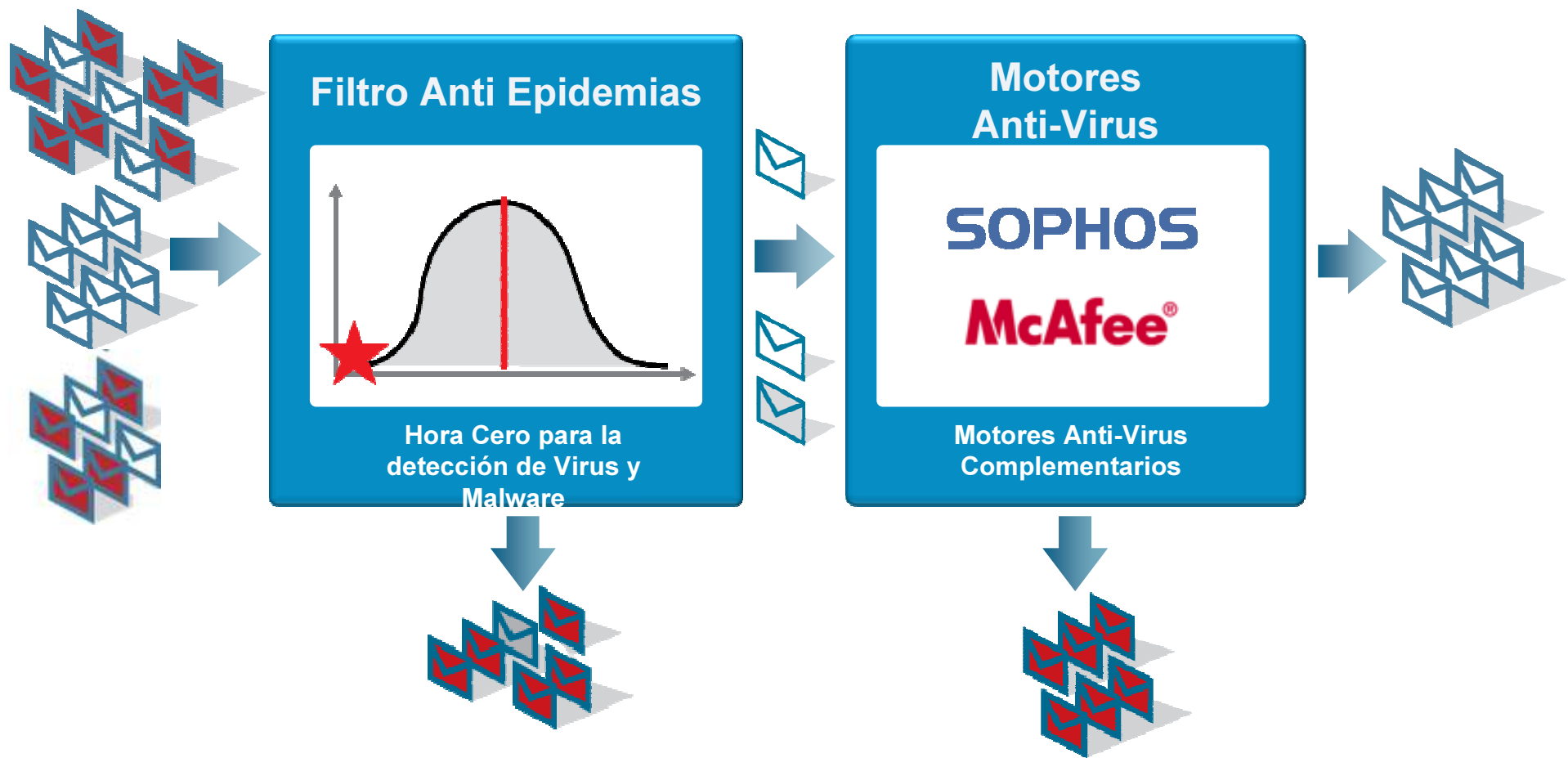


Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida



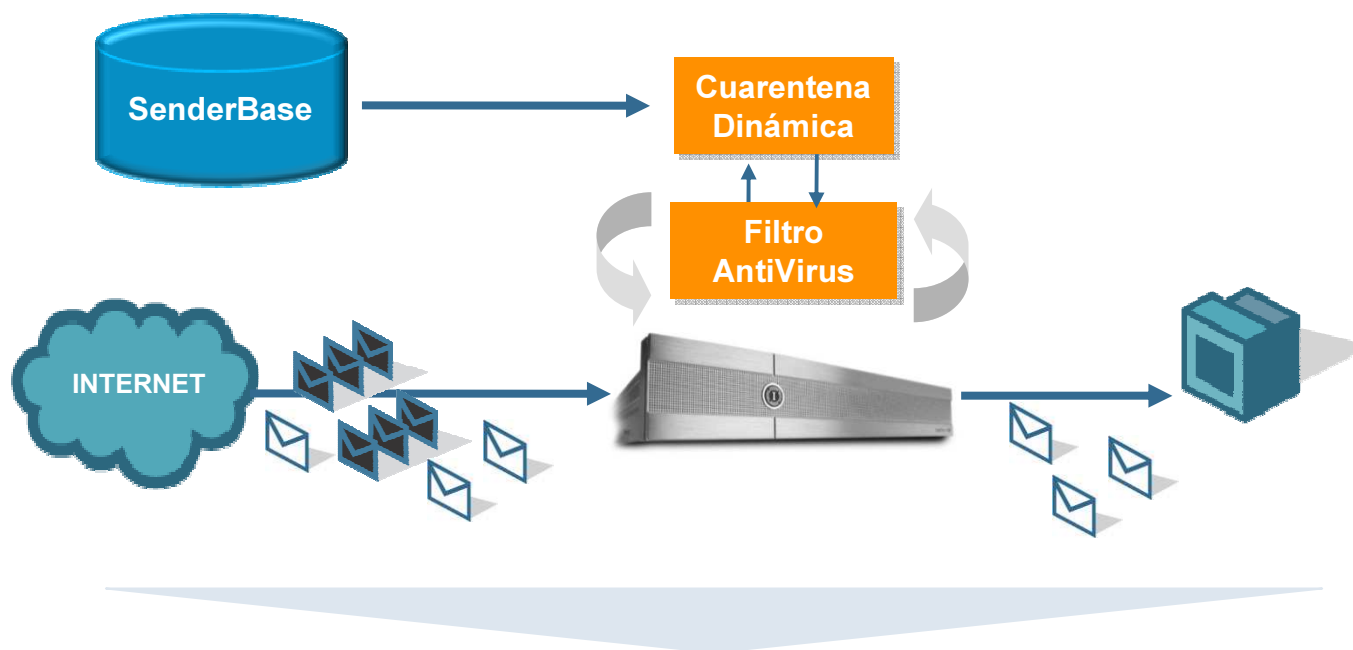
Defensa Anti-Virus en Profundidad



Cisco IronPort Filtro Anti Epidemia

Prevención Malware Hora Cero

Filtro Anti Epidemia en Acción



Ventaja Filtro Anti Epidemias

Promedio tiempo de Anticipo*.....sobre 13 horas
Epidemias bloqueadas*291 Epidemias
Incremento Protección*.....sobre 157 días

"Since VOF we have not had a single virus outbreak!"



