GRUPO SOROM

S.O.S. Soluciones Optimas Symantec

symantec™

make it HAPPEN!

GRUPO SOROM

… algunas de las preocupaciones

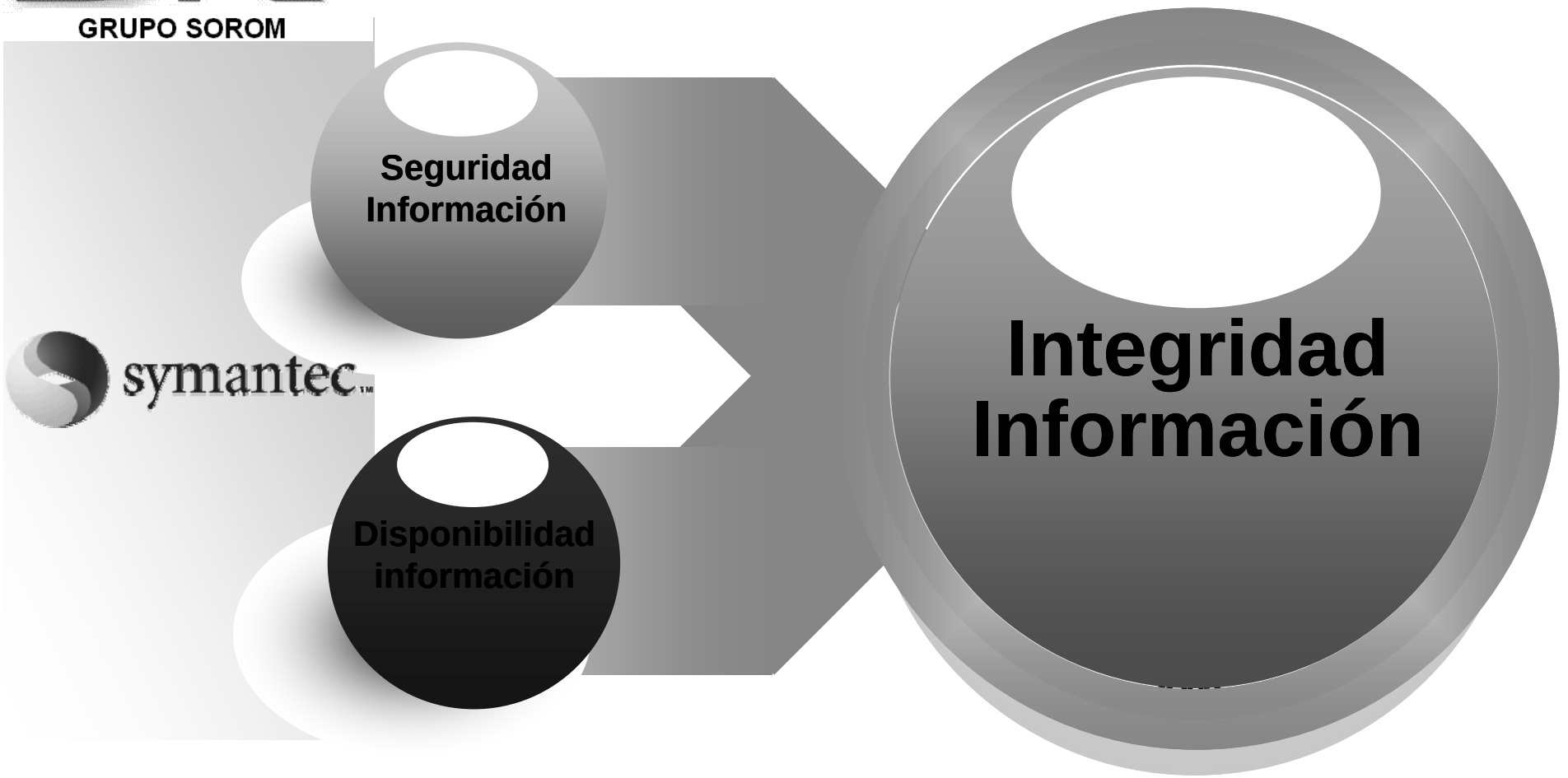
- Un día sin correo electrónico o sin la base de datos…
- Recuperación de los mismos en el tiempo requerido
- Se me daño mi máquina, me prestan otra como me recupero
- Tengo los datos, no tengo aplicaciones
- Me llega correo “basura”
- Mi servidor “esta mandado” correos que no son míos
- No quiero entrar a la página de mi banco, no se si están “espiando” mi computadora
- Me dicen que necesito un “firewall personal” … yo ya tengo un antivirus
- No quiero que mis empleados “naveguen” libremente ni “almacenen” libremente
- Mis usuarios almacenan todo tipo de información: videos, MP3, juegos, etc.

symantec.

Symantec = Integridad de la Información

GRUPO SOROM

symantec



symantec

GRUPO SOROM

y si mi información no es integra ?

symantec.

