TREND MICRO

Securing Your Web World

Agentless Anti-Virus e IDS/IPS

Un nuevo paradigma para la Seguridad en Entornos Virtuales

Jorge Hormigos – Technical Account Manager - Trend Micro

Bloqueos en el viaje hacia la Virtualizacion

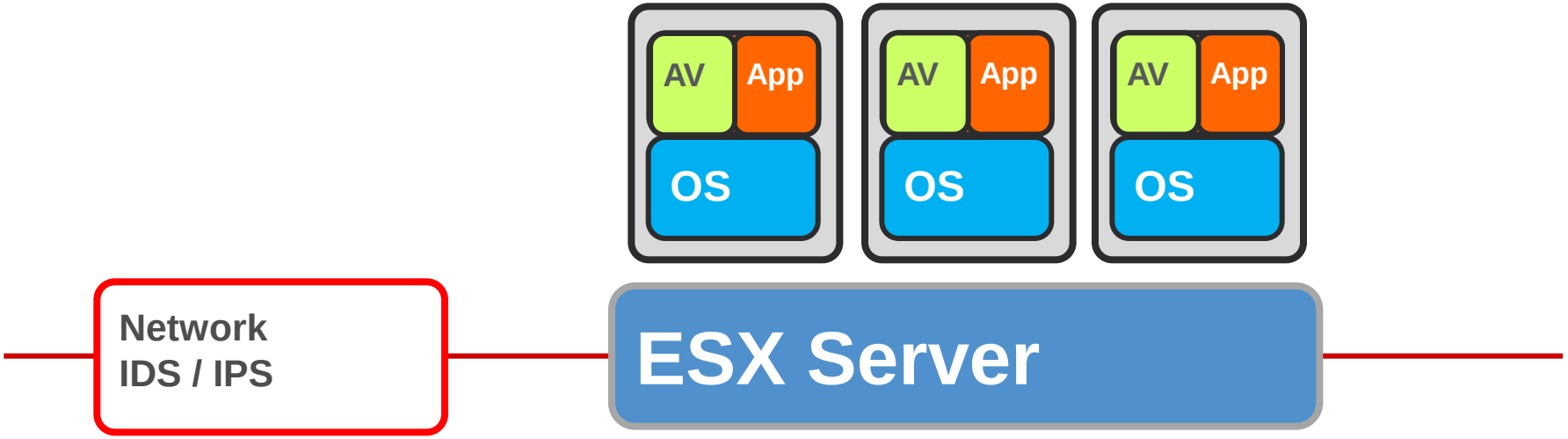
Evolución de las amenazas y los poros del perímetro

Nuevos paradigmas de la seguridad en plataformas vSphere

Trend Micro: Seguridad creada para VMware

TREND MICRO

Seguridad de Servidores: viejas costumbres

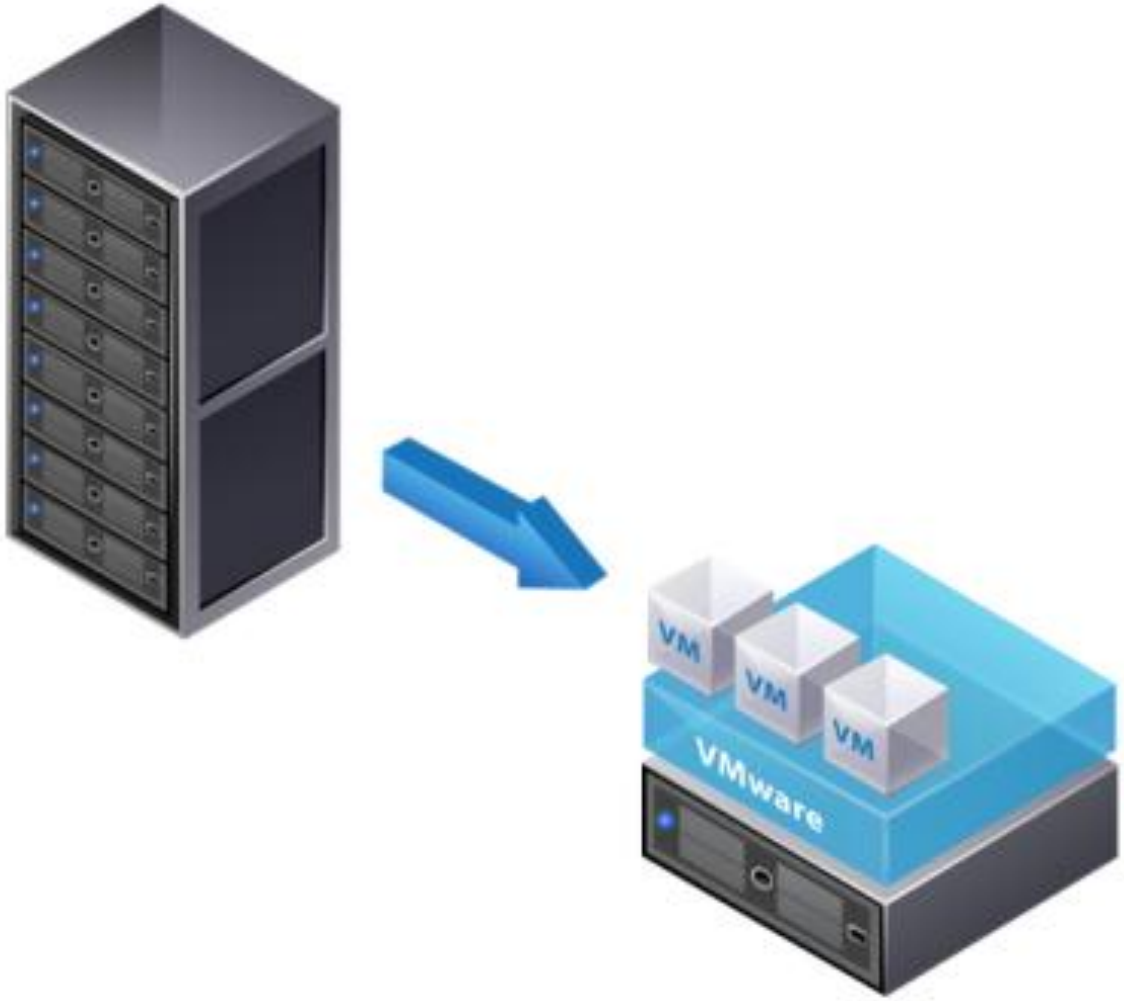


- Anti-virus: Local, protección basada en agente
- IDS / IPS :dispositivos de seguridad de red o software.

