Securing the move to cloud

The route to a successful and secure cloud transformation can be a journey strewn with obstacles and potential pitfalls. Here are some top tips to smooth the way forward.

Nowadays, more and more organizations are relying on cloud. Recent figures show[1] that by 2023, worldwide public cloud spending is expected to reach US$600 billion, contributed by organizations that are driving digital transformation across their ecosystem. In the Middle East, we see digitalization agendas high across key sectors, such as financial institutions and government. In Saudi Arabia, for example, one of the Kingdom's key efforts under the Vision 2030 plan is to deliver on digitalization across public services and banking processes (such as "Know Your Customer" (KYC) procedures) through the use of emerging technologies such as cloud. But in order to do so, it is imperative to understand the risks of operating in the cloud with a new approach to security and the necessary privacy.

What does cloud security mean in practice? Not many companies have started from scratch in their move to cloud; some may have already adopted a level of cloud usage, e.g., leveraging cloud for non-production workloads, for non-critical workloads, or for ones permitted by regulators. This has provided an understanding of the known unknowns, for example, the challenges associated with data. Data is often fragmented across a business, perhaps stored in cloud applications already purchased and used ad hoc by individual departments, and frequently without the knowledge of the CIO. This lack of strong governance in technology adoption can lead to siloed data and application islands, limiting an organization's ability to take advantage of cloud's benefits. Many enterprises now tackle this by performing a cloud security maturity assessment and defining a unified cloud strategy based on the results.

The approach

As rising security threats, risks, and compliance requirements become more important to businesses, it is recommended to follow steps 1- 6 (outlined below) for a cloud transformation journey. These elements are not security driven, but rather focus on an overall cloud transformation. However, security and privacy are integrated aspects that need to be considered at every step.

1. Baseline
Assess the current IT footprint, including in-flight projects and constraints. Capture issues and opportunities and perform a security maturity assessment of the current state cloud estate.

2. Vision
Get business alignment, define guiding principles, and set the pace of the journey to cloud, including the security and privacy vision.

3. Strategic decisions
Find the right mix of public, private, or hybrid cloud. Evaluate key platforms taking security and privacy aspects into account, and decide on the transformation approach.

4. Organizational impact
Define the future governance and organization, including processes, considering DevSecOps (the philosophy of integrating security practices within the DevOps process) principles. Highlight impact on talent acquisition.

5. Financial impact
Calculate the value case. Show costs, potential savings, and the impact on both capital expenditure for upfront IT investments and operational expenditure, based on a subscription model for IT consumption.

6. Roadmap
Wrap up decisions of previous phases into a bought-in plan, including dependencies and key milestones.

Nowadays, more and more organizations are relying on cloud

To make this more tangible, the following are three key areas to address as part of a cloud security strategy, which will be part of an overall cloud transformation. Firstly, the importance of building a security strategy with identity at its heart. Next, the emergence of DevSecOps for building modern security from the ground up. And finally, how monitoring can ensure knowing exactly what's going on in the cloud environment at any time. This list is not exhaustive, but highlights some of the critical challenges faced moving from traditional to cloud-based environments.

1. Identity

An organization's traditional security perimeter used to be a physical boundary; it is now a digital one. This approach is still used initially, but is no longer as effective as using business applications. IT, in general, has changed significantly; with the growth of mobility and cloud, it is still just as important to protect and manage sensitive data outside the confines of an organization. With cloud enabling a new generation of employees who can work from anywhere, across any device, creating the waves of data flowing freely, a new perimeter of identity and access management needs to be defined. Cloud security strategy must be based on credentials: who is the employee, partner, or contractor and what access are they allowed to particular data and services, under which conditions, and from where? For example, identification to access data might be different if it is done from country "x" compared to country "y." This is particularly relevant in the Middle East as government agencies and the private sector are increasingly open to foreign talent and organizations to support their business. Getting identity and access management right is crucial and needs to be a central element in every cloud transformation.

2. DevSecOps

In the cloud environment, organizations need stronger collaboration between the development, security, and operational functions to develop business applications more rapidly or to have a more agile way to extend their IT infrastructure. It is where we see the convergence of the traditional security team with the software development and the IT operations team within an organization. The initial concept was called DevOps and is now extended to include security and privacy at its core with DevSecOps. Incorporating culture, practices, and collaboration, DevSecOps leverages the best of all worlds. It sees the security, development, and operations teams working together holistically to ensure security is embedded from the very beginning and into each phase of the DevSecOps pipeline.

This may be no easy task initially[2] and will be as much a cultural issue as a technical challenge. Some employees may be reluctant to embrace the new way of working, which means business leaders may need to educate them to instill this mentality throughout the organization. The main challenge is to ensure all stakeholders adapt to the new approach and work together. It is important to establish foundational DevSecOps governance in the early stages to provide a roadmap to transform people, processes, and technology.

3. Cloud security and compliance monitoring

Another key area is to establish continuous, proactive monitoring of the cloud environment to ensure security and compliance controls are being adhered to. This will enable detection of possible intrusions, as well as security and compliance policy violations, and ensure a quick response to any threats and compliance breaches. Continuous cloud monitoring will not only help detect cyberthreats, but will also enable clear sight of all workloads migrated to cloud to monitor whether they are running as they should on a day-to-day basis, ensuring optimum cost-efficiency and that they fulfill all security, privacy, and compliance requirements.

> With cloud enabling a new generation of employees who can work from anywhere, across any device, creating the waves of data flowing freely, a new perimeter of identity and access management needs to be defined

In conclusion

As with many unknowns, the move to a virtual data centre and hyperscale global networking sees many organizations try to reinvent their IT strategy. They expect not just IT operations, but also security and privacy to adapt rapidly to this new way of digitalization to keep information and systems compliant, secure, and available. As a CIO, CISO, CFO, or even a CEO, you need to ensure that your organization has a unified cloud security framework that supports your overall cloud adoption strategy.

By **Simon Rohan Chandran**, Partner, Risk Advisory, Deloitte Middle East

Endnotes

1. https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022#:~:text=Worldwide%20end%2Duser%20spending%20on,to%20reach%20nearly%20%24600%20billion
2. https://www.tanium.com/press_releases/tanium-study-strained-relationships-between-security-and-it-ops-teams-leave-businesses-at-risk/