GRUPO SOROM

¿Qué es una amenaza?

- Una actividad que puede ocasionar algún daño
- Puede venir en diferentes formas y fuentes
- Es imposible protegerse de todas ellas
- Spyware & Adware, Spam, Phishing, Virus, Worm, Caballos de Troya, amenazas combinadas
- Debemos protegernos de aquellas que:
  - Afecten al objetivo del negocio
  - Modifiquen la información
  - Protegerse de ellas utilizando los estándares “Mejores Practicas”

symantec.

GRUPO SOROM

¿Qué son las vulnerabilidades?

- Debilidades que permiten que las amenazas nos afecten
  - Las vulnerabilidades permiten crear amenazas
- Debe venir acompañada de una amenaza para que tenga efecto
  - Las vulnerabilidades no tienen efecto hasta que alguien las aplica
- Se pueden prevenir (Si se les conoce con antelación)
  - Estar enterado con antelación de los problemas nos permite tomar medidas antes de que las cosas pasen

symantec.

GRUPO SOROM

¿Qué es un riesgo?

- Es la probabilidad de que algo malo pase con la información
  - Algunos riesgos no pueden controlarse
- La exposición a una amenaza
  - Las vulnerabilidades pueden crear amenazas
- El riesgo es subjetivo
  - Para algunas personas caminar por la calle puede ser seguro
- Depende de la situación y del momento

symantec.

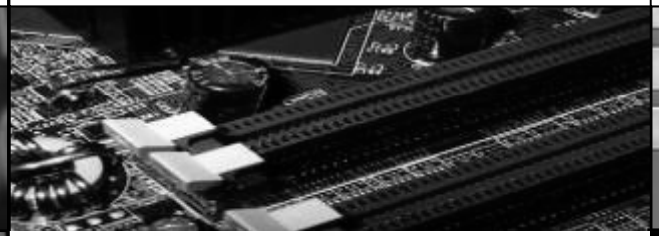
GRUPO SOROM

Riesgos

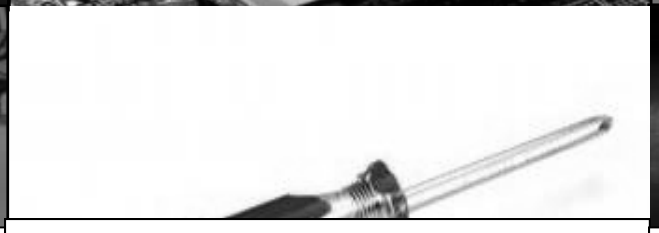
CORRUPCION DE DATOS

FALLA DE COMPONENTES

FALLA DE APLICACIONES



ERROR HUMANO



MANTENIMIENTOS

CATASTROFES

symantec.

GRUPO SOROM

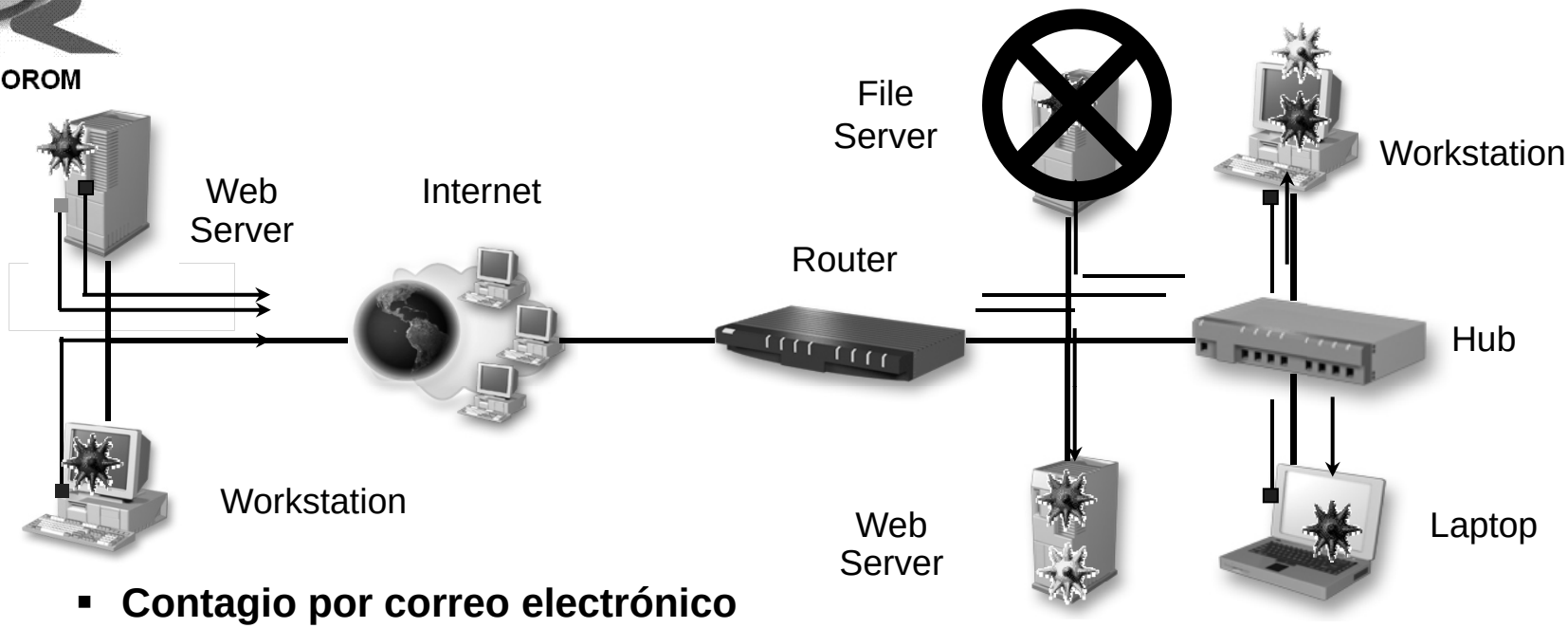
Relación riesgo, amenaza, vulnerabilidad

