TATA CONSULTANCY SERVICES

Building on belief

Envisioning security for a cloud-first approach

Abstract

While digital transformation has picked up across industries and cloud has been a key driver, it is imperative to understand the complexities involved. On the one hand, cloud offers greater flexibility, agility, resilience and scalability, but on the other it poses risks and challenges in terms of regulatory compliance, increased exposure, distributed data and identity, misconfigurations and consistent enforcement of enterprise security policy.

Securing a cloud-based enterprise IT requires a robust cloud security strategy to unlock the potential value of digitalization, fuel innovation in business models and prevent financial and reputational losses. Moreover, the cloud security strategy needs to be integrated into the larger business strategy as the digital footprint expands.

We look at the key elements that are necessary to build a secure enterprise — in-built security, a data-centric and automation-first framework, and a holistic approach.

Introduction

The business of the 2020s will, no doubt, live and breathe in the cloud. As newer digital technologies like AI, automation, 5G, and IoT permeate the digital ecosystem in which today's business thrives, securing the unifying fabric of these technologies- that is, the cloud- has become synonymous with building value that lasts. The market size of cloud security is expected to reach $68.5 billion by 2025[1]– a large investment that can go a long way to secure brand value — some of the top brands of today can potentially lose over $200 billion worth of brand value with inadequate attention to the enterprise's footprint on the cloud. Therefore, cloud security has become a question of business value, as much as that of justifying the costs associated with achieving it.

Understanding the risk (and security) landscape

The risk and security landscape has been evolving at an exponentially rapid rate as businesses accelerate their cloud adoption strategies and mature digitally, in these five ways:

- As enterprises wade into hybrid multi-cloud environments, mapping the risk exposure of enterprise data at rest and in transit is becoming a high-complexity problem. Moreover, high-availability computing paradigms and a rapidly expanding application environment further add to the difficulty of gaining control over the data.

---

[1] https://www.marketsandmarkets.com/Market-Reports/cloud-security-market-100018098.html

- As data-intensive technologies and high-speed networking technologies such as WiF-6 and 5G become a value proposition that drives competitive advantage, the velocity, variability and volume of data that drives solutions powered by AI and ML technologies are becoming subject to a variety of privacy and ethical concerns.

- The regulatory paradigm is catching up to the speed at which the technology landscape is evolving. Legislations in the EU and the Americas have enforced increasingly stringent environments such as the GDPR and the CCPA. At the same time, risk-sharing arrangements between cloud service providers and adopters have been nullified as the onus of ensuring data security and privacy has been declared on the business that sells to the customer base in question.

- The senior management remains at odds in organizations that struggle with adequate cloud security assurance. First, the spend on cloud security hasn't shown a positive correlation with the levels of security; and second, the CEOs, the CFOs, the CTOs, and the CSOs often remain unaligned in their ask with respect to outlook on digital security budgets.

- Lastly, security is often conceived from outdated business and technology approaches that seldom work in today's digital business. For example, a perimeter-based approach to securing the enterprise's digital footprint, and an inefficient prioritization of the digital assets that need to be safeguarded from both internal and external threats further contribute to the risk exposure.

Businesses that want to forge a cloud security strategy for the next decade must abstract and address five key themes: the current technology ecosystem view, risks posed by the adoption of disruptive technologies (by adopters and attackers alike), the regulatory worldview of digital business, synergizing the senior management's expectations from the cloud security spend and adoption of novel approaches that justify the business value of the security spend.

Enterprise cloud security: A 2021 perspective

As business and digital gain synonymity, cloud security for the coming decade must be envisioned along the following lines:

- Watertight operations through complete visibility: In order to know what will hit them, enterprises must first understand their exposure to risk. Here, visibility becomes the foremost factor that affects response and readiness. While highly regulated industries are building a complementary granular and birds-eye view of their information systems, others are leveraging APIs and other native services to build interactive dashboards that provide a comprehensive view of affected systems and notify the right roles when mishaps occur.

- Build operational security through the right measures: While role- and attribute-based access controls can help secure sensitive data through a tiered and layered approach to protecting sensitive information, simple policies and educative measures can help enterprises dodge some of the largest, yet the simplest type of attacks that can result in regulatory disasters and consequently, big equity and brand-value losses like phishing and spoofing.

- Integrate security into development and deployment: To unleash DevSecOps beyond the hype cycle, enterprises must build security milestones into their CI/CD pipelines. For instance, validation of security in the design and architecture, a security review alongside code reviews, and building security testing milestones in the larger testing agenda of an application in the process of development and deployment.

- Adopt an extended enterprise worldview: This is critical to ensuring security beyond the blurred perimeters of the limitless digital enterprise. Therefore, educating the customers/end-users on the enterprise's approach to security, educating them on best practices, and incorporating the partners, third parties, and vendors in the larger digital risk management framework will be the key to sealing the leakages in the larger security directives.

But how can these standards be achieved, and more importantly, how can enterprises align themselves to the business value of the security spend?

