COMMVAULT

SOLUTION BRIEF

Commvault's immutable infrastructure architecture

Securing your data protection environment

Introduction

The best indicator that you have a reliable backup solution is your ability to recover data quickly. This comes in part from proper planning and architecting your backup and recovery solution. However, this can be a difficult challenge when your data is up against so much opposition. In the past, hardware failures, natural disasters, and human error were likely "top of mind" outage threats. Today, ransomware and insider threats have taken over as top concerns. It's apparent that planning and architecture design is not enough; today's backup and recovery solution must be immutable, so you have peace of mind that your data is safe.

The term immutable means "unchangeable or changeless." When applying this to backup data, whatever data you backup according to your set policies will be the available data to restore; unchanged and unmodified. Immutability protects within, as well as outside of the backup solution.

With every environment having its own mix of infrastructure, securing backup data against random unauthorized changes can seem challenging. Therefore, Commvault has taken an agnostic approach to immutability. With Commvault, you do not need special hardware or cloud storage accounts to lock backup data against ransomware threats. If you happen to have Write-Once, Read Many (WORM), object lock, or snapshot supported hardware (which Commvault fully supports), you can still use Commvault's built-in locking capabilities to complement and layer on top of existing security controls. Having the ability to layer security controls across different infrastructure types is what sets Commvault's immutable solution ahead of its competitors.

Commvault's immutable infrastructure architecture

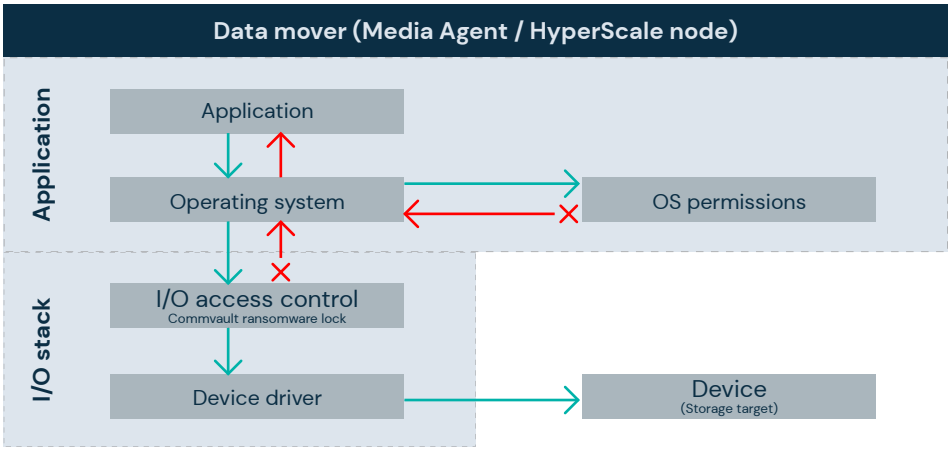
Commvault employs a multi-layered approach to protect against various threat vectors and ensure data is safe. Also, Commvault includes storage locking and controls up and down the backup and recovery stack to provide comprehensive protection. Commvault's machine learning platform extends the immutable protection capabilities by providing a proactive platform for detecting and responding to threats accordingly. At a high level, the immutable architecture includes these five layers:

Commvault's immutable architecture

Storage I/O controls (Ransomware lock)	Lock storage by monitoring I/O requests and only allowing access to authenticated and authorized Commvault binaries
Zero trust AAA controls (Authentication, authorization, auditing)	Continuously validate trust and monitor access requests using multi-level authentication controls
Infrastructure hardening	Harden infrastructure using CIS and STIGS to reduce the attack surface
Zero trust isolation and air gap	Segment, compartmentalize and air gap backup data using TLS encrypted network topologies reducing the attack surface
Data validation	Data validation using CRC, and Commvault HyperScale file system erasure coding

Storage I/O controls (ransomware lock)

The first line of defense is Commvault's ability to lock random changes to backup storage using low-level storage I/O controls. This feature is often referred to as the "Ransomware Protection" lock, and it is designed to lock Commvault HyperScale™, as well as Windows and Linux data movers (media agents) against ransomware. However, the protection goes beyond just ransomware.



