

La Seguridad sin Inteligencia no es Seguridad

Santiago de Chile, 12 de agosto de 2009

Alejandro Viola

Alejandro.viola@bluecoat.com



Blue Coat® and the Blue Coat logo are trademarks of Blue Coat Systems, Inc., and may be registered in certain jurisdictions. All other product or service names are the property of their respective owners.

© Blue Coat Systems, Inc. 2008. All Rights Reserved. Confidential



- Blue Coat Coopera con las organizaciones de TI en la optimización y aseguramiento de la entrega de aplicaciones a los usuarios a través de la empresa distribuida, incluyendo las oficinas remotas y los usuarios móviles
- Como resultado, nuestros clientes pueden alinear sus inversiones en redes con los requerimientos del negocio mientras aseguran una línea de defensa proactiva



- Fundada en 1996, 12 años acelerando y asegurando el tráfico de datos.
- Una de las compañías de mas rápido crecimiento en nuestro mercado (62% este trimestre)
- 15,000+ Clientes Globales
- 2,800 + socios de negocios
- 1,500+ Empleados
- 97 de Fortune 100



- Múltiples reconocimientos de revistas especializadas y analistas
- El Mas reciente: “Editor’s Choice, Network Computing Magazine”, WAN Acceleration Product of the year

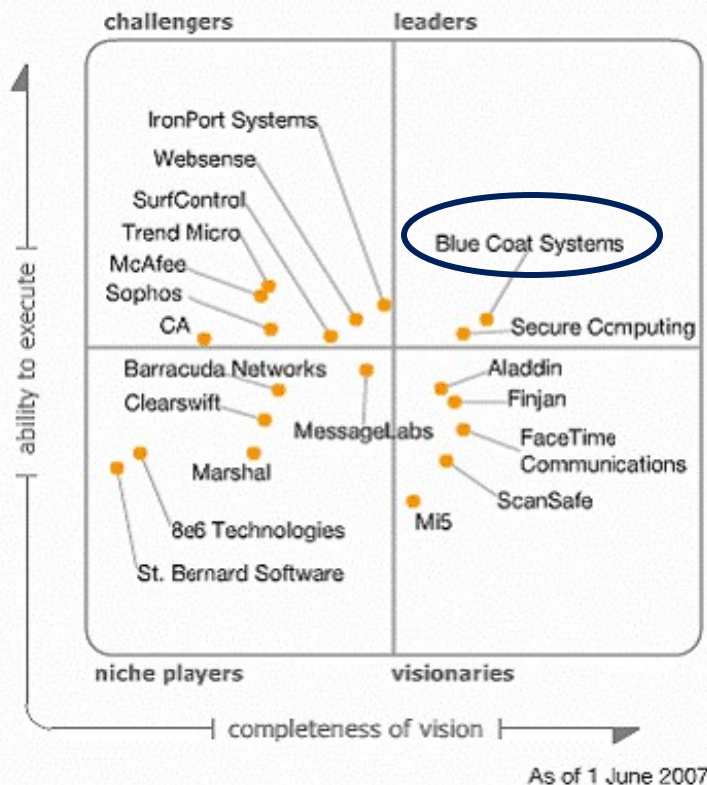
MercuryNews.com
The Mercury News Silicon Valley 150





