Commvault - Metallic

With Commvault Metallic, you're not just protecting your data; you're investing in the future of your business. Discover how our solution can unlock the potential of your data, turning challenges into opportunities and ushering in a new era of security, management and innovation. Welcome to a world where your data is more than an asset: it's the key to your success. Welcome to the future with Commvault Metallic!

Welcome to the revolutionary world of Commvault Metallic, a cutting-edge solution designed to meet the growing need for data protection in an ever-changing digital environment. Commvault Metallic represents excellence in data backup and recovery, offering a comprehensive suite of cloud services to ensure the security, availability and efficient management of your critical information.

This innovative platform combines the power of traditional backup with the flexibility and scalability of the cloud, offering a complete, easy-to-use solution for businesses of all sizes. Whether you're a small business looking to protect your sensitive data, or a large organization requiring an enterprise-wide, scalable solution, Commvault Metallic adapts to your specific needs.

Commvault Metallic is much more than just a data backup and recovery solution. It's a complete immersion in the modern world of data management, an experience that goes beyond conventional expectations. In a world where digital transformation is the key to success, Commvault Metallic is positioned as the ideal partner, offering a comprehensive suite of advanced features, all designed to meet the complex and dynamic challenges facing businesses.

Imagine a platform where the power of traditional backup is transcended by the infinite advantages of the cloud. Commvault Metallic offers exceptional agility, enabling your business to adapt quickly to change, while guaranteeing the security and availability of your most critical data. This harmonious fusion of proven technologies and innovative cloud solutions offers unprecedented flexibility, adapting perfectly to the specific needs of your business, whatever its size or complexity.

Whether you want to optimize your day-to-day data management, strengthen your company's resilience against digital threats or simply ensure uninterrupted operational continuity, Commvault Metallic is your answer. Explore advanced features for automated backup, rapid recovery and intelligent data management, all in a user-friendly, intuitive environment.

With Commvault Metallic, you're not just protecting your data; you're investing in the future of your business. Discover how our solution can unlock the potential of your data, turning challenges into opportunities and ushering in a new era of security, management and innovation. Welcome to a world where your data is more than an asset: it's the key to your success. Welcome to the future with Commvault Metallic!
For more details on each of the Commvault Metallic solutions, we invite you to consult the fact sheets on the following pages (English only).

DATA SHEET

Commvault® Cloud: Backup and Recovery for Microsoft 365

Your docs, inboxes, and conversations need protection too

Commvault Cloud, powered by Metallic AI, delivers powerful, enterprise-grade Microsoft 365 data protection. With broad-ranging coverage across the entire Microsoft 365 environment, Commvault keeps valuable data safe from deletion, corruption, and ransomware attack—all with the simplicity of SaaS.

DATA RESILIENCY AND CYBER RECOVERY

- Advanced privacy, data security, and AI built-in
- Isolated and immutable backups, outside production environments
- Dedicated controls to meet SLA and compliance requirements

Complete coverage

Comprehensive protection across Exchange, Teams, OneDrive, and SharePoint data. Effortlessly locate active or deleted data, rapidly recover from attack, and meet your SLA and compliance requirements with ease.

- Long term, extended retention, beyond recycle bin limitations
- Granular search and eDiscovery
- Flexible point-in-time and out-of-place recovery options
- Deduplication and compression for optimized performance
- Self-service, end user restore options

Enterprise- grade protection

Go above and beyond for your critical Microsoft 365 data. With stringent security standards, privacy protocols, and zero-trust access controls built-in, Commvault Cloud provides multi-layer data protection minimize cyber attacks and combat today's data loss threats.

- Isolated, air-gapped backups from source data
- Layered security plus GDPR compliance
- At-rest and in-flight data encryption
- Role-based, SSO, SAML authentication controls
- Advanced security insights and threat monitoring

Award- winning SaaS

With Metallic® Backup for Microsoft 365, you get cost-effectivedata protection, without the complexity. Metallic means hasslefree deployments, maintenance, and management. SaaS that's proven to reduce costs and eliminate headaches—so you only pay for what you need.

