LTIMindtree

WHITEPAPER

Data Resiliency Across Multi-Cloud

A Zero Trust Approach for Data Continuity

Contents

Abstract

The multi-cloud strategy, which integrates multiple public cloud services with on-premises infrastructure, offers flexibility and scalability but introduces complexity in data protection and management. With a focus on storage, backup, and cyber resilience, this whitepaper explores methods for achieving data resiliency in multi-cloud environments. It advocates a Zero Trust security framework, applying its tenets to storage architecture, network security, and operational procedures to strengthen data protection against evolving threats, including those posed by AI and quantum computing.

Introduction

Organizations increasingly adopt multi-cloud strategies to leverage both on-premises and public cloud environments. However, this distributed architecture severely impacts data management and security. Traditional security perimeters are ineffective when data is spread across multiple locations and managed through various methodologies. This whitepaper presents a comprehensive data resiliency strategy that incorporates backup, storage, and cyber resilience, all grounded in the Zero Trust security framework.

The challenge of multi-cloud data resilience

Consider a multinational enterprise utilizing a multi-cloud approach. Sales data is stored in Azure, product data in AWS, and customer data in an on-site data center. The marketing team uses Google Cloud to run machine learning models and analytics. This distributed architecture presents several challenges:

Data sprawl

It is challenging to keep a cohesive perspective of the data when customers, products, and sales data are dispersed throughout several locations.

Inconsistent security policies

The company uses different security configurations in AWS, Azure, and Google Cloud, leading to potential security gaps.

Increased attack surface

Because the data is distributed, hackers can target the weakest link in a multi-cloud scenario, increasing the danger of cyberattacks.

Data mobility and integration

The business needs strong data management capabilities to move data between on-premises systems and cloud platforms for processing and analysis.

Governance and compliance

The business must make sure that all its cloud environments comply with data privacy laws like General Data Protection Regulation (GDPR), which calls for meticulous preparation and cooperation.

Besides these data resiliency challenges in multi-cloud scenarios, new encounters is being created by the emergence of artificial intelligence (AI) and quantum computing. To guarantee strong data management and protection, enterprises must confront these new risks and difficulties it presents.

Key concerns include:

Data explosion and complexity

AI-driven applications generate massive amounts of real-time data. Managing these large, fragmented datasets across multi-cloud environments increases scalability, cost, and operational challenges.

Security and compliance risks

AI heightens vulnerabilities to ransomware and compliance complexities due to the sensitive and distributed nature of data.

Quantum-resistant cryptography

Traditional encryption methods, such as RSA and ECC, are vulnerable to quantum computing threats.

Outdated cryptographic protocols

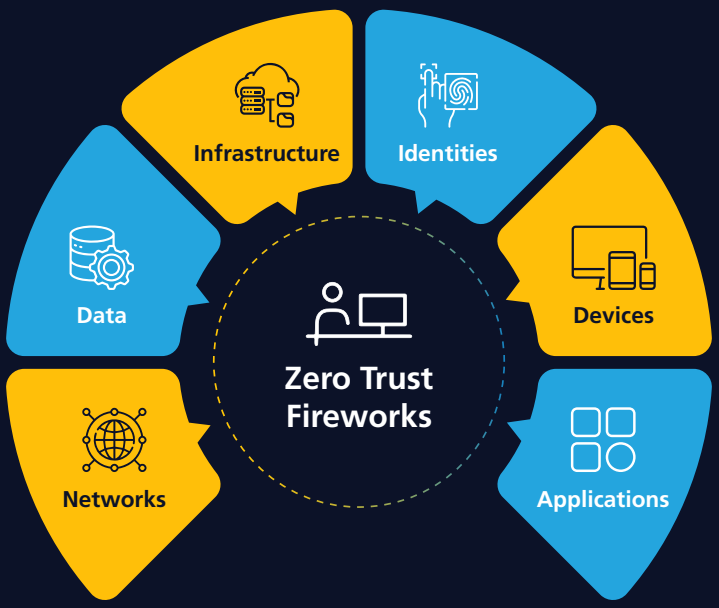
Legacy encryption techniques must be updated to mitigate emerging quantum risks.

Given the multi-layered impact of these challenges, organizations must implement cyber resilience best practices through a Zero Trust security framework. This includes data encryption, multi-factor authentication (MFA), micro-segmentation, and continuous monitoring across all its settings. These measures enhance regulatory compliance and fortify data protection.

Now, let us take a deep dive to find a way to emerge successfully from this labyrinth of complexities.

