WHITE PAPER

Strengthen ransomware resilience with data isolation and air-gap technologies

Securing and defending your data is essential to the rapid recovery of clean backups. You must be vigilant and take a proactive, multilayered approach. That means actively defending your data and its recoverability across a broad range of production and backup workloads and environments. Commvault Cloud Autonomous Recovery and Commvault Cloud Backup & Recovery deliver proven, cyber-resilient data protection for unrivaled business continuity. Commvault® Cloud, powered by Metallic® AI is focused on enabling cyber resilience—the industry's first platform for true cloud data security that empowers businesses to secure data, predict risks, minimize damage, and rapidly recover.

DATA ISOLATION

Best cyber resilience practices revolve around separating backup copies from source environments to minimize the threat of data loss or cyber breach. Commvault isolates your backup data to maintain secondary/tertiary copies in a separate network and security domain. LAN/VLAN switching, firewalls, least-privilege protocols, and foundational security that includes zero-trust principles to secure your data and reduce the attack surface to contain cyberthreats. Data stored within Commvault is not only isolated, but also immutable. This means that it cannot be alerted, deleted, or changed, while restricting inbound communication and enabling outbound connections to reduce your attack surface. Commvault also tunnels securely between isolated targets and sources for data security and replication.

AIR GAPPING

Air gapping is a data security technique that isolates data from corporate networks. It works like surrounding a castle with a moat; access is controlled via a drawbridge that can be deployed as needed. When data does not need to be accessed, communication is blocked by disabling ports, VLANs, and firewalls. Commvault provides secure replication of backup data to an isolated environment, coordinating when connections can be opened and closed. Outgoing connections are restricted, reducing the attack surface and allowing data to remain air-gapped until recovery or replication is needed.

KEY FOUNDATIONAL ADVANTAGES

Commvault's cyber resilience platform delivers key architectural components and tools, offering businesses of every size a durable, resilient, and proven backup framework:

Outbound communication only: All inbound access to the isolated data is blocked. Only restricted outbound connections are allowed from the isolated data to the source data for replication.

Air gap–ready: On-premises and hybrid configurations can be set up easily to create functionally secure air gaps within your environment Commvault Cloud Air Gap Protect provides a turnkey cloud air-gap solution that can be up and running in minutes and/or use Commvault Cloud HyperScale™ X for a secondary storage target on premises.

Hardware agnostic: When using Commvault as an air-gap solution, any supported storage can be used, including the Commvault HyperScale™ Appliance. Commvault also supports write once, read many (WORM) storage policies and immutable locks used with third-party storage devices.

Data integrity verification: Commvault validates data integrity during backup, when data is at rest, and during data-copy operations.

- Verification operations run automatically, using the data signatures to validate the backup data at rest. When copying the data, the signatures are used again to validate the data blocks during the copy operation.

Industry-leading security controls: Commvault's AAA Security Framework (authentication, authorization, and accounting) provides a suite of security and access controls to harden the Commvault platform itself–reducing risks from malicious actors and inside threats via a least-privilege approach to authorization. Advanced controls include:

- Strong multifactor authentication and multiperson authentication controls, retention locks, and command authorization to protect data from accidents as well as limit potentially destructive actions.
- Integration with privileged access management (PAM) and enhanced identity and access management (IAM) tools such as CyberArk, YubiKey, and biometrics for added user authentication and assurance (AAL3).
- End-to-end data encryption (while allowing external key-management platforms to manage and control keys), and certificate authentication–protecting against malicious data access.

Foundational hardening: The Commvault platform foundation is hardened using industry-leading CIS Level 1 benchmarks to reduce your attack surface.

Immutable backups: Commvault's hardware-agnostic approach offers ransomware-protection locks for just about any storage. Prevent unauthorized activity within the I/O stack (attempts to delete, change, or modify backup data) while preserving the integrity of backups:

- Ensure a fully immutable storage target with HyperScale X, leveraging scalable software-defined storage.
- Native OS and file-system controls embedded within the HyperScale X platform protect data from unauthorized or random modifications.
- Commvault Cloud Air Gap Protect easily provides immutability to house data in a secure, air-gapped cloud storage target.

Ransomware detection: Going beyond data validation, Commvault provides insights into suspicious and changed files with layered anomaly detection, honeypots, threat analysis, and file data analysis.

