



# PANDA CLOUD PROTECTION

*Simply... Evolution*



A new technological paradigm sets  
the trend for the security industry:  
**SECURITY FROM THE CLOUD**



## Abstract

---

In its report about emerging technologies and maturity cycles, Gartner identifies Cloud Computing as one of the 1,650 technologies that will define future trends. As the market is still maturing, there is considerable confusion concerning definitions: Cloud Computing versus SaaS (Software-as-a-Service) versus Cloud Security versus Security from the Cloud.

All of them share a similar cloud-based framework, and represent the market segments set to expand most over the coming years, with a consequent decline in traditional applications based on local infrastructure. IDC predicts a market increase of 300% by 2013 and expects that the players who move towards this philosophy will be those that survive.

Simply put, cost optimization is the main reason clients opt for IT services hosted in the cloud. Consequently it is one of the technologies expected to mature most rapidly and to attract many new players into the arena.

In April 2009, Panda Security, The Cloud Security Company, which throughout its 20 year history has reinvested some 30% of revenue into R&D&i, became the first company to launch a cloud-based antivirus. Without impacting local computer resources, this protection offers maximum detection capacity by leveraging its proprietary Collective Intelligence knowledge base.



## Contents

---

1. Defining cloud concepts
2. Cloud Security: Emerging technologies and analysts' predictions
3. Security from the cloud: Panda's technological vision



## Defining cloud concepts

---

The cloud is hot. The evolution of Internet technologies has made the migration of applications from local PCs or servers to other intangible hosts a reality. This, in turn, opens the way for a new business model catering to markets that demand increasingly agile, fast and scalable solutions.

As a new, rapidly-rising market, there is much confusion over concepts which themselves are continuing to be defined as new technologies evolve and mature. The most obvious predecessor is the SaaS model (Software-as-a-Service or Security-as-a-Service, depending on the specific market segment).

Bruce Schneier <sup>(1)</sup> says of **Cloud Computing** that the concept is nothing new in that, *"It's the modern version of the timesharing model from the 1960s, which was eventually killed by the rise of the personal computer"*. Adding that, *"It's what Hotmail and Gmail have been doing all these years, and it's social networking sites, remote backup companies, and remote email filtering companies such as MessageLabs. Any IT outsourcing --network infrastructure, security monitoring, remote hosting-- is a form of cloud computing."*

In 2009 there has been a convergence of definitions regarding the cloud computing concept and its derivatives.

According to cloudcomputing.org <sup>(2)</sup>, **"Cloud Computing** is a nebulous term covering an array of technologies and services including: grid computing, utility computing, Software as a Service (SaaS), storage in the cloud and

*virtualization. There is no shortage of buzzwords and definitions differ depending on who you talk to."*

Leading analysts have also sought to define the term, offering varying explanations which, although they don't coincide completely, have much in common.

IDC <sup>(3)</sup> defines **Cloud Computing** as *"Consumer and business products, services and solutions delivered and consumed in real-time over the Internet."* It also defines eight attributes that a solution should have in order to be cataloged under cloud computing. These are:

- **Shared, standard service:** Built for a market (public), not a single customer
- **Solution-packaged:** A 'turnkey' offering, integrates required resources.
- **Self-service:** Admin, provisioning, may require some 'on-boarding' support .
- **Elastic scaling:** Dynamic and fine-grained.
- **Use-based pricing.**
- **Accessible via the Internet / IP:** Ubiquitous (authorized) network access.
- **-Standard UI technologies:** Browsers, RIA clients and underlying technologies.
- **-Published service interface/API.**



IDC also describes two cloud deployment models, **public and private**. The eight key attributes mentioned above correspond to public cloud models; services such as Amazon, Google or Salesforce. Private models, by definition, do not have the same scope, yet still offer significant improvements with respect to traditional private deployment models.

**Forrester** <sup>(4)</sup> defines **Cloud Computing** "standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way."

This definition is similar to that offered by Gartner <sup>(5)</sup>, who talk of "a style of computing where massively scalable IT-related capabilities are provided 'as a service' using Internet technologies to multiple external customers."

### Difference between Cloud Computing and SaaS

Some writers coincide in that Cloud Computing as a term has evolved from SaaS (Software-as-a-Service), while others classify SaaS as part of the process of delivering services from the cloud.