- Azure storage and extended retention included
- No hardware or large upfront capital investments
- Zero egress fees or hidden storage charges
- Automatic updates and maintenance built-in

SUPPORTED PLATFORMS AND APPLICATIONS

Platforms

Windows	Apps: · Microsoft 365 Exchange Online · Microsoft 365 Teams · Microsoft 365 SharePoint · Microsoft 365 OneDrive · Microsoft 365 Groups · Microsoft 365 Project Online

Environments and Storage

Environments	· Commercial · GCC · GCC High
Storage	· Extended storage and retention included

To learn more, visit **commvault.com**

metallic®
A Commvault Venture

Metallic® SaaS Backup

Security Overview

Introduction

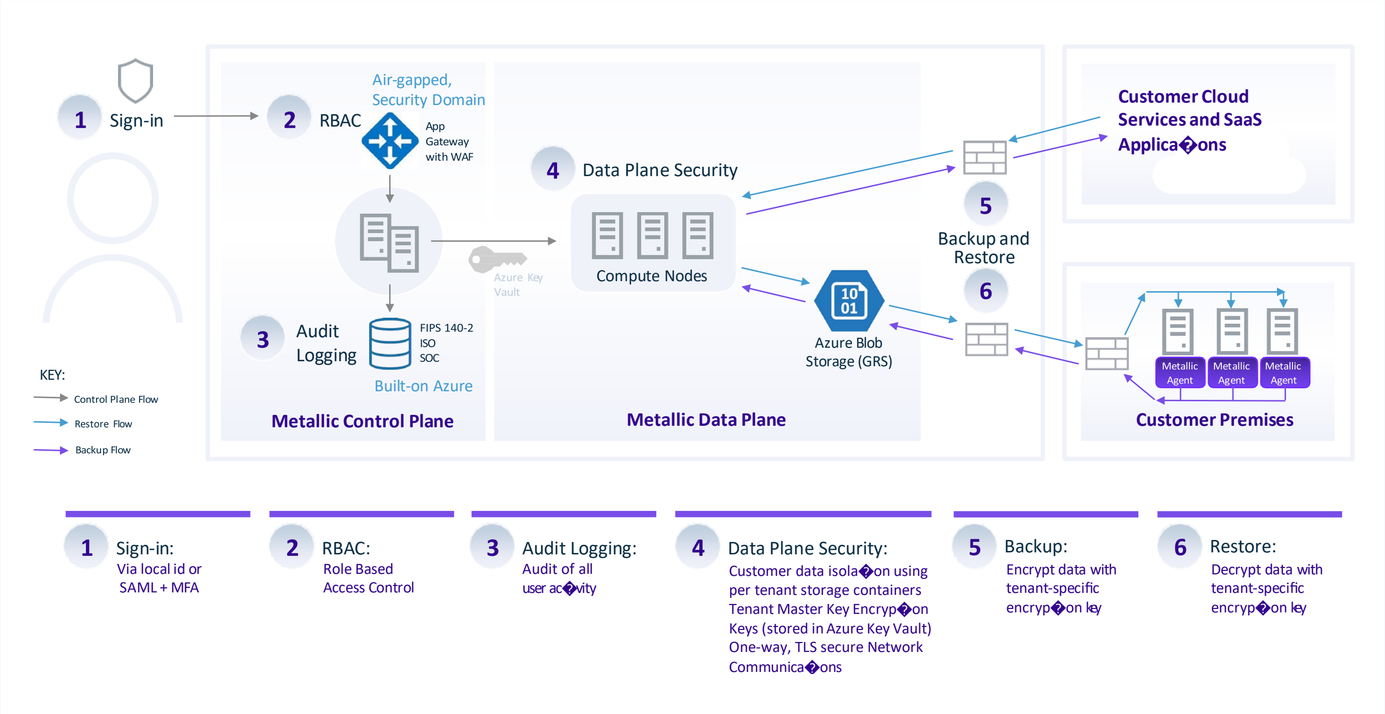
Metallic® is the BaaS (backup-as-a-service) division of Commvault®, a worldwide leader in intelligent data management. Built leveraging Commvault IP, and with the best of Azure PaaS and native services, Metallic delivers enterprise-grade backup with the simplicity of SaaS. With sophisticated protocols and a hardened, multi-layered security approach, Metallic® SaaS Backup helps customers protect critical endpoints, SaaS applications, and cloud and on-premises workloads now and in the future - as IT strategies continue to shift and evolve. The following is a summary; for a full description of Metallic security, features and functionality, and user terms and conditions, please see the associated user documentation.