"Over 24,000 virus positive messages stopped in 9 months"

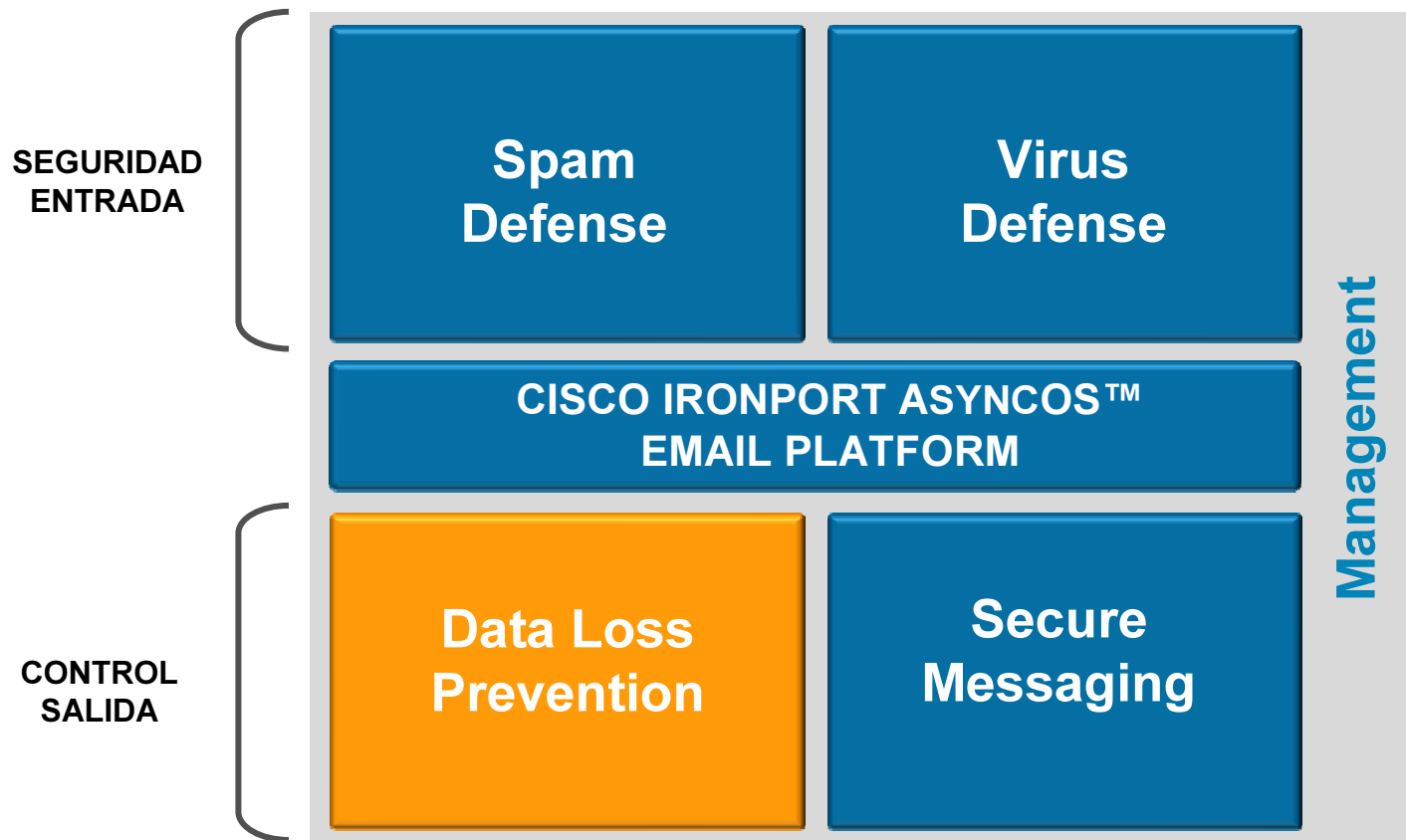


"VOF has stopped more than 12,000 separate viral messages in the last year"



Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida



DLP - Data Loss Prevention

Configuración Simple

- Con “3 click” de configuración estas usando los filtros de contenidos.
- Cuenta con categorías de contenido pre-definidas o puedes crear o personalizar las propias.
- Pueden ser utilizadas en determinados usuarios en ciertas circunstancias.

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

☐ Contains text:

*

☒ Contains smart identifier:

ABA Routing Number

☐ Contains term in content dictionary:

HIPAA-Dictionary_txt

Number of matches required: (1-1000)

For content dictionaries, the number of matches is term weight.

☒ Import from local computer:

☐ Import from the *configuration* directory on your IronPort appliance:

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

Smart Identifiers: ?

Enable Smart Identifiers	Weight
☒ Credit Card Numbers	1 v
☒ Social Security Numbers	1 v
☒ ABA Routing Numbers	1 v
☒ CUSIPs	1 v

DLP - Data Loss Prevention

Tratamiento Flexible y Reporting

- Múltiples acciones configurables: cifrar, cuarentena, descartar, rebotar, BCC, eliminación del contenido.
- Destaca el contenido fuera de norma en la cuarentena para facilitar el análisis.
- Reportes basados en usuarios o políticas.

The screenshot displays a configuration window for DLP actions. On the left, a list of actions is shown under the heading 'Quarantine'. The actions include: Strip Attachment by Content, Strip Attachment by File Info, Add Disclaimer Text, Bypass Outbreak Filter Scanning, Send Copy (Bcc:), Notify, Change Recipient to, Send to Alternate Destination Host, Deliver from IP Interface, Strip Header, Add Header, Encrypt and Deliver (Final Action), Bounce (Final Action), Deliver (Final Action), and Drop (Final Action). On the right, a detailed view of the 'Quarantine' action is shown. It includes a description: 'Flags the message to be held in one of the areas.' Below this, there is a field 'Send message to quarantine:' with a dropdown menu set to 'Policy'. Further down, there is a checkbox labeled 'Duplicate message' with a descriptive note: 'Send a copy of the message to the specified quarantine area. The message will continue processing the original message and the actions will apply to the original message.'

Quarantine
Strip Attachment by Content
Strip Attachment by File Info
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add Header
Encrypt and Deliver (Final Action)
Bounce (Final Action)
Deliver (Final Action)
Drop (Final Action)

Quarantine

Flags the message to be held in one of the areas.

