Clumio Protection Against Data Loss and Ransomware

Providing an Air Gap for Robust Data Security

"According to a poll by CSO, the rate and variety of cyberattacks is growing every year, and it is already the largest financial threat to most businesses. Estimates suggest that by 2021, the total cost of cyberattacks will hit $6 trillion."

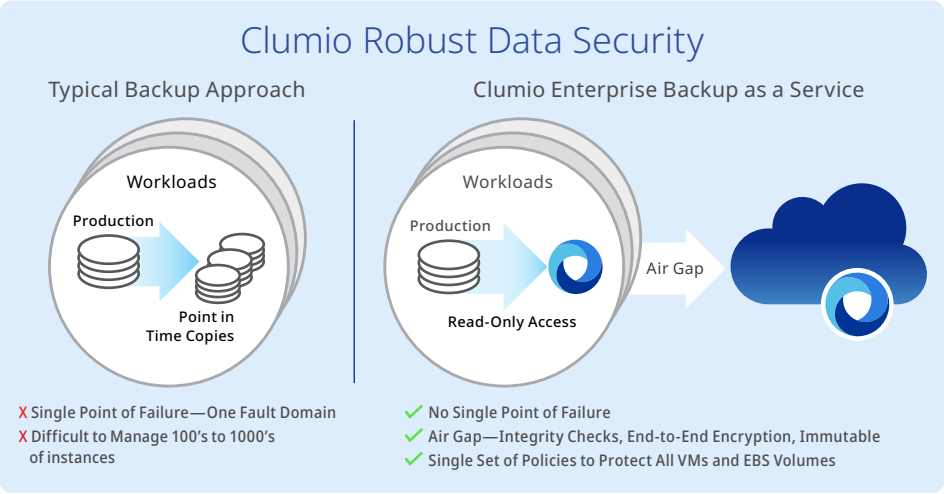
The Challenge

Traditional filesystems are vulnerable and often targeted for encryption during a ransomware attack. In most data protection environments, backup files, as well as the backup catalog are stored in production filesystems or volumes. Traditional backup appliances are particularly vulnerable to these types of attacks, due to the locality of data and inherent filesystem architecture. Here is how Clumio's SaaS solution provides additional layers of protection from data loss and ransomware attacks.

The Solution

During backups, Clumio directly writes all backup data, encrypted before transit, to an immutable S3 object store that resides in the Clumio Service, which means:

