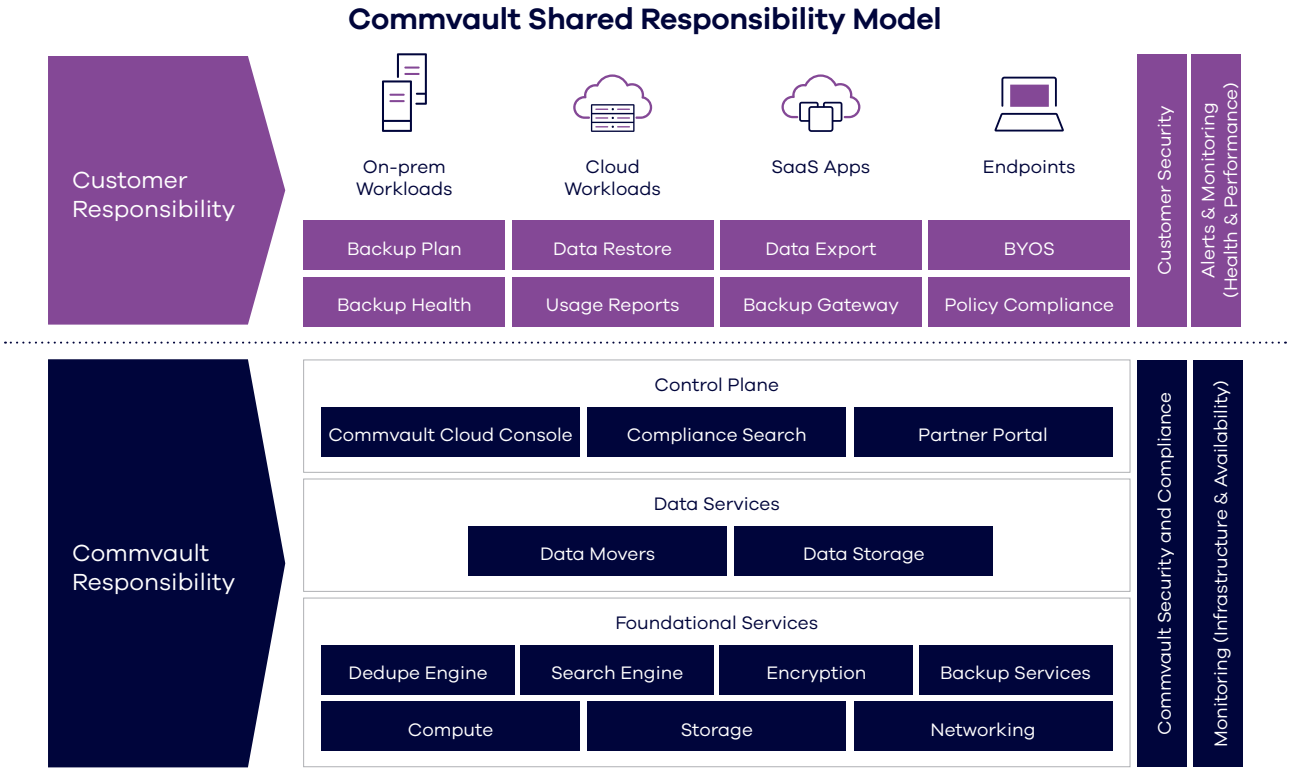
WHITEPAPER

Shared Responsibility Model

The following whitepaper details the Commvault® Cloud Shared Responsibility Model. It serves to clearly define the roles and obligations of Commvault (as the provider of SaaS delivered backup and recovery capabilities) and its customers (as the consumers of these capabilities).

WHAT IS SHARED RESPONSIBILITY?

Shared responsibility refers to a common framework where the ownership of specific tasks and obligations are shared between the cloud service provider and its users. Outlining the division of duties, is essential in ensuring transparency. As a cloud-delivered cyber resilience offering, Commvault is responsible for maintaining the infrastructure, availability, and performance of the service, while the customer takes responsibility for provisioning, configuring, and conducting routine backup and restore operations.



PROVISIONING

The provisioning phase includes initial configuration of the source connection, discovery of instances, and assignment of plans and policies. Initial provisioning is the customer's responsibility and includes ensuring all provisioning pre-requirements are met, as well as configuring proper user access (IAM), backup policies (RPO), and plan options (Storage and Retention). It is the Commvault responsibility to provide all customers with detailed pre-requirements, pre-checks, and recommended best practices to ensure a streamlined setup and provisioning process.

Identity and Access Management (IAM)

The Commvault Cloud provides customers with granular, role-based access controls (RBAC) and policies, to restrict access to authorized users and user groups only. By using Commvault, the customer maintains responsibility of ensuring the right Users and Administrators are setup and operational within their environment. Should the customer experience any related challenges while establishing or maintaining access, it is the customers' responsibility to notify the Commvault team for resolution.