Metallic Architecture

Metallic is architected for scale and performance and separates the control plane and the data plane:

The control plane, provides features and functionality such as the user experience, job management and user security. The control plane runs in Microsoft Azure and provides a web-based interface for user access. Customer data itself 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 ac�vity

4 Data Plane Security: Customer data isola�on using per tenant storage containers Tenant Master Key Encryp�on Keys (stored in Azure Key Vault) One-way, TLS secure Network Communica�ons

5 Backup: Encrypt data with tenant-specific encryp�on key

6 Restore: Decrypt data with tenant-specific encryp�on key

Storage

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

- Metallic® Cloud Storage Service: Metallic offers a fully-managed cloud backup storage, built on Microsoft Azure. Customers can set policies to place their backup data in one or more Azure regions helping meet data residency requirements. Unlimited Metallic Cloud Storage is included in Metallic® backup solutions for Office 365, Dynamics 365, Salesforce, and Endpoints as part of the per user subscription costs.
- SaaS Plus: For hybrid-cloud workloads like Metallic® Database, Metallic® File & Object, and Metallic® VM & Kubernetes, Metallic 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 or AWS
  - Metallic® Cloud Storage Service – cloud storage target that's fully-managed by Metallic
  - 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

Metallic® Cloud Storage Service (included with Metallic® Backup solutions for Office 365, Dynamics 365, Salesforce, and Endpoints and offered as a standalone service), is a cloud backup storage target, built on Microsoft Azure. To ensure durability and availability for disaster recovery, stored data is replicated six times across two geographically separated regions. By default, Metallic will geo-locate the user and provision storage in the nearest Metallic Azure data center. Customers also have full autonomy to choose one or more Azure storage regions around the world and associate users to those regions, ensuring that their backup data is stored in locations that meet data residency and compliance requirements. For more information on data center regions currently supported with Metallic, please see our documentation here: https://docs.metallic.io/metallic/147962_metallic_and_metallic_cloud_storage_service_mcss_data_center_regions.html

Immutability

Metallic leverages a hardened, multi-layered approach to data protection, providing robust controls that prevent threats on backup data and ensure copies are highly recoverable from deletion or malicious attack. Natively, we protect all backups at the storage level. Backup copies and operations live in a virtually air-gapped location, in a separate security domain, decoupled from source environments. Retention locks are applied to prevent unwarranted modifications to data retention policies. Multi-factor authentication, AES 256 bit at-rest/in-flight encryption, firewalls, and zero-trust 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 SOC2 type II and ISO27001:2013 compliance requirements.

Deduplication and Compression

Metallic'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.

Networking and Communications

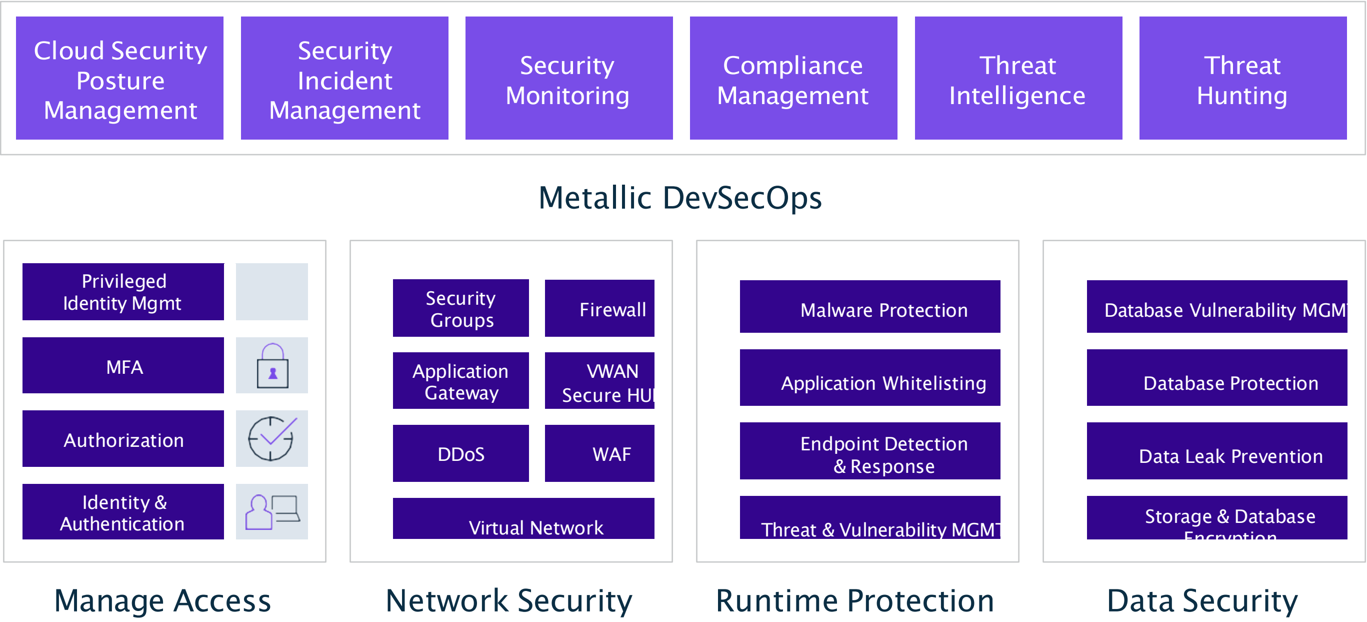
All network communications are managed via mutually authenticated SSL (MA-SSL) connections. Certificate generation, revocation and renewal are automatically managed. Control connections from on-premises components to the Metallic service control plane are outbound only over port 443, minimizing the network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

