

Is Cloud Computing a gateway drug?

What is the cloud?

The National Institute of Standards and Technology (NIST) define five characteristics of “the Cloud”:

1. On demand/self service
2. Ubiquitous network access
3. Location independent
4. Rapid elasticity
5. Pay-for-use.

This is a very broad description and covers a lot of ground such as ‘Software as a service’, ‘Platform as a service’, ‘infrastructure as a service’ and ‘anything else you can imagine as a service’.

The one characteristic that is not intrinsic to the cloud ‘x as a services’ is security. There are a number of barriers, contract tie-in to existing suppliers being one of them, and the opaque approach of vendors to security being another. A maturity cycle is clearly discernable – non-mission critical activity, through quality of service (and more mission-centric) activities, through additional capacity to offer greater business agility, and, at the ultimate stage ubiquitous.

“All data is not created equal”

This picture is not uniform – in the US, adoption is faster than in the UK; while the financial sector is yet to embrace The Cloud wholeheartedly, parts of UK HMG and other European governments are. Examples are Denmark and Lithuania. In January 2011, ENISA released a report stating that the cloud was unsuitable for sensitive data. ENISA says that so-called private clouds are currently the most viable option for public sector bodies "since they offer the highest level of governance, control and visibility". As a program manager in the Army's Office of the Chief Marketing Officer, recently commented on overcoming the security concerns of his



department by stating: “All data is not created equal...(and) all the challenges we've faced have been self-imposed. We're not putting nuclear launch codes on Salesforce.com, we're putting the street addresses of 17-year-olds.”

But once the capability is there, how will its application be policed? Many security experts believe that the notion of putting more data and more applications on the Internet via the cloud model could present vast new opportunities for criminal activity through identity theft and misappropriating intellectual property, hacking, and other forms of malicious activities. The drivers are very much around cost efficiency, scalability and ease of use – but does this outweigh the risks? Moreover, given the speed with which national technical agencies are able to issue guidelines, can they really be expected to offer timely parameters for use in government and supporting area ?

Is Cloud Computing a gateway drug?



Simon Walker and Javad Malik

The key issue with cloud security is that the user organisation is not responsible for anything below the level of their own data. Senior management need control to accept accountability – but how to balance both sides of the equation if audit is not possible. Some vendors put the responsibility for security on the user – but all this does is sidestep the question

Key challenges

- Bringing up dormant machines – out-of-date patch levels mean controls are weak
- Compromised machine allows access across the hypervisor – thereby negating any controls
- Segmentation on the same hypervisor – differing trust levels. Implications for, for example, PCI scope (where does it end?)
- Fundamental issue of multi-tenancy – who are your neighbours? Penetration of the perimeter, such as it is, is essentially easy.

Addressing these involves answering some questions, the most basic of these being how to maintain control.

Given that firewalls are shared, these will be configured for the lowest common denominator.

Similar considerations will apply to network controls, not to mention the controls over hypervisors. There is the fundamental question of the ease of breaking out of virtual machines.

- Can your virtual machines, or those of you “neighbours”, be stolen?
- Can the segmentation, or indeed any other technical or management characteristics, be audited?
- How will data be transferred or destroyed on termination?
- How is encryption handled?
- Where is your data, and does this have any regulatory implications?

Cloud service providers have an interest in limiting the variation of hardware – introducing too many bespoke, tailored platforms has serious cost implications.

A change of perspective

These factors mean that, from a security perspective, there is a burning need to focus on the logical layer. This means a number of things:

1. Treating the network as public – you can’t manage your “neighbours”, so this is something you must accept.
2. Hardening virtual machines. The object here is to draw in the scope of the perimeter from the potentially flakier limits of the hypervisor to that of the virtual machine itself.
3. Consider what additional products you may need. For example data encryption solutions which holds the keys outside the cloud or software which builds security into the virtual machine.

But the most crucial factor is to re-orientate your thinking about security – thinking inside out from the virtual machine to the perimeter rather than outside in securing the perimeter, then considering what lies on the “light” side will help you.



1 Cornhill, London EC3V 3ND
+44 (0) 20 7125 0364
info@quantainia.com
www.quantainia.com

Innovation Quality Excellence