WHITE PAPER

Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment

Sponsored by: Amazon Web Services

Pete Lindstrom
July 2015

SECURITY PERCEPTIONS RESULT IN CLOUD TREPIDATION

If cloud architectures were human beings, their development stage would fall squarely in the middle of adolescence. Enterprises are at an inflection point with their cloud deployments as they migrate from ad hoc projects to full-fledged, mature, integrated cloud architectures. The discussion around cloud reflects the trepidation and uncertainty that come with adolescence: Cloud advocates express excitement, whereas others voice concern about these developments.

Invariably, one top cloud adoption concern is security. The most recent IDC *CloudView Survey* cites security concerns as the number 1 inhibitor regarding the adoption of cloud technologies and services, with almost 50% of respondents identifying it; security's close cousins, reliability (33%) and compliance (30%), were second and third, respectively (see Figure 1).

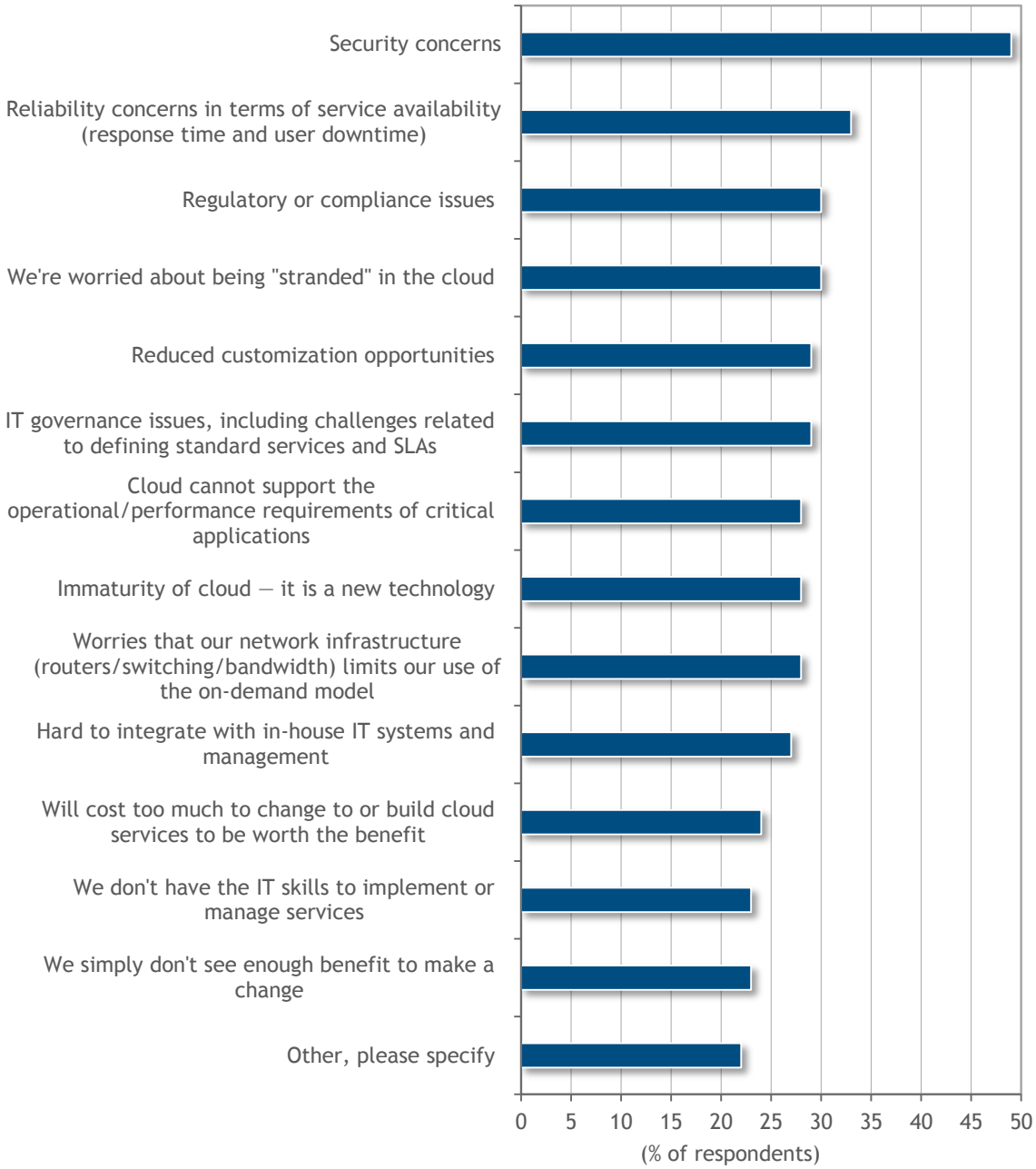
Security is an emotional topic for enterprises, and they are loath to relinquish the only semblance of security they can count on — control. There is a perception that the cloud takes away this control but not the corresponding accountability.

