Public clouds, private clouds and your security

The world is becoming increasingly interconnected; we've seen one example of this in how events in the US financial markets reverberated across the globe. But something else is happening too; the planet is becoming smarter. That is, intelligence is being infused into the way the world literally works—into systems, processes and infrastructures.

And a smarter planet requires businesses to think differently about the IT infrastructure they will need to respond to market forces and the pace of business and society. Companies of all sizes will begin to utilize more adaptive capabilities like cloud computing to deliver new services with agility and speed, while driving down costs.

But while cloud models provide rapid and cost-effective access to business technology, not all of these services provide the same degree of flexibility or security control. How does cloud computing fit with your company's security policies? Understanding the differences between private and public cloud computing models can go a long way in getting the most out of data—and securing it.

Security in the public cloud model

The reason public, Internet-based cloud computing has become so attractive is hardly a mystery. Thanks to the proliferation of mobile devices, high-speed connections and data-intensive applications, many organizations find it difficult to continuously meet the demand for more computing power. For end users, cloud computing often means browser-based interfaces that allow IT to be ordered and accessed almost immediately. For businesses, the pull of cloud computing can be found in radically reduced costs.

Data protection shouldn't be watered down just because technology is available on tap, says Phil Hochmuth, senior analyst at research firm Yankee Group, who notes that using browsers to access IT can substantially change security plans and considerations. "Once you move your core applications into a cloud-type scenario, all you really have as an interface is a Web browser, which makes access control and password management and identity management incredibly important," he explains. "You're not securing pieces or chunks of the network anymore. You're securing the end user—how they access the network and what they do once they're on. You're really entrusting the provider with a lot—make sure that they can provide best practices for access management and identity management."

"You're securing the end user—how they access the network and what they do once they're on."

With next-generation identity management tools, Hochmuth says, data can remain inside an organization, and be accessed only by the right people. Hochmuth suggests that companies select a cloud provider that offers best practices for access management and identity management. If the cloud provider is capable of handling security for multiple users, midsized companies can enjoy comprehensive data protection in addition to faster and less-expensive IT provisioning. And, as he points out, specialization in IT delivery often makes cloud providers better suited to delivering and securing applications.

Powering a dynamic infrastructure through cloud computing

Leveraging cloud computing is one way midsized businesses can enhance their IT infrastructure to be just as dynamic as today's business climate. And a dynamic infrastructure can be managed on-site, remotely or totally outsourced.

The cloud computing model enables access to needed, standardized IT resources without re-engineering the entire infrastructure–or, in some cases, without having an infrastructure at all. But some concerns about the suitability of public clouds for highly sensitive data are valid, says Hochmuth.

In most organizations, data protection levels vary depending on the use of technology. Familiar software applications for general business use—such as scheduling and productivity software found in Google Docs, IBM® LotusLive and Salesforce.com—are rarely seen as being as critical as databases or programs that hold sensitive information specific to an individual business.

But when a cloud environment is created inside a firewall, it can provide users with the same rapid access to IT as the public model, but with less exposure to Internet security risks. This can often make private clouds more appropriate for specialized programs and systems unique to organizations with extremely sensitive data that must be protected.

Private models also provide more control than public clouds, where the provider usually acts as a landlord renting out applications to multiple user tenants. Vendors of private clouds, however, typically provide extra storage capacity for technologies that their clients already own.

Automated security protects data in new cloud models

However, software and systems that are accessed through private clouds rather than public Internet connections make it easier for existing security measures and standards to remain intact. Hochmuth says that as a result, "in terms of very sensitive data—handling customer data or medical records and things like that—private clouds are starting to be something that is gaining more interest."

To be sure, removing the Internet from the IT provisioning equation helps secure data, but in order for private clouds to effectively protect data, a number of safeguards also must be in place. As Hochmuth notes, any cloud computing model changes the way data is accessed, and private clouds must have safeguards in place to protect an organization's most critical and sensitive data. But with automated tools for identity and password management that typically accompany provisioning tools in a dynamic infrastructure, organizations can set standards and policies—and spend either less or no time on securing IT.

Mixing and matching to meet security needs

Still, Hochmuth says that companies now often use a mix of cloud models, depending on how critical data is for particular applications and uses. Public clouds, he says, are often a wise choice for a number of activities and situations, such as word processing, document management, scheduling and social media. "It's a matter of the core competency of the organization and how well can they support an application that's core to their business," he says.

In comparison, private cloud scenarios can allow smaller companies with data-intensive processes to expand their infrastructure when needed, and not worry about vital information getting into the wrong hands. For example, many private cloud providers take over IT provisioning tasks from storage to applications, but use virtualization technologies to partition off technologies and applications specific to a particular company.

Creating a flexible computing strategy is an important part of establishing a dynamic infrastructure. Many organizations employ a mix of computing options to create the most effective solution to meet their needs. The underlying technologies associated with cloud computing can be focused on creation of a more dynamic infrastructure, as applications and the services they provide are no longer locked to a fixed, underlying infrastructure and can adjust quickly to change.

But are midsized companies ready for clouds? According to Hochmuth, the answer is yes. Cloud computing provides access to IT resources to rapidly deploy new applications and services without re-engineering the entire infrastructure—or, in some cases, without having to have an infrastructure at all.

And with a variety of options available, midsized companies can get a clear view of how cloud computing will impact security policies—and still take advantage of the cost savings that accompany this new model of provisioning IT.

Cloud models are one example of how midsized businesses are thinking differently about their IT. As the digital and physical infrastructures of the world converge, and we continue to infuse intelligence into more and more things, companies will see more ways to change, to improve safety and efficiency, and to become smarter.