5 Things to Look for in a Cloud Provider When it Comes to Security

In This Paper

- Internal technology services that lack resources, rigor or efficiencies are prime candidates for the cloud
- Understand the business and regulatory requirements around the data to be moved to the cloud
- Know your cloud provider's security and privacy commitments, and what responsibilities you retain

a QuinStreet Executive Brief. © 2013

eSecurity Planet
Executive Brief

Cloud computing is changing the way enterprises do business. Technology has long been a facilitator for business processes, so cloud computing is not unusual in that regard. Few technologies, however, have been adapted as rapidly or have had the wide-reaching ripple effects of cloud computing.

Many things are fueling cloud growth, from its ease of use to its low initial investment, but a key driver for enterprises has been the way cloud computing provides technology services in a less expensive and more efficient manner than had previously been possible. This allows enterprises to focus on their core business and leaves the management of IT services to cloud providers that are experts in technology services.

While this easy access to information provides many benefits, it also introduces a number of concerns. Security and related operational risks rank among the top concerns for organizations considering moving to the cloud.

Security is a concern with any new technology, but by its very nature, cloud computing impacts not just what is in the cloud but also the security of the entire enterprise. If the cloud is the weakest link in the security chain, the entire enterprise will feel its vulnerability.

"Never has it been more critical to think about safeguarding business data," explains Gail Coury, Vice President of Risk Management for Cloud Services at Oracle. Data security, privacy, risk and compliance should be the primary focus for any enterprise that has a cloud computing component of its IT services. An enterprise must understand the criticality and sensitivity of the information being managed within a cloud service and then ensure that the cloud provider has the appropriate controls to properly protect it.

Moving the 'Right' Apps to the 'Right' Cloud

An inherent part of building a cloud ecosystem often means allowing your cloud provider to become a custodian of your information. Depending on the capabilities of the provider, an enterprise could actually improve the overall security compared to what it might otherwise be able to resource on its own. What can an enterprise do to ensure it is getting the security it needs from a cloud ecosystem?

First and foremost, it is imperative to move the right technology services and information to the right kind of cloud. The very first question to ask when developing a cloud strategy is not about the technology. It is "which business problems can be solved by moving to the cloud?" says Ben Nelson, Senior Director, Cloud Security and Compliance at Oracle. Before considering what type of cloud services to use, enterprises should evaluate what technology services would provide the most immediate benefit when moved to the cloud.

"First and foremost, it is imperative to move the right technology services and information to the right kind of cloud. "

What is a prime candidate for the cloud? Nelson says to look for internal technology services that lack resources, rigor or efficiencies. Some applications, he explains, will be better maintained in the cloud, particularly if the enterprise does not have the resources to maintain or secure that application. Sending those services to the cloud reduces risk and delivers a more robust solution than can be developed in-house.

It is important to understand business and regulatory requirements around the data that a buyer wants to move to the cloud for a cloud strategy to be successful. Knowing these requirements will narrow the cloud choices initially. Later, during the vendor selection process, it will enable you to be clear about your expectations and your enterprise's requirements, allowing you to evaluate each vendor based on its own merits. Keep in mind that not all cloud providers are equal in the security services that they provide, so knowing your requirements and mapping these to the provider's capabilities will ensure that you select the best fit for your risk tolerance and regulatory needs.

While the cloud providers themselves are varied in their strengths, weaknesses, and overall quality, it is important to start with the kind of cloud that best meets your needs before evaluating the vendors themselves.

Once you've assessed your needs, it is time to look at the available types of cloud offerings. There are a few general cloud types to consider: private on-premise, Software-as-a-Service (SaaS) running in a public cloud and managed private cloud. Each has its own set of advantages, disadvantages and associated security implications. Typically, a private on-premise cloud is designed for the exclusive use of one organization. It resides on-premise in the data center and is controlled and managed by internal IT. A private on-premises cloud enables the enterprise to have complete control over security. The flipside of this is that the security is completely reliant on IT and limited to the enterprise's available resources. Whether this is the best choice depends on what security measures and infrastructure the enterprise has in place.

