Merit
SOLUTIONS

Cloud Security: Bringing Clarity to Common Myths and Misconceptions

Authors:
Dan McCue, SVP Finance & Accounting
Sutherland Global

Bill Burke, CEO
Merit Solutions

Contents

Introduction

Companies in today's economic environment are all facing the age-old business conundrum: how can we do more with less? To help improve capacity but drive down costs, organizations are increasingly turning to cloud-based technologies.

Cloud-based Enterprise Resource Planning (ERP) can be deployed quickly, minimizes the initial investment, reduces the Total Cost of Ownership (TCO) and offers seamless upgrades. Although many CEOs, CFOs, CIOs and key stakeholders look to cloud computing to help realize tremendous savings, there are concerns about cloud-based data solutions.

In the age of cyber-attacks and the seemingly ever-growing list of online security threats, senior executives worry about the safety of their cloud-based information. Physical location, data transmission, access security and disaster recovery represent the four top-of-mind security concerns.

This white paper will look at some of the key aspects of cloud security and examine some of the myths and misconceptions. Research also shows that while senior executives are apprehensive about cloud-based security, only a small percentage conduct due diligence on their providers. This white paper also includes a checklist of 10 questions that organizations should ask their potential providers.

The Rise of Cloud Computing

A survey by CDW found that 28% of US-based organizations are using cloud computing today, and 73% of those organizations took their first step by implementing a single cloud application. Interestingly, the vast majority of the survey respondents (84%) say they "have already employed at least one cloud application." So, in essence, there are a lot of first steps being taken, and wider cloud adoption is foreseeable.

There's no doubt the cloud is garnering attention as companies cautiously explore cloud applications. According to a Forrester Research report titled "Sizing the Cloud" the global cloud computing market is estimated to reach $241 billion in 2020. Yet, despite the rise of cloud computing, there are a number of misconceptions floating around, with security at the top of the list.

Top 5 Cloud ERP Misconceptions

1. With a cloud ERP solution, our data isn't as secure as it is onsite.

2. Cloud ERP solutions provide only basic ERP functionality.

3. Cloud ERP solutions can't be customized.

4. It's difficult to integrate cloud ERP systems with other systems.

5. If the Internet goes down, the business goes down.

As companies transition from low-risk "testing the waters" to taking the plunge with cloud ERP for more mission-critical functions like Finance and Accounting, the issue of cloud security is inevitable. The question most often asked is, "Just how secure is our data?"

It's a legitimate question. It was only a few short years ago that cloud-based ERP systems were the exception rather than the norm for most companies. The idea of not having all data, infrastructure, software and hardware on-site was new, intriguing and fraught with concerns. Entrusting private business data and applications to an outside hosting service made (and continues to make) some organizations uncomfortable.

Despite the cloud's shift into the mainstream, security and compliance still top the list of apprehensions inhibiting cloud adoption. Some of this apprehension is caused in part by confusion around a lack of industry standards; expectations and definitions of security can vary from industry to industry. Different regions and countries are subject to different data protection policies and legislation that could compromise data privacy. Companies need to conduct due diligence on their prospective cloud providers.

Data security and privacy issues are very real concerns no matter whether a company implements a cloud ERP solution or one that is on-premise. Both require knowledge of data: which data is sensitive, the degree of sensitivity and the protocols required to protect it.

Yet, the pervasive myth that cloud-based ERP simply isn't as secure as on-premise solutions continues to linger. The myth persists based on four misconceptions about the security of physical location, transmission, access security, and disaster security.

Physical Location

The Misconception:

A cloud-based solution is nebulous and can't be secured.

The Reality:

Cloud computing is eyed suspiciously and has the appearance of being risky because you cannot secure its perimeter—where are a cloud's boundaries? A study by the Ponemon Institute found that IT professionals believed security risks were more difficult to curtail in the cloud, including securing the physical location of data assets and restricting privileged user access to sensitive data.

Yet, as CIO Magazine pointed out:

"…respondents only gave the on-premise alternative a 56% positive rating! In other words, nearly half the respondents believe that their own internal data centers do not do a good job of securing the physical environments of their data centers."

The reality is that often on-premise ERP security does not measure up to the same standards as a world-class data state-of-the-art facility.

An ideal data center should be secure, free of windows, and built with cement or steel fortifications with 24/7 on-site security. Most IT departments reside in a department or on a floor of commercial buildings and office towers, which rarely have these conditions.

Transmission

Misconception:

Cloud-based solutions are more vulnerable to hacking and other attacks.