RIESGO = AMENAZA X VULNERABILIDAD

symantec.

GRUPO SOROM

Evolución de las amenazas



- **Contagio por correo electrónico**
- **Contagio por acceso a Web Server**
- **Contagio de archivos contenidos en la pc**
- **Contagio por navegación**
- **Contagio por recursos compartidos**
- **Perdida de Informacion, NO HAY RESPALDOS**

► Resultado: 2.2M de sistemas afectados en 3 días

symantec.

GRUPO SOROM

Resultados - estudio Spyware (Estados Unidos)

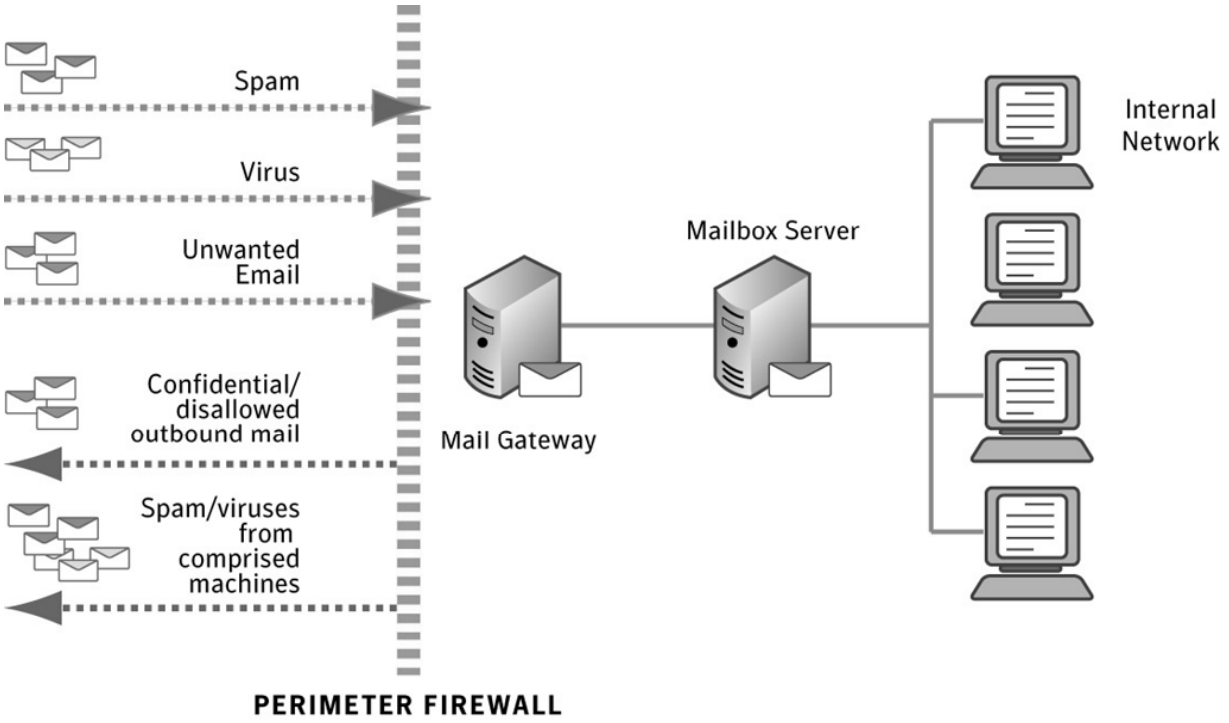
Amenazas encontradas	Noticias	Niños	Deportes	Compras
Adware	3	359	17	0
Spyware	1	0	2	0
Hijackers	0	3	0	0
Cookies	26	31	72	10
Espacio en disco (Mg)	33,782,646	73,080,832	34,684,928	28,639,232
Archivos guardados en disco	2,578	1,801	2,219	2,623

symantec.

