CIO Decision Series

In this Guide

CIO decisions - Choosing the Right Cloud for Your Business

Choosing which type of cloud deployment is right for you depends on many factors, including the industry your organization is involved in, the regulatory requirements it may be subject to and even the type of customers you have, as well as the key benefits you wish to reap.

CIO decisions – Should I out source my datacenter?

How much is too much? It's hard to say – especially with datacenters. It's a subject that has troubled CIOs who have over-provisioned in the face of soaring business demands and need to cut costs at the same time.

CIO Decisions - Tips for choosing a Managed Security Services Provider (MSSP)

According to research and advisory firm Gartner Inc., at most companies, the staff responsible for IT security functions is also responsible for other activities and spends most of its time on non-security projects. For any resource-constrained organization, the added responsibility of managing security is often just too taxing. Gartner has concluded that in-house teams struggle to understand and defend against the latest security threats because this requires constant system monitoring – something that few businesses can afford.

CIO decisions - Choosing the Right Cloud for Your Business

Choosing which type of cloud deployment is right for you depends on many factors, including the industry your organization is involved in, the regulatory requirements it may be subject to and even the type of customers you have, as well as the key benefits you wish to reap.

The benefits of cloud computing services can be very valuable, and include reduced IT costs, optimized resource utilization and greatly enhanced operational agility. Before deciding to pursue a cloud strategy it is vital to establish which type of cloud would be best for your business: a public cloud, a private cloud or a hybrid cloud.

In a public cloud, the cloud infrastructure is located in one or more external datacenters, owned by a service provider and shared by multiple customers. Since the infrastructure is very large, public clouds provide practically unlimited scalability on demand.

By contrast, private cloud infrastructure service is used exclusively by a single organization. In most cases the infrastructure is also owned by the organization and can be located and managed in a corporate data center or an external datacenter.

As the name suggests, a hybrid cloud is a combination of private and public cloud. Data and applications can be moved from one cloud to another when necessary – for example workloads can be moved from a private to a public cloud to provide extra capacity during periods of high demand.

Public, Private or Hybrid? Which One is Right for You?

Public clouds

One of the important benefits of a public cloud is that it involves very limited up-front capital costs. That is because your organization pays only for the resources that it consumes, on a monthly basis, scaling workloads up or down and provisioning new services on demand. A public cloud allows your company to benefit from the economies of scale of a shared infrastructure and the expertise of specialist staff employed by the service provider.

One of the major drawbacks to the public cloud model for some organizations is that infrastructure is shared between customers. Many organizations worry about this from a security point of view, although it is not clear that using shared infrastructure in a public cloud managed by a suitably security-aware service provider necessarily poses a greater security risk than keeping IT operations in house.

Private Cloud

A public cloud implementation may not be practical if your company holds data that is governed by regulations such as PCI, HIPPA or FISMA, or if regulatory or legal requirements dictate that you carry out highly detailed logging of access to data or require data access to be limited using specific authentication methods such as hardware tokens.

A private cloud overcomes the problems of security and regulatory compliance associated with public cloud deployments and also enables you to run any specialist applications you want, but it does so at a price. Owning and managing your own cloud infrastructure means that you will incur up-front capital costs while building the private cloud. And while a private cloud can provide operational agility by enabling you to provision applications on demand and scale workloads up and down rapidly, you won't benefit from the virtually limitless instant scalability that a public cloud can provide. You will also be responsible for maintaining a suitably skilled IT staff and making arrangements for contingency planning in case of a disaster.

Hybrid Clouds

Hybrid models allow you to leverage the advantages of both public and private clouds by placing the more common, less regulated applications and services into the public cloud while keeping legacy, or performance

sensitive applications in a private cloud. Several service providers offer this kind of functionality.

Many industry experts believe that the hybrid cloud model is the one that will emerge as the most popular in the long term, offering a combination of high levels of control and security, with access to virtually unlimited extra capacity on demand, paid for only when needed. You can take advantage of hybrid clouds to provide “cloud bursting” capabilities: additional capacity during demand spikes that may coincide with occasional events such as a new product launch or a particular promotion, or to provide additional capacity for specific workloads for longer periods until it makes sense to purchase new equipment and implement it in-house.