Only specific Commvault authenticated processes are permitted to modify backup storage. Since this control is implemented within the underlying Operating System I/O stack and is independent of operating system permissions, any process, including those from rogue attempts to manipulate or change backup data on the locked data mover (MediaAgent/ Commvault HyperScale node), is explicitly denied. The ransomware lock is supported on Commvault

Zero trust AAA controls (authentication, authorization, auditing)

Zero trust principles ensure user access is continuously validated and monitored for Authentication and Authorization while constantly Audited. The underlying philosophy for zero trust is, "Never assume trust, but continuously validate trust." Commvault leverages security controls such as multi-factor authentication for everyday administrative tasks, privacy locks, and data encryption. User access can be compartmentalized, explicitly denying CommCell level access, while applying roles to micro-segmented groups of resources through multi-tenant configurations. Zero trust controls help limit internal lateral movement to prevent data loss and unauthorized access to data.

Commvault makes it simple to apply zero trust AAA controls by using the Security Health Assessment Dashboard. The dashboard provides a single pane of glass for identifying controls, highlighting potential risks within the backup environment, and recommending interactive actions to apply controls. For more information, see this video.

Infrastructure hardening

Center for Internet Security® (CIS®) Benchmarks and Security Technical Implementation Guides (STIGs) are two primary third-party baselines adopted across public and private organizations for infrastructure hardening. Both hardening standards share many similarities; however, while CIS is primarily adopted across a wide range of commercial organizations, STIGs are primarily used across US government sectors since they contain specific language mandated by the US government. Using standardized hardening guidelines equips organizations with the best available information for closing infrastructure gaps. It also helps organizations remain compliant within their respective industries. Commvault has validated CIS hardening standards for the core platform infrastructure. Taking it one step further, Commvault HyperScale storage is pre-hardened using STIGs, so it is ready for deployment across government sectors.

In addition to the infrastructure hardening, Commvault digitally signs all binaries included with the Commvault platform to ensure application-level trust. Hardening and digitally signing application binaries helps reduce infrastructure and application-level attack surfaces.

Zero trust isolation and air gap

Isolating data targets through network segmentation is a highly effective strategy for reducing the likelihood of ransomware or unauthorized threat actors gaining access to backups (mostly secondary or tertiary backup copies). Although network segmentation is an infrastructure change, Commvault network topologies allows you to create zero trust policies for authorizing and controlling communication within the backup environment. Network topologies have the following advantages:

- They provide Transport Layer Security (TLS) encrypted one-way tunnels outbound from secure storage targets allowing all inbound communication to be blocked. You can also use a gateway or proxy between your public and secure zones.
- Communication between backup resources is authorized using certificate authentication.
- Only hosts configured within the topology can communicate explicitly, denying all other communication attempts from other hosts.

Commvault uses built-in intelligence to control power management of virtual gateway/proxies and virtual media agents. This effectively gaps the communication to the storage, so ransomware cannot reach it.

Greater ransomware prevention with data isolation and air gap technologies **Read >**

Data validation

Data validation is an inherent capability within the core Commvault platform. Commvault uses cyclic redundancy check (CRC) as one method of validating blocks of data are not corrupt, so that corrective measure can be taken. CRC's are generated against blocks of data at the source. When data is transferred to the destination storage, the CRC is validated to ensure no corruption or changes to the data. The validated CRC is then stored with the backup data so backups can be continuously checked at rest using administrative tasks. Additionally, Commvault HyperScale's file system provides improved data reliability and resiliency through erasure coding's inherent benefits.

Immutable storage options

Now that we have covered Commvault's immutable architecture let's put it all together. If you are looking for an all-in-one immutable storage target solution that is simple, look no further than Commvault HyperScale.™ Commvault HyperScale will provide everything into a converged hardened storage target that can be isolated and locked.

There may be a few additional gaps to close off for existing disk infrastructure since it is not a hyperconverged solution, like Commvault HyperScale. Enable Commvault's storage locking and follow hardening and isolation guidelines to protect Windows Server or Linux based media agents across any attached storage targets.

Commvault also supports WORM, object lock, and storage snapshot technologies provided by specialized storage hardware and cloud. Each of the supported storage paths offers various benefits, and their use cases depend on the organization's requirements. As we explore this further, you will see how Commvault's built-in locks perfectly complement cloud and hardware lock controls.

