

## Making Clouds secure

The concept of Cloud Computing — what just about every IT community is dreaming about these days — has a multitude of indisputable advantages over more traditional modes of software distribution and usage. But Cloud Computing has a long way to go before it takes over the market — not in terms of technology, but in terms of how it is perceived by potential clients. For the majority of them, Cloud Computing seems like an interesting — but not very secure — idea.

If you were to review the evolution of the concept (which, incidentally, is considerably older than it might seem), you would see the close connections between Cloud Computing and information security. As Enomaly founder and Chief Technologist Reuven Cohen has rightly noted, the Cloud Computing concept was first mastered by cyber criminals who had created rogue networks as early as ten years ago. Not much time passed before people started using Cloud Computing for legitimate purposes, and the technology is just now beginning to come into its own.

### What is a “Cloud”?

Let’s take a look at the formal definition of the concept before we tackle the modern aspects of security and Cloud Computing. There is still no common or generally recognized definition of “Cloud Computing” in the IT industry, and most experts, analysts, and users have their own understanding of the term.

In order to come to a more precise definition, we first need to move from the general to the specific. In general, Cloud Computing is a concept whereby a number of different computing resources (applications, platforms or infrastructures) are made available to users via the Internet. While this definition seems to capture the essence of Cloud Computing, in practice it is much too abstract and broad. If you wanted to, you could include practically everything even vaguely related to the Internet in that definition. The definition needs to be made more specific, and in order to do so, we will first take a look at the position of the scientific and expert community.

The work “Above the Clouds,” published by the RAD Lab at UC Berkeley, has identified the three most common features of Cloud Computing:

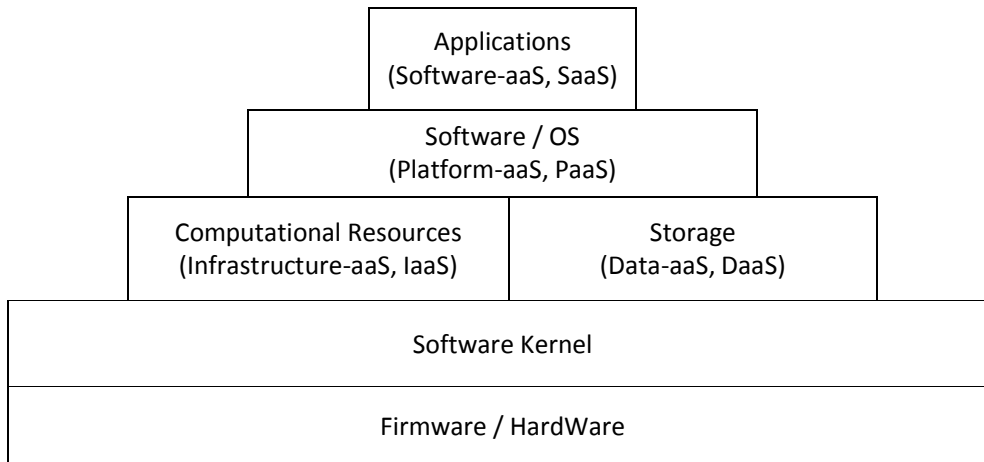
- The illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning.
- The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.
- The ability to pay for use of computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

The specifications for building a Cloud platform, such as virtualization, global distribution or scale, are not so much features of Cloud Computing, but merely help put this paradigm into practice. In particular, the use of virtualization technologies helps achieve the “illusion of infinite computing resources” mentioned above.

The main features of any Cloud service are the kinds of resources it offers users via the Internet. Depending on these resources, all services can be divided into a number of different categories (see

Figure 1). Each of these carries the suffix \*aaS, where the asterisk represents the letter S, P, I or D, and the abbreviation “aaS” means “as a service.”

**Figure 1. The ontology of Cloud services**



Essentially, Cloud Computing makes resources available through the Internet and has three fundamental features, as noted above. The types of resources made available may be software (SaaS), a platform (PaaS), an infrastructure (IaaS), or storage (DaaS).

