Security in the Cloud
Is All About Visibility and Control

When it comes to security in the cloud, organizations are confident in their cloud providers, but also and reluctant to expose certain types of data and applications, according to IT industry association CompTIA. Security vendors maintain the problem is one of visibility and control, and each has a solution

by Thor Olavsrud - Fri, February 17, 2012

It's an oft-repeated mantra: Organizations engaged in or investigating cloud computing in any of its many flavors are concerned about security. In fact, concerns about security, data privacy and data residency are often cited as inhibitors to cloud adoption. But are the concerns justified? Some security experts say visibility and control are the missing elements.

In a recent study of IT and business executives, CompTIA, the IT industry association, found that 50 percent of respondents cited greater reliance on Internet-based applications like cloud computing and software-as-a-service as a driving factor in their cyber security concerns. But a number of cloud experts say that in many ways data in the cloud is more secure than in an on-premise installation—or at least rapidly becoming that way—especially for smaller organizations that don't have the resources to dedicate to security technology and expert staff.

Security Staffing Issues?

Access to enough IT staff with security expertise may be particularly tricky for organizations of all sizes. CompTIA says 41 percent of organizations reported moderate or significant deficiencies in security expertise among IT staff. On average, CompTIA says organizations were about 30 percent short of their headcount devoted to security. According to the Bureau of Labor Statistics (BLS), which adds the category of Information Security Analyst in 2011, unemployment for people employed in the category stands at 0 percent.

Christopher Primault, co-founder and managing director of GetApp.com, a business software marketplace that vets cloud-based apps and organizes information about them for small businesses, says that cloud services help organizations get around this problem because they provide professionals dedicated to safeguarding your information.

"Your data is probably safer with the vast majority of vendors than if you keep it on your premises," Primault says. "I really believe it's true."

He adds, "We only use cloud services, so we were born in the cloud. The cost for me to keep data in-house and protect that data would be high. Frankly, by having my data in the cloud, I feel more secure."

Primault is not alone. According to CompTIA, 85 percent of organizations using cloud services are confident or very confident in their cloud service provider when it comes to security. But those same organizations are reluctant to put certain types of data or applications in the cloud.

"There is a slight paradox among users of the cloud right now," says Tim Herbert, research vice president with CompTIA. "They convey very strong confidence in cloud service provider security. At the same time, many companies are very reluctant to put certain types of data or applications into a cloud environment. Companies have moved some of the non-critical systems into the cloud, but they are not there yet in terms of moving their most critical systems to the cloud."

Firms are especially reluctant to put confidential company financial data and credit card data in the cloud. CompTIA found 49 percent of small firms, 55 percent of medium firms and 56 percent of large firms were unwilling to put confidential company financial data in the cloud. When it came to credit card data, 50 percent of small firms, 50 percent of medium firms and 53 percent of large firms were reluctant.

Cloud Security Assessment Shortcomings

Even as organizations struggle between confidence in the security measures of cloud service providers and reluctance to place sensitive data in the cloud, they are also on the whole overlooking critical elements of cloud security when evaluating service providers' security policies, Herbert says. In particular, regulatory compliance, geolocation of data and the credentials of the provider are often glossed over.

"Despite some of the concerns, only 29 percent of the companies in the study say they engage in a heavy or comprehensive review of the cloud service providers' security practices," Herbert says.

In the study, 50 percent of respondents say they either sometimes or rarely/never assess the geographic location of a cloud provider's data centers. A further 46 percent say they either sometimes or rarely/never assess the regulatory compliance of cloud providers. And 44 percent say they either sometimes or rarely/never assess a provider's identity and access management.

This can lead to some unpleasant surprises, according to CompTIA.

"Recently, the City of Los Angeles and Google learned the hard way what happens when an uncertain regulatory variable is introduced into a cloud deployment," CompTIA says in its 9th Annual Information Security Trends Study. "LA had to alter its plan to shift 30,000 city employees to Google Apps when it was discovered that Google Apps was not fully compliant with the FBI's security requirements for connecting to the Criminal Justice Information System (CJIS), a clearinghouse of law enforcement data administered by the Department of Justice."

CompTIA adds, "This is one notable example of what is sure to be a more regular occurrence- organizations making the transition to the cloud only to discover a security-related element that forces a change of plans. As the cloud model matures, some of these issues may naturally work themselves out, but in the shorter-term, IT solution providers and cloud vendors can provide a valuable service in reducing the likelihood of these types of situations, Longer term, third party assessments of cloud service provider security policies, procedures and capabilities may become standard."

Securing the Cloud

In the meantime, security vendors are determined to make the cloud a trusted environment in which organizations can do business.

