Panda Virtual
GateDefender Performa
Consolidate the cloud into your virtual IT infrastructure

Is perimeter security an enhancement or a hindrance to your virtualization program?

Not being able to align security within IT virtual infrastructure exacerbates the already complicated challenge of virtual implementation and can ultimately off set its numerable benefits.

Panda Security's VMware Ready™ Virtual GateDefender Performa enhances the operational benefits of virtualization through a consolidated, hassle free solution that harness the power of cloud detection while maintaining all the control of an on-premise solution.

Solution

Panda Security's VMware Ready™ Virtual GateDefender Performa enables companies to consolidate preventive measures against today's complex and ever changing threat landscape without having to compromise their virtualization approach by:

- **Proactively protecting the perimeter with cloud and best of breed technology** that delivers a practically 100% malware and spam detection rate

- **Aligning with** virtualization objectives and seamlessly integrating in existing systems

- **Simplifying installation and management.** Set it and forget it. **Centralized protection management** (antispam, antimalware, web filtering, content filtering and IM/P2P/VoIP filtering)

- **Heightening control** over web-based activities, employee productivity and business resources such as broadband

Main benefits

- **Hard as a rock real-time security:** Practically a **100% detection** rate of Internet threats and spam

- **Hassle free management:**
  - **Set it and forget it.** Deploys in-line in minutes and **integrates seamlessly** in virtual servers
  - **Consolidation:** All protection modules from one virtual appliance

- **Your perimeter under control:** Administrators gain **greater control** over web and email traffic, user productivity and broadband usage

- **Efficency through virtualization and consolidation:** Save time, space, enegry and money

Real-time protection / real-time reporting

Consolidated real-time reporting identifies security and traffic issues and helps to justify technology investment
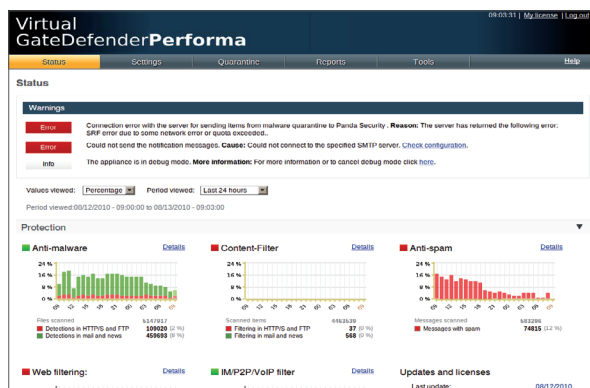
Main features

- **Integrated proactive technology. Cloud** based Collective intelligence, heuristic engines and quarantine optimize threat detection

- **Consolidated best-of-breed protections:** Antimalware and potentially dangerous content ; spam; unproductive Web content and Web 2.0 protocols / applications are also controlled

- **Highly scalable:** Automatic load balancing and high availability

- **Simple integration** with **AD and LDAP**

- **Quality of Service** (QoS) prioritize and allocate broadband

- **VMware Ready™**

Regardless of network topology or traffic volumes all business security needs are covered

PRODUCT VERSION		VGDP 50	VGDP 100	VGDP 250	VGDP 500	VGDP 1000	VGDP 2500	VGDP 5000	VGDP 10000
Up to X users		50	100	250	500	1000	2500	5000	10000
HTTP	Mbps	70	95	130	180	220	280	350	500
	Concurrent connections	450	900	2200	3000	5000	8000	11500	15500
HTTPS	Mbps	90	105	130	145	170	200	235	280
SMTP	Messages/sec	50	75	130	180	215	280	350	500
	Concurrent connections	450	900	2200	3000	5000	8000	11500	15500

System performance for each product version

10 reasons why you should consolidate the cloud into your IT infrastructure

Real-time perimeter protection
An almost 100% detection rate for incoming and outgoing Internet threats and spam at the perimeter thanks to the unique combination of cloud technologies, heuristic engines and best-of-breed technologies

Hassle free management
All protection modules available in a single virtual appliance which detects and blocks all types of Internet-borne threats before they enter the network and can be managed from a single user friendly web based console

Set it and forget it
It deploys in-line in a matter of minutes and integrates seamlessly with existing systems (Active Directory / LDAP) without redirecting network traffic

Zombie detection
The detection of zombies prevents system hijacking and botnet recruitment, mitigating the risks of legal action and PR disasters

Prioritize and optimize bandwidth
Using the Quality of Service (QoS) feature administrators can prioritize bandwidth usage ensuring a more efficient and business focused usage

Improve change management
Virtual servers can be copied and/or moved to make the most of available capacity at any given moment. Improve "trailing" by testing in test environments before going live

Web access control
Increase employee productivity by putting an end to frivolous non work related and non productive web browsing. New real-time cloud protection guarantees maximum detection ratios

Highly scalable
Scales effortlessly to meet business expansion requirements. Automatic load balancing and intelligent high availability ensure a fast return on investment and optimized network operations

Improve risk management
Granular profile based policies enable administrators to reinforce security enforcement

VMware Ready™
VMware Ready™ verification guarantees the Virtual GateDefender Performa is optimized to run on your VMware infrastructure.

Why hybrid cloud?

COLLECTIVE **INTELLIGENCE**

HYBRID CLOUD

The hybrid cloud enables companies to maintain a **100% on-premise control** over their data, including logs and registries, while harnessing the detection capacity of the cloud.

All the **flexibility and control** of an on-premise solution with the **real-time** detection capacity of the cloud.

ANTIMALWARE
Engines:	Cloud, Heuristics, signature file
Protocols scanned:	SMTP - POP3 - IMAP4 - NNTP - HTTP - HTTPS - FTP
Known threats:	100%
Unknown threats:	Yes
Quarantine:	Yes

CONTENT FILTER
Mail, Web and news protocols filtered:	SMTP - POP3 - IMAP4 - NNTP - HTTP - HTTPS - FTP
Analysis of incoming and outgoing traffic:	Yes
Quarantine:	Yes
File filtering:	Yes
Message filtering:	Yes

ANTISPAM
Engines:	Signature with CI micro updates every 60 secs
Protocols scanned:	SMTP - POP3 - IMAP4 - NNTP
Black and white lists:	Yes
Sensitivity levels:	Yes
RBLs / DNSBLs / NDR / BATV:	Yes
Quarantine for spam and probable spam:	Yes

WEB FILTER
Engines:	Cloud
Protocols scanned:	HTTP - HTTPS
Filtering by URL category / sub category:	YES more than 70 (Social Networking etc.)
Different policies for users / groups:	Yes
List of VIP users excluded from filtering:	Yes

APPLICATION FILTER
Instant Messaging:	Yes
Peer-to-Peer programs (P2P):	Yes (Bittorent, eDonkey etc.)
Web 2.0 Protocols:	Yes (Skype, Spotify etc.)

Technical requirements:

VMWare versions:
- VMware ESX / ESXi: 4.0 / 4.1
- VMware Server: 2

Web administration console:
- Internet Explorer 8.0 and Firefox 3.5

Hardware requirements for physical machine that will host the virtual server, segmented by users:

HARDWARE \ USERS	50	100	250	500	1000	1000 +
MEMORY	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

Panda Security Awards and Certifications