In order to make the best decision in this matter, you should define the top priorities are for your company. Do you need to control the infrastructure? Then private cloud is your best option. Are you most interested in reducing costs and having an easy way to access your resources, in a utility based model? Then public cloud might be the answer for you.

CIO decisions – Should I outsource my datacenter?

How much is too much? It's hard to say – especially with datacenters. It's a subject that has troubled CIOs who have over-provisioned in the face of soaring business demands and need to cut costs at the same time.

More and more frequently, the balancing act brings CIOs to one question: should they build and maintain their own datacenters or let others run it to help manage costs and enable growth?

The current slowdown is pushing more CIOs towards evaluating an outsourcing strategy. Only half in jest, one CIO says that in a time of crisis, even God outsourced the building of the Ark to Noah. By turning to managed hosting services, CIOs hope to better control capital and operational costs while enabling their organizations to be more agile to address changing market scenarios.

While the datacenter is crucial to the operations of your business, you should be cautious of allowing it to take precedence over other business operations. Unless your company is a datacenter services provider, you should consider outsourcing your datacenter. Building a datacenter requires time, space, resources and competent staffing. A datacenter should run 24/7, which means staffing it around the clock. By paying someone else to host and manage your servers, networks and other computer equipment, you free yourself to focus on the core functions of your business.

There are many benefits of outsourcing datacenters. Some of the more important ones include:

Scaling on-demand:

Depending on how fast your business grows; you may need to scale-up your IT infrastructure to meet demand. If the business slows down, it means scaling down the same to avoid wastage. This can be expensive and time consuming for you if you are managing the datacenter on your own. When you out source, you use as much or little resources as your business requires on the go. You get to enjoy this scaling flexibility without impacting your capital investment, what is referred to as capital expense in the industry.
Enjoy purpose-built infrastructure:

Because a datacenter provider operates as an Infrastructure-as-a-Service (IaaS) company, they are able to set up highly redundant facility infrastructure that meets all the requirements of an efficient and highly available datacenter. Other important components of an outsourced datacenter are:

- Fire suppression technology to prevent data loss due to fires.
- Guaranteed security. Both on-site surveillance and authentication systems ensure that only authorized persons can access your networks. These systems are constantly improved to counter new hacking techniques.
- Constant system upgrades at little or no cost. IT Infrastructure components get outdated and obsolete quite fast. The IaaS Company you are using has the capacity to change hardware and systems in line with changes in technology without affecting your business.

Reduced cost of operation:

A good hosting service provider should help you save between 1/3 and ½ of your total datacenter operation costs or more. When you factor in the amount of money you would spend on upgrades every year, it becomes clear that the expense is unnecessary, especially if you can enjoy high quality and redundant outsourced services for less. Datacenter companies charge a fixed rate for the duration of the contract, billed as operational expenses or OpEx. This rate is inclusive of upgrades and all other services, unless otherwise stated in the contract.

Guaranteed Connectivity and Increased Bandwidth:

Outsourced datacenter connectivity provides greater redundancy, which ensures that your applications are always accessible. In addition, you enjoy burstable bandwidth, which ensures that your availability is stable even when there is a spike in demand.

So are you looking at outsourcing your datacenter? Considering the numerous business benefits that it has to offer, taking a decision to out source should not be so difficult. If you are still concerned about trusting a datacenter provider with your mission critical business applications, please drop a note and I will get back to you.

CIO Decisions - Tips for choosing a Managed Security Services Provider (MSSP)

According to research and advisory firm Gartner Inc., at most companies, the staff responsible for IT security functions is also responsible for other activities and spends most of its time on non-security projects. For any resource-constrained organization, the added responsibility of managing security is often just too taxing. Gartner has concluded that in-house teams struggle to understand and defend against the latest security threats because this requires constant system monitoring – something that few businesses can afford

For those IT staffs that take on the task, the challenges are daunting. After all, this normally entails formulating a security policy and implementing firewall, intrusion detection, virus detection, and other security technologies. But even after taking these steps, the challenge remains of how to manage the security effort. Security, after all, isn't static, and enterprises must be prepared to proactively monitor, maintain, and upgrade their network protection.

