



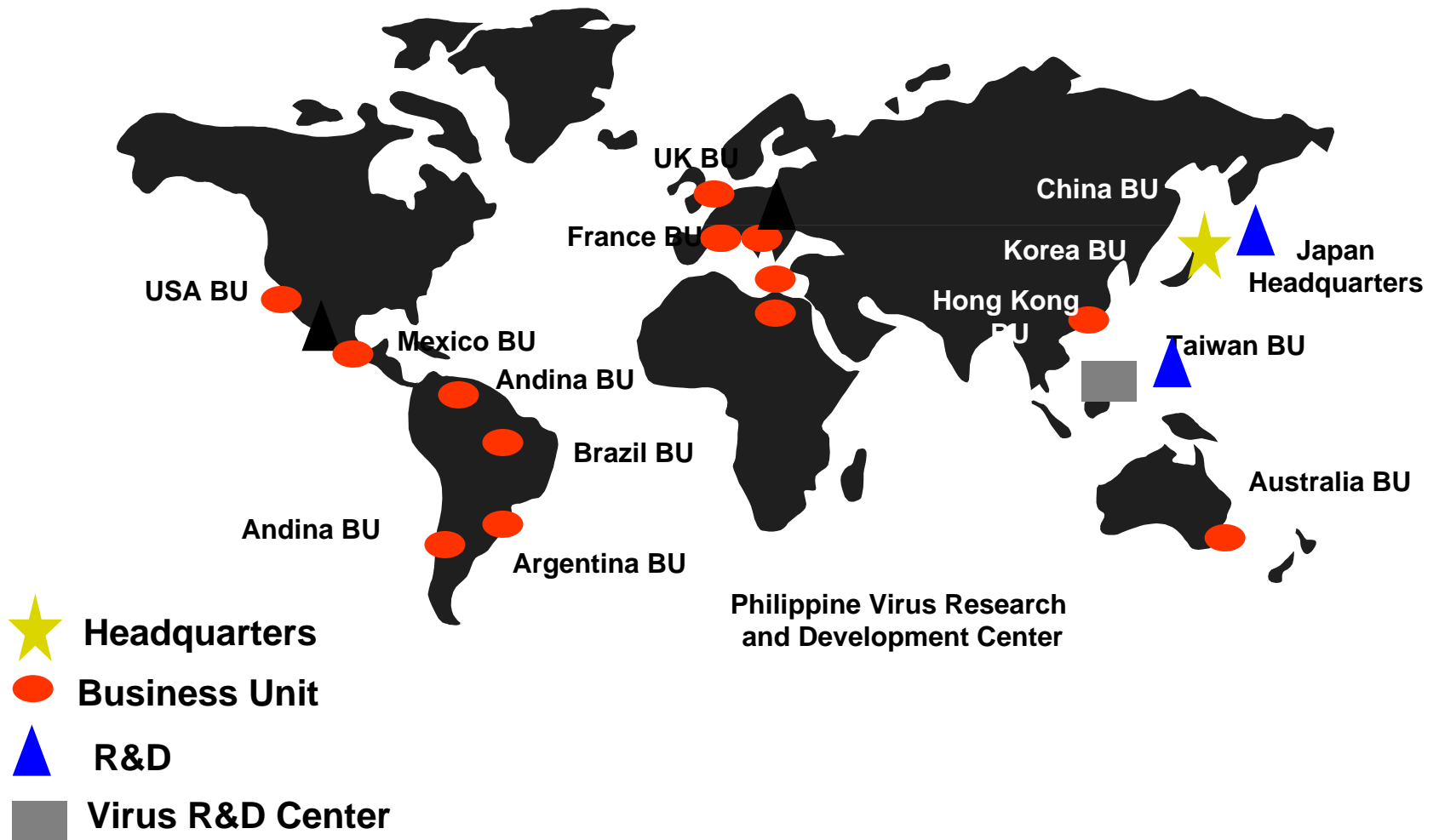
# Trend Micro

## Su Organización y Estructura



- Líder global en antivirus y software de seguridad de información.
  - #1 Líder global de mercado en protección de virus basada en servidores.
  - #1 Líder global de mercado en protección de gateway y servidores de correo electrónico.
- Establecida en USA en 1988;
- Oficina central en Tokio, Japón
  - Su fundador y CEO ,Steve Chang.
  - 47 % de crecimiento Q3 02 vs Q3 03.
  - Cotiza en los mercados públicos de USA y Japón
  - + de 1800 empleados, 23 unidades de negocio en el mundo.
- Más de 450 ingenieros de virus en el mundo