TREND MICRO

Viaje hacia la virtualización

Fase1: Consolidación de servidores

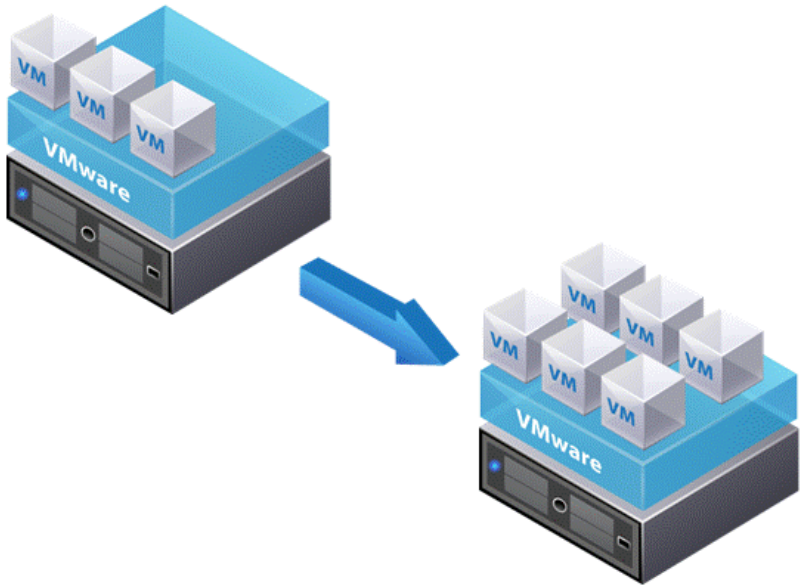


TREND MICRO

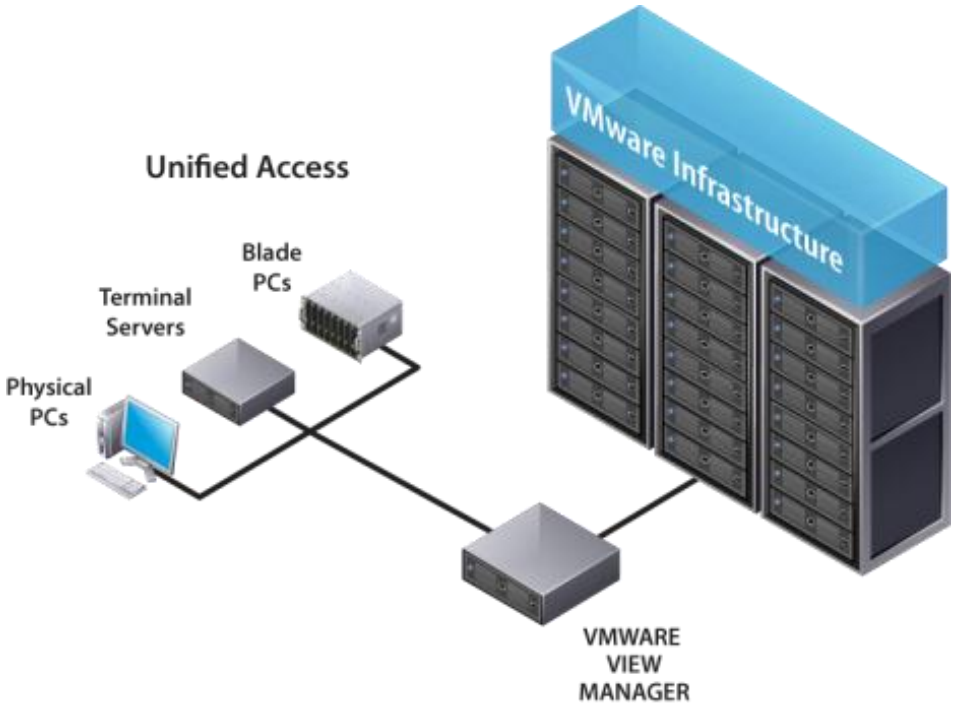
Viaje hacia la virtualización

Fase 2: Expansión & Desktop

Aumento de Servidores Virtualizados



Virtualizacion del Desktop



Viaje hacia la virtualización

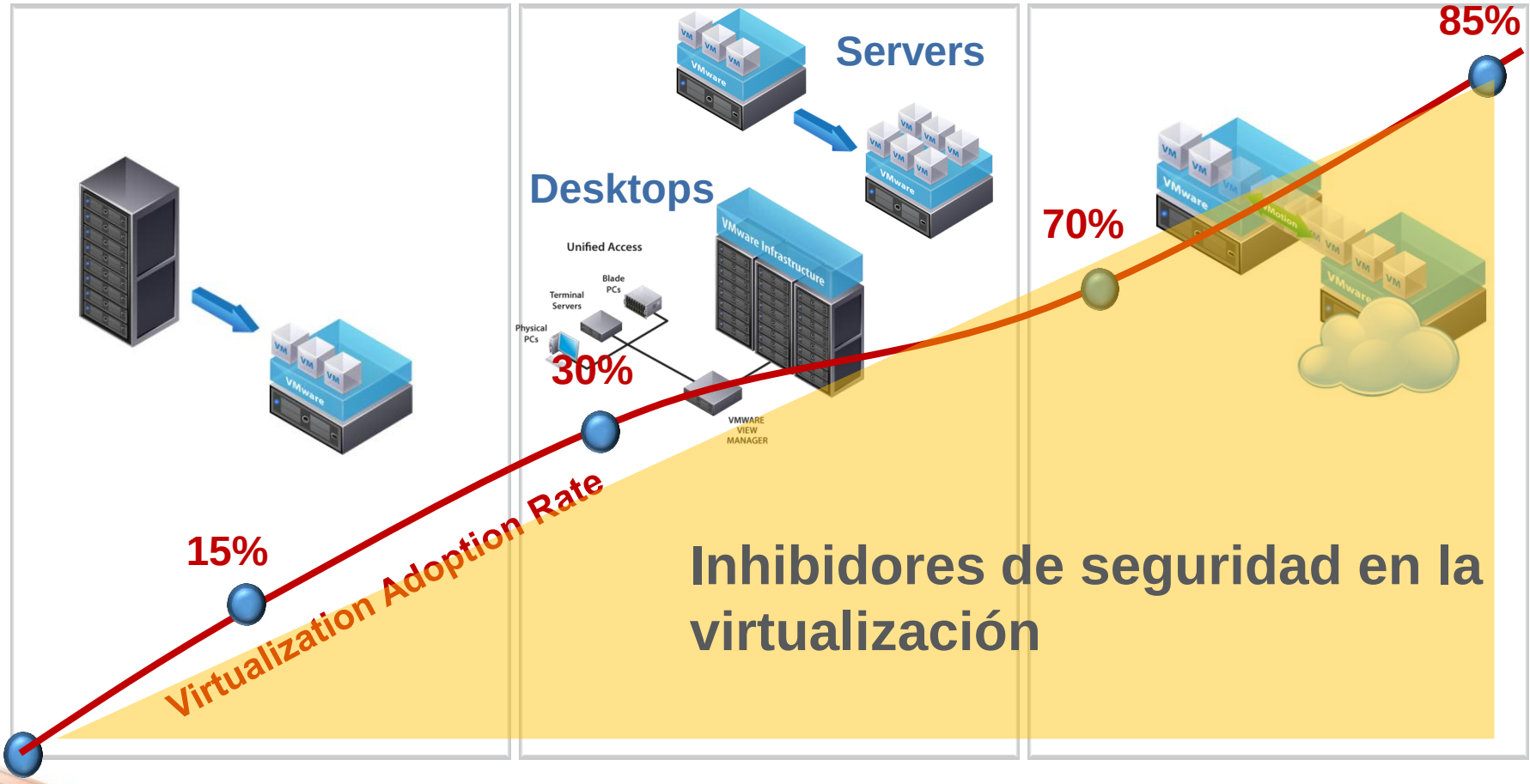
Fase 3: de la nube privada a la publica

Viaje hacia la virtualización

Paso 1: Produccion IT
Beneficio: coste eficiente

Paso 2: Negocio.
\+ Calidad servicio

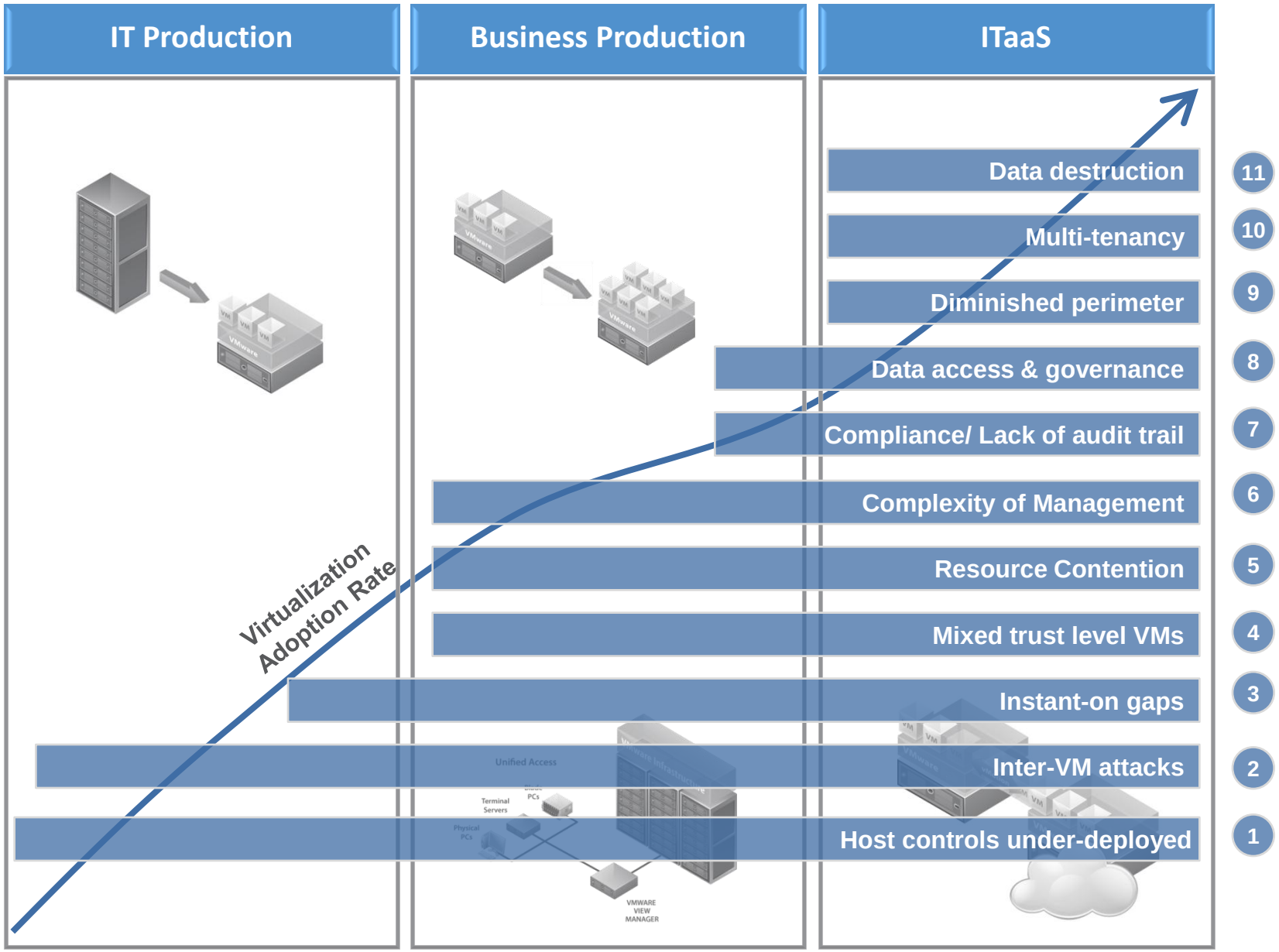
Stage 3: ITaaS
\+ Agilidad en negocio



ITaaS: Integrated Training and Accident Analysis System

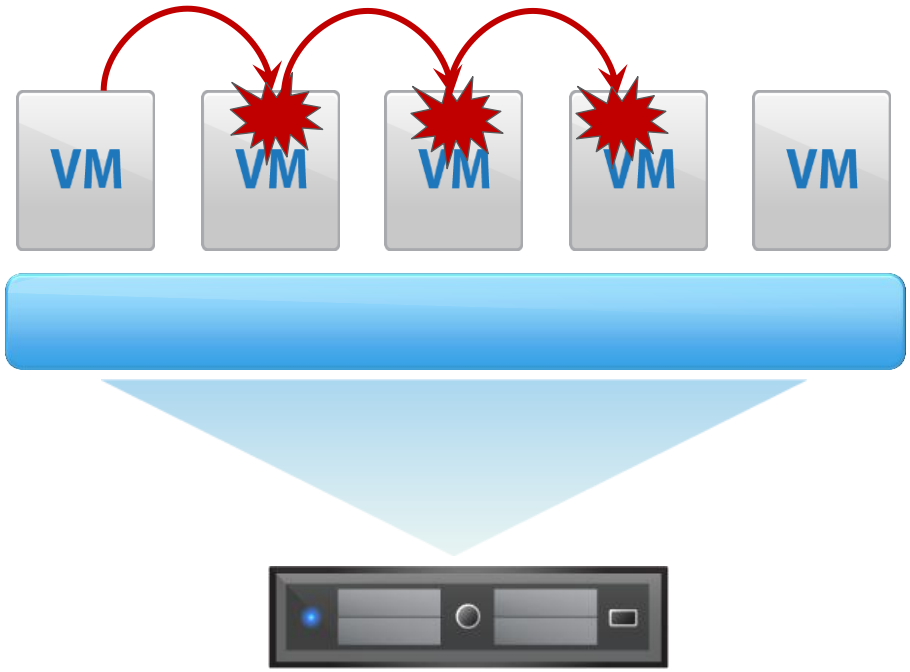
TREND MICRO

Security Challenges Along the Virtualization Journey



Inhibidores de seguridad en la virtualización