This white paper dispels cloud security myths and lays out a framework for assessing risk while comparing existing complex datacenter environments with new architectures in the cloud (including all the hybrid variations in between). It ultimately shows how enterprises can be, and likely will be, more secure in the cloud.

July 2015, IDC #257920

FIGURE 1

Top Cloud Adoption Concerns



n = 1,581

Source: IDC's *CloudView Survey,* 2015

Thinking About Cloud Security Means Taking a Wider View

Emotions often run high when discussing the security of cloud architectures. People often combine initial impressions with bits and pieces that they've read online to conclude that security is a problem in cloud environments. This is simplistic, or at least incomplete, thinking.

The debate about whether the cloud is more secure or less secure than the datacenter began when public infrastructure as a service (IaaS) started to gain mindshare in enterprises. IaaS opened up the possibilities of new IT architectures for organizations and forced consideration of its viability from a security perspective.

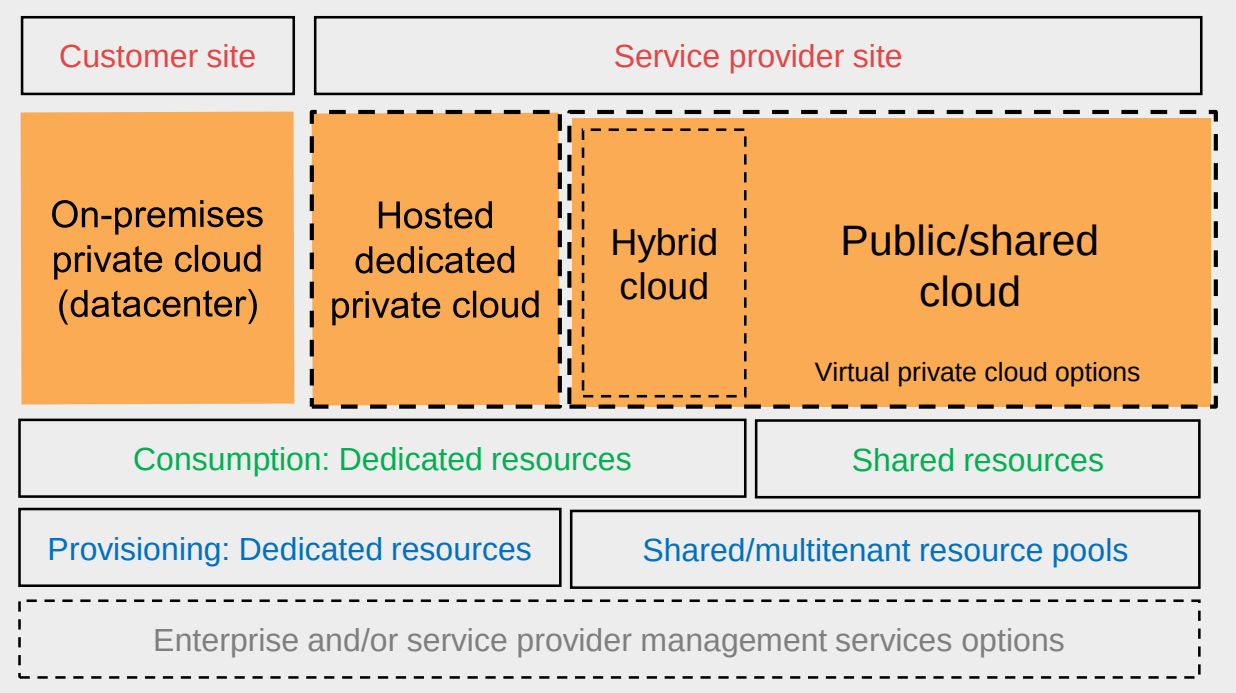
Today, many cloud architecture options provide various levels of control and operate at different levels of risk tolerance. IDC works with a model that identifies options based on location of resources, management responsibilities, and extent of shared resources (see Figure 2).

