WHITE PAPER

Commvault® Cloud

SaaS technical overview

Introduction

Commvault® Cloud, powered by Metallic® AI, offers enterprise-grade cyber resiliency from a unified platform. With flexible SaaS and software delivery models, Commvault Cloud offers a hardened and multilayered approach to securing data. Built leveraging Commvault IP, and with the best of Azure PaaS and native services, Commvault's SaaS-delivered solutions provide enterprise-grade backup as a service for critical workloads in the cloud and on-premises, including VMs (VMWare, AVS, VMC, Hyper-V), Kubernetes, enterprise databases (SQL, SAP HANA, Oracle) unstructured data (Windows, Linux, Azure Blob, Azure Files), SaaS applications (Office 365, Salesforce) and laptops/desktops.

Commvault Cloud delivers all the benefits of a SaaS-delivered solution, including hassle-free deployment, reduced management overhead, simple subscription pricing with no capex, automatic upgrades, and hands-off maintenance. At the same time, differentiated storage flexibility simplifies the move to cloud, by providing the unique option to leverage cloud or on-premises storage for the fastest recovery of hybrid cloud workloads. Through the breadth of the Commvault Cloud offerings, the unlimited scale, sophisticated layered security, and simple management, customers can stay protected now and for the future, as their IT strategies continue to shift and evolve.

COMMVAULT CLOUD SAAS SERVICE DESCRIPTION

Components

There are two major elements that comprise Commvault Cloud's SaaS-delivered solutions—the control plane and the data plane. The control plane, which provides features and functionality such as user experience, job management, and user security, runs in Microsoft Azure and provides a web-based user interface. Customer data does not flow through the control plane, minimizing network bandwidth requirements. The data plane encompasses all features and functionality of data protection and management operations and ensures that backup data flows can be optimized to protect and manage production data wherever it might reside—on-premises, public cloud, or private cloud.

In SaaS-to-SaaS data protection scenarios, such as Office 365, Salesforce, or Azure VMs, the data plane is managed by Commvault Cloud completely. No software deployment or additional infrastructure is required, other than optional customer-provided cloud storage. For these workloads, Commvault Cloud uses customer-provided credentials to connect to the customer's cloud services and backup the data. The data is transferred directly between the SaaS service and Commvault Cloud.

In hybrid cloud scenarios where data resides on-premises, limited software deployment is required to interface with the applications and platforms to be protected, provide for a secure communications channel to Commvault Cloud, and to support an optional on-premises copy of backup data. Backup gateways are deployed on-premises to facilitate communication with Commvault Cloud connect to optional on-premises, customer-controlled storage for a local backup copy. For workloads like VMware, where data protection can be performed agentless, the backup gateways handle the interface with the production workload. Commvault Cloud agents are deployed on production servers to leverage the APIs provided by applications and platforms such as Microsoft SQL Server and SAP HANA, which cannot be used remotely.

The Commvault® Cloud HyperScale™ X appliance can be used for the on-premises backup gateway, simplifying the deployment requirements even further and providing the necessary compute and storage resources to protect large on-premises workloads in a scalable manner.

In all deployment scenarios, the Commvault Cloud components are managed by Commvault Cloud operations, including upgrades/patching of Commvault Cloud software with no interaction required by customer administrators. This minimizes the management overhead of any service components.

Storage

Commvault has several options for backup storage, depending on the specific Commvault Cloud SaaS offering. These flexible storage options, tailored to each offering, were designed with our customers' input to optimally meet their RTO and RPOs. For all storage options, customers have complete control over where their data resides in order to meet data residency requirements.

With Office 365 Backup and Salesforce Backup, unlimited Commvault cloud storage is included with no transaction, ingress, or egress charges, for an all-inclusive TCO. This storage is based on Azure blob storage, replicated six times across two geographically separated regions. Unlimited retention for backups is also included at no extra charge. Customers can choose one or more storage regions worldwide and associate users to those regions, ensuring that their data storage location meets regulatory requirements. In addition to built-in Commvault cloud storage, Salesforce customers also have the option to bring their own AWS storage.

Endpoint Backup also includes unlimited Commvault cloud storage with no transaction, ingress, or egress charges. Retention of backup data is 1 year. The Commvault cloud storage redundancy and location specifications are similar to those with the Office 365 Backup and Salesforce Backup solution.

