



Security in the Cloud

Clavister White Paper

Cloud computing terminology

- Software as a Service (SaaS) – software applications are licensed for use as a service provided to customers on demand. This means that customers do not have to equip a device with every application and so reduces End User License Agreement software maintenance, ongoing operation patches, and patch support complexity in an organization.
- Platform as a Service (PaaS) – takes SaaS a step further by taking all of the facilities required to support the complete lifecycle of building and delivering web applications and services entirely available from the Internet with no software downloads or installation for developers, IT managers or end-users.
- Infrastructure as a Service (IaaS) – is the delivery of a computer infrastructure (typically a platform virtualization environment) as a service and is an example of the 'everything as a service' trend. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service and is typically billed on a utility computing basis.

Introduction

The image of a cloud is often used to represent the Internet or any other large networked environment and now it has given rise to the IT industry's latest buzz phrase 'cloud computing'.

Cloud computing involves a provider delivering a variety of IT enabled resources to consumers as a service over the Internet and industry pundits have claimed that in five years, cloud technology will have a footprint in every business that does IT, changing the entire computer industry.

At the front end are the client computers and the application required to access the cloud computing system. At the back end are the various computers, servers and data storage systems that create the 'cloud' of computing services.

Because these resources are provided 'as a service', the idea is that users need not have any knowledge or expertise in the systems that support them, or indeed any control over those systems. They just need to have confidence in the ability to send data to the cloud and to receive data back.

However, for many, that is a 'head in the clouds' attitude. They have grave concerns over the privacy and security of their data and the idea of handing over important company information to another organization worries them. They hesitate to take advantage of cloud computing because they believe they can no longer keep their data under lock and key.

So, is there really anything to worry about or are the facts being obscured by sensationalism and cloudy thinking? Here we take a closer look at security in the cloud.

About cloud computing

Businesses need to provide their staff with the appropriate software and hardware to function efficiently but that can be an incrementally expensive and often restrictive exercise. Not only do you have to buy the hardware but you also have to purchase software licenses and when more people join, then you must purchase more software or

extend the licenses which can limit the number of applications you can provide.

Now there is another way, and that is cloud computing. Remote machines owned by another company run everything. All your staff's needs are hosted and provided as a Web-based service so instead of installing a suite of software on each computer, the application only needs to be loaded once.

Benefits of cloud computing

Large scale distributed computing offers a number of advantages. One of the biggest is that a user may no longer have to be tethered to a traditional computer to use an application, or have to buy a version that's specifically configured for a phone, PDA or other device. It's likely that at some point any device that can access the Internet will be able to run a cloud-based application.

Also, regardless of the device being used, there may be fewer maintenance issues. Deployment of applications is much quicker and users don't have to worry about storage capacity, compatibility or other concerns. When you're accessing an application on the cloud, you know you're getting the latest version—without having the bother of upgrading the version that's residing on your hard drive—and you won't have to wait as long for your computer to boot up, since cloud applications are always on.

Other advantages include:

- **Reduced cost**
Cloud technology is paid incrementally, saving organizations money.
- **Increased storage**
More data can be stored than is possible on private computer systems.

- **Flexibility**

Cloud computing offers much more flexibility than past computing methods. Organizations can choose to out-source their whole infrastructure or just segments of it.

- **Greater mobility**

Employees can access information wherever they are, rather than having to remain at their desks.

- **Shift of IT focus**

No longer having to worry about constant server updates and other computing issues, organizations will be free to concentrate on innovation.