Backup Plans

While the Commvault Cloud delivers the capabilities for data backups, each customer manages their own unique backup and retention requirements. This includes what resources to backup, where to backup data, and backup retention policies. Modifying and adjusting these backup preferences is also the customer's responsibility. Once configured, Commvault is responsible for backing up customer data in accordance with the policy configured. Commvault will also configure data aging in accordance with the customer's retention policy.

USAGE TRACKING

Commvault is responsible for providing customers with peak daily usage and monthly usage reports along with historical data and trends inside the Commvault Cloud platform. The customer is responsible for tracking ongoing usage in the Commvault Cloud portal to ensure it is in accordance with their existing service agreement.

BACKUP HEALTH

Commvault is responsible for providing detailed inventory of backed up instances and backup health reports to track the status of successful and failed backups. It is the customers responsibility to leverage these reports to monitor the health of their backups across the complete Commvault Cloud platform.

CUSTOMERS OPERATIONS

Data Restores

While Commvault provides controls for granular, flexible data recovery, the responsibility of performing a data restore lies with the customer. It is the customers' role to dictate the dataset and desired location for a restore.

Data Export

Should a customer's subscription end or is suspended, the customer responsible to extract their data prior to deletion. Please see the data deletion policies in the **Commvault Terms and Conditions** for more information.

CUSTOMERS INFRASTRUCTURE

Customers are responsible for the availability and access management to their data sources. Additionally, depending on the location of the customers data, a backup gateway might be required. Optionally, customers can use their own storage depending on where their data source is located.

Backup Gateway

Backing up on-prem and AWS data will require a backup gateway (proxy) to connect into the Commvault Cloud over a secure connection. Commvault is responsible for maintaining a secure connection to perform all backup and restore operations. The customer is responsible for provisioning this Backup Gateway and ensuring it is operational. Commvault will provide an automated deployment workflow (eg: deploying and configuring the VM and configuring the Commvault software) and

continuously alert users on health of this gateway.

Customer Provided Storage (BYOS)
In cases where a customer chooses to bring their own backup storage, applicable costs, infrastructure, lifecycle, and availability of this storage target lie with the customer.

COMMVAULT CLOUD SaaS INFRASTRUCTURE AND SERVICES

Commvault Cloud SaaS is built on highly available public cloud infrastructure and includes Foundational Services, Data Services, and the Commvault Cloud control plane. These services together deliver the backup, eDiscovery, and restore capabilities of the cyber resilience platform as a multitenant service.

Commvault maintains responsibility of the entire Infrastructure Lifecycle from initial deployment and scaling, to monitoring, securing, and patching the system. One of the key benefits of the SaaS model is rapid development and delivery of innovation and Commvault's responsibility is to deliver these updates in a timely, non-disruptive manner.

Also, based on our commitment to our customers, Commvault is accountable to deliver Commvault Cloud Service Availability of 99.9%.

Monitoring
Commvault is responsible for continually monitoring the Commvault Cloud operated infrastructure along with the Job execution to ensure all customer Jobs are running successfully. When Commvault detects an issue within the customer's environment, appropriate notifications are sent within the application via the Notifications, Status and Reports sections to provide actionable alerts to kickstart remediation.

The customer is responsible for monitoring infrastructure running within their own environment along with access and availability to the customers data sources. Additionally, the customer is primarily responsible for monitoring access of their protected Resources. The table below lists some customer responsibilities based on protected resource type:

Protected Resource	Customer Responsibility
Office 365, Dynamics 365, and Salesforce	Access to Data Source (incl. Credential management)
File and Object	On-Prem: Backup gateway Azure: None
VM, K8s, Databases (running in a VM), AWS	Backup Gateway
Commvault Cloud Storage Service (i.e., Clean Room Recovery)	None
BYOS	Availability and access to the data store

Reports & Alerts

Commvault is responsible for providing Reports and Alerts that enable a customer to track their RPO/RTO to their configured protection plans. Examples of some reports are as follows:

- Usage Reports: Daily or Monthly usage trends by Subscription
- Storage Utilization by Application includes application size as well as backup size.
- Backup Health including RPO status

Audit Trail

Commvault is responsible for providing a verifiable Audit trail for any operation on the customers backup data, performed either by a tenant or Commvault and particularly those that impact data retention or deletion.

Security and Compliance

Commvault is responsible for the underlying application security and employs a DevSecOps approach to enhance information and operational security. Additionally, Commvault is responsible for maintaining compliance with obtained compliance standards, such as FIPS 140-2, ISO 27001, SOC Type 2, STI and FedRAMP High. For additional information on Commvault Cloud security protocols, please see the **Commvault Security Whitepaper here**.

Commvault Cloud SaaS Security overview **here**.