- Anomaly detection looks for suspicious behavior and activity within the backup data.
- Commvault® Cloud Threat Scan* detects malicious content. It performs a deep scan of the backup content, leveraging available scanning/antivirus tools to identify malware and files that have been encrypted, corrupted, or significantly changed so you can recover clean data and avoid file reinfection.
- Threat Scan Predict finds AI-driven ransomware to predict threats before they infect backups.
- Honeypots and file anomaly detection to actively detect threats in the live environment.
- Commvault Cloud Threatwise™ provides industry-unique early-warning threat detection technology to surface advanced cyber threats in production environments.

Rapid incident remediation and recovery:

- Curated data restores ensure that the last-known good copy of the backup is automatically selected when restoring data.
- Malware files are surgically and automatically purged from the Commvault index.
- Powerful cross-platform and cross-cloud restore capabilities to rapidly recover data, meet SLA compliance, and fulfill forensic analysis.
- Commvault provides instant recovery options to provide rapid access to critical data and systems.
- With Cleanroom as a Service gain capabilities to identify and ensure clean recovery, plus the ability to guarantee safe recovery to a cleanroom in the cloud.
- Cloudburst Recovery combines infrastructure-as-code and cloud scaling to ensure fast, predictable, and reliable cyber recovery at scale.

*Available with Commvault software only.

HOW DATA ISOLATION AND AIR GAPPING WORK

On-premises air-gap solutions require a mix of network architecture and software configurations. From an architectural perspective, storage must first be isolated and segmented on the network–without allowing inbound connections to that storage. Leveraging the components above, the Commvault software layer, network topologies, and workflows provide the basis for controlling data-pipe tunnels and orchestrating air-gap controls. In addition, Commvault's flexibility allows seamless integration with the topology or security profiles that organizations commonly deploy.

Direct connection for data isolation

Figure 1 depicts the high-level functionality of Commvault data isolation using direct connections. Site A represents the public portion of the production backup environment. Site B is a segmented portion of the environment, which has been isolated both logically and physically. Site B communicates through the firewall over a single outbound port. Everything else is blocked. The tunnel between the two sites supports HTTPS encapsulation using the TLS 1.3 protocol. The tunnel will connect only once certificate authentication is successful. This protects against man-in-the-middle and spoofing attacks.

Data transfer is multistreamed through the tunnel to ensure the fastest backup possible. Commvault's security controls, encryption, WORM, threat analysis, data analysis, and native ransomware locks for immutable storage protect data residing on the storage target on Site B from ransomware and accidental deletion. Data replication is deduplicated to further optimize bandwidth and storage considerations.

Once data transfer is complete, connectivity can be severed by turning off routing, enabling firewall rules, or shutting down systems. Connection severance can be scheduled around virtual machine (VM) power management or blackout windows.

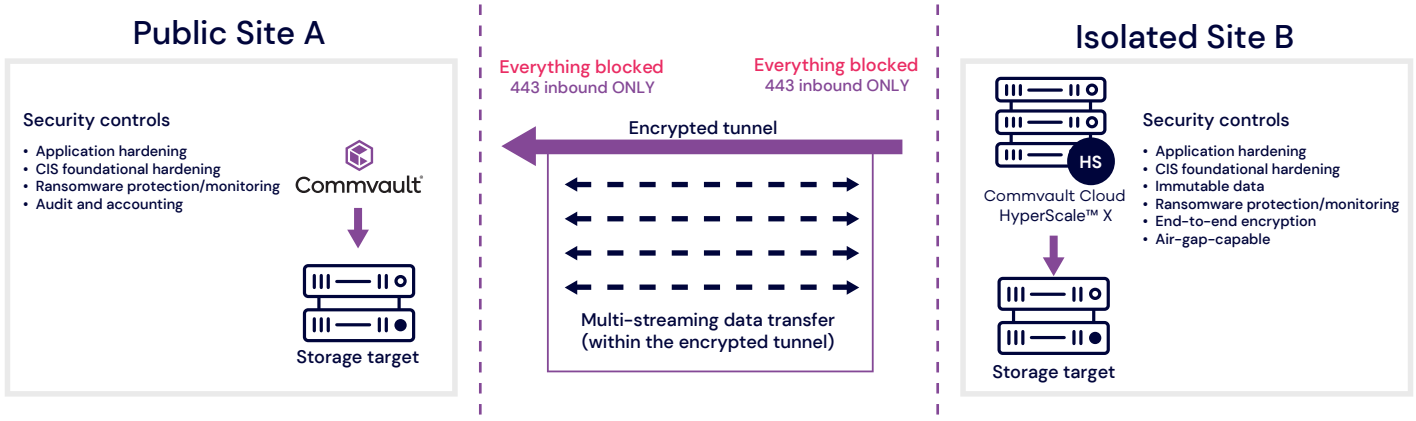

Figure 1 - Data isolation using direct connections

PROXY/NETWORK GATEWAY CONNECTION

A proxy-based configuration (Figure 2) has the same ransomware and encryption benefits as a direct connection. However, proxy-based isolation differs in that both sites communicate using a proxy located between the isolated and public networks (possibly a DMZ). All inbound connectivity is blocked between the sites, providing isolation capabilities on both sites. Proxy-based configurations are prevalent, especially when data moves between remote geographic locations across the internet.

