

# Greater ransomware protection with data isolation and air gap technologies

Protecting your data and ensuring its availability is your top priority. Like a castle in medieval times, you must always defend it and have built-in defense mechanisms. It is under attack from external and internal sources, and you do not know when or where it will come from. Vigilance is required, and you want multiple levels of safeguards for greater data protection. The same is true for your organization; a single event can threaten the bottom line or define a career. So how do you prepare? By making sure you're recovery ready.

## Ransomware protection with data isolation and air gap

With cyber threats becoming increasingly sophisticated, having a layered approach to securing your data greatly reduces the risk and impact to your organization. Commvault Complete™ Backup & Recovery software includes several layers and tools to protect and restore your data and applications. Two proven techniques for reducing the attack surface on your backup data are data isolation and air gapping.

The goal of **isolating** backup data with Commvault is to have secondary and/or tertiary copies of backup storage targets segmented and unreachable from the public portions of the environment using virtual LAN (VLAN) switching, next generation firewalls, or zero trust technologies. If your organization is infiltrated by ransomware, or a malicious attacker, the cyber threat will have a limited attack surface. The public portions of the environment may get infected, but the isolated data will not because it cannot be accessed. To be most effective, isolated environments should not be accessible to public networks of the organization as well as the internet. Physical access to isolated resources should be secured and heavily controlled. All inbound network communication is blocked, and only restricted outbound access is allowed. Commvault will then securely tunnel from the isolated storage targets to the Commvault resources and source storage targets for data replication.

**Air Gapping** is another technique that complements data isolation. Traditionally, air gapped networks have absolutely no connectivity to public networks. Tape is a traditional medium for air gapped backups, because tape can be removed from the tape library and stored offsite. To air gap secondary backup targets on disk, or cloud, some access is needed, but when it is not needed, communication is severed. Air gapping works like a medieval castle. The castle is surrounded by a moat with water, and the walls are impenetrable. The only access allowed to the castle is the drawbridge that is let down periodically to bridge the gap. When the isolated data does not need to be accessed, communication is severed either by turning communication ports off, disabling VLAN switching, enabling next gen firewall controls or turning systems off. This process is fully orchestrated and automatic using the Commvault workflow engine.

Commvault provides secure replication of data to an isolated environment with air gap capabilities. The isolated environment is completely blocked from all incoming connections. Outgoing connections are restricted, which greatly reduces the attack surface of cyber threats. Once data is fully replicated, the connection can be severed, and the secondary data becomes air gapped until data needs to replicate again or recovered.

## Key advantages and value of Commvault data protection

Commvault data protection with data isolation and air gap provides organizations the following advantages against ransomware:

### Communication is initiated from the isolated site

All access to the isolated data is blocked. Only restricted outbound connections are allowed from the isolated data to the source data for replication. This can be referred to as a pull configuration (as opposed to push), where Commvault manages data protection and retention, but communication initiates from the secured isolated side.

### Air gap ready

Replicated data can be air gapped by severing the encrypted tunnel initiated from the isolated site. The Commvault automation framework makes it simple to customize this functionality as required.

### Industry leading security controls

Commvault's AAA Security Framework (Authentication, Authorization, Accounting), provides a suite of security controls to harden the Commvault platform. Additionally, Commvault uses end-to-end encryption, and certificate authentication protecting against malicious data access, man-in-the-middle attacks, and spoofing.

### Foundational hardening

Harden the Commvault platform foundation using industry-leading CIS Level-1 benchmarks.

### Immutable backups

Utilizing layered security controls, write once read many (WORM) capabilities as well as built-in ransomware protection for backup data; Commvault locks backup data from unauthorized random changes. This also helps prevent intentional and unintentional bad actors from modifying or deleting backup data in order to preserve the integrity of backups.

### Data verification

Commvault validates data integrity during backup, when data is at rest, and during data copy operations. When data is backed up for the first time, CRC checksums are computed for each data block on the source client. These signatures are used to validate the initial backup data and are stored with the backup. Verification operations run automatically utilizing the signatures to validate the backup data at rest. When copying the data, the signatures are used to validate the blocks of data during the copy operation.

### Cyber/Ransomware attack protection

Backup data is locked and can only be modified by Commvault processes. Any ransomware, application, or user that attempts to delete, change or modify backup data from the data mover (media agent), will be rejected within the I/O stack unless it is an authorized Commvault process. Additionally, Commvault uses machine learning algorithms to detect file-based anomalies that may indicate a ransomware attack on a Commvault resource.

### Hardware agnostic

Commvault supports a variety of disk, cloud, and object storage vendors. When using Commvault for an air gap solution, any supported storage vendor can be used, including the Commvault HyperScale™ Appliance. Commvault also supports WORM, and immutable locks used with third-party storage devices.

