

Content Security at network perimeter



Panda **GateDefender** Performa 9000 Series

Your first line of defense

The Importance of Perimeter Protection

Internet-based threats are increasing in both frequency and impact across today's enterprises. Unsolicited e-mails are creating major problems for all companies, either in the form of security threats, consuming excessive network bandwidth and storage, or by reducing employee productivity by permitting large volumes of spam to reach users' desktops.

According to the Messaging Anti-Abuse Working Group (MAAWG), 82-87% of all incoming email is currently categorized as spam or 'abusive email'.¹ The amount of spam is already enormous, and is increasing every year:²

- 1978 – An e-mail spam is sent to 600 addresses
- 1994 – First large-scale spam sent to 6,000 newsgroups, reaching millions of people
- 2005 – (June) 30 billion spam emails sent per day
- 2006 – (June) 55 billion spam emails sent per day
- 2006 – (December) 85 billion spam emails sent per day
- 2007 – (February) 90 billion spam emails sent per day

Less frequent than spam, but more dangerous by far are the various forms of Internet-based security threats that are targeting enterprises. These threats are often either politically or financially motivated. A recent article from the BBC News Bureau illustrates this trend dramatically. They connected an unprotected Windows XP machine to the Internet with no firewall or anti-virus software to see how long it would be before it was hit by something devastating from the Net. In just eight seconds, the unprotected PC was hit by Sasser – one of the fastest spreading worms on the Internet!³

Latest concerns about security have their origin in the internal network. The loss of critical or sensitive information stored in the corporate network can affect organizations dramatically. Personal or financial data sent out from the enterprise network can cause inestimable legal and economical damages. These damages must be avoided through a rationally customized Security Policy enforced by a robust and proper tool with a strategic position in the network.

However, any Security Solution must guarantee the reception of important information. A false positive on detecting spam or potentially dangerous contents can cause delays and critical information loss, turning the solution into a part of the problem.

In addition, the amount of traffic received or sent by today's enterprises is growing continuously day by day, what makes the gateway a critical point in the network where any added device must guarantee the traffic flow with no interference.

¹ http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf

² http://en.wikipedia.org/wiki/E-mail_spam

³ http://news.bbc.co.uk/1/hi/programmes/click_online/4423733.stm

Secure Content Management (SCM) Solutions

Hardware perimeter protection devices can effectively prevent Internet-based threats from reaching the enterprise's internal network.

However, different types of threats are best dealt with by different categories of dedicated devices. Some of these solutions offer content-based protection; others include protection against network-level threats.

Appliances dedicated to protecting against content-based threats are known as Secure Content Management devices. But very few vendors are able to offer solutions that can deliver complete dedicated protection for corporate networks.

Some vendors simply offer point solutions that are specialized dedicated devices for detecting against just one specific type of content-based threat, such as spam. Other vendors offer protocol-specific specialized devices. These appliances concentrate on only one type of traffic, such as e-mail (SMTP, POP3, or IMAP).

Due to the complexity and variety of Content based threats the trend in the enterprise perimeter security is the convergence of email and browsing content protections in one single device, according to market analysts:

“By 2010, viable solutions will offer inbound scanning across protocols to keep the bad content out, and outbound scanning across protocols.”

- Gartner

Panda GateDefender Performa is a hardware device incorporating high performance, dedicated software to prevent content-based threats, including malware, potentially risky contents, spam, and inappropriate Web content, from entering the corporate network. It combines reactive protection with a preventive heuristic detection engine to guarantee security – even against the latest unknown threats.

Panda GateDefender Performa - Your proactive first line of defense

Panda GateDefender Performa offer companies of all sizes highly scalable and comprehensive gateway-level protection against all kind of Content-based threats.

