**time**for
your**business**

**Protect** your company, freeing up time for your **business.**

PANDA SECURITY | 20th Anniversary 1990-2010

www.pandasecurity.com

# CONTENTS

# 1. Can companies achieve real peace of mind in the face of increasing amounts of malware?

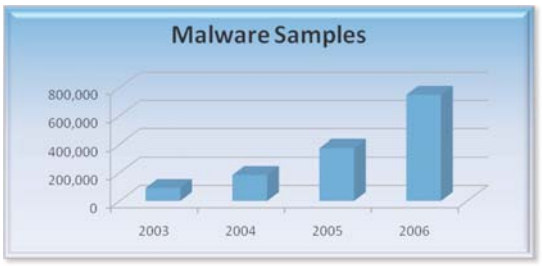
It has been a long time now since widespread epidemics regularly hit the headlines, and mainstream news channels reported infections such as ILoveYou or Sircam. Back then, hackers were after notoriety; they wanted to outstrip the feats of others, infecting more computers as quickly as possible.

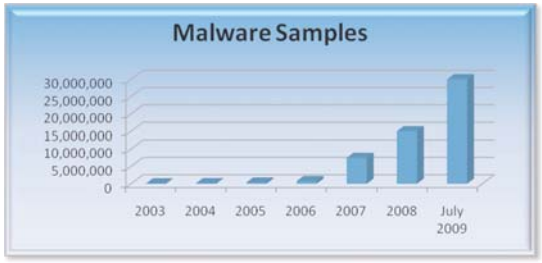
Now, in the 21st Century, the situation has changed. For some time now security providers have been warning of how hackers have become professionals, focusing their efforts on profiting from their activity. They achieve this principally by deceiving users –businesses and consumers alike- and the repercussions of this change of focus have been enormous.

On the one hand, companies have seen how their attempts to safeguard their businesses have been largely unsuccessful. Meanwhile, security vendors have been forced to adopt a new security model to cope with the current scenario.

## A vast avalanche of malware

In recent years, the amount of malware in circulation has risen dramatically and has become notably more sophisticated. The graph below illustrates the malware situation between 2003 and 2006, a period in which the amount of malware in circulation doubled every year:



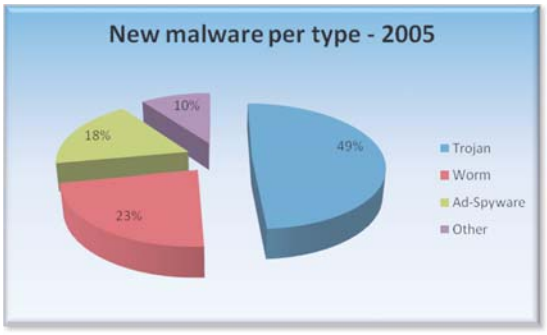




About five years ago, there were just 92,000 strains of malware, yet by the end of 2008 there were some 15 million. By the time the present study was completed –in July 2009- PandaLabs had detected more than 30 million examples of malware.

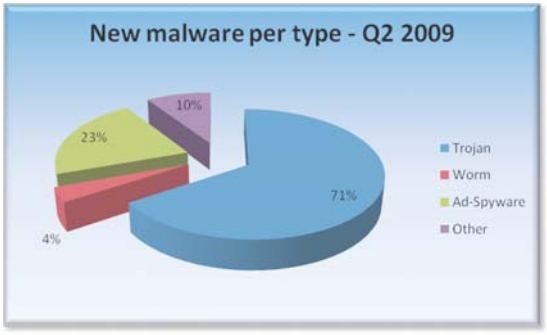
The reason for this spectacular increase is clear: money. The year 2003 saw the creation of the first banker Trojans. Since then, these malicious codes designed to steal login credentials for online bank services have become one of the most widespread varieties of malware.

Every day, increasingly sophisticated variants emerge, designed to evade the security measures put in place by banks. Organizations such as the Anti-Phishing Working Group (www.antiphishing.org) have tried to bring together members of the IT security industry to counteract the activities of cyber-criminals. It is a long hard struggle however, and it is not yet clear that it is one we can win.

In general, the reason that more Trojans, keyloggers and bots are created than other types of malware is that they are more useful for identity theft. In 2005, almost half of new malicious codes were Trojans:




Now, in the second half of 2009, the situation is worse still, with Trojans accounting for 71 percent of new malware:




As with any other business, cyber-crooks seek to maximize the effectiveness of their operations. When developing Trojans, they have to decide which platforms to attack and the number of potential victims. Unsurprisingly, Windows is the target in 99 percent of cases, as it is the most widely-used operating system.