# Servicio y soporte de excelencia

- Premium Support
  - + 450 ingenieros en el mundo
  - TAM dedicados.
- Entrenamiento y certificación.
  - Certificación local.
  - + de 150 en Venezuela
- TrendLabs Certifications ISO 9002
  - 2 hrs tiempo de respuesta para clientes Premium Support.





Issued at BQR Ltd, Fitchburg, MA,01420, USA

*Certificate of Registration*  
to  
**ISO 9002:94**

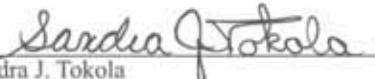
**Trend Micro Incorporated**  
**(TDSC, Trend Development and Support Center)**  
**15<sup>th</sup> Floor, IBM Plaza, #8 Eastwood Ave., Eastwood City Cyber Park,**  
**E. Rodriguez Jr. Ave., Bagumbayan, Quezon City, 1110 Philippines**

The Quality System was audited and meets the requirements of ISO 9002:(1994)  
Scope of Registration SIC / NACE 34 Engineering Services-Providers 24\*7 Antivirus and Trend Product  
Solution to Worldwide Customers

**This Certificate Valid until Nov. 27, 2003**  
Original certificate issued on Nov. 27, 2000

Certificate # T2000-331



  
Sandra J. Tokola  
Business Manager U.S. Operations  
Cert ISO 9000 Rev 5-16-200

11-29-00  
Date of Issue



- **3 Unidades de Negocio**
  - Brasil
  - México
  - Andina
- **10 oficinas de venta**
  - Caracas, Bogotá, México DF, Monterrey, Buenos Aires, Sao Paulo, Rio de Janeiro, Porto Alegre, Santiago, Panamá.
- **Sólida estructura de soporte regional**



- **Oficina de ventas**

- Representación local
- 51 cursos de certificaciones realizados
- Más de 250 certificados en el país.
- Soporte local Nivel III.
- Canal de ventas certificado: Soluciones Integrales Delta P, C.A.
- Niveles de servicio locales y escalables.
- <http://www.trendmicro.com.ve> / <http://www.deltap.com.ve>



# E.P.S II

## ESTRATEGIA DE PROTECCION EMPRESARIAL



## ¿ Porqué la solución actual es insuficiente ?

- Listas de virus desactualizadas, Antivirus no presente en todas las maquinas y servidores
  - Ausencia de control y actualización central = detecciones perdidas
- Los dispositivos de seguridad no se coordinan
  - Las empresas deben coordinar su protección con múltiples proveedores



