GILLIAM SECURITY

Security through Cloud or On-Premise?

Where the cloud came from and understand how it is beneficial and detrimental.

One of the most common techniques of vendors is to immediately up sell going to the cloud; however, is the cloud always the best choice?

To understand the true benefits of the cloud, one must first understand what the cloud is. Often this is alluded to a mega-structure with Fort Knox style security as well as availability that promises your infrastructure to never be hacked or to have an SLA of 99.999 Percent (or no more than more than 26 seconds a month of planned downtime). As one who grew up as an using on-premise infrastructure and now using cloud, it is important to really understand its benefits before jumping to the mysterious cloud.

That said, let's understand what cloud is, what benefits it reports to have, whether you should use it or not, and what the gotcha is from lessons learned. Before you stop reading, know this article take both an IT, information security and business approach to explaining the cloud.

What is Cloud?

Cloud is simple. Simply put "Cloud" is data centers on the internet that belong to others, by which you have the benefit of being able to use. By now, tomatoes are being thrown because of user citing no it is high availability, it is scalability, etc. Yes, that is true; however, those are the results of certain features one elects to have within cloud. The cloud actually started with the advent of the internet via ARPANET. ARPANET was the first computer network that eventually led to the internet. ARPANET was used by the government and research institutions.

Let's fast forward. So AWS was the first cloud provider, or was it?

In short, No. Recall cloud is data centers on the internet that belong to others. One of the pioneers in the IT industry prior to the word "cloud" was coined was H. Ross Perot. Perot started a company called Electronic Data Systems (commonly known as "EDS"), that would later be acquired by General Motors, Hewlett-Packard, Hewlett-Packard Enterprise and recently DXC Technology.

Perot's business model was based on mainframes. Mainframes may not be the fastest but they handle a lot of data and typically have cycles to spare when not being used. This was the birth of the "Cloud" as organizations now were able to outsource their processing to others when the mainframes were not in use.

So where does information security come into play?

So we know we are using the data centers of others and that we are using CPU cycles not used by others. How secure is that really? Modern client-server architecture does have much more security than its mainframe predecessor but also has a lot of drawbacks that one needs to understand before committing to a SaaS, PaaS, or IaaS. Trust me there are acronyms for every type of service but let's keep it simple. Let me explain those acronyms and we can explain the others later.

- *SaaS, meaning "Software as a Service"*

  This is perhaps the simplest version of cloud today. You pay for a software and you get access to it. You are also paying for security, availability, and performance.

  The security concern comes into play in that you are surrendering yourself to the security posture of another. You do not have capability to do penetration testing, firewall rules, VLANs, etc.

  One of the key considerations in this space is to understand what the tenant architecture is to understand what your exposures are should a security incident take place. It is also pivotal to

understand the downtime and SLA, as you will not have access to the software if the host is down.

For example, if an SLA of 99.999 Percent is in place with a downtime of 6 PM to 6 AM ET, and you have a follow the sun cycle, your worker on the west coast of the United States and abroad will most likely be unable to work if their job requires use of the job.

Secondly, as far as a security incident goes, your organization will be at the mercy of the provider to have the appropriate controls in place to know if an incident took place and whether they have the knowledge to know how to inform you of it.

- *PaaS, meaning "Platform as a Service"*

  This is similar to SaaS in terms of where the software is and what the SLA is; however, you are able to play with the software more. One of the key benefits to a PaaS is an organization can start to utilize an Application Programming Interface, commonly known as an "API", to interact with the application as well as code parts of the software and in some cases deploy it to your organizations own cloud, commonly known as "private cloud." In some cases, your organization can bring this software back on premise.

- *IaaS, meaning "Infrastructure as a Service"*

  Let's keep this simple: you are leasing another one's servers and data center space. This is great for three things: expense, scalability and disaster recovery.

  Why expense? An organization can pay for what infrastructure is used and nothing more. Financially this can be bad as it is all an operational expense since you are not depreciating the cost.

  Why scalability? To the point above, you are paying for what you use. For example, if you are launching a new brand at the super bowl, you may need a thousand servers to handle all your web traffic and then the next day you may only need one-hundred. You are only paying for what you use.

  Why disaster recovery? At the very beginning, I mentioned other company's data centers. With this approach you can have your applications at the ready to deploy across multiple geographies in the event something with your primary location goes wrong. This is similar to the on-premise way of thinking "hot site," "warm site," and "cold site."

Before you jump over to the "Cloud," your challenge needs to be understanding the security of the organization that will host your organization's software and information. As part of this, understand if that organization's risk tolerance aligns with your organization's risk tolerance. Secondly, understand where your data is. If your data is stored in California but your entire risk and compliance program is not built to meet these requirements, your organization will need to add this to its scope as the data is now resting in California.

At an estimated $180 / record to recover from a breach, it may not always make sense. Additionally, one could have several other expenses that may not have been thought of including the retraining of resources, the displacement of resources no longer needed, the need for a bigger compliance function, the need for more security tools to monitor the organization's network boundary as the cloud is now part of your boundary, and so much more!

Sound scary? Contact Gilliam Security via the Contact Us form on the Contact Us page and we would be glad to help you out to understand if cloud really gives you the benefits you desire as well as the maintenance, or enhancement, of your information security posture.

Why Gilliam Security?

Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.

Contact Us Today at sales@gilliamsecurity.com