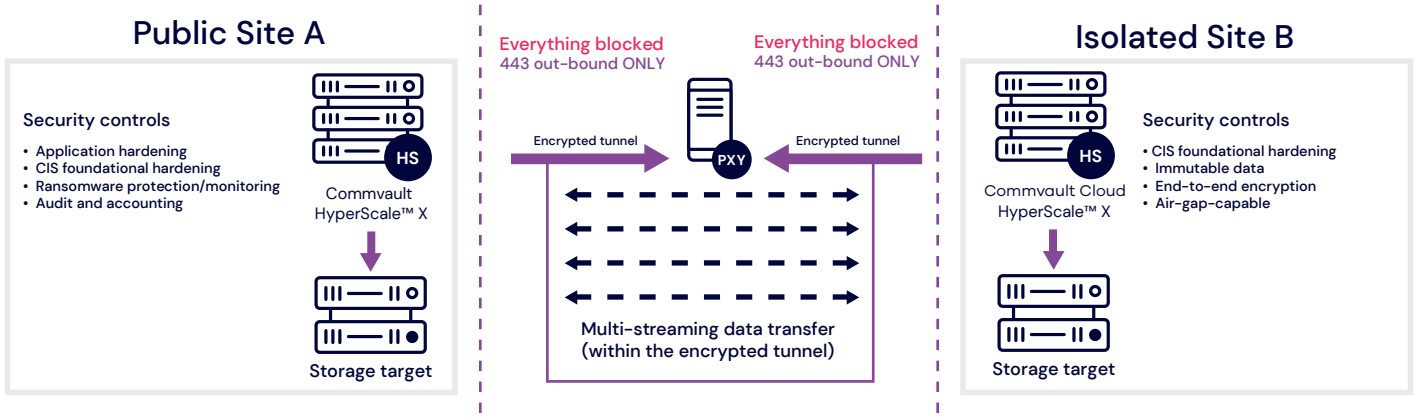

Figure 2 - Data isolation using a proxy-based network gateway connection

USING OBJECT STORAGE AND THE CLOUD

Object storage targets enable secure backup data isolation with WORM and immutable locks. Commvault integrates these storage targets for retention, encryption, and security. API calls over HTTPS provide more on-demand access and help reduce the ransomware attack surface. Object storage is ideal for secondary and tertiary copies, providing a secure, isolated target.

USING CLOUD STORAGE: COMMVAULT CLOUD AIR GAP PROTECT

Cloud storage targets (such as Azure and AWS) offer benefits similar to those of object storage solutions. The key difference is that cloud solutions are inherently isolated because they don't reside on premises with the rest of the organization's environment. This makes cloud storage a very economical solution because the copy is stored offsite and resources are readily available, elastic, and multitiered.

Commvault Cloud Air Gap Protect makes it easy to achieve secure and scalable cloud storage in just minutes, allowing you to meet the needs of your organization's hybrid cloud strategy while providing an additional layer of ransomware protection. With Commvault Cloud Air Gap Protect you can seamlessly adopt air-gapped cloud storage and gain predictable costs and reduced overhead. It can also be the foundation for improving your cyber recovery strategy by leveraging a fully integrated, secondary cloud storage target for Commvault Cloud HyperScale™ X.

