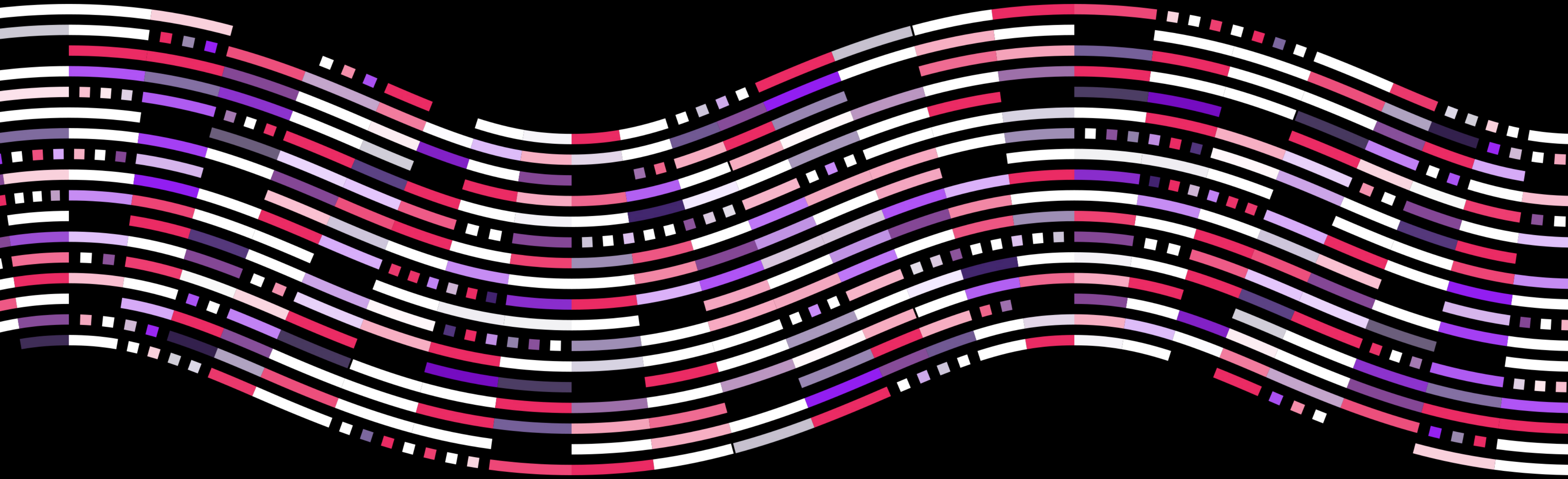
Commvault®

BUYER'S GUIDE

Cyber Recovery for Your SaaS App Data

Protecting SaaS app data is your responsibility: Don't do it alone. Commvault delivers trusted data security protection for your SaaS app data — and beyond.

Safeguarding your SaaS app data is crucial, and you don't have to do it alone. Commvault® Cloud, powered by Metallic® AI, offers trusted data security protection for your SaaS app data and more. It is purpose-built to enable cyber recovery in the hybrid world, providing the highest security, intelligence, and recovery speed. With Commvault Cloud, secure your data, predict risks, minimize damage, and quickly recover from any threat.



Metallic AI for Advanced SaaS 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 best advanced data protection solutions in the industry. One of the key 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.

Commvault Cloud Architecture Advantage

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 wherever it might reside — on-premises, public cloud, or private cloud. Since your data is not tied to the control plane, it can be easily moved or migrated to different environments or storage locations without disrupting operations or requiring complex configurations.

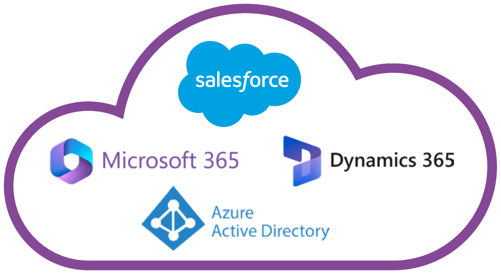
Complete Cyber Protection for SaaS Apps with Commvault

In today's threat landscape, ransomware significantly challenges business continuity and resilience. It is more pervasive and autonomous than ever before. Organizations must be resilient to survive and compete, as it's not a matter of "if" you will be breached but "when." Building cyber resiliency across your SaaS apps in the face of an attack has become necessary.

