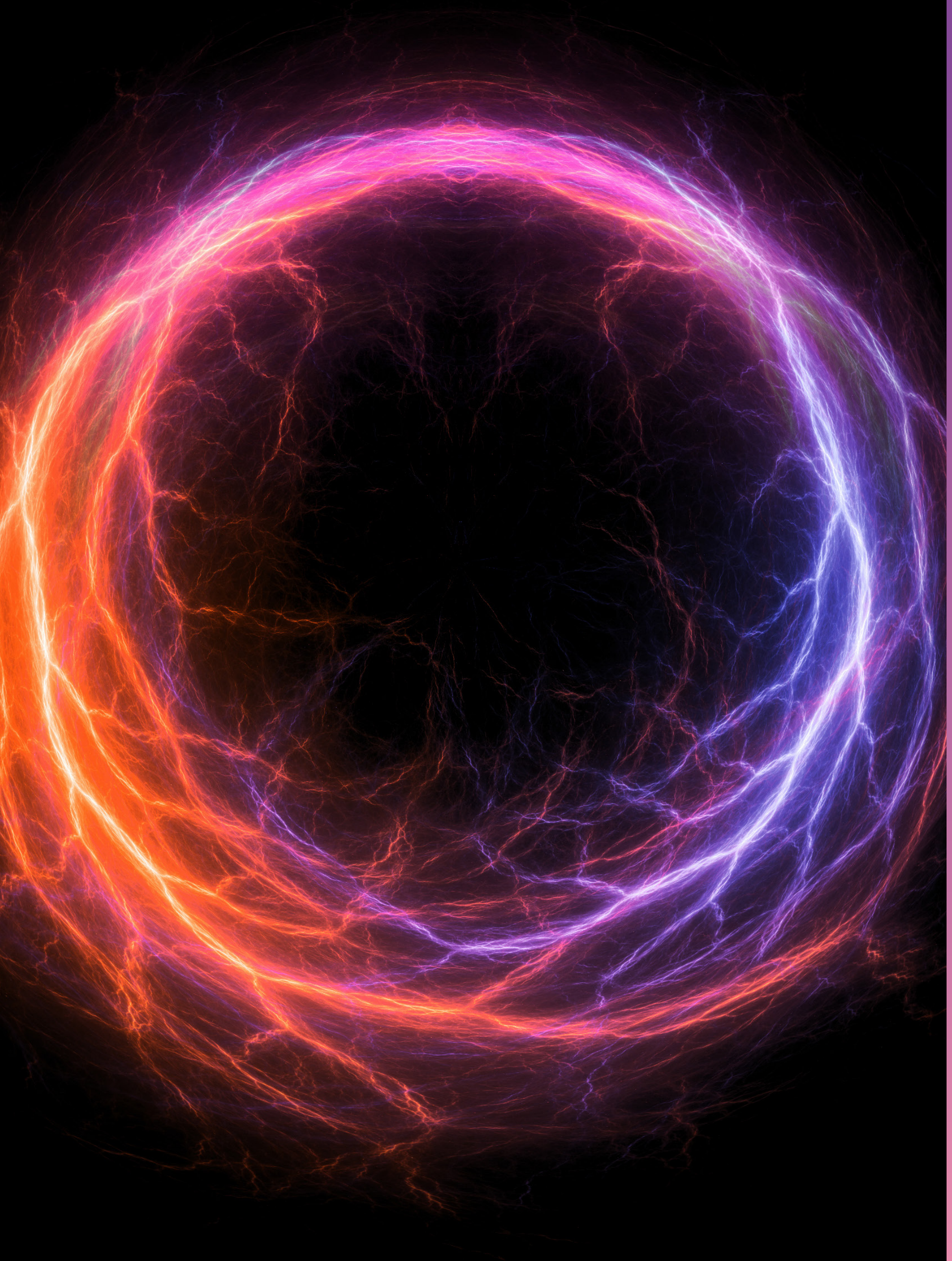


Commvault

BUYER'S GUIDE

Cyber Recovery for Any Cloud, Any Workload, Anywhere

Navigating the Challenges of Hybrid Cloud

Hybrid cloud combines at least one private cloud with one or more public cloud services. These "hybrid environments" can create siloed data and complexity as many companies look to enable the sharing and managing of data and applications between both.

On top of that, organizations are creating unfathomable amounts of data distributed across clouds, regions, applications, and partners. This brings it a complexity that poses a significant challenge to ensuring cyber recovery.

