



CloudUp!

An analysis of security in the cloud

Introduction

In a world that sees new technological trends blossom and wither on almost a daily basis, one new trend promises more permanence. This trend is called cloud computing, and it will change the way we use computer in both our professional and personal lives.

Cloud computing signals a major change in how we store information and run applications. Instead of running programs and data on an individual desktop computer, everything is hosted in the “cloud” – a nebulous assemblage of computers and servers accessed via the Internet freeing customers from the need to invest in large technical infrastructure that otherwise would have been required. Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the limits of the desktop and making it easier for group members to work together in different locations.

This technology has gained popularity in a weakened economy as enterprises seek ways to save money, however it is not free of risk. Implemented poorly, this emerging technology presents certain risks, and it could open an organisation to security vulnerabilities and threats.

In order to keep your enterprise secure, it is important to understand exactly how cloud computing infrastructure works. It should be preferable then for cloud customers to know that their providers expect security challenges and continuously act to block them before they occur.

Understanding how the cloud computing provider builds its services and manages the data is critical because it can mean the difference between real cost savings and false economy.

This paper explores the reality of web-based threats today, the drivers for cloud-based computing and the benefits that organisations will see from use of a dedicated service provider for handling functions that are necessary, but that are not a core competence of the organisation.

This paper is meant to be read by executives at companies of all sizes, and especially those at small and medium organisations that have little to gain from running such in-house infrastructure themselves.

Security Architecture

Security architecture is a cohesive design that address the requirements and in particular the risks of a particular environment/scenario and specify security controls to be applied.

Security requirements will change from customer to customer, so rather than providing a one-size-fits all security blanket, some providers offer tailored security solutions for each of their clients.

Solid security architecture depends on both hardware and software components.

From a hardware component, a firewall option such as CISCO is a good example. Protection behind Cisco firewalls prevent common attacks such as denial of service (DoS) and synch attacks. Cisco offers a variety of options and settings, including the ability for web filtering, anti-virus, intrusion detection and interface choices.

Many providers also form relationship with security product providers such as Symantec and Sophos, who provides virus scanning, vulnerability management and reporting with links to remediate databases. For example, Symantec cloud services secure and manage information stored on endpoints and exchanged through email, Web, and IM interactions. These services help protect against viruses, spam, spyware, phishing, DoS attacks, directory harvest attacks, data leaks, and other organisation-damaging threats.

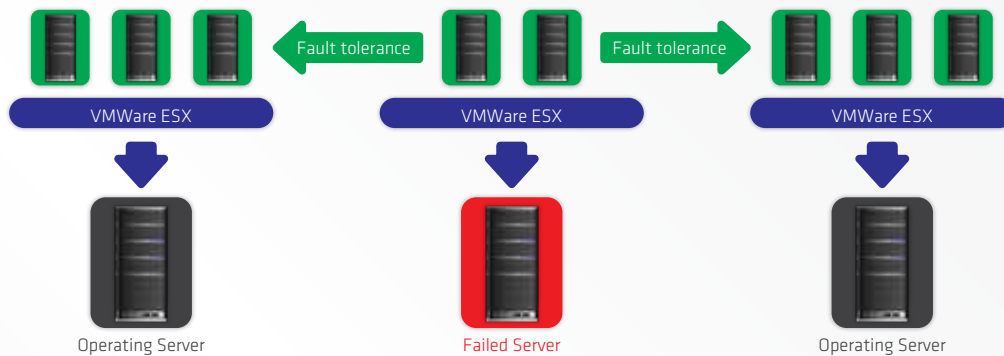


Document Automation Experts

+61 1300 378 836 (Australia) | +44 203 355 1237 (UK)
+1 (213) 291 0523 (USA) | +63 2 817 4901 (Philippines)
info@redmap.com | www.redmap.com

Certain providers utilise the power of VMware solutions. This solution brings to the industry a new platform which provides the software and services to build complete internal and hosted clouds and connect the two together in a federated environment. VMware technology provides clients with Virtual Servers, also known as Virtual Private Servers (VPS). These virtual servers can provide customers with higher performance, higher availability and more secure servers. VMware virtualises four key hardware resources: processing, memory, storage, and network, using a best of breed hypervisor to allocate these resources dynamically to balance changing application needs.

