



Web content filtering in the corporate network perimeter

The information contained in this document represents the current view of Panda Software International, S.L. on the issues discussed herein as of the date of publication. This document is for informational purposes only. Panda Software International, S.L. makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Panda Software International, S.L.

Panda Software International, S.L. may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Panda Software International, S.L. the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.



Content

1	Introduction.....	2
1.1	Objective.....	2
1.2	Audience.....	2
2	Why is web filtering needed?	3
2.1	Economic impact	3
2.1.1	Lower staff productivity	3
2.1.2	Increasing use of network resources.....	3
2.1.3	Increasing security risks	3
2.1.4	Increasing legal risks	3
2.2	Quantative studies.....	3
3	Preventing access to undesirable Internet content.....	4
3.1	Possible alternatives	4
3.1.1	Corporate policy.....	4
3.1.2	Monitoring	4
3.1.3	Restrict access through a proxy server:	4
3.1.4	Intelligent web content filtering	4
4	The GateDefender Performa web filtering solution.....	5
4.1	Automatic filtering.....	5
4.1.1	Creating a category file.....	7
4.1.2	Intelligent scanning of web pages	7
4.2	Manual filtering	8
4.2.1	White list	8
4.2.2	Blacklist.....	8
4.2.3	Excluded from filtering (VIP list)	8
4.3	Actions.....	9
5	Main benefits of GateDefender Performa	10
6	Technical details	11
6.1	Operating system and interception software.....	11
6.2	Self-repair system:	11
6.3	Watchdog: fault tolerance system	11
6.4	Load balancing.....	12
7	Summary and conclusions.....	13



1 Introduction

Internet is the source of information most widely used by companies worldwide. Two in three employees use it as a work tool. However, the Internet also offers a wide range of non work-related content, such as leisure services, online shopping and a large list of etceteras, which employees with Internet access could also access during work hours.

For this reason, it is vital for companies to be able to control **Internet content** that their employees can access, and ensure beneficial use of this technology and avoid **loss of productivity**.

1.1 Objective

Discover the different techniques for preventing the users in a corporate network from accessing Internet content that is not relevant to the company and how GateDefender Performa handles undesirable Internet content and the filtering function of GateDefender Performa.

1.2 Audience

The content of this document is aimed at:

- IT users.
- Network administrators.
- Security experts.
- CTOs (Chief Technology Officer).
- CIOs (Chief Information Officer).



2 Why is web filtering needed?

Internet provides a wide range of content related to all topics. A large part of it is necessary to develop business activity. For this reason, companies in the twenty first century need the information available on the Internet to guarantee good results.

However, the **universal nature of this content** allows employees with Internet access to make **personal use** of company resources, accessing content that is not related to their work, and thereby degrading the company's profitability.

2.1 Economic impact

Misuse of the Internet has a negative influence on companies' results by:

2.1.1 Lower staff productivity

Companies lose productivity when their employees waste time visiting non work related web content , not only content related to their hobbies but also personal matters, such as online banking, employment offers, chats, etc. The loss to the company can be measures in the cost of the hours employees spend visiting these types of websites.

2.1.2 Increasing use of network resources

All the information transferred between the Internet and the corporate network uses costly network resources, such as bandwidth. If employees use these resources to access content that does not benefit the company, the traffic of information that is important to the company will be affected, delaying the processing of this information and the work of colleagues

2.1.3 Increasing security risks

The weakest part of a security system is the human component. Employees downloading potentially dangerous programs or files from the Internet could infect the network with threats like spyware, capable of extracting confidential information and sending it to third-parties.

2.1.4 Increasing legal risks

Accessing web pages with illegal, offensive sexual or violent content or downloading these types of content can damage corporate image, which should always try to guarantee a dignified work environment for its employees. The damage to the corporate image is worsened if this content is forwarded from a corporate workstation.

2.2 Quantative studies

Companies need to be able to access their employees' Internet access. Between **30 and 40 percent of Internet use is non-work related**. At least **60 percent of employees use** the Internet at work **for personal reasons** (chats, auctions, online shopping, etc). What's more, data shows that 70 percent of accesses to web pages with pornographic content are visited during working hours, forcing companies to consider non-work related Internet use as a responsibility that they must assume.

The damage that access to irrelevant web content can cause the companies is varied.

There is **financial damage**, as it reduced employee productivity generating huge costs calculated as working hours.

