HITACHI
Inspire the Next

Reliable Ransomware Recovery

WHITE PAPER

# Greater Ransomware Protection Using Data Isolation and Air Gap Technologies

## Hitachi Data Protection Suite (HDPS) Powered by Commvault and Hitachi Content Platform (HCP)

By Hitachi Vantara

# Contents

## Reliable Ransomware Recovery

Protecting your data and ensuring its' availability is one of your top priorities. 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. The prevalence of ransomware and the sharp increase in users working from home and on any device adds further complexity and broadens the attack surfaces available to bad actors. So much so, that your organization being hit with ransomware is almost unavoidable. While preventing attacks is important, you also need to prepare for the inevitable fallout of a ransomware incident.

Here are just a few datapoints from recent research around ransomware:[1]

- Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
- Ransomware is expected to attack a business every 11 seconds by the end of 2021
- 75% of the world's population (6 Billion people) will be online by 2022.
- Phishing scams account for 90% of attacks.
- 55% of small businesses pay hackers the ransom
- Ransomware costs are predicted to be 57x more over a span of 6 years by 2021
- New ransomware strains destroy backups, steal credentials, publicly expose victims, leak stolen data, and some even threaten the victim's customers

So how do you prepare? By making sure you're recovery ready with a layered approach to securing your data. Two proven techniques for reducing the attack surface on your data are data isolation and air gapping. Hitachi Vantara and Commvault deliver this kind of protection with the combination of Hitachi Data Protection Suite (HDPS) and Hitachi Content Platform (HCP) which includes several layers and tools to protect and restore your data and applications from the edge of your business to the core data centers.

---

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://blog.knowbe4.com/ransomware-predicted-to-cost-20-billion-in-damages-globally-by-2021
https://heimdalsecurity.com/blog/ransomware-payouts/

## Intelligent Data Recovery for Ransomware Using Data Isolation and Air Gaps

The goal of isolating backup data with HDPS 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. HDPS will then securely tunnel from the isolated storage targets to the HDPS resources and source storage targets for data replication.

Air gapping is another technique that compliments data isolation. Traditionally, air gapped networks have absolutely no connectivity to public networks. To air gap secondary backup targets on HCP, some access is needed, but when it is not needed communication is severed. Air gapping works like a medieval castle. The castle (in this case, HCP) is surrounded by a moat with water, and the walls are impenetrable. The only access allowed to the castle is the drawbridge (HDPS) 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 HDPS workflow engine.

HDPS 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.

HCP's robust data immutability features, like WORM and S3 Object Lock, ensure that data can never be overwritten. When new writes occur a new version of that file is created. Therefore, should ransomware infiltrate your environment and encrypt any of your data, there is still a viable copy available for recovery. (Figure 1 provides a very high-level overview of the solution.)

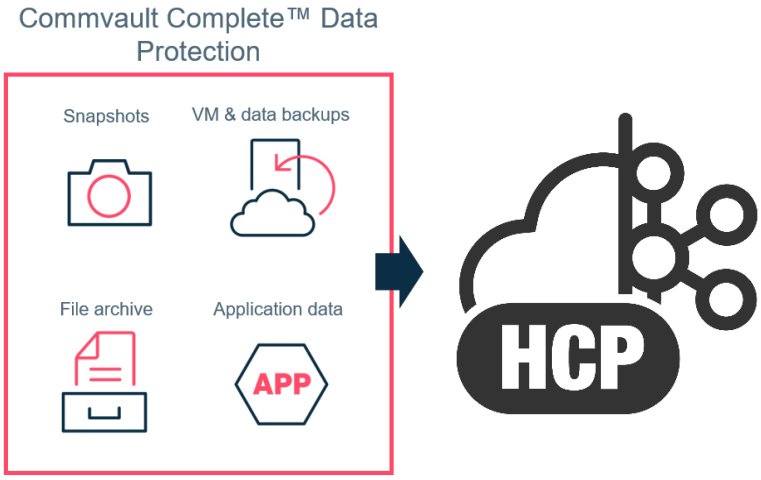


Figure 1

## Key Advantages of This Approach

### 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. Should an attack make its way through to the HCP, WORM, S3 Object Lock and file versioning will prevent overwriting of existing data and preserve the older versions for easy recovery.

