STAYING SAFE IN THE CLOUD

ADDRESSING SECURITY CONCERNS WITH **CLOUD-BASED DATA SYSTEMS**

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

The traditional view on data security is that it is best served by maintaining direct control over both the data and the hardware on which the data resides. This view is likely responsible for the persistent idea that cloud-based solutions are inherently less secure than a company's own proprietary data center. While this may once have been true, cloud services have come a long way since their inception.

In many ways, modern, cloud-based solutions can be more secure than company-owned data centers. Nowhere is this more apparent than when considering today's mobile workforce. In the old days, employees traveled to work. Today, work travels with them. Many employees work from home or from the road; they need to access their data to do so. Provisioning that type of service securely from a company-owned data center would be prohibitively expensive, if not impossible. It is only thanks to the availability of specialized cloud services that reliable, secure, mobile access to data is even a possibility.

The business world is often compared to a war zone. If business is war, then it is no longer enough to build a fence around the perimeter and watch for the enemy, guns at the ready. Instead, the data itself should be armored against threats before it is sent onto the battlefield. Given the authorization, encryption, and authentication requirements to do that however, it is much more cost effective to rely on the expertise of cloud services providers who specialize in providing exactly those skills.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

Making use of cloud services for business critical computing is not a foregone conclusion, however. Before making a decision on whether to go with company owned data services, or a cloud-based solution, it's important to carefully consider the security implications of both.

THE PROS AND CONS: PREMISE-BASED VERSUS CLOUD-BASED COMPUTING

There are advantages and disadvantages to both approaches. While cloud-based solutions might be the better fit for most businesses, there are cases when a premise-based approach makes more sense —particularly when it comes to business-critical computing.

PREMISES-BASED

- Dedicated computing power and capacity
- Dedicated storage
- Simplified security, budgeting, and provisioning
- Lacks mobility
- Requires over-provisioning against contingencies

CLOUD-BASED

- Scalable storage and computing capacity
- Delivery of data and applications wherever needed
- Private cloud solutions alleviate the need for restructuring
- Security risks in application and network layers

In terms of security, the difference between premise-based and cloud-based solutions can be reduced to the idea that cloud computing offers flexibility and

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

mobility, while premise-based computing sacrifices those attributes in favor of a simpler security apparatus. While cloud-based security is by necessity more complex, the level of complexity depends on the type of cloud solution used.

PUBLIC CLOUD, PRIVATE CLOUD, OR A COMBINATION?

Cloud-computing options are generally divided into three areas; public cloud, private cloud, and hybrid cloud. In the public cloud, computing infrastructure is shared between all clients, and service level agreements are very rare. With private cloud solutions, each client has sole use of the computing hardware, which is designed to conform to the requirements of an SLA.

Generally, public cloud solutions provide flexibility and ease of deployment, while private options often have better security. There is a growing trend towards hybrid solutions. The hybrid cloud leverages the advantages of both the public and private cloud, while minimizing the disadvantages of each.

THE PRIVATE CLOUD OPTION

Similar to a premise-based data center, the private cloud provides greater control over all security options, but can be prone to over-procurement of resources.
The private cloud is not the same as a premises-based data center though.

One of the key advantages a private cloud option has over running a premise-based data center is that it allows you to start taking advantage of the cloud's flexibility without the need to overhaul existing systems.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

A key benefit that the private cloud has over the public cloud is its ability to help companies in industries with tight regulatory data compliance needs. The level of control necessary in these industries can make the public cloud unfeasible.

When moving to a private cloud solution, there are a couple of points to keep firmly in mind when choosing a provider. Ideally, the provider should allow you to implement and manage your own network security. Just because the machines are in someone else's hands doesn't mean control of those machines should be. Also, it is important to check what OSI level connections a provider uses. All the main connections should be at least layer 2 to avoid needless complexity and enforce network isolation.

THE PUBLIC CLOUD OPTION

When businesses say they are worried about security in the cloud, it's the public cloud they are referring to. While it's true that businesses that use public cloud solutions have little or no visibility into the underlying infrastructure or its users, lack of visibility does not mean lack of control. Public clouds can be almost as secure as private clouds—but it does take a bit more work. Security in the public cloud has to be implemented at a very granular level, and consistently throughout the network.

The biggest issues to pay attention to in a public cloud environment are provisioning of adequate firewalling, QOS, and DDoS mitigation measures. Public cloud providers don't usually take care of this; businesses using

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

the public cloud must do so. The other main issue, and probably the most important, is ensuring the use of robust authentication and security controls. Since businesses can't control who knocks on the door in the public cloud, it's better to know who is knocking before you open it.

THE HYBRID OPTION

A hybrid approach can be the perfect option for businesses to address issues like unpredictable computing resource needs, a desire for the enhanced security control of private cloud solutions, and the desire to pursue aggressive testing and development of new processes without sacrificing business continuity.

By mixing of both types of cloud, the hybrid approach allows a business to transition more easily from a traditional data center model to a cloud-centric one. In order to prevent the lower security level of the public cloud from breaching the higher one of the private cloud, all traffic between the two will need to be encrypted, and an identity-based authentication system is a must.

When choosing a hybrid provider, a business should make sure the provider allows users to use the business's existing tools and vLAN topology. It is also important to make sure the provider offers flexible resource usage. A properly implemented vLAN on a layer 2 connection allows connections to both private and public clouds while keeping both networks safely separated. The primary advantage of the public cloud element is that business's only pay for the resources that are used.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

WHAT ABOUT COMPLIANCE?

Many industries are bound by industry and governmental regulations regarding data compliance. For certain businesses, the ability of a cloud provider to comply with those regulations can make a crucial difference in choosing a provider. While every business will have different needs with respect to compliance, qualities to look for in a provider include the ability to make HIPAA Business Associate Agreements and whether the provider maintains third party compliance auditing.

Other questions to ask include whether the provider will accommodate unique security needs. At the end of the day, compliance or non-compliance is the responsibility of the business. It's vital to make sure a cloud provider can address business needs in that regard.

IDENTITY: THE CORNERSTONE OF CLOUD SECURITY

From a network mapping standpoint, a cloud-based data system can be a crazy-quilt of different nodes and connections. While these can be incredibly complex and difficult to understand from a technical perspective, the user's perspective needs to be simple and unified. That means that even when using a variety of different applications in a variety of different locations, the user needs to experience a consistent login and usage experience. One password for everything.

The way to achieve this is to base users' access to data and applications according to the user's identity rather than location or device. Thankfully, this is relatively simple to do in a cloud based system and has advantageous

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900com

ENTERPRISE VISIONS
DIGITAL TRANSFORMATION SIMPLIFIED

roll-on effects in rapid provisioning and de-provisioning of resources on a user by user or group basis. Adequate identity management tools are vital to a successful and rewarding cloud computing experience.

There are a number of powerful and flexible identity management tools that can be used effectively in a cloud environment. Secure file sharing tools allow data to be used where it's needed without compromising compliance. Single sign-on protocols are quite easy to implement in the cloud, and still allow for multi-factor authentication where required or desired. With everything keyed off of user identity, it becomes trivial to initialize access to new applications, modify access to existing applications, or provision applications for new users.

CONCLUSION

For businesses to stay competitive, flexibility, mobility, and the ability to react to changing conditions is key. However, those qualities can't come at the expense of security. Thanks to modern cloud services providers, trading security for capability is no longer an issue. Businesses can choose exactly the right type of cloud service to get the perfect balance of flexibility and security.

Enterprise Visions – Twin Cities Office
1030 West County Road E Suite 150
St Paul, MN 55126
651.450.7900