WHITEPAPER

Greater Ransomware Protection with Data Isolation and Air-Gap Technologies

Protecting your data and ensuring its availability is everyone's top priority. It is a lot like safeguarding a fortress in that constant vigilance is required, and you must have multiple built-in defense mechanisms in place at all times. So how do you prepare? Start by making sure you're recovery ready.

Ransomware protection with data isolation and air gapping

With cyberthreats becoming increasingly sophisticated, having a layered approach to securing your data can greatly reduces the risk and potential impact on 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 that often go hand in hand 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. This is accomplished using virtual LAN (VLAN) switching, next-generation firewalls, or zero trust technologies. If ransomware or a malicious attacker infiltrates your organization, the cyberthreat will have a limited attack surface to work within. The public portions of the environment may get infected, but the isolated data will not because it's inaccessible. To be most effective, isolated environments should not be accessible to public networks of the organization, which often include the internet. Physical access to isolated resources should be secured, heavily controlled, and audited via organizational security policies. All inbound network communication is blocked, and only restricted outbound connections are allowed. In this setup, the Commvault solution can still replicate data by securely tunneling from the isolated storage targets to Commvault resources and source storage targets.

Air gapping is another technique that complements data isolation. Traditionally, air-gapped networks have 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 in the cloud, some access is needed, but communication is severed when it is not needed. Air gapping works like security in 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 lowered periodically to bridge the gap. When the isolated data does not need to be accessed, communication is severed 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. These tactics completely isolate and block the environment from all incoming connections. Outgoing connections are restricted, which greatly reduces the cyberthreat attack surface. Once data is fully replicated, the connection can be severed, and the secondary data becomes air-gapped until data needs to replicate again or be recovered.

Key advantages and value of Commvault data protection

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

Outbound communication

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. 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 using scripts or proxy power management.

Industry-leading security controls

Commvault's AAA Security Framework (Authentication, Authorization, Accounting), provides a suite of security controls to harden the Commvault platform and management. Strong multi-factor authentication controls, retention locks, and command authorization protect data from accidents as well as malicious destructive actions. Additionally, Commvault uses end-to-end encryption while allowing external Key Management platforms to manage and control keys, 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 to reduce the attack surface.

Immutable backups

Commvault's hardware-agnostic approach offers ransomware-protection locks for just about any storage that can reject any ransomware, aberrant application, or unauthorized user within the I/O stack that attempts to delete, change, or modify backup data from the data mover (media agent). However, centering the data protection solution around Commvault's HyperScale™ X ensures a fully immutable storage target leveraging scalable software-defined storage underneath. Native OS and file system controls embedded within the HyperScale X platform, protect data from unauthorized random changes and modifications. This preserves the integrity of backups by helping to prevent intentional modifications and deletions.

Data Integrity 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, Cyclic Redundancy Check 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, using 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.

Ransomware activity monitoring

Using the file anomaly and honeypot framework, the Commvault platform provides insights into when files are suspicious or being changed by a potential malware application. This framework is powered by machine learning, and monitors backed-up and live source data, ensuring insights can be derived prior to replication to the air-gapped storage.

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 write once, ready many (WORM) and immutable locks used with third-party storage devices.

Commvault backup and recovery software integration

Features such as indexing, analytics, and deduplication are all part of our data isolation and air-gap solutions.

How it works

Overview

On-premises air-gap solutions require a mix of network architecture and software configurations. From an architecture perspective, storage must first be isolated and segmented on the network, and no inbound connections to storage can be allowed. Within the Commvault software layer, network topologies and workflows provide the basis for controlling data-pipe tunnels and orchestrating air-gap controls. In addition, the platform's flexibility allows seamless integration with most topology or security profiles that organizations commonly deploy.

Direct connection for data isolation

Figure 1 below 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 1.3 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 via 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.