It could also cause **legal damage**, as the company could be related to illegal Internet content, such as fraud, piracy, pedophilia, etc.

The **technical damage** must also be considered, as unproductive web browsing could use costly resources like bandwidth and generally degrades local network performance.



3 Preventing access to undesirable Internet content

There are many different ways of preventing employees from access irrelevant content in the Internet. However, not all are truly effective.

3.1 Possible alternatives

Given the structure of the Internet, the only way of preventing access to undesirable content is to increase employee awareness.

3.1.1 Corporate policy

Many companies establish rules in their policy that prohibit employees from accessing certain types of pages. In large companies the problem is difficult to control, as the large number of employees makes prevents companies from ensuring that all employees adhere to the corporate policies.

3.1.2 Monitoring

Attempting to control employee access through supervision is an expensive option, as it requires staff dedicated to analyzing Internet access. In companies with a large staff or large volume of Internet traffic it is impossible to implement this option.

3.1.3 Restrict access through a proxy server:

There are network components known as proxies, which can be hardware or software devices and prevent certain computers in the corporate network from accessing certain Internet IP addresses. However, this solution is difficult to maintain, as the IP address of pages with undesirable content change every day.

What's more, access is restricted based on IP addresses and not content. This restricts access to entire domains, in which not all information is irrelevant and could contain material that is very to useful for the company's staff.

3.1.4 Intelligent web content filtering

This option involves the company restricting access to certain content and preventing this undesirable content from reaching employees. What's more, it offers manual control over access to certain web pages and allows users to be excluded from the web filtering, making the only truly effective option available for implementing reliable content filtering.



4 The GateDefender Performa web filtering solution

Panda GateDefender Performa offers the most effective protection for preventing users of the corporate network from accessing undesirable web content, 'intelligently' analyzing employees' requests for access to web pages and offering a rapid and effective response if these pages are considered undesirable for the company.

4.1 Automatic filtering

The corporate network administrator can access a series of categories and allow or deny access to them. These **categories** are divided into groups and access can be allowed or restricted for each group or each sub-category.

The 59 undesirable content categories in GateDefender Performa range from media to online auctions, through **spyware**, violent content, instant messaging, etc.

It is obvious that it is not easy to add a web page to a certain category based on simple coincidences.

To sum up, the only thing the administrator needs to do to filter web content is select the content categories that must not be downloaded. By doing this, GateDefender Performa blocks access to web pages containing elements that fall under this category.