Leveraging key VMware technology advancements, including VMware vMotion, VMware Storage vMotion, VMware Distributed Resources Scheduler and VMware vCenter Servers, customers know they can easily move virtual machines without downtime. This gives customers the ability to manage, move and operate applications in the cloud as easily as they are in more traditional IT environment.



The use of VMware's DRS technology, provides instant IT infrastructure for your business

Business Continuity Services

When selecting your cloud provider, be sure to consider the issue of reliability and uptime and qualify how your service provider has configured their infrastructure for redundancy and failover.

Organisations should look for a service provider that has multiple geographical failover and redundancy in the case of one data centre being unavailable. The system should use load balancing techniques to route web traffic to the nearest available data centre so that performance latency is minimised in order to maintain a fast browsing experience, which can be further enhanced through use of download acceleration and high-performance proxies.

Role-Based Access Control Management

Role-based access control (RBAC) is an access control method that organisations implement to ensure that access to data is performed by authorised users. Unlike other access control methods, role-based access control assigns users to specific roles, and permissions are granted to each role based on the user's job requirements. Users can be assigned any number of roles in order to conduct day-to-day tasks. Some roles maybe Super Users, Billing Users, Read Only Users, System Users. Each role would define the permissions that are needed to access different objects. For instance a system user will most likely to deploy servers but cannot view an invoice or alter billing information.

Data Security

When considering solutions to monitor activity on dynamic database servers, the key is to find a methodology that is easily deployed on new database servers without management involvement. That almost certainly requires a distributed model where each instance in the cloud has a sensor or agent running locally. This software must have the ability to be provisioned automatically along with the database software—without requiring intrusive system management.

In a multi-tenancy environment, it will not always be possible to reboot whenever you need to install, upgrade or update the agents and the cloud vendor may put limitations on installation of software requiring certain privileges. The right architecture will allow you to see exactly where your databases are hosted at any point in time. It will allow you to centrally log all activity and flag suspicious events across all servers wherever they reside.

A better approach when securing databases in cloud computing is to utilise a distributed monitoring solution based on "smart" agents so that, once a security policy is set for a monitored database, that agent or sensor is able to implement the necessary protection and alerting locally. This will prevent the network from becoming the gating factor for performance.

For remote management of distributed datacentres, you'll also want to test the WAN capabilities of your chosen software. It should encrypt all traffic between the management console and sensors in order to limit exposure of sensitive data. Performance can also be enhanced through various compression techniques so that policy updates and alerts are efficiently transmitted.

Physical Security

Physical security also plays a large role with datacentres. Customers need to be assured that the machine their data exists on are safe from compromise by not just hackers, but physical intruders and natural disasters such as fire or flood.

Physical security measures may include 24/7 security guards on site, CCTV surveillance throughout the building, proximity readers and electronic passes restricting access to sensitive areas and an escort for all visitors to the facility.

Power, cooling and fire suppression all play into physical security as well. Be sure that your provider's datacentre houses adequate backup generators, cooling and fire suppression methods to accommodate the size of their datacentre as well as the entire building.

Individual User

Every employee at a company, who uses, moves, transports, files, disposes and creates information and data is critically important to the success of the data and information security program. The users' actions or failures to act in some instances can result in exposing the company to some very risky situations.

To facilitate better security, users may have to take more personal responsibility and trade some privacy for security.

Inherent Security Benefits of Cloud Computing

With all this talk and reporting about security concerns, let's change the channel for a moment and assess the potential security benefits of Cloud Computing. In our research, there are some strong technical security arguments in favour of Cloud Computing.

Here are some of the ways that cloud computing addresses the pain points of today's IT environment.

Centralised data

The biggest benefit is the centralisation of data. Organisations have an issue with asset protection, in no small part because of data being stored in numerous places, laptops, USB drives, external hard drives, tablets, cellphones and the workstations. And the problem is only getting worse.