There is a perception that the move to shared resources and externalized management follows a general path from lower risk to higher risk. Simply put, inherent risk increases from left to right across Figure 2 as more resources are shared and the corresponding levels of separation move from physical to logical modes.

But that doesn't really tell the security story. That is, although *perceived* inherent risk may be increasing, CISOs really need to take a wider view. To properly assess the risk of a particular cloud environment, a CISO as a technology risk manager must first understand how risks change and then understand how control environments can be applied to address those risks.

FIGURE 2

Cloud Architecture Options



Source: IDC, 2015

Major Risk Factors Are Independent of the Cloud

As with any major changes to IT architectures, it is useful to leverage the concepts of risk management so they can be appropriately applied to new scenarios. This is especially true with contentious topics such as cloud security where the security professional also has the opportunity to apply controls in new ways that can offset the risk most effectively.

Risk is a function of probability (i.e., the chance that some unwanted outcome will occur within a population of events or resources) and magnitude (i.e., the consequences associated with that outcome). In technology risk management, the probability of an unwanted outcome translates to the likelihood of a breach occurring. And this likelihood, in turn, is affected by two components inherent to the nature of system usage: threats and vulnerabilities and controls, which should be used to mitigate and offset the impact of threats and vulnerabilities. Therefore, the technology risk manager assesses risks by looking at the threats and vulnerabilities associated with the cloud architecture and applying controls in context to effectively manage those risks.

If there are no changes in the way systems are used, the threat increases proportionally with increases in sources of activity (e.g., connections), and likewise, the threat decreases with a corresponding decrease in connections. Practically speaking, then, one can look at two scenarios — in this case, an existing IT environment and a proposed cloud architecture — and determine whether the connections and, correspondingly, threats are likely to increase or decrease in volume.

With respect to the destination or the target system side, vulnerability also increases proportionally with the set of resources (e.g., servers, applications) being deployed. As with threats, CISOs can evaluate a proposed cloud scenario compared with the existing on-premises environment, looking for relative changes in computing resources.

By examining both threats and vulnerabilities and applying appropriate controls, the technology risk manager can remove buzz and innuendo from the equation and evaluate the change to threats and vulnerabilities regardless of whether the environments exist on-premises or in the cloud. These major risk factors and corresponding controls are independent of the cloud.

It is worth noting that any company that continues to build out its IT resources is increasing its risk. That is the nature of risk: The greater the value and the higher the usage, the more an organization stands to lose. So the healthiest growth-oriented organizations are also those in which risk is increasing the fastest. However, the levels of risk — and the opportunities for mitigation — can vary significantly across different architecture models.

CLOUD OFFERS OPPORTUNITIES TO DO THINGS DIFFERENTLY

With a more robust understanding of applied risk management, the CISO and the technology risk manager can more effectively compare their organization's current environment with one or more proposed future states by looking at the "marginal utility" associated with the threat and vulnerability differences for each architecture option. With respect to the cloud, an organization must consider the complexity and breadth of its own resources compared with those of the cloud service provider.

One of the more challenging aspects of this type of risk assessment is comparing on-premises with cloud security controls. Since existing on-premises deployments already have an established set of controls in place, it can be difficult to compare one deployment model with another. In addition, there is often an entrenched group protecting "the way things have always been done."

