TREND MICRO™ Securing Your Journey to the Cloud

Is your security as good as the cloud's?

Written by Dave Asprey, VP Cloud Security, Trend Micro

Introduction

For many businesses taking their first tentative steps into the brave new world of cloud computing, the $64,000 question is: "How secure actually is the cloud?" While Gartner advocates that cloud computing should be the number one priority for CIOs in 2011, the analysts also recognize that security and privacy are critical concerns for those considering adoption of cloud-based technologies. These concerns outweigh the sum of other factors such as performance, compliance and immaturity and must be addressed head on if cloud computing is to gain genuine traction in the business mainstream.

Navigating the current cloud computing landscape can be a tricky task, which is why firms need to do their homework before deciding whether to take the plunge. Outsourcing some or all of your computing to the cloud is not a decision to be taken lightly. It requires a serious amount of due diligence, planning and forethought to ascertain both what model is best for your organization's needs – Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) – and which provider will offer the right level of security assurances.

The differences between Software-as-a-Service and Infrastructure-as-a-Service are significant, so businesses must first assess the relative merits of both models in order to determine whether they are likely to provide better or worse security than they can currently manage in-house.

SaaS and IaaS – a definition

In the **Software-as-a-Service** model, all the computing heavy-lifting is done by the cloud provider, which usually then licenses the applications to the end customer in a pay-per-use model. What this means from an infrastructure standpoint is that the end user has virtually no responsibility for the running or securing of that application – almost everything is done by the SaaS provider which hosts and secures in their own datacenter before delivering via the internet to the customer. Whether it's Salesforce.com or Google Apps, the visibility and control afforded to the IT manager is usually minimal.

Infrastructure-as-a-Service, as the name suggests, is a very different beast from SaaS in that it allows the customer to rent servers, software, storage and networking capabilities on a pay-per-use basis from the service provider. The customer has more visibility and control over their outsourced computing environment and greater flexibility over which applications and operating systems they run on top of it. However, typically there is more responsibility on their part to secure this infrastructure, as the IaaS provider's own security provisions can be basic.

How good is SaaS security?

If an organization goes down a SaaS path, there will be very little security to actually take care of. In fact, the only responsibility the CISO has is to protect the username, password and browser sessions of their staff with the appropriate endpoint security controls. All other security is handled by the SaaS provider, so it is somewhat reassuring to know that most big-name providers are pretty good when it comes to the resources they throw into security.

For the most part, reputable cloud providers are likely to be well resourced, security accredited to a good standard (ie SAS70), and with a dedicated and highly trained security team which can protect their customers' apps and underlying infrastructure better than many IT managers could themselves.

In other words, the SaaS vendor will put all of its eggs in one basket and protect that basket extremely well via measures such as:

- Strict corporate security policies, covering everything from networks to change management and datacenter security
- Frequent staff security and awareness training
- Dedicated physical security teams
- Audits for compliance with key statutory and regulatory requirements including SOX, PCI
- Strict authentication and authorization controls
- Malware scanning
- Vulnerability management/remediation
- Network security (firewall/ACL)
- Hardened OS
- Up-to-date patching of apps, OS

Visibility issues

However, some CISOs may find the lack of visibility afforded from an operational level into things like operating system files and logs makes SaaS a poor choice for their organization. In December 2010 a Microsoft misconfiguration error meant customers of the firm's hosted BPOS suite could access and download data belonging to other users of the service. If SaaS providers can't show how they'd prevent against this kind of internal error then they risk losing potential customers.

How good is IaaS security

For those who do want more control over their outsourced IT environment and have the resources to pay for it, IaaS may be a more attractive option. It enables the IT manager to run any application they want on any set-up. However, the other side of this double-edged sword is that they will need to provide [and pay for] more in the way of security controls.

Many public cloud IaaS environments provide only minimal security and those that have enhanced their services with improved security measures have done so in a piecemeal fashion so that there is no uniform landscape in the IaaS industry. Some providers will offer little more than a bare, open virtual machine for the customer, while others may provide options such as a virtual private network which enables customers to securely connect their cloud and on-premise resources. Amazon Web Services recently upped its own security game by adding the ability for customers to carry out network configuration between virtual machines in the cloud as well as other basic security measures.

This means that IT managers must proceed with caution. They need to carry out due diligence on any prospective IaaS vendor to ensure they know where security is provided and where there are gaps which they will need to fill themselves. Organizations must also be prepared to implement strong encryption on all of their data as an emergency failsafe in case their security controls fail to prevent a data breach.

The risks

Traditionally, the security risks of IaaS lie mainly around the shared public cloud infrastructure. Users may share the same lowest common denominator firewall, the same network inside the firewall, the same storage and the same physical server. This is not the case with all environments, but without thorough security measures there could be a risk of attack via the hypervisor.

Another risk was recently revealed when it was found that a pre-built machine image uploaded by a member of the AWS community to be used by others was found to still have the publisher's SSH key on it, meaning the publisher in question could technically log in to any instance running that image. Although pre-built images can be a handy way of saving time and speeding the start-up process, this incident raised important questions about the potential security risks inherent in this particular system at present.

Best practice tips

Bearing in mind that all IaaS vendors are not created equal when it comes to security, organizations should consider the following best practice steps:

- Patch and update OS/apps with most up-to-date versions
- Purchase, deploy and configure host-based agents for every instance/VM separately (DLP, IDS/IPS, firewall).
- Encrypt everything – network traffic, block storage and shared storage and only allow decryption keys to enter the cloud during decryption; don't store in the cloud.
- Lock down access to systems. Don't allow password-based authentication for shell access or passwords for sudo access.
- Back-up regularly outside the cloud
- Keep particularly sensitive data in a separate database
- Minimize the no. of services per VM instance with the goal one per instance
- Only open the ports you need
- Specify source addresses and only allow HTTP global access
- Ensure pre-built cloud images come from a reputable vendor and are cryptographically signed

Further issues to consider

Even having taken these precautions, CISOs should be aware that risks persist with the IaaS model. There are still issues with how much visibility the customer has into their cloud environment – access to the cloud provider's physical or admin access logs could be denied and visibility into network traffic may not be high enough for some organizations, for example. Also, the lack of roles-based account access in certain IaaS packages may be prove problematic for some organizations.

Conclusion

So, is your security better than the cloud's? The reality is that for the average SMB, the SaaS provider may be able to offer more comprehensive security for your apps than you can in-house. The downside of this, however, is the lack of visibility you'll have into the SaaS provider's environment.

If, on the other hand, you decide you need a more flexible set up allowing you to run the apps and infrastructure you want, then IaaS is likely to be the preferred choice. However, IT managers must be aware that there's no level playing field when it comes to security standards in the IaaS industry and serious due diligence is essential in order to ascertain exactly how much security the prospective IaaS provider will offer. Having planned out exactly what their configured set-up will look like in the cloud, organizations must be prepared, to a lesser or greater extent, to take care of any security gaps and provide extra encryption as a final safety precaution.

In any case, it's important to look at the T&Cs of your prospective cloud provider (whether SaaS or Iaas) and check against any industry regulations or legal requirements relevant to your organization to see if it is a viable alternative to a traditional in-house set up. Regardless of the security measures that the customer and IaaS provider have put in place, it should be understood that in most cases, responsibility for the safety and security of the customer's data ultimately lies with the customer.