TATA CONSULTANCY SERVICES

Building on belief

Rethinking security in the multi-cloud era

Abstract

Multi-cloud strategies are becoming more common, given the advantages they provide. However, one of the key challenges involved is to put in place renewed security protocols that are in sync with the complexity that is inherent in a multi-cloud setup. We recommend that companies lead with a cloud-agnostic approach and operate with a centralized security monitoring system as a foundation for a robust multi-cloud security strategy. Additional approaches such as the setting up of a landing zone and following CIS benchmarks can also be used to ensure that your company's systems and data are never compromised.

Introduction

Cloud computing has steadily grown over the past two decades to become a key pillar of companies in the information age. Gartner predicts worldwide public-cloud user spending to increase by 18% by the end of 2021, a trend that was in no small part due to the pandemic[1].

The rising adoption of cloud services has brought with them a concomitant rise in data breaches. In the U.S. alone, the number of records that were compromised increased ten-fold over the past decade.[2] Given that most companies tend to adopt a multi-cloud strategy to run their operations, it is imperative that they should have a robust multi-cloud security strategy in place.

The general perception regarding the cloud has matured beyond immediate efficiency gains. It is no longer about cost optimization, but more about ensuring business continuity, resiliency, and innovation. Consequently, the cloud adoption process has moved away from the lift-and-shift model. It then moved on to the utilization of third-party hyperscaler services and settled on the current model of the cloud-agnostic, multi-cloud solution.

Security concerns in a multi-cloud setup

The evolution of the multi-cloud strategy was born out of a necessity to accommodate the kind of specific IT support that various lines of businesses needed, but could not get.[3] Primarily, organizations vastly prefer the multi-cloud approach to prevent vendor lock-in or take advantage of the 'best-of-breed solutions'[4], but the promise of superior security against varied threats was the ultimate draw for most adopters.

---

[1] https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021

[2] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=Data%20breaches%20vs.&text=While%20the%20number%20of%20data,not%20seen%20such%20noticeable%20change.

[3] https://techbeacon.com/enterprise-it/why-multi-cloud-approach-gaining-such-popularity

[4] https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy/

Pursuing multi-cloud strategies brings many variables into play. Multiple cloud providers that are spread out across different geographies and time zones, coupled with the expertise required to manage and integrate each of them into a whole, are some of the concerns that contribute to a more complex cloud setup. Naturally, this extends to security concerns as well, the most prominent of which are:

- Inconsistent performance across the ecosystem: Network intelligence provider Thousandeyes found out that multi-cloud performance tends to be inconsistent across public cloud providers and geographies, in no small part due to the CSPs' inability to coordinate their networks and resources with each other[5]. Consistency is important because it ensures that applications can run from anywhere with minimal changes and that configurations can be maintained in singular channels.[6] Inconsistency can throw up multiple loopholes in different parts of the company's network that would require several modifications to the company's security strategy, as opposed to a unified one that would work across all cloud environments. Inconsistency provides varied opportunities for malicious entities to engineer significantly more effective breaches and cyber-attacks, the aftereffects of which can be deleterious to the company's long-term prospects.

- Lack of a common implementation framework: Putting in place a multi-cloud strategy means that IT teams don't have the option of starting with a uniform security framework that suits the business needs of the company. To ensure that chaos doesn't take over down the line, it is important to find a security framework that not only supports the models provided by different cloud providers but also is preferably decoupled from any particular one.

  Lack of a common framework for deployment and enforcement means that companies end up adopting mass-market solutions that will never suit the kind of nuances that their respective business might need. Sidestepping this crucial step would bring up vast swaths of operational issues that will place a lot of stress on IT teams and end up costing the company quite a bit.

- No centralized management: One of the biggest advantages of a multi-cloud strategy is that it alleviates the stress that is placed on IT teams by offering a simplified, centralized management console that can be used to manage applications and workloads across multiple clouds.[8] In this context, it is quite surprising to note that companies tend to skip out on this feature altogether and face coordination issues.

