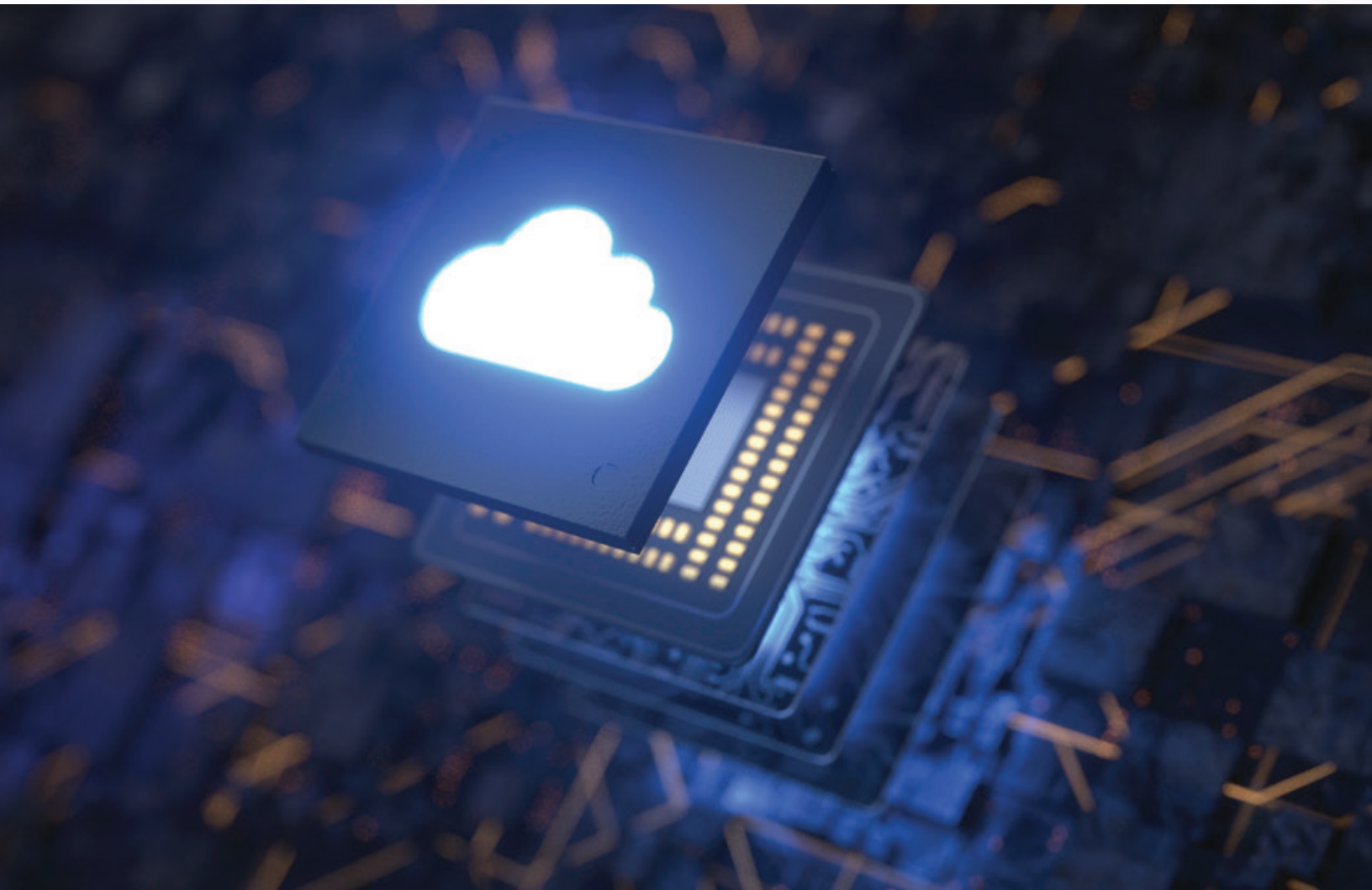
LTIMindtree

Point of View

Necessity is the Mother of Cloud Security Reinvention

Author: Dibya Ranjan Nath



Organizations today are struggling to enhance the security and compliance hygiene of their cloud landscape against emerging threats.

Maximizing cloud safety investments, and protecting the business from internal, external attacks/ breaches, and getting the optimum coverage vis-à-vis cloud security is a key challenge.

A better way

The world is evolving at a rapid rate with state-of-the-art technologies and digital transformation like never before where enterprises are adopting the cloud journey IoT/OT, digital twin as part of the fourth industrial revolution.

The Cloud journey has become the new normal for most organizations in the world, after the pandemic began last year.