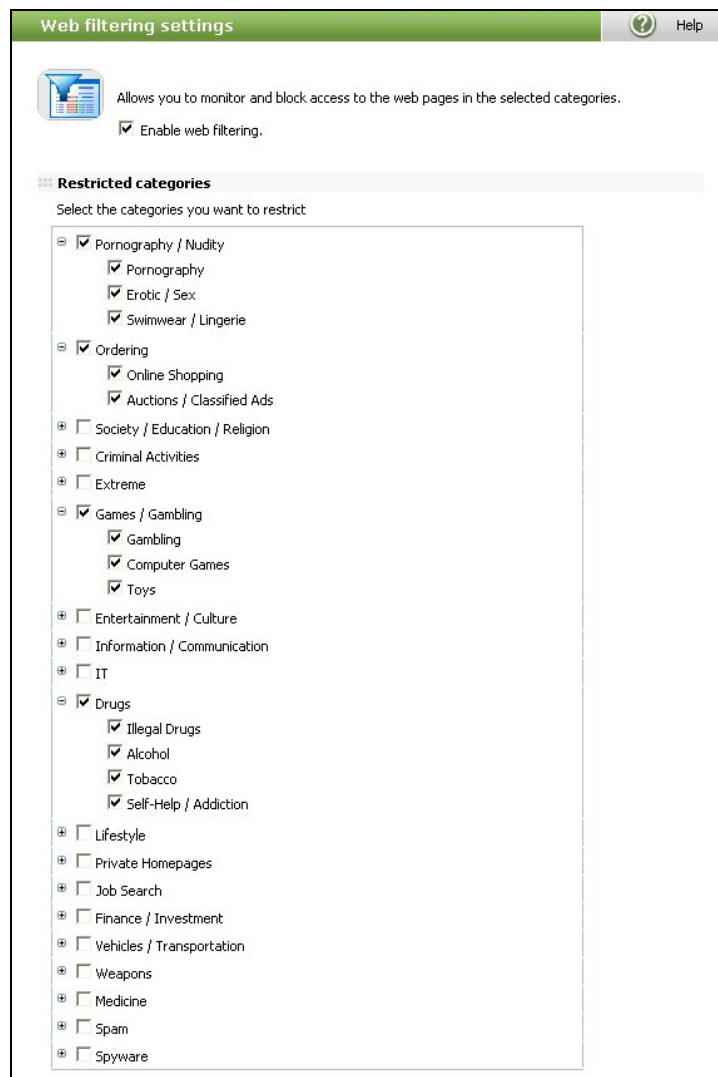


Figure 1: Configuring web filtering by categories



Web content filtering in the corporate network perimeter



In order to include web pages in one category or another, an extremely advanced intelligent analysis method is used, and the results are included in a file.



4.1.1 Creating a category file

The page file organized into categories is generated remotely and automatically updated every 90 minutes without user intervention. This prevents GateDefender Performa from having to analyze every page viewed, which would delay access to the page, making web browsing extremely tedious.

In order to create category files, servers located in different geographical locations are constantly scanning the Internet for these types of contents. Over 2,600 million pages are scanned and added to the file, generating over 100,000 new entries a day. This results in the biggest database of URLs in the world, which grows every day and is automatically updated without degrading its filtering activity.

4.1.2 Intelligent scanning of web pages

Each web page found is thoroughly scanned using different methods.

- Text analysis
- Image analysis

Intelligent analysis of a web page through both of these methods allows pages to be accurately added to a category, as an in-depth scan of the web pages prevents classification errors.

Text analysis

A medical page or psychiatric page contains words related to violence as it describes mental health problems and could, therefore, easily be included in the violence category. However, this would not happen with the scan for generating the categories, as it does not only look for single words but analyzes the content in which they appear.

Some pages could easily be classified as undesirable could include texts in images that the text analysis would not pick up.

However, the text analysis engine incorporates OCR (Optical Character Recognition) capable of analyzing text inserted in images as of it were written text on the page.

Image analysis

The images in a web page allow pages to be identified as online shopping, pages with sexual content, etc,

The image analysis engine can detect the content of each web page, distinguishing

- Faces
- Nudity
- Logos
- Objects

What's more, its powerful texture analysis feature helps determine the nature of each image. This is better explained using an example:

When a face is detected in an image, the percentage of the image that corresponds to the face is calculated. If the image is much bigger than the face, it is probably a photograph of a full body. In this case the texture of the face is analyzed (the skin) and the percentage of the image with a similar texture is evaluated. If the percentage of the skin texture in the photograph is quite high, it is easy to determine that the image corresponds to a naked body.

The real analysis process is much more complex than described in the example in order to avoid mistakes, but it is without a doubt an artificially intelligent engine, capable of detecting the nature of every image analyzed.

Once a web page has been blocked by both engines, the page is classified based



on the result of each analysis. As you can see the classification implemented by the automatic filtering by categories is extremely reliable and the most interesting aspect of this process is that GateDefender Performa does not have to carry it out, as this is done remotely and the results are entered in GateDefender Performa, resulting in optimum performance.

4.2 Manual filtering

A tool is also available to administrators to manually add or exclude the content of certain pages from filtering.

4.2.1 White list

The administrator can add trusted domains, URLs or IP addresses to the white list that network users will always be able to access, regardless of the category or whether they are prohibited or not. This is better explained using an example.

A company may not want employees to be able to access news sites to prevent them from wasting time. If the newspapers and magazine category is selected, this content will be filtered and users will not be able to access them. However, a publication could contain information that is important for the company and therefore, employees need to be able to access it. Simply add the domain of this publication to the white list and access will be permitted.

It is important that access to a page in the GateDefender Performa white list is never analyzed to check the category it belongs to. Access is allowed, optimizing the speed and taking the workload off GateDefender Performa.

4.2.2 Blacklist

The blacklist does just the opposite to the white list. The administrator can add trusted domains, URLs or IP addresses to the blacklist that network users will never be able to access, regardless of the category or whether these pages are in a prohibited category or not. This is better explained using an example.

It is understandable that a company does not want its employees to access rival companies' websites that offer jobs in order to prevent staff from being lost to these companies. If the company activity is "normal", the websites of these companies probably don't belong to an undesirable web content category and GateDefender Performa will not block access. In this case, the domains of rival companies can be added to the blacklist. This will prevent corporate network users from accessing these pages.