Application Security

Metallic employs a DevSecOps approach to enhance 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, anti-virus assessments and system and process audits.

Metallic 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. Metallic also follows Open Web Application Security Project (OWASP) best practices to secure web services and APIs, and maintains SOC2 Type II and ISO.IEC 27001:2013 certifications.

Metallic.io Security Architecture



Cloud Security Posture Management

Security Incident Management

Security Monitoring

Compliance Management

Threat Intelligence

Threat Hunting

Metallic DevSecOps

Privileged Identity Mgmt

MFA

Authorization

Identity & Authentication

Manage Access

Security Groups

Firewall

Application Gateway

VWAN Secure HU

DDoS

WAF

Virtual Network

Network Security

Malware Protection

Application Whitelisting

Endpoint Detection & Response

Threat & Vulnerability MGMT

Runtime Protection

Database Vulnerability MGM

Database Protection

Data Leak Prevention

Storage & Database Encryption

Data Security

Data Security

Separate Security Domain

Metallic 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

Metallic is a multi-tenant SaaS Platform with built in-segregation between tenants. Customer data is completely isolated and stored in separate locations, with unique data encryption keys per tenant. Metallic also leverages zero-trust access controls, permitting only the data owners (customer) access through the Metallic Service.

Encryption

Encryption is an integral part of Metallic. All backup data is compressed, deduplicated, and encrypted by default from the source, on the network, and at rest using AES256. 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. Metallic is FIPS 140-2 certified.

Data Access

Customer data backed up within Metallic is encrypted and not accessible or readable by Commvault employees. Access to data stored within Metallic is solely subject to Customer's policies and authorized user permissions.

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 also manage the secure storage of these keys. To create the keys, Metallic 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.

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

- Metallic generates a master key for each storage policy copy
- Metallic 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.
- Metallic encrypts both the master key and RSA public-private key pair, and stores them in a secure lockbox.

Metallic uses AES Key Wrap Specification to securely encrypt and secure all keys with CRC32 embedded. Metallic 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 elevated and unauthorized access to both data and service infrastructure. We employ industry standard security best practices 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

Metallic supports SAML and MFA authentication, where customers can 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. Metallic 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 Metallic. 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 Metallic.

Role-Based Security

Metallic 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. Metallic roles and entities can be assigned directly to an external group or user.

SAML Support

Metallic 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

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

Infrastructure Access

Physical Access

Metallic is a Software as a Service consuming Azure Cloud IaaS. Leveraging the cloud's shared responsibility model, Metallic helps ensure all data and access to the data is secured. Metallic leverages Microsoft Azure for perimeter and physical access controls. For Azure data centers, see the link for an in-depth security review. https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Governance and Risk Management

Metallic is ISO27001:2013 and SOC 2 type II compliant, maintaining and implementing industry standard security and privacy policies. 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 are 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

Metallic audit trails allow you to track user operations who have access to Metallic services and can help in determining the root cause or source of operations performed within the environment. All changes are logged per Metallic SRE and DevSecOps requirements and follows SOC2 Type II and ISO27001:2013 compliances and standards.

