The top 3 multicloud security challenges and how to build strategies

Some of the best security practices have appeared with the development of multicloud environments and there are several important steps that all organizations should take when they develop their own security strategies.

According to security experts, some of the best security practices have emerged with the development of multicloud environments and there are some important steps that all organizations should take when they develop strategies. Security of their own.

Data breaches or intruders warning will make security groups more active in preventing damage and identifying the cause.

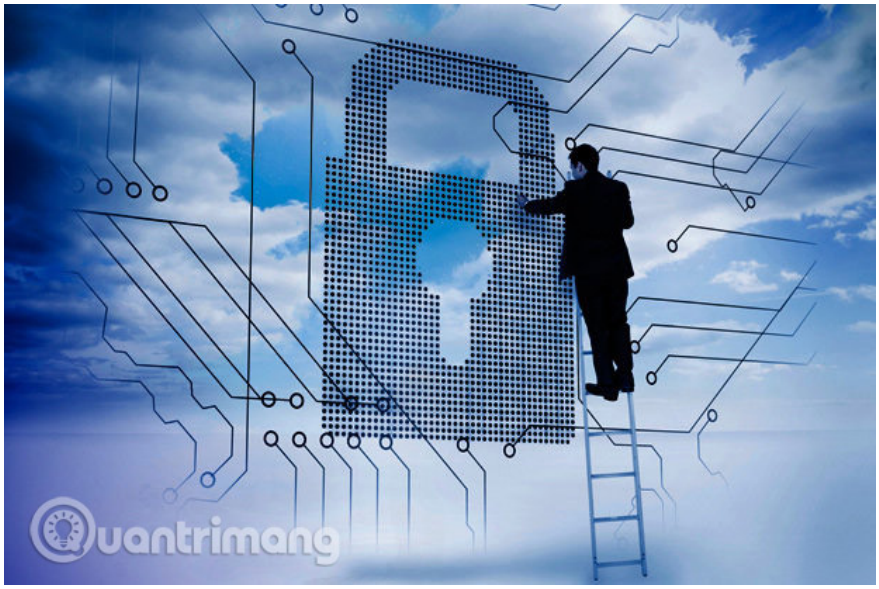
That task is always challenging even if a real IT person runs all activities on his or her own infrastructure. This task is becoming increasingly complicated because organizations have moved their workload to the cloud and then to many cloud providers.

The 2018 cloud activity report from RightScale, a cloud service provider, found that 77% of technology experts (equivalent to 997 respondents) said cloud security was a challenge, and 29% of these think it is a huge challenge.

Security experts say they are not surprised, especially given that 81% of RightScale's survey respondents are using a multicloud strategy.

'Multicloud environments will make the way you manage and manage security controls more complex' - said Ron Lefferts, managing director and chief technology consultant of the consulting firm. Reasoning Protiviti.

He and other security leaders say organizations are very active in maintaining high security when they move more workloads to the cloud.



Top multicloud security challenges

1. Multicloud security challenge
2. Build multicloud strategy
3. Set expectations for suppliers
4. Use of current new technologies

Multicloud security challenge

But they should also admit that the multicloud environment comes with the challenges that need to be addressed. This is part of a comprehensive security strategy.

Christos K. Dimitriadis, director and former chairman of ISACA, a professional association, focusing on IT governance, said: 'In this multicloud world, the prerequisite is coordination. between technology and human intelligence. Now if something goes wrong, you need to make sure that all entities are coordinated to identify violations, analyze and develop improvement plans for more effective control. "

Here are three factors that experts think are complex security strategies for multicloud environments.

1. **Increasing complexity** : Coordinating security policies, processes, and feedback from multiple cloud providers as well as a wide range of extended access points will increase complexity.

Juan Perez-Etchegoyen, a researcher, co-chair of the ERP Security Working Group at the non-profit Cloud Security Alliance (CSA), said: 'You have a data center extension in many places. gender. And then you must comply with the regulations of all countries or regions where you are located data centers. The number of regulations is very large and increasing. These regulations are driving control and mechanisms that companies need to implement. All of which increases the complexity of the way we protect data. '

1. **Lack of visibility** : IT organizations often do not know all cloud services are being used by employees, who can easily bypass enterprise IT strategies and purchase software services under service type or other

cloud-based services.

"Therefore, we are trying to protect data, services and the business itself without having to understand the location of the data," Dimitriadis said.

1. **New threats** : According to Jeff Spivey, founder and chief executive officer of Security Risk Management Inc., business security leaders should also recognize that rapid development of the environment Multicloud can give rise to new threats.

"We are creating something new, at which we have no knowledge of all security holes. But we can detect those holes as we continue to move forward." , he said.

Build multicloud strategy

According to security experts, some of the best security practices have emerged with the development of multicloud environments and there are some important steps that all organizations should take when they develop strategies. Security of their own.

