

Navigate the Cloud Securely

Cloud Computing Offers Obvious Advantages for Your Business. But Is Your Critical Data Protected — as Well as Leveraged to Its Full Potential?

BY JOSEPH KING



In the information technology (IT) world, perhaps no topic today is receiving more attention than cloud computing. Once viewed as a cost-effective, flexible option for small or midsize companies, cloud computing is now generating interest from even the largest businesses, whose executives once believed that their data was too critical, too sensitive or too complex to relegate to a cloud services model.

Increasingly, companies of all types and sizes are realizing the benefits of leveraging a cloud approach for application hosting, hardware hosting and data management, which offer clear cost and efficiency advantages — and also allow the organization to focus on key strategic challenges instead of administrative tasks.

Cloud computing offers dynamic capabilities, such as flexible configurations, as well as ubiquitous user access from every geographic location and time zone. For core business activities such as transportation scheduling, warehouse management and point-of-sale (POS) data collection, cloud computing is ideally suited to manage extremely large data volumes and multiple collaborative relationships across the supply chain, seamlessly and invisibly.

In the event of a natural disaster or other significant business disruption, cloud computing also offers peace of mind and reliable business continuity. When JDA executives visited Asia in the wake of the Japanese earthquake and tsunami in 2011, business continuity was the single most pressing issue on every customer's mind — and cloud computing offers an easy, cost-effective solution to address these concerns.

Cloud computing also delivers extremely rapid time to value, with full software and data hosting occurring in as little as 15 days. Your business can immediately start realizing a return on its technology investments, instead of waiting for an internal IT infrastructure to be provisioned and configured.

While cloud computing offers a host of benefits, it's not always easy to trust another company with the critical data that represents the lifeblood of your business. Maintaining your hardware, software and precious information at an off-site facility certainly makes good business sense — but it requires real trust, based on sound operating practices. High-profile data security breaches at credit card companies, healthcare providers, universities and government agencies often grab headlines, reminding us of the dangers of doing business in today's real-time, technology-connected world.

Before your business makes the leap into cloud computing, or increases its investments in the cloud, it's essential to address the topic of data security with your provider. Navigating the cloud safely means ensuring that your most critical data is protected with a high degree of rigor that meets or exceeds your organization's needs. Your data should be safe, secure and ready to apply to your most urgent competitive challenges anytime, anywhere.

Where Exactly Is My Data? Public Versus Private Clouds

One of the first issues your business needs to understand is the all-important distinction between public and private clouds.

The online world is filled with public clouds, which enable customers to subscribe to and buy data storage space. While public clouds may be cost-effective, businesses should be aware that public storage providers are likely not employing the same systematic approach to firewalls, data encryption and other security protocols that exist within their own organizations. And, because public clouds are not designed to store mission-critical data, 24/7 access might be a problem. Outages are common, whether due to site maintenance, upgrades or other issues. While public clouds are perfect for consumers' needs, they lack most of the serious performance features and security protocols that you need to run your business with a high degree of confidence.

Conversely, private clouds are built with a single customer, or group of customers, in mind. Segregation, separation and data protection are key concepts. Because private cloud providers understand the real everyday needs of your business, continuous access is also a high priority — and your team members will be able to remotely access the applications and data they need to do their jobs, 24/7, from any location in the world.

When working in a private cloud, your employees will also benefit from custom-designed, Web-based interfaces that are seamless and easy to use. The best private clouds are invisible to your team members, who only see an extension of your own business when they access solutions and data in the cloud.

In addition, private clouds are generally characterized by stringent security measures that ensure the safety, integrity and real-time availability of your most important data.





How Protected Is My Data? Establishing the Right Protocols

Any IT professional can list the “three As” of data security: authentication, authorization and accountability. Your own IT and compliance teams have worked diligently to ensure that all the information stored within your own walls is protected, in keeping these three essential themes. In your relationships with external trading partners, your business has also worked to ensure that all third parties are accessing your data in a safe, secure manner.