Panda GateDefender Performa is the most powerful SCM device in its class. It provides a more comprehensive solution than specialized protection appliances thanks to its modular structure. Companies can choose the anti-malware, anti-spam, and Web filtering models they want to enable. Panda GateDefender's modular protection system means that the solution can be adapted to the protection needs of the company. The protection modules are illustrated in the following table:

Panda GateDefender Performa module	Protection included
Anti-malware module	Anti-malware protection
	Content-Filter protection
Anti-spam module	Anti-spam protection
Web filter module	P2P and instant messaging application filter
	Web Filter

Table 1. Modules contained in Panda GateDefender Performa.

Included Protections

- 1. Anti-Malware Protection:** GateDefender Performa detects and blocks all types of Internet-borne malicious code before it reaches the corporate network. Files containing unknown or non-disinfectable malware can be stored in a special quarantine and eliminated later. Suspect malware can even be automatically sent to PandaLabs in order to be automatically classified and disinfected accordingly, with no administrator intervention.
- 2. Content Filter:** GateDefender Performa enables administrators to establish a corporate security policy to filter out potentially dangerous content and prevent confidential or personal data from leaving the company.
- 3. Anti-Spam Protection:** The solution verifies all inbound and outbound mail. Every message is classified as spam, probably spam, or not spam. The sensitivity of the anti-spam filter can also be adapted to each network user.
- 4. Blocking of P2P and IM Applications:** Peer-to-peer applications eat up corporate bandwidth and represent an important security hole, as files are often divided into small packets and cannot be scanned. Instant messaging also affects productivity as it is most frequently used for personal ends by workers. Panda GateDefender Performa can block the use of these kinds of applications from within the corporate network.
- 5. Web Filter:** Administrators can define the categories of inappropriate Web content. They can also establish white and black lists of restricted or permitted pages. This optimizes resource usage and improves user productivity. It also shut down access to offensive, violent, or any other inappropriate content.

If a company does not use certain communication protocols, GateDefender Performa offers the option to disable any of the six protocols which it can scan: HTTP, FTP, SMTP, POP3, IMAP4, and NNTP. By scanning fewer protocols, performance is improved. But there is a possibility that other protocols will need to be protected in the future. Enterprises can add these protocols at any time to increase the span of protection.

Panda GateDefender Performa provides the most up-to-date protection on the network, as it automatically and transparently downloads malware signature files and classified URLs every 90 minutes, while spam data are downloaded every minute to guarantee the quickest response to this threat. In addition, the solution uses the leading technologies on the market in each module to ensure the best results, including anti-malware from Panda Security, anti-spam from Cloudmark, and Web filter from Cobion.

Panda GateDefender Performa allows the definition of user based profiles and the adaptation of corporate Security Policy to every single user or group needs, making the protection as flexible or robust as every particular situation demand.

Key features

- **Connect and Forget:** Panda GateDefender Performa operates as a transparent bridge, so its installation is as simple as physically placing the device between the Internet and the corporate network. Transparent bridging is a self-configuring system that eliminates the need for administrators to redirect traffic. Once installed, Panda GateDefender Performa scans traffic in both directions between the Internet and the corporate network.
- **Preventive Protection:** Panda GateDefender Performa optimizes signature-based detection with the use of heuristic engines. These enable detection of new threats that have not yet been catalogued. In addition, signatures file is continuously updated with all the malware knowledge detected by Panda's Collective Intelligence.