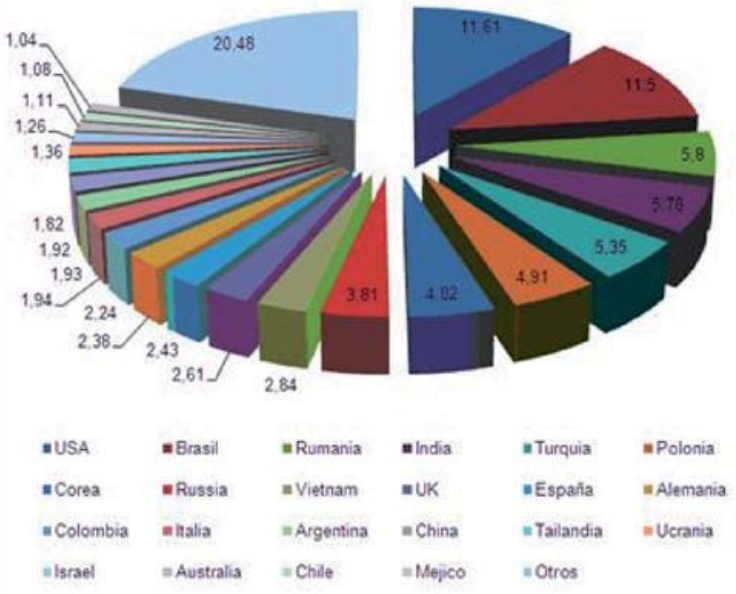
The ultimate objective of cyber-criminals is to profit financially from malware. Trojans are the perfect tool for stealing information, yet this information still has to be converted into hard cash, and criminals are always on the lookout for innovative ways of achieving this.

## Spam

It's a similar story when we talk about spam. Less than seven percent of emails that reached companies in the first quarter of 2009 were legitimate correspondence. Some 90.92% of messages were spam, while 1.66% were infected with some type of malware. These statistics are the result of the analysis of more than 69 million emails by Panda Security between January and July 2009.

The USA continued to figure as the leading source of spam in Q1 2009, accounting for 11.61% of the total, followed by Brazil (11.5%) and Romania (5.8%).

| País | % |
|---|---|
| EEUU | 11,61 |
| Brasil | 11,5 |
| Rumania | 5,8 |
| India | 5,76 |
| Turquía | 5,35 |
| Polonia | 4,91 |
| Corea | 4,82 |
| Rusia | 3,81 |
| Vietnam | 2,84 |
| GB | 2,61 |
| España | 2,43 |
| Alemania | 2,38 |
| Colombia | 2,24 |
| Italia | 1,94 |
| Argentina | 1,93 |
| China | 1,92 |
| Tailandia | 1,82 |
| Ucrania | 1,36 |
| Israel | 1,26 |
| Australia | 1,11 |
| Chile | 1,08 |
| Méjico | 1,04 |
| Otros | 20,48 |




## New infection trends

As security companies become more adept at detecting avalanches of new threats and covering more infection fronts, hackers are busy discovering and exploiting others.

The dangers of infection from the Internet are well known: either through visiting dubious sites that silently infect users, or through downloading files from unreliable sources, etc.

But recently, another trend has emerged for reaching potential victims: blackhat SEO techniques.

BlackHat SEO techniques are not new, although we have seen a sharp increase in their use over the second quarter of 2009. SEO stands for Search Engine Optimization and basically refers to the techniques used to improve the ranking of websites in search engines (Yahoo, Google, etc.). BlackHat SEO refers specifically to the use of SEO techniques by cyber-criminals to promote their Web pages.

To illustrate this situation, on June 1 Microsoft announced in E3 it's "Project Natal", the new system which allows interaction with Xbox 360 without the need for manual controls. This was a widely covered story.

Less than 24 hours later, when searching Google with the words "Youtube Natal", the first result returned was a malicious Web page. When searching for malicious pages created by the same cyber-criminals, we found the following pages with the corresponding subjects:

- **16,000** links **"TV Online"**
- **16,000** links **"YouTube"**
- **10,500** links **"France" (Airline Crash)**
- **8,930** links **"Microsoft" (Project Natal**)
- **3,380** links **"E3"**
- **2,900** links **"Eminem" (MTV Awards/Bruno Incident)**
- **2,850** links **"Sony"**

Youtube has also been a major target for cyber-crooks this quarter. Basically, Youtube lets registered users add comments to the pages displaying the videos. In this case, criminals have been creating accounts and then generating a series of comments automatically. These comments include links to malicious websites designed to infect users. In total, more than 30,000 such malicious comments have been created.