For enterprises that prefer to keep their data in a private cloud but lack the resources, Oracle has a solution that offers the best of both worlds — private managed cloud. An Oracle Managed Cloud is physically located in either Oracle's data center or in the customer's data center, but the cloud services themselves are managed by Oracle. Oracle Managed Cloud Services provides the initial setup, ongoing management, monitoring, upgrading and security in one of Oracle's data centers, or, if the enterprise prefers, on-premise in its own data center. The customer has dedicated environments that it can customize, extend or integrate with other applications, and it has the ability to control management and timing of maintenance and upgrades to their services. Managed Cloud Services allows the customer to leverage license investments already made and move to a more predictable operating expense for delivery of services.

By using SaaS services in a public cloud, enterprises can obtain new functionality much faster and less expensively than they would with a private on-premises cloud, as the SaaS service is standard and can be provisioned quickly. There is no capital investment and all costs are treated as operating expenses; costs are typically determined by the amount of services consumed. SaaS services generally offer a great level of configurability while retaining the ability to scale and maintain common operational controls across the environment.

Most enterprises ultimately end up with a hybrid combination of public and private clouds working together to create a cohesive end-user experience. A hybrid cloud enables applications to run across public and private clouds as though they were one. Hybrid cloud environments are becoming increasingly popular with enterprises. As hybrid clouds and coexistence strategies become more common, it is ever more important to address data security across multiple clouds, systems and on-premises applications.

In some cases, an enterprise's industry will dictate the type of cloud needed. Financial services companies, for example, often require updates and additional security services, as the industry has very specific regulations about where data resides and how it must be administered and controlled.

In addition, businesses that operate globally will need to take into account 24/7 support, data jurisdiction, cross-border data transfer, data location, and most importantly, the privacy regulations of where they're doing business. Global issues, Nelson notes, are typically privacy related. "Privacy is the hot button," Nelson says, explaining that privacy and security are linked, but privacy is driving the conversation when it comes to customer requirements.

Oracle's strong international presence means it must be able to contend with the multitude of data and security regulations from country-to-country and industry-to-industry. As a result, Oracle offers "the broadest regulatory compliance portfolio and a large base of employees handling cloud operations. We have very deep cloud expertise, and we leverage that at every turn," Nelson said.

The company has a large staff dedicated to regulatory compliance and privacy requirements in various industries and regions. Oracle is able to modify and tailor services to meet the requirements of customers' respective industries and regions.

5 Security Areas to Look at When Evaluating a Cloud Provider

Hence, choosing a cloud provider is no easy task. While cost is a factor, this is not solely a commodity decision. Research is critical to determine whether what the vendor offers matches up to business needs and the criticality or sensitivity of the data.

When evaluating cloud providers, these five attributes must be examined. The right answer will vary depending on your security needs and objectives.

1. Transparency of cloud provider

When an enterprise chooses a cloud provider, it is not simply making a purchase or signing an agreement. Although a contract is typically involved for the relationship between the customer and cloud provider to engage, the customer must have a clear understanding of the provider's commitments related to security and privacy, and what responsibilities the customer retains.

> *"A key risk in moving enterprise services to the cloud is managing the end-user access to ensure only authorized access is permitted to the information stored."*

Transparency is critical. Coury notes, "It truly is a partnership between yourself and your provider; the more critical and sensitive the information, the more critical that partnership." The vendor should be able to make clear commitments about what controls are in place, where the data resides, who is managing the underlying technology and other responsibilities it will assume as custodian of the data.

Other important questions to ask are:

- Does the provider have an accountable security officer?
- Does it have a security group with which you can engage?
- Does the provider have independent audits of its security controls?
- Does the provider offer the security capabilities or service options to address specific requirements for regulated data?

The answers to these questions, Coury says, "help you measure the maturity of the cloud provider."

2. Risk mitigation

Risk mitigation is a key component of any security strategy. Consigning data to a third party has the potential to reduce or increase risk. As part of its own security strategy, an enterprise must investigate what steps the cloud provider is taking to mitigate risk surrounding its service offerings.

As enterprises move mission-critical services into the cloud, Nelson believes it is changing the way CIOs need to think. Risk management is now as much a part of a CIO's role as overseeing cost controls and maximizing efficiencies have traditionally been. Cloud has the potential to offer advantage in all three areas. While the efficiencies and cost effectiveness of the cloud are clear, the risk management benefits that cloud delivers can vary by offering and provider.

