ANOMALIX

ANOMALIX
WHITE PAPER

Mitigating The Risk Of Operating In The Public Cloud



Mitigating The Risk Of Operating In The Public Cloud

Public Cloud Benefits

Public Cloud Infrastructure services offer reliable, cost effective solutions for enterprises of all sizes. Platforms offered by Microsoft, Amazon, Google and other large Cloud Service Providers (CSPs) offer their "public cloud" to organizations who need Infrastructure as a Service (IaaS), data storage, and Software as a Service (SaaS) solutions.

While it's typically more expensive to operate a Private Cloud, many organizations continue to use Public Clouds because of their cost effectiveness, data storage, reliability, and scalability. Leading CSP's also offer advanced technical solutions that may be unavailable to server-based networks or private cloud users.

CSP services offer speed-to-market, especially for high growth corporations. But organizations remain liable and accountable for data protection and cloud operations. Handing over data and development operations (DevOps) to a CSP (or multiple CSP's) has inherent security risks to understand and manage.

Public Cloud Growth

According to Gartner, the number of CSP's is expected to triple within the next year. The growth and adoption of cloud services also means increased risk as more providers enter the market. Security and Compliance executives remain concerned about rapidly expanding applications and data stored in the cloud, changes in CSP contract terms, customer responsibility, and potentially unknown, third-party access to cloud data.

CSP's are turning to Artificial Intelligence (AI) to remain competitive in their cloud management products. But a competitive job market combined with a shortage of skilled AI professionals may leave these companies without the expertise they need to deploy their solutions effectively. This could impact the services they sell and their client base.

All of this adds up to a growing need for cyber security solutions as well as infrastructure and data access governance solutions to operate, manage and control their clients' data and applications..

Conducting Due Diligence

CSPs provide the infrastructure, but companies remain responsible for infrastructure configuration and data protection. Given this responsibility, due diligence is critical to choosing a CSP.

Experienced CSPs will have protocols in place to safely transition information from the current architecture (server-based or other CSP) to their public cloud. It may be advisable to select multiple CSPs in order to diversify risk.

Credible CSP's will provide a well-crafted transition plan to develop and deploy an organization's data and processes into the public cloud. A proven CSP will offer not only cloud services, but expertise in project management and deployment. The chosen CSP should also assist in monitoring the production environment before fully implementing the cloud solution. Decommissioning may also be required when transitioning from one CSP to another.

VISION

Shared responsibility for data security

A company's primary responsibility is to limit access and protect data without reducing employee productivity or causing a poor customer experience. Whether it is customer data, corporate IP, patient data, or internal financial data, a company maintains responsibility for its safety and privacy no matter where it is stored.

Cloud Operations Management

Cloud operations are designed to scale infrastructure necessary for growing companies to adapt and grow, but not overburden their IT and Security departments. Advanced tools are required to prevent accidental misconfiguration that may expose sensitive data and increase risk. Cloud operations provide a significant enhancement over traditional server-based systems. They reduce manual and redundant processes that increase both cost and risk.

Industry best practices developed by NIST, CIS, and PCI provide the blueprint for effective and efficient cloud operations. In addition to federal and trade guidelines, existing policies and procedures should ensure consistent cloud operations management that are in alignment with business goals. Cloud operations management includes not only instituting these best practices, but providing instant notification when standards, policies, or procedures have been compromised.

Effective cloud operations allow companies to remain secure and compliant, but also provide alerts and notifications in the event of a malicious attack. Quicker notification leads to timely resolution of the issue and reduction of associated financial risks and costs.

Infrastructure Governance

Infrastructure Governance are the policies and procedures that allow certain users the rights to perform distinct functions. In an IT context, this is achieved first through infrastructure configuration policies and procedures and secondly through Identity Access Management (IAM).

It is vital to put access controls in place that identify user roles and assign appropriate access. Identify Access Management (IAM) systems provide the framework that assigns the right access to the right users which often include Multi-Factor Authentication (MFA) to ensure that data stays protected.

The first step is to assign user access rights and require that IT and Security departments understand not only the individuals who need access, but what role they play, and what access they need to perform their job. This can be a daunting task, but using proven effective solutions, CSP customers can drastically reduce the burden on DevOps, Security and Compliance teams.

Once user access is in place, there should be policies and procedures to enforce those protocols. Organizations should coordinate with their CSP to implement those policies and understand what limitations or protocols they require for deployment. The result is a holistic cloud governance system that prevents unauthorized access, ensures appropriate infrastructure configuration, and guards against compliance violations.

Reduced Risk of Network and Host Threats

While a cloud platform has many benefits, professionals must still guard against two types of threats. First, network threats may arise from malicious external parties or inadvertently within the network. Organizations need to protect their network by identifying potential threats from unknown IP addresses and other sources that result in crypto-jacking, ransomware and other breach-related activities.

Server-based environments may not offer the enhanced monitoring tools necessary to quickly identify and alert professionals to suspicious activities. CSPs are not responsible for insecure access configurations to applications, data or infrastructure. CSP customers are often struggling to become cybersecurity companies to ensure access to cloud applications and data are secure.

Threats can also occur within the host system if patches or misconfigurations happen. It is imperative that DevOps and Security teams are quickly notified to prevent a potential attack. CSPs do not offer real-time monitoring to remain compliant and provide alerts of security maintenance and failure.

Conclusion

Anomalix focuses on ensuring that your data access program is robust, compliant, and secure. We work with companies to ensure their onsite and cloud service data is protected by ensuring that data access meets all standard and advanced protocols.

IdGenius public cloud protection enables threat defense and continuous compliance assurance. *IdGenius Total Cloud* Protection Platform, a cloud native SaaS solution, uses the next generation of AI and machine learning to identify, correlate, and monitor and audit security and compliance activity. With IdGenius, organizations are empowered to govern security and enable security operations across multiple public cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

Benefits of using IdGenius include reduced financial risk due to security breaches, reduced cost of compliance reporting as well as reduced security operations costs associated with manual and redundant activity.

Where to Begin

If you currently operate in a server-based environment and are considering a public cloud solution, you should start by evaluating your level of risk. How much is your firm ready to invest to reduce the potential risk of data loss or adverse events? Your level of investment will provide the baseline of what solutions are available.

Next, identify specific risks to your data, hardware and software, customers and reputation. This will help identify where you are most vulnerable and where investment is most needed. Considering not only today's risks, but the potential issues that may arise on a one, three, or five year time horizon must be considered.

Once your specific issues have been identified, it's time to choose a CSP. How do you know if you are choosing the right one for your company? First, look to fit. Your CSP is a long term, day-to-day relationship that needs to be a cultural and logical fit. Their sales brochure will tell you what they do, but vendor interviews are the chance to understand how they work with their clients.

A critical part of your public cloud solution are tools that provide scalable infrastructure, infrastructure governance tools, and network reporting features that allow your team to be proactive. Finding a solution that is rigorous, but doesn't impede workflow and productivity, means you need a vendor solution that will help you navigate both culture and compliance issues.

Finally, make sure you have executive support. Cloud solutions are long term investments that impact a company's most important asset: their data. Making sure executives understand why you need a cloud solution and how it will benefit the company for the long term is essential to getting critical C-suite support for the project.



Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144