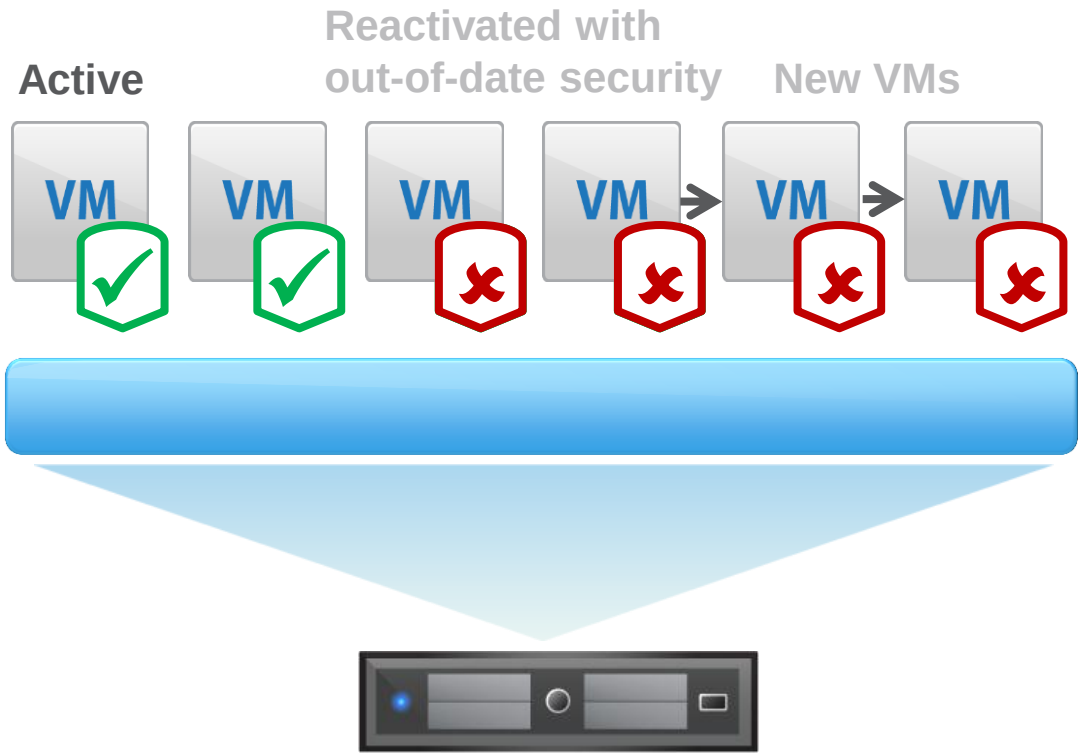
1 Ataques entre VMs/puntos ciegos



TREND MICRO

Inhibidores de seguridad en la virtualización

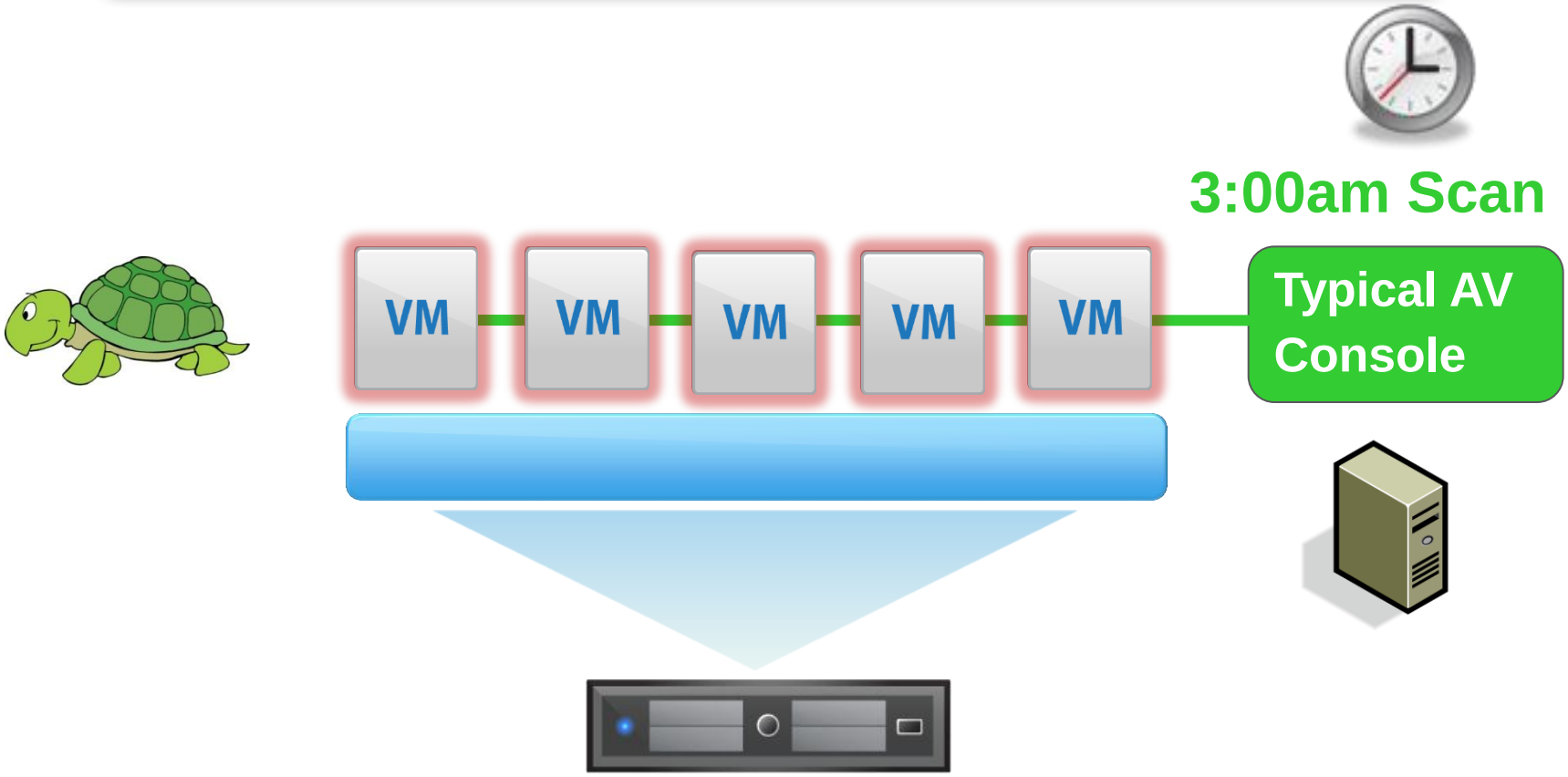
2 Huecos en sistemas instant-on



TREND MICRO

Inhibidores de seguridad en la virtualización

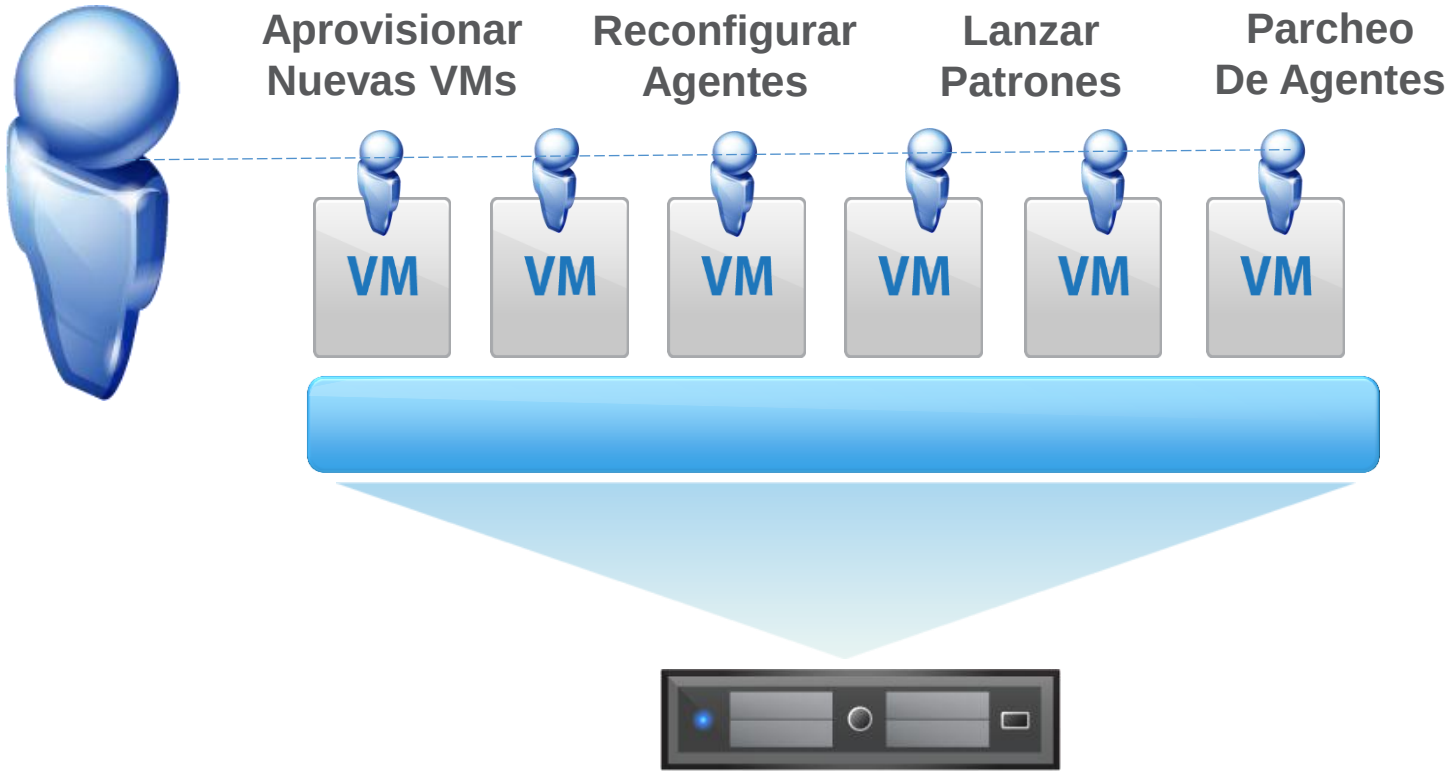
3 Malgasto de recursos en escaneos



TREND MICRO

Inhibidores de seguridad en la virtualización

4 Complejidad en la gestión



TREND MICRO

Bloqueos en el viaje hacia la Virtualizacion

Evolución de las amenazas y los poros del perímetro

Nuevos paradigmas de la seguridad en plataformas vSphere

Trend Micro: Seguridad creada para VMware

Las amenazas hoy en día…

- **Más rentables**
  - $100 billion: Beneficios estimados del cibercrímen total.
    -- *Chicago Tribune, 2008*