GRUPO SOROM

El correo en el perímetro es el principal blanco de ataques

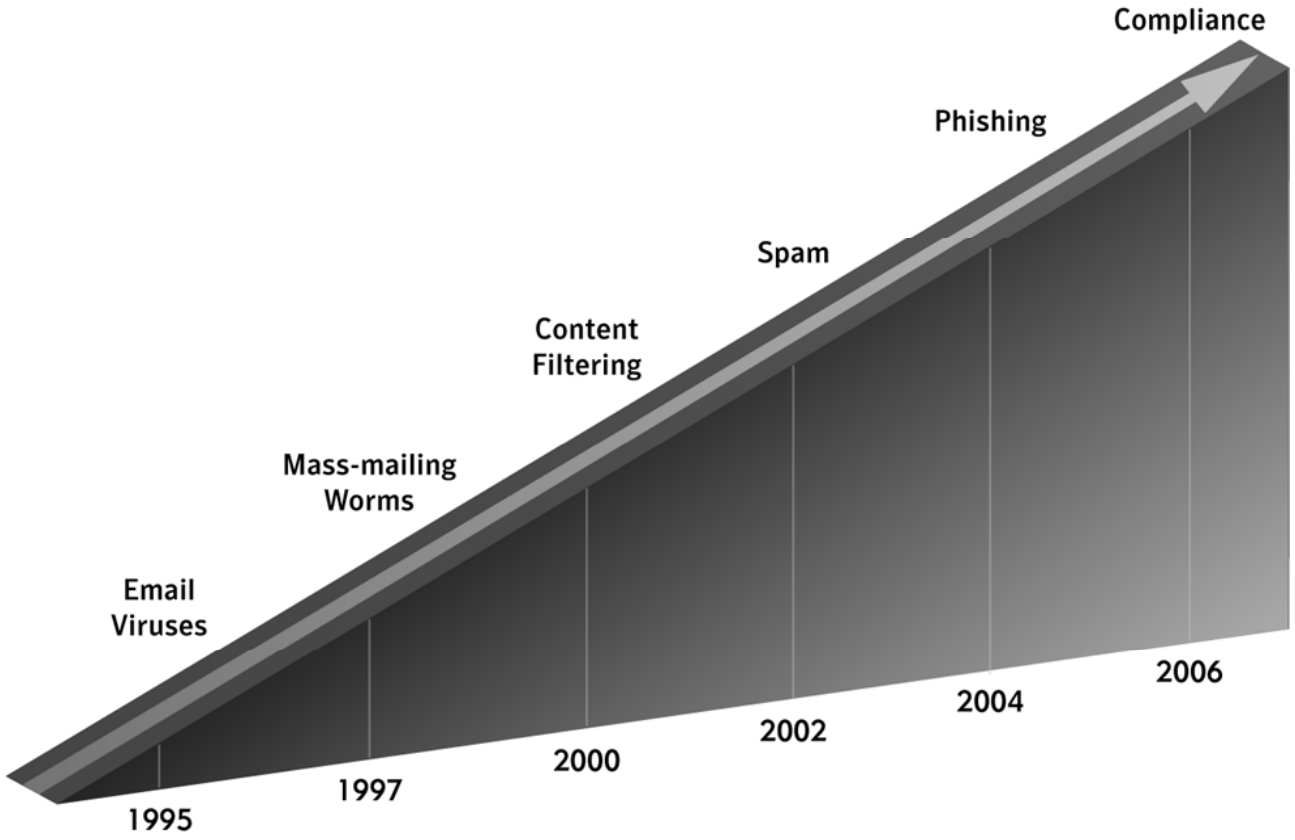
- Tráfico de entrada puede tener código malicioso
- Tráfico de salida puede contener información confidencial



symantec

GRUPO SOROM

Evolución de la problemática del correo



symantec

GRUPO SOROM

Problemas de seguridad en el correo

Spam

- Pérdida productividad
- Desperdicio recursos
- Manejo de falsos positivos

Viruses and Malicious Content

- Caídas de sistemas
- Equipos comprometidos

Escalating Unwanted Traffic at Gateway

- Mala utilización ancho banda
- Sobrecarga de recurso en el servidor y
- Incremento en el costo

Content Control

- Falta de reforzamiento de políticas
- Vulnerabilidades
- Demandas

Retos para los administradores de correo

1. Mantener a salvo la organización de los ataques al correo
2. Mantener el flujo de correo vital de fuentes legítimas
3. Hacer lo anterior con la menor administración posible

symantec.

GRUPO SOROM

Ya respaldo mis servidores … ¿necesito respaldar mis PCs?

60% del capital intelectual (información del negocio) esta fuera del site y reside en las PCs / laptops de los empleados.

