SECURITY THREATS IN THE MULTI-CLOUD

Today, a majority of organizations are not only actively moving most of their workloads to the cloud, but many of them are also using a multi-cloud model. By leveraging one provider for a specific functionality and another for its cost or location, companies are finding that cloud diversification can help them to meet all of their business commitments while at the same time avoiding cloud vendor lock-in.

While using multiple clouds has obvious advantages, it can quickly become a nightmare for IT professionals and chief information security officers (CISOs). Data is being distributed and processed across a large variety of cloud-based applications and services, with some of these also utilizing private clouds that must be managed, as well. With these hybrid environments not only moving data and workflows, but also being accessed and managed with a range of applications, things only get complicated further.

Although using multiple clouds is highly beneficial in most situations, it creates some unique and complex problems that organizations need to be proactive about, with security concerns ranking high on the list. The good news is that as long as companies are aware of the security threats in the multi-cloud, and put adequate measures in place to prevent them and react to them, the benefits can clearly outweigh the risks.

Multiple Secure Clouds vs Secure Multi-Cloud

Even if an organization's security team has complete control of all its individual clouds, having

multiple secure clouds is not the same thing as having a secure multi-cloud.

A secure multi-cloud is a much more complex process as it requires a single secure enterprise network to span the data center as well as all of the private and public clouds to which the company subscribes to and utilizes. This distinction is important to understand as workloads are increasingly connecting from the data center to a public cloud or are moving between clouds. If these clouds run in silos, CISOs are able to see into each cloud individually but not all at once, leaving them often on the defensive, and in a lot of instances, running blind.

Security Threats in the Multi-Cloud

While there are many potential threats that can arise in the multi-cloud, some of the most common include lack of consistency, the overall lack of speed, data unpredictability, poor visibility, and the evolution of today's advanced cybercrimes.

Lack of Consistency

One of the most common threats organizations see in the multi-cloud is sheer lack of consistency of security in general. Even though companies might understand how necessary it is to apply security at every stage along the attack surface, most deploy their multi-cloud infrastructure on a per-project basis, leading to solution sprawl with devices being managed across separate consoles. This lack of overall stability makes it difficult to centralize visibility across the extended landscape or consistently apply security protocols and policies.

Lack of Speed

Given the nature of current technologies, and the need to almost instantly respond to user demands, organizations are often turning to automation to attempt to accelerate the decision making process. This gets particularly tricky when the billions of SaaS applications and connected IoT devices that are running greatly increase the volume of data that needs to be protected, not to mention that half of those are encrypted, as well.

Given the higher throughputs and the overall volume, businesses are choosing to not inspect or secure a percentage of data over the risk of having security become a bottleneck within the business.

Unpredictability

One of the biggest draws of a cloud-based environment is its scalability. Resources can be added infinitely to address workload processing demands, and data can be rerouted to meet user needs. One of the negatives of this type of change is that data can shift in unpredictable ways, not something a security teams wants to have to deal with. Especially in today's complex and asynchronous environments, enforcing policies and protocols quickly becomes a difficult, if not impossible, task.

Poor Visibility

While hosting SaaS applications has given companies more freedom than ever before, running all of these in silos is becoming a huge security risk. Instead of tearing those silos down, SaaS applications are only builder stronger and higher walls. CISOs are able to see into each of these clouds individually, but not all at the same time, so they never have a comprehensive and holistic view of what is happening at any given moment.

As companies deploy more and more applications, none of which are integrated or able to share data, it becomes increasingly difficult to have one set of expectations or even a single understanding across all departments, especially when it comes to mitigating security threats.

Evolution of Cyber Crimes

One of the final main security threats in the multi-cloud is the advanced attacks cybercriminals are developing. These criminals understand the complexity of the multi-cloud environment as well as the challenges that come with trying to detect and track sophisticated attacks within it. They have come to depend on the fact that different security devices aren't integrated and can't see each other, which allows them to take advantage of the gaps that exist. This is just one more reason why it is necessary to stay ahead of the game and prevent these gaps from happening.

Practical Solutions

Adopt an Integrated Security Framework

For the most part, it can seem impossible to secure a highly elastic multi-cloud environment using the traditional security strategies and solutions. Fortunately, there are other options companies can turn to in today's digital environments.

One of the best ways to start is by adopting an integrated security framework which is designed to operate effectively at the speed that networks currently require. Security technologies deployed across the network need to be able to share the threat information they gather, which is where tools like antivirus and antimalware, next-gen firewalls, and advanced protection are especially beneficial.

Focus on Automation

Another way to decrease security threats in the multi-cloud is by leveraging automation. By doing things such as updating your governance rules specifically for the cloud and adopting a continuous risk treatment approach, you will be ensuring all security best practices are being managed effectively with minimal margin for error. Continuous integration and continuous deployment cycles can give you a serious advantage compared to the competition, as long as you guarantee it is highly secure by design.

Prioritize Visibility

As one of the biggest issues with clouds in silos is that they all can't be monitored simultaneously, choosing technologies that help provide a holistic view and are able of taking action on the shared threat is absolutely vital for organizations. With the speeds of cyberthreats, and the complexity of

today's cybercriminals, time is truly of the essence and not even a second can be wasted. Including SIEM (security, information, and event management) technologies is a good first step to bolster advanced threat detection, helping to prioritize indicators and automate a collective response.

Honor the Shared Responsibility Model

Last, but not least, it is vital that companies understand, and comply with, the shared responsibility model. When you take advantage of a public cloud, no matter who the vendor may be, they are only responsible for the security of the cloud itself. This means that it is up strictly up to you to secure everything that is in the cloud, including applications, data, and other systems that interact with it. If someone should log in without permissions and compromise data, that responsibility is on you.

Conclusion

No matter what SaaS applications you choose to run, having adopting a multi-cloud environment is highly beneficial for most organizations as it saves money, provides a higher level of freedom and flexibility, and gives you the best of the best. As long as you keep security best practices at the forefront, and follow the tips listed above, you will ensure that your multi-cloud environment is highly secure and continues to exceed your expectations.

Operational Intelligence

Make security actionable with vulnerability information enriched by operational data to prioritize threats based on the impact within your specific operating environment.

Multi-Tier Remediation

Drive consistency, scalability, and flexibility with automated remediation that is capable of considering the application, the process, and the severity of each issue.

Continuous Security Monitoring

Achieve security and compliance at the speed of DevOps by incorporating policies and best practices in pre-release scans so you can make changes before you release to production.