- **Más sofisticados**
  - "Los agujeros de seguridad no se descubren durante semanas e incluso meses en el 75% de los casos"
    -- *Verizon Breach Report, 2009*

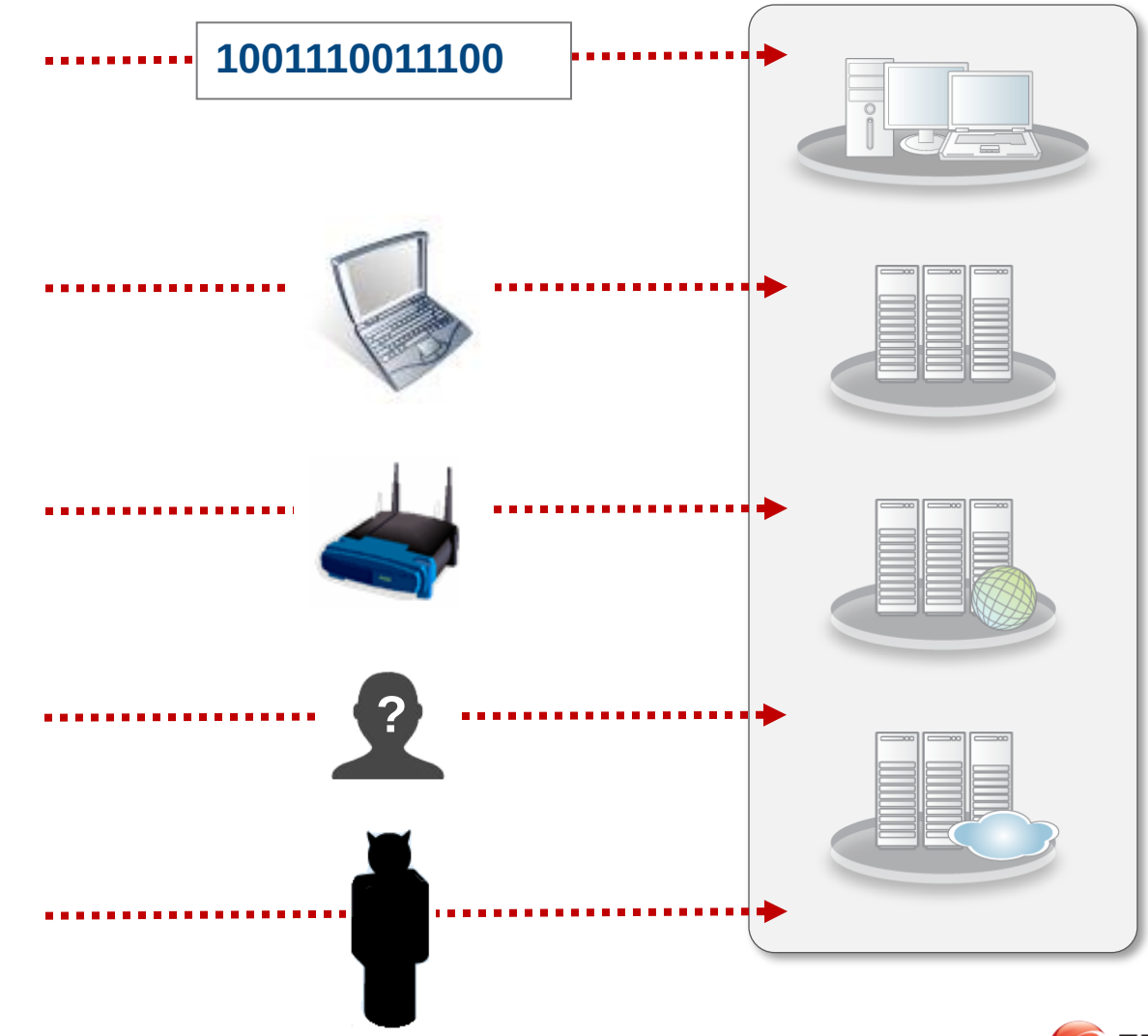
- **Más frecuentes**
  - "Harvard and Harvard Medical School son atacados cada 7 segundos, las 24 horas del día y durante 7 días a la semana."
    -- *John Halamka, CIO*

- **Destinados a víctimas específicas**
  - "27% de los encuestados afirmó haber sufrido algún ataque.
    -- *2008 CSI Computer Crime & Security Survey*

TREND MICRO

La defensa en el perímetro NO es suficiente

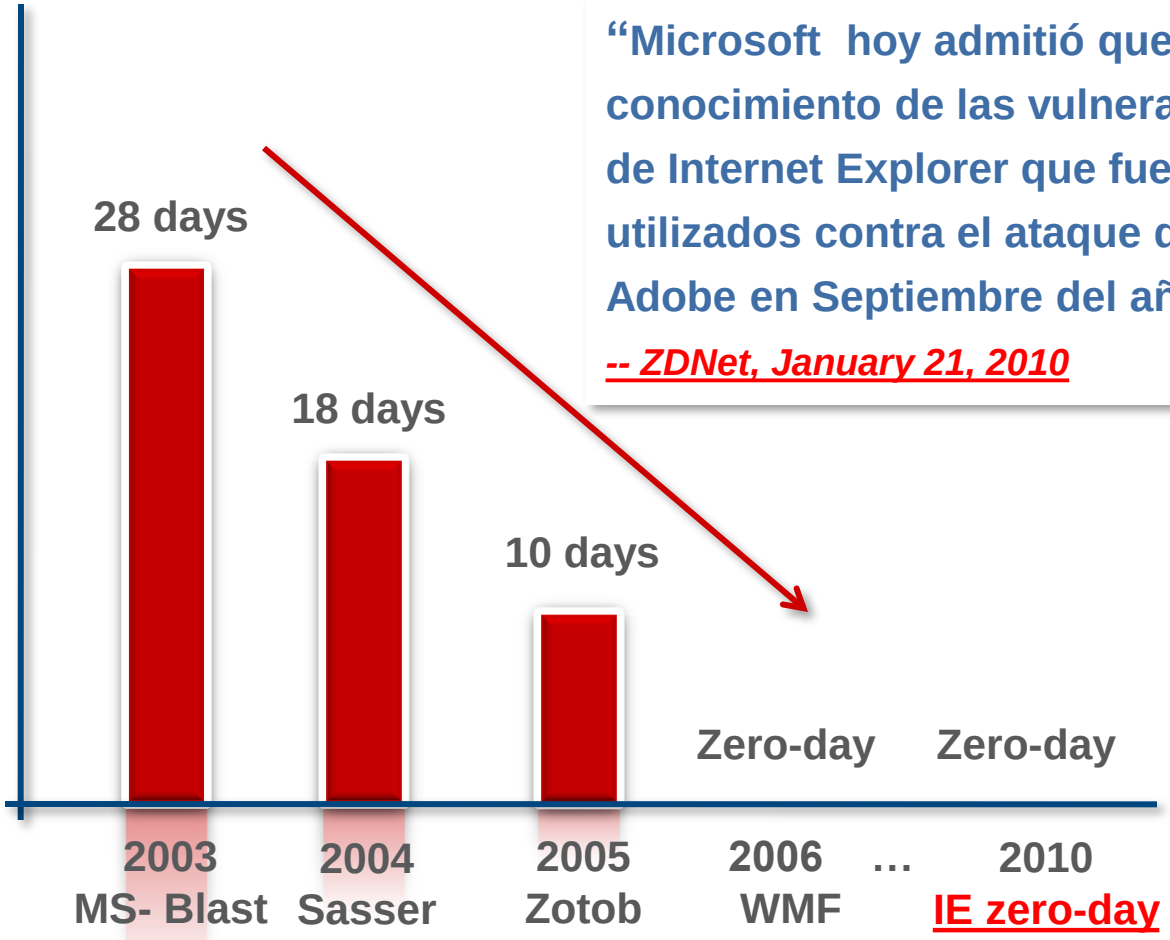
1. **Ataques cifrados**
2. Ordenadores portátiles
3. **Redes Inalámbricas**
4. Usuarios inesperados
5. **Atacantes Internos**



TREND MICRO

Los exploits están surgiendo ANTES de que existan parches para las vulnerabilidades

Nº de días hasta que la vulnerabilidad es explotada. El parche se publica a posteriori