– IDC, April 2002

… le robaron la laptop al director, tenemos su respaldo?

… ya que el gerente de ventas borró un directorio (clientes y forecast)

… un empleado dejo la Empresa, está disponible su información?

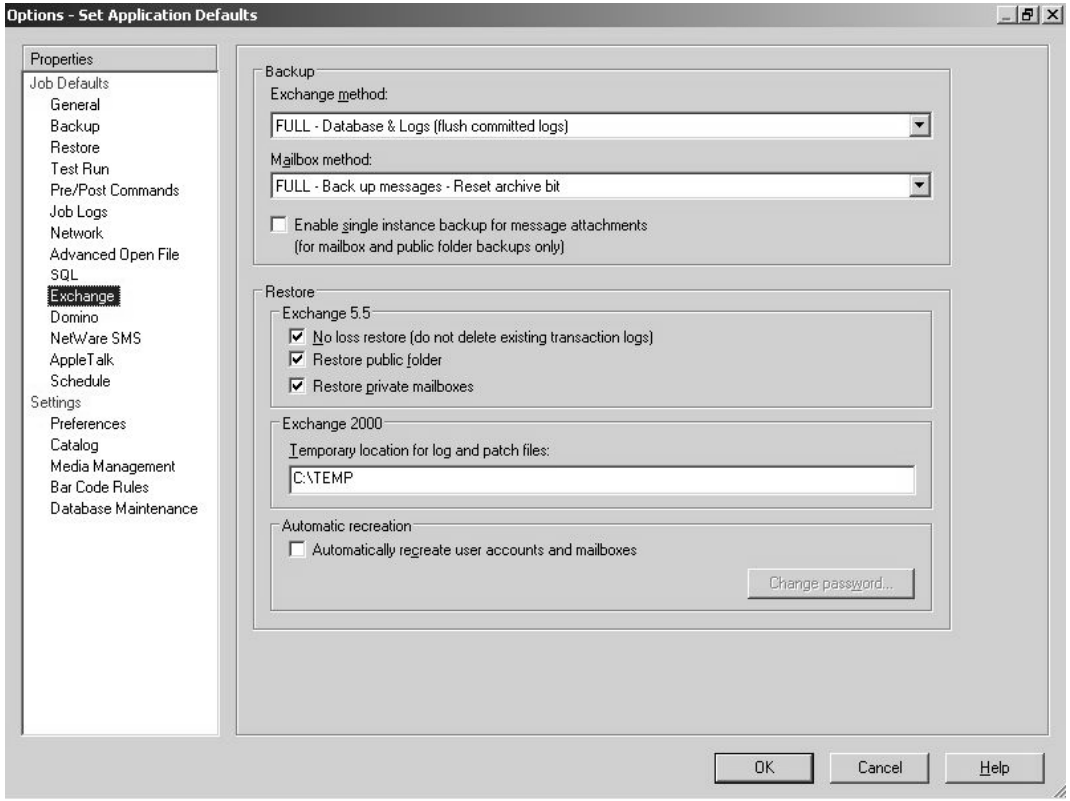
… el área de mercadotecnia “no encuentra” su información

… ya que cuentas por cobrar no sabe a quien cobrar PERDIO 1 archivo

symantec.

GRUPO SOROM

Proteger en línea mis servidores



Microsoft Windows Server System

ORACLE

SAP

DB2. Information Management Software

Lotus. software

SYBASE

Opción de archivos abiertos para aplicaciones no soportadas:

