WHITE PAPER

Commvault® Cloud

SaaS security overview

WHITE PAPER

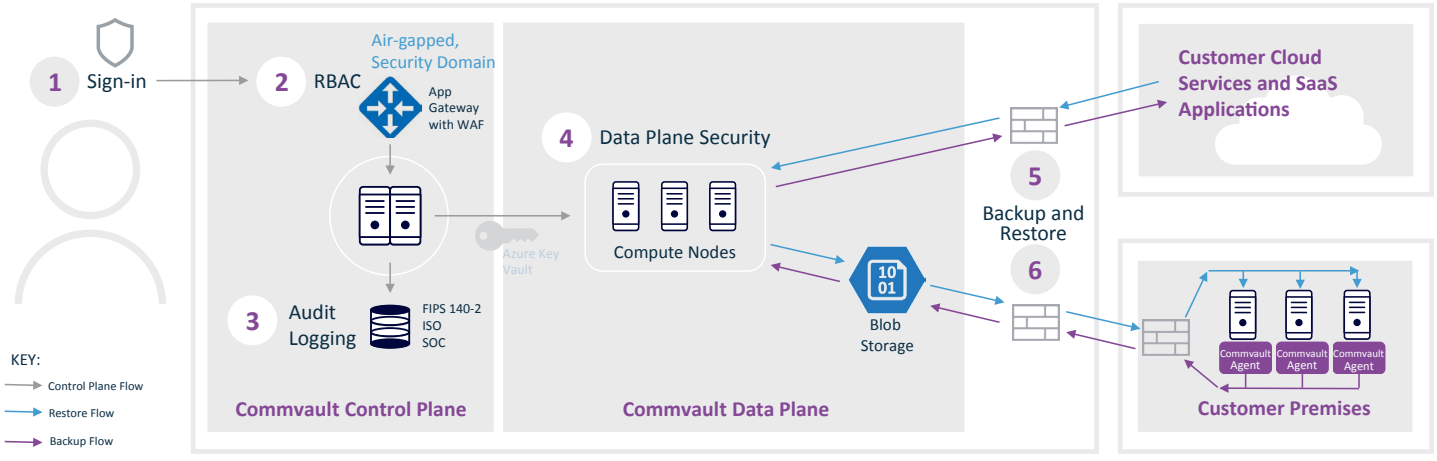
Introduction

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. The following is an overview of security and compliance protocols for Commvault Cloud's SaaS-delivered solutions. For a full description of features, functions, user terms, and conditions, please see the associated user documentation.

COMMVAULT ARCHITECTURE

Commvault Cloud is architected for scale and performance with separate control and data planes:

- **The control plane** provides features and functionality such as backup job management, data restores, tenant security administration, and more. The control plane for Commvault Cloud's SaaS-delivered solutions runs in Microsoft Azure and provides a web-based interface for user access. 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. It 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.



1 Sign-in: Via local id or SAML + MFA

2 RBAC: Role Based Access Control

3 Audit Logging: Audit of all user activity

4 Data Plane Security: Customer data isolation using per tenant storage containers Tenant Master Key Encryption Keys (stored in Azure Key Vault) One-way, TLS secure Network Communications

5 Backup: Encrypt data with tenant-specific encryption key

6 Restore: Decrypt data with tenant-specific encryption key

STORAGE

Commvault Cloud has several options for backup storage to help customers meet their RPO and RTO objectives:

- Air Gap Protect (MMR has been rebranded to Air Gap Protect): Commvault Cloud offers fully-managed, cloud backup storage. Customers can set policies to place their backup data in specific cloud service provider regions helping meet data residency requirements. For Microsoft 365, Dynamics 365, Salesforce, Endpoints, and Azure AD, cloud storage is included as part of the per user subscription costs.
- SaaS Plus: For hybrid-cloud workloads like protecting databases, file systems, VMs, cloud workloads, and containers, Commvault Cloud offers unique storage target flexibility. Customers can leverage both cloud native storage and local backup copies in concert, for stronger data resiliency and recoverability, including:
  - Bring Your Own Cloud Storage—customer cloud, such as Azure, OCI, or AWS
  - Air Gap Protect—cloud storage target that's fully managed by Commvault
  - Bring Your Own On-Premises Storage—customer on-premises server via any disk or NAS device
  - Hyperscale™ X—Commvault appliance, used for on-premises backup storage

DATA RESIDENCY

Cloud storage is included with Commvault Cloud protection for Microsoft 365, Dynamics 365, Salesforce, Endpoints, and Azure Active Directory, and is available as a standalone cloud backup storage target in Air Gap Protect. To provide high durability and availability. Commvault stores and synchronously replicates data among three availability zones in a primary region where the data resides. This provides a high level of resiliency, while ensuring data is never replicated outside specified regions to meet compliance with data residency requirements. For more information on data center regions and availability domains currently supported, please see our documentation.

