EarthLink BUSINESS™

Whitepaper

Security in the Cloud:

Mitigating Risk Outside Enterprise Boundaries

INTRODUCTION

Traditionally, sensitive data and applications have been deployed, managed, and accessed within the trusted boundaries established by IT. Those boundaries are now bending in response to business and customer demand. Endpoints are now a mix of corporate and user-owned devices. Applications and data are hosted on both enterprise and third party servers, available over private, partner, and public networks. They're housed in both enterprise and third party data centers.

These changes bring about significant business value, enhancing agility, mobility, and collaboration while reducing upfront capital expenditures. But they also present a new challenge: IT no longer controls all the assets, yet is still accountable for ensuring security and compliance.

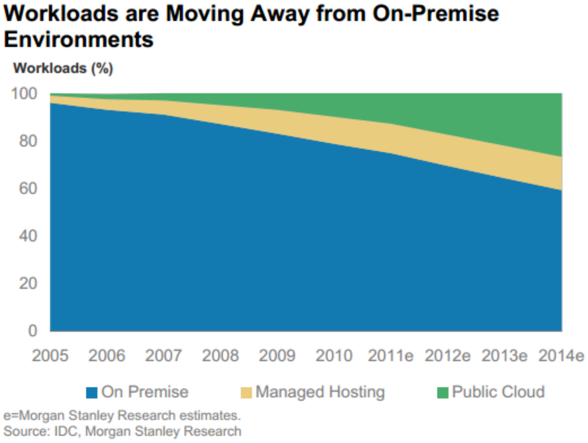
- How do you assess the risks associated with moving to the cloud and third party resources?
- How do you identify gaps in corporate security policies and compliance requirements?
- What additional security measures are required, and who is accountable?

This whitepaper will outline the benefits and risks associated with moving to the cloud, and provide a framework for working with vendors to mitigate those risks.

SHIFT TO THE CLOUD: BENDING BOUNDARIES

The most obvious way to secure digital assets is to lock them down behind network and application firewalls in one's own building. But organizations are heading in the opposite direction, bending boundaries to harness the business benefits of moving to the cloud.

For both SMB and Enterprise businesses, Morgan Stanley predicts workloads in virtualized or private cloud environments to nearly double from 2011 through 2013. SaaS workloads as percentage of total workloads are also expected to more than double in that time period.[1]



There are clear business benefits to moving to the cloud, including the opportunity to reduce upfront capital expenditures, scale up or down based on business needs, improve service with SLA guarantees, and support workforce collaboration and mobility.

> "Today, scalability and cost are seen as the primary drivers for cloud usage, while agility and innovation are quickly emerging as a key factor for adoption"
>
> Future of Cloud Computing Survey (GigaOM, Northbridge Venture Partners, 451 Group).

In many cases business users have driven these changes, maneuvering around IT to gain direct access to SaaS applications. The use of mobile and BYOD (Bring Your Own Device) creates additional risk, as more and more consumer-owned devices are used to access corporate data and applications in the cloud. According to a 2011 ISACA "Shopping on the Job" Survey, nearly one-third of consumers say that they plan to do more shopping than last year using their work-supplied or BYOD device (32%), increasing the risk of malware and other security threats being introduced to the larger organization through personal use of corporate assets.[2]

So– IT organizations are now faced with devices they don't own, accessing data over networks they don't administer, running on infrastructure in data centers they don't host. But rather than fighting the trend, IT organizations are embracing the cloud, both for business benefit and to ensure consistency in areas such as service levels and security.

SECURING THE CLOUD: CONTRACT-IT-IN VS. BUILD-IT-IN

How do you manage security and compliance when you don't host the assets? The very transfer of control of enterprise assets from in-house platforms to the virtual world, coinciding with a widening net of regulatory requirements and security threats means redefining how you select and manage vendor relationships. You can't simply select a cloud vendor based on their ability to support your outsourced data or application requirements. You need to be able to trust that cloud vendor, and ensure that they can support your requirements with respect to security and compliance. Your reputation and your ability to service your user and customer base are in their hands. This is even more critical in industries subject to regulation, such as healthcare (HIPAA), financial services (GLBA), retail (PCI),

> Rather than investing time and resources in establishing a strong in-house security program, IT organizations now need to shift their attention to building a trusted relationship with their cloud vendors.