Concerns and responsibilities surrounding cloud computing

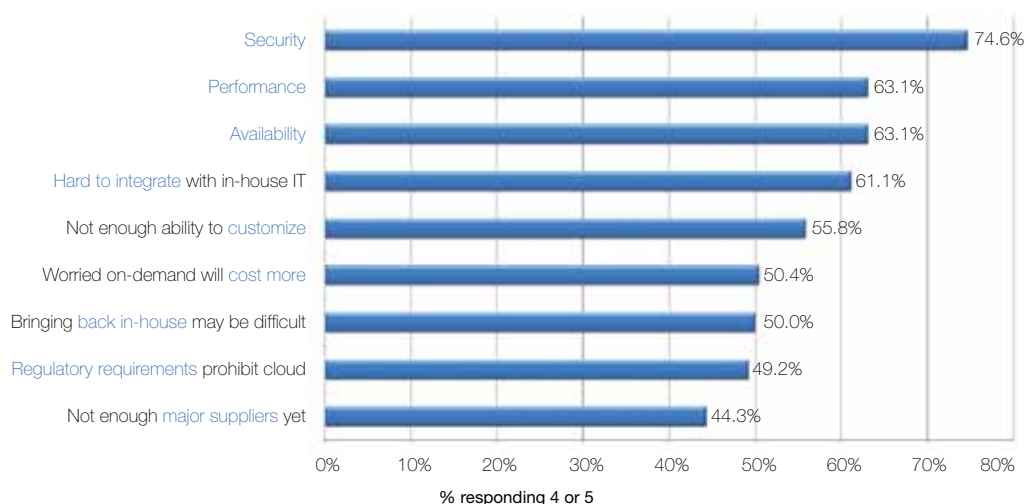
Security

The biggest concerns about cloud computing are security and privacy because, understandably, companies are wary of handing over their critical data to another company. According to a recent IDC¹ survey 74 per cent of IT executives and CIOs cited security as the top challenge preventing their adoption of the cloud services model.

Of course the success of cloud computing vendors relies heavily on their reputation so it is vital that they have reliable security measures in place and implement the latest technology to protect client data. However, while they may have firewalls and other mechanisms to prevent intrusion, these are usually designed to support generic security policies and are not tailored to you and your specific systems. Even though your resources are located in the cloud, it is still up to you to ensure that your security policies are being maintained.

There are specific security issues that anyone considering cloud computing must address to ensure that they will still have

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1 = not significant, 5 = very significant)



Source: IDC Enterprise Panel August 2008

¹ Source: IDC's IT Cloud Services User Survey pt. 2, October 2nd, 2008

adequate security policy control over applications and services; as well as meeting customer service level agreements on security while remaining compliant with rules and regulations on data security.

Virtualization in the cloud

For anyone wanting to reap the benefits of cloud computing, it is essential to replicate their normal security policies inside the cloud and ensure that they can maintain control of them via visibility of logs and compliance reporting and such like.

Virtualization, or the ability to create shared pools of resources by enabling the creation of many virtual machines on just one physical server, causes the same concerns in the cloud as it does in a more traditional infrastructure.

Because of the co-location of multiple virtual machines in the cloud, it is important to combat the threat of malicious activity spreading between the virtual machines. Segmentation in a physical environment prevents this, but in a virtualized environment you do not have that segmentation so a hacker in your Web system can easily jump over to your financial systems or databases.

One of the best ways to ensure that your security policies are being maintained in the cloud is to implement a Virtual Security Gateway into your environment, enabling you to apply the same critical rules, log-ins and access privileges, just as if the resources are located in-house in your own environment.

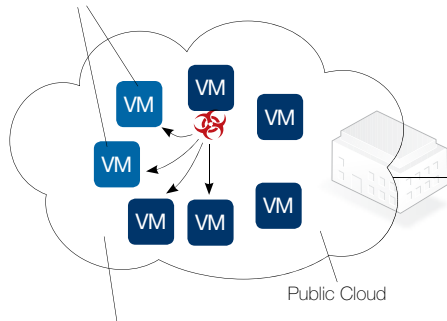
A Virtual Security Gateway of the type developed by Clavister is a firewall that runs inside your virtual infrastructure and ensures that security policies are enforced for all communications inside the virtual environment. Virtual machines are not allowed to talk to each other unless they go through the security gateway.

The Gateway uses VPN encryption to secure communication between virtual machines. Since the Virtual Security Gateway can be run inside the virtual infrastructure, security auditing can be achieved and so regulatory compliance requirements can be met. Users have the scalability to simply deploy new security gateways as they expand their environment. Also, since the virtual security gateway is part of the virtual infrastructure, it becomes easier to create lab/test environments which decreases complexity of security tests and in turn, improves the overall security.