Other social network sites, such as Twitter or Facebook, have also been used to distribute malware.

A worm appeared in April which used a cross-site scripting technique to infect Twitter users when they visited the profiles of other infected users. It then infected the new user's profile to continue propagating. New variants soon appeared of this worm, created by one Mikey Mooney, who apparently wanted to attract users to a service competing with Twitter.

In early June, Twitter was the focus of other attacks, this time using different techniques: basically a variation of BlackHat SEO for Twitter. This social networking service has a feature called "Twitter Trends", which is a list of the most popular topics on Twitter. When users select a topic through this feature, they will see all 'tweets' published related to this issue. As these are the topics that most people read, they make an obvious target for cyber-crooks.

In this case, malicious users were writing tweets about the topics listed in Twitter Trends with links to malicious Web pages from which malware was downloaded. The first attack focused on just one of the topics, but just a few days later the scope of the attack increased and all popular topics contained malicious links. When the actor David Carradine died, in just a few hours there were hundreds of malicious tweets, and the same occurred with other popular issues on Twitter.

Traditional viruses are history. Cybercriminals are now looking to profit from their activities. To do this, they try to sneak under the radar of security vendors, saturate laboratories with waves of malware, or snare victims -corporate and consumer- through social engineering.

Trojans are the most common problem, along with other types of malware that can be used for identity theft. Search engine optimization is also used to trick victims, and social networks are used as platforms to spread malware.

## Current trends in figures

The problem we are witnessing can only be fully grasped by looking at the figures:

- 50,000 files are received every day, of which 37,000 are new malware samples. 99.4% of the files are automatically processed by Collective Intelligence, taking an average of six minutes per case.
- 52% of the new malware processed by Collective Intelligence exists for just 24 hours.
- In the first quarter of 2009, Collective Intelligence processed 4,474,350 files.
- To do this manually would require 1,898 and 926,347 hours of work.
- The Collective Intelligence database occupies more than 18,000 GB.
- If this amount of information were in text format, it would be equivalent to 727,373 volumes of the Encyclopedia Britannica, with almost 33 billion pages.
- Laid end-to-end, these printed pages would stretch for over 9 million kilometers, the equivalent of going to the moon and back twelve times.
- And if we had to send this information across a standard ADSL connection, it would take 1,045 days.

## What risks does this situation present for companies

All too often, the risks are seen as distant and hypothetical, and businesses rarely stop to think about the real impact they might have.

Many obvious risks readily spring to mind, yet there are others whose effects on a company's finances are impossible to predict.

What are these risks?

Logically, all risks can result in financial loss, whether as a result of having to shut down systems or through employees wasting time or hackers accessing confidential data and stealing money.

But have you ever calculated the impact of clients losing their faith in your company?

Imagine the effects of an attack that exposes your client database, or your computers sending spam or phishing without your knowledge, or if anyone who buys from your website having their details stole by a banker Trojan…

*The bigger your company, the more risks you face…*

Some things that might not trouble a small company could be a real nightmare for larger organizations… Imagine if data on prototypes goes missing from a company that relies heavily on its patents.

The usual reaction is to think "it won't happen to me".

So let's take a look at some real examples:

*Only the most spectacular cases are reported. Have you ever stopped to wonder how many companies are infected every day? And whether they even realize? .*

November 2008: Three British hospitals -protected by McAfee- are infected by a virus dating back to 2005 and are brought to a standstill.

February 2009: 75% of French naval vessels are left without communication as systems are brought down by malware…

February 2009: The Houston Justice Department is paralyzed by the Conficker virus.

February 2009: IT systems of the British Ministry of Defense and the French and German armies are crippled for several days by a virus.

May 2009: The FBI and US Marshalls' communications are brought to a standstill due to a virus.

February 2009: The British Ministry of Defense aborts the landing of an aircraft as its Windows systems are affected by a 'global virus'.

May 2009: Three Spanish hospitals and 112 emergency services are paralyzed by a virus.

* Incidents reported in online media. References in the final chapter.