It is important that GateDefender Performa denies access to a page in the blacklist without analyzing it to check the category it belongs to, optimizing the speed and taking the workload off GateDefender Performa.

4.2.3 Excluded from filtering (VIP list)

Administrators can access a list called the VIP list, where they add the address of computers that will be able to access all Internet content. These users will be excluded from web filtering.



4.3 Actions

When a computer connected to the corporate network tries to access undesirable web content, GateDefender Performa will block access to the page. The network administrator can define the alternative page that will be displayed. The content of this page can be edited by the administrator in the preferred language to inform network users that access to the page is restricted.

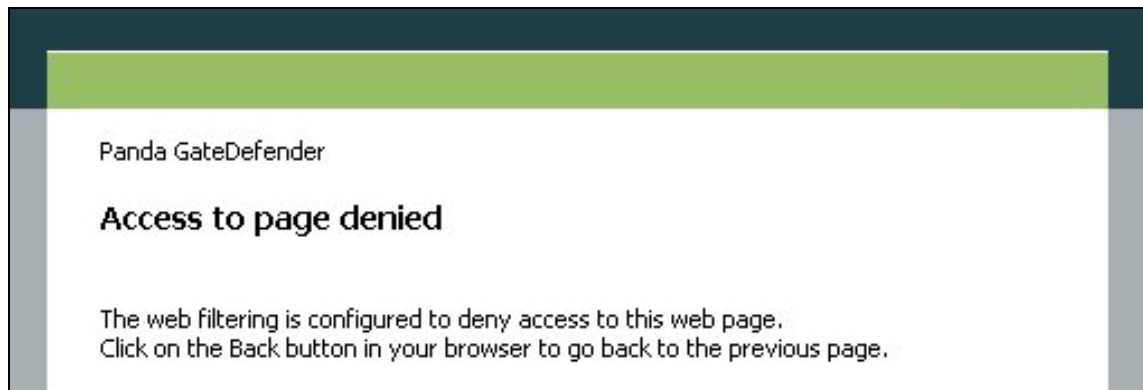


Figure 2: Alternative window for prohibited URLs

Whenever necessary, administrators can access real-time graphic information about the functioning of the web filtering system. What's more, GateDefender Performa automatically generates detailed graphic reports on access blocked or allowed from corporate network workstations. The content of the reports and the fields to include can be easily defined by the administrator.

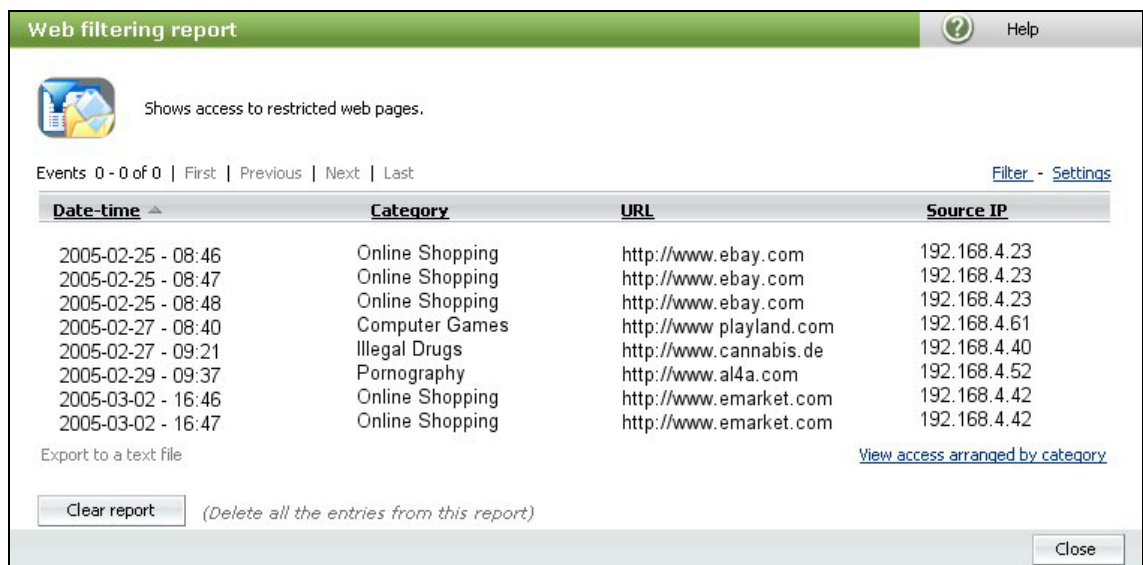


Figure 3: Report on web access filtered



5 Main benefits of GateDefender Performa

The main advantages of the new version of GateDefender Performa are its efficiency, automatic updates, ease of use ('plug-in and forget') and high performance and scalability.