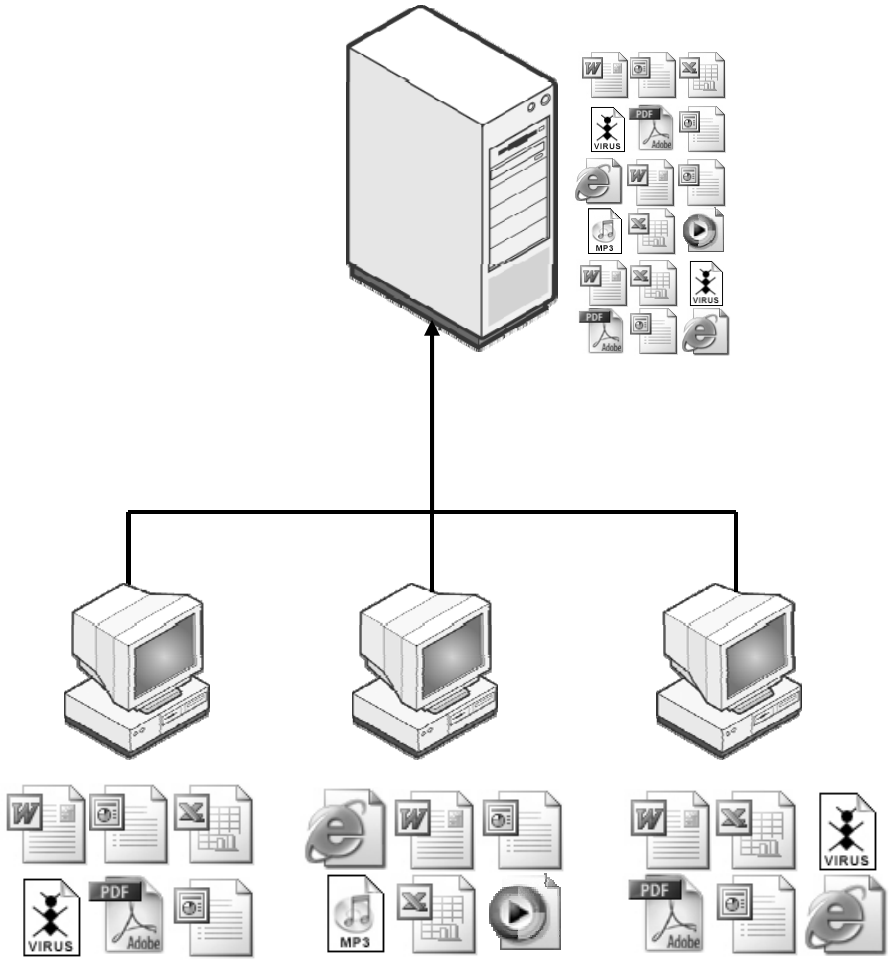
PROGRESS SOFTWARE

SIEBEL

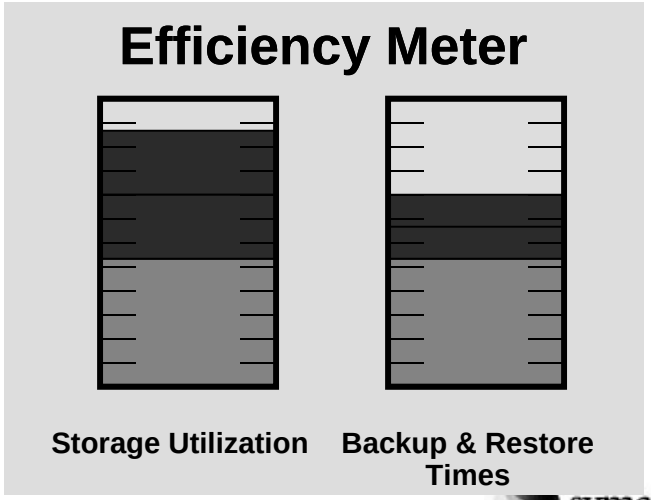
symantec.

GRUPO SOROM

¿Qué se almacena en los servidores



- Usuarios guardando…
- Almacenamos todo, lo que sea, sin limite y control
- Uso ineficiente de los recursos
- Incrementamos los tiempos de respaldos