### 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 the solution 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 solution's 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. The Hitachi Content Platform brings additional layers of protection with WORM, data immutability and S3 Object Lock storage, file versioning, content integrity checking, encryption, access controls, event logging and much more.

### 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) and S3 Object Lock capabilities as well as built-in ransomware protection for backup data; the solution locks backup data from unauthorized random changes. This also helps prevent intentional and unintentional bad actors from modifying or deleting backup data to preserve the integrity of backups.

### Data Verification

The solution 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.

### Edge to Core Coverage

Given that user behavior is often the weakest link in ransomware defenses, you need to account for these attack surfaces as well. Adding Hitachi Content Platform Anywhere to user devices and Hitachi Content Platform Gateways as file servers for remote offices ensures that these data sets are also protected by Hitachi Content Platform for easy recovery from ransomware attacks

## 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 2 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.

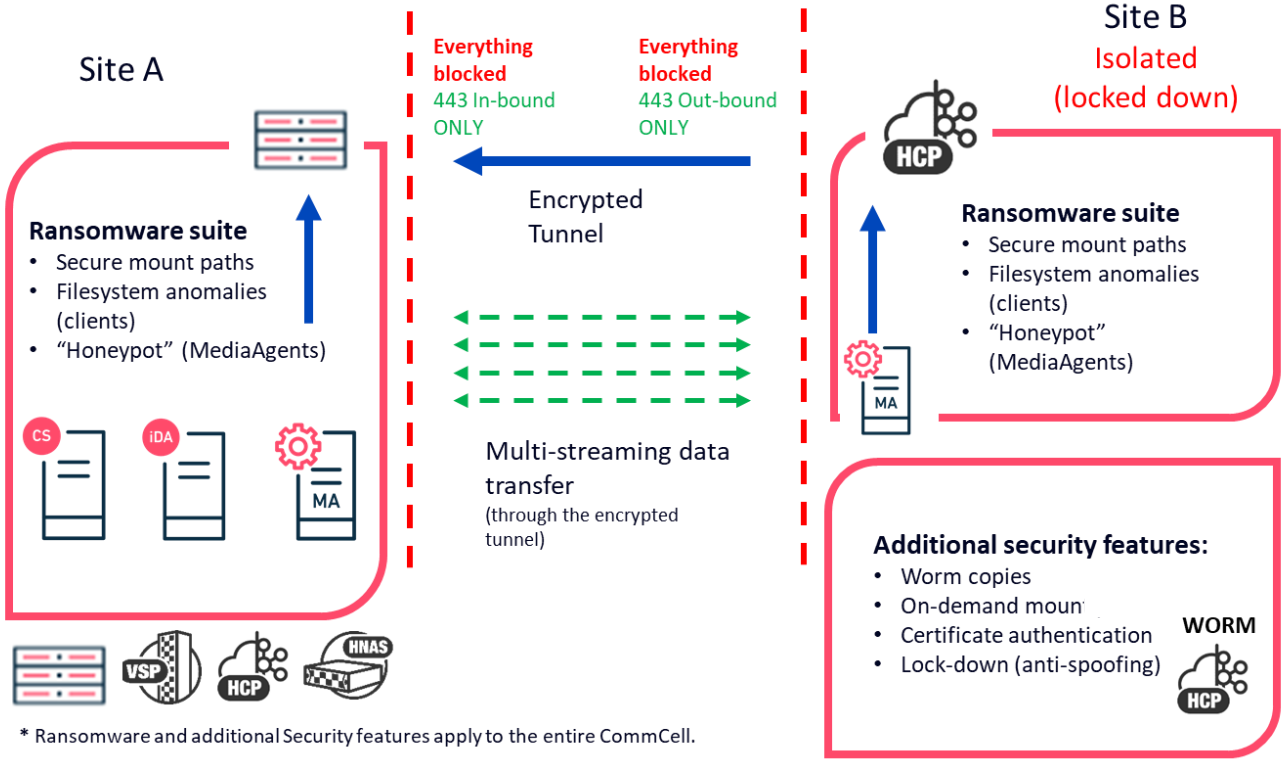


Figure 2

## Proxy/Network Gateway Connection

Proxy based configuration (Figure 3) 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.