# 1. Common infection channels

It is not easy to get an idea of the vast amount of threats that we face every day. They come in all shapes and sizes, depending on what the creator is aiming for, how they are distributed, how they reach victims, etc.

It would take a long time to explain them all in detail. But we can simplify the classification by looking at the three most frequently used infection channels.

- Attacks or infections via email.
- Infections over the Internet.
- Infections from the individual PC of the user.

## Attacks or infections via email

Email is now an essential channel of communication for all companies. It is simple, efficient and quick. It is also however the principal channel for spam and phishing along with other types of malware, such as viruses, worms and Trojans.

Not only do employees waste time deleting these threats from mailboxes -with the consequent financial impact for the company-, but there is also the risk that users are not sufficiently aware of how to detect messages that could pose a threat.

It is therefore essential that there is protection at server level as well as at the level of the individual mail client to ensure the responsibility for threat prevention does not fall entirely on individual users.

## Infections over the Internet

Internet-borne threats are becoming increasingly common. One of the main risks is when malicious content is disguised in order to get users to download -knowingly or unknowingly- files that could be infected.

Typical cases include plugins to watch certain videos, apparently genuine program files, pdf documents hiding malware, etc. The risk becomes even greater given the proliferation of spoof websites. These fake Web pages are designed to trick users into thinking they have accessed the website on their own bank.

## Infections from the individual PC of the user

Another major risk comes from the security of users' individual computers. There are many possible factors that play a part in allowing a virus to infiltrate an organization:

- Basic company security policies have not been followed, such as strong passwords.
- Regular security patches for Microsoft Windows have not been applied.
- There is no security protection. The correct security product has not been installed or is out of date.
- Remote users are connecting from anywhere without adequate security policies or monitoring.
- Etc.

Any of the above cases could present a serious risk for the integrity of the company systems.

Moreover, it's not just a question of unwitting users simply downloading potentially dangerous files from the Internet, there are also risks in social networks and communities, with no controls over the links that users click on, the sites they visit or the services they subscribe to.

It has also become increasingly popular to share information through removable drives, such as USB memories, and these are also being used to distribute malware.

The three main malware infection vectors are:

- Email
- Internet
- Individual users' PCs

# 3. What the companies say…

Panda Security has published in 2009 its first International Security Barometer (available from *www.pandasecurity.com*).

The results of this study reveal that malware really is a problem for people in business today, and is a concern that affects their everyday work.

- Some 58% of companies have been infected at some time by malware.
- Malware infections have caused 30% of businesses in Europe to shut down their business activity, while 36% of SMBs suffered productivity losses and 15% lost important data.
- These infections occurred despite 93% of European SMEs having some type of security system installed.
- With respect to the type of protection installed, 27% of those with a security system have a free software solution.
- When companies were asked about the reason for not having a security system installed, a third of them answered that they were too expensive. Also, 8% replied that it was not necessary to have a security system installed.
- As for the role played by security in companies, 55% of companies in Europe consider security an important business asset. However, only 64% have someone dedicated exclusively to security.

If companies protect themselves and are aware of the problem… What is causing these security holes?

While traditional security solutions are critical as a first line of defense, companies of all sizes still face the risk of numerous security holes which are exploited by modern malware techniques. Today, malware silently infiltrates corporate networks for several reasons:

- There is no security strategy to cover the main infection vectors.
- Companies allow remote users or offices to connect to the main network with devices that could be infected.
- Incorrect management of remote offices.
- There is no serious training or information about the latest infection techniques or ruses used by hackers. This means that easily exploited technologies, such as file sharing, multimedia and instant messaging, pose a serious threat to network integrity.
- Too many computers are inadequately maintained, laptops of contractors or collaborators, sharing of files through USB drives, etc…

# 4. How to achieve true peace of mind against malware and hackers.

With the current malware and cyber-crime situation, the only way to achieve real peace of mind is to opt for protection from the best security service provider:

- Leading-edge technology capable of combating any potential problems.
- Solutions specifically designed to achieve maximum security for your business.
- Comprehensive technical support, so you can concentrate on your business, and leave the security of your company in the hands of experts.

# 5. Our technological vision

Panda Security has always been in the vanguard of security technology, providing groundbreaking anti-malware security solutions. As a visionary company, Panda's innovations have always been years ahead of competitors in the IT security sector.