Complete protection: It scans the HTTP web browsing protocol through all the ports defined by the network administrator.

High performance, transparent to users: Panda GateDefender Performa takes over the workload of the traditional protection, optimizing use of the network resources.

It guarantees excellent performance and the highest scanning capability of its class. It can scan up to 30 Mbps completely transparently to corporate network users and without degrading network performance.

Auto-updates: The updates system against new spam messages is programmed by default to be carried out completely automatically every hour and a half. This means that Panda GateDefender Performa will be the most up-to-date protection across the network.

Simple administration. Plug-in and forget: Panda GateDefender Performa is designed to be implemented simply in any network, with no need for redirecting network traffic.

GateDefender Performa sends to the administrator in a proactive way all relevant information about the Web Filtering activity, in real time graphic reports. It is managed remotely and securely through a simple and intuitive web console.

Low cost of ownership: By preventing saturation of network resources and loss of productivity, Panda GateDefender Performa offers higher resource management capabilities. All of this, along with its 'plug-in and forget' operation, requiring minimum administrator intervention, results in low cost of ownership of Panda GateDefender Performa.

High scalability and load balancing: GateDefender Performa adapts perfectly to the needs of all small to large companies, adjusting scan capacity to the overall volume of network traffic.

Its load balancing is completely automatic and native, allowing workload to be shared across multiple units. The result is increased scalability and improved antivirus performance for complete protection of your network perimeter.

Detailed reports and customizable alerts: GateDefender Performa offers graphic statistics on the network traffic and system activity. It also offers comprehensive web filtering graphic reports, as well as customizable alerts and notifications.

Other options available: As well as the web filtering protection, GateDefender Performa also offer other types of protection

Anti-malware protection: This prevents unknown viruses, worms or any other malicious code from getting into the company and saves network resources and bandwidth, blocking potentially dangerous content before it enters the network.

Anti-spam protection: This prevents junk mail from reaching corporate network users, avoiding unnecessary use of corporate network resources and optimizing employee productivity, as they do not have to waste valuable time opening, reading and deleting spam messages.



6 Technical details

6.1 Operating system and interception software

The software incorporated in GateDefender Performa is based on the **GNU/Linux** operating system, reinforced and optimized to offer maximum security and high performance. The operating system used in GateDefender Performa only includes the services and processes it needs to function correctly.

Panda GateDefender Performa acts as a transparent bridge between the Internet and the corporate network. This means that the traffic passes through **transparently** and the device intercepts HTTP sessions.

6.2 Self-repair system:

Under extreme circumstances (excessive heat, etc.) damage could be caused to the Panda GateDefender Performa hardware, such as hard disk corruptions or physical errors in some partitions, etc.

To prevent system failures in these cases and ensure continuous perimeter antivirus services, Panda GateDefender Performa includes a system for controlling partitions or a **self-repair system**. When Panda GateDefender Performa starts, a control partitions starts up that determines which work partition will be used to run the anti-spam system.

If the self-repair detects that the work partition has failed for any reason, the next work partition established will be started up. It also incorporates a process for **restoring the partition** that has failed in order to guarantee that it works in subsequent startups. The partitions are kept updated with the latest versions of the software, in order to make recovery as little traumatic as possible.

There are other perimeter solutions that promise high-availability using SCSI RAID disks. Panda Software believes that **SCSI RAID disks** are only necessary for storage servers that have to protect data and provide high-availability. However, SCSI RAID disks don't offer any benefits in devices that are not geared to storing data, such as Panda GateDefender Performa or other appliances on the market. This is really just another marketing angle that does no more than add to the cost for the end-user and Panda Software would prefer to **eliminate unnecessary costs**. Panda GateDefender Performa offers high-availability by using tools like **WatchDog** and its **Self-Repair system**, as well as **load balancing**.

6.3 Watchdog: fault tolerance system

The motherboard of GateDefender Performa incorporates a system monitoring circuit to prevent the system from blocking or failing for long periods of time. The WatchDog system receives signals indicating that it is functioning correctly and if it does not receive this signal within a specific interval, WatchDog will completely reset the system from the motherboard, avoiding loss of network services for excessive periods of time.