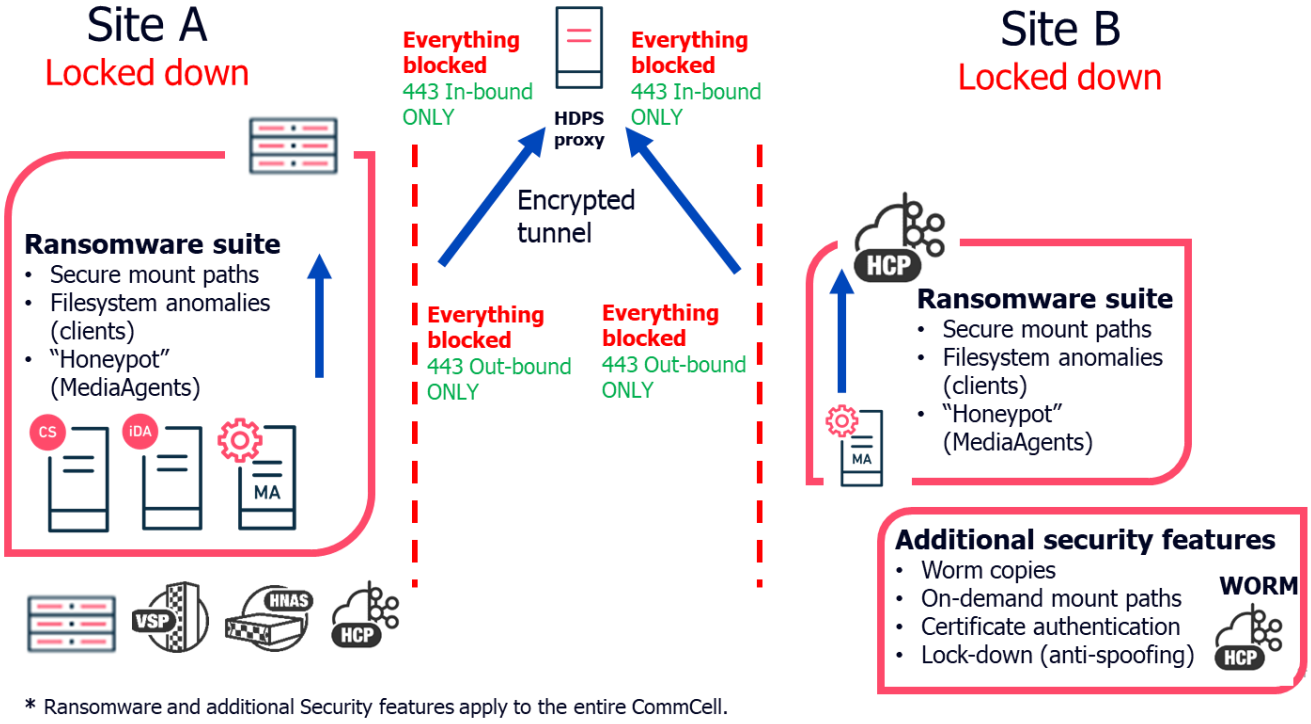


Figure 3

## Utilizing Hitachi Content Platform as the Storage Target

Being hardware agnostic is one of the HDPS key advantages. Object storage targets can be another strategic way of isolating backup data. The Hitachi Content Platform, is one of the most secure object stores in the industry. Its versioning and data immutability capabilities enrich and complement any existing ransomware strategy. Hitachi Content Platform Gateway extends these capabilities to remote/branch offices.

HCP has its own WORM and immutable locks built within the hardware platform. HDPS seamlessly integrates with those capabilities, while still managing retention, data encryption, and software application security controls.

HCP uses 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.

Learn More about HCP Portfolio and how it protects against Ransomware - https://www.hitachivantara.com/en-us/pdf/solution-profile/overcome-risks-ransomware-with-hcp-portfolio-solution-profile.pdf

### 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 the HDPS existing security controls and immutable locks (ransomware protection, WORM, S3 Object Lock and encryption), in combination with Data Isolation and Air Gapping techniques provides a well-protected solution. With HDPS and HCP you are recovery ready!

## Hitachi Vantara


Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com |community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact





WP-747-1 Author H/Vantara October 2020.