Thick clients are able to download files and maintain them on the hard drive and there are plenty of laptops out there with non-encrypted files. Using thin clients creates a better chance for centralised data storage. As such, there's less chance for data leakage.

Centralisation also provides the opportunity for better monitoring. That data is in one place makes it easier to check in on your data and see that everything is okay.

Offloading Work

Another security benefit isn't so much a technology, but the fact that you don't have to do it yourself. It's up to the cloud provider to provide adequate security. After all, can your organisation afford 24/7 IT security staffing? The fact of the matter is that your cloud provider might offer more security features than you had before.

Multi-tenanted datacentre's allow cloud providers to have beefier security, simply because of the economy of scale involved. That is, there are many paying clients so the provider is able to do more, because there is more money in the pot. Plus it's to the provider's benefit to offer more, because they cannot afford a bad reputation.

Logging

Logging is also improved. It's something that usually gets the short end of the stick in-house. But in the virtualised world of cloud computing, providers can add as much memory as they need to extend logging.

Incident Response/Forensics

If there is a breach, the cloud provider can respond to the incident with less downtime than if you had to investigate the breach locally. It is easy to build a forensic server online and it costs almost nothing until it comes into use.

If there is a problem, the virtual machine can be cloned for easy offline analysis. Further, many companies don't have a dedicated in house incident response team. If there is a problem, IT staff have to quickly figure out their new job of taking the server down, quickly investigating and getting it back online for minimal production downtime.

Drive vendors to create more efficient security software

Billable CPU cycles get noticed. More attention will be paid to inefficient processes; e.g. poorly tuned security agents. Process accounting will make a comeback as customers target 'expensive' processes. Security vendors that understand how to squeeze the most performance from their software will win.

Redundancy

When formulating your cloud infrastructure, be sure to consider the issue of reliability and uptime and ask your service provider to configure your computing infrastructure for redundancy and failover.

In your LAN, redundancy used to mean that another server or two were added to the datacentre in case there was a problem. These days with virtualisation, redundancy might mean a virtual server being cloned onto the same device, or all the virtual servers of one machine being cloned onto a second physical server.

It becomes more complex in the cloud. While you may think of your server being hosted at the datacentre of your cloud provider, it's not as easy to nail down. Parts of your data may be housed in one location and the other parts scattered throughout the country (possibly even the world) and when the provider adds a redundant system, again the data is scattered throughout their cloud. So it's not an issue of the service provider wheeling in a new server to provide redundant services. Rather, they simply reallocate resources to provide you with a redundant system.

This is one of the key points of benefit for cloud computing- the fact that failover and redundancy are inherent parts of the architecture. However, it's best to ask about these features and make sure they are included.

Conclusion:

Threats to security will always be an issue, whether inside or outside the Cloud. It's a matter of educating ourselves on the different countermeasures available to minimise the risks involved. The use of web security tools and infrastructure can do much to control risks emanating from the Internet and provide organisations peace of mind that their employees and networks are safe.

However in this weakened economy, organisations are seeking ways to reduce their cost and to do more with fewer resources. Where an activity is not core to the organisation, as in the case with preventing malware and other exploits from damaging resources, it makes sense to consider outsourcing capabilities to experts that have the necessary resources and systems in place to provide a secure service at a compelling price.

Certainly the cloud has this potential of taking organisations to the next level. Similar to an airplane, a cloud can enable businesses to soar to its destination with greater speed and efficiency as opposed to driving a car or riding a sailboat using the traditional IT environment. Although riding a plane will involve some risk to life and has costs to consider, they are calculated risks that we are willing to take because we are well informed. It's the uncertainty of not knowing that puts us in the state of fear. Our ability to cope with risk lies on our ability to learn. Our ability to learn and understand change is the means to bridge the gap and finally take advantage of this new technology within risk tolerances that the business understands and accepts.



Document Automation Experts

+61 1300 378 836 (Australia) | +44 203 355 1237 (UK)
+1 (213) 291 0523 (USA) | +63 2 817 4901 (Philippines)
info@redmap.com | www.redmap.com