Realizing the business value of cloud security

Here are a few ways to align the cloud security strategy to the larger business strategy, and move cybersecurity from an unjustifiable, unmeasurable and unmovable capital expenditure to a justifiable spend that delivers measurable and equitable business value:

- Bring the talk to the boardroom: Enterprises must bring their security teams into the boardroom where attacks and approaches to mitigating risks become the C-level's concerns and the business goals, regulatory requirements, and value-demonstration of the security spend become the CSO and their teams' concerns. For example, the cybersecurity teams must talk about how a solution will help safeguard the privacy of sensitive data of their customer base, which, if compromised, could cost enterprises up to 4% of their global revenue (as per the GDPR framework)[2].

- Invest in business problems: Instead of delegating the investments in cloud security to a systems perspective, understand, measure, and quantify the vitality of the impact that a potential measure would bring against a spend. This can help enterprises roll down the coaster of disillusionment of policy and governance-based measures in opposition to bleeding-edge technology that bleeds resources outside the research centers.

- Budget with a tiered approach and monetize: While risks like internal adversaries and asset access can be tackled using role-based access controls (RBACs) and automated background monitoring, other issues like unsecured IoT networks might require automation of network audits logs, controls, and other continuous assessment paradigms. The board must also consider monetizing their cloud security spend by highlighting it in their marketing strategy when appropriate and consequently recovering their spend by proactively selling privacy and trust as a value proposition in the product/service roadmap.

- Combat with intelligence at scale: As attackers leverage high-power computation and advanced technologies to attack and seize systems, enterprises must consider the limits of human expertise and headcount when combating at scale. Leveraging advanced AI techniques to ensure endpoint security, predicting events, taking automated response measures, unearthing vulnerabilities, and deploying continuous monitoring can prove equitable when enterprises must secure systems at scale.

To align the cloud security strategy with its business impact, CIOs, CTOs and CSOs must collaborate to visualize the business' value chain from a systemic risk perspective.
This is the key to generating the stakeholders' interest in cloud security and facilitating an organic, cross-functional interest in cloud security as it takes to the front foot in today's digital business.
Lastly, as businesses operate in a physically distributed and digitally interconnected environment, monitoring the activity of internal roles that can pose significant threats to the organization has become critical to ensuring a baseline level of safety and bringing zero-trust paradigms into action.

---

[2] https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(5)%20GDPR%2C%20the,fiscal%20year%2C%20whichever%20is%20higher.

Conclusion

Over 40% of cloud providers disperse the enterprise's digital assets geographically, and 89% do not support encryption of data at rest by default. Cloud isn't inherently secure and in fact, takes a considerable degree of planning and thoughtful formulation and execution of the cloud security strategy to avoid turning the upsides of cloud adoption to financial and reputational losses for the enterprise.

In the coming years, businesses will need to integrate their cloud security strategy into the larger business strategy, since the digital footprint of the digital business is bound to expand and diversify further. Therefore, optimizing and demonstrating the business value of the spend on cloud security will become critical in maintaining the cost-competitiveness, flexibility, and scalability that cloud brings to enterprises today. It is time for senior leaders to spark the conversation and ease the discussion into the overarching business strategy to truly enmesh the security, systems, and business view and build a responsible roadmap to end-user centricity.

References

1. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

2. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf

3. https://www.redhat.com/files/summit/2014/seifried_w_0230_cloud_security.pdf

4. https://www.redhat.com/cms/managed-files/pa-google-cloud-security-brief-f20405-201911-en.pdf

5. https://www.wsj.com/articles/concerns-about-cloud-security-prompt-more-scrutiny-from-financial-regulators-11579125998

About the authors

Raghvendra Singh, Head, Cloud Security CoE, Cyber Security Unit, TCS

Raghvenda has more than 12 years' experience in enterprise security. He helps organizations across industries define cloud security strategies and develop a partner ecosystem.

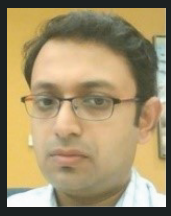
He holds a Bachelor of Engineering in Electronics and Communication, also certified in CISSP, AWS Certified Solution Architect, Certified Ethical Hacker and ITIL V3.

Nirjhar Roy, Solution Architect, Microsoft Business Unit, TCS

Nirjhar has more than 15 years of experience in IT industry across data warehouse architecture and AI/ML product development.

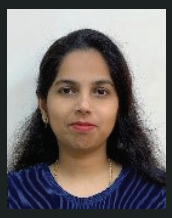
Arunkumar Selvaraj, Head, Security & Compliance, TCS Enterprise Cloud

Arunkumar has been working in the areas of cloud security and business transformation for over 27 years. He supports companies across go-to-market strategies, finance management and business solutions.



Subhrangsu Shekhar Kayal, Cloud Architect, Google Business Unit, TCS

Subhrangsu has more than 20 years' experience across data center design, infrastructure architecture, cloud architecture and service delivery.



Raji Krishnamoorthy, Head, Security & Compliance, AWS, TCS

Raji Krishnamoorthy leads TCS' Public Cloud Center of Excellence. Raji advocates cloud strategy to enterprises to bridge the divide between the services that the customers have invested in and those offered by cloud service providers, helping realize both technology and business benefits from cloud. With more than 16 years of experience in the IT industry, Raji has held various roles at TCS.

Contact

Visit the Cloud Technology 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 488,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

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

Corporate Marketing | Design Services | M | 06 | 21