Thanks to this fault tolerance system, Panda Antivirus GateDefender Performa can recover automatically from service failures either in the applications or the operating system.

As well as WatchDog hardware, Panda GateDefender Performa also incorporates WatchDog software, which periodically monitors the status of all the processes that are running. If it detects a process is not responding, WatchDog will try to recover it without needing to restart the system. If it cannot be recovered through the software, GateDefender Performa will be completely restarted from the WatchDog hardware. Thanks to this fault tolerance software system Panda GateDefender Performa can



recover automatically from service failures without needing to completely restart the system.

6.4 Load balancing

Load balancing allows the workload to be shared across multiple GateDefender Performa units, providing improved performance and higher availability. No additional hardware or software is needed to implement load balancing across multiple GateDefender Performa units and although it is highly advisable to use switches, these can also be connected through hubs.

One of the appliances will act as the master, with the rest acting as slaves. From the administration console, users can view all the appliances in the load balancing system and the mode each one is running in.

When several GateDefender Performa units are installed in parallel, they will automatically negotiate the role or mode of functioning of each one and whenever a new appliance is incorporated, the modes of functioning will be re-negotiated.

The master appliance implements a load balancing algorithm and redirects connections to the different slave appliances in order to balance the system workload. The master appliance will also scan connections and let clean traffic through.

Slave appliances will not let traffic through and will simply scan the connections redirected to them, returning clean traffic to the master appliance.



7 Summary and conclusions

The **negative impact** of browsing undesirable web content during working hours on companies is a proven fact. As is nearly always the case, adopting **preventative measures** is actually more profitable than having to correct an undesirable situation which may increase the risk of damaging the **reputation of the organization**.

Employees must therefore, be kept **well informed** when it comes to using Internet resources to do their job without causing drops in performance during working hours.

Controlling Internet access **manually** in companies and using no other method is not an option. The same can be said for **banning Internet browsing entirely**.

Although all members of the company should be involved in preventing the dangers of using the Internet for personal use someone – the network administrator– must coordinate these efforts. And this **coordination task is much easier** if the administrator has a tool like **GateDefender Performa** which allows the web content filtering policy to be installed, maintained and supervised with a minimum effort.



APPENDIX A. Glossary of terms

Proxy: Device for centralizing Internet queries from a network.

IP: Internet Protocol

IP address: Address of each network devices, compatible with the routing mode of the IP protocol (Internet Protocol).

URL: Stands for Uniform Resource Location. This is the location of a specific resource.