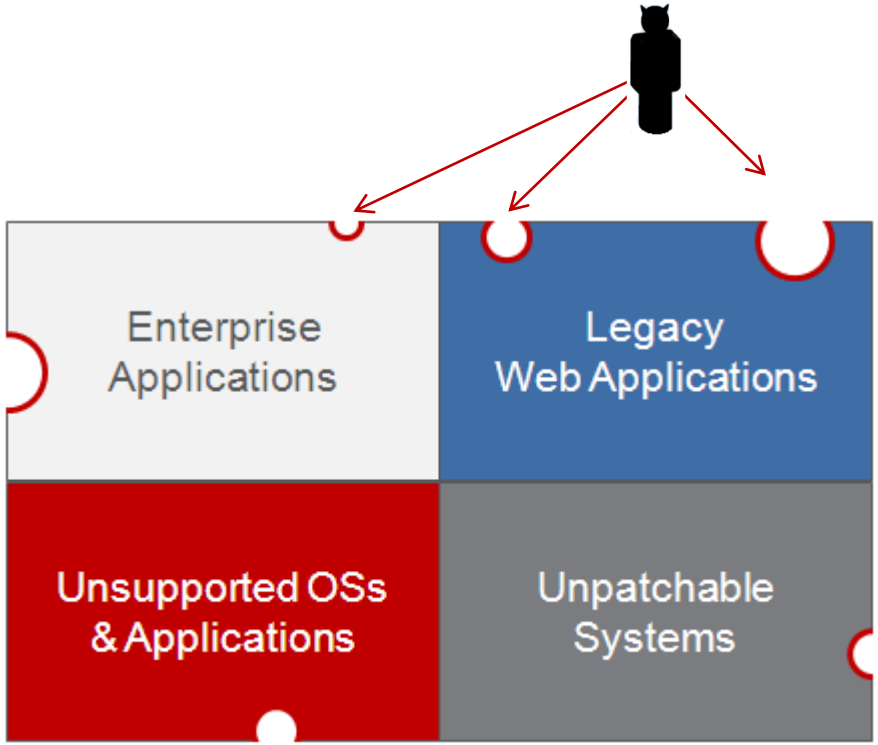
"Microsoft hoy admitió que tenía conocimiento de las vulnerabilidades de Internet Explorer que fueron utilizados contra el ataque de Google y Adobe en Septiembre del año pasado.

-- ZDNet, January 21, 2010

¿En qué punto es vulnerable?

Transcurren días e incluso meses hasta que los parches están disponibles y se han probado/ desplegado

- "Microsoft Tuesday"
- Oracle
- Adobe



Desarrolladores no disponibles para soluconar las vulnerabilidades

- Ya no están en la compañía
- Trabajan en otros proyectos

No pueden ser parcheados por el elevado coste, normativas o SLAs

- POS: puntos de venta
- casetas de obra
- dispositivos médicos…

Los parches ya no se despliegan más

- Red Hat 3 -- Oct 2010
- Windows 2000 -- Jul 2010
- Solaris 8 -- Mar 2009
- Oracle 10.1 -- Jan 2009

TREND MICRO

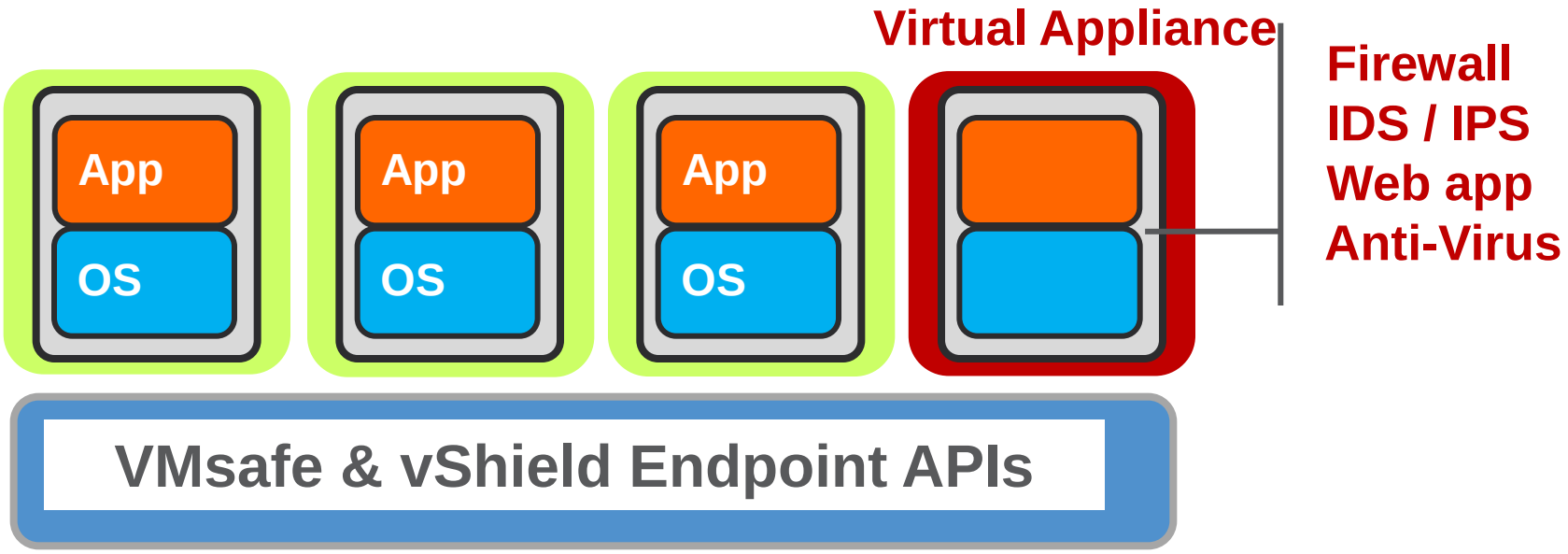
Bloqueos en el viaje hacia la Virtualizacion

Evolución de las amenazas y los poros del perímetro

Nuevos paradigmas de la seguridad en plataformas vSphere

Trend Micro: Seguridad creada para VMware

Nuevo Paradigma#1:
Seguridad desde el Hypervisor.

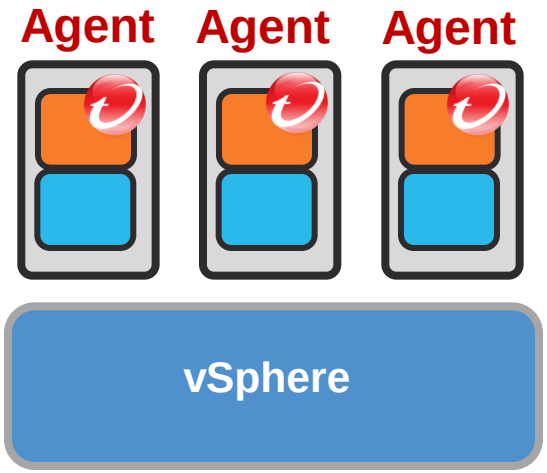


- vShield Endpoint ofrece AV scanning sin agente
- Proteccion desde fuera y sin cambios en las VMs

