LYVE™ Cloud

Solution Brief
RANSOMWARE DATA PROTECTION

Safeguard Enterprise Data from Ransomware

Lyve Cloud offers a safe and efficient S3 object storage target to support your anti-ransomware strategies.

Solution Summary

Proactive detection and secure backups are the solution to protecting enterprise data from ransomware attacks. Lyve™ Cloud S3 object storage provides enterprises with a secure, flexible, and cost-efficient backup storage target. Security features such as object immutability safeguard data backups from manipulation or deletion while enabling fast retrieval and cloud-based disaster recovery. Designed for compatibility with a variety of applications, Lyve Cloud storage as a service is simple to use with the backup management tools of your choice.

Benefits Summary

- **Top-Tier Security:** Lyve Cloud features multi-level authentication, object immutability, and encryption for data at rest and in motion, enabling continuous data protection.
- **Simple Pricing:** Lyve Cloud customers only pay for the data storage they use. With no additional API charges or egress fees, admins can retrieve data freely.
- **Flexible Design:** Lyve Cloud's adaptable API enables customers to easily connect to S3-compatible independent software vendor (ISV) backup software applications for frictionless, automated backups.
- **Disaster Recovery:** Lyve Cloud's frictionless cloud storage experience enables disaster recovery in the cloud.

Cyberattacks are on the rise, commonly targeting and encrypting enterprise data for monetary reward. These attacks can halt business operations, expose private information, and injure the well-being of victims. Many businesses attempt to restore operations from their backups if they have them but struggle to recover quickly. This process is both time consuming and expensive, leaving businesses to choose between paying the cyber criminals or losing their data. Either way, they still must pay the cost of recovering operations and accept lost business. To prevent these attacks, data must be safeguarded from end to end with a trusted backup solution.

Introduction

Ransomware is a type of malware practice that targets network data and holds it hostage. This data is locked with encryption that requires undisclosed keys to regain access. These keys are then offered in exchange for monetary compensation. When it comes to ransomware, there are no limits—attackers will target organizations of any size and any type of data. This form of data extortion has become very sophisticated, and can even lie dormant for weeks before the threat is detected. As a result, businesses are forced to either pay the ransom or lose business-critical data.

Fortunately, there are three key strategies businesses can employ to overcome ransomware:

- Proactive detection
- Efficient recovery plan
- Comprehensive backup and storage strategy supporting the recovery plan

The Challenge

To protect business-critical records and data, businesses must incorporate sophisticated backup strategies. The effects of ransomware attacks can drain companies of their resources, earnings, and priceless information. These attacks have become harder to recover from and are growing in number, with attackers now targeting backup storage in addition to primary storage. According to cybersecurity firm SonicWall's 2021 report, attacks rose by 62% worldwide between 2019 and 2020. In North America alone, attacks rose by 158% during the same span of time.

Further complicating matters in the wake of these attacks is the reality that the recovery process is time consuming, which extends operational and business losses. In addition to ransom and recovery costs, many cloud providers charge to move and retrieve this data. This leaves businesses to choose between paying high fees, losing data, or in some cases, paying the ransom. Top-tier security prevention with affordable cloud services is fundamental to safeguarding data against ransomware threats.

Solution Approach

The best strategies for protecting a business against ransomware attacks include a robust and comprehensive backup and restore plan. This should encompass: an inventory of data that's to be protected; an ISV backup software application with anti-ransomware features; an automated and customized backup cycle; a durable and efficient immutable storage target that offers air-gap-like data protection; and a frequently demonstrated restore and disaster recovery plan that minimizes the time it takes to recover business operations. Businesses should have the ability to quickly restore the most recent backup copy of their business data so they can reduce the time needed to resume work flow in the event of disruption.

When deployed as a storage target for backups, Lyve Cloud offers a robust and cost-effective solution with extended features that support anti-ransomware strategies. This ensures data is protected from end to end.

Features include:

- Data object immutability options with configurable retention times at the S3 bucket level
- Replication at the S3 bucket level
- Always-on data availability and data encryption
- Predictable pricing without egress fees and API charges
- Multi-factor authentication for validated access
- Flexible S3 API

Seagate Solution

Leveraging over 40 years of industry-leading data storage experience, Seagate® prioritizes security first. Lyve Cloud is designed to protect enterprises from common causes of data corruption such as viruses and ransomware. This commitment to the most stringent globally recognized security standards is demonstrated by Lyve Cloud's ISO 27001:2013 and SOC2 certifications. With multi-level login authentication and encryption in flight and at rest, data privacy is protected at all times. Object immutability options on Lyve Cloud's S3 object storage protect data from alteration or deletion.

Object Immutability is the ultimate feature for ransomware protection, delivering tape-like air-gap data protection. This combined with automatic replication provides ultimate protection for backups stored in Lyve Cloud. With its simple, trusted, and efficient design, Lyve Cloud enables seamless integration with leading industry backup software providers. These layers of security allow enterprises to seamlessly backup, scale out, and protect their data from cyberthreats.

Total Solution

Data retrieval can be costly, leaving businesses to pay for delayed operations, restore costs, and possible ransom payments. Other cloud providers often charge users additional fees when they need to retrieve or quickly activate data backups. With Lyve Cloud's simple pricing model, customers are only charged for the data storage they use. There are no additional API or egress fees, making data retrieval efficient and cost effective. Backup data is always on with Lyve Cloud at no extra cost, which enables the ability to instantly restore operations with Lyve Cloud for disaster recovery.

Backups are the solution to ransomware recovery. To prevent ransomware attacks on Lyve Cloud backup targets, Lyve Cloud offers replication and modern immutable object storage that is like air gapping to ensure the highest levels of protection against deletion or manipulation. This functionality can also be leveraged with the customer's choice of S3 applications for data management and instant recovery of data backups on Lyve Cloud storage. Lyve Cloud helps maintain business compliance, further enhancing it to ensure business continuity. When used with the right tools, Lyve Cloud provides proactive insights that alert administrators in event of data manipulation.

In Conclusion

Lyve Cloud supports efficient strategies for ransomware protection and business continuity. Multi-layer security—including backup software abilities, unlimited backups, and overwrite periods supported by Lyve cloud attributes like replication, object immutability, and zero egress costs—result in the lowest total cost for your end-to-end anti-ransomware data protection strategy. Ultimately, this supports business continuity by ensuring backup data is always accessible for restore and disaster recovery in the cloud.

Benefits Summary

- Flexible API to complement any S3-compatible backup software vendor
- Air-gap-like object immutability that locks objects to prohibit anyone—including ransomware—from encrypting, modifying, or deleting data
- Replication at S3 bucket level
- Always-on data encryption for data at rest and in motion
- Multi-factor authentication
- Cost-efficient price model for seamless data backups

Ready to Learn More?

Visit us at www.seagate.com/lyvecloud or download the brochure

seagate.com

SEAGATE