IMMUTABILITY

Commvault leverages a hardened, multi-layered approach to data protection, providing robust controls that prevent various types of threats on backup data and ensures copies are highly recoverable from accidental deletion or malicious attack. Natively, all backup data is protected at the storage level. Backup copies and operations live in a virtually air-gapped location, in an isolated security domain, decoupled from source environments. Retention locks can also applied to prevent unwarranted modifications to data retention policies. Multi-factor authentication, dual AES 256 bit at-rest encryption, firewalls, and zerotrust access controls block internal and external movement of data by unauthorized parties. All security protocols employed adhere to security best practices and are based upon NIST 800-53, SOC2 type II, and ISO27001:2013 guidelines and compliance requirements.

DEDUPLICATION AND COMPRESSION

Commvault's compression and block-level deduplication improves network bandwidth utilization and reduces storage footprint. Cloud native storage APIs are used to efficiently send and retrieve data to the cloud when using cloud storage. Data deduplication enables further protection against data exfiltration and unauthorized usage as it is unreadable even after being decrypted without Metallic/Commvault proprietary deduplication engine.

NETWORKING AND COMMUNICATIONS

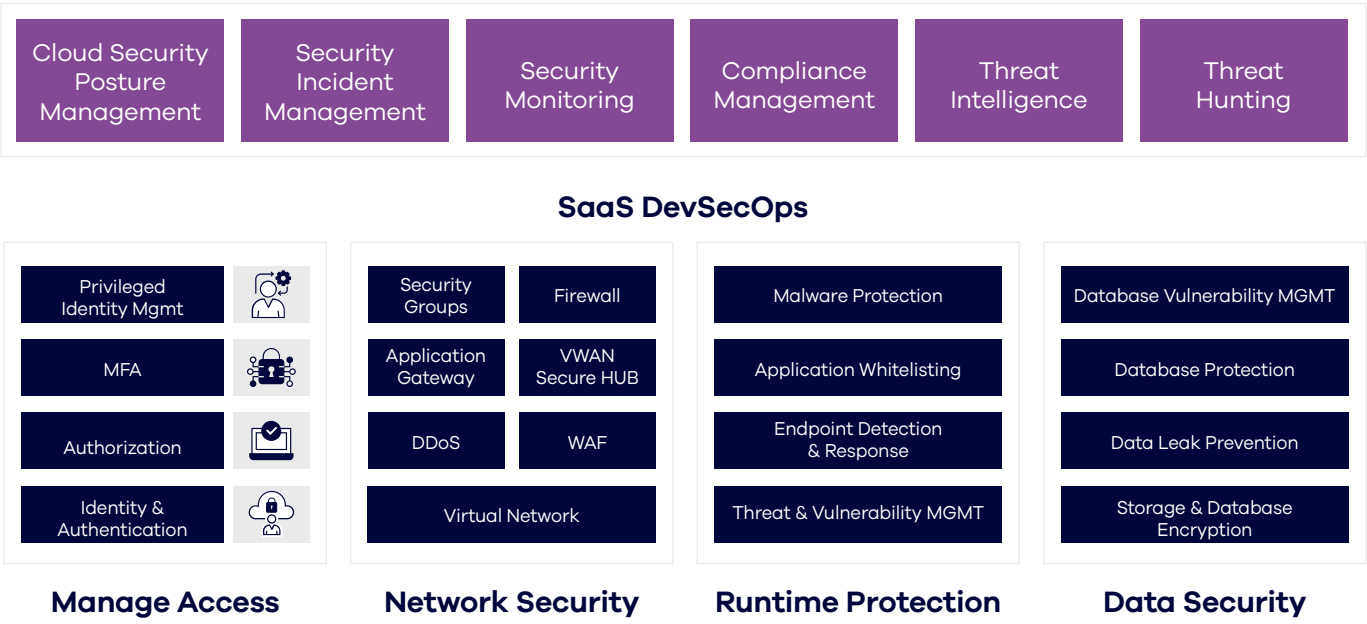
All network communications are managed via TLS (mTLS) using TLS 1.2 connections. Certificate generation, revocation, and renewal are automatically managed. Control connections from on-premises components to the Commvault Cloud SaaS service control plane are outbound only over port 443, minimizing the network access necessary to leverage Commvault Cloud. Connections to cloud storage also use HTTPS on port 443 outbound only. Data is always encrypted at source and in transit.