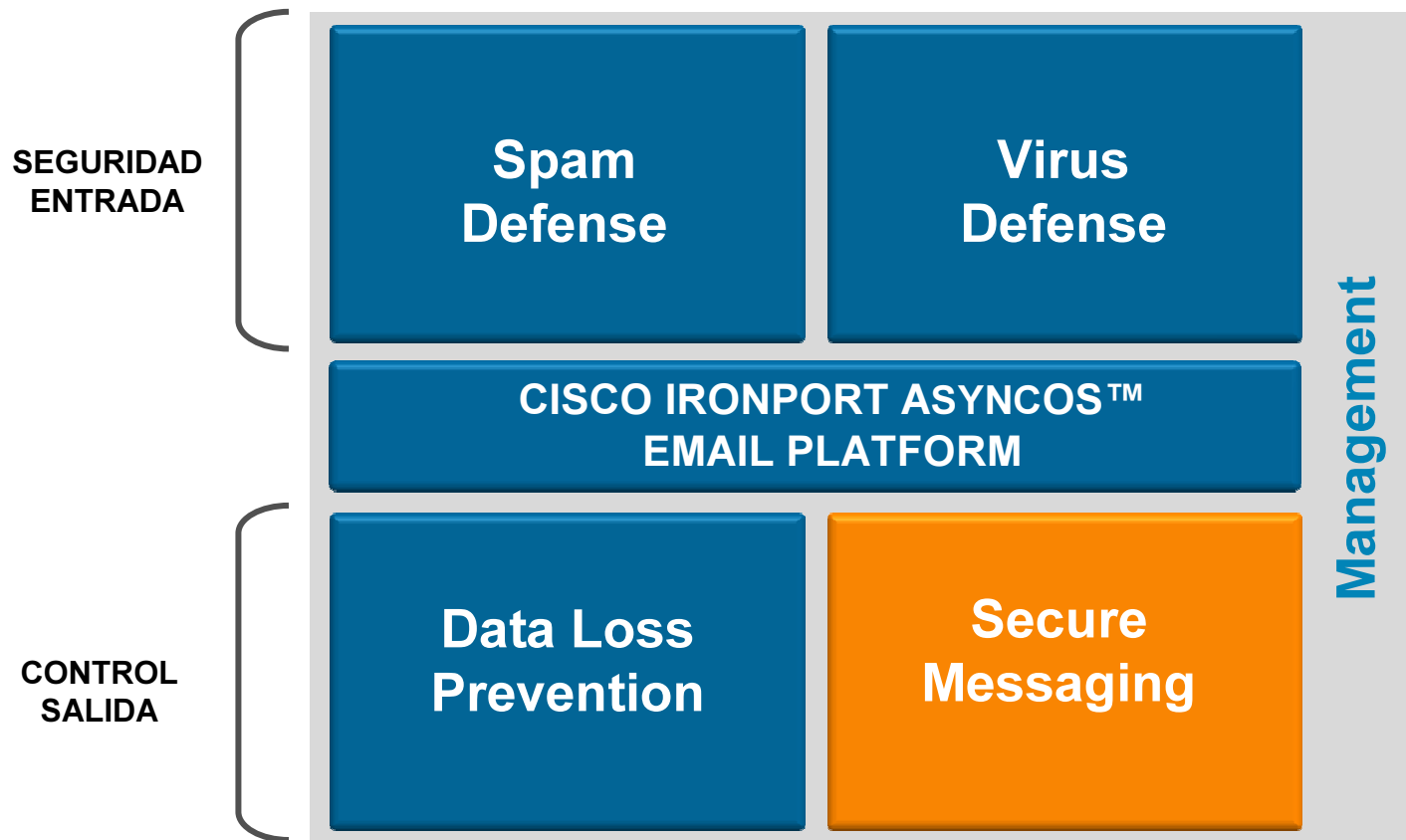
Send message to quarantine: Policy

☐ Duplicate message

Send a copy of the message to the specified quarantine area. The message will continue processing the original message and the actions will apply to the original message.

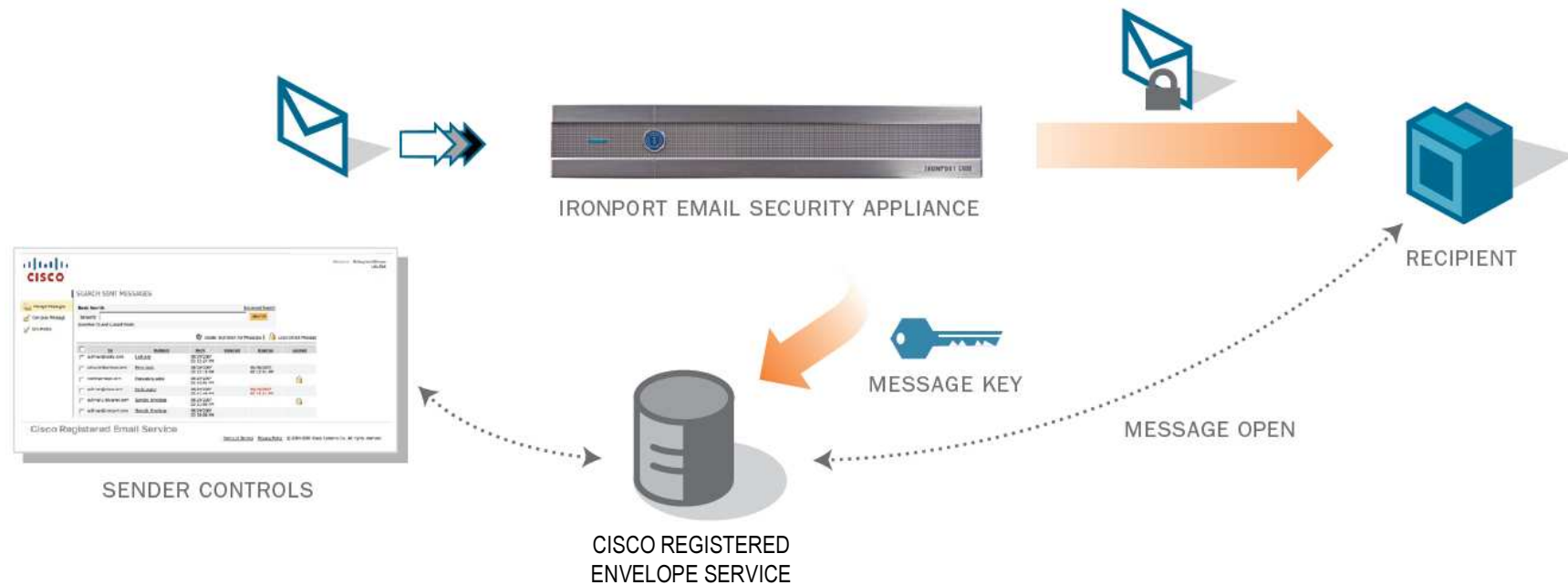
Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida



Cisco IronPort Cifrado de Correos

Fácil para el originador. . .

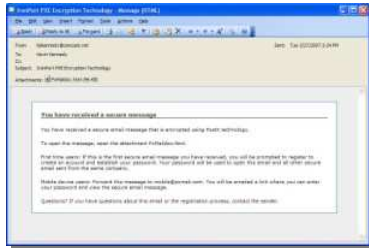


- Manejo de Llaves automáticas.
- No requiere software adicional.
- Compatible con cualquier sistema de correo.

Cisco IronPort Cifrado de Correo

Fácil para el receptor. . .