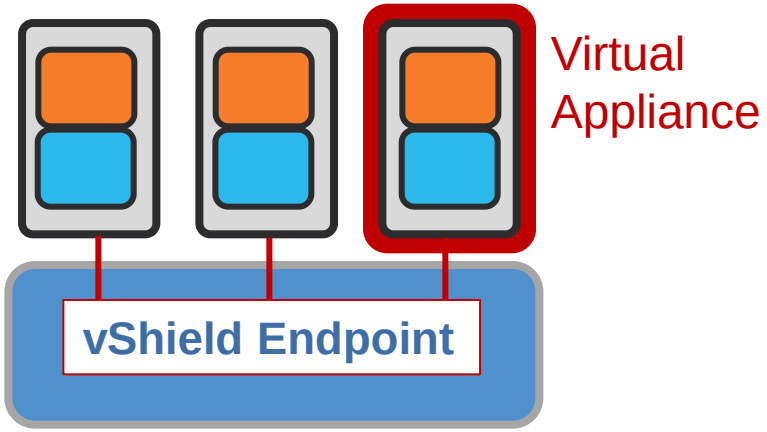
TREND MICRO

La oportunidad con Agentless Anti-malware

Antes



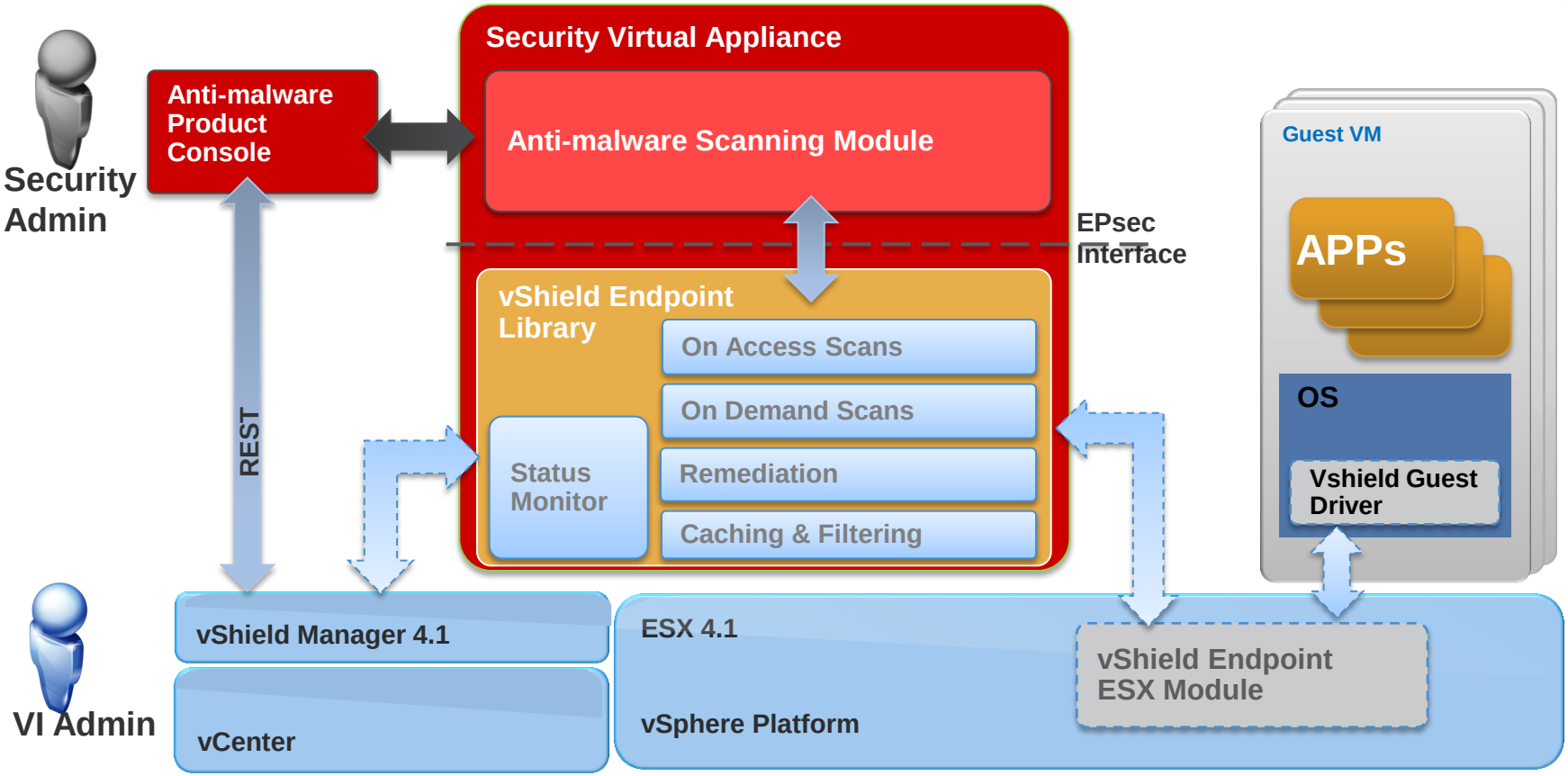
Hoy con vShield Endpoint



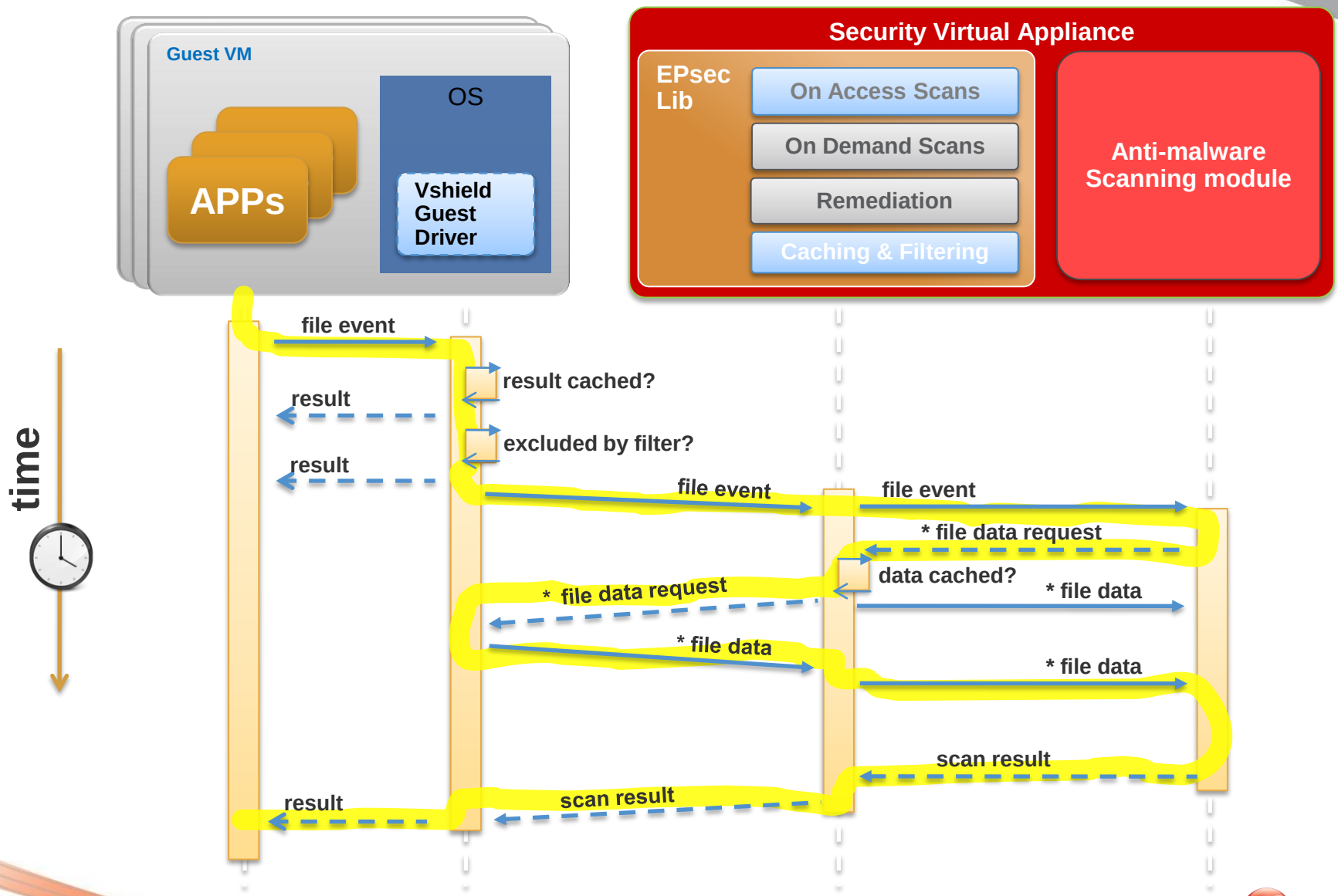
- **Mas manejable:** sin agentes, actualizaciones, parches…
- **Mayor rendimiento:** sin impacto por AV Storms
- **Mayor seguridad:** protección instantanea+ tamper-proofing
- **Mas consolidación:** operaciones mas eficientes.

TREND MICRO

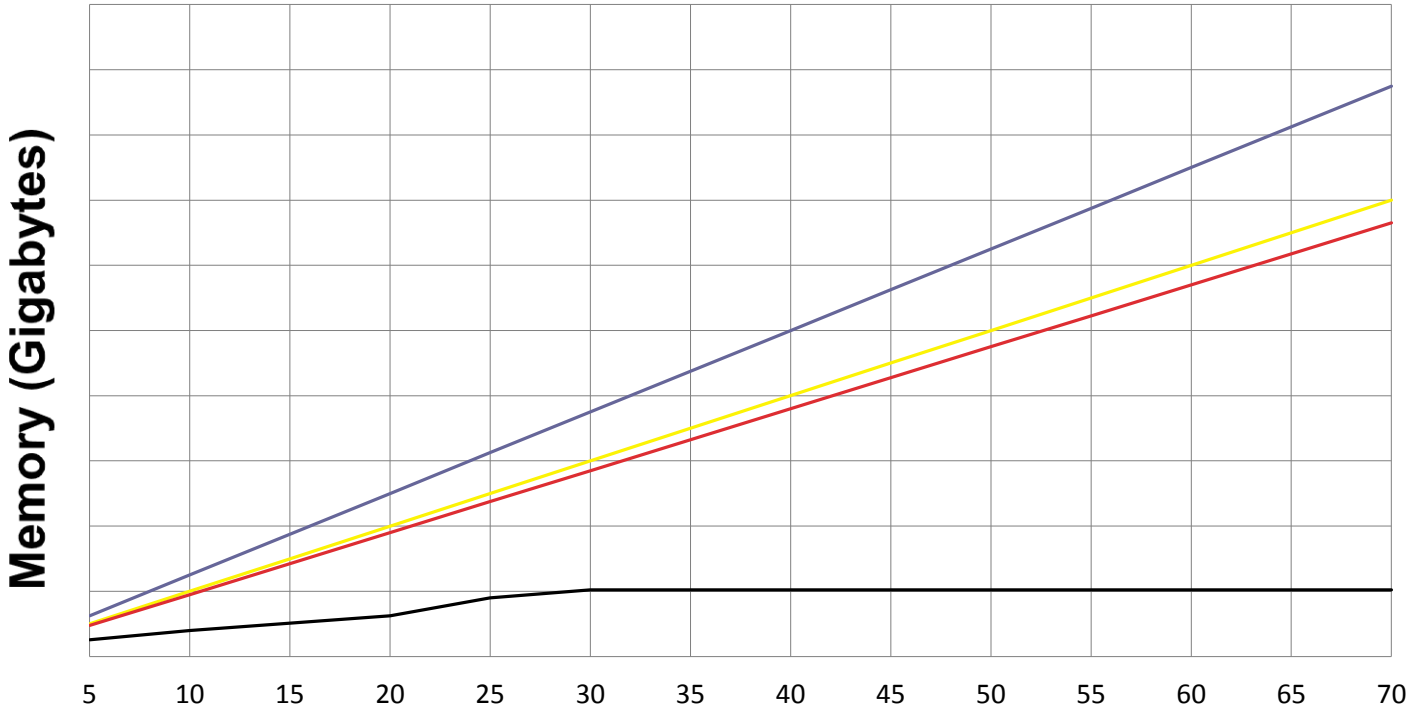
Agentless anti-malware: Arquitectura



Agentless Anti-malware: Process flow



Agentless AV usa menos memoria ESX



Anti-Virus "B"

Anti-Virus "Y"