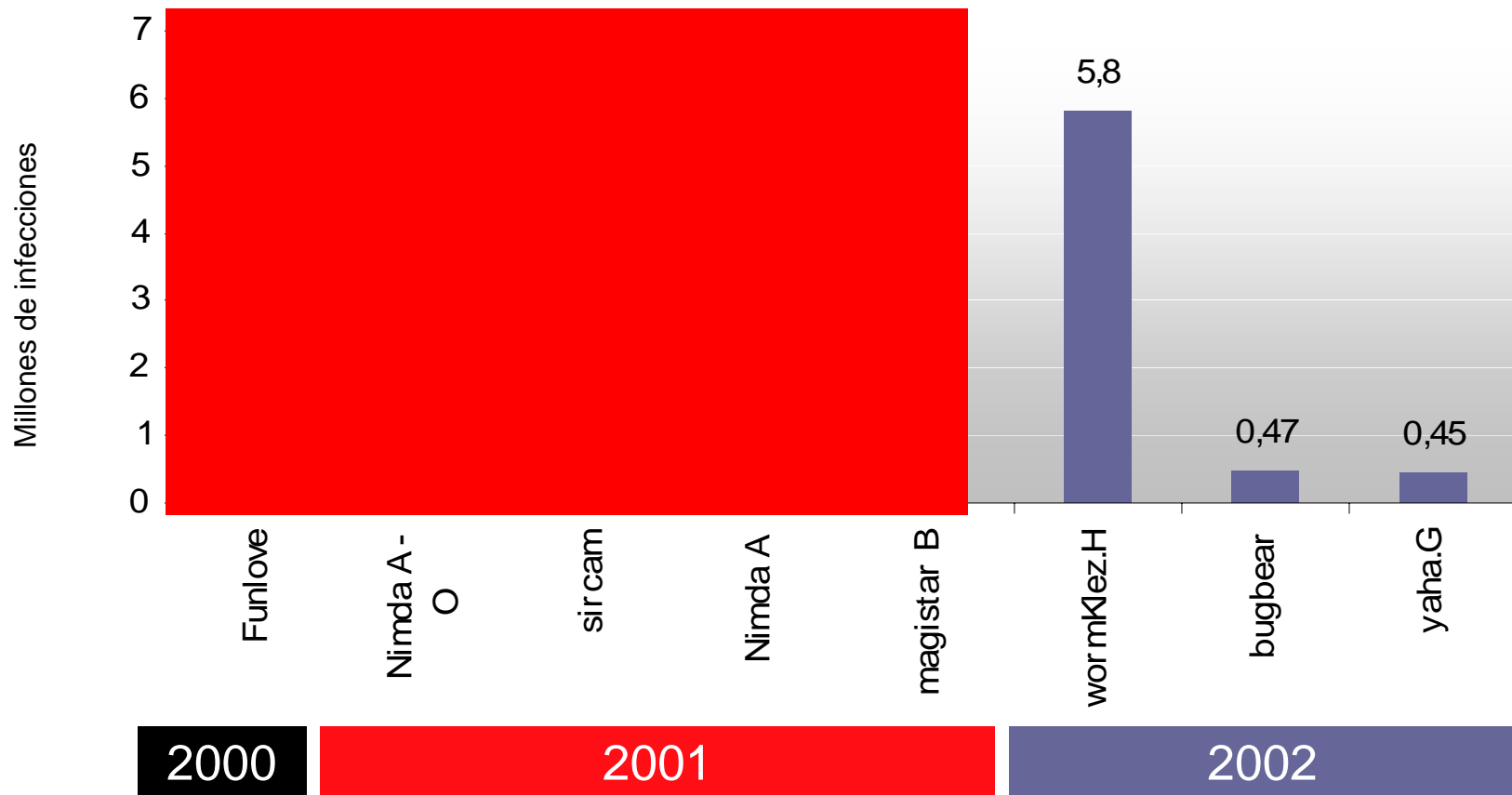
- El ciclo de vida de los virus = la experiencia del cliente
  - El TCO empresarial y la pérdida de productividad afectan al cliente en todas las etapas del ciclo de vida