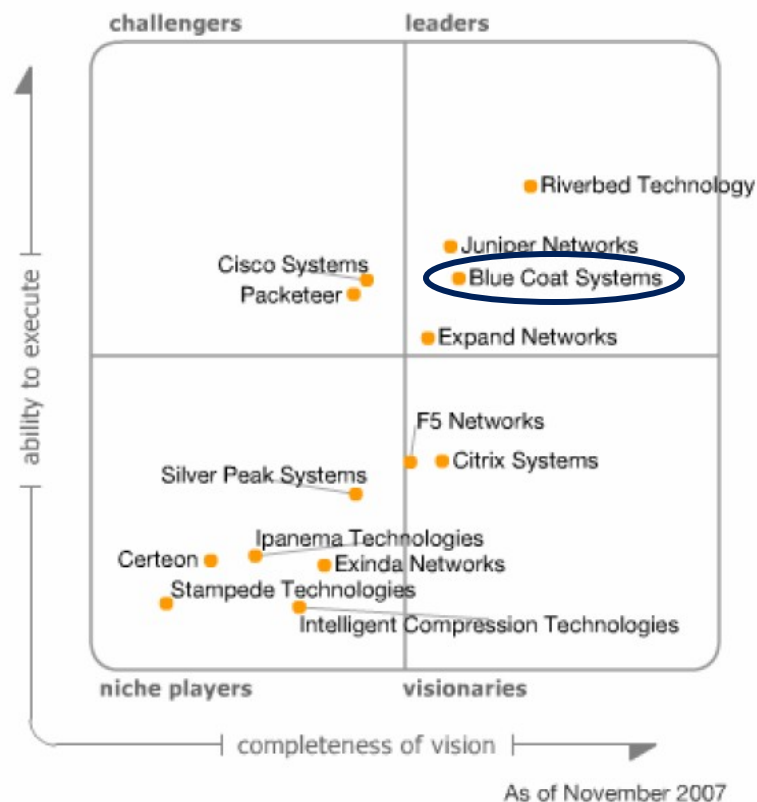
Secure Web Gateway, 2007

*“Blue Coat is one of the few vendors in this market that has **proved its scalability and performance**”*



WAN Optimization Controller, 2007

*“Blue Coat has **strong market understanding, demonstrated** through its broad WOC range and feature set. This includes **HTTPS acceleration, ECDN, a software client (“SoftWOC”) and support for streaming media.**”*





Nuestros clientes confían en nosotros porque:

- ➔ El reto es convertir a TI de un centro de **costos** a un centro de **valor** para el negocio
- ➔ Se requiere tener el **control sobre la entrega de las aplicaciones**
- ➔ Mejorar **la capacidad de respuesta** a los cambios del negocio
- ➔ Proveer **visibilidad** al cumplimiento de normas **y prevención de riesgos**



Nuestros clientes confían en nosotros porque:

- ➔ El reto es convertir a TI de un centro de **costos** a un centro de **valor** para el negocio
- ➔ Se requiere tener el **control sobre la entrega de las aplicaciones**
- ➔ Mejorar **la capacidad de respuesta** a los cambios del negocio
- ➔ Proveer **visibilidad** al cumplimiento de normas y **prevención de riesgos**



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Las empresas cuentan con un buen nivel de control de la red a nivel de **paquetes**. ruteadores, switches y conectividad básica

Hoy se presenta una nueva mezcla de aplicaciones, métodos de acceso y modelos de negocio

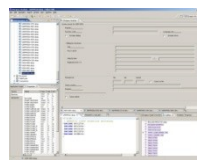


Hay una capacidad limitada para conocer:
Quien está en la red
Que está siendo transportado
y si las expectativas de desempeño están siendo alcanzadas



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

El crecimiento de la demanda genera mayor tráfico en la red



Aplicaciones Críticas

**Red de Entrega
de Paquetes**

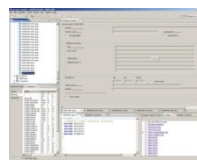
Dificulta mantener el desempeño

Limita la consistencia en la experiencia del Usuario (ERP, CRM, VoIP)



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Malware representa una gran amenaza:



Aplicaciones Críticas



Malware

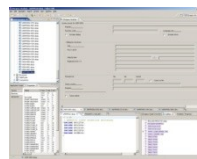
Red de Entrega
de Paquetes

Existen 11 millones de Variantes
75% de las organizaciones serán infectadas (Gartner)



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Se requiere soporte para nuevas aplicaciones basadas en Web



Aplicaciones Críticas



Malware

Red de Entrega
de Paquetes



Aplicaciones
basadas en Web

E-mail
SharePoint, Etc...



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Rápido crecimiento de web 2.0, SaaS, contenido multimedia



Esto genera una gran demanda hacia la red
Algunas son productivas, la mayoría son recreacionales



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Estamos hablando de...

Entrega de Aplicaciones

Como controlarlo???





- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Estamos hablando de...

Entrega de Aplicaciones

Como controlarlo???