### Commvault backup and recovery software integration

Commvault features such as indexing, analytics, and deduplication are all part of the data isolation and air gap solutions.

## How it works

### Overview

Commvault's network topology and workflow engine provide the basis for configuring data isolation and air gap solutions. The flexibility of the platform allows seamless integration with most topology or security profiles that organization have deployed.

### Direct connection for data isolation

The Figure 1 diagram represents the overall 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, isolated logically and physically. Site B communicates through the firewall over a single outbound port. Everything else is blocked. The tunnel supports HTTPS encapsulation using the TLS 1.2 protocol. The tunnel will only connect once certificate authentication is successful. This protects against man-in-the-middle, and spoofing attacks.

Data transfer is multi-streamed through the tunnel to ensure the fastest backup possible. Data residing on the storage target on Site B is protected from ransomware and accidental deletion by utilizing Commvault's security controls, encryption, WORM and native ransomware locks for immutable storage. 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 systems down. Severing the connection can be scheduled around VM power management, or blackout windows.

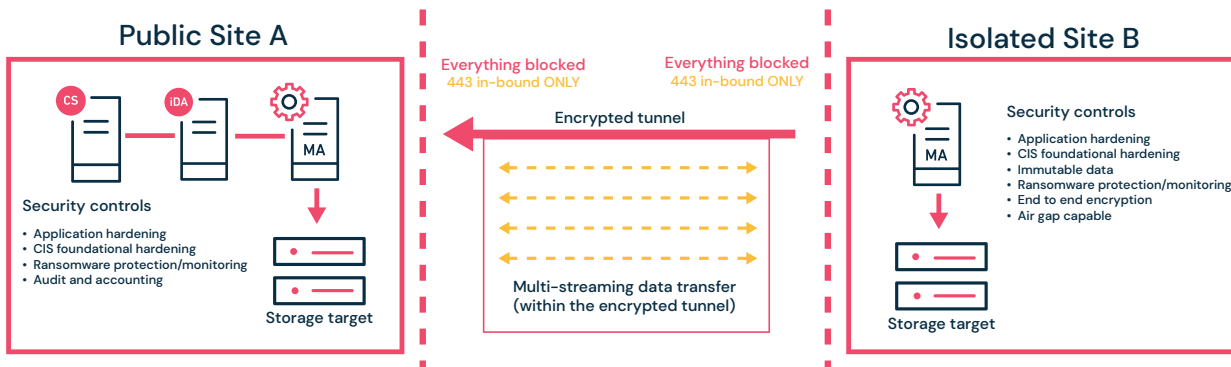


Figure 1 – Direct connection

### Proxy/Network gateway connection

Proxy based configuration (Figure 2) has the same ransomware, and encryption benefits as Direct Connection. Proxy based isolation differs from Direct Connection in that both sites communicate between each other using a proxy located between the isolated and public networks (possibly DMZ). All inbound connectivity is blocked between the sites providing isolation capabilities on both sites. Proxy based configurations are very common especially when data is moving between remote geographic locations across the internet.

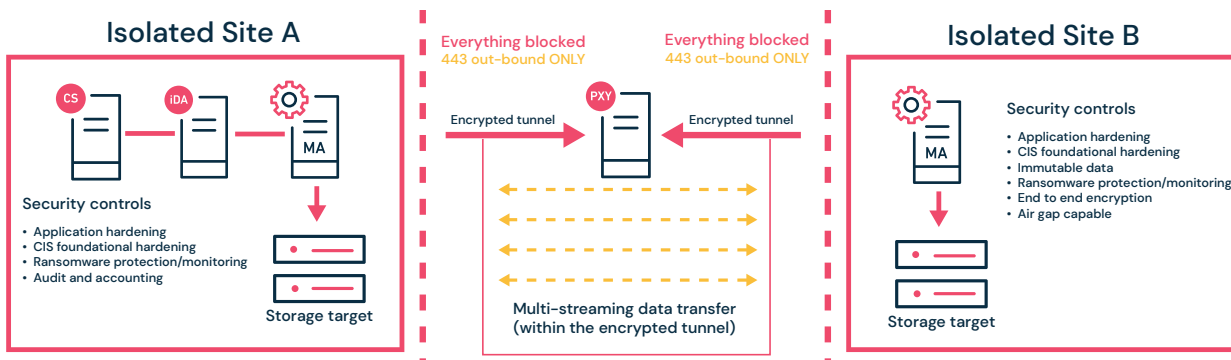


Figure 2 – Proxy/Network gateway connection

**Utilizing object storage and cloud**

Being hardware agnostic is one of Commvault’s key advantages. Object storage targets can be another strategic way of isolating backup data. Object storage targets typically have their own WORM and immutable locks built within the hardware platform. Commvault seamlessly integrates with those capabilities, while still managing retention, data encryption, and software application security controls.

