CLUMIO

SECURITY WHITEPAPER

Secure, immutable, air-gapped data protection

The Challenge

Businesses have no choice but to responsibly manage the protection, compliance, and governance of their data. But achieving sufficient protection and compliance requires secure processes and technologies. With increased cloud adoption, data gets distributed further, increasing the attack surface. As a result organizations are now faced with higher data risks and disaster recovery challenges. Most companies must invest heavily in the administration of multiple backup systems that drive significant complexity and management overhead. The additional threat of ransomware threatens to make any legacy backup solution all but useless and calls for a modern data protection solution that thwarts such attacks.

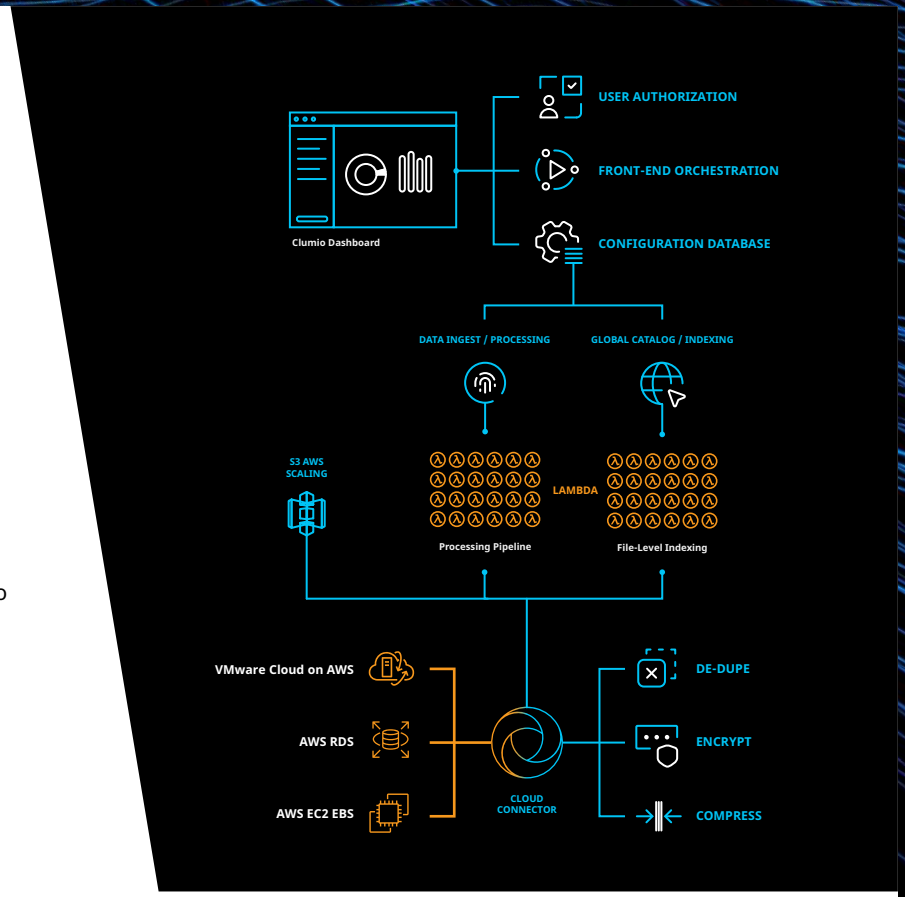
The Solution

The Clumio service is designed to securely protect data in an immutable, secured, and air-gapped platform. Clumio eliminates the need for enterprises to manage any backup infrastructure while allowing administrators to ensure their business stays compliant and protected from ransomware.

In today's world of frequent security breaches, the Clumio service is built from the ground up to preserve the integrity and security of customer data while providing critical separation from your cloud environment. From day one, Clumio "baked" security into its platform to ensure the highest level of data protection.

The Clumio Architecture

A single IAM role is required for the Clumio service to discover and protect your cloud data assets. This service is responsible for inventory detection, deduplication, compression, encryption, as well as for securely moving data between the customer's cloud environment and the Clumio data protection platform. Customer data is encrypted in-transit and at-rest while using the Clumio service. Other controls within the Clumio architecture ensure that customer's data is always encrypted when post- processing or other activities are performed.