Framework for data resilience based on Zero Trust

Under the Zero Trust security framework, every access request, regardless of origin (within or outside the conventional network boundary), must be verified under the Zero Trust security framework, which is founded on the idea of "never trust, always verify." The following components are critical for applying the Zero Trust security framework to data resiliency:



01 Micro-segmentation

To lessen the impact of breaches, micro-segmentation splits the network and storage infrastructure into smaller, isolated sections. This helps to better manage access to sensitive data and apps by establishing granular security zones. For example, a financial institution can segregate client data from other infrastructure components to prevent unauthorized access in case of a compromise.

02 Least privilege access

A key component of the Zero Trust security framework is granting users and apps only the minimal amount of access rights required to access data. Organizations can lessen the possible harm that compromised accounts could create by restricting access rights. An IT administrator, for instance, has more extensive rights than a marketing analyst, who might only have access to client data. This strategy reduces the possibility of illegal data modification and data breaches.

03 Multi-factor authentication

Strengthening security through MFA ensures that access to management consoles, backup systems, and storage infrastructure requires multiple verification factors. The implementation of MFA necessitates that users present various verification methods, including a password and a one-time code delivered to their mobile device through SMS2. If a user's credentials are compromised, this additional security measure helps thwart unauthorized access. Further, to lower the danger of unwanted access, employees, who want to access the company's cloud storage, must input both their password and a token from their authenticator app.

04 Continuous monitoring and recording

Maintaining data resilience requires putting in place thorough recording and monitoring to identify questionable activity and guarantee accountability. Real-time tracking of network traffic, system events, and user activity is part of continuous monitoring. An organization can utilize a security information and event management (SIEM) system to collect and analyze logs from multiple sources, identify security incidents, and generate alerts for further investigation.

05 Data encryption

A fundamental aspect of the Zero Trust security framework is the encryption of data both while it is being transmitted and when it is stored. This ensures that any encrypted data remains unreadable, even if it is intercepted or accessed without proper authorization. For instance, companies can use secure communication protocols to transfer data between systems and encrypt patient records stored in the cloud. This strategy is designed to defend against data breaches and restrict unauthorized access to sensitive data.

By incorporating these Zero Trust security framework principles, organizations can enhance their cyber resilience best practices and maintain a robust defense against emerging threats in multi-cloud environments.

Resilient storage in multiple clouds

Ensuring data availability and integrity in the face of hardware malfunctions, software errors, and cyberattacks is the primary objective of storage resilience. Achieving storage resiliency in a multi-cloud environment requires the following key strategies:

01 Data synchronization and replication

Implementing synchronous or asynchronous replication between on-premises and cloud storage is essential for business continuity and disaster recovery. Synchronous replication ensures real-time data consistency by writing data to multiple locations simultaneously. For instance, an organization can mirror transaction data between its on-premises data center and a cloud provider to maintain continuous availability. In contrast, asynchronous replication, which involves a slight delay in synchronization, may be a more cost-effective option for less critical data.

02 Immutable storage

Implementing write-once-read-many (WORM) storage or object locking helps protect against ransomware and accidental deletions, ensuring data cannot be altered or erased. For example, organizations can use immutable storage to safeguard patient records from unauthorized modifications, preserving data integrity and ensuring compliance with relevant regulations.

03 Storage tiering

To optimize storage costs and performance, automated tiering should be used to move data across different storage tiers based on access frequency and performance requirements. Storage tiering involves categorizing data based on how often it is accessed, and organizing it into various levels, including hot, warm, and cold storage. For instance, an organization can employ cold storage for archival footage, warm storage for less frequently accessible content, and hot storage for regularly accessed video content. Automated tiering dynamically shifts data between tiers to balance performance and cost efficiency.

Recovery and backup in multiple clouds

Effective backup and recovery strategies are critical for restoring data following a disaster or security incident. A Zero Trust backup solution incorporates several key strategies to ensure data security, availability, and redundancy:

01 Air-gapped backups

Offline or isolated backups provide protection against ransomware and other cyber threats. Because air-gapped backups are disconnected from the network, attackers cannot access them. For instance, an organization can create air-gapped copies of critical data using offline storage devices or tape backups. Logical air-gapping, achieved through immutable storage, further prevents data from being modified or deleted. This approach ensures backup data remains intact even if the primary copies are compromised.

02 3-2-1 backup rule

Maintaining data availability requires adherence to the 3-2-1 backup rule. In line with this guideline, it is advisable to keep three copies of data: two stored on separate media types and one kept off-site. For example, an organization might store its data on-site, in the cloud, and at an offsite backup facility.