(\*) Computer Economics, 2002

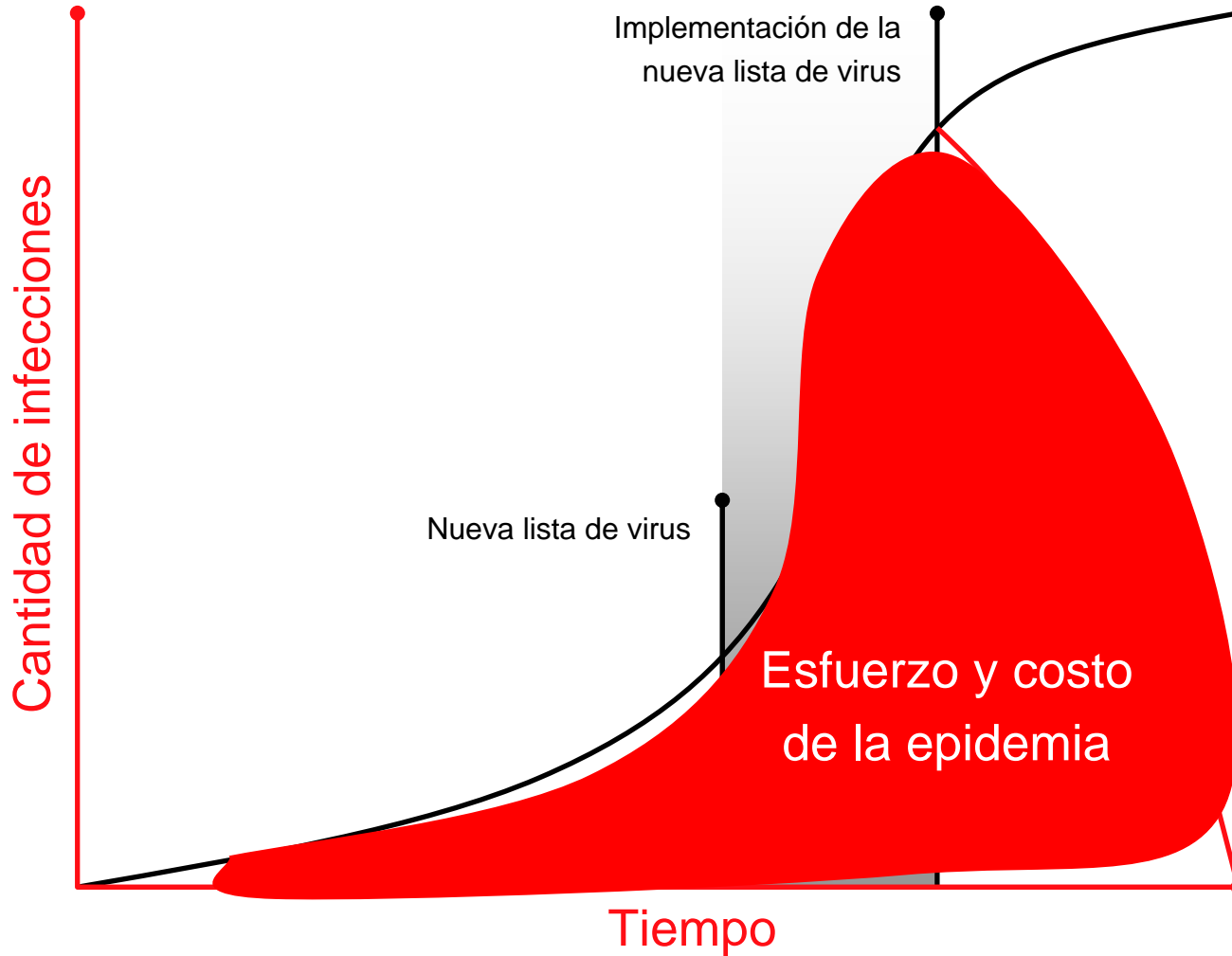


- Los Top 2 al 5 de 2002 existen ya desde entre 1 y 2 años



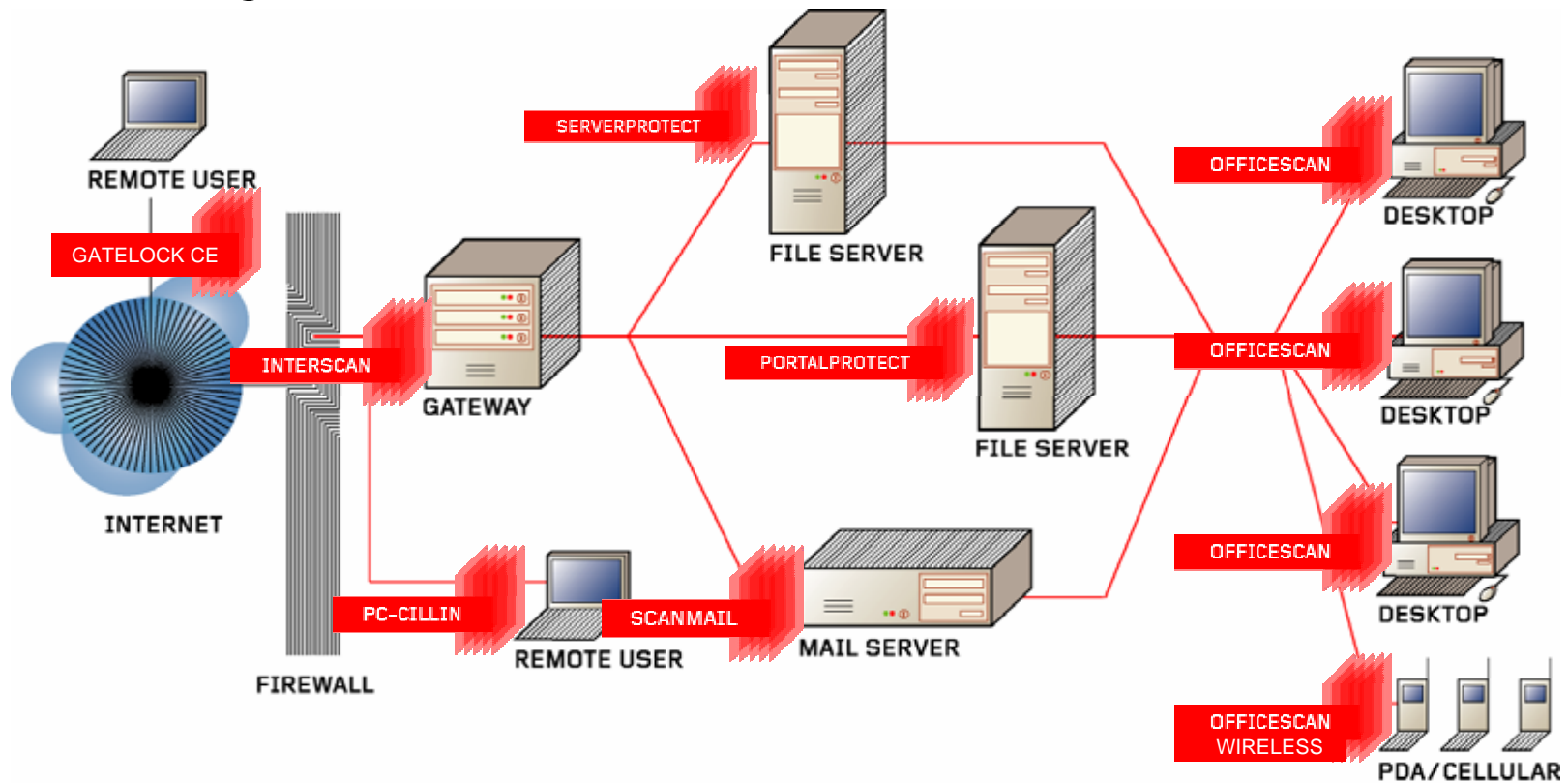