The bottom line: maintaining the necessary vigilance in these days of “zero-day” attacks requires significant investments in staff, IT systems, and training.

The alternative is for enterprises to outsource the management and monitoring of their security to a Managed Security Service Provider (MSSP). An MSSP can combine advanced technology with expert human analysis, enabling an enterprise to cost-effectively strengthen its security posture. An MSSP can also provide a level of technology and expertise that ensures rapid response to real threats or “defense in depth”.

Increasingly, enterprises are recognizing the importance of “defense in depth.” This involves a comprehensive approach to securing critical assets, networks, and information systems while implementing robust defenses against hackers, viruses, and other online threats. Defense in depth recognizes that today's environment is one increasingly beset by so-called blended threats that dynamically target the vulnerabilities of isolated security products. As a result, companies must adopt a deep, integrated strategy that addresses security at all tiers: gateway, server, and client. It is precisely this kind of strategy that an MSSP can help enterprises execute.

So how should an enterprise go about choosing an MSSP? The following criteria should be considered:

Longevity

Entrusting sensitive corporate data to a third party is not a decision to be taken lightly. When partnering with an MSSP, invest the time and resources to ensure that the service is addressing your organization's most critical needs. As a result, special emphasis must be placed on choosing a partner that has a proven track record of delivering quality security services to a broad range of industry sectors over a long period of time.
Real-time analysis and response

An MSSP must have the ability to accurately correlate, analyze, and interpret large volumes of network security in real time. It must be able to separate real security threats from a spate of “false positives.”
State-of-the-art facilities

An MSSP should have multiple security operations centers, or SOCs, that run 24×7x365. Having two or more SOCs allows for cross-monitoring, ensuring constant compliance with security standards. They can also provide backup in times of disaster.

Global intelligence

An MSSP should have security experts positioned to monitor and analyze threat data from security vendors and customers around the world. This global

intelligence enables an MSSP to issue real-time alerts and recommend actions to be taken in a timely fashion.

Annual revenues

What is the prospective MSSP's financial status? For publicly traded companies, Gartner estimates that annual run rates of more than $10 million (convert this to INR) per year in managed security services contracts indicate a sufficient base of revenue to support growth and enhancement of services.

Management experience

For leading MSSPs, management experience will include backgrounds in military, security vendors and government.

Breadth of services

This key consideration indicates an MSSP's ability to meet the security management needs of a wide variety of companies. It includes real-time monitoring and management of firewalls, intrusion detection systems, virtual private networks, and other security products.

Security management processes

An MSSP should be able to provide documented standards and policies for handling typical and atypical operations and threats. An MSSP should offer a variety of attack alert notification methods to allow customers' staff the ability to mitigate risk in real time.

Vendor neutrality

An MSSP should employ security specialists with certified expertise across a broad range of security products from a variety of security providers. This allows a company the freedom to select best-of-breed solutions.

Auditing

While trust is one of the most important factors in selecting an MSSP, the vendor must have facilities, processes, and procedures in place that are validated and certified by a third-party auditor.

Reporting

Reports provided by MSSPs should be detailed enough to support decisions to enhance security efforts and to determine the cost-effectiveness of the managed services. Thorough reports will include information gleaned from the managed devices, recommended responses, any changes the MSSP made to the devices, and information about the latest threats. In addition, enterprises are increasingly reacting to legislation that will entail stringent compliance reviews. An MSSP should therefore be in a position to consolidate and analyze security log data.

All organizations can benefit from the continuous management and monitoring of their security operations. In this regard, an MSSP can help develop a company-wide security policy that sets appropriate access control rules governing all employees. This is essential because it recognizes that the majority of security breaches come from within. (Most MSSP contracts include monitoring of all security-related activities on the internal network.) Before signing on with an MSSP, make sure all employees are aware of the corporate security policy and what the MSSP is contracted to do.

Conclusion

Managed security services can remove the volatility associated with IT staffing and the need to respond to unpredictable network threats, allowing enterprises to better manage their day-to-day business requirements, resources, and costs. This is especially important today as threats increase in severity and complexity. Enterprises that are seriously considering outsourcing their security should know that this can be a smart business decision, as well as one that assists them as they face new reporting requirements.