HOW AND WHY CLOUD CUSTOMERS MUST PROTECT THEIR DATA

Cloud adoption has accelerated IT modernization through simplified scalability, reduced OpEx and the technical flexibility to transform IT models based on evolving business requirements. At the same time, cloud adoption has also disrupted the traditional security models designed to secure data and apps operating via on-premise servers.

Consider the recent N2WS survey of 750 re:Invent attendees, with 40 percent spending over $100,000 monthly on AWS cloud offerings. According to the survey, 25 percent of the respondents were using scripts to back up their AWS data, while 23 percent had no backup solution at all. While 36 percent were working on a disaster recovery strategy, 45 percent of the respondents had no disaster recovery plan in place.

These findings suggest that customers rely heavily on cloud vendors to secure the infrastructure, assuming their data is inherently secure within well-protected cloud environments. In reality however, the customers themselves are responsible to ensure that their data is always available, protected and recoverable based on the necessary technical and business requirements. These requirements may lead to additional security challenges for organizations handling confidential government data, serving tightly regulated healthcare industry or required to comply with the EU GDPR legislation, among others.

The transformation of IT toward a shared cybersecurity responsibility model involving multiple vendors across the hybrid infrastructure environment requires a strategic approach for the design,

development and implementation of a cloud-centric security program. An effective data security protection program for cloud environments can include the following strategies and best practices:

Plan for Security

Define the unique security profile for various cloud environments deployed or proposed for your organization. The process may begin from defining the scope and boundaries of the infrastructure requirements, leading to the definition of Information Security Management Systems (ISMS) policy for your cloud-bound data assets, apps and processes.

Understand the various deployment models in context of your risk tolerance, security and compliance considerations as well as potential risk exposure to data, apps, processes and end-users. Map the data flows between your organization, cloud environments and end-users to determine the appropriate security protocols and control frameworks for each workload. This information will enable your IT to support the diverse security needs of multiple data sets and services, tools and capabilities required to protect sensitive data. Further management approval would also be required to account for the residual risk that may appear despite the security controls in place.

For different cloud solutions, it's important to work with the vendors to understand the true requirements of the shared security responsibility model.

Mitigate Vulnerabilities

For dynamic cloud architecture models, the perimeter of security controls may deviate and require organizations to take additional measures in protecting their assets in the cloud. It's important to understand that cloud networks are not physically separated and isolated like the traditional on-premise network infrastructure. Organizations must build security from the ground up, extending security across all layers of the network that may evolve over time. The following controls and best practices can help mitigate risk associated with the cloud-bound assets:

- Encrypt the data at rest, in process and in transition between the networks. Healthcare, defense and governmental institutions may enforce stringent encryption requirements for data security in cloud environments where data workloads shift dynamically across a scalable infrastructure network.
- To protect the data at rest, manage access privileges to limit access to confidential information. Employ the principle of least privilege that allows users the bare minimum controls over the data as necessary. Extend these controls to prevent data integrity compromise, through resource permissions, data integrity checks, backup, replication and versioning.
- To protect data in transit, encrypt the data and ensure that data can survive potential availability issues and outages. Infuse redundancy into the system so that data can be replicated at the application level and remain accessible as required. In addition to protection against data disclosure and modification, organizations must also ensure the communication channels are equally protected against identity spoofing and man-in-the-middle attacks.
- Establish trust controls across federated cloud environments between multiple vendors and delivery models. This means that organizations will be required to manage identity and access, authentication, audits and API security across multiple cloud vendors and infrastructure. Understand how these controls can be standardized, prioritized and automated across the

hybrid cloud environments through a DevOps approach. For controls that cannot be automated, organizations must train their workforce to follow the necessary standardized procedures.

Choosing the Right Cloud Vendor

Data security in the cloud is not just a technological decision but also a business decision evaluating the cloud options from a high level. This involves considerations associated with the vendor's security and risk management practices, financial stability, transparency toward compliance, long term strategy and past track record in relevant contextual situations.

The choice may be influenced by the vendor support to facilitate customers in fulfilling their role of the shared cybersecurity model. This may be through tools, service management support or policies that make it easier for their customers to manage access, backup and disaster recover, and compliance based on unique business requirements.

At the same time, if the vendor has a history of compliance failures, costly outages or an uncertain financial outlook for the future, it may not be able to deliver services long into the future. This uncertainty adds to the risk of data access, availability and security in the future for customers of the cloud service.

Additionally, account for the cost and vendor policies associated with terminating the contract and moving data to another datacenter. A cloud vendor may lock organizations into their services through low-cost options for small-scale use cases while charging exponentially higher for large-scale services. Worst yet, the data and application transfer risk between cloud vendors or data centers could be a technical and cost nightmare. The migration process may raise questions around the responsibilities associated with performing the data migration, ensuring availability throughout the migration procedure and reconfigurations that may be required for your apps to work with another cloud infrastructure. At that point, organizations may be forced to tradeoff data security, availability and performance by reducing operating expenses to survive the vendor lock-in.