# Midiendo la efectividad de la seguridad





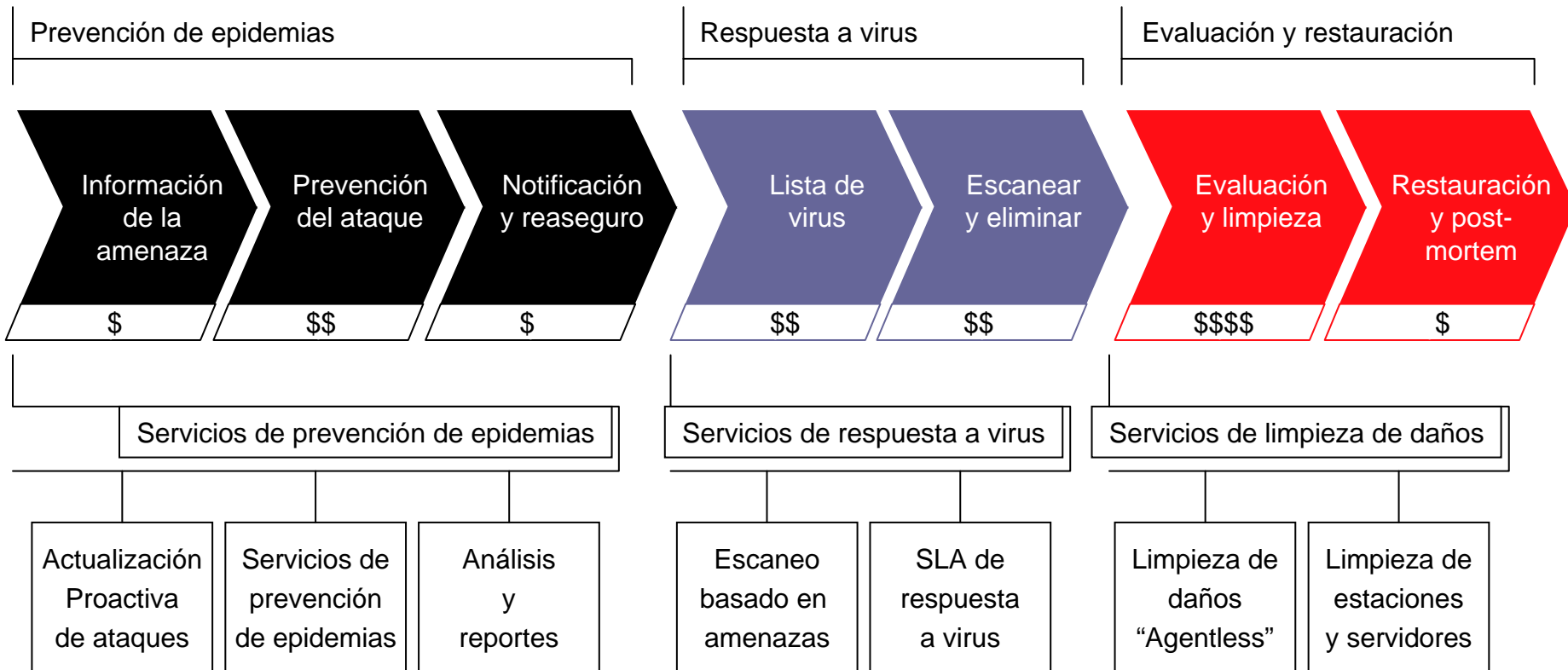
- Todos los Servicios y comunicaciones para la propagación del código malicioso