- ➔ Conectar a los usuarios a las aplicaciones
- ➔ Cumplir los SLAs
- ➔ Proveer un desempeño consistente
- ➔ Esto requiere:
 - ➔ Una medición constante de la experiencia del usuario
 - ➔ Habilidad para identificar la causa de las desviaciones
 - ➔ Herramientas para optimizar y eliminar fallos



Malware

Aplicaciones Críticas

Red de Entrega
de Paquetes



Aplicaciones
basadas en Web



Web 2.0
SaaS, Video

Un enfoque en la entrega de aplicaciones requiere capacidades que van mas allá de una infraestructura de administración de paquetes



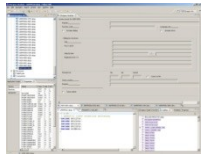
- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Estamos hablando de...

Entrega de Aplicaciones

No se trata solo de acelerar, se trata de:
 Entender las características de la aplicación en la red
 respecto a localidades específicas,
 usuarios específicos
 y la mezcla de otras aplicaciones que están
 ejecutándose simultáneamente

Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega
de Paquetes



Aplicaciones
basadas en Web



Web 2.0
SaaS, Video



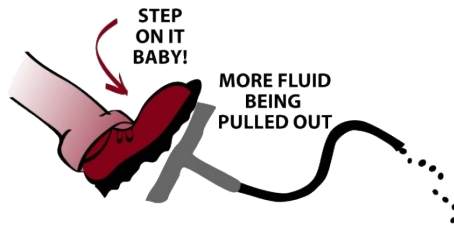
**Un enfoque en la entrega de aplicaciones requiere
 capacidades que van mas allá de una infraestructura
 de administración de paquetes**



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

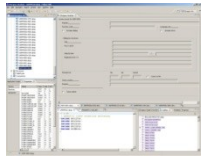
Estamos hablando de...

+ Entrega de Aplicaciones +



Adicionalmente,
la infraestructura se vuelve mas compleja, pues:

Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega de Paquetes



Aplicaciones basadas en Web



Web 2.0 SaaS, Video

Hay nuevos usuarios, cada vez mas distribuidos:

- ➔ Oficinas remotas
- ➔ Usuario móviles
- ➔ Socios de negocios



La distancia entre aplicaciones y usuarios es mayor

- ➔ Consolidación
- ➔ Hosting externo





- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

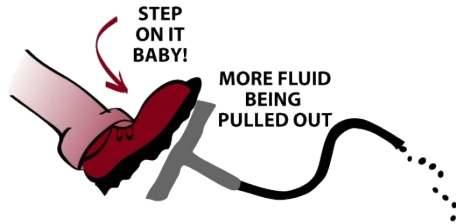
Estamos hablando de...



+ Entrega de Aplicaciones +



Prioridades de IT (Encuesta)



Incremento al Ancho de Banda



Que está pasando por la red?
 Como se desempeñan las aplicaciones?
 Que debe ser modificado?



Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega de Paquetes



Aplicaciones basadas en Web



Web 2.0 SaaS, Video



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

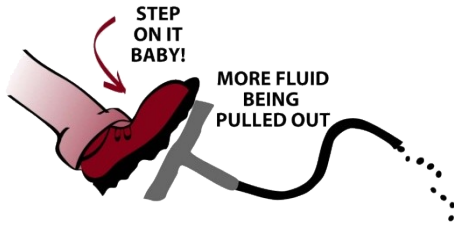
Estamos hablando de...



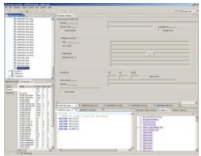
+ Entrega de Aplicaciones +



Prioridades



Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega de Paquetes



Aplicaciones basadas en Web



Web 2.0 SaaS, Video

Incremento al Ancho de Banda



Que pasa Desempeño
Que cambiar

Desempeño de Aplicaciones



+Desempeño
+Acertividad
+Ahorro

Seguridad en la red



Es Malicioso? Alto!!!
Control Usuarios



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

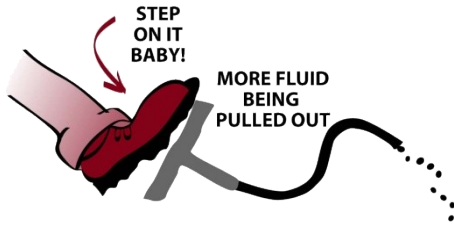
Estamos hablando de...



