Broadview NETWORKS®

Seven Questions to Ask Any Cloud Vendor

Seven Questions to Ask Any Cloud Vendor

Are you ready to move your business to the cloud but have concerns about keeping your company's data secure? Regardless of where your company's data lives, you face security concerns, but there is much more risk involved when housing your data on site. When done right, the cloud offers you more security than you could achieve on your own, even with in-house systems and staff.

The trick to knowing that your data is secure in the cloud is to ask the right questions of your potential cloud vendors.

In the recent InfoWorld article "Gartner: Seven Cloud-Computing Security Risks," Jon Brodkin highlights what technology analyst and consulting firm Gartner considers to be the top security concerns that companies face when moving to the cloud. Getting answers to these questions will help you avoid common security pitfalls.

Many companies considering implementing cloud-computing services raise concerns regarding the security of data, such as theirs, that is stored and accessed via the Internet.

According to Gartner's report "Assessing the Security Risks of Cloud Computing," cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing." No matter how large or small your business, protecting your company's livelihood (customer and prospect data, proprietary information, critical business apps, etc.) should always be #1 on your "Security To-Do" list.

Gartner lists seven security issues to bear in mind when considering a particular cloud vendor's services:

1 *PRIVILEGED USER ACCESS*

Enquire about who has access to data and about the vendor's hiring and management of such administrators.

If you are entrusting your company's data and/or business applications to a cloud vendor, then you have a right to know who at that company can access your data. Gartner recommends that you "[ask] providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access." Offsite data protection provided by a trusted cloud vendor is easier to manage and costs less than protecting your data on site, but the key term in the relationship between a vendor and customer is "trust." While some data loss is the result of a natural disaster or hardware failure, other data loss is simply due to human error. Therefore, when you're choosing a cloud vendor, it's essential that you feel comfortable with the administrators that they hire to manage your company's sensitive data.

Offsite data protection provided by a trusted cloud vendor is easier to manage and costs less than protecting your data on site

If you choose to host your data and/or applications in Broadview Networks' cloud-computing data centers, you can rest assured that only privileged administrators are granted access. As well, full-time security guards are stationed at the entrance of all of Broadview data centers.

2 *REGULATORY COMPLIANCE*

Make sure the vendor is willing to undergo external audits and/or security certifications.

With its low barrier to entry, the cloud-computing market is flooded with new service providers, who are all vying for your business. Again, companies need to consider that not all cloud vendors, especially new market

entrants, adhere to the same stringent security audits. Gartner cautions companies searching for a cloud vendor, warning that cloud-services providers who refuse to undergo security audits are "signaling that customers can only use them for the most trivial functions."

Establishing a certain level of trust with your cloud vendor is not enough to ensure that your company's sensitive data is being guarded by a reputable service provider. Luckily, you don't have to rely on trust alone; there is a regulatory agency that scrutinizes and verifies a cloud vendor's data-storage practices so that you have peace of mind.

The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) developed a certification that verifies whether a cloud-services provider has been through an in-depth audit of its control objectives and control activities, which include controls over information technology and related processes.

Look for cloud vendors who have demonstrated that they have adequate controls and safeguards when they host or process data belonging to their customers. These cloud vendors operate data centers that are SAS 70 Type II certified by the Auditing Standards Board of the AICPA.

Look for cloud vendors who have demonstrated that they have adequate controls and safeguards

All of Broadview's cloud-computing data centers have been SAS 70 Type II certified by the AICPA and, in 2012, will be updated to the next security level, SSAE-16.

3 DATA LOCATION

Ask if the provider provides you with the control over the location of the data.

Generally speaking, security is usually improved by keeping data in one logically centralized environment rather than in disparate locations, including laptops, desktops and USB devices. In SAS 70 Type II-certified data centers, security is typically better than in traditional systems, in part because cloud-services providers are able to put advanced management, security, redundancy and control systems and practices in place that many organizations may not be able to cost justify.

Storing your company's data in an SAS 70 Type II-certified data center provides some security against irretrievable data loss, but not complete security. Look for a cloud vendor whose data centers are geographically dispersed, have multiple carrier access to the Internet and have backup forms of power, should the primary source go down. In essence, one data center is not enough. True data-center redundancy is only achieved by those cloud vendors who have multiple data centers located in different geographic locations; this ensures that if a natural disaster destroys one data center, your company's data is safely stored in your vendor's other data centers.

Look for a cloud vendor whose data centers are geographically dispersed, have multiple carrier access to the Internet and have backup forms of power, should the primary source go down.

Broadview's cloud-computing infrastructure exists in a distributed-data-center design, such that there is no single point of failure and all data is mirrored between geographically separated data-center locations. Each data center has multiple electrical grids, battery and diesel power backups, and multiple carriers using dual-entrance facilities. Each data center is also SAS 70 Type II audited, providing independent third-party verification of its control over all aspects of data-center operations. This ensures that equipment, communications, physical access, personnel screening and infrastructure are all secure and meet the highest commercial standards.

4 DATA SEGREGATION

Make sure that encryption is available at all stages.

According to Gartner, "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability." What is Gartner's advice? "Find out what is done to segregate data at rest." Your cloud vendor should be able to prove that its "encryption schemes were designed and tested by experienced professionals."