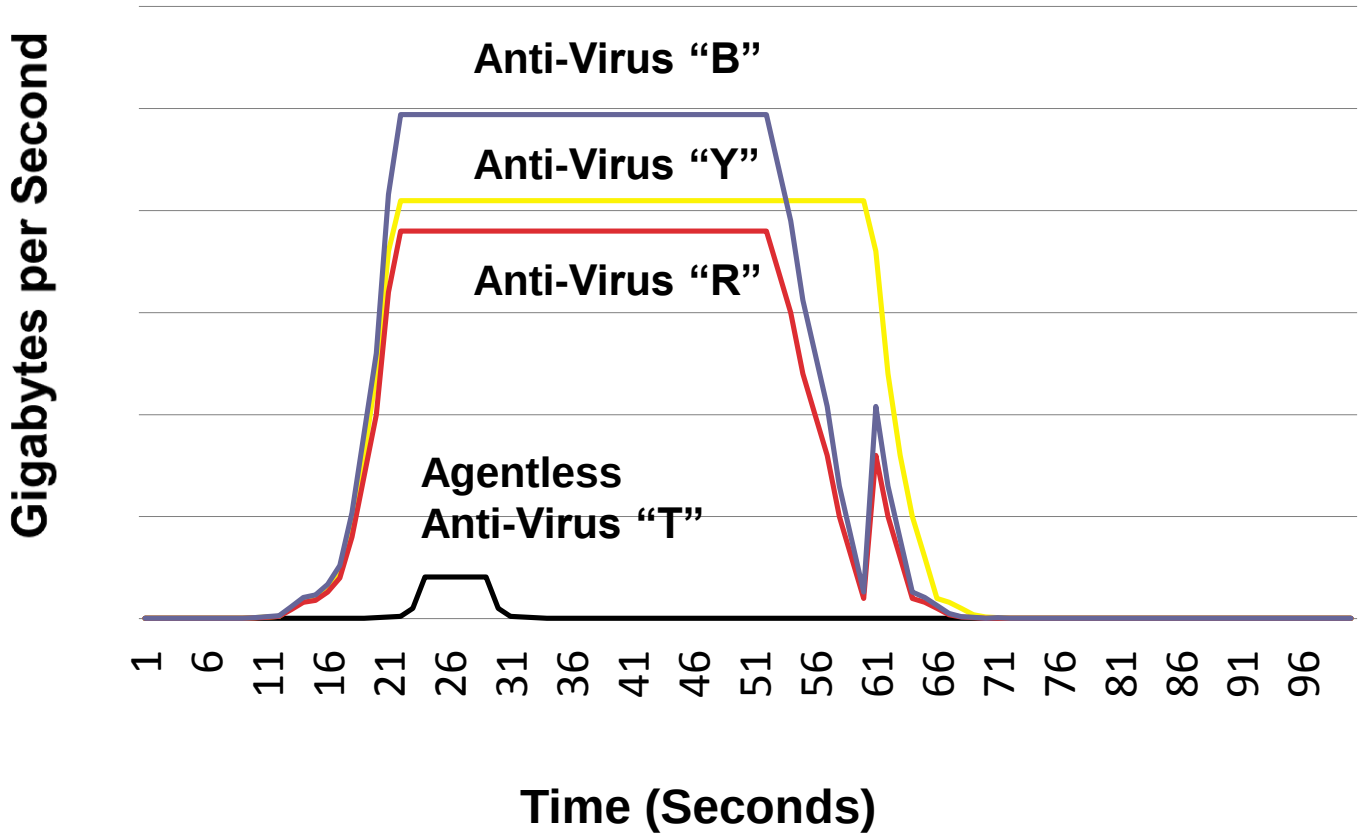
Anti-Virus "R"

Agentless Anti-Virus "T"

# of Guest VMs

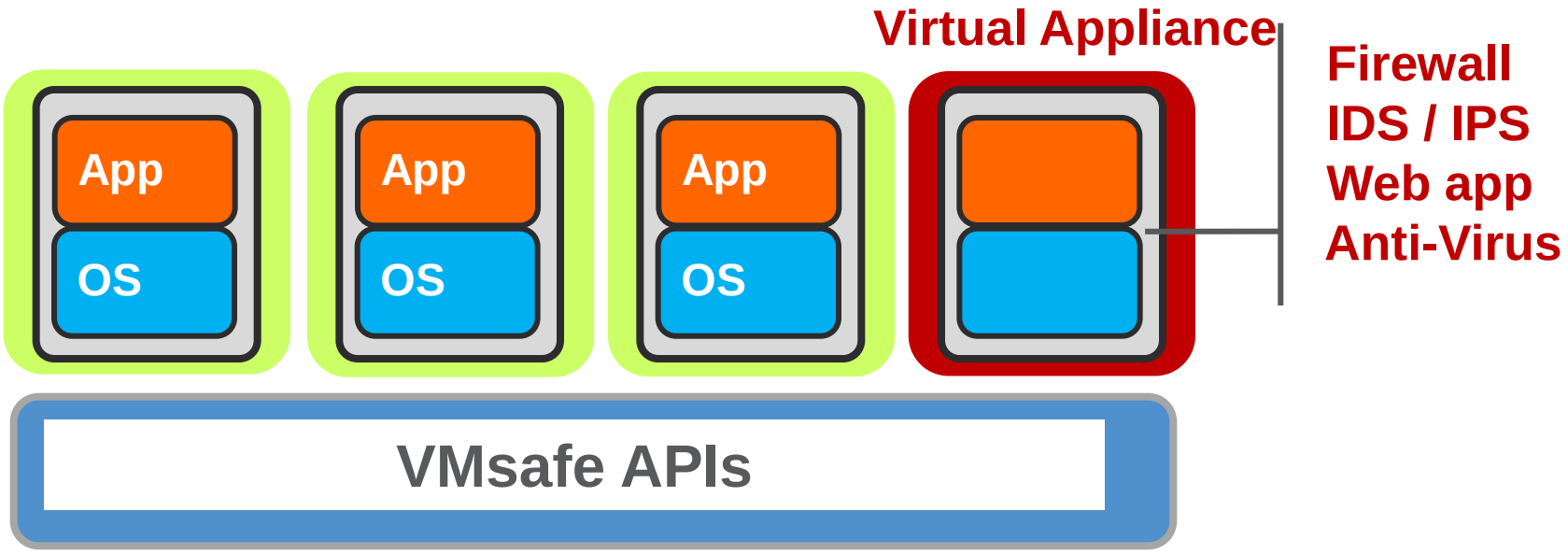
Agentless AV usa menos ancho de banda

Actualización de patrones para 10 agentes



Nuevo Paradigma#2:

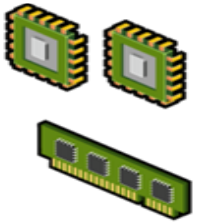
Oportunidad de mejoras en la seguridad



- VMsafe permite suplementar su seguridad perimetral.
- IDS/IPS, Firewall y proteccion de aplicaciones sin agente

TREND MICRO

VMsafe™ APIs



Inspección de CPU/Memoria

- Inspeccion de paginas de memoria especificas
- Conocimiento del estado de la CPU
- Aplicación de políticas mediante la asignación de recursos

Networking

- Visión de todo el trafico IO en el host
- Intercepta, ve, modifica y replica el trafico IO
- Proporciona protección en línea o pasiva

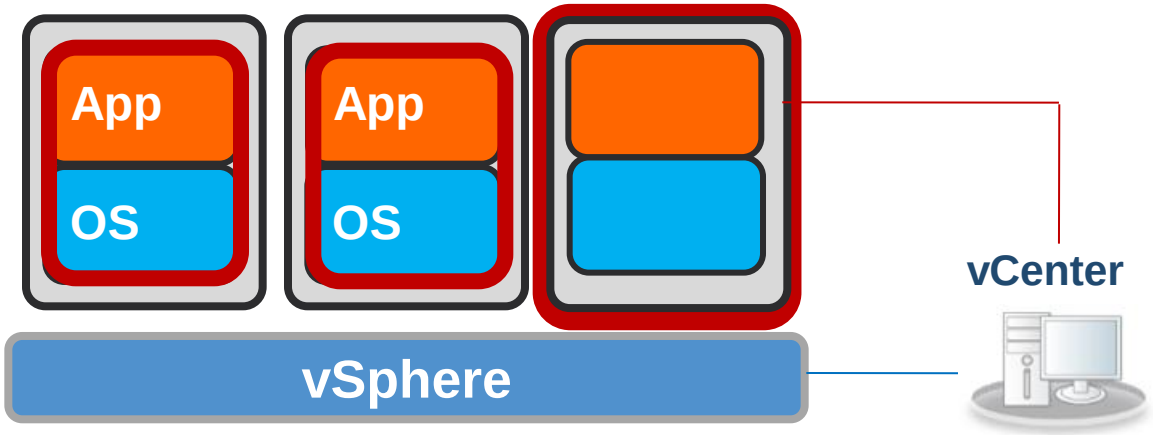
Almacenamiento

- Monta y lee discos virtuales(VMDK)
- Inspecciona IO de lectura/escritura a los dispositivos de almacenamiento
- Transparente para el dispositivo y en línea con el ESX Storage stack

TREND MICRO

Nuevo Paradigma# 3

Agentes AV para el entorno virtual



- Integrado con vCenter permite la visibilidad del entorno
- Escenarios: escritorios offline, conformidad de estándares, defensa mas exhaustiva

TREND MICRO

Bloqueos en el viaje hacia la Virtualizacion

Evolución de las amenazas y los poros del perímetro

Nuevos paradigmas de la seguridad en plataformas vSphere

Trend Micro: Seguridad creada para VMware

Security Built for VMware

Trend Micro soluciones de seguridad y conformidad ayuda a los clientes de VMware:

- Acelerar y completar su viaje hacia la virtualización
- Aprovechar completamente sus inversiones en Vmware
- Maximizar su ROI en su plataforma virtual

vmware PARTNER
TECHNOLOGY ALLIANCE

Founded	**United States, 1988**
Headquarters	**Tokyo, Japan**
Offices	**23 countries**
Employees	**4,350**
Market	**Internet Content Security**
Leadership	**US $1 Billion annual revenue**