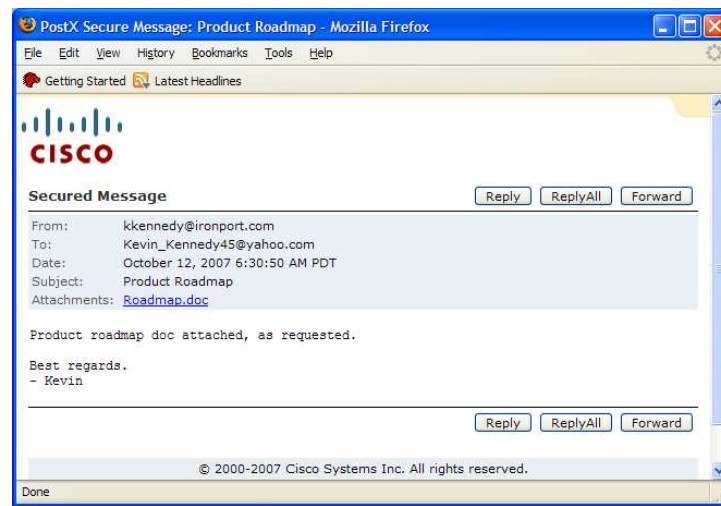
1. Abrir Adjunto



2. Ingresar Clave

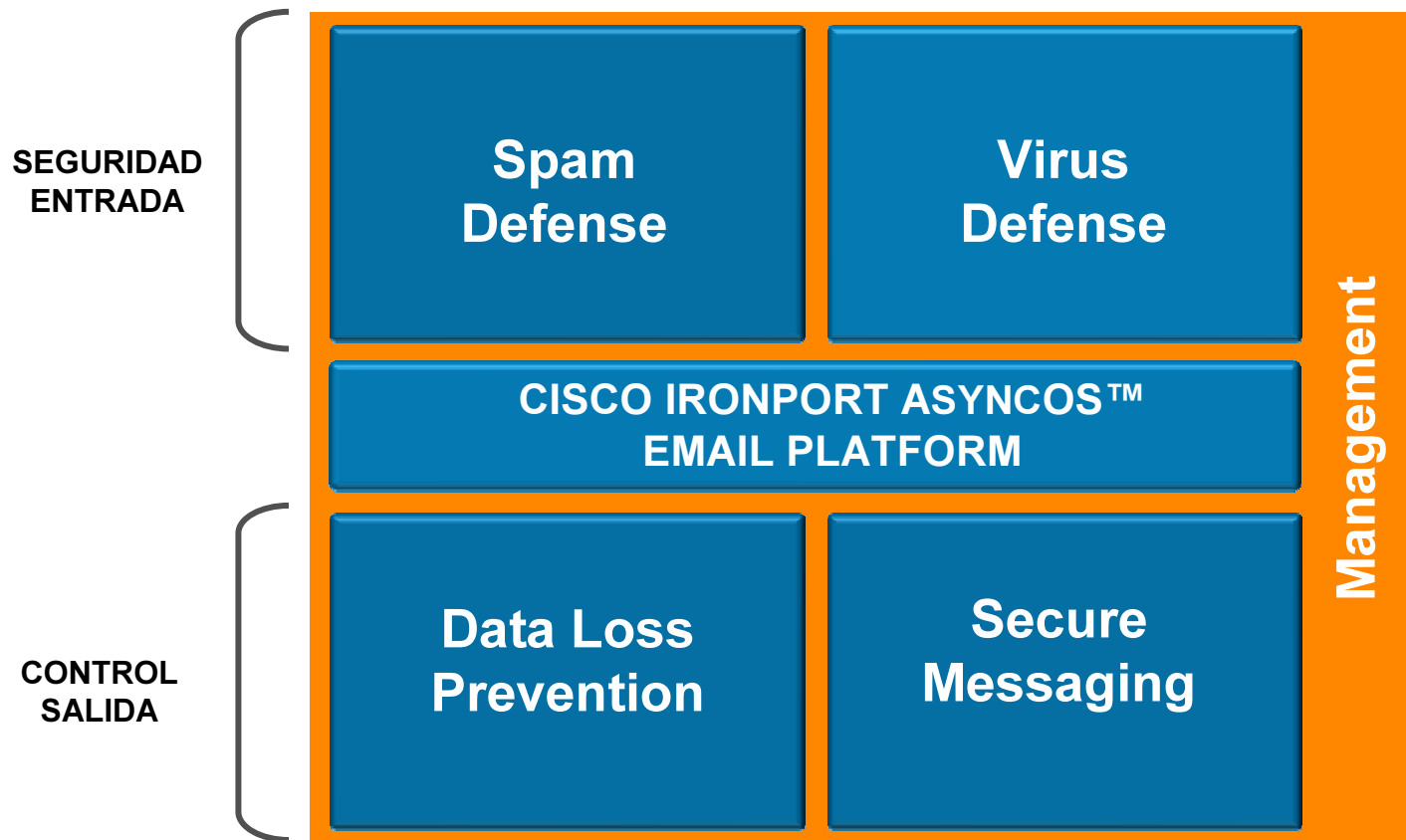


3. Ver el Mensaje



Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida



Cisco IronPort Administración

Una vista para todas las políticas

Incoming Mail Policies

Find Policies

Email Address: ☒ Recipient ☐ Sender

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key:

Categorías: por Dominio,
nombre de usuario, o
LDAP

- Permite todos los tipos de Archivos
- Ejecutables a Cuarentena
- Marcar y entregar el Spam
- Borrar los Ejecutables
- Archivar todo los Mensajes
- Filtro anti Epidemias desactivado para todos los archivos .doc



IT



VENTAS



LEGAL

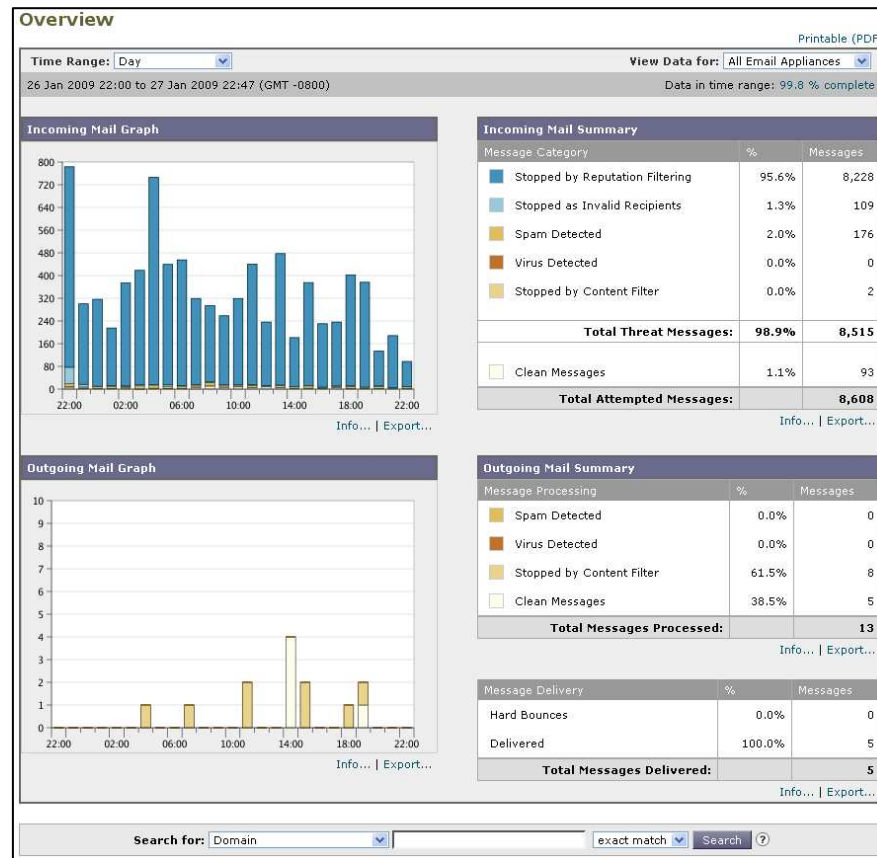
“IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance.” – PC Magazine