### **Defining security problems on Cloud servers**

Practically every expert in the industry approaches Cloud Computing with their own interpretation of the concept. As a result, after examining numerous published works on the subject, one might get the impression that there is really no standardization at all. Questions regarding the security of Skype — a typical consumer Cloud service — get jumbled up with the business aspects of installing SaaS, while Microsoft Live Mesh is already becoming a headache for companies that never even planned on using it in the first place.

That’s why it would make complete sense to deconstruct the problem of Cloud Computing security into several high-level categories. In the end, all aspects of Cloud service security can be put into one of four main categories:

- Security issues with consumer Cloud and Web 2.0 services. As a rule, these problems don’t have as much to do with security as they do with privacy and the protection of personal data. Similar problems are common among most major Internet service providers — just think about all of the accusations against Google or Microsoft that come up from time to time with regard to tracking user activity.
- Corporate-level security issues resulting from the popularity of consumer Cloud services. This becomes a problem when employees get together on sites like Facebook and gossip about corporate secrets.
- Cloud computing security issues related to corporate usage, and the use of SaaS in particular.
- Issues concerning the use of the Cloud Computing concept in information security solutions.

In order to avoid any confusion or contradictions, we will address only the third category from the list above, since this is the most serious issue in terms of corporate information system security. Consumer Cloud services have already won over Internet users, and there are really no security problems that

could break that trend. The hottest topic right now is just how quickly Cloud Computing can become a corporate platform suitable not only for SMEs, but for large international organizations as well.

### **Deconstructing corporate Cloud services**

IDC analysts who spoke at the IDC Cloud Computing Forum in February 2009 stated that information security is the top concern among companies interested in using Cloud Computing. According to IDC, 75% of IT managers are concerned about Cloud service security.

In order to understand why, we need to continue our deconstruction of the security issue. For corporations using Cloud services, all security issues can be further divided into three main categories:

- The security of a platform that is located on the premises of the service provider;
- The security of workstations (endpoints) that are located directly on the client's premises;
- And finally, the security of data that are transferred from endpoints to the platform.

The last point concerning the security of transferred data is *de facto* already resolved using data encryption technologies, secure connections, and VPN. Practically all modern Cloud services support these mechanisms, and transferring data from endpoints to a platform can now be seen as a fully secure process.

### **The platform: trust and functionality problems**

Clearly, security issues related to service platform functionality are the biggest headache for IT managers today. For many, figuring out how to ensure the security of something that cannot be directly controlled is not a very straightforward process. The platform of a typical Cloud service is not simply located on the premises of a third-party organization, but often at an unknown data center in an unknown country.

In other words, Cloud Computing's basic security problem comes down to issues of client trust (and verifying trust) in service providers and is a continuation of the same issues that arise with any type of outsourcing: company specialists and management are simply not accustomed to outsourcing something as crucial as the security of business data. However, one can be certain that this problem will be resolved since other forms of outsourcing for the same IT processes and resources no longer give rise to any fundamental concerns.

What is this certainty based on? First of all, it is considerably easier for Cloud service providers to ensure the security of the data centers where available resources are located. This is due to the scale effect: since the service provider is offering services to a relatively large number of clients, it will provide security for each of them at the same time and, as a result, can use more complex and effective types of protection. Of course, companies like Google or Microsoft have more resources to ensure platform security than a small contracting firm or even a large corporation with its own data center.

Second, using Cloud services between client and provider organizations is always based on their respective Cloud services quality agreements (SLA), which clearly set out the provider's responsibility for various information security issues. Third, the provider's business directly depends on its reputation, which is why it will strive to ensure information security at the highest possible level.

In addition to verification and trust issues, Cloud platform clients also worry about the full functionality of information security. While most in-house systems already support this feature (thanks to many years of evolution), the situation is much more complicated when it comes to Cloud services.

Gartner's brochure "Assessing the Security Risks of Cloud Computing" examines seven of the most relevant Cloud service security problems, most of which are directly related to the idiosyncrasies of the way Cloud systems function. In particular, Gartner recommends looking at Cloud system functions from the viewpoint of access rights distribution, data recovery capabilities, investigative support and auditing.