According to [www.cloudcomputing.org.es](http://www.cloudcomputing.org.es) <sup>(6)</sup> regardless of the difficulty involved in defining the concept of cloud computing, there is general consensus regarding its classification by the type of services of technologies:

- **Software as a Service (SaaS):** A software distribution model where a company delivers maintenance, support and operation of the service during the time for which the client has contracted it. Clients use the system hosted by this company, which will store clients' information on its system and provide the resources necessary to leverage this information. Examples: Salesforce, Basecamp.
- **Infrastructure as a Service (IaaS):** The delivery of computer infrastructure as a service, normally by means of a virtualization platform. Rather than buying servers, data center space or network equipment, clients buy these resources from an external service provider. The fundamental difference with virtual hosting is that the provisioning of the services is entirely Web-based. Examples: Amazon Web Services EC2 and GoGrid.

**Cloud Services**

Consumer and Business products, services and solutions delivered and consumed in real-time over the Internet

**Key Attributes**

- ☐ Shared, standard service – built for a market (public), not a single customer
- ☐ Solution-packaged – a "turnkey" offering, integrates required resources
- ☐ Self-service – admin, provisioning; may require some "on-boarding" support
- ☐ Elastic scaling – dynamic and fine-grained
- ☐ Use-based pricing – supported by service metering
- ☐ Accessible via the Internet – ubiquitous (authorized) network access
- ☐ Standard UI technologies – browsers, RIA clients and underlying technologies
- ☐ Published service interface/API – web services, other common Internet APIs

**Deployment Models**

<b>Public</b> - open to a largely unrestricted universe of potential users; designed for a market, not a single enterprise
<b>Private</b> - designed for, and access restricted to, a single enterprise (or extended enterprise); an internal shared resource, not a commercial offering; IT Org is the "vendor" of the shared/std service to its users

Source: IDC, 2009



- **Platform as a Service (PaaS):** Although often presented as an evolution of SaaS, it is more of a model offering all that is necessary to support lifecycle -building and set up- of applications and services completely available across the Internet. Another important feature is that there are no software downloads to install on developers computers. PaaS offers multiple services, but all provisioned as a global solution on the Web.
- Don't generalize on cloud security: The security considerations for every cloud service are different.

Therefore in this case, when we talk of Cloud Security, we are not talking about local security for users or security from the cloud, but security for the cloud.

### Cloud Security

So that is Cloud Computing, but what about Cloud Security? Microsoft defines Cloud Security as protecting the cloud. The article Security by Default (7), describes the five tenets upon which Microsoft has designed the security of its products:

- Discuss risk with customers. Figuring out where the responsibilities lie with respect to a customer's data is an important conversation.
- Pay attention to compliance.
- Better standards needed. The large cloud providers need to work together to standardize across their platforms.
- Privacy and security are not so different.





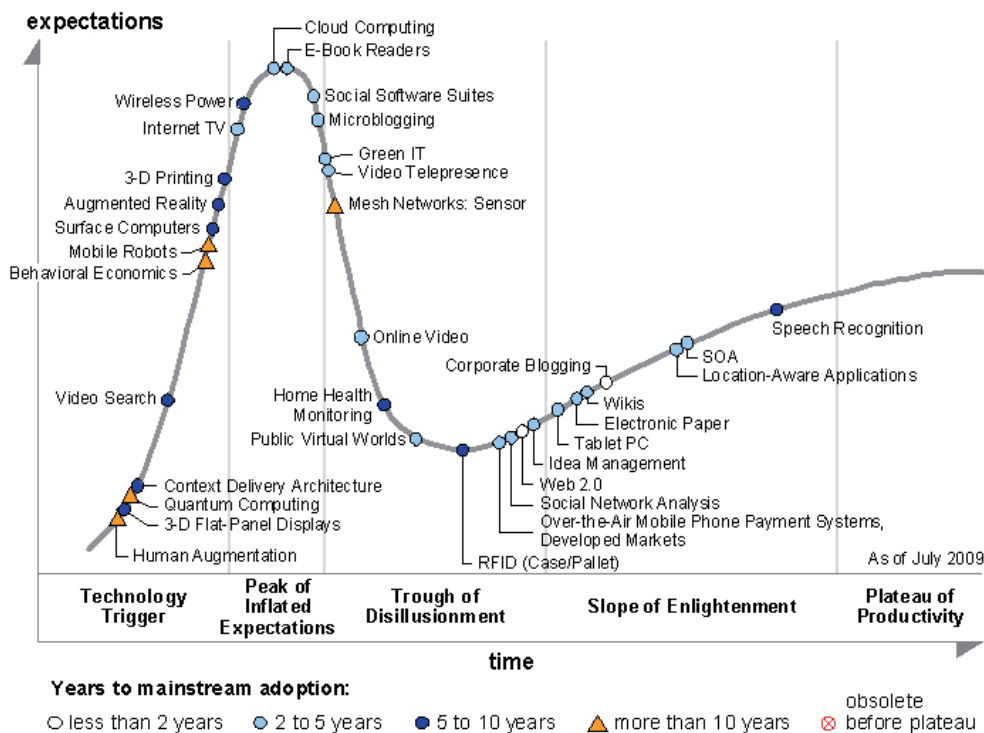
## Cloud Security: Emerging technologies and analysts predictions

The pace at which new technologies emerge to address new market demands has accelerated in recent years. The technological panorama and market needs combined with trends defined by economic cycles and the maturity flow has increased the pace with which new solutions emerge, are adopted and mature.