  The most common approach to security management that is offered by most CSPs lacks the amount of context that is unique to each company. Following such a one-size-fits-all approach throws all sorts of challenges at the IT team, which prevents them from being able to see the big picture issues and come up with preventive measures that are better for the company's security in the long term.

- Increased complexity: Despite being a technology that was initially envisioned to reduce the complexity of IT teams, multi-cloud approaches seem to have exacerbated the problems faced by IT teams. As for why this happens, it all boils down to the details. For instance, the increasing use of unstructured data without any native schemas, coupled with the use of IoT devices that generate and stream massive amounts of data, creates a data deluge that is near impossible to manage.[9] Archaic practices such as the continued practice of building single-purpose databases to maintain apps mean that strategies haven't yet adapted to the new normal.

---

[5] https://solutionsreview.com/cloud-platforms/multicloud-performance-is-inconsistent-among-public-cloud-providers/

[6] https://thenewstack.io/multicloud-challenges-and-solutions/

[7] https://enterprisersproject.com/article/2019/10/multi-cloud-security-issues-watch?page=0%2C0

[8] https://www.vmware.com/topics/glossary/content/multi-cloud-management

[9] https://www.itworldcanada.com/sponsored/overcoming-multi-cloud-complexity-in-an-increasingly-complicated-world

- Fractured solution suite: Normally, having a wide solution suite that spoils your customers for choice is a good thing. But, when your company is busy experimenting to come up with multiple products and solutions, it becomes harder to unify them and deliver them consistently across the cloud, especially when adopting a multi-cloud approach. In an era of massive consolidation, mergers, and acquisitions across industries, the problem of integrating differing IT frameworks is too significant to ignore.[10] The likelihood of choosing between applications with competing priorities and clashing workloads can faze even the most accomplished IT teams and lay waste to months of hard work.

- Skills deficit: The lack of seasoned cybersecurity professionals continues to be a problem for many companies. With a shortage of under 3 million workers, it's no surprise that surveys of companies reveal that more than half of them are grappling with a problematic shortage of cybersecurity skills at their organization.[11] Even prior to the surge in the adoption of multi-cloud strategies, there was a serious supply problem across multiple IT specialties, namely cloud-native security, DevSecOps, and container security. These problems are only compounded when spread across multiple cloud environments. With over 80% of companies having a multi-cloud strategy in place, it isn't hard to see just how much of a problem this really is.

Five essential traits for a multi-cloud security strategy

Cloud security strategy can be daunting, especially for companies that are not digitally native. The same challenges, when distributed across different cloud environments, can be all the more challenging. Fortunately, there have been ample success stories that have demonstrated that any company can have a proper security strategy in place, provided that they adopt the following principles:

- Cloud agnostic: This goes without saying as multi-cloud means that you leverage the power of public and private clouds (from multiple CSPs) to get the kind of setup that suits your business needs. While this does increase the number of variables that you have to manage, the payoff can be immense, both from a security as well as a business value perspective.
- Consistency: Functional and operational consistency is paramount to the success of the strategy. Uniformity amongst controls, processes, frameworks as well as operational modes ensures that applications run smoothly across all environments and geographies, which means that your security strategy will scale across the entire domain. Essentially, consistency in security strategy, application design, and definition across multiple-cloud environments is a key predictor of success in a multi-cloud security strategy.
- Digitization: It might be tempting to always have someone from the IT team on standby to detect any and all security threats, but it should be avoided at all costs. Cybersecurity strategies on a multi-cloud platform should be agnostic on both fronts: people, as well as CSPs. Implementing platforms that are capable of proactively seeking out threats and neutralizing them in time is the way forward. Such systems require a minimal investment upfront and are often built to function right out of the box.
- Future-proofing: Foundational security practices usually have native security controls that are rapidly approaching obsolescence. For instance, a major telecommunications company enhanced its security and vigilance by implementing a multi-cloud strategy that shipped with a security

---

[10] https://www.rackspace.com/solve/opportunity-youre-missing-during-ma-it-integration#:~:text=The%20objectives%20of%20an%20M%26A,opportunities%20for%20new%20business%20models.