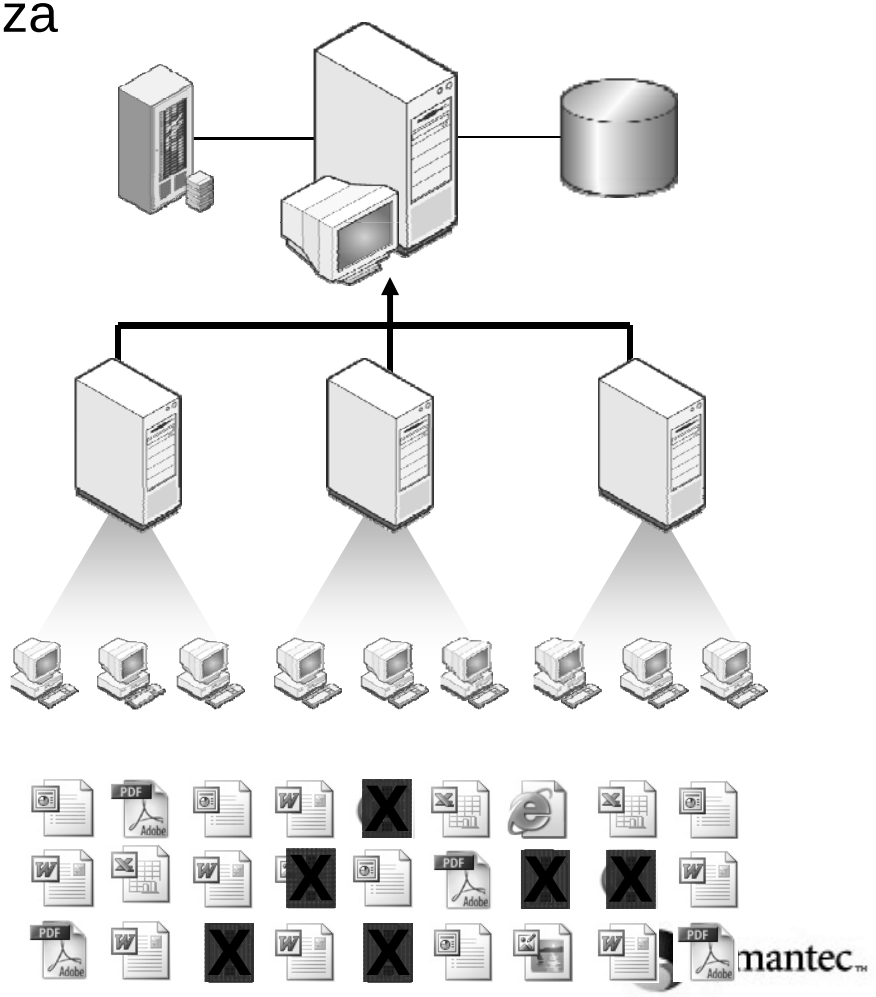


symantec™

GRUPO SOROM

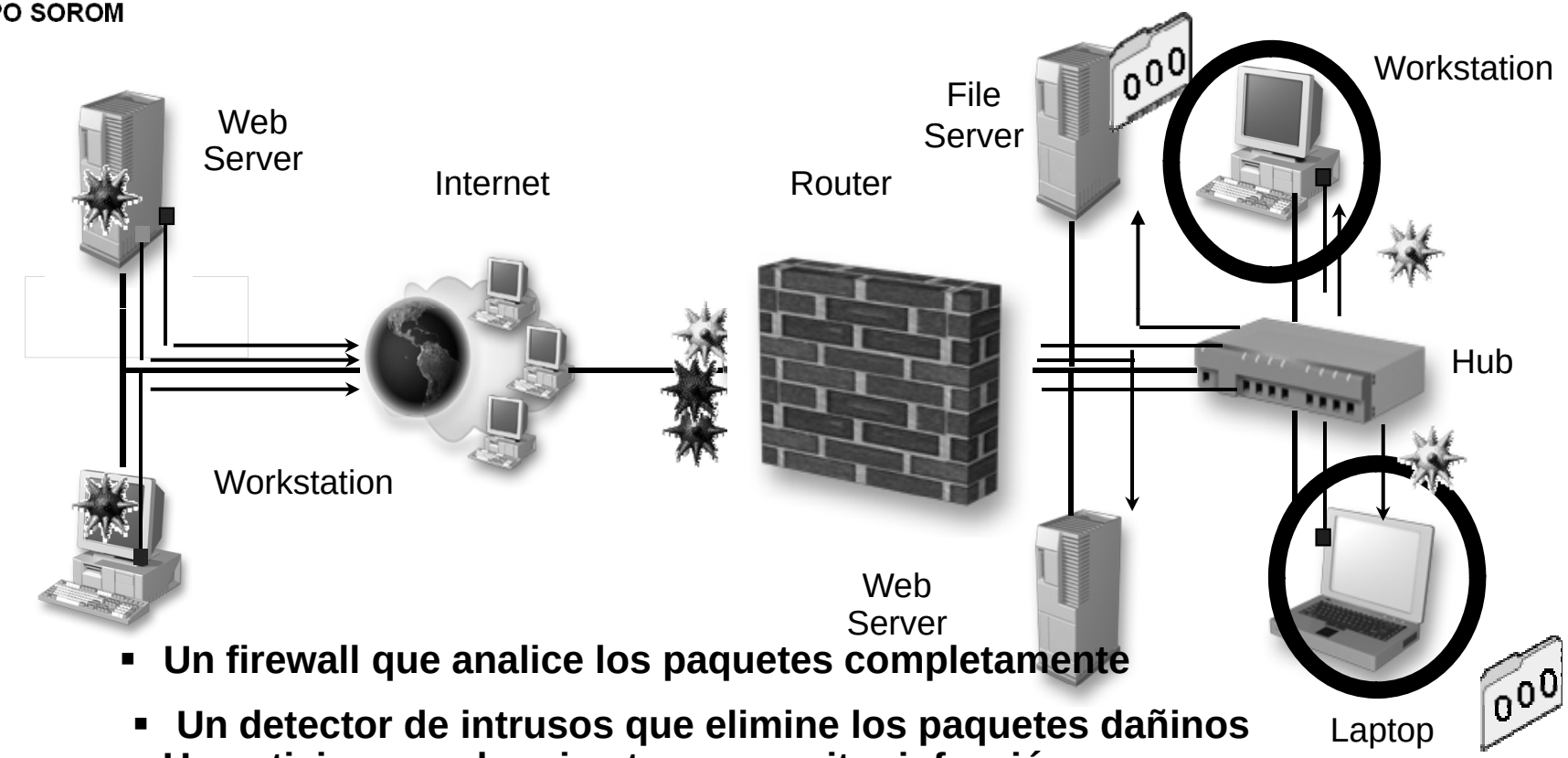
Libera espacio en tus servidores y estaciones