Today, the standard of security for third party providers largely remains the humble firewall, augmented by web-application and application-aware firewalls that guard against OWASP (Open Web Application Security Project) Top 10 and other known vulnerability exploits. But still, these are provincial in view rather than part of an overall strategy. There are also a variety of point solutions, but no seamless strategy for securing front-end applications or back-end data in a consistent, policy-driven manner. An array of certifications is no guarantee, because they focus on compliance rather than true security.

So with the business pushing for a move to outsourcing, how do you ensure that your risk, in terms of both security and compliance, are covered? IT organizations need to take a new approach: contract it in rather than build it in. Historically, IT organizations have invested in security, compliance, and business continuity by developing the business justification, obtaining buy in, and executing against a strategy. In a cloud scenario, the emphasis shifts to the vendor. That is, assessing and defining your vendors' ability to guarantee service levels, provide transparency where required, and provide vital security services to support your organization's requirements. It also means being clearly aligned on roles and responsibilities.

Many organizations are already taking a proactive approach to ensuring the security of outsourced services. According to a survey of IT organizations by the Aberdeen Group called "Security and Cloud Best practices", almost half are asking their cloud service providers to implement strong security practices.[3]

ASSESSING YOUR RISK

What should you expect of your cloud provider? This depends on the data and applications you are outsourcing, and the compliance requirements and security policies that apply to your organization. If the expectation is that you will safeguard sensitive data such as that related to credit cards, patient data, privacy, or financial transactions, then you need to have that same expectation for your cloud partners.

There is obviously no such thing as risk-free. If transactions are being executed over shared resources, the strategy should be to determine the level of your risk and to either mitigate, transfer, avoid, or accept that risk. Some compliance bodies use the term "compensating controls," i.e. there is a known window of vulnerability, and these are the solutions and procedures put in place to account for that.

Risk is the likelihood of a threat exploiting a vulnerability to produce harm to an asset. It is contextual, and driven by the intersection of assets, threats, and vulnerabilities.

- When identifying and prioritizing risks, considerations include:

- What are the gaps, in terms of corporate, compliance, and security policies?
- What are the possible consequences of a breach, in terms of customer impact, employee impact, penalties, public relations, or share price?
- Various regulations require protection of data, which often translates into encryption. What do your outside auditors require in terms of that encryption? AES 192? AES 256? Triple DES?
- Are you hosting data and/or applications for another party, and if so, what are their expectations and requirements?
- How strong do your password policies need to be?
- What periodic reviews, internal audits, or reporting must be conducted to ascertain the current security posture relative to the risk?

In the end your organization is responsible to your users for securing all the pieces you have assembled for executing transactions and securing the data that result from those transactions; it's critical that you work closely with your vendors as part of your attendant infrastructure.

TEN KEY ELEMENTS OF CLOUD SECURITY

What should you ask your cloud provider?

Once you've selected a short list of vendors and assessed your risk, what should you ask your cloud provider to ensure that they can support you effectively? While your selection criteria and contract requirements may vary, the following questions provide a starting point for ensuring that requirements and responsibilities are clearly understood by both parties.

Security Requirements:

Will your provider work with you to understand your security and business requirements?

When selecting a vendor, make sure they are willing to tailor and integrate a security solution with your cloud service, rather than providing a "one-sized fits all" solution. Roles and responsibilities should be clearly defined and the delineation of responsibilities should align with your organization's needs.

Third Party Certifications:

Does the vendor employ independent and verifiable audits?

The provider should have achieved key certifications, such as SSAE 16 (formerly SAS 70), demonstrating their commitment to maintaining a secure, controlled environment for your data and applications. Ask the vendor if they are subject to periodic validation of their security infrastructure, and if they regularly conduct penetration and other testing to achieve certification or validation.

Service Level Agreements (SLA):

What is included in the vendor's SLA?