The Reality:

Organizations typically invest in hardware, software and applications to thwart specific security challenges: spam, security breaches, malware, non-compliance, and so forth. Unfortunately, many of these products have limited life cycles, are difficult to scale and, from a security point of view, often only produce single points of failure. Additionally, the latest technologies to scramble and encrypt data – RSA, Secure Socket Layer (SSL), Data Encryption Standard (DES), or Triple DES, etc. – can quickly drain IT budgets.

With traditional licensed ERP software, organizations typically must wait for the next release to benefit from the latest features, upgrades, or security patches. Sometimes limited resources can mean that upgrades aren't always deployed in a timely manner. In fact, two-thirds of mid-size businesses are running outdated versions of their ERP software. This can leave these companies vulnerable.

Under the SaaS (Software as a Service) delivery model that forms the basis of cloud ERP, the provider continuously and unobtrusively adds the latest features and upgrades, which means that users can be assured that they're actually using—rather than waiting for—the latest security technology.

By their very nature, external applications like cloud-based technologies must adopt a "trust no one" approach. Layers of security controls, encryption of all sensitive data and security testing at the application level, as well as countless other safeguards are necessary for cloud security.

A world-class cloud ERP provider will perform rigorous internal vulnerability scans, log threats, and are audited for SSAE 16 Type 2 compliance. Data is fully secured, both in transmission and at rest. There are no software or hardware purchases, and updates are seamless.

Access Security

The Misconception:

An on-premise solution offers more security over who may access information.

The Reality:

The myth that a cloud solution simply cannot be as secure as an on-premise solution has very much to do with the notion of "seeing is believing." Often companies feel more in control of their data when it resides under their own roof.

When ERP is on-site, it is the sole responsibility of the IT department to authenticate and log all access to data in order to prevent unwanted users, both internal and external, from accessing information or resources.

Access security for on-premise ERP systems may be enforced through business logic or at the database layer. This authenticates users and provides them with specific rights to data objects. For example, a payroll clerk would only have access to payroll data, not customer records.

A cloud-based ERP is no different - you control access to data throughout by managing security restrictions on forms, records and data fields for specific user groups and domains, and define and assign rights according to how you want security restrictions managed. Also, when companies deploy in a single-tenant environment, there is no risk of data being inadvertently exposed to other users due to poor implementation of the access management process.

While a secure cloud ERP system doesn't increase the vulnerability of your business data, authenticated users have "anywhere, anytime, any device" access, which is a tremendous advantage for global collaboration, monitoring and managing.

Security From Disaster

The Misconception:

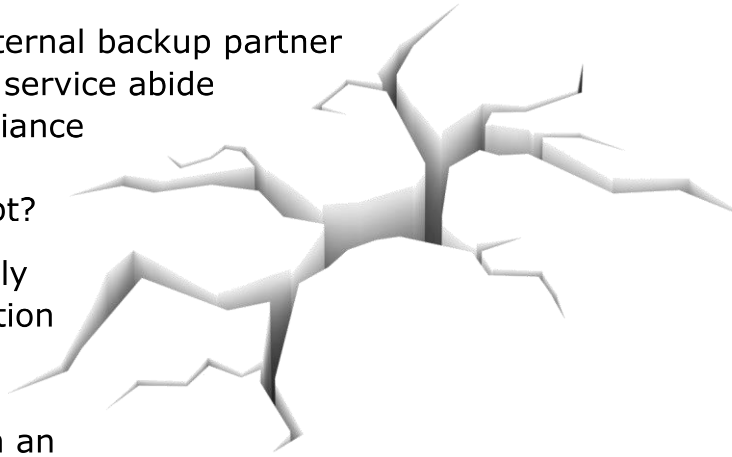
It's better to handle backups internally to be able to access data more quickly in case of a disaster.

The Reality:

Companies must examine how often they back up data and where the backups are the stored. Companies looking to third-party back-up systems and business continuity facilities must thoroughly examine the security standards that are in place. The truth of the matter is that all businesses need to invest in a rigorous program for data backups with offsite storage in a secure location separate from the main data center.

Key questions to ask before choosing an external backup partner include: Does the third-party data recovery service abide by recognized security standards and compliance requirements? What happens if there is a power failure? How long will my data be kept?

Most cloud-based solutions ensure full nightly backups which are stored in an off-site location and are maintained for years. As well, the data centers have multiple power sources and redundant incoming lines provisioned in an N+1 configuration for continuous power.



Conclusion

Traditional and cloud ERP share many of the same security issues, from preventing unauthorized access to safe and secure backups. As the "new kid on the block", cloud technology is unfamiliar and not fully trusted.

However, most organizations that adopt a cloud-based ERP solution find that security is actually improved. In cases of cyber-attacks, cyber espionage, malware, human error and disasters - cloud-based service providers often times have higher levels of security.