Due to this shift, the on-premise security/ enterprise perimeter security layer has started diluting. That's because employees working from home often require access to data and assets from remote locations across the globe.

On the other hand, we have also noticed a never-before increase in cloud security breaches, threats, highly sophisticated attacks, and their huge implications on cost, efficiency and downtime.

These reasons have made cloud-security a must-have for enterprises to reimagine their cloud security plan, strategy, response.

It's vital for organizations to **secure cloud workloads, data, infrastructure and identities** by allowing access to authorized users only.

Are you undergoing cloud transformation journey?

Asset, Data, Identity, Network, All applications are in Cloud. Ensure safety with right cloud protection strategy

New cloud threats are emerging by the day across the globe at an exponential rate. To keep pace with these threats, industry security leaders have started rethinking, reassessing and redesigning their current cloud security plans and strategies. These include protecting their cloud workloads and landscape against new emerging threats and sophisticated attacks, however the crux is to baseline the as-is cloud security posture to identify the gaps and deploy the right mix of solution and skillset to mitigate these gaps.

Is our Cloud Estate Secure Enough in Reality?

Let's take a step back and try to ask some of the following questions to assess our organization's cloud security posture and whether we are prepared to withstand such attacks?

- Have we ever encountered cloud breaches/attacks, and do we know the root cause of it?
- Do we have skilled cloud security expertise in the organization?
- Do we have a strong end to end security governance committee for cloud governance?
- Do we have a cloud risk assessment process and mitigation plan?
- Have we secured our identity, data, asset, network, app in the cloud?
- Do we have a cloud security breach response and management plan?
- Do we have effective real-time security monitoring, detection, and response?
- Do we assess continuously to maintain security and compliance hygiene?
- A fair evaluation of the above-mentioned questions would help any enterprise to assess the right stage of cloud security maturity and protect it from the emanating threat landscape.

The Cloud Security Dilemma

Looking into the market research, study, interactions and discussions with multiple security stakeholders in the industry, which include - CDO, CIO, CISO, and other key cloud security professionals, we can safely say there are **seven key cloud security challenges:**

1. Maintaining the security and regulatory compliance hygiene of cloud workloads with a 360-degree centralized view
2. Early detection of emerging known/ unknown threats, misconfiguration, and protecting cloud workloads and landscape
3. Protecting the data, assets, identity, network in the cloud and assess through a robust security governance program
4. Follow Shift-Security-Left paradigm approach to bring security concept, requirement, culture at the time of product development phase
5. Real-time view of security vulnerability, security posture for known and shadow workloads in the cloud
6. Detecting the excessive, deprecated, and external access
7. Establishing the zero-trust network architecture and access

Cloud Security and Risk Management are the need of the hour

Now that we know the challenges, the next obvious question is – how to solve these challenges? Here are some approaches that we recommend:

- Strategic initiative from the top leadership for cloud and digital transformation journey
- Management committee for the security of the cloud and digital transformation journey
- Identify what data, applications, or assets are needed to move into the cloud?
- Identify the risks associated with the cloud and digital transformation journey
- Choose frictionless technologies to migrate and monitor
- Define baselines for a cloud security control framework
- Deploy tools for a centralized 360-degree view in real-time
- Regularly discover shadow-IT and known assets running in the cloud

Monitor real-time info and enhance security and compliance hygiene in the cloud

Review and remove excessive, deprecated, and external access

Perform regular risk assessment for workloads in the cloud

Create an effective cloud security governance committee to assess

Establish "Shift-Security-Left" paradigm approach at an early stage of product development

Build the zero-trust network architecture to verify device, user, location, etc.

Deploy solutions to perform real-time vulnerability scanning, detection, and remediation

Regularly monitor and respond to cloud threats and incidents appearing in the organization

Scan and protect container, Kubernetes, and registries

Lastly, protect the data, assets, identity, network, and application in the cloud by deploying the correct solution

Conclusion

Enterprises need to have a well-crafted blueprint for cloud security to attain the right level security maturity. The key focus area for enterprises should be - managing cyber threats and vulnerabilities on cloud applications, ensuring compliance by meeting the necessary security hygiene requirements for workloads, enforcing data security, identity management best practices and having robust threat detection capability. This can be achieved by deploying the right mix of people-process-technology along with a comprehensive governance mechanism.

About the Author

Dibya Ranjan Nath

Cloud Security & Data Security Practice CoE Lead, LTIMindtree

Dibya is a Cloud Security and Architecture Expert Advisor along with Cyber Security and GRC security domains. He has 11+ years of work experience into wide range of security domains. He has worked for a broad range of clients across the world in various domains, which include Banking and Insurance, Telecommunications, Retail industries. At LTIMindtree, Dibya leads the Cloud and Data Security Practice CoE program.