Panda Virtual
GateDefender Performa

Consolide el cloud en su Infraestructura IT virtualizada

¿Supone la seguridad perimetral una mejora o un obstáculo para su programa de virtualización?

No ser capaz de alinear la seguridad del perímetro con la infraestructura informática de virtualización complica aún más el ya de por sí difícil reto de implementar la tecnología virtual y puede acabar contrarrestando sus numerables beneficios.

Panda Virtual GateDefender Performa aumenta los beneficios operativos de la virtualización gracias a una solución sencilla e integral que se beneficia del poder de detección desde la nube a la vez que ofrece todo el control de una solución 'on-premise'.

Solución

Panda Virtual GateDefender Performa permite a las empresas consolidar medidas preventivas contra el cambiante y complejo panorama del malware sin tener que poner en peligro su estrategia de virtualización, todo:

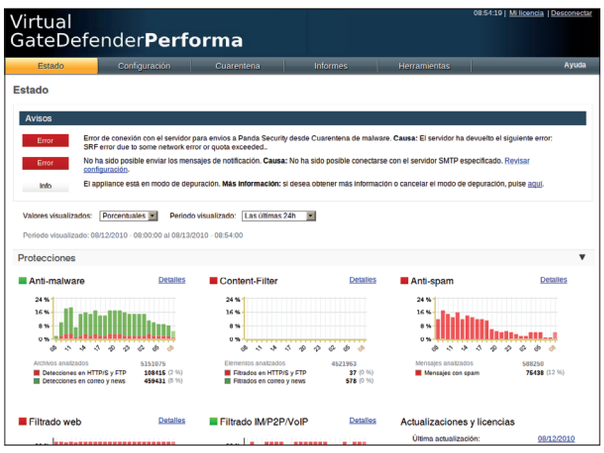
- **Protegiendo el perímetro de forma proactiva** mediante las tecnologías en la nube más innovadoras, capaces de ofrecer un índice de detección de malware y spam de prácticamente el 100%
- **Alineándose con los objetivos de** virtualización e integrándose sin fisuras en los sistemas existentes
- **Simplificando la instalación y administración** (Conectar y olvidar). **Gestión centralizada de la protección** (antispam, antimalware, filtrado Web, filtrado de contenidos y filtrado de aplicaciones de MI/P2P/VoIP)
- **Aumentando el control** sobre las actividades Web, productividad de los usuarios y recursos de la empresa

Principales beneficios

- **Seguridad en tiempo real tan sólida como una roca:** Prácticamente un **100% de detección** de spam y amenazas de Internet
- **Fácil administración:**
  - **Conectar y olvidar.** Se despliega en línea en minutos y se integra perfectamente con los sistemas existentes
  - **Integración:** Gestión de todos los módulos de protección desde un único appliance virtual
- **Mantenga su perímetro bajo control: Mayor control** por parte de los administradores del tráfico Web y de correo, la productividad de los usuarios y el consumo de ancho de banda
- **Mayor eficacia gracias a la virtualización y consolidación:** Ahorre tiempo, espacio, energía y dinero

Protección e informes en tiempo real

Informes unificados y en tiempo real que identifican problemas de seguridad y de tráfico y justifican la inversión tecnológica



Principales características

- **Tecnología proactiva integral.** La Inteligencia Colectiva basada en la **nube**, los motores heurísticos y la cuarentena optimizan la detección de amenazas
- **Protección completa e integral:** Antimalware y control de contenido potencialmente peligroso, spam; contenido Web no productivo y protocolos y aplicaciones Web 2.0
- **Altamente escalable:** Balanceo automático de carga y alta disponibilidad
- **Integración sencilla** con **AD y LDAP**
- **Calidad de Servicio** (QoS). Priorización y asignación de ancho de banda

Cubre todas las necesidades de la empresa independientemente de la topología de la red o el volumen de tráfico

VERSION DE PRODUCTO		VGDP 50	VGDP 100	VGDP 250	VGDP 500	VGDP 1000	VGDP 2500	VGDP 5000	VGDP 10000
Para X usuarios		50	100	250	500	1000	2500	5000	10000
HTTP	Mbps	20	30	60	120	250	400	500	650
	Conexiones concurrentes	550	450	1500	1800	7000	10000	12000	14000
HTTPS	Mbps	6	14	25	180	85	115	145	200
SMTP	Mensajes/sec	20	30	60	90	150	300	450	600
	Conexiones concurrentes	300	450	1500	18000	7000	10000	12000	14000

Rendimiento del sistema por cada versión de producto

10 razones para consolidar el cloud en su Infraestructura IT virtualizada

Protección perimetral en tiempo real
Prácticamente un 100% de detección de spam y amenazas entrantes y salientes de Internet en el perímetro gracias a la combinación única de tecnologías en la nube, motores heurísticos y las mejoras tecnologías de su gama

Fácil administración
Integración de todos los módulos de protección en un único appliance virtual administrable desde una única y sencilla consola Web