APPENDIX B. Panda Software worldwide

<p>Panda Headquarters in Europe</p> <p>Ronda de Poniente 19 Tres Cantos 28760 Madrid, España</p> <p>Phone: +34 91 806 37 00</p> <p>E-mail: info@pandasoftware.com</p>	<p>Panda Headquarters in USA</p> <p>230 N. Maryland, Suite 303 P.O. Box 10578 Glendale, CA 91209, USA</p> <p>Phone: +00 1 818 543 6901</p> <p>E- mail: usa@pandasoftware.com</p>
<p>Panda Software Germany</p> <p>Dr.-Detlev-Karsten-Rohwedder-Str. 19 47228 Duisburg</p> <p>Phone: +49 20 65 9 87 654</p> <p>E-mail: germany@pandasoftware.com</p>	<p>Panda Software Saudi Arabia</p> <p>P.O.BOX # 2797, AL KHOBAR 31952, KSA</p> <p>Phone: + 966 3 897 9956</p> <p>E-mail: saudiarabia@pandasoftware.com</p>
<p>Panda Software Argentina</p> <p>Calle Roque Saenz Peña 1160, piso9b Buenos Aires 1035</p> <p>Phone: +00 5411 508 10500</p> <p>E-mail: argentina@pandasoftware.com</p>	<p>Panda Software Austria</p> <p>Rennweg 98 Top 7 A – 1030 Wien</p> <p>Phone: +49 02065 987654</p> <p>E-mail: austria@pandasoftware.com</p>
<p>Panda Software Belgium</p> <p>Mechelen Campus Schaliënhoeverdreef 20d 2800 Mechelen Belgium</p> <p>Phone: +32 2 756 08 80</p> <p>E-mail: belgium@pandasoftware.com</p>	<p>Panda Software Bolivia</p> <p>Calle Landaeta # 221, Edificio Gamarra 3er Piso La Paz – Bolivia Código postal 11433</p> <p>Phone: +591 2 211 4777</p> <p>E-mail: bolivia@pandasoftware.com</p>
<p>Panda Software Canada</p> <p>SECURE RDG CANADA INC 100 Allstate Parkway Suite 502 Markham, CANADA</p> <p>Phone: +1 (905) 479 2208</p> <p>E-mail: canada@pandasoftware.com</p>	<p>Panda Software Bulgaria</p> <p>26-28, Christo Stanishev str. Sofia 1225 BULGARIA</p> <p>Phone: +359 2 81 328 11</p> <p>E-mail: bulgaria@pandasoftware.com</p>
<p>Panda Software China</p> <p>Room 1003,10F,Minfang Building, 593 Fuxing Road(M), 200020 Shanghai</p> <p>Phone: +86 21 2402 8800 +86 21 2402 8526</p> <p>E-mail: china@pandasoftware.com</p>	<p>Panda Software Chile</p> <p>Mosqueto 459 ofic. 202 8320112, Santiago-Centro Chile</p> <p>Phone: +56 2 639 7541</p> <p>E-mail: chile@pandasoftware.com</p>
<p>Panda Software South Korea</p> <p>3Fl. SungWoo Bldg. 114-29 SamSung-Dong, KangNam-Gu, Seoul - Korea</p> <p>Phone: +82-2-555-8600</p> <p>E-mail: korea@pandasoftware.com</p>	<p>Panda Software Colombia</p> <p>Carrera 41 N.46-26 Itagui Antioquia</p> <p>Phone: + 57 4-3735588</p> <p>E-mail: colombia@pandasoftware.com</p>
<p>Panda Software Denmark</p> <p>Ny Vestergardsvej 15 DK 3500 – Værløse</p> <p>Phone: +45 44 355 375</p> <p>E-mail: denmark@pandasoftware.com</p>	<p>Panda Software Costa Rica</p> <p>Calle 25, Ave 6 y 8 #648 San José</p> <p>Phone: 00 506 258 0100</p> <p>E-mail: costarica@pandasoftware.com</p>



<p>Panda Software Slovakia Lublanska 1 83102 Bratislava Phone: +421 2 444 55 702 E-mail: slovakia@pandasoftware.com</p>	<p>Panda Software UAE Bldg-5 Office No. 5G-15 P O Box 41573 – Hamriyah Free Zone, Sharjah Phone: +971 (6-526.30.14) E-mail: UAE@pandasoftware.com</p>
<p>Panda Software Spain Ronda de Poniente 19 Tres Cantos 28760 Madrid Phone: 902 365 505 E-mail: info@pandasoftware.es</p>	<p>Panda Software Slovenia Stari trg 5A, SI-8210 Trebnje Phone: +386 7 34 61 020 E-mail: slovenia@pandasoftware.com</p>
<p>Panda Software Finland Hyvidata Oy Nuutisarankatu 14, 33900 Tampere Phone: +358 3 339 26 700 E-mail: finland@pandasoftware.com</p>	<p>Panda Software USA 230 N. Maryland, Suite 303 P.O. Box 10578 Glendale, CA 91209, USA Phone: +00 1 818 543 6901 E-mail: usa@pandasoftware.com</p>
<p>Panda Software UK 5 Signet Court, Swanns Road Cambridge CB5 8LA Phone: +44 (0)870 444 5640 E-mail: uk@pandasoftware.com</p>	<p>Panda Software France 33 bis Boulevard Gambetta. 78300 Poissy Phone: +33 1 30 06 15 15 E-mail: france@pandasoftware.com</p>
<p>Panda Software Guatemala 5 Av. 5-55 Zona 14, Euro plaza Torre 1 Nivel 2. Ciudad de Guatemala Phone: +502 2386-8866/67/68 E-mail: guatemala@pandasoftware.com</p>	<p>Panda Software Greece 82 Zanni St. Piraeus, ZIP Code 18537 Phone: +30 2 10 4588 085 E-mail: greece@pandasoftware.com</p>
<p>Panda Software Hungary Szugló utca 54 1145 Budapest Phone: +36 1 469 70 97 E-mail: hungary@pandasoftware.com</p>	<p>Panda Software Netherlands Stephensonweg 14 4207 HB Gorinchem Phone: +31 183 699020 E-mail: netherlands@pandasoftware.com</p>
<p>Panda Software Israel 43 Hamelacha street, New Industrial Zone 42504 Natanya Phone: +972 9 – 8859611 E-mail: israel@pandasoftware.com</p>	<p>Panda Software India E-9, Connaught House Connaught Place New Delhi-110001 Phone: +91 11 2341 8199 E-mail: india@pandasoftware.com</p>
<p>Panda Software Japan Nakameguro GT Tower 7F, 2-1-1 Kamimeguro, Meguro-ku, Tokyo 153-0051 Phone: +81-3-6412-6020 E-mail: japan@pandasoftware.com</p>	<p>Panda Software Italy Viale E. Marelli 165 20099 Sesto S. Giovanni (Mi) Phone: 02-24 20 22 08 E-mail: italy@pandasoftware.com</p>
<p>Panda Software Lithuania Žemaitės st. 21, LT – 2009 Vilnius Phone: +370 5 2397833 E-mail: lithuania@pandasoftware.com</p>	<p>Panda Software Latvia Merkela Street 1 1050 Riga Phone: +371 7211636 E-mail: latvia@pandasoftware.com</p>