The vendor's SLA should include the guarantees required for the applications and data they will be hosting, based on risk assessment, as described earlier in this whitepaper.

Reliability/Business Continuity:

How does the vendor ensure uptime, throughput, and other requirements as defined in the SLA?

Ask the vendor about the procedures they have in place for backup and disaster recovery, and how often those processes validated and tested.

Maintenance:

Does the vendor conduct regular maintenance, patching, and upgrades?

The vendor may offer tiered service options, as well as additional integrated security services such as periodic vulnerability scanning.

TEN KEY ELEMENTS OF CLOUD SECURITY (continued)

VM-Specific Security:

Does the vendor configure security in multi-tenant virtual networks?

If you will be sharing servers with their other customers, ask the vendor how separation is ensured, so that no data or access is shared. This can be established in several ways depending on your requirements, for example by creating private network segments or by installing virtual or physical firewalls.

Secure Access:

How does the provider verify the credentials of users and determine their level of access? Are the endpoint machines accessing the vendor secured?

It's important to discuss how, where, and from what devices applications and data will be accessed, and in some cases your vendor may offer endpoint security or asset management in addition to cloud services.

Data Security:

What controls are in place to protect data in production, in transit, and in backup?

Your requirements may vary based on the sensitivity of the data and regulatory environment. In that context, ask your provider how sensitive data will be protected (such as through encryption or firewalls), who will have access to the data, and what measures they have in place to protect against data loss in the event of a disaster.

Visibility:

Does your provider offer visibility into the security of the hosted service?

Review the tools the vendor provides to give you control over the services they will be providing, and ensure that they can support any reporting requirements required for audits or compliance.

Physical Security:

Does the vendor follow best practices in securing their data center facilities?

Security controls should include badge-protected facilities, 24x7 cameras, and most importantly, a policy on separation of duties and physical access to servers for their personnel. If you are subject to regulatory requirements pertaining to "data jurisdiction", verify the physical location of servers.

SUMMARY

It's no longer a question of whether you should move to the cloud, as the evolution is already well underway, and there are clear business advantages to outsourcing. The question is, can you move to the cloud, and still maintain control of IT security and ensure compliance? The answer is yes, but the approach for mitigating risk is different. Rather than investing time and resources in establishing a strong in-house security program, IT organizations now need to shift their attention to building a trusted relationship with their cloud vendors.

Assess risk and gaps in the context of application/data security requirements, compliance requirements, and enterprise security policies. Incorporate the ability for vendors to support your security requirements into your vendor selection process. Ask the right questions and establish an SLA to ensure that both you and the vendor are clearly aligned on requirements, roles, and responsibilities. Last and most importantly, make it a priority to establish a trusted, long-term partnership with your vendors, as communication and alignment on business goals is critical to long term success.

ABOUT EARTHLINK BUSINESS

EarthLink is a leading IT services, network and communications provider to more than 150,000 businesses. With a comprehensive security portfolio, CISSP® & CISA-certified professionals, SSAE 16 compliant data centers, and over 3,000 deployments across industries including financial services, healthcare, retail, energy, transportation, and government, EarthLink enables businesses of all sizes to mitigate risk as they move to the cloud.

Our security services integrate with our cloud hosting and IP voice and data services, and include application penetration testing, information security, business continuity and disaster recovery, asset management, monitoring, content filtering, firewall, intrusion detection/intrusion prevention (IDS/IPS), laptop security, and secure remote access.

To learn more about how EarthLink can help your organization to mitigate risk, email getinfo@earthlinkbusiness.com, call 1-877-355-1501, or visit www.earthlinkbusiness.com.

References:

1. "Cloud Computing Takes Off", Morgan Stanley Research, May 23, 2011 (http://www.morganstanley.com/views/perspectives/cloud_computing.pdf <http://www.morganstanley.com/views/perspectives/cloud_computing.pdf>)

2. 2011 ISACA Shopping on the Job Survey, Prepared by the Ketchum Global Research Network, November 2011 (www.isaca.org/online-shopping-risk <http://www.isaca.org/online-shopping-risk>)

3. Security and Cloud Best Practices", Derek Brink, Aberdeen Group, July 2011