Protección consolidada
Gestión de todos los módulos de protección desde un único appliance virtual que detecta y bloquea todo tipo de amenazas de Internet antes de que penetren en la red

Conectar y olvidar
Se despliega en línea en cuestión de minutos y se integra perfectamente con los sistemas existentes (AD/ LDAP/VMware)

Detección de zombies
La detección de zombies reduce el riesgo de que se produzcan problemas legales y imagen corporativa

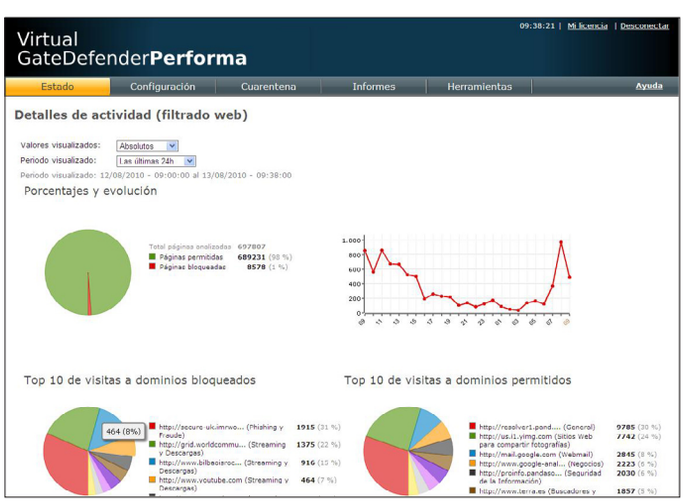
Priorización y optimización del ancho de banda
La función de Calidad del Servicio (QoS) permite a los administradores priorizar el uso del ancho de banda asegurando una utilización del mismo más eficaz

Mejora la gestión de cambios
Posibilidad de copiar y/o mover el servidor virtual, aprovechando al máximo la capacidad disponible en todo momento

Control del acceso a Internet
Aumente la productividad de los empleados acabando con la navegación improductiva no relacionada con el trabajo

Altamente escalable
Fácilmente escalable para adaptarse a las necesidades de expansión de la empresa con balanceo de carga automático y el sistema inteligente de alta disponibilidad

Mejora la gestión de riesgos
Políticas granulares basadas en perfiles que permiten a los administradores reforzar los sistemas de seguridad



¿Por qué una nube híbrida?

La nube híbrida permite a las empresas **mantener el control local** de sus datos, incluyendo logs y registros, beneficiándose a la vez de la capacidad de detección de la nube.

Toda la **flexibilidad y control** de una solución 'on-premise' con la capacidad de detección en tiempo real de la nube.

ANTIMALWARE	
Motores:	Nube, heurística, archivo de identificadores
Protocolos analizados:	SMTP - POP3 - IMAP4 - NNTP - HTTP - HTTPS - FTP
Amenazas conocidas:	100%
Amenazas desconocidas:	Sí
Cuarentena:	Sí
CONTENT FILTER	
Protocolos filtrados de correo, web y noticias:	SMTP - POP3 - IMAP4 - NNTP - HTTP - HTTPS - FTP
Análisis de tráfico entrante y saliente:	Sí
Cuarentena:	Sí
Filtrado de archivos:	Sí
Filtrado de mensajes:	Sí
ANTISPAM	
Motores:	Identificadores con micro-actualizaciones de la IC cada 60 segs.
Protocolos analizados:	SMTP - POP3 - IMAP4 - NNTP
Listas blancas y negras:	Sí
Niveles de sensibilidad:	Sí
RBLs / DNSBLs / NDR / BATV:	Sí
Cuarentena de spam y probable spam:	Sí
FILTRADO WEB	
Motores:	Nube
Protocolos analizados:	HTTP - HTTPS
Filtrado por categoría/subcategoría de URL:	SÍ más de 70 (Redes sociales, etc.)
Políticas por usuario/grupo:	Sí
Lista de clientes VIP excluidos del filtrado:	Sí
FILTRO DE APLICACIONES	
Mensajería instantánea:	Sí
Programas Peer-to-Peer (P2P):	Sí (Bittorent, eDonkey, etc.)
Protocolos de Web 2.0:	Sí (Skype, Spotify, etc.)

Requisitos técnicos

Versiones de VMWare:
- VMware ESX / ESXi: 4.0 / 4.1
- VMware Server: 2

Consola de administración Web:
- Internet Explorer 8.0 and Firefox 3.5

Requisitos de hardware para la máquina local que albergará el servidor virtual, por número de usuarios:

HARDWARE \ USUARIOS	50	100	250	500	1000	1000 +
MEMORIA	2 GB		4 GB			8 GB
CPU	Intel Dual Core		2x Intel (R) Dual Core CPU 3.2 GHz			2x Intel Quad Core
HDD	80GB		80GB			80GB

Certificaciones y reconocimientos de Panda Security