Visión Completa

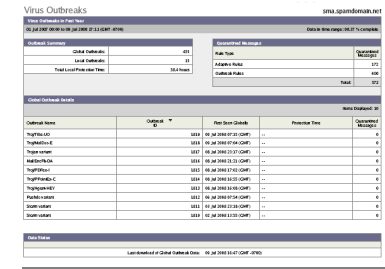
Reportes Unificados

Reportes Consolidados

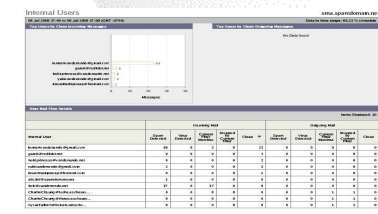
- Vista unificada para toda la organización.
- Reportes en tiempo real sobre tráfico de correo y amenazas de seguridad.
- Reportes drill down.



Múltiples puntos de información



Volúmenes de Correo
Contadores de Spam
Violaciones a las políticas
Reportes de Virus
Correos Salientes
Servicio de Reputación
Salud del Sistema



Visibilidad de los Mensajes

Tracking de Mensajes

¿Qué pasó con el correo que envíe hace 2 horas?

✓ Tracking de mensajes individuales.

¿Quién recibió mensajes similares?

✓ Análisis forense para compliance.

Message Tracking

Search

Available Time Range: 08 Oct 2007 09:10 to 27 Jan 2009 22:51 (GMT -0800) Data in time range: 91.25% complete

Envelope Sender: ? Begins With

Envelope Recipient: ? Begins With

Subject: Begins With

Message Received: ☒ Last Day ☐ Last Week ☐ Custom Range

Start Date: 01/26/2009 Time: 22:00 and End Date: 01/27/2009 Time: 22:52 (GMT -0800)

Advanced

Sender IP Address:

☐ Search rejected connections only ☒ Search messages

Message Event: Selecting multiple events will expand your search to include messages that match each event type. However, combining an event type with other search criteria will narrow the search.

☐ Virus Positive	☐ Hard bounced
☐ Spam Positive	☐ Soft bounced
☐ Suspect Spam	☐ Currently in Outbreak Quarantine
☐ Delivered	☐ Quarantined as Spam

Message ID Header:

IronPort MID:

IronPort Host: All Hosts

Query Settings: ?

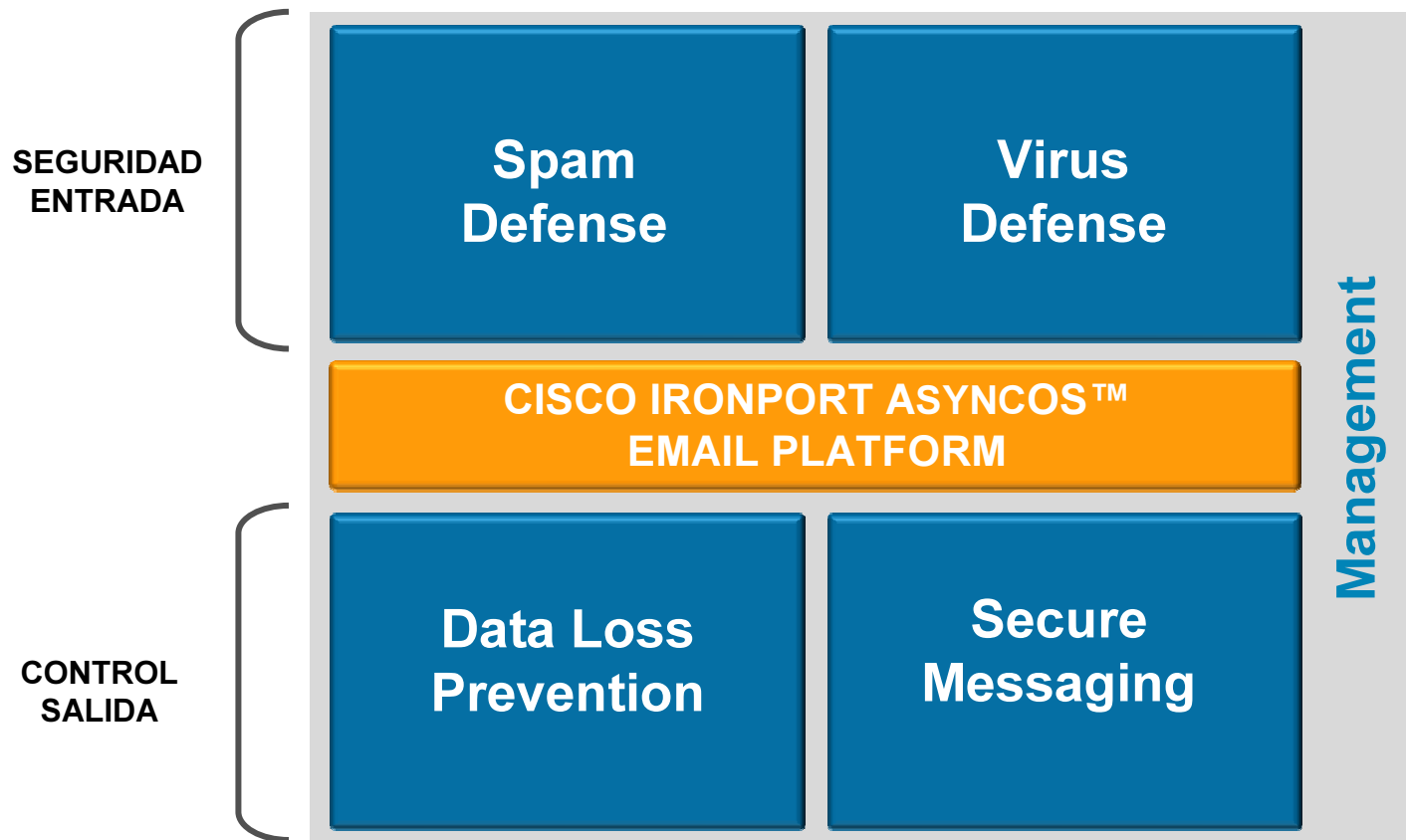
Query timeout: 1 minute

Max. results returned: 250

Clear Search

Arquitectura Seguridad de Correo

Seguridad Entrada, Control de Salida



Cisco IronPort AsyncOS

Herramienta Robusta de Protección

Encriptación TLS

Encriptación entre Gateways

Sanitización de HTML

Elimina spoofed URLs

Verificación SPF

Verifica si los mensajes fueron originados desde los servidores designados como Emisores válidos