What many people don't realize is that credible cloud vendors adhere to strict privacy policies and sophisticated security measures, with data encryption being just one example. Companies moving to the cloud can choose to encrypt data even before storing it on a third-party provider's servers. Thus, many cloud vendors offer their clients greater data security and confidentiality than companies that choose to store their data in house. However, not all vendors offer the same level of security.

Many cloud vendors offer their clients greater data security and confidentiality than companies that choose to store their data in house

Broadview understands the regulatory pressure that is placed upon companies who must ensure that their data is secure. That is why Broadview provides TLS (Transport Layer Security) encryption of data at all stages.

5 RECOVERY

Find out what will happen to data in the case of a disaster: does the vendor offer complete restoration, and, if so, how long would that take?

Do you know how much money your company would hemorrhage if data were lost? It's probably more than you think. Dr. David Smith of Pepperdine University estimates in his report entitled "The Cost of Lost Data" that a single lost megabyte could cost your company upwards of $10,000. Now ask yourself if that is a risk your company is willing, or can afford, to make.

If you prefer to play it safe and store your data in a cloud vendor's secure data centers rather than on your own premises, then Gartner advises you to search for a vendor who replicates data across multiple, geographically dispersed data centers. Your cloud vendor should tell you not only where your data is being stored but also what steps will be taken to recover your data in the event of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. The firm recommends that you ask your cloud-services provider if it has "the ability to do a complete restoration, and how long it will take."

Your cloud vendor should tell you not only where your data is being stored but also what steps will be taken to recover your data in the event of a disaster

Because Broadview's cloud-computing data centers are geographically redundant, a client would be restored in one to four hours in the unlikely event that one site goes down.

6 INVESTIGATIVE SUPPORT

Inquire whether a vendor has the ability to investigate any inappropriate or illegal activity.

Not all cloud vendors have the ability to investigate inappropriate or illegal activity. Gartner suggests this precaution:

"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."

Broadview's services include the ability to be "Compliance Officer Ready," meaning that company investigators and administrators can filter messages for keywords and other indicators in order to look for inappropriate and potentially illegal activity.

LONG-TERM VIABILITY

Ask what will happen to data if the company goes out of business.

Retrieving your data from a cloud vendor that has gone out of business can be an ordeal, so the safest route may be to to trust a proven incumbent. Thus, be prudent and exercise due diligence by thoroughly researching a prospective cloud vendor's financial statements. Find out how many years the company has been in business, how many customers it has and how long it has been providing cloud-based services. By choosing to store your data with a financially sound, reputable and experienced cloud vendor, you will avoid any data loss that may ensue due to a provider having to close its doors.

Gartner advises, "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application."

Even if the cloud provider your company chooses is financially stable, you should still know how you will be able to retrieve data if, for any unforeseen reason, it must shut down. Gartner advises, "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application."

Broadview Networks has been in business for over fifteen years, and has thousands of business customers across the country. Broadview is committed to staying ahead of the technology curve and to investing heavily in our cloud-computing infrastructure.

Conclusion

While there are inherent risks with almost all IT decisions, choosing a credible cloud vendor that can address all your security concerns will help you to mitigate these risks. Again, the risks far outweigh the benefits your organization will receive by moving to the cloud.

Moving to a cloud-computing model can help your organization survive in a tough economic climate by equipping you with the latest business tools and by giving you access to advanced technologies at a fraction of the cost of purchasing and running the same systems in house. Check that your provider can deliver the level of security and quality of service you require, and before you know it, you'll be able to enjoy the organizational benefits and competitive advantages of cloud computing.

About Broadview Networks

A fundamental shift is underway as organizations migrate away from capital-intensive and rigid information technology infrastructures to more flexible environments that improve availability, productivity, flexibility and security, while reducing the overall cost of ownership. According to analysts, 75% of companies will be using enterprise-class cloud-computing solutions within five years .

Broadview Networks is enabling these organizations to embrace the shift to cloud-based services on their own timetable, with the experience, support and knowledge required to make the transition seamless. Broadview Networks is the premier information technology and communications partner for businesses across the country. Our all-encompassing approach allows companies to concentrate their efforts on running their business, not their IT environment or communications infrastructure.

Every day, tens of thousands of businesses rely on Broadview Networks for their mission critical communications and IT needs. Broadview delivers cloud computing productivity software including hosted versions of Microsoft Office®, SharePoint® and Exchange®, hosting for all of a business's applications, a full suite of cloud-based managed network security applications and desktop and server data backup services. It also provides a patented hosted IP phone solution, data networking applications including VPN- and MPLS-enabled services, high-speed Internet access services, as well as traditional local and long-distance voice communications and other related services. Broadview also provides its customers with new levels of transparency through its award-winning eCare Enterprise customer service portal and can even help organizations make it all work together with IT and professional services.

What's Your Cloud Strategy?

To develop your plan, contact your Broadview Networks representative, or call *1-800-BROADVIEW*.
www/broadveiwnet.com/cloud

Broadview NETWORKS®

1-800-BROADVIEW | *www.broadviewnet.com*

Sources:
http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
http://www.gartner.com/DisplayDocument?id=685308
http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/