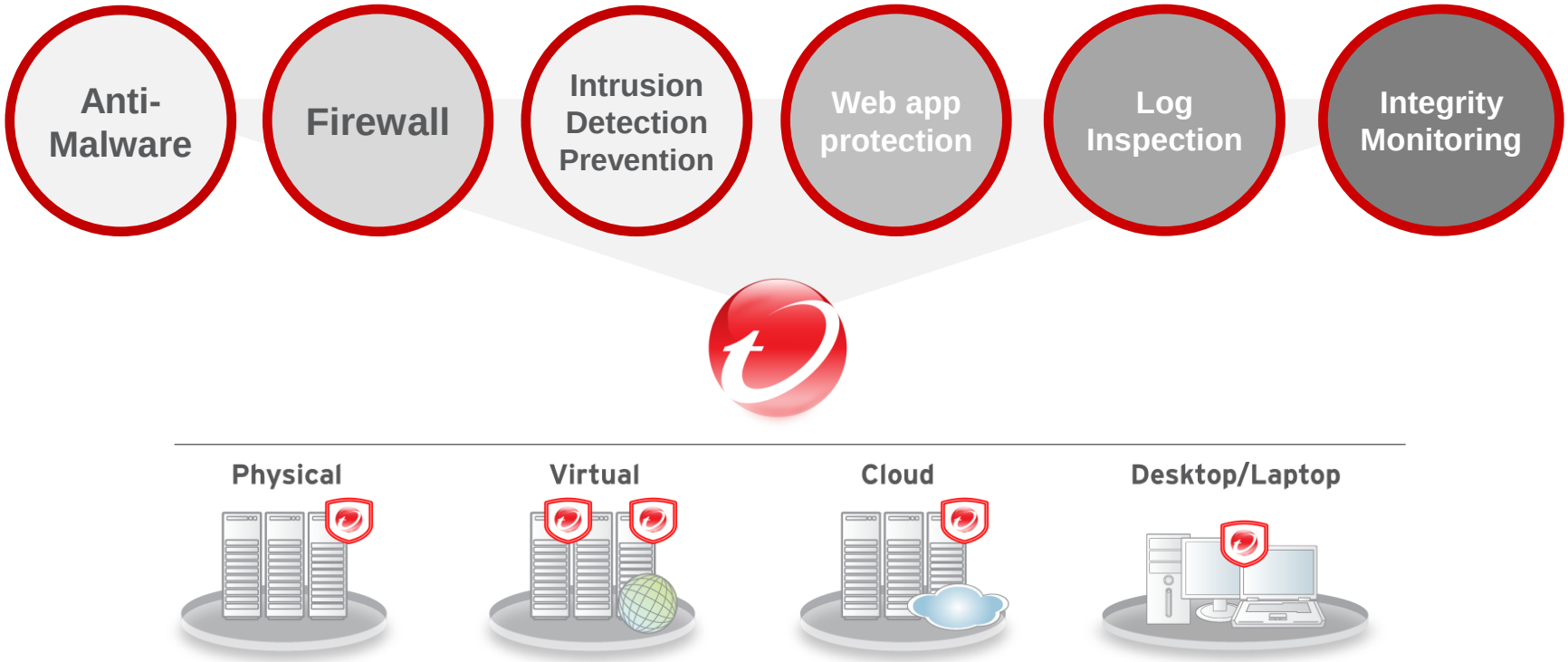
TrendLabs
Global Technical Support & R&D Center of TREND MICRO

1,000+ Threat Research Experts
10 labs. 24x7 ops
Real-time alerts for new threats

Trend Micro Deep Security

Protección de servidor y de aplicaciones

- El último módulo antimalware se une al resto de módulos para crear una solución de seguridad máxima.



TREND MICRO

Trend Micro Deep Security

Protección de servidores y aplicaciones

5 módulos de protección

Deep Packet Inspection

- IDS / IPS
- Web Application Protection
- Application Control

Detecta y bloquea ataques conocidos y ataques Zero Day que intentan explotar vulnerabilidades

Pone escudos a vulnerabilidades en aplicaciones web

Mejora en la visibilidad interna y control de aplicaciones de la red.

Firewall

Reduce la superficie de ataque. Evita DOS y escaneos no autorizados

Anti-Virus

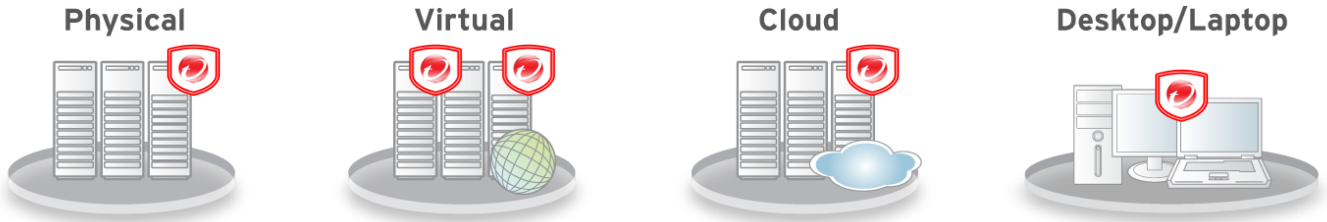
Detecta y bloquea mallware (web threats, viruses & worms, Trojans)

Log Inspection

Optimiza la identificación de eventos de seguridad importantes contenidos en entradas de logs

Integrity Monitoring

Detecta cambios maliciosos y no autorizados en ficheros, claves de registro etc.



Protección mediante Agente y/o Virtual Appliance

Trend Micro Deep Security

Security Built for VMware

1 Inline virtual appliance:

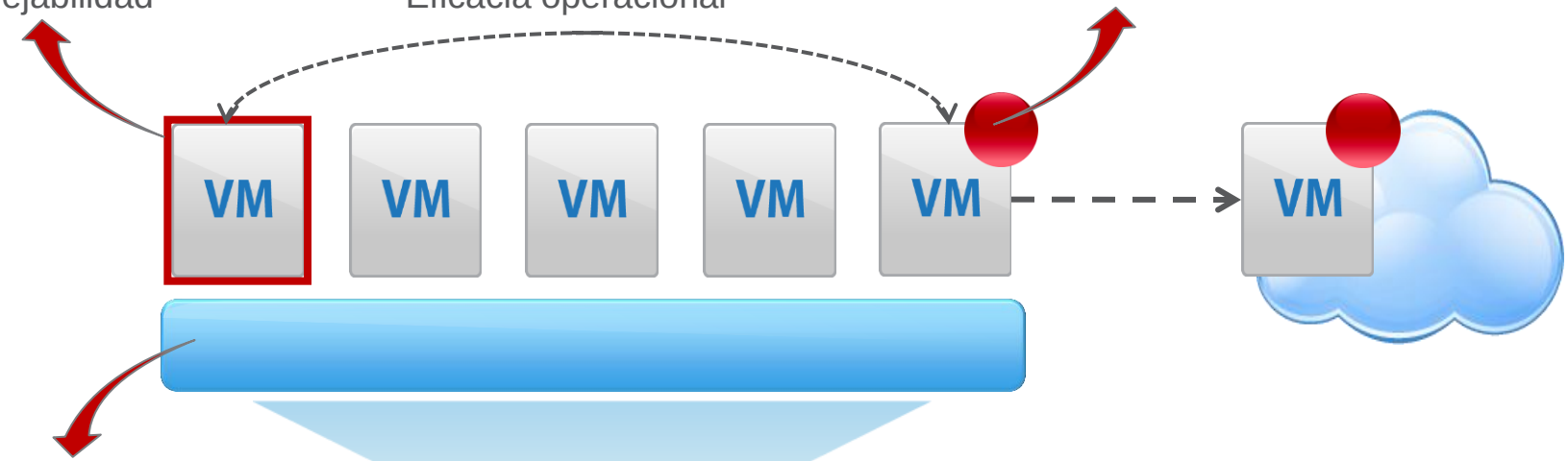
- AV, IDS/IPS, FW
- Mayor eficiencia
- Manejabilidad

3 Protección Coordinada:

- Optimización
- Eficacia operacional

2 Seguridad basada en Agente:

- Protección integral del datacenter
- Movilidad– protección extendida a la nube publica



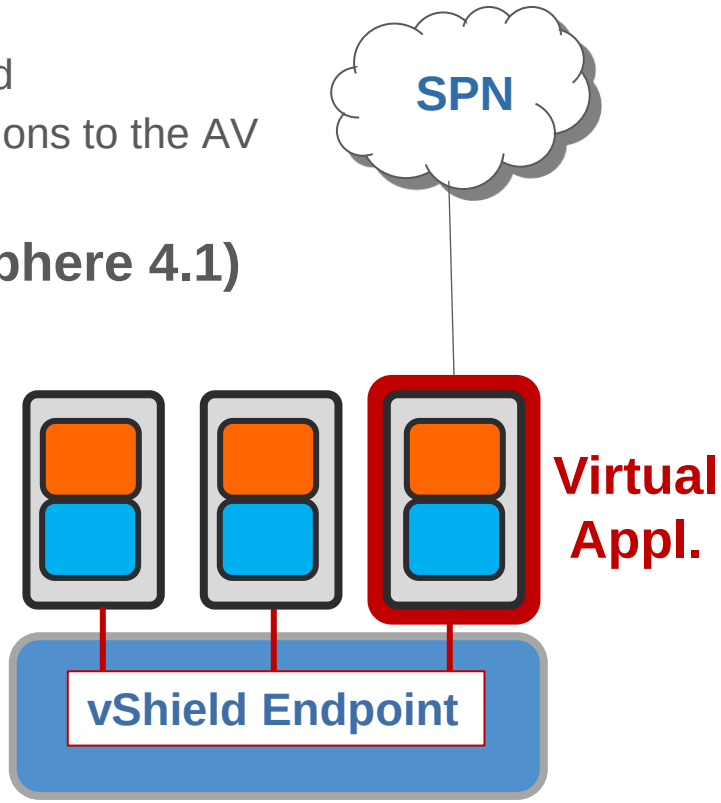
4 Integración con Hypervisor / vCenter :

- Permite seguridad para entornos virtuales
- Elimina las brechas de seguridad en entornos instant-on

TREND MICRO

Deep Security 7.5 Integrates vShield Endpoint & VMsafe

- **Agent-Less Real Time Scan**
  - Triggers notifications to AV engine on file open/close
  - Provides access to file data for scanning
- **Agent-Less Manual and Schedule Scan**
  - On demand scans are coordinated and staggered
  - Traverses guest file-system and triggers notifications to the AV engine
- **Integrates with vShield Endpoint (in vSphere 4.1)**
- **Zero Day Protection**
  - Trend Micro SPN Integration
- **Agent-Less Remediation**
  - Active Action, Delete, Pass, Quarantine, Clean
- **API Level Caching**
  - Caching of data and results to minimize data traffic and optimize performance



TREND MICRO

Thank You!

www.trendmicro.com/deepsecurity

Jorge Hormigos