72% of companies are using a Hybrid IT approach today.[1]

98% of global tech executives report their business has been impacted by increasing complexity of data across the cloud.[2]

Add the new breed of AI-fueled attacks designed to exploit today's hybrid world, and you have a recipe for chaos, and ransomware thrives in chaos.

82% of breaches involve data stored in the cloud—public, private, or multiple environments.[3]

To avoid data loss and maintain a comprehensive level of cyber recovery across your entire environment, it's imperative to understand how and why to deploy hybrid environments and critical considerations for successfully protecting and securing those environments.

Companies who want to benefit from cloud-delivered solutions must demand the necessary breadth, flexibility, and security to meet their needs today and as their business evolves. If the past few years are any indication, the pace of change will only increase.

Safeguard all Your Clouds with Commvault® Cloud

Commvault offers a scalable and cost-effective approach to data security. The Commvault Cloud platform lives in a separate security domain, virtually air-gapped from any customer environment. All data is encrypted in flight and at rest, with multi-factor, zero-trust authentication, and zero-trust access protocols in place to ensure data immutability and tamper prevention.

Additionally, it is hardened with industry-leading standards built in (such as SOC 2: Type II and ISO 2700. In addition, Commvault's SaaS is FedRAMP High In Process final PMO review with the approved Department of Treasury ATO being signed 12 July 2023. Commvault continues its commitment to being the first and currently only FedRAMP High Backup and Recovery and Disaster Recovery SaaS solution in the market) for an enterprise-grade security model in the cloud — that limits internal lateral movement and external data loss and delivers rapid cyber recovery. This multi-faceted approach ensures that Commvault meets stringent confidentiality, integrity, availability standards, and applicable compliance certifications, so our partners and customers can confidently leverage our services.

Commvault Cloud Architecture

Commvault Cloud is architected for scale and performance with separate control and data planes, with the latter providing features and functionality such as backup job management, data restores, tenant security administration, and more.

The control plane 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 the features and functionality of cyber recovery operations. It ensures that backup data flows can be optimized to secure and manage production data, whether on-premises, public, or private.

Metallic AI for Advanced Protection

Metallic AI is the powerful engine behind Commvault Cloud, revolutionizing data protection intelligence. With its intelligent management and control capabilities, Metallic AI combines machine learning and automation to deliver one of the industry's most advanced data protection solutions.

One of the critical features of Commvault Cloud is Arlie, an AI co-pilot available 24/7 to assist users. Arlie can respond to inquiries in plain, simple language, providing personalized and actionable responses. Behind the scenes, Arlie interfaces with generative AI models that consolidate information and reports, enabling users to verify clean recovery points for critical systems or generate requested code within seconds.

With Metallic AI and Arlie, Commvault Cloud empowers users with advanced AI capabilities, enhancing their data protection experience and enabling them to navigate complex tasks and improve efficiency and cost-effectiveness.

Storage

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

Air Gap Protect: 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 hybrid-cloud workloads, Commvault offers storage target flexibility. Customers can leverage both cloud native storage and local backup copies together for stronger data resiliency and recoverability, including:

- Bring Your Own Cloud Storage: customer cloud, such as Azure, OCI, or AWS
- Commvault Cloud Air Gap Protect: cloud storage target that Commvault fully manages
- Bring Your Own On-Premises Storage: customer on-premises server via any disk or NAS device
- Commvault Cloud HyperScale™ X: Commvault appliance used for on-premises backup storage

Commvault Cloud Security Solutions

Backup & Recovery provides data availability and business continuity across your entire data estate—from a single unified platform. You can back up everything everywhere and recover clean data faster.

Cleanroom Recovery can help reduce the complexity and costs of managing on-premises cleanrooms, as it offers Recovery as a Service. Cleanroom Recovery provides clean data and recovery readiness through affordable, frequent testing and meets compliance requirements with auditable evidence for rapid and clean recovery when it matters most. This capability safeguards your data from infected hardware and offers AI-powered recovery scaling for fast and reliable massive data restoration.

Cloudburst Recovery is a game-changing capability for organizations, as it uses massively parallel recovery and infrastructure-as-code automation to restore multiple data sets simultaneously. It leverages the scalability and efficiency of the cloud, allowing businesses to replicate their data in near real-time and minimize data loss. In the event of a cyberattack or disaster, Cloudburst Recovery enables rapid failover to the cloud, allowing for seamless access to applications and data. Organizations can quickly restore operations to their primary infrastructure with automated failback and testing.