Regardless of which SaaS application you protect, cloud service providers offer some native controls for temporary data replication, but they may not provide long-term retention and resiliency. Data experts emphasize the importance of a proactive data security strategy, and leading providers like Microsoft[1], and Salesforce[2], recommend implementing third-party backup solutions. Commvault's best practices focus on safeguarding data within SaaS applications by:

- Keeping backup copy data separate from the source data, ensuring air-gapped and immutable copies for enhanced security.
- Providing extended retention of active and deleted data, ensuring data is protected for as long as required.
- Adhering to pre-established SLAs, contracts, and relevant legislation to ensure compliance and data governance.
- Enabling granular backups, flexible restore options, and rapid recovery capabilities, ensuring quick and efficient data restoration when needed.
- Offering advanced security insights and threat monitoring, providing valuable insights into potential risks and vulnerabilities.

Commvault Cloud, powered by Metallic AI



Commvault Cloud protects leading **SaaS applications**, including Microsoft 365, Salesforce, Dynamics 365, and Azure Active Directory. Across these products, we provide highly performant security and recovery capabilities with the simplicity of SaaS. Know that your critical information is backed up, recoverable, and protected against potential threats.

SaaS Shared Responsibility Model (SRM)

The SaaS Shared Responsibility Model (SRM) is crucial in cloud security. It divides responsibilities between cloud providers and customers for securing data and applications. Providers secure the infrastructure, while customers safeguard their data. This model ensures clarity and accountability, enabling companies to benefit from cloud scalability and flexibility with confidence in their provider's secure infrastructure. It's important to note that cloud service providers follow this **shared responsibility model**, with providers maintaining solution uptime and customers protecting their data. Cloud providers have different approaches to securing their customers' data, meaning their responsibilities can vary significantly. Even though cloud providers are responsible for offering secure environments and tools, there is no guarantee that customer data will remain private or secure if companies fail to implement best practices such as access control, encryption, and other necessary measures. Therefore, businesses must clearly understand each provider's responsibilities regarding data protection to select the most suitable partner for their specific needs. Commvault's true cloud security platform makes keeping your cloud data safe easy.

Navigating the Challenges of Hybrid Cloud

Hybrid cloud combines private and public cloud services, creating a need for effective data sharing and management. This can be achieved through software or SaaS solutions. Approximately 72% of companies are adopting a hybrid IT approach[3], leveraging the benefits of both public and private clouds. However, protecting and securing data in hybrid environments is crucial as threats evolve with cloud modernization. Ensuring data integrity requires a different approach in the cloud, isolating production data workloads and reliable backup and recovery systems.

Additionally, hardware failure and other potential scenarios must be considered for on-premises options. A comprehensive security strategy is essential as hybrid cloud becomes a long-term reality for many companies. Commvault offers IT directors the benefit of dynamically flexing and expanding their IT infrastructure to meet changing needs, overcoming the hybrid complexity and security risks associated with cloud migration efforts.

Cyber Recovery in Kubernetes Environments

Flexibility, scalability, and comprehensive protection are crucial for cyber recovery in Kubernetes-based containers. However, many solutions rely on multiple tools or third-party products for backup, and some mistakenly assume container-based apps can be backed up like individual apps.

Commvault Cloud Backup & Recovery for VM & Kubernetes simplifies the process. It offers a cloud-native approach, providing backup and recovery for VMs and containers, including Kubernetes apps and persistent volumes for all CNCF-certified distributions. It seamlessly integrates with developer workflows, automatically discovering and protecting applications based on namespaces and labels.

With granular options, you can recover YAML manifests or entire volumes as needed. Commvault streamlines the backup and recovery process, ensuring your data remains secure and recoverable in any hybrid cloud environment.

Secure Your Data Beyond the Reach of Cybercriminals

Cyber recovery acts as a last line of defense, and the effective way to limit damage from ransomware attacks is to keep data and infrastructure beyond the reach of cybercriminals. 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.