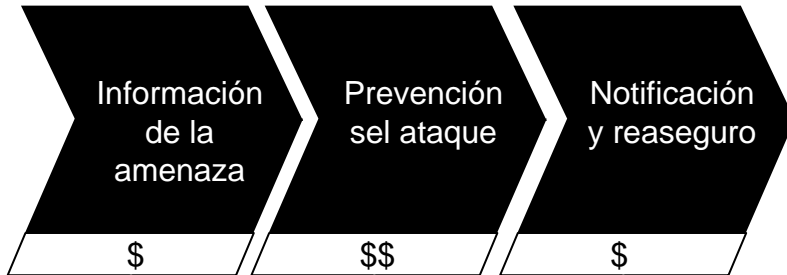




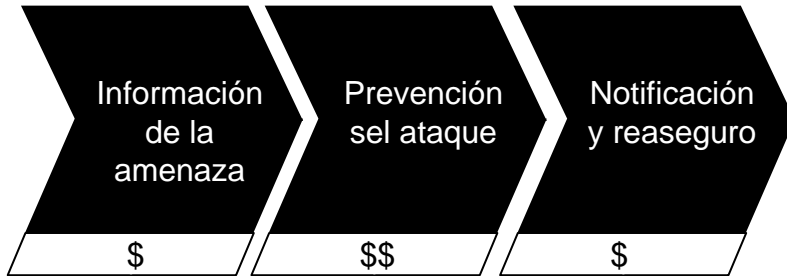
# Enterprise Protection Strategy

Administración centralizada = Administración del ciclo de vida completo de virus





- Servicios de prevención de epidemias
  - Información detallada de las amenazas ni bien son reconocidas
  - Provee políticas de prevención de epidemias específicas para cada ataque
  - Bloquea e impide el código malicioso ingresar o esparcirse por la red



- Servicios de prevención de epidemias
  - Permite aprobar e implementar políticas manuales o automáticas
  - Reporte en tiempo real del estado y la implementación de políticas



- SLA de respuesta a virus
  - Resuelve la etapa de respuesta a virus en la epidemia Virus Response SLA
  - Garantiza la detección de virus en dos horas máximo para los casos reportados
  - Entrega un reaseguro al negocio de que las epidemias no serán virus permanentes
  - Trend Micro eleva la barra en performance



- Escaneo basado en amenazas
  - Motor de políticas empaquetado con el motor de escaneo
  - Busca sólo donde está la amenaza
  - Políticas activadas por Trend o por el cliente
  - Permite construir marcos de acción para virus de tipo específico