Air Gap Protect helps to ensure quick recoverability by incorporating air-gapped backup storage infrastructure. SaaS-delivered cyber recovery solutions offer a virtual airgap for backups and restore operations. Backup data copies are stored in isolated, immutable locations, preventing tampering, alteration, or deletion. These measures protect businesses from ransomware attacks that target on-premises tools and enable cyber recovery operations in a secure environment.

Threatwise changes the game in ransomware protection, combining sophisticated early warning with comprehensive data security. It enables businesses of every size to neutralize silent attacks before they cause harm, detecting and diverting the bad actors that evade conventional security tools and perimeter defenses. It's lightweight, fast, and easy—enabling you to dynamically deploy more deceptive assets sooner at a much lower cost. It is purpose-built to directly engage threats flagging recon, lateral movement, and unwanted privileged access that silently breach defenses.

Threatwise Security IQ provides customers with advanced tools and unprecedented visibility into backup environments. Seamlessly integrated across the entire Commvault portfolio, Security IQ offers a single place for IT admins to bolster security posture quickly, identify risks in real-time, and rapidly recover data.

Flexible Deployment Considerations

Stay SaaS Protected

SaaS-delivered cyber recovery has become one of the primary approaches for modern enterprises. The shared responsibility model for managing hybrid cloud and SaaS applications dictates that data backup and recovery is the customer's responsibility. SaaS applications must have dedicated solutions in place for the long term to protect data from the threat of ransomware attacks, internal malicious actors, accidental deletion, or corruption. And for companies who are running critical productivity and customer engagement applications in the cloud, pairing SaaS-delivered data backup and recovery capabilities is a seamless option. Look for a comprehensive solution like Commvault to **ensure broad coverage of applications and workloads**.

Think Hybrid First

As companies take a hybrid approach to technology and infrastructure, look for solutions that allow **seamless management of both cloud and on-premises data** without degrading performance. You should be free to back up and restore broad data types to the appropriate target – to cloud or on-premises storage – and send secondary backup copies to cloud platforms for long-term data retention and air-gapped ransomware protection. SaaS-delivered cyber recovery solutions that don't provide on-premises data management options can have customers waiting up to 10 days for a restore.

On-premises and cloud data shouldn't require mutually exclusive cyber recovery solutions. Thanks to Commvault offering storage flexibility, companies can seamlessly back up to cloud or on-premises with a single pane of glass management. Customers can control and protect their on-premises data through a simple SaaS-delivered solution without data ever having to leave on-premises.

Start Migration Planning Today

As your data migrations and backup needs rise, your cyber recovery solution should **operate seamlessly across cloud instances and on-premises infrastructure** to handle your enterprise-critical workloads. These workloads can be many and varied.

By anticipating where your data will be processed, you can ensure the cyber recovery solutions are already in place to keep data secure, whether at rest or in flight. In addition, putting your data security in the cloud with a SaaS-delivered solution can be a practical early step to a planned migration, setting the table for your cloud transformation.

Stay Secure End-to-end

As you transition from traditional application platforms to containerized approaches such as Kubernetes, your cyber recovery and data security must remain a top priority. With stateful enterprise applications moving into containers, the security needs have changed, shifting to backing up the Kubernetes application and its associated data, images, and cluster control plane.

While high availability can bring the containers back during disaster scenarios, the application cannot recover and be fully operational if the underlying data is corrupted or lost. Securing your Kubernetes data ensures **full recovery, rapidly restoring applications with minimal disruption** to business. Commvault also offers SaaS-delivered cyber recovery for Kubernetes, supporting all CNCF-certified distributions.

Engage Unified Management

Avoid using many tools and platforms that create overly complex cyber recovery interfaces. A solution that operates through a single-pane-of-glass dashboard protects all your workloads while your data security remains as efficient and comprehensive as possible.

Commvault provides this critical visibility and simplified workload with the ability to **manage any data anywhere from one console**. You can select SaaS and self-managed solutions if your strategy requires and still enjoy industry-leading technology. With HyperScale X, companies can store backups locally to recover extensive on-premises data sets faster. You get everything you need to modernize your cloud journey from a single vendor.

Total Cost of Ownership

Deploying outdated strategies for data protection is an expensive mistake—and it's not just about minimizing downtime for business continuity. Commvault's unique platform capabilities are designed to help enterprises reduce costs by simplifying management, optimizing cloud strategies, reducing security risks, and improving business continuity.