Guaranteed Clean Data and Rapid Recovery

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

Rapid Data Recovery at Scale

Commvault Cloud 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 achieve minimal data loss. In the event of a cyberattack or disaster, **Cloudburst Recovery** enables rapid failover to the cloud, ensuring seamless access to applications and data. Organizations can easily restore operations to their primary infrastructure with automated failback and testing.

Protect Your Business from Emerging Ransomware Threats

Commvault's ransomware protection, powered by Metallic AI, offers advanced defense against the growing threat of ransomware attacks. With AI technology, Metallic AI actively detects and combats ransomware AI, providing a powerful defense mechanism for your data. This innovative solution identifies and tags sensitive data using static or dynamic patterns, ensuring comprehensive protection against diverse ransomware variants. By leveraging the power of AI, Commvault enables businesses to proactively safeguard their endpoints, SaaS applications, and hybrid cloud environments.

Stay One Step Ahead of Cyber Threats

Proactively respond to cyber threats and secure your data before it is compromised. By utilizing cyber deception, **Threatwise** disguises itself as legitimate business resources, engaging attackers as soon as an attack begins. This provides early warning signals and exposes unknown and zero-day attacks, empowering businesses to respond and minimize threats. With patented deception technology, Threatwise offers comprehensive data security and changes the game in ransomware protection. It is lightweight, fast, and easy to deploy, allowing businesses to dynamically deploy deceptive assets at a lower cost. By alerting organizations to attacks in progress, Threatwise offers multi-layered protection for your data estates.

Safeguarding Hybrid and Remote Workforces

Commvault Cloud Endpoint Backup and Recovery is designed to protect and safeguard the data of hybrid and remote workforces. It ensures that valuable endpoint data is secure and recoverable in the face of user deletion, corruption, or ransomware attacks. With Commvault, organizations can achieve cost-effective data protection without complexity, extended retention, and eDiscovery search capabilities to meet SLA compliance. The capability reduces risk by providing secure endpoint data protection, enabling fast recovery options to minimize downtime. It also eases the burden on IT teams with user self-service options and centralized access to laptop and desktop data. Endpoint Backup and Recovery offers robust data security and resilience for today's distributed workforce.

Streamline Active Directory Cyber Recovery

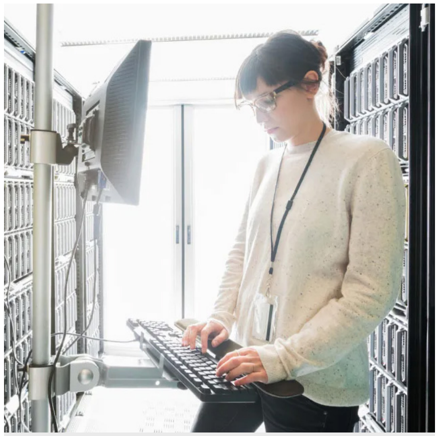
Commvault Cloud Active Directory Backup provides comprehensive protection for critical Active Directory data, ensuring its resilience and recoverability. With Commvault, organizations can safeguard their Microsoft AD and Azure AD data from threats, all from a single solution. The platform offers purpose-built tools to prevent, detect, and recover from cyberattacks and robust control to undo damaging changes. It enables fast, granular, and accurate recovery of missing, damaged, or misconfigured items. With Commvault's multi-layered defense mechanisms, deep security insights, and hassle-free administration, organizations can confidently protect their Active Directory environment and maintain business continuity.

Choose the Perfect Cyber Resilient Protection Package

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**

Commvault®

Take the next step

Simplify and save with Commvault Cloud-delivered SaaS cyber protection. Experience cost and complexity reduction with hassle-free deployment, hands-off maintenance, and no big upfront investments required. 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 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] Microsoft Services Agreement, Service Availability, microsoft.com/en-us/servicesagreement

[2] Salesforce, Best practices to backup Salesforce data, What about restoring my data?, October 2023, help.salesforce.com/s/articleView?id=000386692&language=en_US&type=1

[3] State of the Cloud Report, Flexera, 2023