"The real challenge is that companies need to move to the cloud," says Dave Canellos, CEO of Toronto-based PerspecSys, a provider of privacy, residency and security solutions for the cloud. "This isn't a fad. It's really about how you manage that responsibility and ensure that you protect the information that you are now managing."

Nicholas Popp, vice president of product management and development at Symantec, acknowledges that the cloud is not quite up to par with on-premise installations when it comes to security. But he also says he believes the time is rapidly approaching.

"The cloud eventually will be more secure," he says. "Security as a do-it-yourself operation is getting more and more difficult."

Popp predicted that within three to five years, the cloud will be the more secure environment for small and mid-sized businesses (SMBs), while the horizon for larger enterprises is probably in the 10-year range.

"A lot of people will claim that the cloud is fundamentally insecure," he says. "The real issue is not security, it's more about control and visibility. It's a trust issue. Salesforce and Google need to have good security. From a security standpoint, they're going to be much better than most companies."

The problem, Popp says, is that organizations don't have a good mechanism for injecting their own security policies into cloud services and they don't have the ability to access logs.

"The issue is that the cloud guys do not provide IT with enough control to set their own policy," he says. "It's actually difficult because every cloud is different. You have different APIs and security frameworks. They're all going to have different ways to do security and expose that security. We need to create a new control point so IT can inject their own policies on top of these cloud services."

Additionally, he says, an organization's IT staff needs to have access to logs and backups for both regulatory compliance and the capability to perform forensics if something does get compromised.

Symantec's answer is O3, a cloud information gateway that it likens to the earth's ozone layer. It's intended to sit between an organization and its cloud services and act as a sort of cloud firewall. Popp says it will provide three layers of control: an identity and access control layer, an information protection layer and an information management layer. The first layer provides role-based access to information in the cloud, while the second enforces and organization's security policy. The final layer will capture all the logs and allow organizations to demonstrate regulatory compliance.

PerspecSys takes another tack, though like Symantec it focuses on the message of control.

"We make cloud applications mission-critical for companies by ensuring that their sensitive data never moves outside the company's network," explains Canellos. "We help you use the application in the cloud, but keep the sensitive data behind your firewall at all times."

PerspecSys focuses on protecting data in flight with an approach that Canellos says helps reduce the risk of data transfer, data processing and storage in the cloud.

"If you talk to data centers or the cloud providers, when the data is under their control, within the perimeter of their data center, they can give you all the assurances that the data is probably more secure than if it is with the perimeter of an SMB network," he says. "But what happens when the data is in flight? At that point, if you look at the agreements companies have with data centers, that is no longer their responsibility."

The PerspecSys Cloud Control Gateway uses tokenization to replace sensitive data in the cloud.

"Our solution sits between the conversation of the end user of the cloud application and the cloud," Canellos says. "Essentially, we're moderating the transaction between the end user and the cloud. Whatever the company has deemed to be sensitive information, we go ahead and steer that information to a local database behind the company firewall. In its place, we use replacement data."

Israeli-firm Porticor also believes that trust and control of data in the cloud is the problem, but its answer is all about encryption and key management. Gilad Parann-Nissany, Porticor co-founder and CEO, likens Porticor's solution to a safety deposit box in a Swiss bank. Porticor uses encryption key—splitting technology to give the customer a master encryption key common to all data objects in an application, while Porticor keeps its own set of encryption keys-'banker keys' as Parann-Nissany refers to them-for each data object. When an application accesses the data store, it uses both parts of the key to dynamically encrypt and decrypt the data. The master key itself is homomorphically encrypted so it is never exposed, even when in use.

"The customer has control through the customer master key and the banker works very hard to secure every file and disk," Parann-Nissany says. "Only the combination of the customer key and the banker key will open a disk."

Moreover, the keys in Porticor's possession are encrypted with the master key, so Porticor can't even access the keys without the customer.

"Suppose you're not dealing with a hacker," Parann-Nissany says. "Your attacker is a business rival and they go to court and get a court order for your data. Because of the nature of the solution, we have nothing. Even the banker key is not there, it's encrypted through the master key. They have to go to the customer if they want the data."

He added, "The banker can never see the customer key. Even when it is being combined with the other keys, it is itself encrypted through this technique. The key point is that we can manage the customer keys without ever touching them or knowing them ourselves."

CompTIA recommends that organizations use the Cloud Security Alliance (CSA) as a resource for security questions when evaluating cloud service providers. The CSA, a nonprofit organization, has a list of more than 200 questions covering data integrity, security architecture, audits, regulatory compliance, governance, physical security, legal and more. It also publishes a top-level security roadmap for cloud operations.

Thor Olavsrud is a senior writer for CIO.com. Follow him @ThorOlavsrud