Firma y Verificación DKIM

Verificación del Enviador



Integración con LDAP

LDAP referrals, múltiples servidores LDAP, wizard de configuración en 3 pasos

Verificación de Rebotes

Elimina Rebotes mal dirigidos

Listas Negras y Blancas + Cuarentena

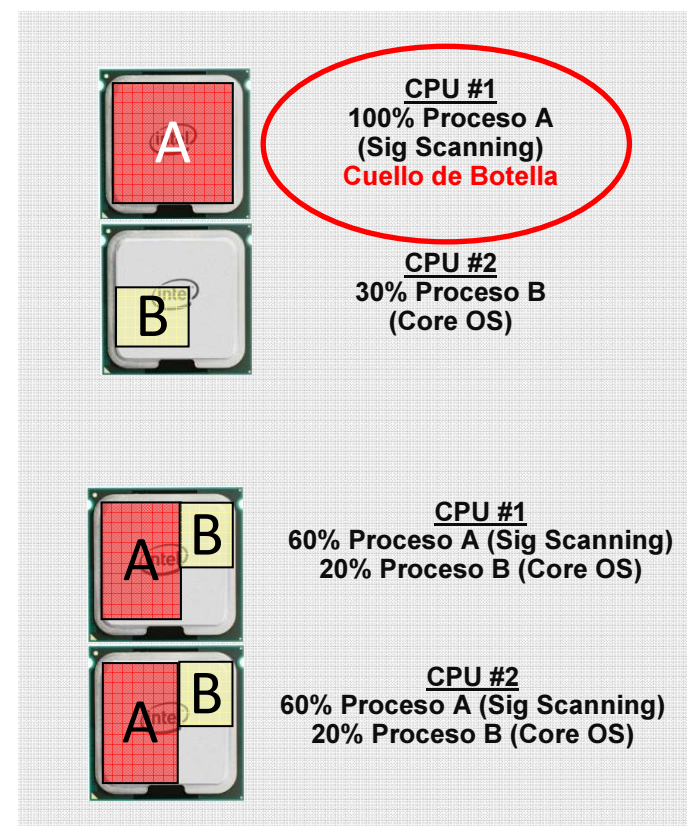
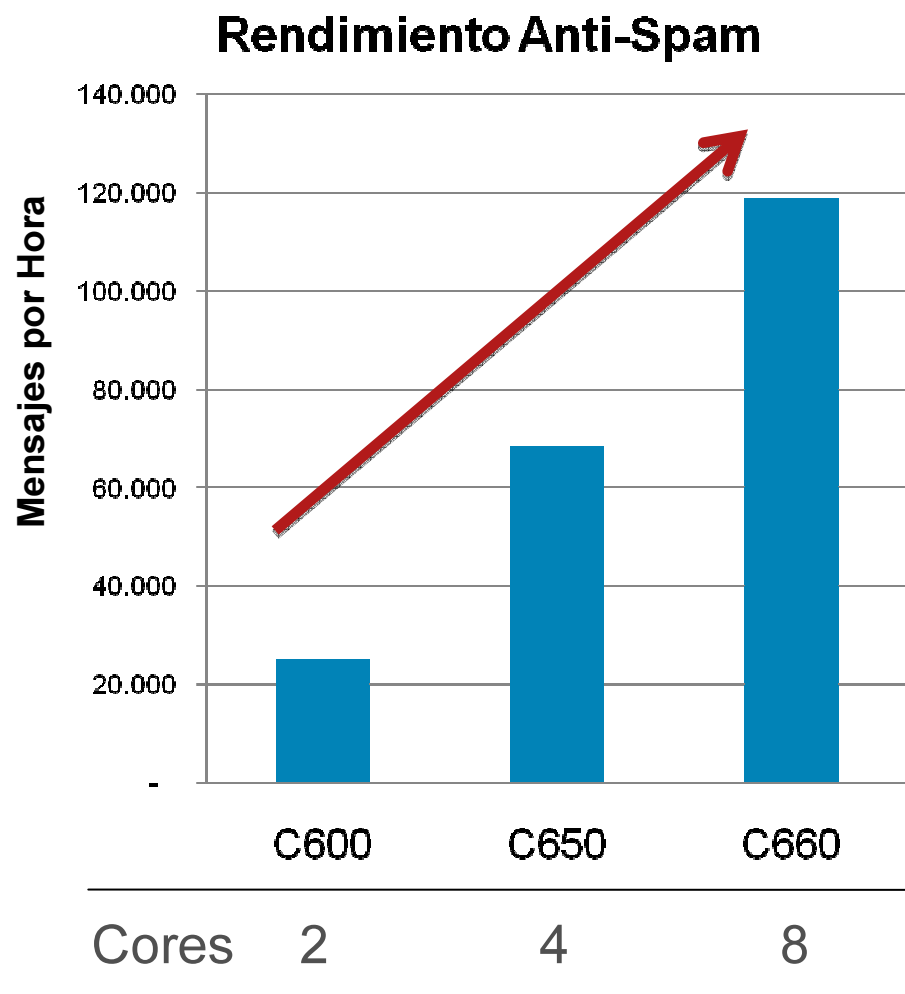
Controladas por el Usuario Final

Validación del Receptor

Elimina Mensajes enviados a destinatarios inexistentes

Arquitectura

Tecnología Multi-Core elimina los Cuellos de Botella



Oferta de Servicios Personalizables

Ofrece amplia Protección y Control

Anti-Spam

- Filtro de Reputación SenderBase
- IronPort Anti-Spam (IPAS)

DLP

- Filtro de Contenido
- Identificadores Inteligentes
- Diccionarios de Contenidos con Peso