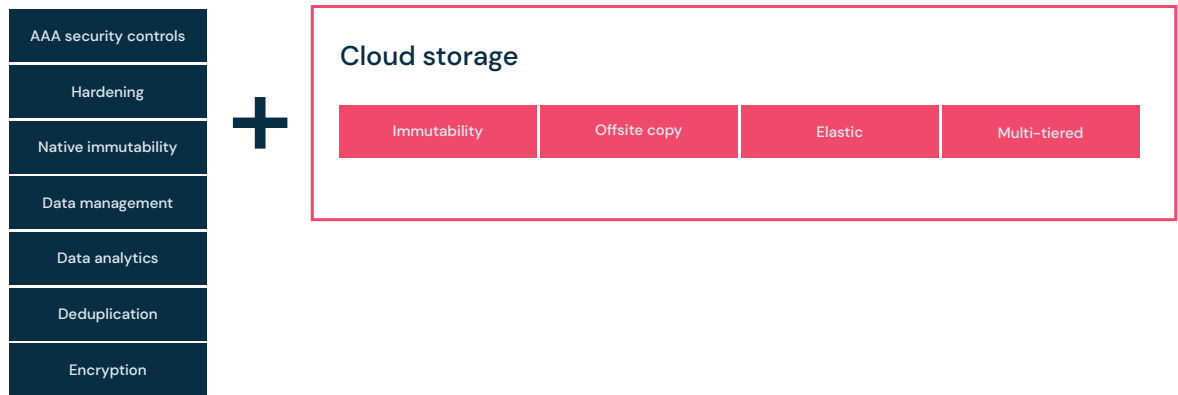
Object storage targets use authenticated API calls over HTTPS for reading and writing data. This allows common protocols frequently used by ransomware to be turned off reducing the attack surface. The REST API interface also provides more on-demand access compared to other protocols. The data backed up to the object storage device is not exposed when not in use. Only authenticated API calls can read and write to the storage target.

Object storage-based solutions are commonly leveraged for secondary and tertiary copies and can serve as an isolated secure target.

**Utilizing cloud storage**

Cloud storage targets (such as Azure and AWS) have similar benefits to object storage solutions. The key difference is that cloud solutions are inherently isolated, in the sense that they do not reside on-premises with the rest of the organization’s environment. This makes cloud a very economical solution because not only is the copy offsite, resources are readily available, elastic, as well as multi-tiered.

**Commvault platform**



Commvault supports the most common cloud platforms, while applying source side encryption, deduplication, data management, and analytic capabilities. Using the immutability locks provided by cloud providers, and role-based security will protect backup data while also supplying a remote isolated offsite data copy.

**Severing the connection and air gapping**

In a lot of cases, a properly isolated and segmented data center, in combination with the security controls built into Commvault is enough to reduce risks. Air gapping is another control, which further limits the ability to access backup data when not in use. The downside to air gapping is planning around recovery point objectives (RPO’s), because when resources are turned off, data replication will not run. Depending on the environment, resources, and service level requirements data replication will queue when destination targets are offline. To help reduce the effects of this downside, 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. VM power management is a capability within Commvault to automatically shut down media agent virtual machines (data mover virtual machines) when not in use. The VM will then start up, when needed. This method requires a hypervisor in the isolated environment and does not need additional scripts.

Another method of air gapping is to use blackout windows, scripts and workflows. Blackout windows define what time frames 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 shutdown to air gap the isolated site.

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

- Stop and start Commvault services on the isolated media agents/storage targets
- Disable/enable network interfaces on media agents around blackout windows
- Disable/enable VLAN routing policies around blackout windows
- Disable/enable firewall policies around windows using scripts

Any combination of the above will properly disconnect the resources and air gap the data. In the above examples the Commvault workflow framework executes and controls the scripts, API requests, or command line operations to orchestrate air gapping. The workflow framework provides a manageable, yet customizable platform to fulfill any air gap orchestration needs. Additionally, scripts can be hosted within the isolated environment, and executed using other scheduling tools such as Microsoft Windows Task Scheduler, or Unix cron.

## Conclusion

Just as a castle has multiple layers of protection both to ward off external and internal threats, so must your backup data. Taking a layered approach to securing backup data is the best way to ensure its security and availability. Using Commvault’s existing security controls and immutable locks (ransomware protection, WORM, and encryption), in combination with Data Isolation and Air Gapping techniques provides a well-protected solution. With Commvault you are recovery ready!

Commvault data protection delivers a layered approach for securing your data and applications. [Learn >](#)