For on-premises workloads, CommvaultCloud can backup directly to Commvault cloud storage as well as Azure or AWS object storage that the customer purchases directly from Azure or AWS. The on-premises components perform compression and block-level deduplication to minimize network bandwidth utilization and natively integrate with cloud storage APIs to efficiently send and retrieve data. In addition, Commvault Cloud can maintain a local backup copy to any disk or NAS device. This local copy ensures that a backup is kept close to the production workloads, allowing Commvault Cloud to protect workloads of any scale and provide the fastest recovery possible. Retention on the local copy is completely configurable by customer administrators. Local copies of backups can be combined with cloud copies for longer term, offsite retention for resilience against ransomware and site disasters and cost optimization. When performing restores, Commvault Cloud will automatically retrieve data from disk or cloud storage in an optimized manner.

HyperScale X can be leveraged for on-premises backup storage as well for a fully integrated experience.

Networking and Communications

All Commvault Cloud network communications with the control plane are via mutually authenticated SSL (MA-SSL) connections. Certificate generation, revocation, and renewal are automatically managed.

Control connections from on-premises components to the Commvault Cloud service control plane are outbound only over port 443, minimizing the network access necessary to leverage Commvault Cloud. Connections to cloud storage also use HTTPS on port 443 outbound only.

COMMVAULT CLOUD SAAS SECURITY AND COMPLIANCE

Service Security

Commvault Cloud maintains a multi-layer approach to security, starting with partnering with Microsoft Azure to build on a robust, highly secure, and performant platform with a broad global presence. Azure provides hardened, redundant data centers with state-of-the-art physical and digital controls and maintains dozens of certifications, including FedRAMP High, across all Azure regions in the US. Commvault Cloud is built on Commvault technology, proven in enterprise and government environments to be highly secure. Capabilities such as role-based access control, auditing, integration with customer-owned authentication technologies like SAML, and encryption of all intra-service communications as well as data during transmission and at rest ensure that customer data is handled securely.

The technology in Commvault Cloud is developed to be secure right from the start, using a DevSecOps approach to make sure that information and operational security are always a priority when developing code. Testing and review for security defects are performed regularly by both in-house and external resources, including penetration testing, red team activities, and audits.

Commvault combines technology with operational excellence to complete the multi-layered approach. Commvault Cloud maintains SOC2 Type II and ISO.IEC 27001:2013 certifications, which incorporate controls, testing, and auditing of both the architecture and service configurations as well as policies governing personnel. A SIEM-based zero trust approach is used to ensure that all service elements are continuously monitored for anomalous events, which are handled appropriately. The SOC2 and ISO reports are available under NDA.

Additionally, all backup data is compressed, deduplicated, and encrypted by default from the source, on the network, and at rest using AES256. Multiple keys are used, so the compromise of any single key will not expose all data. Compression and deduplication also obfuscate data, providing additional security if the backup storage is compromised.

Ransomware

Commvault Cloud is well positioned to be the last line of defense in a customer's end-to-end security plan. As an air-gapped data protection service in a separate security domain, malware cannot spread from a customer's environment to the service, ensuring that the backup data is well protected and the service itself is available for rapid recovery. Global indexing with search capabilities combined with high performance enables customers to rapidly recover from attacks and minimize downtime.

In addition to providing rapid recovery of affected data, Commvault Cloud incorporates machine learning and other mechanisms to understand data change rate patterns. Should the service detect anomalous activity, it will send alerts to customer administrators to notify them of the potential of attack. This provides an avenue for ransomware detection that does not depend on detecting the digital signature of the ransomware itself.

GDPR

When providing services to EU customers as a data processor on their behalf, Commvault Cloud ensures compliance with the specific requirements for data processors. When third parties are appointed to act as sub-processors, appropriate terms are in place to comply with the GDPR and safeguard customers' data.

One of the aims of GDPR was to minimize the fragmentation of data privacy laws throughout the EU. However, EU Member States in certain cases are still able to introduce national legislation to further specify the application of GDPR rules. In addition, GDPR is subject to interpretation by Data Protection Authorities and courts (e.g. through of guidelines, decisions). Through closely monitoring of all relevant developments around GDPR, Commvault's solutions enable customers to stay on top of the changing data protection compliance landscape.

BAAS WITH NO COMPROMISE

Hybrid cloud is not an interim state. Companies need flexible, scalable and cost-optimized mechanisms to adopt new cloud technologies with peace of mind. When they do, they need to harness the best of the cloud to work together with the best of on-premises technology—with no disruption, eliminating data silos, and mitigating risk of attack. By incorporating sophisticated security innovations that Commvault has developed over 20 years of supporting secure backup connections, coupled with the strength of the Azure cloud platform, Commvault customers can adopt BaaS without compromise.

To learn more, visit **commvault.com/free-trial**