Incident Response Plans

Metallic has an Incident Response Plan (IRP) program and it is 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

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

GDPR

When providing services, Metallic 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

Metallic Government Cloud, 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. Metallic Government Cloud is hosted exclusively on Azure Government Cloud, and incorporates 421 required security controls to meet the most stringent confidentiality, integrity, and availability standards set forth by the US government. For more information on Metallic Government Cloud, please visit the following page for more details.

Certifications and Compliance

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

Commvault reserves the rights to change and/or modify these features and functionalities at any time, without notice.

DATA SHEET

Preserve data with less headaches and fewer oversights

Commvault® Cloud: eDiscovery + compliance

Microsoft 365 + Endpoint eDiscovery provides a single interface to drive organizational compliance with better speed and precision.

Paired with Commvault Cloud data security and protection, businesses get the best of industry-leading cyber resiliency combined with advanced tools to satisfy regulatory compliance – all from one SaaS platform.

Say goodbye to disparate applications and expensive third-party solutions.

With eDiscovery for Commvault Cloud, you get inclusive coverage that fluidly spans across Microsoft 365 and endpoint workloads, making compliance a breeze.

- Rapidly identify pertinent emails and files – active or deleted
- Uncover data buried deep within workloads
- Seamlessly locate records across Microsoft 365 and endpoint environments, in unison
- Preserve data for legal and regulatory purpose with flexible pst exports
- Maintain EDRM compliance, adhering to identification, collection and processing protocols

eDiscovery across:

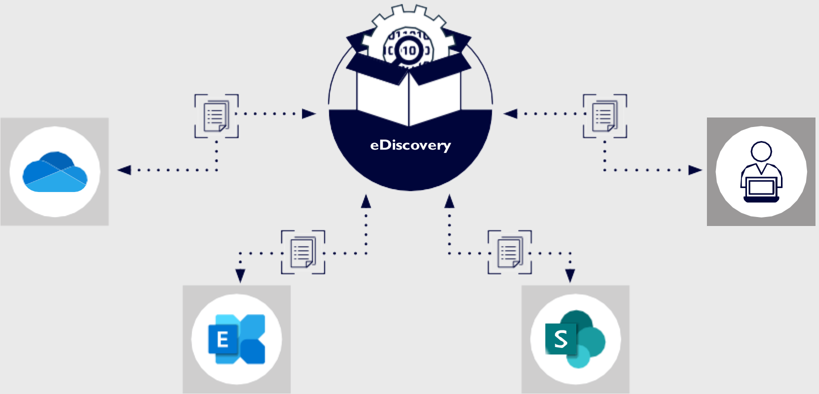
Exchange Online

SharePoint Online

OneDrive

Endpoints

A single experience to drive compliance across critical workloads.



To learn more, visit **commvault.com**

commvault.com | 888.746.3849

DATA SHEET

No-compromise solutions for optimal cyber resilience

Commvault® Cyber Resilience for hybrid cloud data protection

As companies modernize their IT strategies, every journey to the cloud is unique. Companies need flexible, powerful and ultimately secure cyber resilience to meet them where they are today, and help them reach where they want to go tomorrow. With broad support of on-premises and cloud-native workloads, virtualized environments, and containers, plus unique storage flexibility, Commvault cyber resilience helps you innovate with peace of mind. Safeguard your data while making the most of your IT resources, reducing data silos, and mitigating the growing risk of ransomware and cyberattack.

HOW WE ARE DIFFERENT:

- Award-winning cloud-based data backup and recovery from industry-leader Commvault
- Reduced management overhead, rapid deployment
- Future-proof scalability, from 1TB to 1,000+
- Unique hybrid cloud storage flexibility for performance and value
- Enterprise-grade data protection at hyper-speed
- Flexible, subscription-based pricing with no capex investment
- Ultimate, layered security for ransomware protection

Powerful data security with the simplicity of SaaS. With Commvault you get single-solution cyber resilience for critical hybrid cloud data—wherever it lives. Safeguard on-premises, cloud, containers and beyond, for future-proof cyber resilience across your entire data estate.