Seguridad Entrada

Control de Salida

Cisco IronPort
Solución
Seguridad
Correo

Anti-Virus

- Filtro Anti Epidemias (VOF)
- McAfee Anti-Virus
- Sophos Anti-Virus

Cifrado

- Entrega Segura de Mensajes
- TLS

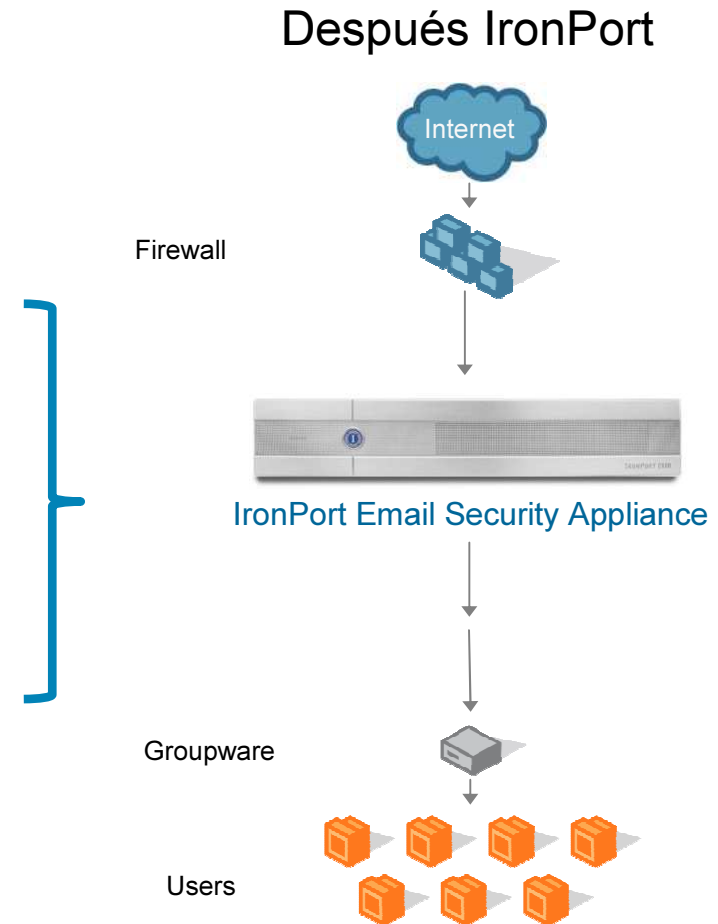
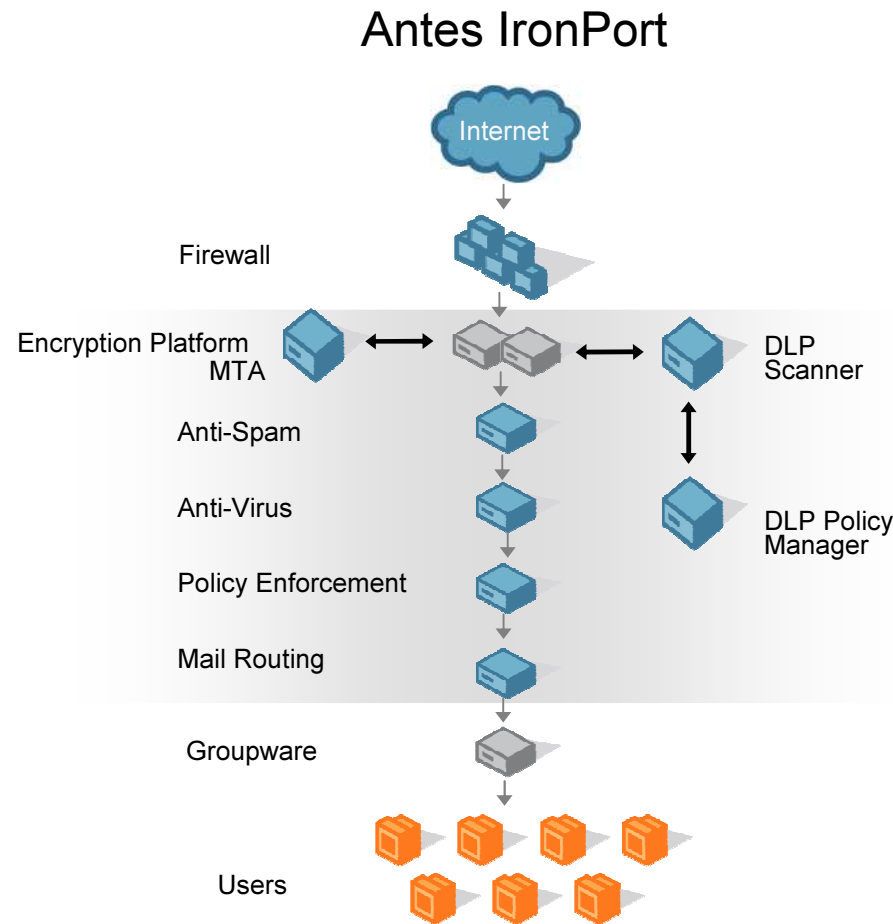