Some organizations may take additional strategic initiatives to "mix and match" storage and technologies. For example, the cloud not only provides immutability with object lock, but it also satisfies requirements for offline copies. Even in this use case, Commvault's locking technologies can be applied to on-premise storage to provide a layered solution. In that case, mixing Commvault HyperScale immutability with offline cloud immutability would be a perfectly layered multi-pronged approach.

Greater data protection: Immutable backups to the cloud with Commvault **Read >**

Another use case is to leverage existing capabilities such as snapshots or WORM on the hardware device. Once again, with this configuration profile, Commvault can apply additional locks on top of remaining storage targets that do not have snapshot or WORM capabilities and use locks on the snapshot capable hardware to protect the active data.

No doubt about it, a "mix and match" approach may add some complexity to the solution; however, layering the solution is a solid strategy and helps reduce risk. Commvault makes it easy to lock your data, whether using Commvault HyperScale,™ cloud, physical hardware, or any combination.

Threat monitoring

Commvault's monitoring platform is a powerful extension to the immutable architecture. Using historical metrics and machine learning algorithms, the Commvault platform can raise awareness of various anomalous activities and events in the backup environment. In context, these events help bubble-up exceptions in the environment that could indicate a threat in action.

Active monitoring

The apps used to backup various file systems, applications, and virtual machines work like sensors continuously monitoring metrics for anomalous file system activity such as modifications and deletions. When anomalous changes to the file system are detected, alerts are triggered to provide cause for action. Alerts can integrate with security information and event management (SIEM), other incident response systems, or initiate workflows.

Backup monitoring

In addition to monitoring live file systems, Commvault also monitors for anomalous changes in backups using the index. Anomalies detected in backups help administrators identify potential indicators of ransomware or other threats within backup content.

Threat monitoring powered with machine learning

Active monitoring
Monitors live threats

Backup monitoring
Monitor backups for threats

Honeypot
Detect ransomware activity

Event monitoring
Monitor for malicious event activity

Honeypot

Honeypot monitoring is also an effective way to detect ransomware attacks in action. Commvault uses a file type commonly targeted by ransomware and monitors for signature changes. Since this file is hidden on the file system, changes to the file can indicate a threat, such as ransomware.

Event monitoring

Commvault's machine learning platform is embedded within the event/alert subsystems of the platform. Any event such as failed login attempts or failed access attempts (to name a couple) that occur anomalously will be bubbled-up as an event for investigation. This provides an intelligent way of monitoring for malicious user behaviors within the backup environment.

Threat monitoring conclusion

Commvault's machine learning platform can save the organization valuable time as it focuses on the events and activities in the CommCell that need attention. No longer do you have to spend unnecessary time searching activity logs, hoping to identify suspicious events. When machine learning is applied to ransomware and security monitoring, organizations can continuously evaluate the effectiveness of controls and take proactive measures when needed. Since Commvault monitors live file systems, backups, and events, you can respond quickly to threats providing the best possible outcomes for your organization.

How this helps our customers

Commvault's immutable platform has a proven history of helping our customers keep backup data safe and recovery ready from ransomware.

When City of Sparks was hit with ransomware, virtually all police department operations were halted, including geographic systems. Unlike their previous backup solution, Commvault's immutable platform kept their backup data safe, and they were able to recover and bring all services back online quickly.

Evalueserve is a large analytic company that relies on Commvault to protect their data. Not only has Commvault shortened their backup windows by 55%, improving RPO's significantly; Commvault has also improved their security posture by locking their data from breaches and ransomware. CIO & CISO Sachin Jain said, "Thanks to the encryption and security feature with Commvault, it gives us confidence that our backup copies are in a complete locked state and cannot be touched in the event of ransomware attacks,"

Of course, we cannot forget the City of Colorado, who experienced zero data loss during their ransomware attack. Not only did Commvault's immutable architecture protect their data against ransomware, but Commvault's ransomware monitoring capabilities also provided the first notification that ransomware was present in the environment.

Conclusion

Commvault has an immutable architecture built on a deeply layered system of controls that work in tandem to harden data against ransomware, cyber threats, and bad internal actors.

Extending the immutable architecture with Commvault's AI platform, organizations are being preventative and proactive, reinforcing Commvault as a secure backup and recovery platform. A modern approach to being recovery ready. And that is the immutable truth.

To learn more about Commvault's ransomware protection, visit **commvault.com/ransomware >**