APPLICATION SECURITY

Commvault employs a DevSecOps approach to enhance end-to-end information and operational security. This includes following industry best practices to isolate test, dev, staging, and production environments. Testing and review for security risks are performed regularly by both in-house and external third parties, including routine penetration testing, red team activities, vulnerability assessments, and system and process audits.

Commvault Cloud service deployment uses layered security including firewalls, WAF and MFA to prevent any unauthorized and malicious access. Application Security assessments and vulnerability checks are regularly performed to maintain security hygiene and posture. Commvault also follows Open Web Application Security Project (OWASP) Top 10 best practices to secure web services and APIs, and maintains SOC2 Type II and ISO. IEC 27001:2013 certifications.

COMMVAULT CLOUD SAAS SECURITY ARCHITECTURE



DATA SECURITY

Separate security domain

Commmavult leverages a 100% cloud-native architecture and maintains backup and restore operations outside of customer environments—in a separate security domain. One-way, TLS-encrypted secure tunnels, are used to secure storage targets, without a physical network connection. Air-gapping controls within the solution include the ability to turn off connectivity to data stores when not needed, effectively severing the data path and reducing the risk of successful ransomware attacks in production environments impacting backup copies.

Multi-tenancy/data segregation

Commmavult Cloud is a secure multi-tenant cyber resiliency platform with built in-segregation between tenants. Customer data is completely isolated and stored in separate locations, with unique data encryption keys per tenant. Commvault also leverages zero-trust access controls, only permitting data owners (customer) access through the Commvault Cloud SaaS service.

Encryption

Encryption is an integral part of the Commvault Cloud. All backup data is compressed, deduplicated, and encrypted by default from the source, on the network, and dual encrypted at rest using AES 256 bit encryption. During transport, data is encrypted with a tenant-specific Data Encryption Key (DEK) before transferring the data across networks. Compression and deduplication also obfuscate data, providing additional security. Commvault cryptographic module is FIPS 140-2 certified.

Data access

Customer data backed up within Commvault Cloud is encrypted and not accessible or readable by Commvault employees. Access to data stored within Commvault Cloud is solely subject to policies and authorized user permissions established and managed by the customer.

Data owner right to delete backup data

Data that has been backed up can be permanently deleted so that it is no longer available for browsing and recovery. Data can only be deleted/purged by users with appropriate access and permission. Once data has been securely deleted, it cannot be restored.

Key management and generation

Key management includes the ability to both generate random encryption keys for backup data and manage the secure storage of these keys. To create the keys, Commvault uses CTR_DRBG, which randomly and dynamically generates keys via:

- Random 128-bit or 256-bit data encryption keys (DEK) for every client and storage policy copy combination, and initial vectors (IV) for CBC chaining during data encryption
- Random 128-bit or 256-bit master key for the storage policy copy in absence of third-party key management server

Commvault manages all encryption keys and follows best practices and procedures based on NIST Special Publication 800-57 as follows:

- Commvault generates a master key for each storage policy copy
- Commvault generates a pair of 3072-bit KEK (key encryption keys) RSA public-private keys:
  - Uses a master key to encrypt the private portion of KEK
  - Uses the default key to encrypt the public portion of KEK
- Commvault encrypts both the master key and RSA public-private key pair, and stores them in a secure lockbox

Commvault uses AES Key Wrap Specification to securely encrypt and secure all keys with CRC32 embedded. Commvault also automatically rotates keys every 30-days, without user intervention.

IDENTITY AND ACCESS MANAGEMENT

Access control is based on the Principle of Least Privilege and Zero Trust models in place designed to limit privileged and unauthorized access to both data and service infrastructure. We employ indursty-standard security best practices aligned to NIST 800-53 security guidelines for all access to our services with tight audit controls managed via best-in-class security and DevSecOps tools, services, and processes.

