Whitepaper

Moving Workloads to the Public Cloud? Don't Forget About Security.

Key considerations for developing a cloud-ready cybersecurity strategy

Introduction

For many organizations today, it's not a question of whether they should or should not leverage cloud services. It's a matter of when they should move to the cloud and to what extent.

These services, including public cloud offerings, are compelling for a number of reasons. Among the potential benefits are cost savings, more efficient use of computing resources, greater scalability, and increased agility — to name a few.

Increasingly companies are shifting data and workloads to the public cloud, to take advantage of the cost efficiencies involved in using shared resources that are owned and maintained by a service provider.

The balance of public versus private cloud workloads is relatively even today, according to a new survey, "Stakes Rise for IT: The IT Transformation Journey," by IDG Research sponsored by Datalink, a division of Insight. But despite this, respondents cite concerns regarding their choice to deploy workloads in a public cloud platform, with the most critical worry being security. Compliance, performance concerns, and a perceived lack of control are also high on the list.

Organizations need to have a thorough understanding of the data and applications being moved to the cloud, and of their governance model in place. Lacking these critical pieces of knowledge can result in untentional data disclosure events or other unwanted vulnerabilities in the new environment.

And yet there is still much confusion, even among many IT and security leaders, about who is responsible for which aspects of cybersecurity when a company uses cloud services. In the rush to deploy these services quickly in order to reap the benefits, security often gets left behind as a consideration.

This whitepaper explores some of the main issues and challenges companies are facing as they consider their public cloud strategies, and offers a few best practices for creating a cybersecurity strategy that will help them use the public cloud as securely as possible.

Public cloud and security: confusion reigns

When it comes to information security and the public cloud, many organizations today are not completely clear on who is responsible for which aspects of security — and therefore they are not prepared for the cloud from a security standpoint.

There is a common assumption that the cloud service provider, whether it be Amazon Web Services (AWS®), Microsoft®, Google, or some other provider, is responsible for ensuring that all data and applications in the cloud are safe from intrusions at all times.

Industry research shows that there are clearly a number of misconceptions about security and data management when it comes to the cloud. For example, a 2017 study by research firm Vanson Bourne and data management provider Veritas™ showed that more than two-thirds (69%) of 1,200 global business and IT decision makers wrongfully believe their organization's cloud service provider covers all data privacy, regulatory compliance, and data protection.

A huge majority of the organizations surveyed that use or plan to use Infrastructure as a Service (IaaS) offerings (83%) think their organization's cloud providers will be protecting their workloads and data against outages, and more than half (54%) think it's the responsibility of the cloud service provider to securely transfer data between on premises and the cloud. About half (51%) think the cloud service provider is responsible for backing up workloads in the cloud.

In addition, the assumption that an organization's current governance model and security controls will be sufficient for all cloud-based workloads is shortsighted. Governance models should be updated to include cloud considerations. Current methods of authentication, access control, encryption, and monitoring should all be reviewed to ensure compatability and compliance with cloud initiatives.

Public cloud security responsibilities

Cloud security ownership varies by cloud service type.

Cloud service type	Administration	Applications	Data	Runtime	Middleware	O/S	Virtualization	Servers	Storage	Networking
Infrastructure as a Service	✓	✓	✓	✓	✓	—	—	—	—	—
Platform as a Service	✓	✓	✓	—	—	—	—	—	—	—
Application as a Service	✓	—	—	—	—	—	—	—	—	—

✓ Internal IT responsible — Service provider responsible

A common oversight is that organizations don't conduct needed due diligence before going to the cloud for a variety of reasons. Companies often do not take workload dependencies into account before moving workloads to cloud. They might also neglect to take the time to identify all the different types of data they have and classify them from a risk perspective. In addition, some believe that public cloud providers provide all necessary security measures. The belief is that the comprehensive security offered by the cloud providers combined with the existing provisions of the company using a cloud provider are more than enough to stop data breaches from happening. If one or more of the oversights discussed above are in play, IT leaders may create a false sense of security when leveraging the public cloud.

Perhaps this confusion about security should not come as a surprise, given that there has been somewhat of a rush to deploy cloud-based services in order to reap the business benefits as quickly as possible. In many cases, line-of-business executives or departments might be the drivers for moving to the cloud, and security sometimes gets lost in the shuffle. A lot of this stems from the shadow IT movement of recent years, in which business users or executives deploy cloud services without central IT even knowing about these undertakings.