<p>Panda Software Malaysia Unit A-10-6, Megan Phileo Promenade, 189 Jalan Tun Razak, 50400 Kuala Lumpur Phone: +60 3 2163 2468 E-mail: malaysia@pandasoftware.com</p>	<p>Panda Software Luxemburg Mechelen Campus Schaliënhoedreef 20d 2800 Mechelen Belgium Phone: +32 2 756 08 80 E-mail: luxembourg@pandasoftware.com</p>
<p>Panda Software Norway ViroSafe Norge AS. Skogveien 41 2318 Hamar Phone: 00 47 62 53 96 80 E-mail: norway@pandasoftware.com</p>	<p>Panda Software Mexico Tuxpan 39# 104 y 105, 06760 México, D.F. Phone: +52 5 2642127 E-mail: mexico@pandasoftware.com</p>
<p>Panda Software Peru Calle Lord Cochrane 521 Miraflores – Lima 18 Phone: 00 51 1 221 6001/ 221 0159 E-mail: peru@pandasoftware.com</p>	<p>Panda Software Paraguay Eliseo Reclus 247 Calle Guido Spano Asunción Phone: +00 595 21 607594 E-mail: paraguay@pandasoftware.com</p>
<p>Panda Software Portugal Quinta da francelha - Edificio Sagres, 7B 2685-338 Prior Velho Phone: + 351 219426800 E-mail: portugal@pandasoftware.com</p>	<p>Panda Software Poland Ul. Wiktorska 63 02-587 Warszawa Phone: +48 (22) 540 18 06 E-mail: poland@pandasoftware.com</p>
<p>Panda Software Russia 64-47 Tokarey St., 620109 Yekaterinburg, Sverdlovsk region Phone: +7 3432 78-31-27 E-mail: russia@pandasoftware.com</p>	<p>Panda Software Puerto Rico / Rep. Dominicana Avenida Muñoz Rivera 1058 Edificio Fomento Corporativo - Esquina Yale Río Piedras 00927 Puerto Rico Phone: +1 787 296 1139 E-mail: caribe@pandasoftware.com</p>
<p>Panda Software Sweden Industrivägen 7, S-171 48 Solna Phone: +46 8-545 25030 E-mail: sweeden@pandasoftware.com</p>	<p>Panda Software Singapore 10 Ubi Crescent, # 05-37 Ubi Techpark , Singapore 408564 Teléf:+ (65) 6742 2660 E-mail: singapore@pandasoftware.com</p>
<p>Panda Software Thailand 192 Soi Laprao 107 Bangkapi, Bangkok 10240 Phone: 00 662 7311480 E-mail: thailand@pandasoftware.com</p>	<p>Panda Software Switzerland Route Champ-Colin, 10 1260 Nyon Phone: +41 22 994 89 40 E-mail: switzerland@pandasoftware.com</p>
<p>Panda Software Uruguay Jose Enrique Godó 1955 11200 Montevideo Phone: +5982 4020673 E-mail: uruguay@pandasoftware.com</p>	<p>Panda Software Turkey Darulaceze Cad Karatas Sok. SNS Plaza N° 6 80270 OKMEYDANI – ISTANBUL Teléf.: 90 212 222 1520/90 212 210 2200 E-mail: turkey@pandasoftware.com</p>
<p>Panda Software Venezuela Av. Libertador C.C. Libertador, PH-7 - Caracas Phone: +(58 212) 700.7596 E-mail: venezuela@pandasoftware.com</p>	