COMMVAULT

SOLUTION BRIEF

Protect against ransomware with Commvault and AWS

Introduction

By 2025, ransomware attacks are predicted to cost businesses an estimated $10.5T annually in lost revenue, brand impact, and missed opportunities[1] Numbers like that might seem unfathomable, but the seemingly endless parade of headlines back them up. Browsing the news on any given day you're likely to see stories about new attacks that threaten organizations with massive bounties or substantial data loss and disruption.

In a 2021 Proofpoint survey, 65% of CISOs feel at risk of suffering a cyberattack[2] Organizations are looking for ways to protect their data and alleviate these fears so those CISOs can sleep at night.

Commvault and Amazon Web Services (AWS) combine their industry-leading products to provide a highly secure way to manage, protect, and store data and keep it protected from threats like ransomware.

A multi-layered approach to keep your data protected

Just as quickly as new methods of defense are introduced, ransomware attacks evolve to evade them. To combat these continuously evolving threats, your organization needs a data protection strategy that provides multiple layers of safeguarding. Commvault recommends a framework that meets five different key criteria, offering multiple different protection mechanisms within each category.

Those categories are **Identify, Protect, Monitor, Respond** and **Recover.**

1 Identify: Assess and mitigate risks

Commvault is built on a secure AAA (Authentication, Authorization, and Accounting) Framework that adheres to zero-trust principles. This enables segmentation/isolation of data, role-based access control with least-required privilege, and full granular logging and auditing capability. All these controls work via all access types: UI, command line, or API.

AAA Security framework for controlling access

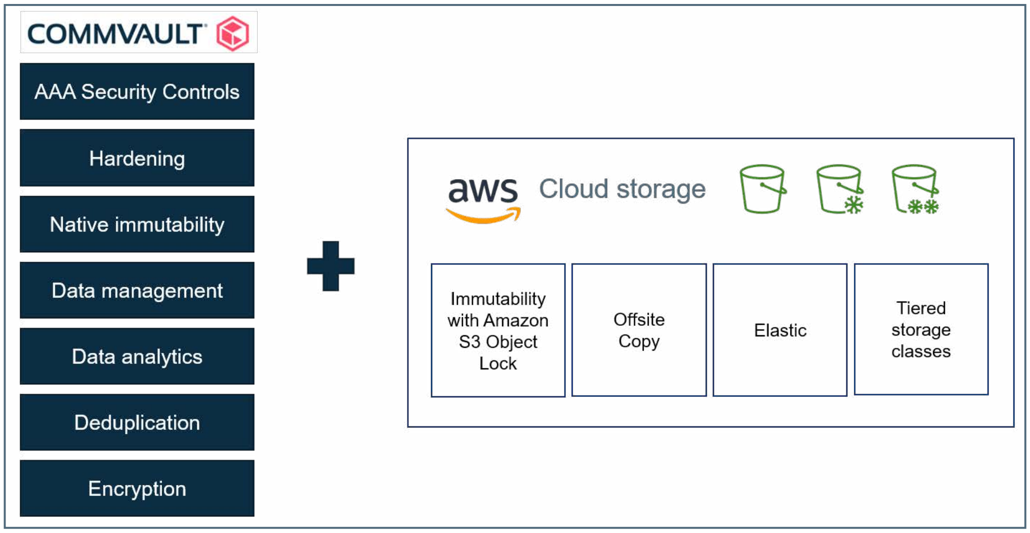
Authentication	Authorization	Accounting
Proving and granting access	Control what level of access is required	Tracking and auditing access and capabilities

For workloads running on AWS. Commvault integrates with AWS Identity and Access Management (IAM) for granular, role-based access, as well as with AWS Security Token Service (STS) AssumeRole for temporary, "just in time" access to resources. These integrations provide a more secure way to access your AWS resources and help prevent dreaded credential leaks leading to unauthorized access.

[1] 2019 Official Annual Cybercrime Report, sponsored by Herjavec Group, Steve Morgan, Editor-in-Chief
[2] Proofpoint, Voice of the CISO 2021 Report, May 12, 2021

2 Protect: Lock and harden data from changes

At the core, Commvault provides end-to-end FIPS-certified encryption to ensure that all data is secure – at the source, in flight, and at rest.



In addition to encryption, your organization should consider immutable backup copies to ensure recoverability in the event of an attack. With Amazon S3 Object Lock and Amazon S3 Glacier Vault Lock, Commvault can write backup data directly to AWS for low-cost, resilient offsite storage with immutability configured to meet your retention SLAs. Once the backups are stored in these "locked" Amazon S3 buckets, any attempts to delete or modify the data are unsuccessful, thus ensuring it can be used for recovery if other data sources become compromised.

3 Monitor: Find anomalous threats

Commvault uses machine learning, artificial intelligence, and honeypots to monitor and detect suspicious or unusual activity for greater insights and faster time to recovery. This built-in intelligence allows your protection to evolve as the attackers do.

4 Respond: Analyze data and perform orchestrated actions

Once threats have been identified, Commvault allows you to respond with intelligent automation and APIs, workflows, and integrations that allow your data to be restored and your business back online within moments.

To help mitigate the threat, Commvault also allows surgical deletion of suspicious or unnecessary files, as well as the ability to do an isolated recovery so you can take all steps to ensure that your data is not reinfected.

5 Recover: Restore clean data quickly

Commvault speeds recovery with flexible restore options for cloud, virtual, and on-premises environments. For instances running on Amazon EC2, Commvault can scale additional EC2 infrastructure to accelerate recovery with parallel data streams.

Summary

With ransomware attacks at an all time high, your organization needs a robust data management solution with multiple layers of protection to ensure your data is safe. Commvault delivers a secure platform with end-to-end encryption, A.I. and M.L. based anomaly detection, and native integration with AWS services that allow you to leverage Amazon S3 and Amazon S3 Glacier as resilient, highly scalable storage with built-in immutability with S3 Object Lock and Glacier Vault Lock. Together, Commvault and AWS can keep your data protected, secure, and recoverable so when the inevitable attacks occur, you'll be ready.

To learn more, visit **commvault.com/aws >**

COMMVAULT® Be ready™

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