Case study

NTT

How one of India’s largest IT firms enable business resiliency & security for a multicloud environment?

How did NTT ensure that this leading IT systems integrator’s data was resilient to ransomware attacks?

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 both in India and the USA.

> *“64% of CISOs feel they’re at risk to an imminent cyberattack.”*
>
> - Proofpoint’s ‘Voice of the CISO’ report, 2021

> *“75% of all IT organizations will face one or more attacks in the next 12 months.”*
>
> - Gartner’s ‘Detect, Protect, Recover’ report, 2021

Summary

For this leading IT Consulting & System Integration company, data is their most critical asset. Over time, however, a multi-cloud data & application sprawl meant their applications and data were spread across multiple hyperscalers, and the client was struggling to maintain a uniform data backup and resiliency framework that could span across multiple cloud platforms.

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

NTT worked with the client to implement a multi-cloud, single-window backup and resiliency solution that that would also mitigate their exposure to ransomware via a consumption-based data resiliency platform, ensuring business resiliency in the event of a ransomware attack.

Challenge

Ensuring a uniform data resiliency framework across a multicloud environment, while also ensuring data protection against ransomware attacks.

With more data being produced now 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 that was being stored on multiple cloud platforms.

Also, despite a fairly wide landscape of disparate protection tools, the client was 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.

Which services?

Managed Data Backup & Resiliency

- Managed Data Backup & Resiliency across the client's multicloud environment:
  - Google Compute Platform
  - AWS
  - Azure
  - On-premise private cloud
- 3-copy backup architecture, including an offsite, air-gapped copy that's completely isolated.

Managed Ransomware protection

- Multi-layered Ransomware protection solution using AI / ML and machine learning to provide:
  - Anomaly detection
  - Alerting
  - Mitigation

Solution Monitoring & Management

- 24 x7 Monitoring & management
- Complete visibility via the NTT Management portal and technology platform dashboard

Transformation

Delivering a uniform data resiliency framework in a multicloud environment.

Working with the client, NTT designed a highly available, redundant and secure Data Protection solution that ensured secured 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 & RPOs.

The second copy is retained on a different region of same provider, thus 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

NTT's 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 helps gain greater insights and faster time to recovery.

This multi-layered 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-premise private cloud, 24x7 visibility into the resiliency platform is critical. NTT provides the customer with visibility and governance into the solution via a combination of the NTT Management Platform (MNP) as well as the native technology dashboards.

Technology plays a crucial role in driving business outcomes, which **is why 85% of the Fortune 500 companies come to us**.
Find out how our full range of capabilities will empower your people, strategy and operations to achieve your business modernization and transformation goals.

Explore our services

Outcomes

Delivering resiliency and security across a hybrid multicloud environment.

With the new backup & resiliency solution, NTT has helped the client achieve a uniform, resilient backup policy across a complex hybrid multicloud environment – something that was lacking prior to NTT's solution.

The NTT 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 a greater control against growing ransomware threats. Even in the face of unknown threats they can respond and remediate threats using NTT's solution and managed service capabilities