WHITE PAPER

Commvault® Cloud HyperScale X Security

INTRODUCTION

As the person responsible for backup management at your company, you've implemented detailed policies and designated storage for the backup of production data. Meeting SLAs and ensuring secondary and tertiary copies of data are made to recover from any issues is routine.

Now, the crucial question arises: **how do you protect these backups for successful recovery?**
Consider these scenarios:

What if . . .	The challenge is . . .
the backup admin accidentally tries to delete a backup job, policy, or library?	how can you protect your backup data from internal threats and mistakes?
an authorized user tries to encrypt, move, or delete files in the system or reformat a disk?	how can you respond to scenarios when ransomware infiltrates your environment?
an authorized user tries to modify or encrypt protected backup data on the storage?	how can systems prevent malicious users from tampering with backup data?
an unauthorized user makes an unsuccessful attempt to access the system?	how can you stay alert and one step ahead of an attempted cyber breach?

Implementing solutions with zero-trust principles is crucial for tackling these security challenges head-on.

Commvault's HyperScale X solution automates and simplifies the overall administration of backup management. It includes enhancements that simplify deployment for complex, security-focused networks, accelerating your time to first backup. In addition, Commvault follows zero-trust principles to help address the security challenges described before.

Here are five security initiatives that Commvault has implemented into its HyperScale X solution and how they help address these challenges:

1. HARDENED OS

The operating system is the core layer of any machine and must be functional before an application can run. It handles various aspects of hardware, software, memory, networking, IO, storage, and many other peripherals. It runs several modules and services to manage all these aspects and administers available network interfaces and ports.

Why is this Important?

As the number of running OS modules and interfaces increases, the surface area available to a potential attacker increases proportionately, thereby creating increased security risk.

Commvault's Capabilities

Commvault Cloud HyperScale X utilizes a specially configured and hardened operating system image for its nodes, eliminating unnecessary packages, services, and open ports. Combined with the built-in firewall, which is active by default, this reduces the associated risk of security vulnerabilities and increases the overall system's security posture.

The hardened OS images are available for the original cluster building and node expansion.

2. AUTOMATED MONTHLY OS SECURITY UPDATES

Hardening the operating system is the first step towards making it secure. Consistently maintaining the system's security is equally important.

Why is this Important?	Over time, new vulnerabilities in the operating system's modules can pose a security risk. Identifying, downloading, and regularly installing the necessary security updates for the OS can be arduous and is often overlooked. Running a system with open vulnerabilities increases the risk of a security breach.

Commvault's Capabilities

Commvault Cloud HyperScale X has a built-in feature to deliver and apply OS security updates as part of its automated patch update framework. Commvault continuously identifies necessary security updates for the operating system, tests them, and integrates them into its monthly software updates. Commvault's quality assurance team also proactively scans the supported OS and software stack for vulnerabilities.

This automated and systematic patching process covers the entire software stack, including OS security updates, to address potential zero-day vulnerabilities.

3. HARDENED "ROOT" USER ACCESS

Why is this Important?	The "root" user has unrestricted access to the entire system, making them a high-risk target for malicious users. If a malicious user gains access as "root," the user can cause irreparable damage that may go undetected until it's too late.

Commvault's Capabilities

Commvault has implemented two robust measures to minimize the risk of malicious users causing damage to systems.

Disabled "root" user access by default	The "root" user is disabled, including the SSH access as "root" user. During installation, a restricted shell user named "cvbackupadmin" is created instead. This restricted user has the necessary permissions to perform all backup admin activities and can effectively manage the system on a daily basis.
Enabling "root" user access requires multi-factor authentication and raises alerts	When "root" access is required, a multi-factor authentication mechanism is engaged to enable it. In addition, alerts are sent immediately when "root" access is requested and enabled.

Our zero-trust architecture improves ransomware protection by preventing unauthorized admin access to protected data. Even privileged users require sufficient authorization for admin access.

In the unlikely scenario where a rogue user is able to steal identity credentials and gain access to multi-factor authentication, the unauthorized activity is immediately flagged as a security event, which triggers an alert.

4. RANSOMWARE PROTECTION VIA MULTI-LAYER IMMUTABILITY

Why is this Important?	Built-in ransomware protection is a fundamental requirement of any modern cyber resilient product. However, data immutability alone does not constitute ransomware protection unless it is backed by secure and robust architecture throughout the software stack.

