COMMVAULT

DATASHEET

Greater data protection: Immutable backups to the cloud with Commvault

Cyber threats are rapidly increasing in sophistication and persistence. As threats increase, security expenditures are expected to reach $133.8 billion worldwide annually by 2022 according to IDC.[1] Despite the increase in awareness and spending, every 14 seconds an organization will still fall victim to ransomware according to the Official Annual Cybercrime Report.[2] These statistics reinforce the importance of recovery readiness. With cloud storage a popular choice for offsite copies, the question of data security becomes an important consideration. To address this, many data protection solutions offer robust WORM and immutability options for stronger cloud protection and security.

Combining Commvault Complete™ Backup & Recovery industry leading security controls, with cloud-based WORM and immutable storage integration, organizations can be assured that their important data cannot be deleted, modified, or accessed by malicious cyber and internal threats maintaining compliance with governing regulations.

AAA security framework controls

Commvault protects access, privacy, and control of backup data residing across copies, including cloud. Commvault immutable backup data utilizes a rich feature set and incorporates the AAA security framework principles:

AAA Security framework for controlling access

Authentication	Authorization	Accounting
Proving and granting access	Control what level of access is required	Tracking and auditing access and capabilities

Authentication controls provide and grant access to backup data. This can be thought of as the "gate-keeper". Features include certificate authentication, two-factor authentication (2FA), and integration with multiple third-party identity providers using secure protocols such as LDAPS, SAML, and OpenID.

Authorization controls determine what level of access is allowed on the Commvault CommCell. Once authentication is allowed, Commvault has various controls such as role-based security, multi-tenancy, privacy locks, and multi-level authentication. Each of these features work in tandem to protect data from being accessed, retrieved, and deleted. Adding these gates create software isolation, where even administrators are blocked from deleting and accessing backup data as well as reversing security controls. Similarly, if a malicious actor steals access into the CommCell, the backup data is secured from malicious activity within the Commvault platform.

1 Worldwide Spending on Security Solutions Forecast To Reach $103.1 Billion in 2019, According To a New IDC Spending Guide, March 20, 2019
2 CPO Magazine, 11 Eye Opening Cyber Security Statistics for 2019, By Matt Powell, June 25, 2019

Lastly, Commvault enforces **accountability** by auditing events, and actions within the CommCell and providing a rich customizable interface to view this information. Hundreds of reports are readily available in the Commvault software store providing deep information on the operations, events and action of the CommCell. Information within reports and dashboards are only visible to users given access. This allows owners to view the same audit reports and dashboards as Administrators, without seeing resources they do not have permission to see. The ability to customize and create your own reports using Commvault data sources, and external APIs, is useful for expanding its capabilities and power. For continuous monitoring, Commvault integrates with third-party tools such as Syslog, Splunk, and SNMP systems. This further expands the accounting and audit capabilities within Commvault and provides flexibility to integrate with whatever systems are already in place within the organization.

Immutable backups in cloud

Commvault Complete Backup & Recovery provides on-premises backup immutability by combining the AAA framework security controls, hardening, data encryption, and native ransomware protection locks. However, when designing a solution to protect against ransomware and cyber threats, offsite copies of data is imperative. Cloud storage is an economical solution because resources are readily available, elastic, and multi-tiered.

When using cloud storage (such as Amazon Web Services (AWS) or Microsoft Azure); immutability options are enabled at the storage level with the cloud vendor. The cloud destination is configured as a library within Commvault for secondary and/or tertiary copies. When cloud immutability is enabled, the entire storage container is locked, and the contents within the container cannot be modified, or deleted for the specified immutability time frame.

