

JULY 02, 2008

Gartner: Seven cloud-computing security risks

Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails

By Jon Brodtkin | Network World

Cloud computing is fraught with security risks, according to analyst firm Gartner. Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor, Gartner says in a June report titled "[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," Gartner says.

Amazon's **EC2** service and Google's **Google App Engine** are examples of cloud computing, which Gartner defines as a type of computing in which "massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies."

Customers must demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators; risk-control processes and technical mechanisms; and the level of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unanticipated vulnerabilities.

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.

1. Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security

certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers.

Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case 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. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "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."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get **acquired** and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "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," Gartner says.