03 Backup encryption

Encrypting backup data during transmission and storage prevents unauthorized access. The backup data becomes unreadable due to this encryption, ensuring that it remains secure even if it is intercepted or accessed without authorization. For instance, a company can utilize secure communication protocols (like TLS) to protect data during transfer and advanced encryption standards (AES) to encrypt backup data stored on cloud services. This method preserves data secrecy and protects sensitive information.

04 Automated backup and recovery testing

Regular testing of backup and recovery processes is essential to ensure they meet recovery time objectives (RTOs) and recovery point objectives (RPOs). Automated testing helps organizations verify backup system reliability and identify potential issues. This proactive approach enhances confidence in recovery capabilities.

05 **Secure backup repositories**

Strict access controls and continuous monitoring are essential to prevent unauthorized access and ensure data integrity. Role-based access control (RBAC) should be used by organizations to restrict backup data access according to user roles and responsibilities. Backup repositories, for instance, should only be accessible by authorized individuals, and all access attempts should be recorded and tracked. This strategy guarantees accountability and helps stop data leaks.

06 **Segregation of duties**

Identity and access management (IAM) policies in conjunction with an audit model will guarantee that production and backup data access are kept apart. To lower the danger of insider threats and unauthorized access, duties must be segregated. This entails distributing responsibilities across several people or groups. For example, backup data should not be accessible to the team in charge of production data management, and vice versa.

Cybersecurity in multiple clouds

Cyber resilience focuses on an organization's ability to anticipate, withstand, recover from, and adapt to cyberattacks. A Zero Trust security framework incorporates several key strategies to strengthen cyber resilience and ensure robust protection:

01 **Threat detection and prevention**

To detect and stop cyber threats in real time, it is essential to use sophisticated threat detection and prevention solutions. This category encompasses various tools such as endpoint detection and response (EDR) software, security information and event management (SIEM) frameworks, along intrusion detection and prevention systems (IDS/IPS). For instance, an organization can use an EDR system to monitor endpoints for suspicious activity and an IDS to analyze network traffic for anomalies. By integrating these tools, organizations gain comprehensive visibility into their multi-cloud environments and can swiftly identify and mitigate threats.

02 **Vulnerability management**

Regular system patching and vulnerability scanning help minimize attack surfaces. Identifying, assessing, and addressing security weaknesses in networks, hardware, and software configurations are critical components of vulnerability management. For instance, automated scanning tools can detect outdated software and misconfigurations in cloud infrastructure. Applying timely patches and updates reduces the risk of exploitation.

03 **Incident response planning**

Establishing and regularly testing incident response plans ensures an efficient and coordinated response to cyberattacks. An incident response plan should outline key steps such as detection, containment, eradication, and recovery. For instance, organizations can conduct tabletop exercises to simulate cyberattack scenarios and evaluate their response effectiveness. Aligning with cyber resilience best practices enables organizations to enhance preparedness and minimize disruptions.

04 **Integration of security information and event management (SIEM)**

Centralizing security logs and events from both cloud and on-premises environments is essential for effective threat detection and response. SIEM systems aggregate and analyze security data from various sources to provide real-time insights. For example, organizations can use a SIEM solution to consolidate logs from cloud services, on-premises servers, and network devices, enabling security analysts to detect patterns and correlations that indicate malicious activity.

05 **Zero Trust micro-segmentation for backup infrastructure**

To stop attackers from moving laterally, backup servers and storage must be isolated from production networks. Creating separate security zones within the network, each with unique access restrictions and security guidelines is known as micro-segmentation. A business can, for instance, divide its backup infrastructure from the rest of the network so that an attacker cannot simply access the backup systems even if they manage to get into the production environment. This strategy decreases the probability that backup data will be jeopardized in the occurrence of a cyberattack.

Impact of AI and quantum computing and mitigation

The rise of artificial intelligence and quantum computing has introduced a new array of challenges while also intensifying pre-existing ones. However, if employed appropriately, AI can assist us in countering and addressing these issues. Therefore, it is imperative to concentrate on utilizing AI to identify and regulate content generated by other AI systems or to mitigate cyberattacks. AI has the potential to detect and analyze threats, automate security processes, and respond effectively to incidents. Some ways in which AI can help us tackle these challenges are -

01 AI-powered threat detection

AI can examine security records to identify anomalies and suspicious activities. For instance, a financial institution can identify fraudulent activity by employing AI-powered threat detection to track user behavior and transactions in real time. Rapid response and mitigation are made possible by AI systems' ability to recognize patterns and abnormalities that point to dangers.