Using Commvault with immutable cloud storage, has key advantages over other backup products:

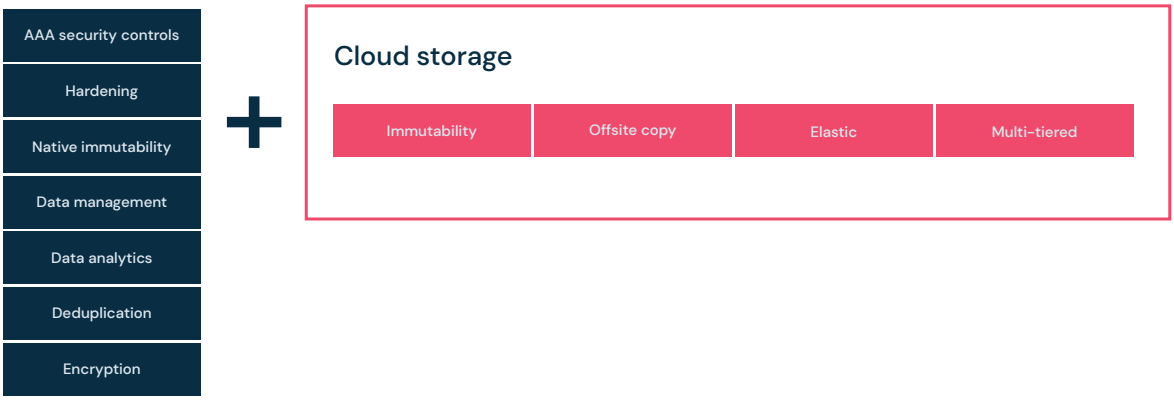
Commvault security controls and hardening

If a bad actor were to obtain your cloud credentials, it would be impossible to delete, encrypt, manipulate or reverse the immutability options applied to the backup data. If a bad actor were to gain access to Commvault, Commvault's AAA security controls and hardening capabilities act as a first line of defense, blocking the bad actor from gaining access and deleting data, while the immutable lock on the storage provides another layer of backup data protection.

Deduplication

When organizations are faced with sending multi-petabytes worth of data to the cloud, cost and bandwidth dominate the conversation. Commvault software deduplication begins where the source data resides. Only changed blocks are sent to cloud, drastically reducing the amount of bandwidth required for copy operations. This also allows more backup cycles (Full, and Incremental backups) to be protected in the cloud, while reducing the storage footprint. Ultimately, Commvault's deduplication allows backup copies to quickly get to the cloud, reduce recovery point objectives, increase recover readiness, and reduce storage footprint costs.

Commvault platform



Encryption and key management

Cloud storage encryption is great for protecting data at rest from being useful if stolen, however, this does not handle source side encryption needs. Commvault's FIPS 140-2 certified encryption module handles encryption at the source, prior to sending data to the cloud. This ensures every block of data transmitted to the cloud is encrypted and secured. For deeper levels of security, encryption keys can be offloaded to external key management servers, including AWS, Azure, or any KMIP compliant system.

Data management and analytics

Commvault manages retention and backup policies, while cloud manages the immutable locks configured at the storage. Using a multi-tiered approach to storing data in the cloud, organizations can take advantage of cold storage options to save cost, while having the index readily available on-premises or in warmer cloud storage tiers for analytic purposes. Commvault allows immutable backups that exist in cold storage to be analyzed in a cost-effective way and can be leveraged for other business purposes. Without the ability to use a tiered storage approach, backups that exist in cold storage would otherwise be very expensive to index and analyze due to egress/access charges from the cloud provider.

Regulatory compliance

Using Cloud WORM and immutable storage options with Commvault helps organizations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations related to the recording, storage, and retention requirements for electronic records. AWS[3] and Azure[4] are both compliant storage options supported by Commvault, designed to meet securities industry requirements for preserving records in a non-rewriteable and non-erasable format using their respective storage locking technologies.

Conclusion

While cyber threats are increasing, your organization can keep pace and mitigate risk. With highly available cloud storage and greater security protection, it is simple to start creating secondary and tertiary data copies in the cloud. Without any extra costs, Commvault Complete Backup & Recovery will manage, analyze, and secure your backup data efficiently, while cloud immutability further locks data from all the various cyber threats rampant today, and in the future. With Commvualt you have the security and protection to store and manage your data on-premises and in the cloud; you are recovery ready.

3 Amazon Glacier with Vault Lock: SEC 17a-4(f) and CFTC 1.31(b)-(c) Compliance Assessment
4 Microsoft Azure Storage: SEC 17a-4(f) and CFTC 1.31(c)-(d) Compliance Assessment

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