User Application Access

Passwords
Commvault Cloud supports SAML 2.0 and MFA authentication, allowing customers to implement their own password management controls and policies. Password complexity is enabled, requiring at least 12 characters, the use of three unique characters, and cannot contain more than two characters from the username. Password change frequency is 42 days, and at least three past password histories are logged. Commvault Cloud uses lockbox and vaults to secure customer passwords and credentials.

Logon attempts
Administrators can limit the number of times a user can attempt to logon to Commvault Cloud. After the limit is reached, the user account is locked for the time period defined by the administrator. For more information, see Limiting User Logon Attempts.

Two-factor authentication
When Two-Factor Authentication is activated, users must enter a 6-digit PIN (Personal Identification Number) along with their passwords to access Commvault Cloud.

Role-based security
Commvault Cloud has built-in Role Based Access Controls (RBACs) to restrict access to authorized users. A role is a collection of permissions administrators assign to users and entities to create a three-way security association. Roles can be assigned to grant appropriate access to any user or user group.

Integration with external domains
Administrators can manage a single set of users through integration with external directory services like Active Directory and Oracle Directory. Commvault Cloud roles and entities can be assigned directly to an external group or user.

SAML support
Commvault Cloud supports SAML authentication. SAML can be used to create a single identity for each user for a single sign-on logon for all applications. A SAML User Registration Workflow is available to create usernames.

Privacy
Commvault Cloud prevents users and administrators who are not client owners from seeing the data on the client. This includes Commvault employees and personnel who do not have access to customer data.

Infrastructure access

Physical access
Commvault Cloud offers a Software as a Service delivery model, utilizing a cloud-shared responsibility model. In this model, Commvault helps ensure all data and access to the data is secured, while leveraging the cloud service provider for perimeter and physical access controls.

GOVERNANCE AND RISK MANAGEMENT

Commvault is ISO27001:2013 and SOC 2 Type II compliant, maintaining and implementing industry-standard security and privacy policies aligned to NIST 800-53 security guidelines. Best-in-class cloud and SaaS service configuration management tools are employed to ensure any deviations from configurations detected are remediated automatically. All access is logged for audit and compliance reasons. Compliance with information security policies and procedures is strictly enforced and all Commvault's employees receive training to ensure they remain aware of their role in maintaining the security, availability, and confidentiality of customer data among their other job responsibilities.

Audit trail
Commvault audit trails allow customers to track user actions within Commvault Cloud services and can help in determining the root cause or source of operations performed within the environment. All changes are logged per Commvault SRE and DevSecOps requirements and follows SOC2 Type II and ISO27001:2013 compliances and standards.

Incident response plans
Commvault has a comprehensive Incident Response Plan (IRP) program, tested annually by a certified third party as part of our normal ISO and SOC2 certification requirements. Daily scanning is performed and procedures are tested through internal and external audits.

Business continuity
Commvault Disaster Recovery (DR) procedures are based on the Commvault Business Continuity and Disaster Recovery (BCDR) policies. The DR procedures encompass all production services within Commvault Cloud, are well established, reviewed every year, and continuously enhanced at scale to support our customers.

GDPR
When providing services, Commvault ensures compliance with specific GDPR 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. Please see our GDPR Compliance page for more details.

FedRAMP High
Commvault Cloud for Government, our portfolio of solutions for US government agencies and private businesses handling federal data, is currently the ONLY data protection solution to meet FedRAMP High status. Commvault Cloud for Government incorporates 421 required security controls to meet the most stringent confidentiality, integrity, and availability standards set forth by the US government. Please visit our Commvault Cloud for Government page for additional information.

Cyber deception
Threatwise™ offers fully-integrated ransomware detection technology across our award-winning portfolio for pre-attack identification and containment. By precisely simulating real resources, Threatwise decoys are indistinguishable and, when engaged, provide high-fidelity warning signals on active attacks in production environments - before data exfiltration, leakage, encryption, or damage. This helps neutralize silent attacks before they cause harm; detecting and diverting the stealthiest of zero-day attacks which evade conventional circumvent security controls. Please visit the Threatwise page for additional information.

Certifications and compliance
For full list of certifications and standards met by Commvault, please visit the following webpage.