HYBRID CLOUD PROTECTION

Backup & Recovery for VM & Kubernetes

For VMware, Hyper-V, Azure VMs, AVS, OCI VMs, Amazon EC2, VMC, Oracle Container Engine for Kubernetes (OKE)

Backup & Recovery for databases

For Microsoft SQL Server, Azure SQL Server, Azure MySQL, Azure MariaDB, Azure PostgreSQL, Azure Cosmos DB, Oracle and Oracle RAC databases, Oracle Database Cloud Service (DBCS), Oracle Exadata Database Service on OCI, Oracle Exadata Database Service on premises, SAP HANA, Amazon RDS, Amazon DynamoDB, Amazon DocumentDB, Amazon Redshift

Backup & Recovery for files & objects

For Windows Server, OCI Object Storage, Linux/UNIX, Azure Blob & Files, Amazon S3

+

SECURE CLOUD STORAGE

Air gap protect

For air-gapped storage with long- and short-term retention

+

ARCHIVE & COMPLIANCE

Commvault Cloud Archive for files & objects

For cost-efficient archiving of unstructured data

Start your free trial today: **commvault.com**

SOLUTION BRIEF

Commvault

Engage better business protection against ransomware

Commvault® Cloud Air Gap Protect

Ransomware is an unfortunate reality that businesses of all sizes need to plan for today. Without proper ransomware readiness, organizations are less likely to recover quickly and ensure business continuity—experiencing data loss and expensive business downtime in an era when users and businesses require their data to be accessible and available around the clock. In short, data protection offers organizations a lifeline to business continuity and faster recovery from disruptions.

Ransomware protection is a critical part of an organization's end-to-end security strategy—and necessitates capabilities to detect threats and protect critical copies of data from being compromised. Within any company's strategy, data protection is a last line of defense, and the right path to limiting damage from ransomware attacks is to place the data and infrastructure out of the reach of cybercriminals. Adding air-gapped backup storage infrastructure can make all the difference to quick recoverability.

Cloud-based data protection solutions provide a virtual air gap of backups and restore operations. Backup data copies are stored in isolated, immutable locations—preventing data from being tampered with, altered, or deleted. Cloud-based data protection solutions insulate businesses from ransomware attacks that compromise on-prem tools and ensure recovery operations with a clean environment.

> 51% of businesses have been impacted by ransomware in the last year."[1]

DISCOVER THE BENEFITS OF MANAGED STORAGE FOR RANSOMWARE PROTECTION

Commvault predicted this growing need for container-based data protection solutions years ago, so the company established support for Docker, Red Hat OpenShift, and proactively started future-proofing customers' IT environments. Commvault also foresaw the unification of storage and data protection needs, which led to complementing their Intelligent Data Management portfolio with differentiated hybrid cloud-native storage for virtualization and containers.

Risk mitigation

Managed cloud storage is a vital part of an overall security posture that every organization needs. Robust access management, anomaly detection, data encryption, hardened security, and comprehensive user access controls are necessary for a successful defense against cybercriminals.

Business continuity

The average IT disruptions are one thing, but wholesale data loss is another ball game. Managed cloud storage removes the prospect of an extended business shutdown, reduces the potential for attack success, and narrows the window for recovery for businesses.

Lower costs

The cost of data protection pales compared to the potential costs of an effective ransomware attack. Costly downtime and lofty payouts threaten to not only halt business operations but can result in permanent customer data loss. Organizations should err on the side of proactive safety and leverage managed cloud storage as a means to secure their valuable data.

THE AIR GAP PROTECT DIFFERENCE

Commvault Cloud leverages a hardened, multi-layered approach to ransomware readiness, providing robust controls to prevent threats and ensure data is highly available and recoverable from cyberattack. With immutable, air-gapped data copies, advanced anomaly detection, and built-in encryption, Commvault Cloud comprehensively safeguards critical data across apps, endpoints, on-prem, and cloud environments. Built on Microsoft Azure, Commvault Cloud offers industry-leading durability, security, scalability, and performance, capable of protecting business data from today's and tomorrow's cyberthreats. Air Gap Protect is a fully managed cloud storage target, offering ultimate security and scale to let organizations seamlessly adopt cloud storage. Available with Backup and Recovery, as well as with the SaaS hybrid cloud portfolio, Air Gap Protect makes it simple to adopt cloud storage—without a steep learning curve and for air-gapped ransomware protection and optimized costs.

