

Who owns security in the Cloud?

by Jim Reavis, founder and executive director, Cloud Security Alliance and
Dave Asprey, vice president of Cloud Security, Trend Micro

In the case of public Cloud, enterprise security perimeter simply doesn't exist. One option is to extend the perimeter into the Cloud. This allows using existing management tools, but the link with the Cloud must be closely monitored. The second option is to extend the Cloud into the enterprise perimeter by installing security servers within the enterprise, which are managed by Managed Security Service Providers (MSSPs). They must be highly trusted, since they are given full access to the enterprise internal systems. In both cases the enterprise must still protect its data by all the available security tools. IT managers should demand visibility of data access logs and seek to establish better access control. It is important to use encryption for data 'at rest' as well as 'in motion', and negotiate strict SLAs with standard compliance.



Jim Reavis is founder and executive director of the Cloud security Alliance. He is also the president of Reavis Consulting Group, LLC, where he advises security companies, large enterprises and other organisations on the implications of new trends such as Cloud. He is also a partner with the MetroSITE Group. Previously, he has been a board member and an executive director of the ISSA, a global not-for-profit association of information security professionals. He was also a co-founder of the Alliance for Enterprise Security Risk Management, a partnership between the ISSA, ISACA and ASIS that was formed to address enterprise risk issues associated with the convergence of logical and traditional security.

Jim Reavis is widely quoted in the press and has worked with hundreds of corporations on their information security strategy and technology roadmap. His innovative thinking about emerging security trends has been published and presented widely throughout the industry. He was recently named as one of the top ten Cloud computing leaders by SearchCloudComputing.com. He has a background in networking technologies, marketing, product management and systems integration. He received a BA in Business Administration/Computer Science from Western Washington University in 1987 and serves on WWU's alumni board.



Dave Asprey is vice president of Cloud security in Trend Micro. He is responsible for thought leadership and technology evangelism for Trend Micro's Cloud computing and virtualization businesses. He created and launched two early Cloud computing service offerings. His writing on the Cloud has been published by the New York Times, GigaOm, Fortune and CNNmoney. PriceWaterhouseCoopers published his book-length piece on systems management. He co-chairs the Cloud security Alliance Virtualization Working Group and sits on RSA China's Program Committee. He is a sought-after speaker and panel moderator who has presented at more than 100 Cloud, virtualization, and security conferences globally.

Mr Asprey joined Trend Micro after spending most of 2010 as an Entrepreneur in Residence at venture capital firm Trinity Ventures, co-founding a Cloud startup and selling a web-based virtual desktop startup. He was previously VP of Technology and VP of Business & Corporate Development at Blue Coat Systems. He spent two years as VP Technology & Marketing at Cloud networking vendor Zeus Technologies. Earlier, he ran strategic planning for Citrix's Virtualization Business Unit and began his career in the Cloud as a co-founder of the professional services group at Exodus Communications, then as senior director of product management at Speedera, now part of Akamai. He also ran the Web & Internet Systems Engineering Program for UC Santa Cruz for five years.

I. Who owns security in the Cloud?

Cloud computing is the technology buzzword of the moment. The provision of on-demand IT software and infrastructure services via the Internet can provide IT teams with unparalleled benefits in efficiencies, cost savings and scalability. However, with these game-changing benefits come a whole new set of challenges which invalidate most traditional approaches to security. While the Cloud offers a vision of simplified, pay-per-use IT, in which much of the heavy lifting is outsourced, it also introduces numerous new compliance headaches

and potential areas of data security risk. Here we attempt to address these issues in the context of the Infrastructure as a Service (IaaS) - that which allows IT managers to rent networking, storage, servers and other operational elements. It also offers enterprises greater autonomy to put more security controls in place than in other models, such as SaaS.

II. Why the Cloud?

On the public Cloud side it comes down to scaling and the ability to use OPEX (Operating Expense) instead of CAPEX (Capital Expense). On-demand

provision of resources also allows firms to scale dynamically, vastly improving business agility. On the private Cloud front, it is all about increased flexibility and responsiveness to internal customers' needs. With these kinds of benefits it's unsurprising to see such interest in the new computing paradigm. A poll from security body ISACA (March 2010) found that a third of European organisations are already using Cloud computing systems, while global consultancy Accenture revealed (July 2010) that half of its clients are running some mission-critical applications (apps) in the Cloud.

III. Perimeter security isn't dead - two approaches to securing the Cloud

Much has been made of the fact that when it comes to the public Cloud model, the traditional enterprise security perimeter simply doesn't exist anymore. Firewalls and other standard security functionality can't extend to the Cloud and instead firms have to rely on the basic level of perimeter protection offered by their Cloud provider. From another perspective, the perimeter-based security model has become a useful part of the security architecture, but not the only part. When dealing with the Cloud, enterprises still have the notion of a perimeter. The choice is whether they extend that perimeter into the Cloud or extend their Cloud inside their perimeter, or both. In either case, additional security layers are necessary. However, both scenarios have similar drawbacks concerning the potential lack of visibility and control. CISOs (*Chief Information Security Officers*) must be vigilant, conduct due diligence and be aware of the risks involved.