The first thing to do is to identify all the clouds where the data is' residing 'and make sure the organization has a powerful data management program -' a complete picture of the data and services, as well as IT assets related to various types of information '(according to Mr. Dimitriadis).

Mr. Dimitriadis is also the head of information security, information compliance and intellectual property protection department at INTRALOT Group, the solution provider and operator, acknowledging that these security proposals Not only is provided for multicloud environment.

However, he said that having such basic on-the-spot measures is becoming more important than ever, as data is gradually "moving" to the cloud and spread across multiple cloud platforms. different.

Statistics show why having a strong security base is important. Report on the threats from the 2018 cloud of KPMG and Oracle, which surveyed over 450 IT and security experts, reported that 90% of businesses classify half of their cloud-based data. They are sensitive.

The report also found that 82% of respondents fear that employees do not comply with cloud security policies and 38% have problems detecting and responding to security incidents in the cloud.

To combat such situations, businesses should classify information to create multiple layers of security - said Ramsés Gallego, a leader at ISACA and a missionary at the CTO office at Symantec. This tells us that not all data requires the same level of trust and verification to access or lock.

Security experts also advise businesses to implement other common security measures on the foundation layers needed to protect the multicloud environment. In addition to the data classification policy, Gallego proposed using encryption, identity and access management (IAM) solutions such as two-factor authentication.

Businesses need to standardize policies and structures to ensure consistent application and automation as much as possible, to help limit deviations from those security standards.

'The level of effort a company poses will depend on the risk and sensitivity of the data. So if you are using the cloud to store or handle non-confidential data, then you don't need the same security method as a cloud holding important information, 'Gadia said.

He also noted that standardization and automation are very effective. These measures not only reduce the total cost, but also allow security leaders to direct more resources for higher value tasks.

According to experts, such fundamental factors should be part of a larger and more coherent strategy. Note that businesses will do everything well, as they apply a framework to manage security-related jobs. Common frameworks include NIST of the National Institute of Standards and Technology; ISACA's control objectives for information technology (COBIT); ISO 27000 Series; and Cloud Security Alliance Cloud Control Matrix (CCM).

Set expectations for suppliers

According to Dimitriadis, the selected framework is not only oriented for businesses but also suppliers.

'What we need to do is combine those frameworks with cloud service providers. You will then be able to build control measures around the data and services you are trying to protect, 'he explained.

Security experts say negotiations with cloud service providers and subsequent service agreements will address data isolation and how data is stored. They will cooperate and coordinate with other cloud providers, then provide services to businesses.

Be aware of the services you are getting from each provider and whether they are able to manage and run the service.

"Be specific about what you expect and how to get there," said Spivey. 'There must be a clear understanding of the services you receive from each provider and whether they are able to manage and run it.'

But according to Mr. Gallego, do not leave security issues to cloud computing service providers.

Cloud service providers often sell their services by emphasizing what they can do on behalf of business customers and often include security services. But that is not enough. Remember that these companies are in the cloud computing business, not in the security field.

Therefore, he argues that business security leaders must build their security plans at a level of detail, such as who has access to what, when and how. Then give it to each cloud provider to support implementation of those plans.

He added: 'Cloud service providers need to win customers' trust.

Use of current new technologies

Policies, administration, and even common security measures such as two-factor authentication are essential, but not enough to handle complex issues that arise when dispersing workloads. on many clouds.

Businesses must adopt emerging technologies, designed to allow enterprise security teams to better manage and enforce their multicloud security strategies.

Mr. Gallego and other researchers point out solutions such as Cloud Access Security Brokers - CASB, a software tool or service located between the on-site infrastructure of the organization and the provider infrastructure. Cloud to strengthen and enforce security measures such as authentication, mapping authentication information, saving device information, detecting encryption and malware.

The tool also lists artificial intelligence technologies and then analyzes network traffic to accurately detect abnormal phenomena that need attention, thus limiting the number of incidents to be verified, rather which redirects those resources to problems that can cause serious consequences.

And experts cite continuing use of automation as an important technology to optimize security in a multicloud environment. As Spivey notes, 'Successful organizations are multi-part automation organizations and focus on governance and management.'

In addition, Spivey and other researchers have argued that although the exact technologies used to secure data through multiple cloud services, such as CASB, may be unique to the environment. multicloud. Experts emphasize that the principle of overall security follows the long-term approach to both people and technology to build the best strategy.

'We are talking about different technologies and scenarios, focusing more on data, but it's like the concepts you have to implement,' said Perez-Etchegoyen, also the CTO of Onapsis. know. "The technical approach will be different for each multicloud environment, but the overall strategy will be the same."

See more:

1. Cloud computing and 10 common security questions

2. How to integrate cloud storage with work
3. The challenge of cloud computing

You finished reading the article "**The top 3 multicloud security challenges and how to build strategies**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