In fact, recent Microsoft research verified the significant IT security advantages from using the cloud. One of the most interesting facts to emerge from the survey was that "35 percent of US companies surveyed have experienced noticeably higher levels of security since moving to the cloud."

Security is always a top concern for companies, but it's time to cut through the fog and bring a little clarity to the situation: Cloud ERP systems and the data they contain are as secure - if not more secure - than traditional ERP systems.

Security Checklist

CompTIA's Annual Information Security Trends survey of U.S. executives with IT responsibilities reported that only 29% of organizations report conducting a heavy review of their cloud service provider's security policies, procedures and capabilities.

It is critical that companies vet their cloud providers by conducting due diligence and asking for proof of physical audits and physical access controls. Here are 10 questions you can ask your provider.

1.) What is your privacy policy?

Your potential solution provider should have a well-defined and clearly articulated privacy policy that spells out exactly who has access to various types of information. It should also describe the organization’s standard operating policies and procedures for ensuring privacy. Your prospective vendor should voluntarily provide you with a copy of this policy information.

2.) What level of security do you use to ensure the safety and integrity of critical data?

To safeguard your data onsite, your prospective solution provider should use a combination of intrusion detection system (IDS) and intrusion prevention system (IPS) products and apply antivirus at various network layers. It should also utilize deep packet inspection (DPI) or an application-level firewall technology that scans all levels of packet transmission. Finally, it should also use secure socket layer (SSL) or https-encrypted transmission to ensure Internet security.

3.) Is your production equipment housed in a state-of-the-art facility?

Your prospective vendor’s data center should be secure, free of windows, and built with cement or steel fortifications. It should also be located somewhere that is not prone to inclement weather.

4.) What are your facility’s physical security arrangements? Are they in place 24 hours a day, seven days a week, and 365 days a year?

Similar to its privacy policy, your potential hosted ERP solution provider should have well-defined and robust security arrangements that are in place at all times.

5.) Do you contract with an independent, third-party organization to conduct periodic external and internal vulnerability scans?

In addition to maintaining an intrusion response system and a prepared response plan, your prospective solution provider should frequently commission both routine and unannounced security audits.

6.) How often do you back up data, and where are the backups stored?

Your potential hosting provider should have in place a rigorous program of data backup and offsite storage in a secure location remote from its main data center.

7.) Do you offer full hardware redundancy to avoid the negative consequences of a power failure?

Your prospective solution provider's data center and backup location should have redundant power supplies, such as battery and diesel generator backups, to avoid the negative consequences associated with a power failure.

8.) Does your staff include a highly qualified operations team that monitors the site 24 hours a day, 365 days a year?

Your prospective vendor should have on staff many certified security experts, including those with the preferred CISSP designation.

9.) Is my data stored in a multi-tenant or single tenant environment?

A multi-tenant cloud-based ERP is a set of pooled computing resources, shared among many different organizations (tenants). In short, various organizations share the same database. In a single tenant environment, customers operate with their own individual database. It is our belief that an isolated single tenant environment best maximizes performance, security, privacy and integration.

10.) How safe is your data center in terms of natural disasters?

Your potential provider should be prepared for any number of natural disasters. In addition to a windowless, cement building with steel fortifications, the provider should have multiple power sources and redundant incoming lines provisioned in an N+1 configuration for continuous power. For example, some data centers' backup generators can power a city of 25,000 people - which allows them to go off grid for 28 days without water, electricity, sewer, or natural gas feeds!

About Merit Solutions

Merit Solutions is a global business process consultant and systems integrator with offices in North America and Europe. We are a focused-strategy company with the goal of being the very best at helping clients automate, grow, and transform their business through process mapping and optimization, change management, and innovative IT consulting and development services.

Merit Solutions works with clients to understand and triangulate their exact business needs in terms of people, workstreams, and enabling systems. From future state business process mapping to systems analysis, fit-gap process definition and scoping, sourcing, design and deployment, integration with other systems, and on-going support - we provide end-to-end global services that help clients successfully transform their business and build a foundation that continuously flows value to their customers.

Our clients are typically medium to large, global enterprises who are challenged by inefficient workstreams that cost money, waste time, and reduce quality; information flows and systems that no longer support the goals of the company; and lack of visibility into business data which impedes effective decision making.

Additional Resources

Related resources to this white paper include:

- Using Enterprise Mobility to Bring Value to Your Business
- A Practical Approach to Empowering Your Mobile Workforce
- Reducing Risk to Enable Successful ERP Implementations

Information on Merit Solutions or other publications can be found on www.meritsolutions.com