Who Owns Security in the New Ambient Cloud?

A Trend Micro Opinion Piece

Trend Micro, Incorporated

» By Dave Asprey, Trend Micro, VP Cloud Security
June 2012

WHAT IS THE NEW AMBIENT CLOUD?

Since cloud computing has become one of the hottest areas of technology over the past few years, IT executives have come to understand that provisioning on-demand IT software and infrastructure services via the internet provides huge benefits in efficiencies, cost savings and scalability. However, with these game-changing benefits we've discovered a whole new set of challenges which invalidate most traditional approaches to security, and IT departments still struggle with the question of who owns security in centralized cloud models.

The paradox at the heart of this new computing paradigm is that while the cloud in one sense offers a vision of simplified, pay-per-use IT in which much of the heavy lifting is outsourced, it also introduces new compliance headaches and potential areas of data security risk.

Things get much more complex when you consider the ambient cloud. To date, cloud computing has meant managing servers or virtual machines or software as a service in a data center somewhere. The rise of mobile devices more powerful than pcs from a few generations ago, combined with consumerization and the rise of a decentralized workforce has created what we now know as the ambient cloud.

The ambient cloud is the set of network connected devices an IT department must manage.

Compared to managing an ambient cloud, managing a cloud in a data center is simple. However, security lessons learned from managing centralized clouds carry over very well to managing decentralized ambient clouds composed of servers, PCs, tablets, and smart phones. The truth is that your data – and probably your work load too - is spread unpredictably across a mix of centralized clouds and ambient clouds.

IT managers are reassessing their options in this 21st century computing environment. They want to know the risks involved and crucially where the security responsibility and accountability lies, across all devices and all workloads.

Here we attempt to address these issues, both in the context of cloud-based security offerings and in the context of the Infrastructure as a Service (IaaS) – that which allows IT managers to rent networking, storage, server and other operational elements, because it offers enterprises greater autonomy to put more security controls in place than models such as SaaS.

The ambient cloud equivalent of IaaS is "mobile device management", where enterprises choose to manage at least some of the data and applications on employee owned devices. The alternative is the older model of simply issuing company owned smart devices that are locked down to a corporate standard.

II. WHY THE CLOUD?

On the public cloud side, it all comes down to scaling and the ability to use opex (Operating Expense) instead of capex (Capital Expense). Cloud computing customers avoid capital expenditure on hardware, software and other infrastructure services by paying their provider only what they use, in a utility model. The on-demand provision of resources also allows firms to scale dynamically according to their computing needs in real-time, vastly improving business agility.

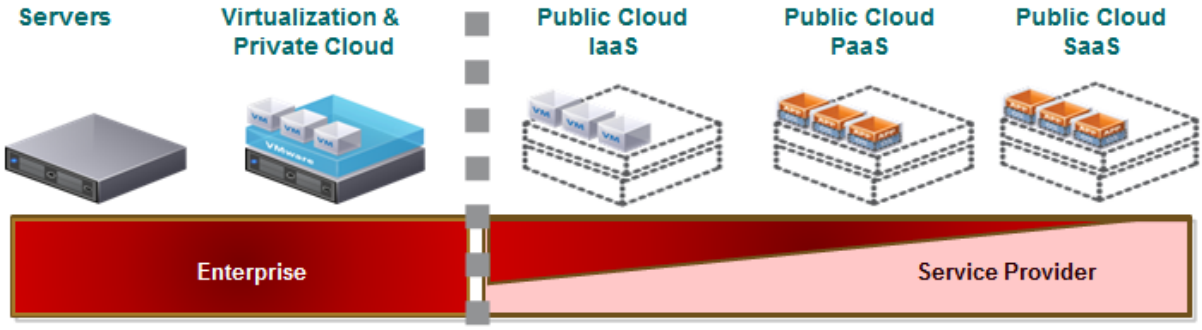
On the private cloud front, it is all about increased flexibility and responsiveness to internal customers' needs because workloads shift around to increase server utilization. Private cloud is also less costly than public cloud for workloads that are static. For enterprises that are willing to use capex over opex, the most effective combination is to use a private cloud for static, predictable workloads, with public cloud for highly variable workloads.