Air-gap backups for ransomware protection

CISA recommends regularly protecting your data in an air-gap backup that stores the backup data outside the enterprise's network or security sphere. Backups stored with Clumio are completely isolated from the customer's AWS account. As a result, any compromise in the customer environment will not compromise data secured in Clumio. More on the CISA recommendation can be found here: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Secure Infrastructure

Clumio operates on Amazon Web Services (AWS). AWS operates an ISO 27001 certified organization and publishes a SOC 2 report under both the SSAE 18 and ISAE 3402 professional standards. More on how Clumio benefits from being deployed natively on AWS can be found here: https://aws.amazon.com/compliance/

Information Security Compliance and Certifications

Clumio operates an ISO/IEC 27001:2013 Information Security Management System and an ISO/IEC 27701:2019 Privacy Information Management System. These controls ensure that Clumio personnel, processes, and systems are trained, aware, and adhering to information security and privacy best practices. An SSAE 18 SOC 2 Type 2 report is available, along with a HIPAA Compliance report and a PCI-DSS SAQ-D. Find out more about Clumio's compliance, security, and privacy here: **https://clumio.com/legal/**

Secure Access to your Data

Clumio customers access the Clumio service via an email address and a password. Passwords adhere to recommended complexity rules. Customers can activate MFA or integrate with an Identity Provider for SAML 2.0 based single sign-on. Additional user controls can be managed through an implementation of Role Based and Entity Based access control, which provides granular control over access to assets — who can access what assets, what operations can be performed on those assets, and who can create or alter access control policies. Clumio also provides an API token based mechanism to be used by clients and client applications to securely access the Clumio API. Use the Clumio Console to securely manage API tokens and integrate Clumio into your existing workflows.

Network Security

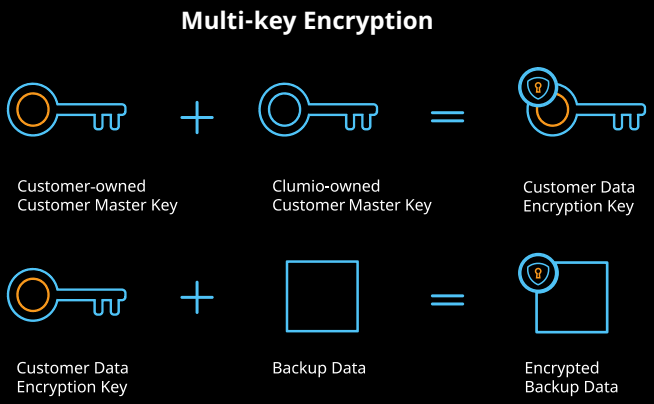
Communication from the customer's cloud environment to Clumio service happens over TLS connections, which prevent passive eavesdropping, active tampering, and forgery of messages. No inbound network ports are required to be opened for use of the service. Policies and roles are used to limit access to only what's necessary to protect customer data securely.

Data Segregation

The Clumio service assigns unique IDs to every registered customer. All future transactions like accessing the Clumio dashboard, performing data backup and restore, performing post-processing on the data always references that ID. The unique ID also has a corresponding key used to encrypt and decrypt data. This approach ensures that customer protected data is only accessible by the owner of that data.

Data Encryption

In addition to providing data segregation, the Clumio service uses AES-256 encryption algorithm. Clumio service uses AWS Key Management Service (KMS) to assign a unique Customer Master Key (CMK) to every single customer. The customer data is encrypted using Data Encryption Keys (DEK), which are derived from the customer specific CMK and are rotated every 30 days.



The Clumio service also supports Bring Your Own Key (BYOK). Many customers leverage their own KMS to create a CMK in their cloud account. The customer data is encrypted using a combination of Clumio- and customer-derived DEKs. This approach allows customers to own the keys to their data and can revoke access for Clumio service at their will. Customers can also audit the access to their keys and view when and why their key was accessed.

Penetration Tested

Clumio engages with a certified security testing firm to perform in-depth source code assisted penetration tests annually; attestations are available on request.

Conclusion

Companies are embracing the power of the cloud while simultaneously grappling with compliance, governance, and security requirements for data protection. Clumio's services follow industry accepted best practices and allow customers to free themselves from the complexity and inadequacies of backup solutions. While protecting against ransomware is a significant and important strategy, you can be assured that your "break-glass" disaster recovery plan has secure, immutable, air-gapped backups to restore to a known good state if the worst case scenario happens.

Request a 1:1 demo:

clumio.com/schedule-a-demo