

Security Issues in Cloud Computing

For many businesses considering cloud computing, the \$64,000 question is: “**How secure is the cloud?**” Consulting firms advocate that those who are considering adopting cloud services recognize that security and privacy are critical concerns of cloud-based technologies. These concerns can often outweigh the sum of other factors such as performance, compliance and immaturity.

Navigating the current cloud computing landscape is tricky; so much so that 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. Outsourcing requires considerable due diligence, planning and forethought to ascertain what cloud model best fits your organization.

There are three standard Cloud offerings:

1. Software-as-a-Service (**SaaS**),
2. Platform-as-a-Service (**PaaS**), and
3. Infrastructure-as-a-Service (**IaaS**)

The security provided for each of these offerings is quite different. Businesses must first assess the relative merits of these models to determine whether they are likely to provide better or worse security than they can currently manage in-house.

Software-as-a-Service (SaaS)

In the SaaS model, the provider sets up the hardware and licenses all the software and usually then licenses the applications to the end customer in a pay-per-use model. In this mode, **the end user has virtually no responsibility for the running or securing of that application.**

The SaaS provider secures hosts and the requested applications in their own datacenter before delivering them to the customer 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.

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 (i.e. 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. Table 1 below lists some of these items.

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

Table 1: SaaS Items That Must Be Managed

SaaS 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.

The Infrastructure-as-a-Service model -- IaaS

IaaS customers can 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.

How good is IaaS Security

Compared to SaaS environments, IaaS providers put more responsibility on the customer's part to secure this infrastructure, as the IaaS provider's own security provisions can be basic.

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, (AWS), recently added the ability for customers to carry out network configuration between virtual machines in the cloud as well as other basic security measures.

A prospective IaaS customer searching through various offerings will soon realize that there is no uniform landscape in the IaaS industry. **If you want more control over their outsourced IT environment, you must commit extra resources to meet your security needs.** If this is done, IaaS will usually be more attractive because your IT managers can run any application they want on any set-up.

IT managers must proceed to an IaaS option 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 needing to be filled. 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 IaaS Security Risks

Traditionally, IaaS security risks lie mainly in the shared public cloud infrastructure. IaaS users may be sharing the same lowest common denominator firewall, the same network inside the firewall, the same storage and the same physical server. Without thorough security measures there could be a risk of attack via the hypervisor.

Some IaaS providers, such as AWS, deliver pre-built images to be used by customers, which can be time savers and expedite the startup process. A researcher found that a pre-built machine image intended to be used by others still contained the publisher's SSH key. This means that the publisher in question could technically log in to any instance running that image. This incident raised important questions about the potential security risks inherent in using pre-built images.

Best practice tips for IaaS Environments

In determining if IaaS is a suitable option, organizations should consider the best practice steps shown in Table 2 below:

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)
Lock down access to systems. Don't allow password-based authentication for shell access or passwords for sudo access.	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.
Back-up regularly outside the cloud	Keep particularly sensitive data in a separate database
Only open the ports you need	Minimize the no. of services per VM instance with the goal one per instance
Specify source addresses and only allow HTTP global access	Ensure pre-built cloud images come from a reputable vendor and are cryptographically signed

Table 2: IaaS Best Practices

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 role-based account access in certain IaaS packages may be problematic for some organizations.

Conclusion

So, is your security better than the cloud’s? The reality is that for the average small to medium sized business, the SaaS provider may be able to offer more comprehensive security for your apps than you can in-house. Even if this is true, you will still lack visibility 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. IT managers must be aware that there are few security standards in the IaaS industry. They must also be willing and able to perform due diligence to determine the extent of the IaaS provider’s security offerings. Once a cloud architecture is determined, organizations must still take care of any security gaps and provide extra encryption as a final safety precaution.

It is important to look at your prospective cloud provider’s offerings in detail. You must check their offerings against any industry regulations or legal requirements relevant to your organization. Only in this way can you determine if a SaaS or IaaS offering is a viable alternative to a traditional in-house set up.

The final caveat is that regardless of the security measures that the customer and IaaS provider have put in place, responsibility for the safety and security of the customer’s data ultimately lies with the customer.