- Automatización de Cuotas Maximiza Recursos de Almacenamiento
- Bloqueo de archivos NO DESEADOS de manera Proactiva Archivos ajenos al negocio
- Generación de reportes



GRUPO SOROM

Cómo ayuda Symantec

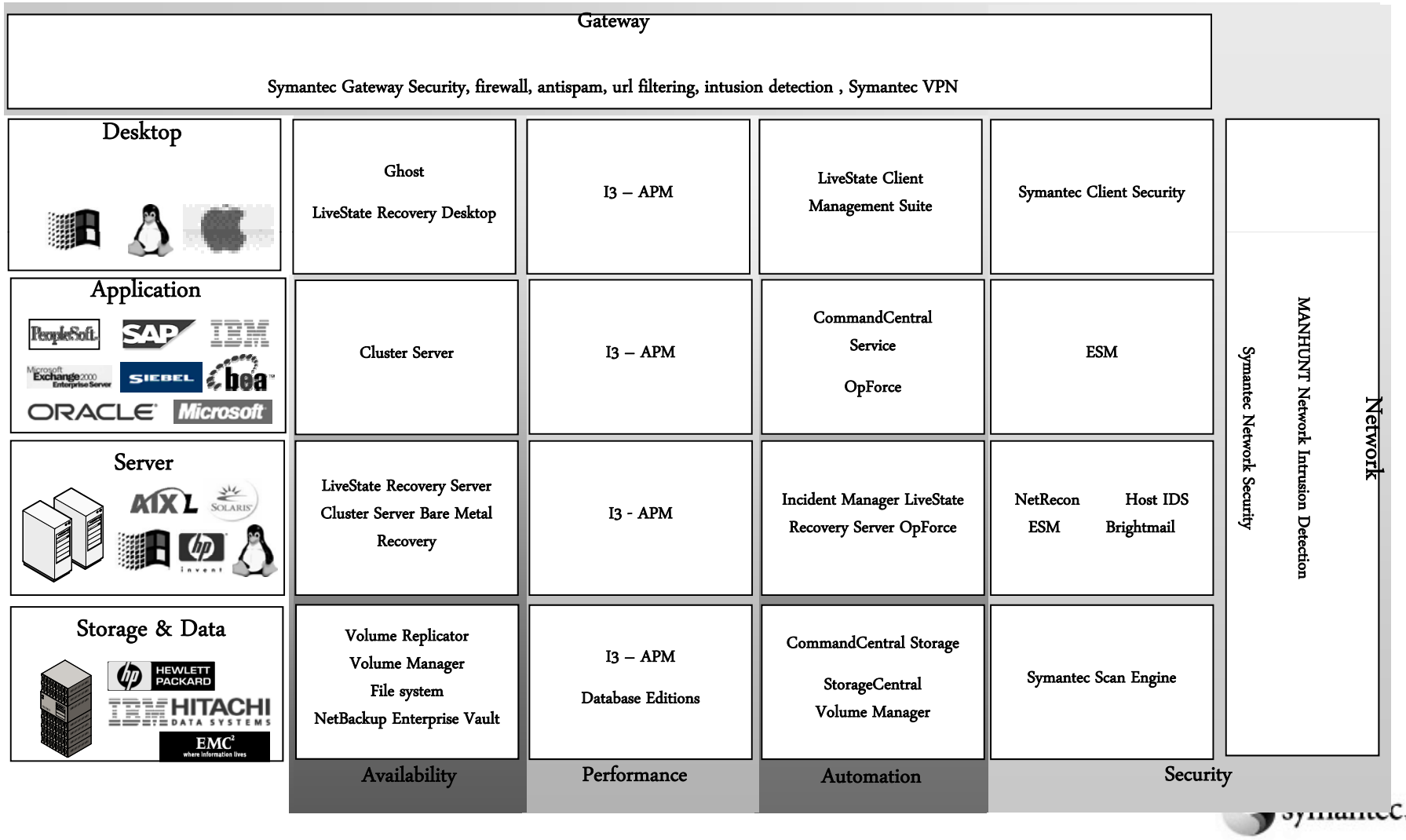


- **Un firewall que analice los paquetes completamente**
- **Un detector de intrusos que elimine los paquetes dañinos**
- **Un antivirus en el perimetro para evitar infección**
- **Reporte con los intentos de ataque, inclusive internos**
  - **Recuperacion de la Informacion Perdida**

symantec.

GRUPO SOROM

Portafolio de Soluciones



Para mayor información:

GRUPO SOROM ASESORES, SA DE CV

Ote 4 #1840 Desp. C
Col. Centro
CP. 94300, Orizaba, Ver.
Email: sorom@prodigy.net.mx
vtasorom@prodigy.net.mx

Tel: (52) 272-724 4211
272-724 7894
272-724 8053

www.grupo-sorom.com.mx