While legacy architectures can rely heavily on these older control models, they are extremely difficult to justify and apply to today's application models.

On the other hand, new cloud environments provide an opportunity to rethink, renew, and reinforce controls that are more likely to match the highly distributed, loosely coupled, component-oriented application architectures being developed today. For example, major problems like the "forgotten server" syndrome associated with incomplete inventories inside datacenters become moot points in the cloud.

In particular, cloud architectures make it easier for organizations to create security models that leverage the following capabilities:

- **More segmentation (separation).** More shared resources means a greater need for more segmentation. In a conventional datacenter, this separation can be very resource intensive, and many organizations believe that the risk is limited. Cloud architectures open eyes to the use of service orientation, grid and mesh communications, and other dynamic capabilities that drive the need for new protection mechanisms.
- **More encryption.** While it seems obvious that public cloud environments need encryption, many organizations have ignored the need inside their existing environments that have often become large and complex themselves. The cloud makes introducing encryption much easier.
- **Stronger authentication.** Enterprises still frequently limit their multifactor authentication capabilities to the edge — remote VPNs accessing enterprise datacenters. The move to the cloud highlights the "anytime, anywhere" use of sensitive applications and reinforces the need for strong authentication everywhere.
- **More logging and monitoring.** Once the bane of any IT shop (as in "too much overhead"), logging and monitoring are facts of life if only to ensure that shared responsibilities between enterprises and service providers have been addressed.

The evaluator who is examining the scenarios involved must determine the nature and extent of a new control environment as well as assess the environment's effect on the risk posture.

COMPLIANCE, RESOURCE SHARING, AND MONITORING AFFECT CLOUD DECISIONS

While there are any number of opportunities to rethink, renew, and reinforce controls when a new deployment architecture is under consideration, on a practical level, cloud risk and security decisions are often driven by three factors: compliance, shared resources, and security monitoring.

Compliance in the Cloud

In the earlier years of the cloud, objections and emotions ran high with compliance as a major barrier. Jurisdictional issues associated with compliance added complexity and confusion to the mix. For some organizations, the perceptions of these problems still exist. Highly risk-averse organizations with low technical knowledge continue to wait for the groundswell of common usage prior to moving in the direction of the cloud as well.

Governing bodies of the rules and regulations are often slow to incorporate new IT architectures such as cloud-oriented architectures. However, the controlling agencies and organizations have recognized the "more secure, less secure" false dichotomy discussed previously and migrated their rules and guidance to reflect the new reality of cloud architectures.

While compliance is a tricky issue due to a lot of variability associated with the personalities and groups involved, there is nothing specific in the most popular regulations to preclude using cloud resources.

The fact is that today, many cloud architecture deployments in production across industries have been audited for compliance with all the major regulations and standards. For example, some financial institutions are already processing personally identifiable information in the cloud and still maintaining compliance.

Shared Cloud Resources

Perhaps the most important consideration in determining an inherent level of risk for a cloud architecture is determining the extent to which resources are shared or, conversely, separated.

Resources can be shared at many different layers. At the network layer, local area networks may be shared among many constituents. Working up the stack, an operating system or a hypervisor may be shared. For SaaS environments, the application code base, operating memory, and database may be shared.

As mentioned previously, the opposite side of the sharing coin is determining what mechanisms are used for separation. Historically, physical separation has been applied at the network layer (e.g., through firewalls), but even now networks routinely separate logically (e.g., using VLANs).

As hinted at in Figure 2, today, cloud architectures often have many different options for separation, such as physical and virtual private clouds, dedicated networks, and dedicated instances. So the level of separation required can be determined and deployed by the customer.

Security Monitoring in the Cloud

With today's complex architectures, security monitoring will make or break a technology risk management program. Instrumenting and logging activities from all resources are key compliance requirements that are often the most difficult to accomplish inside an enterprise. It is easy to see why: These activities take place across the board on heterogeneous platforms, thereby requiring buy-in from the various groups involved.