+ Entrega de Aplicaciones +



Prioridades



Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega de Paquetes



Aplicaciones basadas en Web



Web 2.0 SaaS, Video



Incr... al
Anc... de Banda

Visibilidad

Que pasa
Desempeño
Que cambiar



De... de
Aplicaciones

Aceleración

+Desempeño
+Acertividad
+Ahorro



Se... ad...
Seguridad

Es Malicioso?
Alto!!!
Control Usuarios



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

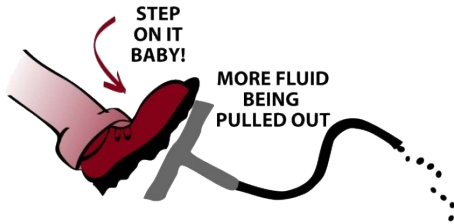
Estamos hablando de...



+ Entrega de Aplicaciones +



Prioridades



Como controlarlo???



Aplicaciones Críticas

Red de Entrega de Paquetes



Aplicaciones basadas en Web



Web 2.0 SaaS, Video

Incremento al Ancho de Banda

Análisis de Tráfico
600+ Aplicaciones
Consumo x App.
Monitoreo
Medición
Alarmas
Estadísticas

Desempeño de Aplicaciones

Aceleración de:
Tráfico Crítico
Donde se requiere
Desempeño
Cualitativo
Técnicas adecuadas
Aceptividad
Ahorro

Seguridad en la red

Detección de Malware
Cloud services
1B de análisis x semana
54M usuarios
Es Malicioso?
Refuerzo de políticas
Control Usuarios



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Estamos hablando de...



+ Entrega de Aplicaciones +



Prioridades



Visibilidad

QUE
COMO
CAMBIAR?

Incremento al
Ancho de Banda

Análisis de Tráfico
600+ Aplicaciones
Consumo x App.
Monitoreo
Medición
Alarmas
Estadísticas



Aceleración

Desempeño
Acertividad
Ahorro

Desempeño de
Aplicaciones

Aceleración de:
Tráfico Crítico
Donde se requiere
Cuando se requiere
Técnicas adecuadas



Seguridad

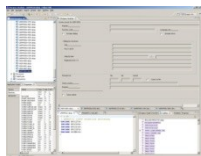
Es Malicioso?
Alto!!!

Control Usuarios

Seguridad
en la red

Detección de Malaware
Cloud services
1B de análisis x semana
54M Usuarios
Refuerzo de políticas

Como controlarlo???



Malware

Aplicaciones Críticas

Red de Entrega
de Paquetes



Aplicaciones
basadas en Web



Web 2.0
SaaS, Video



Estamos hablando de...



+ Entrega de Aplicaciones +



Prioridades

- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos



Integradores

?

?

?

Limitaciones de desempeño, complejidad, alto costo, falta de integración

Aceleradores

X



X

Limitaciones en inteligencia, QoS, multimedia, voz, y aplicaciones externas

Seguridad

X

X



Enfoque solo en la red, limitaciones en web y entrega de aplicaciones complejas

Analizadores



X

X

Visibilidad rudimentaria, falta de integración



- Centro de costos a centro de valor
- Control sobre la entrega de las aplicaciones
- Capacidad de respuesta
- Visibilidad y prevención de riesgos

Estamos hablando de...