In actuality, companies that use public cloud services hold a great deal of the responsibility for ensuring the safety of their own data — and security of data in the cloud goes well beyond whatever existing internal security tools and governance models might be in place. Handing off workloads to a cloud provider does not mean relinquishing accountability for security, or being satisfied with the status quo.

The scope of responsibility for security might vary depending on the cloud service provider being used and the types of cloud services. For example, internal security needs for Platform as a Service (PaaS) and IaaS might be different.

But the fact remains that IT leaders who are utilizing public cloud services cannot expect to leave all elements of security up to the cloud vendor, or rely on traditional approaches to data protection. To do so is inviting a host of potential issues that can end up costing a lot in lost or stolen data, law suits from customers and business partners, lost business, damaged reputation, etc.

This is not an issue of cloud providers being lax in terms of protecting their own infrastructure. In fact, the leading cloud providers have built some of the most secure environments possible, because much of their business model relies on having robust security in their data centers and networks.

Despite the efforts of the cloud providers to bolster security, however, there are no guarantees that all the data owned by companies who use public cloud services will be safe at all times.

Best practices for protecting data and workloads

Enterprises need to follow a number of best practices in order to help ensure the security and integrity of the data and workloads they plan to move to the public cloud.

One of the first things companies need to do is review and update their existing governance model. This is true whether or not they're moving workloads to the cloud — but it's particularly important when shifting data and workloads to the public cloud.

As part of creating this model, they need to identify and understand all of the data they have that needs to be secured, mainly because of the sensitivity of the information but also because of regulatory requirements.

Consider the regulations and compliance requirements that could come into play with data in the cloud. These include Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley 404 Audit (SOX 404), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR) — to name just a few.

Does the company gather and store customer credit card data, personal health information, or customer or employer data that is personally identifiable? Other questions to ask as part of the assessment: Is the company publically traded, does it do work with the federal government, does it process information that originated in the European Union, and is the company considered part of the nation's critical infrastructure? All of these factors come into play to some extent with one or more regulations.

Good governance also means being smart about deciding which workloads are best suited for the public cloud, and which are better suited for a private cloud or on-premises systems. To do so, a comprehensive assessment of each workload should be carried out. Assessments typically span the following areas:

Technology

This includes in-depth discovery and analysis of your current application workloads and their interdependencies with infrastructure. The data that makes up each workload should also be analyzed.

People

Comparing the current state of organizational roles and responsibilities to the desired future state, and evolving the organization from do-it-yourself to managing workloads in public, hybrid, or private IT service delivery models.

Process

Assessing the current state and maturity of key operational processes and business services offered, along with identifying any roadblocks or inhibitors to moving forward.

Finance

Obtaining baseline financials, defining investment costs, reviewing potential "future state" optimized IT models, and developing a financial benefits analysis.

Another aspect of governance is putting the right processes in place, including how to address issues such as shadow IT. If the governance model is done correctly, it should enable organizations to securely move workloads into the public cloud; ensure that appropriate security controls are in place; provide security visibility of cloud resources; meet regulatory and compliance requirements; and mitigate the risk of data outside the traditional corporate perimeter.

The desired outcomes of a governance model are effective cloud security operations, verified security posture, comprehensive security governance, auditable security controls, and a cloud capabilities roadmap.

As part of the governance planning and execution process, enterprises need to involve representatives from several key groups within the organization. These include IT, cybersecurity, legal, human resources, and line-of-business executives.

Other senior executives to include in the cloud governance effort — or at least keep informed — are the CEO, CFO, CIO, and CISO. Cybersecurity has become so critical to the day-to-day operations of companies that to exclude the most senior executives in the company from the governance discussion is a big mistake. If a company suffers a major data breach that exposes customer or employee information, the CEO and other top officials might be held accountable.

Within the IT/security domain, others to include are the director of networking, SOC manager, security analysts, and network administrators. These are the people who will handle or oversee much of the detailed work that needs to be done to put proper controls in place.

Once the governance model is complete, it needs to be tested and verified. Are all the needed security controls working as expected? Are protocols being followed by users? Are applications and workloads behaving as they should on the public cloud, or has user experience been impacted in a negative way?

Another key practice is to provide training for all end users in the organization about security issues related to the cloud. Cybersecurity is everyone's responsibility — not just the security team's — and as such employees must be aware of the threats and vulnerabilities and what they need to do to ensure data protection.

The cloud represents new ways of doing things, and that might create cultural challenges and resistance from some in the organization. But it's up to IT and security management to make sure everyone is onboard with the security program and controls in place. Some of the weakest security links can come from inside the organization.