Although it may be difficult to influence how traffic is routed within the cloud, it is important to try and control how your virtual servers are set up to communicate with each other and with

Security threats in the cloud

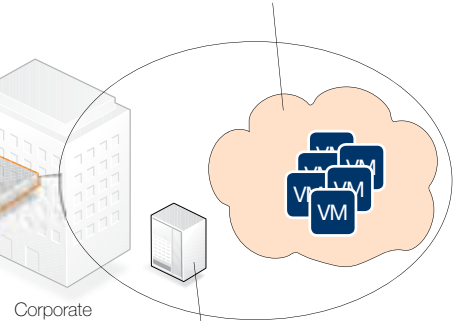
Your Cloud Hosted Virtual Machines & Resources



Uncontrolled Infrastructure

Log management and security management of cloud resources unmanaged and not aligned with corporate IT policy. Generalized firewall security policies mean that it is one fits all and not tailored to specific requirements.

Internal Cloud – e.g. VMware vSphere

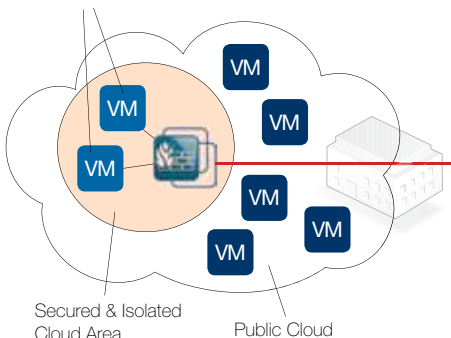


Corporate Data Center

Log Management, Reporting Security Management

The secured cloud

Your Cloud Hosted Virtual Machines & Resources



Secured & Isolated Cloud Area

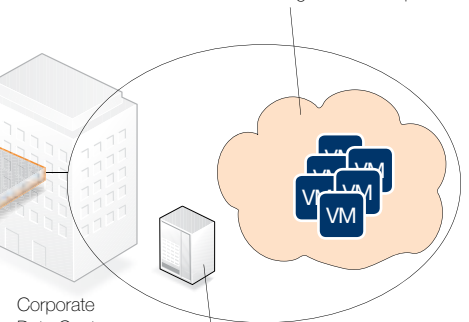
Public Cloud

Encrypted VPN Tunnel



Internet

Internal Cloud – e.g. VMware vSphere



Corporate Data Center

Log Management, Reporting Security Management

the rest of the cloud infrastructure. You should ask these questions to establish that your data is private because it is always possible that a competitor could be sitting on the same physical server and seeing your traffic.

Data in the cloud is positioned in a shared environment alongside data from other companies and it is important to establish that there is adequate data segregation. It is vital to ensure that encryption is in place and that it has been designed and tested by specialists.

VPN networks

If your organization is global, with remote offices around the world, you may want to avoid using a single cloud vendor whose connection speeds may be slow because they are on the other side of the world. It's a good idea to use multiple vendors with similar setups and having a Virtual Security Gateway empowers you to do this. It gives you the ability to establish your own VPN network with full encryption between all your virtual resources around the world, no matter which vendor they are with. In this way, you can make sure that they can all communicate with each other while the data is still encrypted and secure.

To implement this, there are commercial solutions that enable customer-controlled security in a cloud, across multiple clouds and between the physical data centers and clouds. Using an encrypted cloud VPN, they establish a secure bridge between your private infrastructure and the cloud, controlled by you. This means you can confidently leverage the cloud for redundancy, failover and scalability during critical transitions; whether scaling up to grow the business or scaling down to cut costs.

Portability

Another major issue is that of portability – the power to move your resources from one cloud computing vendor to another, should you wish to do so. Ensure that your contract gives you the right to easily move not only your data and images but also your security policies and components to a second supplier. While you cannot take a vendor's physical firewall with you, make sure that all the important policies will be maintained by your own dedicated virtual security.

If you're using an infrastructure service, backing up the files and data should be relatively easy. If you're using a Web application, be sure to have a plan for taking your data with you in case you need to switch to another vendor.