+ Entrega de Aplicaciones +



ADN



Experiencia
Crecimiento
Reconocimiento
Liderazgo

PacketShaper

Intelligence Center

VISIBILIDAD



ProxySG

ProxyClient

Director

ACELERACION



ProxySG

ProxyClient

WebFilter

ProxyAV

WebPulse

Reporter

SEGURIDAD

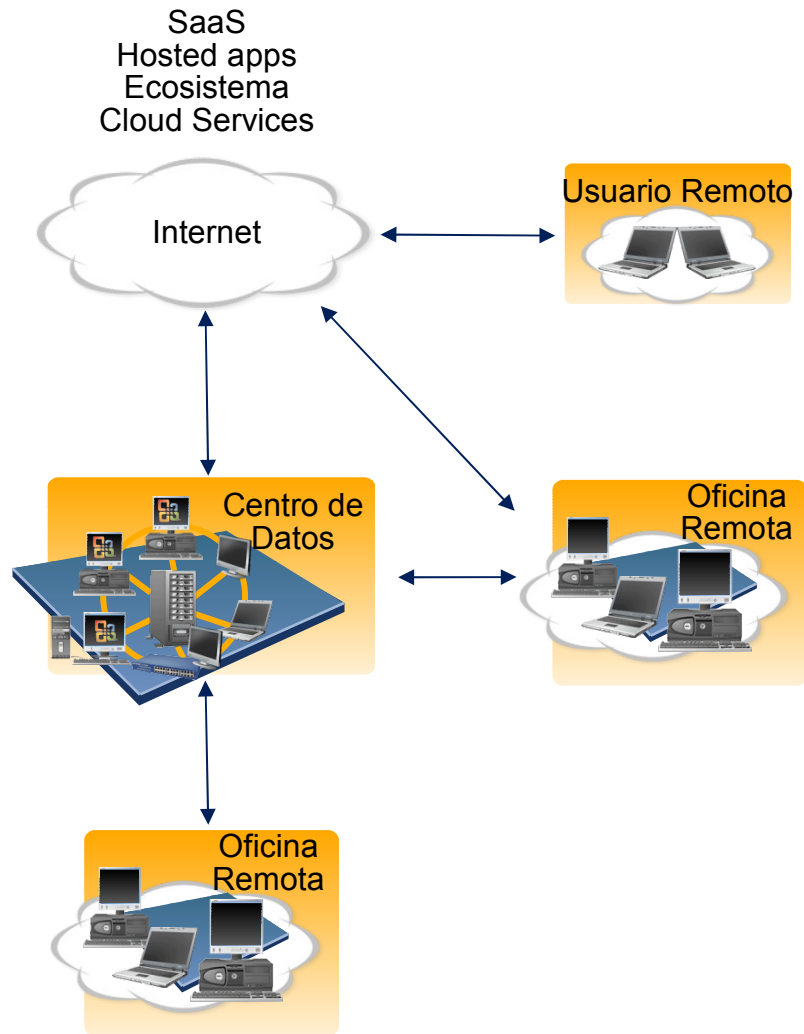
Dirección Futura

Una estrategia agresiva y mapa de soluciones (roadmap) para avanzar en la integración de tecnologías de seguridad, aceleración y visibilidad al corazón de la red de entrega de aplicaciones



Blue  Coat[®]

Gracias!!



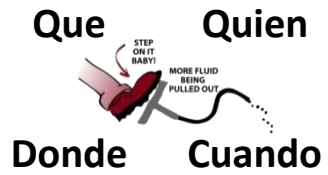
Requerimiento:
Posible causa:
Paradigma:
Solución:
Duda:

Problemas de desempeño
La red
Que está corriendo en la red, lo sabe? (ej. Puerto 80)
Incrementar el ancho de banda vs controlar su uso
Que está pasando por la red?



200 Aplicaciones promedio
Competencia core vs no core

120 Estadísticas que indican:
Que aplicaciones están Corriendo
Que tiempos de respuesta hay
Donde están los retrasos (servidor o red)
Que y quien causa los picos