Nowhere are the concepts embodied by the three As more critical than in your choice of the cloud computing partner who will virtually host your hardware, software and proprietary data. Authentication, authorization and accountability must be foundational to their delivery model.

At the off-site facility where your data is stored, personnel should be issued proximity access cards that authenticate their identity when they enter the facility. Security personnel should be on-site 24/7 to closely monitor access, backed by stringent security systems. When employees log in, user authorization should be required at both the network and system levels.

Accountability should be established via standard operating system event logs that are carefully maintained and monitored. Ongoing alerts should monitor both the health and performance metrics of each technology system. Networks and systems should be safeguarded with a variety of firewalls, including intrusion prevention systems, data loss prevention systems and Web application firewalls.

Cloud managers should ensure that all systems and processes are compliant with standards such as SSAE-16 (SAS-70) and Sarbanes-Oxley — and should schedule security audits on a regular basis to ensure that protocols are upheld stringently over time.

Viruses and system vulnerabilities should be addressed via a highly disciplined series of ongoing patches and scans. This is one area where cloud providers, with their hundreds of vigilant employees, can provide an enormous advantage. For example, managers on the JDA Cloud Services team implemented more than 136 security patches in 2010 alone — including network, operating system, database and middleware components. Each patch had to be fully tested and certified before deployment, which would represent a challenging feat for even the largest companies managing their own IT infrastructure.

Of course, clouds should also provide a high degree of redundancy and availability, minimizing the risk of an extended service outage. Full functionality and access should always be restored quickly, and companies with a high volume of mission-critical data should be able to create custom service agreements that guarantee an extremely fast service and data recovery window. Cloud providers should test their own disaster preparedness on an ongoing basis to assess and improve their capabilities.

Who's Minding the Cloud? Combining IT and General Business Expertise

Even though cloud computing relies heavily on high-quality computing resources and stringent IT protocols, all these technologies and processes are managed on a day-to-day basis by people. It's essential to ask and answer the question: Who is actually managing my data? What are their credentials and skill sets?

The best cloud providers will have teams of hundreds of experts supporting your cloud computing needs every single day. Not only should these cloud managers be subject to background checks, confidentiality agreements and daily security protocols that control their access to the cloud, but they should also have a broad range of hardware, software and business skills.

They should not only be technology experts, but also business generalists who understand your organization's strategic needs for various software applications and operating information — and who can help custom-tailor the cloud's capabilities to best meet your needs. Cloud managers should know not only how to store data, but also how to apply data to help customers streamline processes, reduce risk and expedite business results from software investments that are already in place.

While your internal IT team might only consist of a small group of people, the right cloud provider can supply a team of hundreds of highly qualified, credentialed experts to supplement your team. By relying on this external expertise to streamline your daily computing needs and help you leverage your data to the fullest extent, your IT staff and other professionals can focus on the core strategic priorities that are driving your business.

Making the Most of Your Cloud Investments

With the incredible growth of cloud computing resources, there are very few companies that cannot achieve significant time, cost and efficiency benefits from entering the cloud.

The key is identifying those parts of your business that are right for cloud computing — whether because they are data-intensive, involve partner collaboration or are otherwise well suited — then creating a close partnership with a trusted cloud services provider.

The right partner should combine IT expertise and a commitment to security with a general business approach that helps you maximize your return on your technology investments. Cloud managers should understand both the applications you are running and the data you are storing, as well as how these resources can be applied to your core business challenges. This approach not only helps cloud computing deliver a lower total cost of ownership and quicker returns — but, more important, positions your business for a competitive advantage by turning technology and information into powerful strategic weapons. ■

▶ The JDA Difference

JDA Cloud Services and JDA® Private Cloud

JDA provides continuous value and investment protection of JDA solutions at some of the largest global supply chains, including Dell, BP, Lenovo and PepsiCo. With domain expertise in a multitude of supply chain solutions, JDA Cloud Services delivers value around:

- Rapid deployment and faster time to value
- Improved cost structure and investment protection
- Software currency and risk mitigation



Joseph King is senior vice president, JDA Cloud Services. In this role, he is responsible for JDA's global Cloud Services business, including sales, support and operations.