- Servicios de limpieza de daños
  - Resuelve la etapa de evaluación y limpieza
  - Luego de la implementación de la lista de virus y del motor de escaneo, pueden aún existir troyanos y gusanos que pueden nuevamente atacar la red
  - Las estaciones requieren limpieza del daño sufrido durante la epidemia



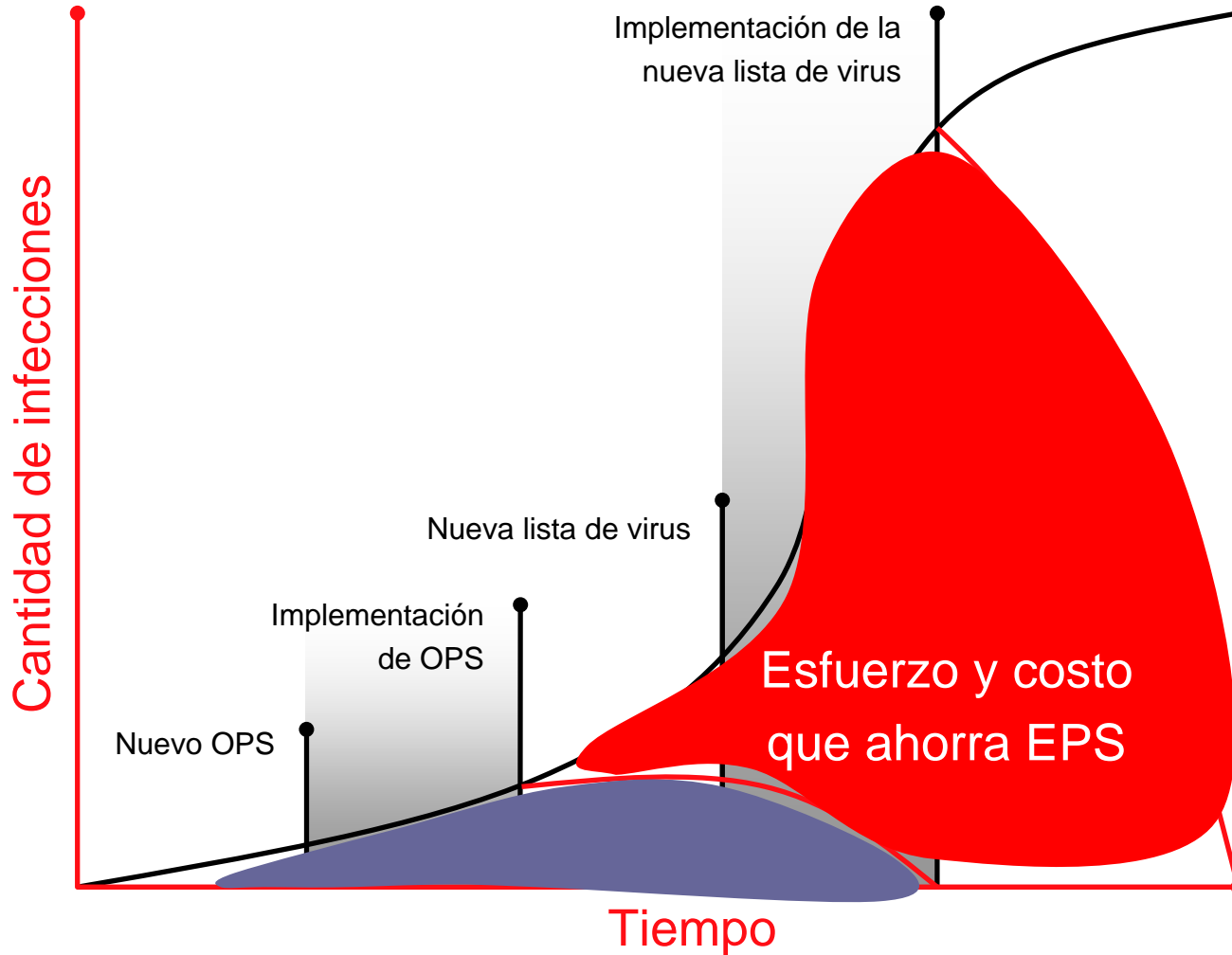
- OfficeScan 5.5 con Damaged Cleanup Services ofrece limpieza gestionada
  - Limpieza basada en agente, que puede ejecutarse remotamente del servidor OfficeScan hacia el cliente