Cloud Computing has been identified by Gartner as one of the ten strategic technologies that will really take off in 2010. According to this major analyst, use of resources from the cloud does not eliminate business IT costs, but it does reduce them <sup>(8)</sup>.

In its report about emerging technologies and maturity cycles, Gartner <sup>(9)</sup> identifies Cloud Computing as one of the 1,650 technologies that will define future trends. It is clear that cost optimization is the main driving factor behind clients opting for IT services hosted in the cloud. That's why it is one of the technologies expected to mature most rapidly and to attract many new players into the arena.

Gartner believes that the technologies that will undergo most transformation and that will set market trends within the next five years will be Web 2.0, cloud computing, Internet TV, virtual worlds and service-oriented architecture (SOA).





# PANDA CLOUD PROTECTION

Simply... *Evolution*



Predictions suggest that Cloud Computing, and all that this concept encompasses, will not just be one of the emerging technologies, but will also experience considerable market growth. Therefore those players already active in the segment will be those that grow most. There will be a clear migration in the industry towards the Cloud Computing and SaaS models.

Market take-up however will be gradual. IDC <sup>(10)</sup> expects growth of between 40 and 42% for the SaaS segment in 2010.

Gartner <sup>(11)</sup> forecasts that security delivered as cloud-based services will have traveled in many

sectors by 2013. *"Security applications delivered as cloud-based services will have a dramatic impact on the industry... Enterprises that use cloud-based security services to reduce the cost of security controls and to address the new security challenges that cloud-based computing will bring are most likely to prosper,"* predicts Gartner.



## *Security from the cloud: Panda's technological vision*

---

Another, very different concept, is Security from the Cloud, which relates to Cloud Computing in the sense that there are hosted services delivered from the cloud, in line with the SaaS model, but with a philosophy based on a very specific strategic 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 two years or more ahead of competitors in the IT security sector.

Such was the case with the 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](#), it is clear that 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 the impact on local resources and delivering SaaS (Software-as-a-Service) solutions.

### *Collective Intelligence*

---

With the rapid increase in the amount of malware in circulation, 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 50,000.

This would require a whole army of technicians working against the clock to process all the new examples of malware received.

At Panda, aware of the situation, we began to develop a series of technologies based on artificial intelligence -called [Collective Intelligence](#)- in 2006. 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 the 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 that this entails is that every time an email is received, for example, the antivirus checks the information against 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.).

More information about Panda [Cloud Protection](http://cloudprotection.pandasecurity.com) is available at:  
<http://cloudprotection.pandasecurity.com>



## References

---

- (1) [http://www.schneier.com/blog/archives/2009/06/cloud\\_computing.html](http://www.schneier.com/blog/archives/2009/06/cloud_computing.html)
- (2) [www.cloudsecurity.org](http://www.cloudsecurity.org)
- (3) <http://blogs.idc.com/ie/?p=422>
- (4) [http://blogs.forrester.com/it\\_infrastructure/cloud-computing/](http://blogs.forrester.com/it_infrastructure/cloud-computing/)
- (5) Research Paper: “**Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones**”
- (6) <http://cloud-computing.org.es/?tag=saas>
- (7) <http://www.securitybydefault.com/2009/09/5-lecciones-sobre-cloud-security-by.html>
- (8) <http://www.itpro.co.uk/616594/cloud-computing-tops-gartner-tech-ranking>
- (9) Gartner’s 2009 Hype Cycle Special Report Evaluates Maturity of 1.650 Technologies.  
<http://www.gartner.com/it/page.jsp?id=1124212>
- (10) <http://itmanagement.earthweb.com/netsys/article.php/3812466/IDC-SaaS-Growth-Coming.htm>
- (11) <http://www.gartner.com/it/page.jsp?id=722307>



## 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](http://www.pandasecurity.com)

© Panda Security 2009. All rights reserved. 1109-WP-CPI-I-1

**PANDA** | 20<sup>th</sup> Anniversary  
SECURITY 1990-2010

[www.pandasecurity.com](http://www.pandasecurity.com)