Commvault's Capabilities

Commvault Cloud HyperScale X has enhanced ransomware protection built-in and enabled by default. It provides multiple layers of immutability across the software, OS, and file system. These layers are designed with zero-trust principles to prevent protected data from being accidentally or maliciously encrypted, modified, or deleted. This provides data recovery in the event of an attack, reducing the risk of financial loss and business interruption due to a software breach while protecting backups from unauthorized data access. These immutable controls are enabled by default at the time of installation.

Commvault's three layers of immutability are:

Software

Misconfigurations and accidental deletions are a common issue for organizations. Commvault software supports WORM (Write Once Read Many) storage policies to prevent the accidental deletion of backup data from an authorized user, including a Commvault backup administrator. By leveraging Commvault's WORM capabilities, backup jobs that haven't met the defined retention rules cannot be deleted, even by a master user within the environment.

Operating System

SELinux (Security Enhanced Linux kernel extension) enhances immutability by providing access policies that restrict file modifications on mount paths and disk-level activities, such as reformatting drives. This protection at the OS level blocks unauthorized users and ransomware attacks through access controls that determine which actions can be performed by which users. With SELinux enabled, only specific and authorized Commvault processes can access stored data for necessary operations.

File System

Commvault's integrated scale-out file system (CVFS) provides immutability at the storage layer to prevent files in the backup mount path from being modified or encrypted at the file system level. This safeguards data at the storage IO level by preventing the bypass of security controls by accessing protected data directly from the Operating System.

The table below describes how the different layers help solve some of the challenges presented earlier.

Challenge	Immutability Layer	Solution
How can you protect your backup data from internal threats and mistakes?	Software (WORM storage policies)	If the backup admin attempts to accidentally delete a backup job, policy, or library, Commvault's WORM (write once, read many) storage policy denies the action.
How can you respond to scenarios when ransomware infiltrates your environment?	OS level (SELinux access controls)	If an authorized user tries to encrypt, move, or delete files or reformat a disk, the OS blocks users and/or ransomware attacks through SELinux defined access controls.
How can systems prevent malicious users from tampering with backup data?	CVFS (File system immutability)	If an authorized or malicious user tries to modify or encrypt protected backup data on the storage, the Commvault File System prevents backup data from being modified or encrypted.

When the immutability controls from Commvault File System and SELinux are combined with our WORM storage policies, customers benefit from robust and comprehensive ransomware protection, which helps mitigate a wide range of threats. Ransomware attacks are not a matter of if, but when they will occur. Commvault's multiple layers of immutability give you peace of mind that your data will be protected and easily recoverable in the event of a cyber incident.

5. SECURITY ALERTS

Why is this Important?	Even if a secure system hasn't been breached, malicious users or ransomware processes may still be lurking in the network trying to gain access. Detecting and stopping these threats early is crucial to preventing potential attacks.

Commvault's Capabilities

Commvault has implemented security alerts to detect rogue activity and validate that all events and activities are from known authorized users and processes.

Scenario	Action	How does it help?
When someone attempts a root login via SSH	An alert is sent	Upon receiving the alert, system admins can trace the event, verify if it was initiated by a known and authorized user, and take appropriate measures.
When someone enables root access	An alert is sent	
When someone disables ransomware protection	An alert is sent	
. . . and more	An alert is sent	

It is essential to stay updated on the latest security measures and risk mitigation plans to minimize cyber breaches. It is equally important to remain informed about events happening in the environment. Commvault alerts can help achieve both.

CONCLUSION

In response to the evolving threat landscape, Commvault is leading the charge towards cyber resilience. A key component of a cyber resilient product is embedded security built on zero-trust principles. Organizations must be confident that their critical business data is protected from ransomware, data breaches, and rogue users, all of which have the potential to cause substantial disruption to their business operations. Commvault implements a multi-layered approach to security, incorporating hardened systems and immutable storage for HyperScale X. Various controls within our software, file system, and operating system prevent malicious or unintended modification of protected data. These security measures are available for Commvault Cloud HyperScale X Appliances and Reference Architecture models.

Our top priority is the security of our customers' data. The "secure by design" principles of Commvault Cloud HyperScale X enable us to deliver one of the most secure enterprise scale-out storage solutions in the market today. This gives customers confidence that their critical business data remains available when needed most.