Indian IT Consulting and System Integrator | India | Technology

Enabling multicloud business resiliency and security for one of India's largest IT firms

Client profile

Incorporated in 1945, the client is a leading global information technology, consulting and business process services company. The Fortune India 500 ranks them as India's 29th largest company by total revenue.

Headquartered in Bengaluru, they have over 220,000 dedicated employees serving clients across six continents, and are listed on stock exchanges in India and the US.

Which services?

Managed data backup and resiliency

- Managed data backup and resiliency across the multicloud environment:
  - Google Compute Platform
  - AWS
  - Azure
  - On-premises private cloud
- 3-copy backup architecture, including an offsite, air-gapped copy that's completely isolated.

> "The CIO and CISO are both now more confident that business critical data is resilient and they have a greater control against growing ransomware threats.

Summary

For this leading IT consulting and system integration company, data is their most critical asset. Over time, however, a multicloud data and application sprawl meant their applications and data were spread across multiple hyperscalers, and they were struggling to maintain a uniform data backup and resiliency framework that could span the multiple cloud platforms.

Their CISO was also concerned about organization's exposure to ransomware, and how it could impact their business. Despite having measures in place for disaster recovery and security to protect against the customary threat landscape, he believed they were underserved when it came to protection against ransomware.

We worked with them to implement a multicloud, single-window backup and resiliency solution that would also mitigate their exposure to ransomware via a consumption-based data resiliency platform.

Business need

Creating a data resiliency framework while protecting against ransomware

With more data being produced than ever before, the client was struggling to effectively manage backup across their multicloud environment. With no visibility or control over protected data, confidence in the existing backup infrastructure and tools was low, as IT teams were unable to correlate data stored on multiple cloud platforms.

In addition, despite have deployed a number of disparate protection tools, they were unable to accurately identify coverage gaps in their threat mitigation capabilities. They were, however, able to clearly see deficiencies in their abilities to ensure data resiliency and business continuity in the event of a ransomware attack.

Solution

Delivering a uniform data resiliency framework in a multicloud environment

Working with the client, we designed a highly available, redundant and secure data protection solution that ensured secure backups and business resiliency across a multicloud environment.

Three distinct backups of all critical data and applications are created — the primary copy is retained within in the same cloud region where the data and applications reside, to ensure the fastest possible restoration times and the best possible RTOs and RPOs.

The second copy is retained in a different region of same provider, safeguarding against regional failures, and the third and final air-gapped copy is stored in a completely isolated location separate from the primary and secondary sites.

An additional protection layer against ransomware

Our solution secures the client's data management environment using intelligent data protection, and monitoring capabilities aimed explicitly against cyberattacks, including ransomware.

The solution employs a multi-layered security approach to thwart ransomware attacks, and constantly protects backed up data by preventing rogue access by malicious actors. Machine learning, artificial intelligence, and honeypots are used to monitor, detect and mitigate suspicious activity. This framework provides the client with greater insight and faster time to recovery.

This approach delivers comprehensive data protection, proactively monitoring the client's machines for any unexpected activity and immediately alerts users in the event of suspicious activity that could potentially be an initiation of a ransomware attack.

Visibility, governance, and management

With over 1,000 VMs spread across all the major hyperscalers as well as an on-premises private cloud, 24/7 visibility into the resiliency platform is critical. We provides them with visibility and governance into the solution via a combination of the NTT Management Platform (MNP) as well as the native technology dashboards.

Outcomes

Delivering resiliency and security across a hybrid multicloud environment

With the new backup and resiliency solution, we have helped the client achieve a uniform, resilient backup policy across a complex hybrid multicloud environment — something that was lacking prior to our solution.

The solution provides unmatched scalability and flexibility to meet their growing data backup and archival needs, allowing them to optimize utilization without any extra administrative overhead. With complete visibility and governance over their backup and retrieval process, they're now confident in the SLA that they provide to the business.

The CIO and CISO are both now more confident that business critical data is resilient and they have greater control against growing ransomware threats. Even in the face of unknown threats they can respond and remediate threats using our solution and managed service capabilities.