Nelson argues that a cloud deployment with a solid foundation, certifications and third-party validations reduces risks for an enterprise that moves data and applications to the cloud.

A key risk in moving enterprise services to the cloud is managing the end-user access to ensure only authorized access is permitted to the information stored. When most people think about "accessing data," they are thinking primarily of provisioning permissions to view or make changes to the data. Coury points out that the bigger risk, and where cloud services add complexity, is in the revocation of access — typically when the person leaves the company.

When an employee leaves the company, his access to on-premises services is easily revoked, usually via the company's internal directory server. However, if this same directory server is not integrated with the company's cloud services, access may not be revoked in a timely manner or at all. The result is this former employee may continue to have access to these services, which could be detrimental to the company. Single sign-on is one solution to this, as it offers a way for enterprises to integrate, manage and revoke access from a centralized database.

However, as Coury notes, as much as companies want the many benefits of single sign-on, they don't want to pass their credentials to third parties. The Federated Identity technology in Oracle's Cloud solves this problem. It provides all of the advantages of single sign-on without any downside. So long as the directory service can speak SAML (Security

Assertion Markup Language), Oracle's Federated Identity technology can accept assertions from a customer directory service and authenticate the user. When someone is removed from the company directory, Federated Identity enables them to be simultaneously removed from the cloud service.

For the end user, the entire process, regardless of where authentication takes place, appears as though it is running within the company network. This smooth integration is unusual and particularly noteworthy when hybrid clouds come into play. Survey data shows that few companies have integrated their on-premise and cloud services.

Economies of scale play a key role in making this possible for Oracle. Coury attributes Oracle's expertise to its own set of experiences. As a large enterprise itself, Oracle has first-hand knowledge of managing a large-scale global presence and understands the risks large enterprises face. Oracle channels that expertise into its offerings to deliver not just sufficient security in the cloud, but also enterprise security that surpasses what customers could do on their own.

"Customers can leapfrog their own security by moving to the cloud. They get the benefits of economies of scale and can customize as needed," Coury says.

Nelson agrees, "They can reduce risk by sending those applications to the cloud because, most often, the cloud implementation is more robust than what could be built in-house."

3. Proof of capabilities

It's all well and good for a cloud provider to talk the talk about what security mechanisms it has in place, but it is more important that it be able to demonstrate verification of controls.

Security certifications are one way to do this. They also offer an easy and objective way for enterprises to compare providers and ensure the provider being selected meets their needs. In regulated industries, such as healthcare or financial services, it is critical that the provider can comply with the enterprise's regulatory requirements. Certification is proof that the provider can meet those requirements.

For some enterprises, compliance is difficult to achieve on their own. For them, it is even more critical to choose a cloud provider that can deliver this service.

Oracle's long list of security certifications and extensive experience has helped many customers scale compliance hurdles. Oracle also offers third-party validations, which serve as proof points for customers and demonstrate that it is following industry standards. Oracle's certifications and accreditations include: ISO 27001, certificate of conformance for ISO 27002, SOC 1, SOC2, US Federal Government NIST 800-53 & DIACAP, and 21 CFR part 11. (Note that 21 CFR part 11 is only available for Oracle Managed Cloud Services.) It is also PCI compliant (level 1), HIPAA-compliant for electronic protected health information (ePHI) and is Safe Harbor certified for onward transfer of data from the European

Union. It is important to note that certifications and accreditations available for specific Oracle Cloud service offerings vary.

Sometimes even a vast portfolio of regulatory frameworks isn't enough or doesn't provide the level of certainty and proof desired. In these situations, it is important to know upfront whether the cloud provider allows customers to perform an audit or penetration test, and under what circumstances — any time, only during certain times, unannounced and so on.

While regulatory compliance is important, and Nelson is quick to point out Oracle has one of the broadest regulatory compliance portfolios in the industry, privacy is perhaps even more critical, particularly for customers with an international presence. In addition to confirming certifications, Nelson suggests, "be sure to ask what additional steps the cloud provider takes to support customer data privacy."