Extending enterprise perimeter to the Cloud

This scenario involves setting up an IPSec (*IP Security protocol*) VPN (*Virtual Private Network*) tunnel to your public Cloud provider's servers, and putting enterprise-grade security on the public Cloud server, usually in the form of security software and virtual appliances. The benefit of this set-up is that you won't have to reconfigure Active Directory and most other existing management tools should work with your Cloud set-up, as your Cloud servers are effectively inside your 'perimeter'. On the disadvantage side, depending on how well you secured your Cloud server, you may have introduced the risks associated with the Cloud to your architecture, as outlined below. To help mitigate these risks, it is important that the link between Cloud and internal server is monitored for suspicious traffic. Another option is to add an extra DMZ (*Data Management Zone*) and firewall, although that creates another perimeter that needs securing.

Many firms forget or ignore this step in their rush to the Cloud, especially those in smaller organizations without the time and IT resources to architect in these safety barriers. It's also essential to put enough security on those Cloud servers so you can trust them, to protect them from malicious attacks etc. CIOs must be aware that their Cloud servers will be subject to different threats from those that threaten internal systems. A major concern is that firms are not likely to be given their Cloud provider's physical or admin access logs. How will they know if an IT admin working for their Cloud provider has accessed their data? This lack of visibility in the Cloud should necessitate widespread adoption of data encryption as standard.

Shared storage also presents an area of risk to firms anxious that their data is not safe if stored alongside

a competitor's data. Some public Cloud providers simply aren't as transparent as they should be. As a starting point, if you're putting mission-critical data into the Cloud you need to look for strict adherence to security best practices, like ISO 27001 and SAS70 II, and rigorously examine your provider's SLAs (*Service Level Agreements*) and security policy.

Another risk is that most Cloud providers are likely only to reimburse in the case of a breach up to the cost of the service they provide, even if it was their fault. A data breach which leads to untold reputational damage, fines and financial loss will have to be absorbed by the customer.

Extending the Cloud into the enterprise

This scenario allows the Cloud to effectively extend inside the enterprise perimeter, and involves agreeing to an IaaS public Cloud provider or Cloud-based MSSP (*Managed Security Service Provider*) installing a Cloud node on site. The benefit of this set-up is that it is a relatively well understood model. MSSPs such as Integralis have been providing remote firewall management services 'from the Cloud' for years. Other examples include the Trend Micro Smart Protection Network, which links security servers inside an enterprise network to a security network of thousands of servers in the Cloud.

However, for all the simplicity of having one of these boxes located in the data centre or branch office and managed or updated centrally by the Cloud provider, the main disadvantage is that it is still essentially a Cloud service and as such could present the IT manager with many of the same risks of the first set-up. This includes risks presented by lack of visibility into physical and/or admin access logs. Liability for negligence leading to loss of mission-critical data will still only go as far as reimbursement for the cost of the service. Although can be turned on and off, when the Cloud extending to the enterprise is 'on' - the Cloud provider is given full access to your network and to the application data, so the Cloud provider must be trusted. If that provider is focused on security and is transparent with its SLAs, this should be less worrying.

It's about differentiating between 'good enough' security and 'optimal' security. A Cloud-based email service set up in your perimeter by a managed security service provider, for example, is likely to be more trustworthy than one provided by a typical public Cloud vendor.

IV. Who owns security in the Cloud and where are the gaps?

The unpalatable truth here is that if you're looking for help from the Cloud provider you're likely to be disappointed. You should secure your Cloud servers as you secure your internal servers. This includes: IDS (*Intrusion Detection System*), IPS (*Intrusion*

Prevention System), DLP (*Data Loss Prevention*) tools, bi-directional firewall, and encryption.

You could run into problems on the network security front in the Cloud environment, as few public Cloud providers are likely to allow you to monitor network traffic as closely as you'd like. This may rule out the Cloud from a compliance point of view, so it's vital you find out how much network monitoring and access your provider will allow. Encryption of data 'at rest' (stored) and in transit (transmitted) becomes extremely important because of the lack of visibility into network traffic and your provider's admin access logs.

Many Cloud providers also offer a worrying lack of role-based access controls at an admin level. In the private Cloud, ownership of security by the IT department is being challenged thanks to the speed at which servers can be created. All the business needs today is to know it can cover the cost of a licence, and in a private Cloud environment a business unit could have a server up and running in one or two days, rather than six weeks. However, each request for a new server has to be properly managed because the security risks will increase as the number of boxes to manage increases. It's important that IT managers put in place a central authorising process which ensures any requests must pass through IT first.

V. Call to action

Enterprises:

- Encrypt data at rest and in motion and be careful to store encryption keys in a location separate from the data, that is, not where they are easily accessible to the Cloud provider.
- Deploy every security tool you deploy on your physical servers in the Cloud as well because all the Cloud providers will give you is a naked OS without adequate security. Cloud providers:
 - Be more open and transparent about security policies and procedures around access controls and network traffic. Customers need to know who did what and when, and they need to be allowed to see the logs.
 - Clarify SLAs so customers are clear what security features you offer and what they will need to do to ensure their data is secured to their own and their regulators' standards.

Private Cloud environments:

- Create a central authorisation process, if there is not one there already, for all new Cloud server requests from the business. You need to know why they need a server, what will be running on the server, how long it will exist and how much traffic will flow through it. You also need to have regular check-ups on these requirements.
 - Be prepared...IT is being forced to accelerate the speed at which it works. For the good of the business, you must be prepared to support these requirements in a timely manner without compromising the security. ●