For ambient clouds, the motivation is to maintain control of company data but to remain responsive to incredible pressure to allow employees at all levels to use their own personal devices such as tablets, smart phones, and PCs. Pressure to embrace consumerization also often comes from Human Resource departments who finds that it is growing increasingly difficult to recruit younger people at companies with restrictive device policies. IT departments have no real choice but to manage a wave of personal and mobile devices in the same way they manage large numbers of servers in the cloud.

III. SO, 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, unless you're paying your cloud provider for specific, well identified cloud security services. In any case, you may even find your job made more difficult by the lack of visibility you have into access logs or the disconcertingly vague wording of security policies.

The short answer is that you, the enterprise, always own security in the cloud, because you are responsible for what happens if cyber-criminals breach your security. The good news is that now it's safe to outsource specific security tasks to your cloud provider, as long as the roles and responsibilities are well defined. Never assume the cloud provider is doing a specific security task unless there is a contract that specifies it. In the image below, it is possible to outsource security tasks in the "red zone" for IaaS, PaaS, and SaaS, but you should expect to pay a premium to your cloud provider if you do not take on those responsibilities for yourself.



Who is responsible for security?

Here are some best practices:

- You should secure your cloud servers as you secure your internal servers. This includes; IDS/IPS, DLP tools, bi-directional firewall, and encryption.
- You should secure your ambient cloud devices just as you secure your corporate-owned mobile devices. This includes encryption, firewall, DLP, and antivirus.
- 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. In your own network, all router/switch configuration and logs are free, and you can sniff any network traffic you want. But in the cloud, none of that is available. 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 and in transit 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. With Amazon EC2, for example, one account owns all the instances, so one member of the organization with account access could effectively have the keys to the kingdom, with the ability to add and subtract boxes at will.

- In the private cloud, ownership of security by the IT department is being challenged thanks to the speed at which you can provision new virtual servers. That natural equilibrium between IT's ability to deliver the servers and the business' need for them is becoming unbalanced as the process accelerates. All the business needs today is to know it can cover the cost of a license, and in a private cloud environment a business unit could have a server up and running in 1-2 days, rather than 6 weeks.

However, each request for a new server - or ambient cloud device - 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 authorizing process which ensures that any requests from the businesses must pass through IT first.

IV. PERIMETER SECURITY ISN'T DEAD: TWO APPROACHES TO SECURING THE CLOUD

Pundits make much of the fact that when it comes to the public cloud model, the traditional enterprise security perimeter simply doesn't exist anymore. Firewalls, intrusion prevention systems and other standard security functionality, the argument goes, can't extend to the cloud and instead, firms have to rely on the very basic default level of protection offered by their cloud provider.

But from another more holistic perspective the perimeter-based security model isn't actually dead at all; it's become a useful part of working security architecture, but not the only part. When dealing with the cloud, enterprises still have the notion of a perimeter. The choice for firms is whether they extend that perimeter into the cloud or extend the cloud inside their perimeter, or both. This goes for both public clouds and for ambient clouds, by the way.

In either case, additional security layers are necessary, just as they are in internal enterprise security environments. However, both scenarios have similar drawbacks concerning the potential lack of visibility and control arising from outsourcing to the cloud. CISOs must be vigilant, conduct due diligence and be aware of the risks involved.

Here are the two methods of addressing perimeter security in the cloud, presented as scenarios.

Scenario 1 – Extend Your Perimeter to the Cloud

Extending your perimeter to the cloud involves setting up an IPSec VPN 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 severs are effectively inside your "perimeter".

From an ambient cloud perspective, this translates to using a mobile device management platform to install enterprise-grade security on employee owned or corporate owned mobile devices. This approach is best suited to corporate-owned devices however because it involves trusting the entire device, at least until mobile device virtualization hits the mainstream.

However, there is a downside. Depending on how well you secured your cloud devices or servers, you may have introduced the risks associated with the cloud to your architecture [outlined below]. To help mitigate these risks, it's important that the link between cloud and internal servers be monitored for suspicious traffic, just as all links to critical servers should be, whether they're in a cloud or not.