[11] https://www.csoonline.com/article/3408618/the-hidden-challenge-of-the-cloud-security-skills-gap.html

posture management service and architecture that was designed and built with security in mind. It helps to have a modernized enterprise security framework and secure operational and governance services as well.

- Centralized management: Not having a unified console to monitor a multi-cloud setup is a problem that compounds over time. Centralized management of multiple cloud environments allows for agility in policy and posture management, managed detection and response (MDR), SecOps, and continuous assurance, as well as improvements that will be required.

Implementing a multi-cloud strategy for the status quo

The successful implementation of a multi-cloud strategy requires the delineation of priorities in decreasing order of urgency. We recommend that companies should first start with securing their network infrastructure to guard against breaches and cyber attacks. This should then be followed by updating the existing tech stack to reflect the multi-cloud capabilities. Finally, companies should seek to modernize their existing tools to prepare for the next generation of technological change.

We believe that this three-pronged approach that covers cyber hygiene, enhancement, and modernization should form the base of your multi-cloud strategy. This addresses the niggling issues that would plague any cloud setup and prevents it from compounding across multiple cloud environments.

- Cyber hygiene: Good practices will always dramatically increase your security posture. The formula for a multi-cloud setup is not vastly different from that of the usual single cloud environment. Costs can be kept to the minimum with a regular review of the management console and the cloud voice while also shutting down systems when not needed.

  Adopting multi-factor authentication (MFA), a carefully configured firewall, and constantly monitoring access logs can help prevent 95% of the cloud hijacking instances. Topping all of these with operational segmentation and constant awareness/training programs would put your company in good stead when it comes to multi-cloud cyber hygiene.
- Cyber enhancement: Existing enterprise capabilities will need to be modified to suit a multi-cloud set up to ensure there are no blind spots in the security strategy. Consistent enforcement and deployment protocols along with centralized management are indispensable for the success of a multi-cloud security strategy. These enhancements will have to be made for the dual purpose of updating existing infrastructure while ensuring that their weaknesses are not translated into a multi-cloud environment.
- Cyber modernization: Shifting to a multi-cloud approach presents an excellent opportunity to modernize cyber-security controls, policies, and services that were left untouched for years prior. The next crop of technologies such as AI-ML, big data operations, automated software solutions presents newer challenges and vastly different risks that will have to be addressed by your company's multi-cloud security strategy. Failing to do so would put you behind the curve, and your company will stand the risk of being compromised in the next wave of technological disruption.

Conclusion

When it comes to multi-cloud approaches, security can no longer be treated as an afterthought or a modular concept. It needs to be developed right alongside the multi-cloud strategy itself to underpin any and all decisions taken in pursuit of fine-tuning your cloud setup. Every aspect of the multi-cloud strategy, right from centralization, consolidation, and consistency, has its own implications for security and will have to be dealt with individually and then unified to form a holistic cybersecurity practice.

About the authors

Raghvendra Singh
Global Head, Cloud Security CoE, TCS

With nearly 13 years of industry experience, Raghvendra has deep expertise in cybersecurity consulting, solution architecture, technology engineering and delivery oversight. In his current role, he is helping enterprises across the globe in securely transforming their IT to cloud. He holds a Bachelor of Engineering in Electronics and Communication, also certified in CISSP, CCSK, ITIL, Google professional Security engg, Azure Security Engg, Microsoft Certified 365 administrator, AWS Certified Solution Architect and Certified Ethical Hacker.

Ankita Sharma
Cloud Security CoE, TCS

Ankita has more than nine years of experience in program design and architecture, compliance, and cloud security assessments. She holds a Bachelor of Engineering degree in information technology. She is passionate about learning new technologies and trends in the market to design innovative solutions for complex business challenges. She holds certifications in Google professional Security engg, Azure Security Engg.

Awards and accolades

Contact

Visit the Cyber Security page on https://www.tcs.com

Email: BusinessAndTechnologyServices.Marketing@TCS.COM

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS**.

Corporate Marketing | Design Services | M | 09 | 21