Aside from governance and training, a big part of delivering strong security in a public cloud environment is deploying the right security technology tools. Companies need to leverage the latest solutions that enable them to manage and control their cloud environment in much the same way as they manage and control their on-premises infrastructure.

Among the key security technologies to consider are identity and access management including multifactor authentication; encryption and key management; mobile security platforms; security incident and event management; threat and vulnerability management; and application and interface security.

Ideally, organizations will have the fewest number of security management consoles as possible, in order to reduce the complexity of security management.

As they begin to move workloads into the public cloud, enterprises need to assess the performance of the workloads to make sure they are performing as expected based on the earlier testing. Are they meeting availability, quality, and user experience requirements?

Last but certainly not least, organizations need to thoroughly evaluate and compare the security offerings of the public cloud providers they are considering. When it comes to security, availability, reliability, and other issues, not all providers are alike and companies who are leveraging public cloud services need to ask a number of questions when making evaluations. For example:

- What sort of directory services platform do they have, as well as what kind of authentication and authorization platform do the providers offer?
- Do they offer information protection?
- What type of encryption technology do they provide and what do they encrypt?
- What types of firewalls do the cloud providers have deployed to protect their infrastructures?
- What compliance provisions do they have in place?

Conclusion and call to action

Moving data and workloads to one or more public cloud services might be a great business decision for a company, but it cannot be a decision that's made lightly and without serious forethought of the potential security consequences.

At many organizations today, the prevailing strategy is to move to the cloud first then think about security later. It's a natural competitive instinct to want to reap the benefits of this efficient IT delivery model as quickly as possible. The compulsion to shift to the public cloud is especially strong when the cloud providers are touting how secure their infrastructures are and how much organizations who are leveraging public cloud services can expect to save on IT costs.

Despite these temptations, it's critical that enterprises not fall into the trap of jumping into the public cloud without first evaluating data and workloads and ensuring that the appropriate security measures are in place.

Certainly IT executives appear to be aware of the security risks. According to the IDG/Datalink report, which surveyed 142 U.S. IT executives online in September 2017, about three-quarters (76%) of those surveyed report being more cautious versus one year ago when making the decision to move particular applications or workloads to a public cloud.

Security is the top concern about the public cloud, even among those who have chosen to deploy applications on a public cloud platform. It was cited as a concern by 58% of the respondents, well ahead of the next most common concern, meeting compliance requirements (41%).

A good number of the organizations surveyed (52%) have actually moved applications and workloads away from the public cloud to an on-premises model. This is an increase since 2016, when 38% reported such a move. Concerns about control over resources or data and the pressure to meet compliance requirements are among the top reasons for moving away from the public cloud.

But there's no need for companies to abandon the cloud as a strategy and potentially miss out on the benefits. They just need to take the right approach and follow best practices. To that end, security should be a major component of the digital transformation strategy, not a bolt-on afterthought.

Depending on which industry a business is in, having strong security can even be a competitive differentiator. In that case the benefits include not only better data protection as workloads move to the cloud, but potentially more customers and revenue.

To learn more about what organizations can do to enhance security when using public clouds, visit datalink.com/Solutions/Security.

Highlights:

More companies are shifting data and workloads to the public cloud, to take advantage of the cost efficiencies, agility, resiliency, stability, and scalability involved in using shared resources that are owned and maintained by a service provider.

There is still much confusion, even among many IT and security leaders, about who is responsible for which aspects of cybersecurity when a company uses cloud services.

The scope of responsibility for security might vary depending on the cloud service provider being used and the types of cloud services.

Enterprises need to follow a number of best practices in order to help ensure the security and integrity of the data and workloads they move to the public cloud, including: review and update their existing governance model; identify and understand all of the data they have that needs to be secured; consider the regulations and compliance requirements that could come into play with data in the cloud; assess which workloads are best suited for the public cloud; test and verify the governance model; provide training for all end users in the organization about security issues related to the cloud; deploy the right security technology tools; assess the performance of workloads once they're in the cloud; and thoroughly evaluate and compare the security offerings of the public cloud providers under consideration.

About Datalink

Datalink, a division of Insight, is a complete IT services and solutions provider that helps companies transform their technology, operations, and service delivery to meet business challenges. Combining extensive experience, a full lifecycle of services, and a comprehensive approach to producing IT innovations that empower positive business outcomes, Datalink delivers success across cloud IT transformation, next-generation technology, and security.

Learn more at:
datalink.com