The monitoring itself can make a difference, too. Make no mistake; the organization still has a significant amount of responsibility in security monitoring and incident response, but service providers often have the best highly trained security professionals on staff looking at how the risk environment affects ongoing operations. These professionals know how risks can be addressed with changes in the security architecture.

Perhaps the key element in security operations decisions revolves around actionable information. While technology risk managers are clamoring for more information that can be leveraged in their never-ending battle to protect their environments, service providers gain the advantage of seeing threat activity across many organizations in real time and can therefore assess situations more quickly and effectively.

THE AMAZON WEB SERVICES SCENARIO

As a leader in cloud deployments, Amazon Web Services (AWS) provides a clear example of how robust capabilities can lead to a more secure environment than an existing or similar architecture in an on-premises datacenter.

Amazon's breadth and depth of security capabilities provide opportunities for security programs that are atypical in traditional enterprises.

Organizations can simply apply the approach described in this white paper to a prospective deployment in AWS. Some typical differentiators that enterprises see when comparing their environments with AWS are as follows:

- **Compliance.** While every organization has the responsibility to ensure its specific architecture is compliant with the applicable regulations and standards, AWS provides a host of resources that demonstrate its own compliance efforts in this area. With so many customers of different types across different industries and in different geographies, AWS must maintain a "clean" program. In addition, AWS can support most, if not all, regional and jurisdictional requirements.
- **Separation.** With its virtual private cloud (VPC) architecture that also leverages built-in firewalls, AWS can provide separation at levels of granularity only being considered in today's on-premises environments. Separating organization's assets from those of other organizations – a key need for cloud security – is straightforward, and taking the next step of internal separation can reduce risk even more.
- **Encrypted communications.** On the data-in-motion front, AWS has broad capabilities to ensure any communications (e.g., on-premises to cloud, cloud to cloud, user to cloud) can be encrypted.
- **Data encryption.** Many enterprises have a difficult time deploying encryption for data at rest. AWS makes tools readily available for encryption and key management, including an option for a hardware security module (HSM).
- **Security monitoring.** With its built-in inventory capabilities, AWS enables a complete understanding of the resources within the environment. With regard to monitoring, user and resource activity can be monitored with AWS CloudTrail and Amazon CloudWatch.

To create a similar environment inside the enterprise that could match the security capabilities available at AWS, an enterprise would need to develop a very robust security program that would require extensive resources. While it may be possible for an organization to build such a program, most organizations will find it beyond their financial means.

CONCLUSION

Determining the relative levels of risk and security strength of any IT architecture requires more than an emotional "gut reaction" to the false dichotomy of a "more secure, less secure" debate. This is particularly true for the cloud with all its options and capabilities. Assessing risk and security is like evaluating a fine wine with its nuances. But even then, the cloud risk analysis can be more objective in its results.

The reality is that many options exist to tip the risk and security equation to one side or the other. In assessing a cloud-oriented architecture at hand, organizations should consider the following points:

- **The existing environment is not as secure as it seems.** Existing environments have never been as secure as they are when they are being compared with cloud environments. The perception, and in some cases reality, of the control on-premises environment drives a bias toward status quo protection, which may be weaker than organizations think.
- **Cloud environments are more secure than organizations think.** The perceived loss of control may be a good thing or a bad thing. More mature cloud service providers are constantly driven by customers to provide strong levels of security while ensuring compliance with all applicable regulations.

- **Adding new controls in the cloud is easier than adding new controls on-premises.** As an organization entertains new cloud architectures, it has the opportunity to rethink, renew, and reinforce controls to meet the needs of the new architecture.
- **Whether environments exist on-premises or in the cloud, organizations can't ignore the risk.** Enterprises that maintain on-premises environments do not get a pass on risk; they are still under attack from all sorts of threats, and so are cloud environments. It is up to the enterprise to determine how to properly address the risk in ways that meets the risk posture of the organization.
- **Organizations can be, and probably will be, more secure in the cloud.** A thoughtful, properly designed security program will be easier to deploy in the cloud and ultimately lead to lower risk.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com