4. Integration options

After you have evaluated the criticality of data being moved and set risk criteria to compare cloud providers, it is time to determine what degree of customization and integration is needed. In general, the more customization and integration required, the more likely a private managed cloud is the preferred solution.

A cloud doesn't exist in a vacuum. Applications that run in the cloud typically must interact with other cloud-based apps in different types of clouds as well as non-cloud-based applications. Some data may be housed on-premise, some in a managed private cloud, and some in a public cloud. No matter how simple the cloud-based service seemingly appears, determining how it fits within the IT infrastructure and the enterprise is an important consideration. Equally important are the connections through which cloud-based data will travel. Also, don't overlook the security options associated with network-to-network connections.

"With Oracle private cloud services, communications between Oracle and its customers can take place via virtual private network-to-network connection, with the customer environments residing on their own VLAN," Coury explains. Although Oracle Managed Cloud Services offers standard solutions for Oracle applications (such as Oracle Fusion Financials, Oracle Fusion Human Capital Management, Oracle E-Business Suite, Oracle PeopleSoft and Oracle Hyperion), these applications can be customized, integrated and augmented with additional services and products depending on the customer's needs. Security services including audit logging, change logging, database encryption, and identity management are also frequently used capabilities.

According to Coury this enables enterprises to extend and customize their local environment without the limitations found in some public cloud SaaS offerings. The typical SaaS vendor provides packaged integration tools with basic capabilities to manage the data of that one application. However, typically a single SaaS solution can perform a single function, and most enterprises require multiple SaaS applications to meet their larger business needs. When integration tools from multiple vendors are combined, the user must manage multiple interfaces and languages. Often, manual management and coding to ensure everything

"Regulatory compliance is important, and Oracle has one of the broadest regulatory compliance portfolios in the industry."

interoperates as intended is involved. Not only is this expensive, but it also increases the operational risks.

Oracle offers the most deployment choices – SaaS services that can be integrated with Managed Cloud Services that can be integrated with on-premise applications — giving customers unparalleled flexibility.

"No other niche SaaS provider can provide that breadth of services," Nelson says. "This makes us incredibly unique in the industry from a SaaS provider standpoint."

"However, it is far from an all-or-nothing proposition," Coury says. Coury has seen some Oracle customers start with SaaS because it is quick and easy to deploy and less expensive. Then they get to the integration stage and realize that it makes sense to invest in a private managed cloud or augment their SaaS service with Oracle Managed Cloud Services. Oracle customers can rely on Oracle to be able to integrate seamlessly between Oracle public SaaS cloud services and an Oracle managed private cloud.

5. Breadth of experience

Oracle's Cloud provides services to customers in multiple industries, including Retail, Financial Services, Healthcare, Government and Life Sciences. Because of this, Oracle has developed expertise in security and compliance from which all customers can benefit. For example, to gain economies of scale, Oracle has looked for the common security controls within industries. Coury says, "about 75 to 80 percent of controls are the same across industries, and these became the baseline controls in all of Oracle's cloud offerings." This consistency in controls allows Oracle to automate the operational management and monitoring of these controls.

Next Step: Carefully Consider Security in Choosing a Cloud Provider

As increasingly mission-critical applications and data are being housed or transmitted through a cloud — be it public, private or private managed — security is becoming ever more important. Hence, when choosing a cloud provider, security capabilities should be a key criteria.

Oracle, a leader in secure data management and controls, recognizes security's importance at every level in the hardware-software stack. Coury emphasizes, "Security is also foundational to Oracle's cloud offerings and is critical to delivery of its cloud services."

Oracle's seamless end-to-end stack offering makes it unique among the many cloud providers. As Nelson explains, full ownership of both the hardware and software stack means Oracle has complete oversight and control of the cloud service. Oracle incorporates IT requirements up front and makes sure the controls are baked into the whole stack. Changes and additions are incorporated, whether they be industry, regulatory or customer driven.

This complete stack approach also benefits enterprises that prefer a private cloud or private managed cloud solution. Oracle's unparalleled depth of resources and years of expertise are inherently woven into offerings that are best suited to meet the increasing demands of its customers.

To learn more about Oracles cloud offerings, go to oracle.com/Cloud and oracle.com/managedcloudservices. ■