Commvault Cloud
Powered by Metallic AI

Architecture matters

Only **Commvault® Cloud** delivers true, cloud cyber resilience.

CONSIDERATION 01

Data Plane Separation

OTHER PROVIDERS

Control planes are not separate

The lack of separation between control and data planes in competing solutions increases the complexity and cost of securing your data across different workloads and elevates the overall risk. A breach in one area can easily compromise another, leaving sensitive recovery processes vulnerable to unauthorized access or manipulation. Moreover, it restricts your ability to thoroughly test and choose recovery options without the risk of contaminating your data, essentially limiting your resilience capabilities. **Without dedicated control and data planes, you're missing out on crucial security controls, exposing your system to more significant cyber threats due to inadequate risk remediation strategies.**

COMMVAULT

Resilient architecture

Keeping backup copies separate from source environments protects your system against potential compromise and helps prevent recovery efforts from being impacted by an attack. Commvault Cloud is the only platform that separates **The Control Plane** from **The Data Plane** from the **Storage** location. This design incorporates strong controls to defend against various threats, including accidental deletions or malicious attacks, keeping your backup operations secure and highly recoverable. Additionally, by safeguarding data at the storage level in a virtually air-gapped location, Commvault enhances your security posture. **This setup allows for the isolation of backup copies, boosting both security and the ability to test recoverability without the risk of contaminating your data.**

CONSIDERATION 02

Comprehensive Security

OTHER PROVIDERS

Requires additional products for complete coverage

Alternative solutions often require additional products to fill gaps in protection capabilities, leading to more data silos, increased operational overheads, and a higher total cost of ownership (TCO). **Limited protection capabilities create inefficiencies, which lead to longer go-to-market cycles and the need for add-on solutions** to achieve comprehensive coverage, which increases costs and complicates the cyber resilience process.

COMMVAULT

Secures more workloads than any other provider

Commvault secures all types of workloads in various environments, providing centralized data security, even across multiple distributed control planes. It allows you to quickly adapt to changing requirements, reduce backup costs, improve operational efficiency, and enhance cyber resilience. It also facilitates rapid integration of acquired data environments, supports shifting workloads to cloud-based infrastructure, and helps shift expenses from Capex to Opex, making costs more predictable.

CONSIDERATION 03

Any-to-Any Portability

OTHER PROVIDERS

Tied to storage architecture

Using solutions that lack any-to-any portability and are tied to storage-centric architectures can be costly. Cross-platform support is limited, and data recovery becomes complicated across different environments. **The absence of any-to-any portability can make migration difficult and expensive, including maintaining hardware, software, and management tools, leading to expensive legacy methods and increased risk.** Organizations may also face higher costs from managing multiple products, purchasing and maintaining physical or virtual appliances, and the costly and time-consuming process of testing and deploying these solutions.

COMMVAULT

Securely and reliably recover from anywhere to anywhere

Commvault's any-to-any portability provides the ability to recover data and applications from any location and restore them to any system. This enables seamless recovery processes that are not limited by vendor lock-in or the need to use a specific cloud environment. Organizations can seamlessly move data across different platforms, allowing them to leverage each cloud environment's best features. **This flexibility allows businesses to adapt to changing requirements, optimize performance, and avoid disruptions.**

CONSIDERATION 04

Risk Remediation

OTHER PROVIDERS

No integrated data access governance

Using solutions without integrated Data Access Governance (DAG) can result in a lack of understanding and control as organizations struggle to identify sensitive data, understand where it resides, and ensure compliance with regulations. Relying on third-party tools without integrated DAG fails to offer a unified way to manage access to data across environments, leading to increased complexity, higher costs, weakened incident response, and a significant burden on IT and security teams. Additionally, **relying on backup environments alone can leave primary data vulnerable, create a false sense of security, and lead to compliance issues.**

COMMVAULT

Automated risk scanning and remediation

Commvault's automated risk scanning and remediation proactively manages risks across both live and backup data to enhance data security and integrity. This system identifies sensitive information, scans for potential threats, makes recommendations to protect sensitive data and can take necessary remediation steps to fix vulnerabilities and help maintain compliance. **Unlike alternatives, Commvault allows for direct actions on detected risks and performs continuous compliance scans.**

CONSIDERATION 05

Early Warning

OTHER PROVIDERS

Reactive detection, 24 hours too late

The absence of early warning systems can delay receiving alerts about emerging risks, leaving critical systems exposed to threats for extended periods. This increases the risk of operational disruptions and downtime, as ransomware and other malware can quickly spread and infect these systems. **Without real-time insights, organizations are forced into a reactive posture, constantly trying to catch up with threats instead of proactively preventing them.**

COMMVAULT

Identify threats, minimize impact, and accelerate recovery

Commvault's early warning capabilities offer immediate, proactive, actionable alerts, allowing organizations to quickly address emerging risks across production and backup environments before they escalate. Our unique capabilities can flag suspicious activities like reconnaissance, lateral movement, and unwanted privileged access that bypass conventional technology. **This approach, combined with intelligent cyber deception recommendations, helps divert zero-day and advanced threats away from critical data assets, reducing the impact of cyberattacks and enabling rapid, reliable, and clean recovery.**

CONSIDERATION 06

Clean Room Recovery

OTHER PROVIDERS

Cost-prohibitive, complex, and risky on your own

Building out physical or virtual recovery environments with all the required infrastructure to test critical application recovery is untenable for most. Alternative solutions' capabilities are limited to disaster recovery, rely on third-party applications, and are constrained by limited workloads and recovery options. They also do not provide end-to-end orchestration of the on-demand Clean Room recovery, meaning that **customers must rely on manual, complex, and expensive testing and recovery processes.**

COMMVAULT

Recover without the cost, complexity, and risk

Commvault® Cloud Cleanroom™ Recovery offers a comprehensive testing and failover solution that helps organizations effectively mitigate cyber risks. It provides a safe and isolated environment for testing cyber recovery plans, conducting forensic analysis, and business continuity in case of a breach. This solution provides secure and quick application recovery in a new, uncontaminated, on-demand cloud environment, providing reliable cyber recovery. The solution also reduces the complexity and costs of managing on-premises cleanrooms, offering uninterrupted business continuity.

Read our eBook to understand the need for solutions that are optimized to work with your existing IT architecture, designed to handle increasing data loads, and minimize the risk of data breaches and cyberattacks.

Commvault

commvault.com | 888.746.3849