Mejores Prácticas de Diseño y Casos de Éxito

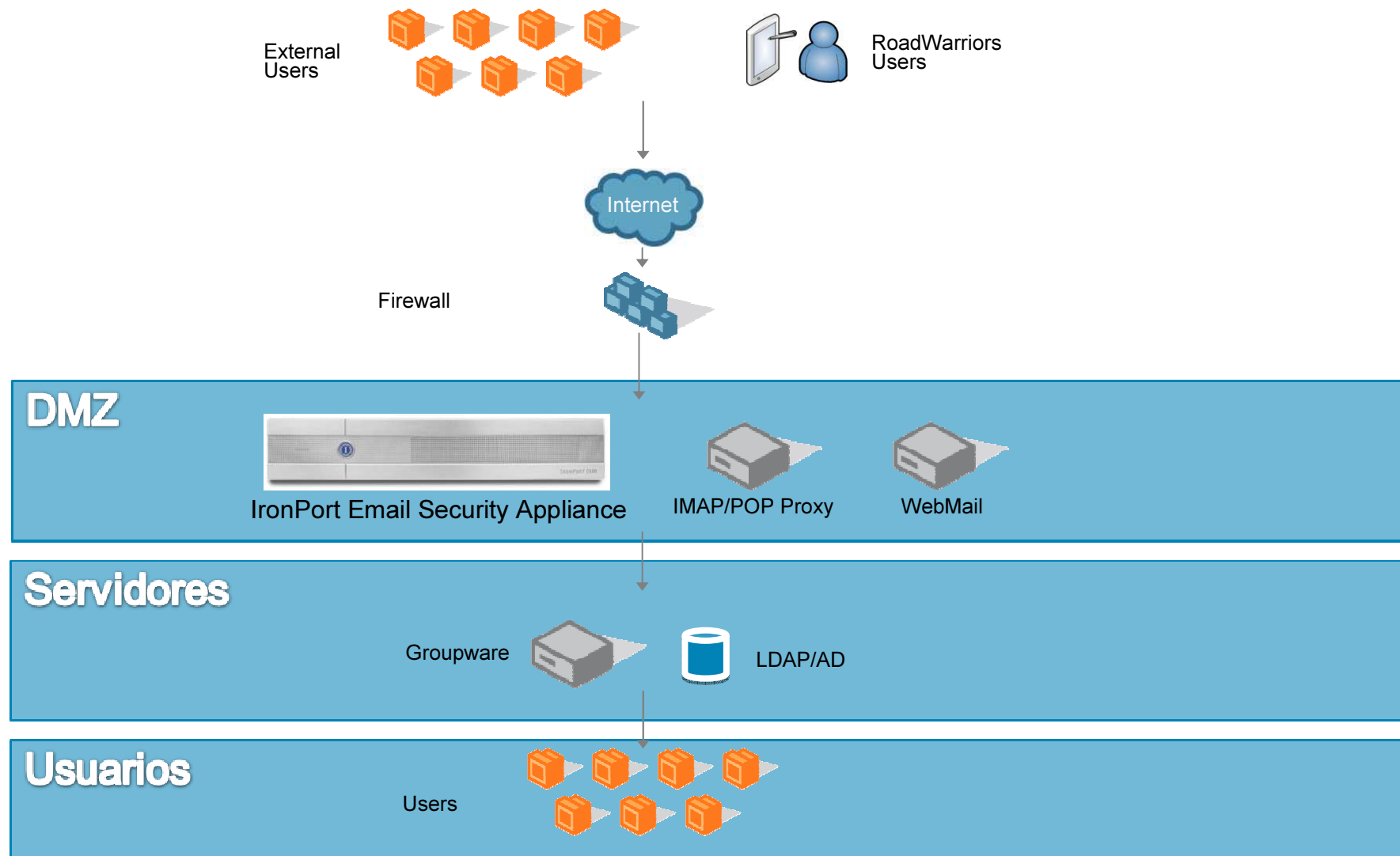


IronPort Consolida la Red Perimetral

Por Seguridad, Confiabilidad y Menor Mantención



Mejores Prácticas en Arquitectura



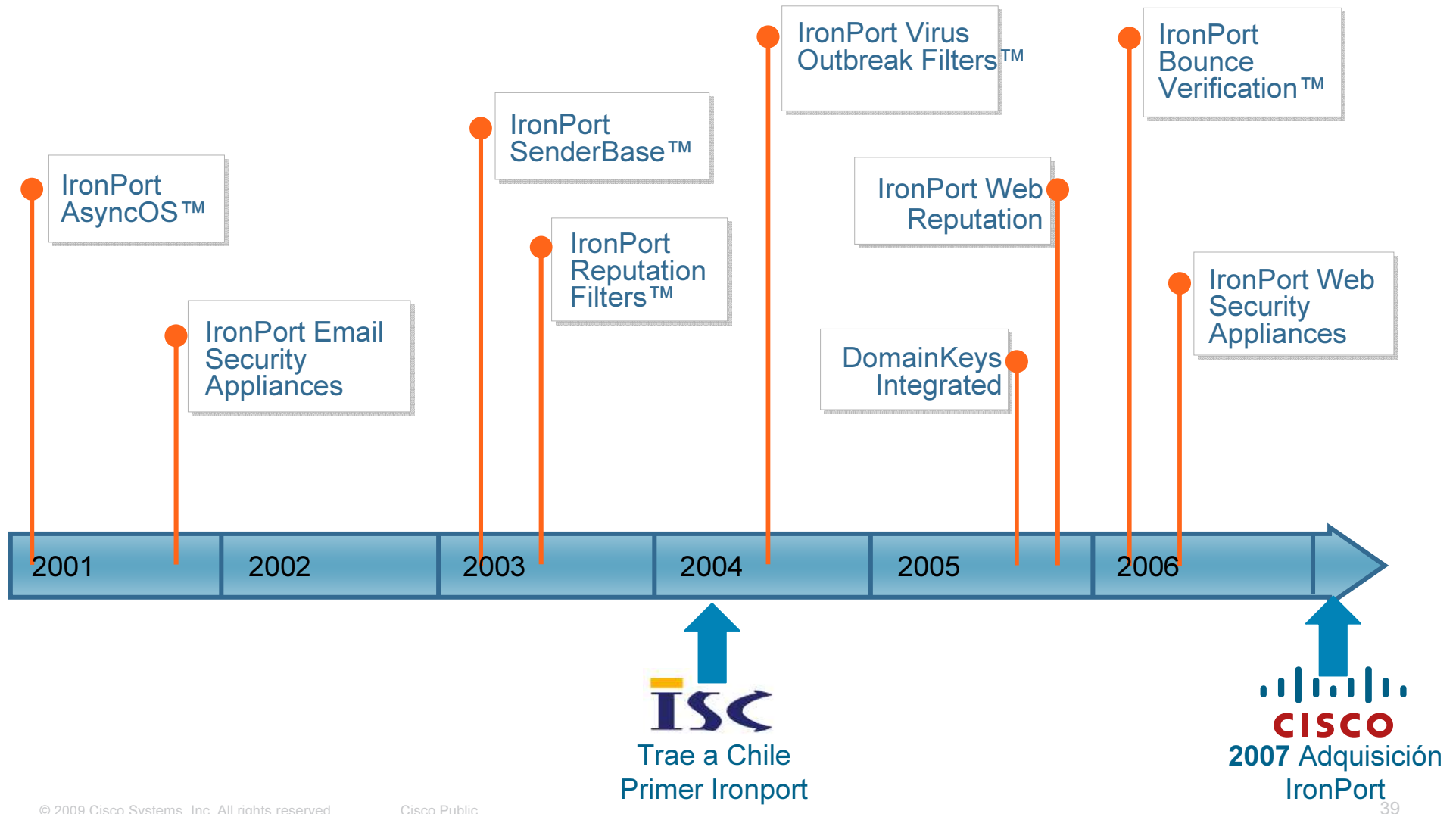


Otras Ventajas



Ingeniería IronPort

Dedicados a la Innovación



IronPort SenderBase

Alcance Global y Precisión

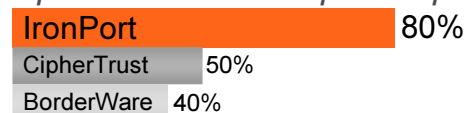
La fuerza dominadora del Tráfico Mundial de Correo y Web.



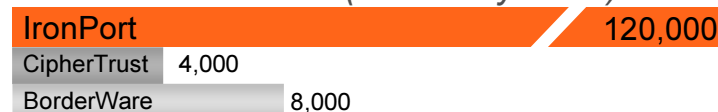
- 5B+ Consultas Diarias
- 150+ Parámetros de Email y Web
- 25% del Tráfico de Correo Mundial

...Resultados en Precisión y protección Avanzada

Spam Identificado por Reputación



Alcances de la Red (Contribuyentes)



Protección Anticipada



* 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.



Beneficios



Beneficios

-  Mejor solución que permite flexibilidad y adaptación al negocio vs mejor control y seguridad en correo.
-  Solución probada y efectiva para todas las amenazas sobre el correo electrónico.
-  Fácil y flexible administración y reportería permitiendo una clara disminución de costos asociados.
-  Minimización de riesgo de fuga y pérdida de información sensible (DLP y PXE).
-  Solución efectiva ante propagación de virus en modalidad epidemia, anticipándose sobre 13 horas al resto de las soluciones.
-  Herramienta robusta para la protección de la plataforma de correo electrónico.
-  Solución especializada, integrada y escalable.
-  Experiencia Local en implementación y soporte en Chile (Líder en el mercado ISP y grandes corporaciones).

Gracias



Preguntas e Inquietudes

Gonzalo Madariaga
gmadariaga@isc.cl