Are there any conceptual restrictions that might make it impossible to put these things into practice? The answer is definitely no: everything that can be done within an organization can technically be executed within a "Cloud." Information security problems essentially depend on the design of specific Cloud products and services.

When it comes to Cloud Computing platform security, we should address yet another important problem with regard to laws and regulations. Difficulties arise because a separation of data takes place between the client and the service provider within the Cloud Computing environment, and that separation often complicates the process of ensuring compliance with various statutory acts and standards. While this is a serious problem, it will no doubt be resolved sooner or later. On the one hand, as Cloud Computing becomes more widespread, the technologies used to ensure compliance with legal requirements will be improved. On the other hand, legislators will have to consider the technical peculiarities of the Cloud Computing environment in new versions of regulatory documents.

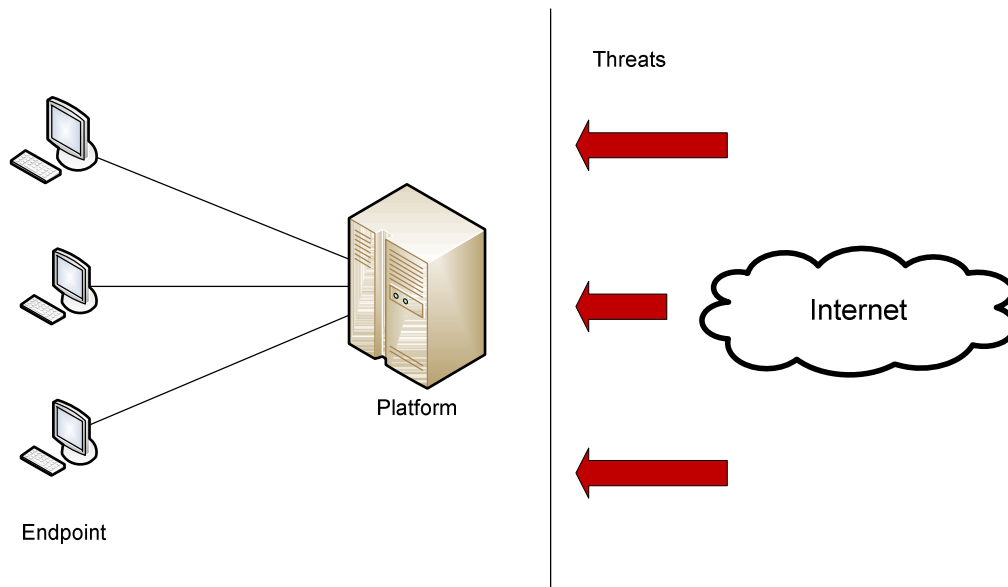
In summary, the concerns about information security as it pertains to the platform component of the Cloud Computing environment lead us to the conclusion that while all of the problems that potential clients have identified do in fact exist today, they will be successfully resolved. There simply are no conceptual restrictions in Cloud Computing.