Such was the case with our TruPrevent proactive detection technologies, which could detect malware even without prior identification. Panda first launched this innovation in 2005, yet similar technologies have only recently been implemented in competitors' products.

This is just one example, but if we look back over the company's 20-year history (http://www.pandasecurity.com/20anniversary), it is clear this has been a constant factor: reinvestment of 30% of turnover in R&D&i to ensure we always offer cutting-edge technologies.

Our current technological vision for protection is based principally on our system for automatically analyzing, classifying and disinfecting malware, which we call Collective Intelligence. It is also based on offering products under Nano architecture to reduce impact on local resources and delivering SaaS (Software-as-a-Service) solutions.

## Collective Intelligence

With the rapid increase in the amount of malware, which Panda Security identified as far back as 2006, we realized it would be practically impossible to protect our clients using the traditional model.

Antivirus laboratories normally follow a set procedure in dealing with malware: the samples are received (a new virus, worm, Trojan…), analyzed by a technician and a corresponding vaccine is created. This is then published across the Internet, so that users can update their local signature file and thus be protected against the new virus.

This model, which had functioned adequately in the past, became useless when laboratories went from receiving 100 samples a day to an average of 37,000.
This would require a whole army of technicians working around the clock to process all the new examples of malware received.

At Panda, aware of the situation, in 2006 we began to develop a series of technologies based on artificial intelligence -called Collective Intelligence-. These technologies can automatically analyze, classify and disinfect 99.5% of the new malware we receive every day at PandaLabs, keeping our clients protected almost in real time.

This leaves our laboratory technicians to process the remaining 0.5% of malware received. These cases, which tend to be more technologically complex, require more than Collective Intelligence to determine whether or not they are malware.

We first released these technologies in 2007 and currently all our solutions benefit from this vast knowledge base, offering protection ratios way above the market average.

## Nano architecture

Our philosophy of protecting clients with Nano architecture aims to minimize the impact of our solutions on system performance.

Inextricably linked to the concept of Collective Intelligence, we look to shift the operation of our solutions to the cloud. This emphasis on Web-based protection requires that only the most basic actions need to be carried out on our clients' infrastructure.

To explain this more clearly, we can first look at the traditional model. In order for a traditional security solution to be able to block a threat, it must first recognize it. This not only implies work in the laboratory, but also that this knowledge must somehow be available in the security solution installed.

Traditional security solutions operate with local signature files and sometimes a set of proactive detection technologies. This means that the entire malware database must be stored on the server or local computer. If there is a database of 30 million unique malware entries, this implies that all of this knowledge must be on the computer.

The problem is that every time, say, an email is received, the antivirus has to check the entire database, consuming resources and slowing down the computer. With solutions based on Nano architecture, this problem is resolved by shifting these operations to the cloud; there is no need for a local database and there is no excessive drain on local resources.

This translates into greater speed and greater availability of memory resources as certain processes are run somewhere other than the computer CPU.

Many Panda Security solutions already function in this way, and all the rest of the traditional solutions are migrating to this architecture model.

## SaaS Model

Finally, offering SaaS (Software-as-a-Service or Security-as-a-Service) security solutions is another competitive advantage. These Web-hosted solutions providing services from the cloud offer the additional advantage of considerable savings for clients on infrastructure, and greatly simplify security management, including the option to delegate it to third-parties (partner, reseller, consultant, etc.).

The technological vision of Panda Security is based on a proprietary system of automatic analysis, classification and disinfection of threats called Collective Intelligence. These technologies, along with Nano-based architecture and delivered through the SaaS model, ensure that Panda's corporate solutions are in the vanguard of security technology:

- Offering virtually real-time protection against the numerous threats in circulation.
- Enabling major cost savings in infrastructure.
- Greatly facilitating security management, eliminating the need for specialized personnel and reducing management time.
- Reducing the workload on local resources, which can then be dedicated to core tasks in the company.
- And finally, allowing solutions to be configured to the specific needs of the client.

# 6. Global Business Protection: Security solutions for your company

Today's malware is designed almost exclusively for financial gain, whereas hackers target small and large companies indiscriminately.

Panda Security's Global Business Protection solutions offer a personalized service to provide global security aimed at the specific needs of your company.

- Traditional solutions, managed services (hosted) or a combination of both.
- Security solutions for email, web traffic, endpoints and servers to guarantee maximum protection.
- Solutions that are simple to install and maintain with a minimal investment.