You don't always need to move all of your data to the new application if you have a way of viewing the data. For example, you don't have to move all of the old time tracking application's data to the new one if you have viewable access to it.

Also, investigate what would happen to your data, or to the application, if your vendor is forced to shut down. This negative aspect might be something that is seldom mentioned in marketing materials. If exporting your data is easy, then the possible shut down of the vendor shouldn't be that dangerous. However, you would still face the problem of finding a suitable new application (or vendor) for your business needs.

Administrative access

Privileged user access is an area of concern, and in cloud computing, this is conducted over the Internet which increases the security risk. Sensitive data processed outside the enterprise can create risk because outsourced services can by-pass the various controls exerted over in-house programs. Hence, it is important to get as much information as possible about who manages and administers your data and how their access is controlled.

Access should be encrypted and should embody some extra strength with one-time password protection or multi-factor authentications. This can be achieved with a Secure Access Gateway which allows you to apply strong authentications and encrypted protection for all administration traffic.

Testing

Once you have established your security policies, it is essential to conduct full scale tests in the same way that you would on an internal infrastructure. These should include aggressive hacking and overload stress tests which will enable you to investigate the dangers and responses in a controlled environment and not an emergency situation.

At the outset, it is also important to test the migration process of moving from your in-house facilities to the outsourced cloud so that there are no operational or security surprises when you deploy as part of a live production environment.

Email is usually a good place to start because it is easy to move from a dedicated server to the cloud because it is one of the most painless IT applications to migrate. This can be done in a phased approach starting with a handful of users to pilot the program before fully committing.

After the pilot program, reassess how the cloud is working for your business needs. If everyone is happy with the performance and cost benefits, it is time to work with your cloud provider and begin a broader deployment.

Remember to evaluate your needs over time to see where you can gain new benefits from the cloud. The cloud is not a static technology and, as such, will continue to evolve and change. Because the cloud provider-vendor relationships are fluid, you can move to better technologies without penalty.

Transparency

One leading industry analyst says that customers must demand transparency, avoiding vendors who refuse to provide detailed information on security programmes. Questions should relate to the qualifications of policy makers, architects, coders and operators; risk control processes and technical mechanisms and the level of testing that has been done to verify operational efficiency and pinpoint any vulnerabilities.

Compliance

Regulatory compliance can be an issue. Companies are ultimately responsible for the security and integrity of their own data even when it is held by a service provider. They need to be able to prove compliance with security standards regardless of the location of their systems. It is important to ensure that cloud

'Ninety per cent of known vulnerabilities exploited had patches available for at least six months prior to the breach'

2008 Data Breach Investigation Report, Verizon Business Risk Team

computing providers are willing to undergo external audits and security certifications in the same way that traditional service providers do.

An important compliance concern is Payment Card Industry Data Security Standard (PCI DSS) which is a set of comprehensive requirements for enhancing payment account data security, developed by the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Virtualization and cloud computing contain a number of issues that PCI Qualified Security Assessors may have concerns about so it is important to be able to demonstrate compliance while deploying virtualization technology in your PCI environment.

Among the most important requirements are:

- Segregation of systems with only one primary function per server.
- Segregation of networks with the isolation of all management and control networks.
- Protection of virtual media which may contain cardholder data.
- Implementation of automated audit trails for all system components.
- PCI DSS requirements on things like patching and change control may require additional processes or technology to ensure compliance in a virtual environment.
- Intrusion protection.

The 2008 Data Breach Investigations Report of the Verizon Business RISK team reveals that 73 per cent of data breaches result from external sources and 59 per cent are caused by hacking and intrusions. In 40 per cent of breach investigations, the study showed that attackers gained entry via some kind of remote access system and Web applications are near the top of the list.

Using shared resources across the Internet can increase the risk so it is essential to question vendors on the effectiveness of their firewalls and request auditable proof that they are not being tampered with.

It is also important to ensure that the responsibilities for efficient patch management are clear cut.