- **Complete Protection for Multiple Protocols:** Panda GateDefender Performa scans the six most widely used protocols: HTTP, FTP, SMTP, POP3, IMAP4, and NNTP for malware, spam, or inappropriate Web content. Organizations can also enter additional ports for each protocol.
- **Separate Quarantine:** Panda GateDefender Performa provides three types of quarantine for malware, spam and objects blocked by Content Filter, in order to guarantee the reception of all important transmissions.
- **Load Balancing:** GateDefender Performa includes both native and automatic load balancing. Loads can be shared among different units adapting to traffic conditions of any company, as a result, increasing the performance of the perimeter protection against viruses, spam, and inappropriate content.
- **High Performance Capacity:** Panda GateDefender Performa offers extraordinary performance and scan capacity: up to 740 messages per second and 360 Mbps, completely transparently to the corporate network.
- **LDAP/AD Integration:** Panda GateDefender Performa provides integration with directory services to ease the correlation of perimeter events and internal users and groups. This provides administrators with access to particular users security information which is useful to quickly adapt the security policy to changing conditions.
- **User and Group based profiles:** Panda GateDefender Performa allows the creation of particular security conditions for the different members of the corporate network.
- **Detailed Reports and Customizable Alerts:** Panda GateDefender Performa provides complete graphic reports on the detection of viruses, spam, and blocking of inappropriate content. Reports can be easily exploited and used to justify security investment. It also includes customizable warnings and notifications about protection activity.
- **Real-Time System Monitoring:** The notification system offers real-time control of statistics on the network traffic and system activity. It also allows remote and centralized monitoring of all devices across the network, using SNMP and Syslog.
- **Minimal Impact on Network Performance:** Bandwidth is a critical and costly resource for Organizations. GateDefender Performa provides optimum functionality with a minimal impact on the speed of the network.
- **Remote Administration:** Panda GateDefender Performa includes secure, remote administration through a simple and intuitive Web console. This console gives administrators the flexibility to access from any computer with a Web browser.

Panda offers four GateDefender Performa hardware models to adapt to the gateway protection level needs of companies of any size (see Table 2 below.) It provides complete flexibility with the ability to quickly and easily move from one hardware model to the next.




Performance Table	GateDefender Performa 9050	GateDefender Performa 9100	GateDefender Performa 9200	GateDefender Performa 9500
				
HTTP (Mbps)	275	320	420	510
SMTP (message/sec.)	115	135	200	220
Concurrent Conections	600	1800	3600	7200

Table 2. Comparison of the four hardware models of GateDefender Performa.

Benefits to the Organization

Panda GateDefender Performa delivers a wide range of benefits to companies of all sizes:

- **Avoids Complexity** due to its transparent bridge behavior that allows an easy install with no need of change on network architecture.
- **Increases the users' productivity** thanks to the liberation of spam in their mailboxes, the restricted use Instant Messaging or Peer to Peer programs and the control on web contents they can access.
- **Reduces the Operating Costs** thanks to the automatic continuous updates that enable an unattended work after install.
- **Contributes to the company Regulatory Compliance** avoiding the critical data leakage based on the content itself or customized by user profile.
- **Enforces Risk Management** because it is highly preventive to detect and disinfect unknown threats, at the perimeter, without administrator intervention.
- **Enables Business Continuity** by optimizing the broadband use on blocking all useless traffic coming from the Internet (around 70%) before it enters the network.

Compared with...	GateDefender Performa has...
Other dedicated SCM appliances	The best performance on the market
Dedicated appliances specialized by protection	Better performance
	Improved scalability, with the possibility to extend to other protection
Dedicated appliances specialized by protocol	Similar performance
	Greater protection capacity
UTM appliances	Better performance
	Greater security by utilizing separate devices

Table 3. Comparison of GateDefender Performa to other categories of perimeter security solutions.

Summary

GateDefender Performa is Panda Security's high-performance SCM appliance that protects the corporate network perimeter. It provides powerful and feature-rich perimeter protection against all types of Internet-borne content threats. Thanks to its anti-malware, anti-spam, and Web filtering features, it fulfils all the security needs of network administrators – detecting and eliminating all content-based threats, removing junk mail, and protecting employees against accessing unproductive Web content.

What's more, outgoing traffic Content is also scanned avoiding sensitive data leakages or involuntary sends of spam or malicious software that can affect to customers, partners, providers, etc.

In addition a customized configuration of protections for every network user or group will guarantee at the same time a flexible but strict application of Corporate Security Policy.