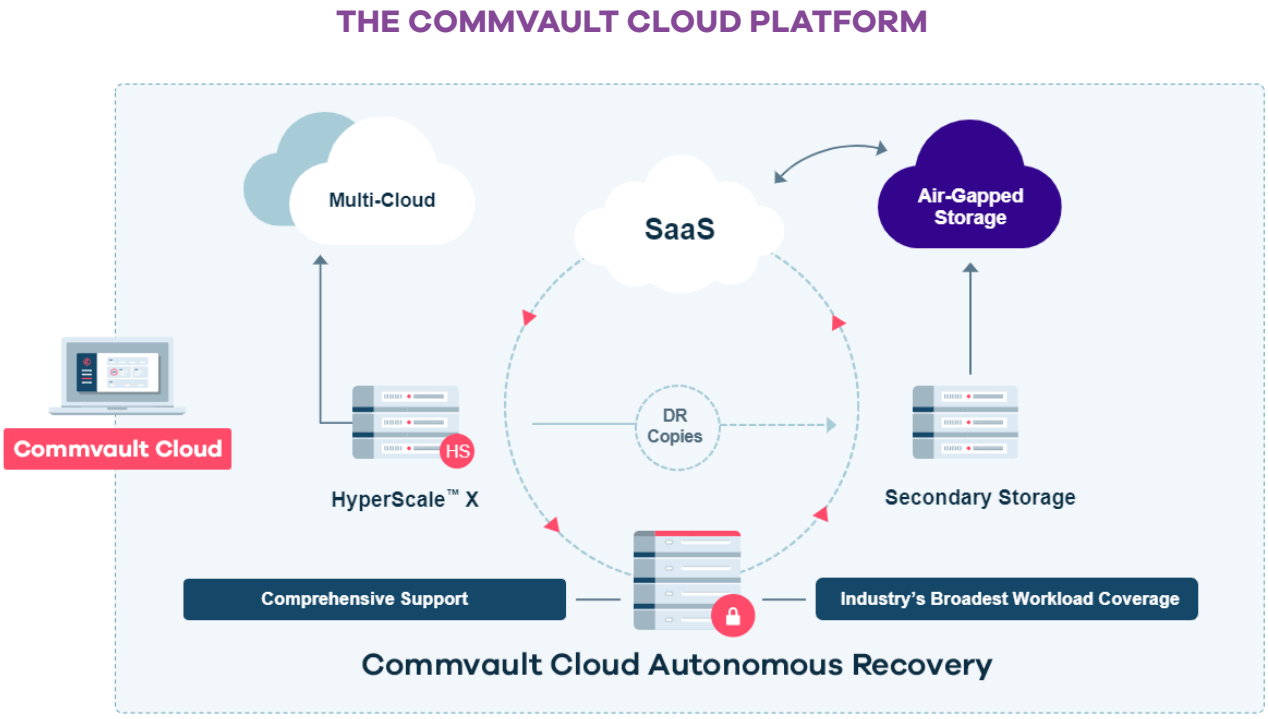

Figure 3 – Commvault provides the broadest workload protection, from on premises to the cloud, multi-cloud, edge, SaaS, and native cloud integration. Using the immutability locks offered by cloud providers in tandem with role-based security can secure backup data while supplying a remote, isolated, offsite data copy.

SEVERING THE CONNECTION AND AIR GAPPING

Combining a properly isolated and segmented data center with Commvault Cloud security controls can substantially reduce risks. Air gapping further limits the ability to access backup data when it's not in use. During air gapping, resources are turned off and data replication doesn't run, which may affect planning around recovery point objectives (RPOs). Depending on the environment, resources, and service level requirements, data replication is likely to queue when destination targets are offline. To help reduce this effect, Commvault incorporates multi-streaming within the one-way encrypted tunnel to maximize backup performance.

The simplest method of air gapping is to use VM power management, a capability within Commvault for automatically shutting down media agent virtual machines (data mover virtual machines) when not in use. The VMs will then start up when needed. This method requires a hypervisor in the isolated environment but does not need additional scripts.

Another method of air gapping is to use blackout windows, scripts, and workflows. Blackout windows define the time frames during which backups and administrative tasks are not allowed to run. During blackout windows, the isolated resources are set offline and made inaccessible using scripts or Commvault workflows. When blackout windows are not in effect, the resources are brought online again using scheduled scripts included on the air-gapped resource, such as the media agent. This method does not require a hypervisor for the VM power management air-gap method, because any storage target or network device can be shut down to air-gap the isolated site.

Here are some examples of using scripts to orchestrate air gapping:

- Stopping and starting Commvault services on the isolated media agents/storage targets
- Disabling/enabling network interfaces on media agents around blackout windows
- Disabling/enabling VLAN routing policies around blackout windows
- Disabling/enabling firewall policies around windows, using scripts

CONCLUSION

Like a castle, your backup data requires multiple layers of protection to defend against internal and external threats. Using Commvault Cloud security controls and immutable locks (ransomware protection, WORM, and encryption), Commvault Cloud Threat Scan, Commvault Cloud Autonomous Recovery, and more–in combination with proven data isolation and air-gapping techniques–provide a well-protected, multilayered strategic solution that ensures you are cyber recovery-ready.