Another option is to add an extra DMZ and firewall, although that creates another perimeter to secure. 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 and devices so you can trust them – IDS/IPS bi-directional firewall, malware protection, web security, etc.

Risks of Scenario 1

CIOs must be aware that their cloud servers and devices will be subject to different threats from the ones they are used to mitigating internally.

- 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 public cloud provider has accessed their data, for example? The insider threat can be mitigated to an extent internally by maintaining access logs, but this lack of visibility in the cloud should force the widespread adoption of data encryption as standard.

  [It has been reported that corporate data belonging to customers of Microsoft's hosted business suite BPOS was accessed and downloaded by other users of the software after a misconfiguration error. Although fixed quickly, it highlights what can potentially go wrong, and the importance of having visibility into your cloud provider's systems to ensure they meet your own and your regulators' standards.]

- The same is true for ambient cloud devices such as mobile phones. You won't have access to all physical or admin access logs on an employee-owned phone, just as you won't have full access to those for a cloud-operated server. That's what you should encrypt enterprise data on mobile phones in the ambient cloud just as you should in a centralized cloud.

- Shared storage also presents an area of risk to firms anxious that their data is not safe if sat alongside a competitor's data on the same disk in the cloud.

- Some public cloud providers simply aren't as vigilant about security, or as transparent about what they are doing, as they should be. As a starting point, if you're putting mission critical data into the cloud, you at least need to look for strict adherence to security best practices, like ISO 27001 and SAS70 II, and rigorously examine your provider's SLAs and security policy.

- Related to the previous point is the fact 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 they are at fault. A data breach which leads to untold reputational damage, fines and financial loss potentially running into the millions, for example, will have to be absorbed by the customer.

Scenario 2 – Extend the Cloud into Your Enterprise

Extending the cloud into the enterprise, allows the cloud to effectively extend inside your perimeter, and involves agreeing to an IaaS public cloud provider or cloud-based MSSP installing a cloud node on site.

The benefit of this set-up, which is starting to become increasingly common among larger enterprises, is that it is a relatively well understood model. Akamai, for example, has done a similar thing for over ten years now, managing a server located within the customer's security perimeter, and 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.

From an ambient cloud perspective, it's common to work with third-party services to manage employee owned or corporate owned mobile devices. When you make that decision, you've effectively outsourced management of your ambient cloud, just as you might outsource management of your central cloud by going with an IaaS service. Alternatively, you could go with the ambient cloud equivalent of a private cloud by installing your own mobile device management platform that applies policy to all employee owned devices that connect to it.

However, for all the simplicity of having one of these boxes located in your data center or branch office and managed or updated centrally by the cloud provider, the main cons are that it is still essentially a cloud service and as such could present the IT manager with many of the risks of the first set-up.

- The risks presented by lack of visibility in to physical and/or admin access logs remain

- Liability for negligence leading to loss of your mission critical data will still only go as far as reimbursement for the cost of the service.

- Although it can be turned on and off, when it's on the cloud provider will have access to your network and application data so it must be trusted. If that provider is focused on security and transparent with its SLAs, there should be less to worry about. However, as discussed, most generalist cloud providers do not have security at the heart of their value proposition.

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.

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, i.e. 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. Deploy every security tool on employee owned consumer devices that you would deploy on enterprise owned devices that are permitted to penetrate – or reside within - your perimeter.

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. This also applies for hosted mobile device management "ambient cloud" platform providers.

Private cloud environments

Create a central authorization process if there is not one already for all new cloud server requests from the business. You need to know why they need one, what will be running on the server, how long it will exist, how much traffic will flow through it and have regular check-ups on these requirements. Replicate the process to register all employee owned ambient cloud devices that will have access to your network and applications.

The growth of public clouds, private clouds, and now consumerization driven ambient clouds is forcing it to accelerate the speed at which it works. For the good of your business, you must be prepared to support these new environments without compromising your security.

TREND MICRO™
Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003

www.trendmicro.com.