### **Endpoint: difficulties remain... and are getting worse**

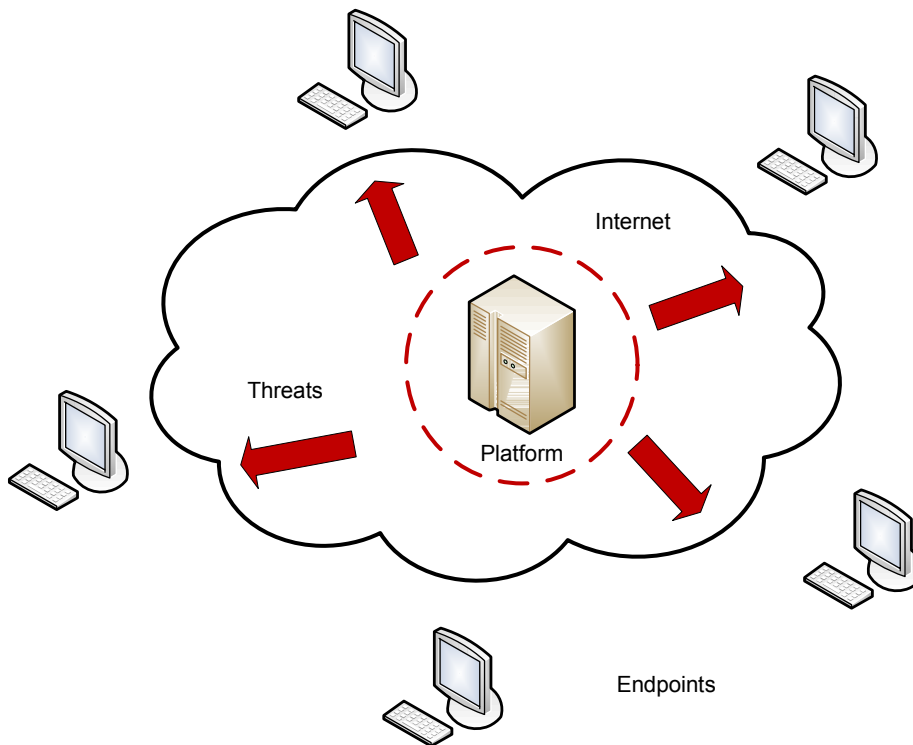
In the theoretically ideal "Cloud World," Cloud Computing security takes place on the platform level and through communication with edge devices, since data is not stored on the devices themselves. This model is still too premature to be put into practice, and the data that reaches the platform is *de facto* created, processed and stored on the endpoint level.

It turns out that there will always be security problems with edge devices in a Cloud environment. In fact there is another much stronger theory that these problems are actually becoming worse. In order to understand why this is happening, let us take a look at some conceptual diagrams of traditional in-house IT models compared to the Cloud Computing environment (Figures 2 and 3).

### **Figure 2. Security threats for traditional models for running software**



**Figure 3. Security threats in a corporate Cloud environment**



In each case, most of the threats are clearly coming from the global network and entering the client's corporate infrastructure. In the in-house system, the main blow is dealt to the platform, in contrast to the Cloud environment, in which the more or less unprotected endpoints suffer. External attackers find it useless to target protected provider Clouds since, as we noted above, the protection level of global Cloud platforms like Google and Microsoft, due to the numerous capabilities, professional expertise and unlimited resources, will be significantly higher than the data protection supplied by any individual corporate IT system. As a result, cyber criminals end up attacking edge devices. The very concept of

Cloud Computing, which presumes access to a platform from wherever and whenever it is convenient to do so, also increases the probability of this type of scenario.

On the other hand, having observed an increase in a variety of attacks on endpoint computers, corporate information security services have had to resort to focusing their efforts on protecting edge devices. It is this task in particular that, it would seem, will become a critical problem for corporate information security.

DeviceLock — a developer of software protection systems against data leakages via ports and endpoint computer peripherals — believes this is a crucial trend. Systems like those designed by DeviceLock become especially valuable in the Cloud Computing environment, since they help reduce the risk of corporate data leakages via endpoints, which are the focus of corporate information security service efforts at companies where Cloud services are used.

#### **Instead of a conclusion...**

"I think a lot of security objections to the Cloud are emotional in nature, it's reflexive," said Joseph Tobolski, director for Cloud Computing at Accenture. Shumacher Group CEO Doug Menafee is also familiar with the emotional aspects: "My IT department came to me with a list of 100 security requirements and I thought, Wait a minute, we don't even have most of that in our own data center".

Deciding to use Cloud Computing is just like getting behind the wheel of a car for the first time. On the one hand, many of your colleagues may have already made the leap, but on the other hand, getting onto a busy highway for the first time can be scary — especially when you keep seeing stories of horrible accidents on the news. However, it's not much more dangerous to drive than it is to drink coffee on a moving train or to wait at a bus stop.

For the most part, the situation with Cloud Computing is the same as with classic software usage models. The Cloud environment requires attention to information security, but we're totally confident that there would be solutions to the problems that currently exist. There are specific nuances in Cloud security, primarily related to a blend of priorities — from perimeter protection to edge device protection. But if data security developers help companies resolve this problem, the future for "Clouds" will be sunny indeed.

**By Alexei Lesnykh, [www.DeviceLock.com](http://www.DeviceLock.com)**