- Damage Cleanup Server 1.0 ofrece limpieza “agentless”
  - Los clientes, sin importar su solución de Antivirus, pueden interoperar con Damage Cleanup Server
  - La consola centralizada registra información del tipo de virus detectado, nombre de la máquina, IP, dirección del cliente limpiado y tiempo de la ejecución de limpieza



# Midiendo la efectividad de la seguridad





## Virus Sample Received

04/17/02; 04:04 a.m.; yellow alert

- Memory resident, carries SMTP engine
- Shared folders read/write
- Uses one of 6 file extensions (EXE, .PIF, COM, BAT, SCR and RAR)

## Outbreak Policies Deployed

- Via support or Outbreak Commander
- Block six file extensions
- Close shared folder access

## Pattern File Deployed

- Scan true file type for profile

## Cleaning Template Deployed

- Remove Klez entries
- Remove registry entries.....
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\run\krn132
- Remove drop files....
  - %systemdir%\krn132.exe

+ :00 min.

+ :07

+ :19

+ 3:42

### Prevención de epidemias

### Respuesta a virus

### Evaluación y restauración

Información de la amenaza

Prevención del ataque

Notificación y reaseguro

\$

\$\$

\$

Lista de virus

Escanear y eliminar

\$\$

\$\$

Evaluación y limpieza

Restauración y post-mortem

\$\$\$\$

\$



Virus Sample Received  
03/29/02; 12:57 a.m.

- UPX compressed worm, VB script
- Propagates through Windows Address Book (WAB)

Outbreak Policies Deployed

- Via support or Outbreak Commander
- Filter header
  - Check out this cool program!
  - Kijk eens naar dit coole programma!
- Block exe. files
  - Cool Program.exe/Cool Programma.exe

Pattern File Deployed

- Scan for 'cool' headers
- Strip and clean

Cleaning Template Deployed

- Delete registry entry
  - HKEY\_LOCAL\_MACHINE>Software >Microsoft>Windows>CurrentVersion>Run

+ :00 min.

+ :20

+ :55

+ :55

Prevencción de epidemias

Respuesta a virus

Evaluación y restauración

Información de la amenaza

Prevencción del ataque

Notificación y reaseguro

\$

\$\$

\$

Lista de virus

Escanear y eliminar

\$\$

\$\$

Evaluación y limpieza

Restauración y post-mortem

\$\$\$\$

\$



- Servicio Outbreak Prevention Policy lanzado en Dic-2001.
- 23 alertas (rojas y amarillas) en el año 2002.



<i>Tiempos de implementación</i>		
<i>Tiempo de creación de la política preventiva</i>	<i>Tiempo de creación de la lista de virus</i>	<i>Tiempo de creación de la política de limpieza</i>
<b>14 min</b>	<b>32 min</b>	<b>3hr: 42min</b> (tiempo máximo)

*El modelo de servicios de emergencias (Outbreak Management) consiguió reducir el tiempo de respuesta en más de un 50% en comparación con el modelo tradicional.*



- Políticas de defensa coordinadas para detener y mitigar los ataques de amenaza mixta
  - Aplicación consistente y coordinada de una política - OPS
  - Más rápida respuesta a las amenazas – OPS y SLA de Virus
- Más impulso al conocimiento clave de Trend Micro
  - Las recomendaciones de políticas provienen de los expertos en Antivirus y contenidos – OPS y DCS
- Agrega capas de protección adicional
  - La flexibilidad de alterar políticas y su implementación para ajustarse a las preferencias de seguridad – OPS
  - Soporte de plataforma heteroénea – Solaris, Windows, Linux – OPS y TMCM



- Reduce la vulnerabilidad empresarial
  - Detecta y elimina el código malicioso que expone las redes al ataque
- Reduce costos
  - Simplifica la coordinación entre departamentos y regiones durante las epidemias – OPS, TMCM
  - Reduce el costo de la limpieza manual del entorno – DCS
- Mejor visibilidad del retorno de inversión en seguridad
  - “Command Center” de Trend Micro Control Manager permite administrar la efectividad de la seguridad en tiempo real
  - Reportes y limpieza evalúan y eliminan las vulnerabilidades



Trend Micro

**Gracias!**