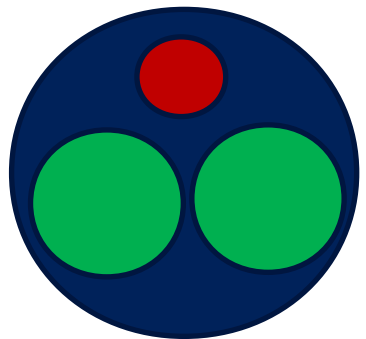


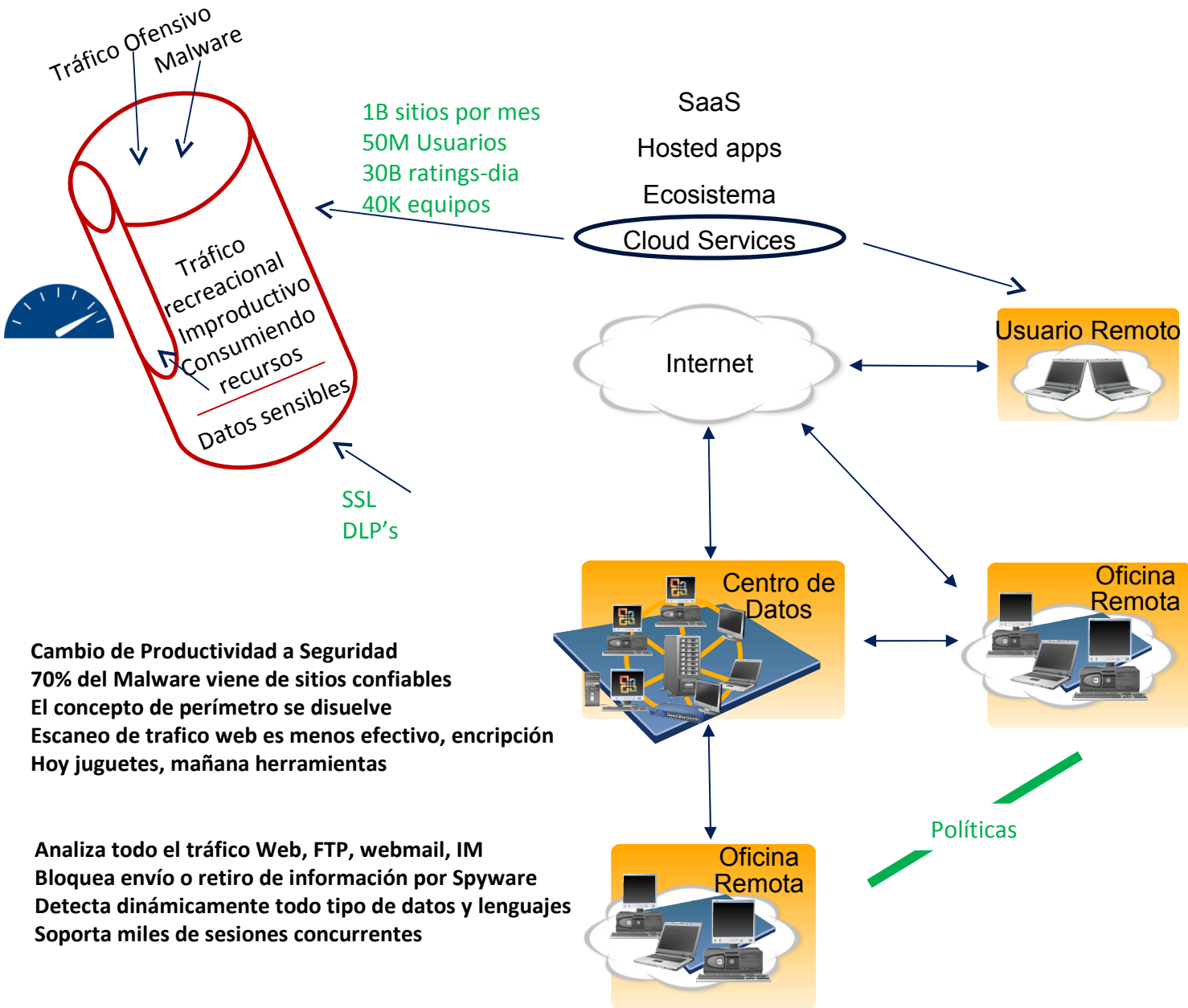
Clasificación de 600+ Aplicaciones
Análisis en capa 7+
Monitoreo de la calidad en audio y video conferencia
En tiempo real, con tráfico real
Analiza y aplica QoS granular al tráfico
Inteligencia de Aplicaciones vs direcciones y puertos
Herramientas para clasificar aplicaciones críticas
Granularidad extrema



Resultados

Mejor administración y planeación del ancho de banda
Maximo aprovechamiento de la infraestructura actual
Ahorro en incrementos de ancho de banda
Reducción de costos operativos
Cumplimiento de SLAs
Aseguramiento de aplicaciones en tiempo real (voz, video)





Cambio de Productividad a Seguridad
 70% del Malware viene de sitios confiables
 El concepto de perímetro se disuelve
 Escaneo de trafico web es menos efectivo, encriptación
 Hoy juguetes, mañana herramientas

Analiza todo el tráfico Web, FTP, webmail, IM
Bloquea envío o retiro de información por Spyware
Detecta dinámicamente todo tipo de datos y lenguajes
Soporta miles de sesiones concurrentes