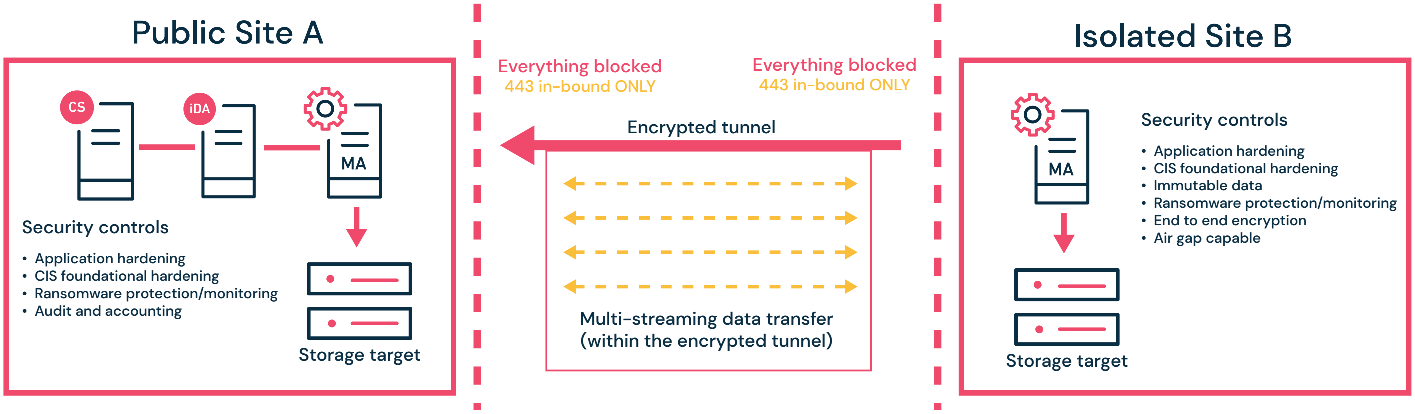

Figure 1 – Data isolation using direct connections

Proxy/Network gateway connection

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 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.

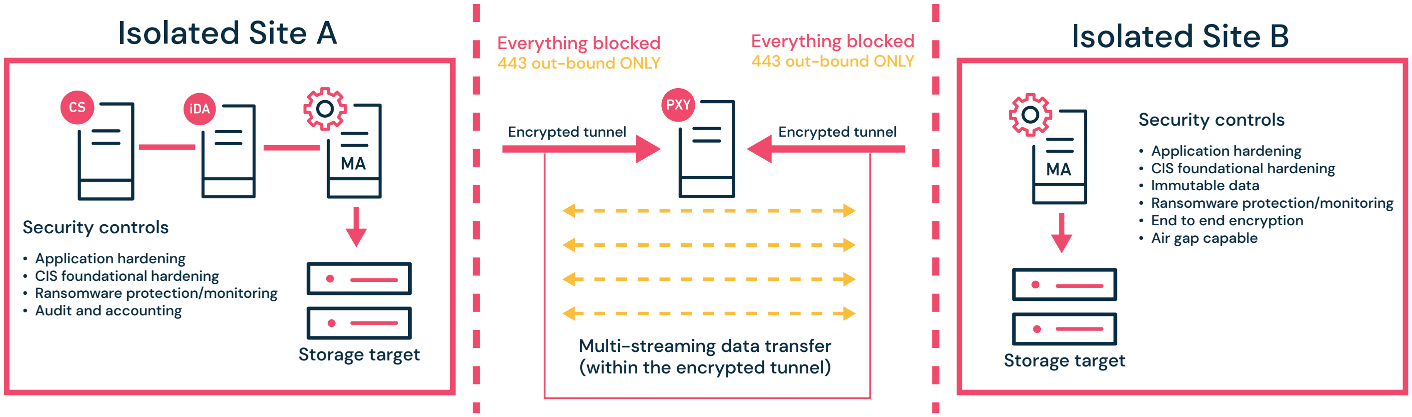

Figure 2. Data isolation using a proxy-based network gateway connection

Using object storage and 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.

