AI-first data protection: A boardroom priority for business resilience

Enterprises can shift quickly from outdated backup systems to modern data protection and cyber recovery, using LTIMindtree's Data Resiliency Service based on the Rubrik Security Cloud.

CIO

The escalating wave of cyberattacks compels IT leaders to reevaluate per Websters their data protection strategies, prioritizing managed services for recovery solutions that provide zero-trust architecture, protection for the backup infrastructure, AI/machine learning (ML) capabilities, and integration with their existing security strategy.

The threat of ransomware is no longer a distant possibility but an operational certainty. Cybercriminals consistently make an organization's backup infrastructure a primary target in their attacks. This alarming trend is substantiated by a report from Rubrik Zero Labs, which found that attackers routinely attempt to remove backup and recovery options from defenders. Specifically, in organizations that reported a successful cyberattack, the findings were stark[1]:

- Attackers tried to affect the backups in 96% of these attacks.

- The attackers were at least partially successful in 74% of those attempts.

When backup infrastructure and data are compromised, an enterprise is left without a viable data recovery plan which is a critical vulnerability. This exposure doesn't just endanger data; it imperils employees, customers, business continuity, and hard-won reputation, ultimately threatening the organization's very existence. Organizations must develop an AI-first data resiliency and recovery strategy to successfully counter such sophisticated cyberattacks.

"IT leaders are not looking at backup today as just an operational recovery tool", says Kaushal Chhaya, global solutions architect, at Rubrik. "They're looking at it strategically. They understand the importance of cyber recovery, which is not possible without resilient data protection and data observability."

Managed services unlock scalable, secure backup modernization

Businesses are discovering the fastest, most cost-effective way to address backup vulnerability is with a well-planned managed service. These services combine a modern, zero-trust, hybrid cloud backup product with comprehensive services for enterprise assessment, deployment, optimization, operations, and support. One example is the Data Resiliency Service from global technology services firm LTIMindtree, based on Rubrik's AI-powered Rubrik Security Cloud.

Prioritize essential capabilities for fast recovery from ransomware attacks

Effective cyber recovery strategies must begin with a zero-trust product architecture, one that inherently assumes cyberattacks are not only possible but probable. Critically, the backup solution itself must be fortified against attack: backups that can be tampered with, deleted, or encrypted during an attack represent a fundamental failure point.

Three critical capabilities make the foundation of a fast and effective cyber recovery.

■ **Data resiliency:** You are assured of a usable backup copy, which will not be impacted during a cyberattack or by a malicious insider.

→ Rubrik ensures data resilience with immutable backups, logical air gaps, end-to-end encryption, and granular access controls.

→ LTIMindtree tailors deployment and operations to enterprise policies, ensuring compliance and operational fit.

■ **Data observability:** At all times, you know if there is a potential cyber threat present in your environment

→ Rubrik leverages AI/ML-driven capabilities to continuously monitor backup data for anomalies and risk signals. Furthermore, Rubrik integrates with leading threat intelligence feeds from providers like Mandiant to scan backup metadata for known attacks and IoCs (indicators of compromise). It also scans your data for sensitive data exposure, helping you improve your overall data security posture.

→ LTIMindtree leverages these Rubrik capabilities to deliver data observability services.

■ **Data recovery:** You reduce or eliminate major business impacts of cyberattacks, disasters, or system failures through clean, reliable, and rapid data restoration.

→ Rubrik enables identification of clean snapshots and orchestrates restoration with just a few clicks.

- LTIMindtree operationalizes these features into tested, automated recovery playbooks.

Besides improving data protection, modernized backup and recovery solutions have two additional business benefits:

1. Ensuring compliance with strict data protection regulations that mandate secure and dependable backup solutions.

2. Streamlining operations and lowering expenses through more efficient and scalable backup.

Key features of Rubrik Secure Cloud include:

- A proprietary file system and APIs to screen the backup software from being visible to attackers.

- GenAI features to simplify interacting with the platform.

- Extensive automation of the platform's capabilities.

Rubrik and LTIMindtree collaborate for enterprise cyber recovery

A close, effective partnership between a cyber recovery vendor and an experienced technology services vendor brings an array of benefits for IT leaders.

The LTIMindtree Data Resiliency Service is designed to help enterprises shift quickly from outdated backup systems to modern cyber recovery and data protection, based on Rubrik Security Cloud.

"We orchestrate the entire solution, so the customer realizes the maximum value not only from the software platform but from people and processes," says Amit Motiwale, practice lead for storage and backup, LTIMindtree.

The LTIMindtree and Rubrik partnership delivers:

- **Accelerated deployment process.**

- **Integration with automation, orchestration, and infrastructure security tools**

- **End-to-end cyber resilience and data protection**

- **Guaranteed fast recovery**

- **Advanced security and compliance**

- **Lower total cost of ownership and operational efficiency**

The bottom line

Rubrik and LTIMindtree deliver a modern blueprint for AI-powered data protection and enterprise-grade cyber recovery. By aligning emerging technology with strategic services, the joint offering enables IT leaders to shift from reactive risk management to a "resilience by design" approach, future-proofing their business against rising ransomware threats.

To learn more about our AI-first data protection solution, please visit:
https://www.ltimindtree.com/data-resiliency-rubrik/

Rubrik partner portal LTIM partnership page:
www.rubrik.com/partners/service-delivery-partners/mindtree

[1] Rubrik Zero Labs, The State of Data Security: Measuring Your Data Risk, p. 27, 2024.