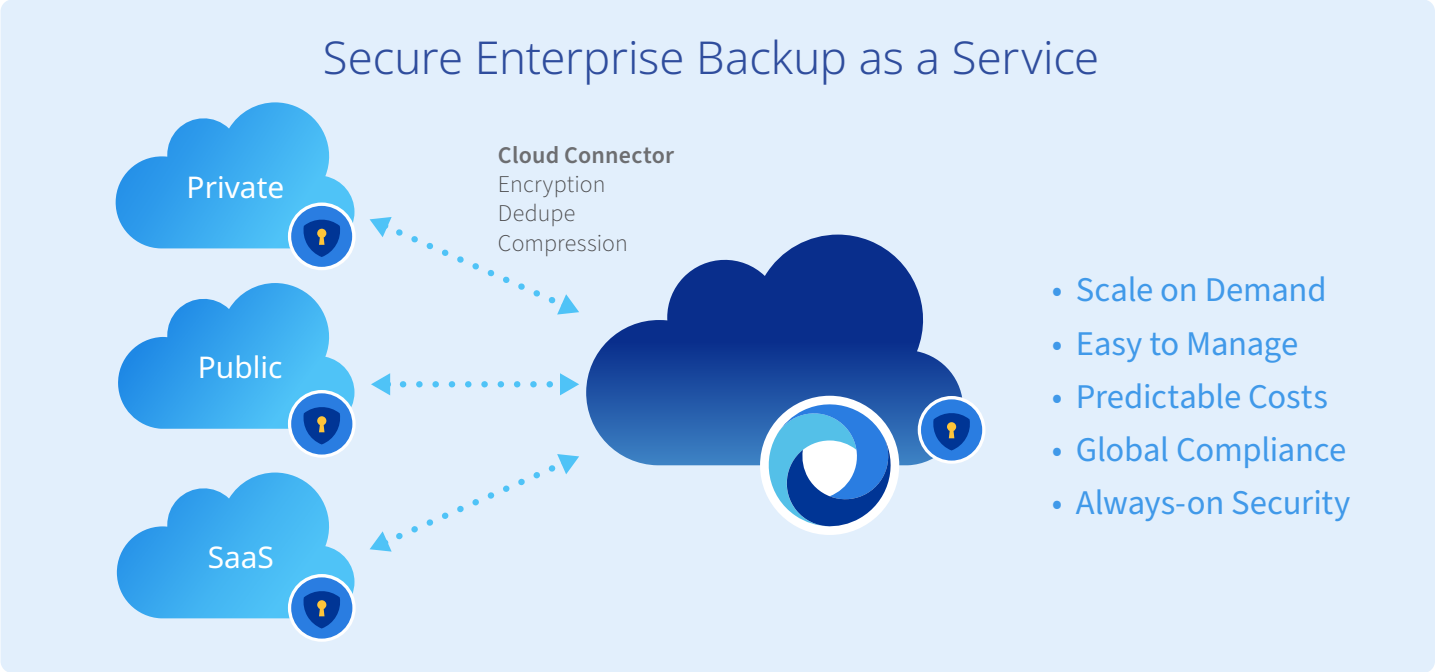
- The data, metadata, and catalog are stored in separate locations where any compromise in the customer environment does not compromise data secured in Clumio. Backup data is stored separately from backup metadata, which ensures that as the amount of protected data grows, no artificial scaling limits or performance bottlenecks are introduced. Furthermore, having the backup catalog secured and accessible outside of the backup data repository adds additional resiliency beyond a traditional appliance-based model. This isolation of backup data in the cloud is similar to not only sending backup tapes to Iron Mountain but also equates to shipping an active, manageable backup catalog to an additional secure location. A significant advantage over shipping tapes, however, is the immediate restore capability provided by Clumio. For additional protection, all Clumio customer accounts are secured independently by encrypting customer data at rest with unique keys. Under NDA, Clumio can discuss the technical processes used to secure all data and services on the platform.
- Backups written to Clumio can never be overwritten. Using a secured S3 object store, Clumio leverages an append-only write structure with versioning enabled, so overwrites or updates create a new version of the object, leaving the original version intact and unharmed. New data is stored in new locations within the S3 object store that provides (11) 9s of durability.



Continually Safe Restore Capability

Backup data can only be accessed through the Clumio UI or REST API calls. The requests go through multiple checkpoints to validate the origin of initiation and appropriate permissions. The customer has neither direct access nor root permissions to the backup data and catalog. There's no filesystem or storage location to mount, which could put existing data at risk in cases of user error, software bugs, or malicious intent. Since Clumio's S3 locations are securely abstracted and not directly accessible via external API calls, it's impossible to prematurely expire existing backups or access backup data directly via a ransomware attack. During a Clumio restore, data is reconstructed from metadata associated with the backup, and validated by comparing fingerprints for authenticity. As always, any data in flight is encrypted before transfer for additional security.

Summary Benefits



The necessity of securing backup data is more critical today than ever before. As the conversation changes from data protection to highly secure data protection, Clumio's SaaS offers many critical advantages over traditional data protection approaches. Clumio's mission is to provide a unified, comprehensive data protection strategy for modern hybrid cloud infrastructures. Clumio dramatically changes the data protection landscape by offering a solution that provides a simple, secure, and predictable opex consumption model for backup, recovery & data management.

Clumio is the innovator of authentic SaaS for enterprise backup. Using this secure service, organizations eliminate hardware and software for on-premise backup and avoid the complexity and cost of running third-party backup software in the cloud. As enterprises move aggressively to cloud, they use Clumio to protect workloads like VMware Cloud on AWS and AWS native services. Born in the public cloud, Clumio can leverage the most modern cloud services to ensure it meets the current and future backup requirements of the most demanding enterprises.

For more information, visit: www.clumio.com

CLUMIO