By complementing a solid, proven technological approach, with an additional protection strategy and the best support services, Global Business Protection offers your company peace of mind, so you can focus on what is really important for your company.

Email

# Panda ManagedEmailProtection

## Clean mail managed service

**Panda Managed Email Protection** is a managed security service that protects all your email traffic, ridding it of 99% of spam and 100% of malware. Panda Managed Email Protection allows your IT personnel to spend their time on other, more profitable initiatives for the company.

- Guarantees delivery of 100% virus-free email.
- Minimizes operating costs.
- Increases productivity.
- Optimizes mail management.
- Guarantees service continuity and effectiveness.
- Contingency measures to deal with mail infrastructure failure.
- Facilitates implementation of email content policies.

Web traffic

Panda
# GateDefender

## Web traffic protection

**Panda GateDefender** GateDefender is a family of appliances offering perimeter protection that adapts perfectly to the needs of your network, consolidating your first line of defense.

As Internet-borne threats account for 99 percent of threats to reach networks, corporate perimeter protection is a necessity not a luxury.

- Plug and Protect.
- No complexity.
- Minimizes operating costs.
- Increases employee productivity.
- Prevents loss of confidential information.

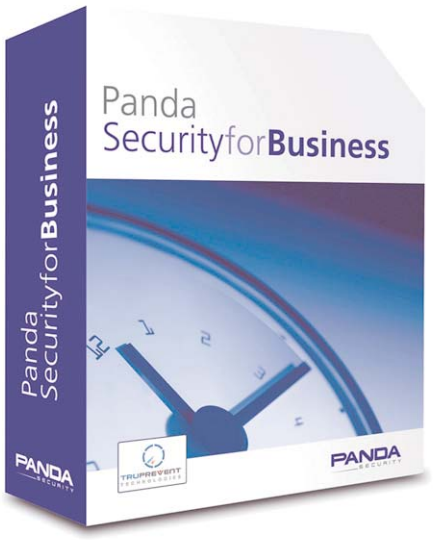
PCs and servers

# Panda
# Corporate Software Solutions

## Proactive, multilayer protection for your assets.

Panda Security Corporate Solutions are based on modular, flexible and scalable architecture.

- Maximum protection and minimum risk of infection.
- Complete, centralized monitoring of the entire network.
- Efficient security solution.
- Helps enforce corporate security policy and optimizes employee productivity .
- Simplifies risk management.
- Protects the company's critical assets.



## PCs and servers

# Panda ManagedOfficeProtection

## Focus on your core business and forget about your antivirus!.

**Panda Managed Office Protection** is a security solution for PCs and servers based on the concept of Software as a Service (SaaS). Software as a Service lets companies focus on their core business, freeing them from the management tasks and operating costs associated with traditional security solutions.

- Ensures maximum protection for PCs, laptops and servers.
- Minimizes operating costs.
- Minimizes resource consumption.
- Easy to use, easy to maintain.
- Improves risk management.
- Prevents identity theft.
- Reinforces regulatory compliance.

# 7. The best tech support services

Panda Security's technological vision and security solutions are based on a simple philosophy: always offering maximum protection to clients. This is why we strive to offer the best services, not just by researching and developing the most competitive technologies in combating malware, but through technical experts whose job it is to make our clients' lives as easy as possible.

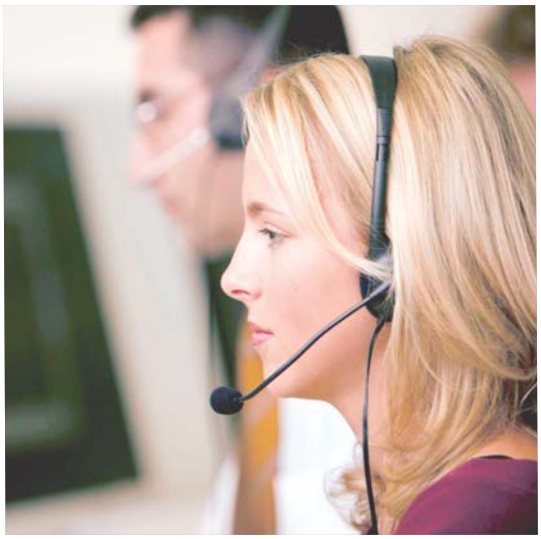
From pre-sales technicians, who will help you through the design and deployment of a security solution that adapts perfectly to your needs, to our post-sales support team, offering 24 x 7 help from 56 countries, we are always ready to deal with any questions or queries you might have.