02 Security automation through AI

The implementation of AI can facilitate the automation of various security functions, such as identifying threats and responding to incidents. For example, during a cyberattack, an organization can swiftly isolate compromised systems and block rogue IP addresses by utilizing AI-driven automation. This minimizes the impact on operations by cutting down on the time needed to control and remediate threats.

03 AI-based security posture management

AI can continuously assess an organization's security posture and identify vulnerabilities. For instance, an AI-driven security tool can monitor a multi-cloud environment for misconfigurations and provide recommendations for mitigating risks, such as updating access controls or patching software vulnerabilities.

Quantum-safe cryptography: As quantum computing advances, traditional encryption methods face potential threats. Organizations should adopt quantum-resistant encryption techniques such as lattice-based cryptography and hash-based signatures to protect sensitive data.

04 Quantum key distribution (QKD)

This method leverages quantum mechanics to securely exchange encryption keys, preventing unauthorized data interception. Organizations can implement QKD to secure communications between cloud providers and data centers.

05 Secure cryptographic hashing

Secure cryptographic hashing: Using cryptographic hash functions ensures data integrity in cloud storage. By regularly comparing stored hash values with original records, organizations can detect unauthorized changes and take corrective action.

06 Quantum-safe Transport Layer Security (TLS)

Implementing quantum-safe Transport Layer Security (TLS) protocols enhances the security of online transactions, ensuring confidentiality even in the presence of quantum-capable adversaries.

Operationalizing Zero Trust for data resiliency

The effectiveness of any new tool or technology depends largely on the policies and processes governing its use. Human error and inadequately defined processes can pose significant risks. Therefore, maintaining strict oversight and adhering to cyber resilience best practices is essential. Operational adjustments are necessary to ensure successful execution.

01
Conducting regular security awareness training to educate employees on cyber threats and recommended cyber resilience best practices.

02
Enforcing robust identity and access management (IAM) policies to strengthen multi-factor authentication (MFA) and apply the principle of least privilege access.

03
Automating security tasks such as vulnerability scanning, patch management, and incident response to enhance efficiency and minimize human error.

Conclusion

Achieving data resiliency in a multi-cloud environment requires a comprehensive approach that integrates backup strategies, storage architecture, and cyber resilience measures. Implementing a Zero Trust security framework ensures data protection against evolving threats by incorporating encryption, multi-factor authentication, least privilege access, micro-segmentation, and continuous monitoring. Cyber resilience is further strengthened through incident response planning, regular vulnerability assessments, and advanced threat detection and prevention mechanisms. Additionally, quantum-resistant encryption and artificial intelligence enhance security protocols.

By adopting the strategies outlined in this white paper, organizations can establish a robust data protection framework across their multi-cloud infrastructure. This proactive approach not only mitigates risks but also enables businesses to fully leverage the benefits of multi-cloud computing while ensuring data security, availability, and integrity. Ultimately, a Zero Trust approach to data resiliency equips organizations with the confidence to navigate the complexities of multi-cloud environments while safeguarding data against emerging cyber threats.

Author bios

Amit Motiwale

Senior Principal Architecture, Cloud and Infrastructure

Amit serves as a Senior Principal Architect, bringing extensive IT experience in solution design, IT consulting, and enterprise storage and backup. He has demonstrated strong leadership in driving strategic infrastructure transformation initiatives and effectively engaging with stakeholders. His expertise enables him to address complex challenges and deliver impactful solutions, particularly in data resiliency and protection

Ashish Gulati

Associate Vice President, Cloud and Infrastructure

Ashish is a leader in hybrid cloud advisory within the IT infrastructure sector. He provides consulting services in infrastructure transformation, solution design, and operations, tailored to diverse geographical standards, industry verticals, and compliance frameworks. As the head of the Hybrid Cloud Practice at LTIMindtree, he specializes in developing end-to-end IT infrastructure solutions, both on-premises and cloud-based. His expertise allows him to navigate complex challenges and deliver effective solutions, particularly in designing and implementing hybrid cloud strategies that ensure data protection against cyberattacks and other disruptions, whether manmade or natural.

For more information, please write to us on *cis.pulse@ltimindtree.com*

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 86,000+ talented and entrepreneurial professionals across more than 40 countries, LTIMindtree — a Larsen & Toubro Group company — solves the most complex business challenges and delivers transformation at scale. For more information, please visit **https://www.ltimindtree.com/**