Single platform. Avoiding the management overhead of procuring and running multiple-point solutions while leveraging a mix of SaaS and software wisely can save on infrastructure costs.

Optimized cloud spend. Through ephemeral infrastructure and power management, deduplication and compression, and scalability on-demand, customers won't end up paying more than they need to leverage the best of the cloud - while enjoying the broadest cloud-native coverage and deep integration with cloud providers.

Early warning. Commvault's unique early warning capabilities enable customers to respond to potential threats faster and thus mitigate the incident's potential impact and "blast radius." Early warning + faster response = lower costs associated with the recovery efforts.

Automated BCDR. Commvault disaster recovery capabilities reduce the need for having dedicated infrastructure on standby "just in case" it's needed. Commvault can instantiate the systems needed for recovery only when needed for DR testing or in the event of an actual recovery incident.

- Coupled with cross-cloud/platform capabilities, Commvault can automate DR to the cloud, further driving efficiencies by bursting into the cloud for recovery.
- Resources and infrastructure used to drive fast restores in the cloud are quickly scaled up and then back down when the job is done, saving costs otherwise needed for expensive compute/storage resources.

Cost-efficient data security. Reduce the operational costs to secure your business by minimizing threat opportunities (damage protection), securing critical data (immutability), and recovering clean "last known good" data after attacks (threat scan).

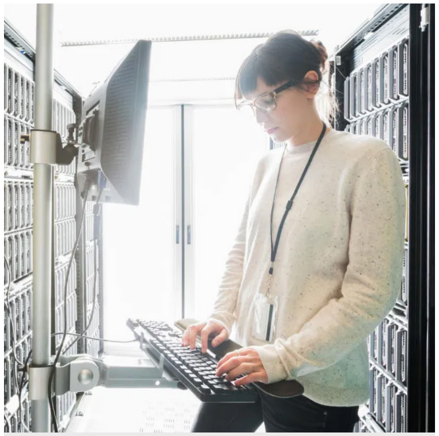
Avoid downtime from critical events. Maintain highly resilient operations, avoid costly downtime of mission-critical applications, and reduce recovery time from security incidents to get back to business faster.

Choose the Best Cyber Resilient Protection Package for Your Hybrid Cloud

Commvault offers a range of packages designed to meet organizations' diverse needs regarding data protection and management. Our packages provide flexibility, breadth of coverage, ultimate security, and cost savings.

Operational Recovery package offers essential data security, recovery, and AI-driven automation.

Autonomous Recovery package adds automated validation, live data replication, and rapid recovery capabilities.



Cyber Recovery package includes advanced features like sensitive data discovery, automated risk remediation, and threat detection.

Platinum Resilience package offers the highest level of protection, combining all capabilities with Commvault's Ransomware Recovery Protection Plan.

To learn more or schedule a demo, visit: **commvault.com/packaging**

Take the next step

Simplify and save with Commvault Cloud-deliver hybrid cloud cyber recovery. Experience cost and complexity reduction with hassle-free deployment, hands-off maintenance, and no significant upfront investments required. It's cyber recovery for wherever your data lives.

VM & Kubernetes
Microsoft Hyper-V, VMware, Azure VM, Kubernetes, Microsoft Azure, AWS, AVS, VMware Cloud.

Database
For Microsoft SQL, Azure PaaS, Oracle, Amazon AWS, SAP HANA.

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

Cloud Storage
For Air-gapped cloud storage.

File & Object Archive
For compliance ready archiving.

Threatwise™
For early warning into threats.

Microsoft 365
For Exchange, Teams, SharePoint, OneDrive, Project, and more.

Microsoft Dynamics 365
For CE applications and Power Platform.

Salesforce
For Salesforce and Cloud data.

Endpoint
For laptops and desktops.

Active Directory
For Azure AD and Microsoft AD.

Security IQ
For actionable threat insights.

Commvault Cloud for Government
FedRAMP high data management (In Process — PMO Review), hosted on Azure Government Cloud).

Get more value from your data—no matter where it lives—and gain true cyber recovery without compromising your business.

Visit **commvault.com** and **contact us** for more information.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®

[1] State of the Cloud Report | Flexera | 2023
[2] Cloud Complexity Report | NetApp | 2023
[3] Cost of a Data Breach Report | IBM | 2023