Our technical support team operates locally from each country, providing support in your native language.

We are committed to offering a rapid intervention service for any of your needs, with a minimal impact on your business.

Similarly, we offer free migrations to solution updates, and exceptional conditions for switching to other solutions in our product portfolio.

We also offer training for your technicians, keeping them up-to-date on the malware situation as well as the most appropriate security policies for your company.



*Our security solutions are designed especially for your peace of mind, so you can focus on what is truly important to you, and leave your security in the hands of real experts.*

# 8. What our clients say…

## PCs and servers

*"After running trials of several security products (Norton, Avast, Kaspersky and Panda Security), Panda proved to be the solution that best met our expectations, particularly through its low resource consumption, centralized management and easy deployment".*

Jean-Yves Andreoletti
Director of systems and network integration platforms / PMR Validation
EADS Defence & Security
France

*"One of the main benefits of Panda Managed Office Protection is cost savings, as well as the peace of mind derived from knowing we are protected against all types of threats".*

José María Domínguez
IT Department at La Provincia Emaus
Escuelas Pias Provincia Emaus
Spain

*"Since 1995, when we first implemented Panda in Grupo Amper, we have witnessed year after year just how shrewd that initial decision was".*

Manuel Fernández
IT Director
Grupo Amper
Spain

## Web traffic

*"Panda GateDefender can block threats in the perimeter and detect malware in inbound and outbound traffic".*

Mr. Ong
Corporate Network Manager
Sin Chew Daily
Malaysia

*"Thanks to GateDefender's Web filtering capability, we've been able to increase our employee productivity".*

Mike Van Fleet
IT Administrator
Matchframe Video
USA

## Email

*"Panda Managed Email Protection provided our clients with a critical solution for spam management, freeing them from routine tasks such as mail filtering and removal. After just 7 days using it they rated it 10 out of 10".*

Joan Vila
Manager
Ordismatic (Channel partner)
Spain

# 8. References


- *http://pandalabs.pandasecurity.com*
- *http://www.fayerwayer.com/2008/11/impresentable-hospitales-de-londres-se-contagian-con-virus-informatico/*
- *http://www.theregister.co.uk/2009/02/02/nhs_worm_infection_aftermath/*
- *http://www.theregister.co.uk/2009/03/09/scot_hostpitals_malware_infection/*
- *http://www.theregister.co.uk/2009/02/09/houston_malware_infection/*
- *http://www.madboxpc.com/conficker-el-virus-que-tiene-revolucionado-a-redmond/*
- *http://www.idg.es/pcworld/Conficker-ha-creado-la-mayor-red-bot-del-mundo/doc79409-Seguridad.htm*
- *http://www.eweek.com/c/a/Security/Conficker-Attacks-700-University-of-Utah-PCs-835179/?kc=rss*
- *http://ecodiario.eleconomista.es/noticias/noticias/878925/11/08/Algunos-ordenadores-del-Pentagono-estan-infectadas-por-un-virus.html*
- *http://www.kriptopolis.org/cazas-franceses-en-tierra-por-virus-conficker*
- *http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html*
- *http://www.kriptopolis.org/virus-colapsa-armada-britanica*
- *http://www.itwire.com/index.php?option=com_content&task=view&id=22716&Itemid=53*
- *http://www.elpais.com/articulo/madrid/virus/cuela/ordenadores/Sanidad/elpepiespmad/20090512elpmad_1/Tes*
- *http://www.theregister.co.uk/2009/05/22/fbi_mystery_viral_infection/*
- *http://www.elmundo.es/elmundo/2009/05/22/navegante/1242982288.html*
- *http://www.cronica.com.mx/nota.php?idc=154655*
- *http://www.elconfidencialdigital.com/Articulo.aspx?IdObjeto=16025*
- *http://terranoticias.terra.es/nacional/articulo/ejercito-virus-ataco-centenares-ordenadores-3074699.htm*
- *http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews?noticia=9702*
- *http://www.pandasecurity.com/spain/homeusers/security-info/tools/reports/*

**PANDA SECURITY**

**Panda SPAIN**
Ronda de Poniente, 17
28760. Tres Cantos. Madrid. SPAIN
Phone: +34 91 806 37 00

**Panda USA**
230 N. Maryland, Suite 303
P.O. Box10578. Glendale, CA 91209 - USA
Phone: +1 (818) 5436 901

**www.pandasecurity.com**