Top challenges of cloud-based ransomware protection

- Increasing cloud costs with cloud expansion and cloud deployments
- Reliable ransomware protection with a secure, air-gapped, offsite data copy
- Trusted backup and recoverability of an organization's most valuable asset: data

HIGHLIGHTS OF AIR GAP PROTECT

Ransomware and risk reduction

- Virtual air-gapped copy of the data with stringent security protection of Azure cloud
- Encryption and access controls within the Commvault environment for powerful added security to ensure recovery from a ransomware attack

Capacity growth

- Meet changing capacity needs on the fly with easy access to cloud

Effectively manage cloud costs

- Predictable storage costs allow IT to build out long-term forecasting and avoid unexpected bills

Hybrid cloud adoption

- Beyond a tape library, leverage cloud-based storage and realize the benefits of agile management, limitless scale, and cost savings of cloud
- Easy onramp to cloud for organizations that lack the skills and want to incorporate cloud in their IT strategy

Secondary backup copies

- Support the 3, 2, 1 rule: Three copies of the data, two in different locations, and one off-site

SHORT AND LONG- TERM RETENTION STORAGE OPTIONS

Air Gap Protect Hot and Cool storage tiers provide greater flexibility for cloud storage options. If an organization is looking for a primary backup copy repository, they can use Hot storage, while those seeking a secondary storage option for longer retention can leverage Cool storage. Both storage tiers can be used together for flexibility and an end-to-end storage strategy.

Hot storage

Fit for short-term retention, typically 30 days or less. Reduce reliance on physical infrastructure or enable cloud-to-cloud backups for quick recovery.

Cool storage

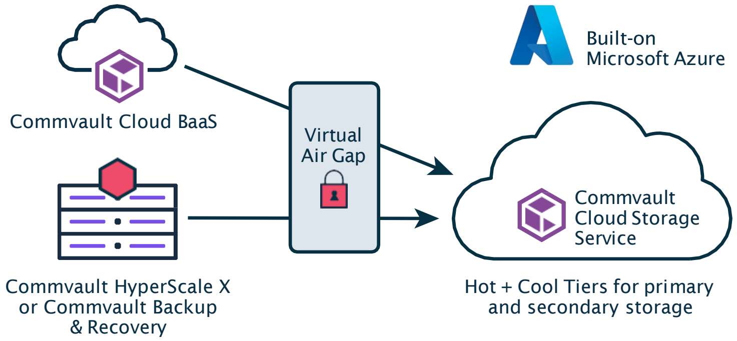
Fit for data retention policies of 30 days or longer. Send secondary copies of backups to secure cloud storage for an agile, modern alternative to tape.

Even though clouds are highly secure, organizations are responsible for data protection—and rapid recovery—of workloads they deploy in the cloud. Whether they choose to recover data to the cloud, from the cloud, between clouds, or within the cloud—Commvault provides this flexibility.

Air Gap Protect makes it simple to adopt cloud storage for backups. Protect against ransomware, optimize costs, reduce risk, and harness the scale of the cloud.

AIR GAPPED MANAGED CLOUD STORAGE TO GUARD AGAINST RANSOMWARE

- Protect with zero-trust access controls and multi-factor authentication
- Detect ransomware with anomaly monitoring and honey pots
- Recover with isolated, air-gapped, immutable copies


Commvault Cloud BaaS
Commvault HyperScale X or Commvault Backup & Recovery
Virtual Air Gap
Built-on Microsoft Azure
Commvault Cloud Storage Service
Hot + Cool Tiers for primary and secondary storage

CLOUD STORAGE FOR COMMVAULT SOFTWARE AND HYPERSCALE X

In addition to use with Air Gap Protect, lets customers seamlessly adopt cloud storage for Backup & Recovery and HyperScale X—with just a few clicks. Flexible primary and secondary backup options allow for any combination of Hot and Cool tiers to replace or augment on-premises backup storage.

[1] State of Ransomware report, Sophos, 2020

To learn more, visit **commvault.com**