Clavister's Intrusion Detection & Prevention System (IDP) provides comprehensive and easy to use protection against current and emerging threats at both the network and the application layer. It is auto-updated which means that many security breaches can be prevented even if users are slow to patch their servers. This delivers an extra layer of security which adds real value and lowers the risk even for companies that do not have the most efficient patch management routines in place.

Vital recovery

Disaster recovery is another important issue. Even if you do not know where your data is, a cloud provider should tell you what will happen to it in the event of a disaster. Industry pundits warn that any offering that does not replicate the data and application infrastructure across multiple sites is 'vulnerable to total failure.' Data replication policies should be established along with proof that the vendor can enact a complete restoration and how long it will take.

Investigative support

There are also concerns over the investigation of inappropriate or illegal activity in cloud computing. Cloud services are especially difficult to investigate because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.

In the long term

Another fundamental requirement is to ensure the long term viability of your data – that it will remain available even in the event of your cloud computing provider going out of business or being acquired by another company.

Getting started

While cloud computing offers many valuable advantages, it is important for companies to investigate how this comparatively new solution meets their specific and individual needs.

- Firstly, learn all you can about cloud computing.
- When considering a provider, ensure that performance is monitored and consistent.

- Check business continuity and disaster recovery arrangements.
- Ensure that scalability meets your changing user demands.
- Finally, one of the greatest concerns for companies releasing their valuable data into the shared environment of 'the cloud' is data security.
- Investigate whether cloud computing security is in line with your own security policies and whether your data is exposed.
- Check that the virtualization platform used by the cloud computing provider enables you to import and export data freely.
- If you want to have the peace of mind that your critical data is secure, get help from network security specialists such as Clavister. Network security is vitally important and as a result, nothing can be left to chance. Due to technological complexities and the wide variety of products on the market, it could be hard deciphering which product best suits you and your company.

To guide you in your choice, Clavister invites you to evaluate a version of the Clavister Security Gateway software by visiting:

www.clavister.com/resources/product-evaluations

Conclusion

When two ground breaking technology innovations are brought together, the potential benefits are enormous but along with the gain comes the danger of pain. The combination of virtualization and cloud computing is a prime example.

By supporting the creation of many virtual machines on just one physical server, virtualization enables businesses to reduce costs and increase the efficiency, utilization rates and flexibility of existing IT assets.

Similarly, cloud computing provides a variety of IT enabled resources to consumers as a service over the Internet, resulting in further significant cost savings, greater flexibility and a wider choice of computing resources.

As cloud computing providers put the two together, the benefits multiply but with many virtual machines from different companies all located on the same physical servers, security can be compromised.

While the cloud computing vendors may provide firewalls and other mechanisms to prevent intrusion from outside, these are generic measures and are not tailored to you and your specific systems. It is still up to you to ensure that your security policies are being maintained, even though the resources are located in the cloud.

The warning is not to let the financial benefits cloud your security vision. Ensure that you can maintain control of your own virtual server resources with a Virtual Security Gateway so you can enjoy the many benefits of cloud computing while sidestepping the dangers.

About Clavister

For over a decade, Clavister has been delivering leading network security solutions, providing commercial advantage to businesses worldwide. The Clavister family of Carrier Telecom Security Systems, unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control. Clavister is a recognized pioneer in virtualization and cloud security. This compliments its portfolio of hardware appliances delivering customers the ultimate choice of network security products. Clavister products are backed by Clavister's award-winning support, maintenance and training program. Clavister boasts an unprecedented track record in pioneering network security solutions including the two largest deployments of Virtual Security Gateways in the world to date.

Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

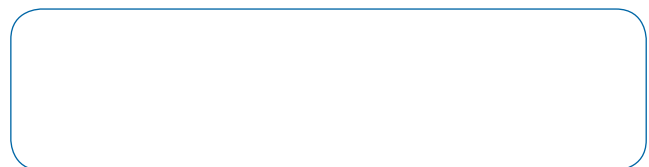
Clavister Contact Information

Sales Offices

www.clavister.com/about-us/contact-us/worldwide-offices

General Contact Form

www.clavister.com/about-us/contact-us/contact-form



CID: clavister-whp-security-in-the-cloud (2011/02)

CLAVISTER®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com