Using cloud storage

Cloud storage targets (such as Azure and AWS) offer benefits that are similar to those of object storage solutions. The key difference is that cloud solutions are inherently isolated because 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, and multitiered.

Metallic® Recovery Reserve™

Metallic Recovery Reserve makes it easy to adopt secure and scalable cloud storage in just minutes, allowing you to meet the needs of your organization's hybrid cloud strategy without requiring additional cloud expertise within your organization. With Metallic Recovery Reserve, you can seamlessly adopt air-gapped cloud storage and gain predictable costs and reduced overhead. It can also be the foundation for improving your ransomware recovery strategy by leveraging a fully integrated, secondary cloud storage target for Commvault® Backup & Recovery or Commvault HyperScale™ X.

Commvault platform

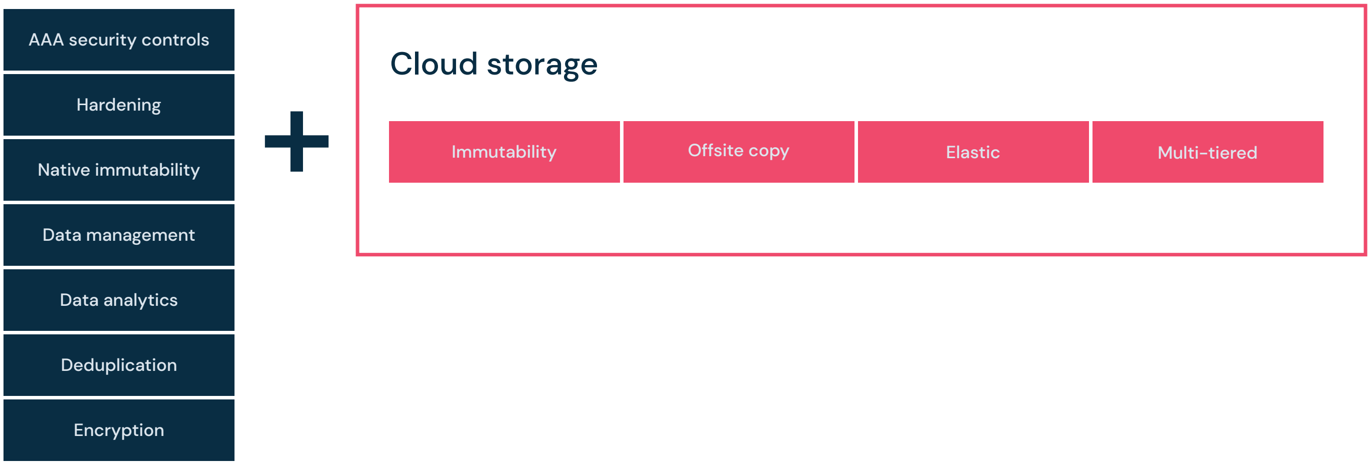

Figure 3. Commvault supports popular cloud platforms while applying source-side encryption, deduplication, data management, and analytic capabilities. Using the immutability locks provided by cloud providers in tandem with role-based security can protect backup data while also supplying a remote, isolated, offsite data copy.

Severing the connection and air gapping

The combination of a properly isolated and segmented data center and Commvault's security controls can substantially reduce risks. Air gapping is another control that further limits the ability to access backup data when not in use. The downside to air gapping is planning around recovery point objectives (RPOs), because when resources are turned off, data replication will not run. 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 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 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:

- 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 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, 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.

An easy way to adopt air-gap capabilities is through Metallic Recovery Reserve™, which is fully integrated with Commvault® Backup & Recovery and Commvault HyperScale™ X.

Conclusion

Like a castle, your backup data requires multiple layers of protection to ward off internal and external threats. Using Commvault's security controls and immutable locks (ransomware protection, WORM, and encryption), in combination with proven data isolation and air-gapping techniques, provides a well-protected, multi-layered strategic solution. With Commvault, you are recovery ready!

Commvault data protection delivers a layered approach for securing your data and applications. **Learn >**