White Paper

Hitachi Mainframe Cyber Resiliency Solution

Protect Your Mainframe Data and Adapt to Any Adverse Conditions

Hitachi Vantara

White Paper

Table of Contents

Protect your mission-critical mainframe data with a physical air gap, without any impact to host access and input.

Executive Summary

With over 45 years of experience supporting IBM® mainframe environments, Hitachi Vantara is committed to continued support and innovation for these environments. We provide new innovative storage solutions designed to improve storage processing, performance, availability, recoverability and management in mainframe environments.

Data is the fuel of today's economy, and mainframe environments have a large quantity of corporate data to be protected against malicious attacks or logical corruption. AI is adding a need for always-on data access. As one of the major storage providers in the mainframe arena, Hitachi Vantara has worked to provide a solution to help organizations provide resiliency against cyber attacks. The mainframe environment has been the most secure environment for several decades, and security has always been at the heart of its developments.

Mainframe Security Initiatives and Innovations

Here are some mainframe security initiatives examples:

- Mainframe resource control access security products have been around for decades and are being adapted to today's world security requirements.
- Data-at-rest encryption (DARE), including integration with key management systems is available on storage systems and has been implemented on Hitachi storage for a long time. It is compliant with FIPS 140-3 level 2.
- IBM FICON® with IBM Fibre Chanel Endpoint Security (IFCES) validates the connectivity by checking the source, and it targets WWNs and encrypts data between the host and storage over the SAN network.

Hitachi has been at the the center of mainframe innovations, including:

- Introduction of mainframe thin provisioning.
- Introduction of 100% data availability storage in 1995.
- Introduction of asynchronous replication pull technology.
- Introduction of eight 9s of storage availability in 2019, still unchallenged.

Cyber Attacks Are on the Rise

Cyber attacks on strategic industry targets have increased dramatically in recent years. For example, hospital, energy, transportation and supply chain operations have been targeted, as their essential services increase pressure to have the ransom quickly paid. One vicious approach, also increasing, is to steal insurance lists of companies covered against ransomware payment and targeting them.

Some analysts' reports indicate that despite paying the ransom, some companies did not recover data, and some recovered only partial data. The 2025 Cyberthreat Defense Report (CDR) from CyberEdge Group* , reported that only about 50% of organizations actually recover their data after paying ransoms to cybercriminals.

In one example of a cyber attack, the ransom was paid, but the decrypting tool provided by the attackers was so slow that the payee continued restoring systems from company's backups. Another study showed that paying the ransom cost double what a company not paying the ransom would spend to recover from the attack.

Nowadays, the decryption outcome is still unpredictable. In many cases, states are enacting laws to prevent companies from paying ransomware, and companies have taken measures to have immutable and resilient backup strategies.

Cybercriminals are using techniques that are increasingly sophisticated, such as taking advantage of AI. AI is now also used to generate malware, enhancing attack scale and efficiency.

In mainframe environments, the stated highest risk is data exfiltration or theft of sensitive data, followed by insiders' attacks (associated with stolen credentials). With data exfiltration, some criminal groups run a con or extortion racket:

1. They fraudulently offer legal assistance to the company to gain access to and exploit company data.
2. If they determine that the data they have acquired from the company contains any violation of local laws, the criminals take advantage of this by filing a lawsuit to exploit the company.

Emerging regulations regarding cybersecurity and easiness of recovery are either guidelines or laws already in place [U.S. Federal Financial Institutions Examination Council (FFIEC), U.S. National Association of Insurance Commissioners (NAIC), European Banking Authority (EBA), European commission: Digital Operational Resilience Act (DORA), NIS2, Hong Kong Association of Banks (HKAB) with Secure Tertiary Data Backup (STBD) Guideline, etc.] or will have to be implemented before a certain date.

The Hitachi storage solution is unique in using in system or standalone open systems storage to protect mainframe data, providing physical as well as administrative separation.

Hitachi Vantara Has Unique Cybersecurity Approach

Hitachi Vantara provides a solution to safely store an organization's consistent images of production in a fortress storage subsystem that is unknown from mainframe, allowing a quick restore of the data. Moreover, the Hitachi storage solution is unique in using in-system or standalone open systems storage to protect mainframe data, providing physical as well as administrative separation.

Physical separation from primary mainframe storage is very important. The separation ensures that, should the production primary subsystem be lost, production data images can still be mounted and restored on another Hitachi mainframe storage system (located up to 100km away from the storage).

These images are mountable on an LPAR, giving you the capability to validate the data, to do forensic analysis, and eventually use them for surgical restore or full restore of data should a disaster occur.

For multivendor environments, Hitachi Vantara and our partner BMC (AMI Vault) offer a solution that meets the requirements for cyber resiliency. The data is stored on Hitachi Content Platform, which allows you to make your stored data immutable with reduced million service units (MSU) needs as data is moved by a process running on the IBM System z® Integrated Information Processor (zIIP).

Cyber Resiliency Definitions

To gain a full sense of what cyber resiliency encompasses, consider these definitions, from:

The U.S. National Institute of Standards and Technology (NIST): Cyber resilience is defined as the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources.

Stockholm University: Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite adverse cyber events.

Kjell Hausken, Faculty of Science and Technology, University of Stavanger, Norway: The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously, at all times.

Current Solutions To Protect Data

At the lowest level, the hard disk drive or solid-state disk (HDD or SSD), some protection is possible. In the case of dynamic sparing, Hitachi storage performs a low-level format of the disk to erase data before maintenance replaces the failing disk.

When the storage is encrypted with data-at-rest encryption, cryptographic erasure (media sanitization) of data is performed when an internal encrypted drive is removed from the storage system. At Hitachi, we have long-term experience across industries globally addressing enterprise security concerns, which is why we've designated a different encryption key for each disk in our storage. Midrange and high-end Hitachi storage platforms can be encrypted. In fact, the data on the Hitachi Vantara Virtual Storage Platform One Block High End (VSP One Block High End) can be encrypted using AES 256-bit keys, quantum safe, with each internal drive having a different key. Keys can be generated, stored and backed up on your key management server or self-created by the storage.

In the mainframe space, Hitachi Vantara offers two different solutions to create disk-to-disk or snapshot copies: IBM FlashCopy® (version 2 and space efficient), as well as Hitachi ShadowImage for Mainframe. Both internal replication technologies allow disk-to-disk copies and fast recovery.

FlashCopy is frequently used for nondisruptive backup due to tight integration with products like IBM DB2®. FlashCopy does not perfectly fit to take a consistent image of a large configuration as, in order to get data consistency, there is a need to freeze the I/Os the time to add all pairs to populate the consistency group.

ShadowImage has a unique feature called "at-time split," allowing the software to take a consistent image of all production data at once, suspending pairs on the fly, based on the server-written timestamps on source volumes. This allows a consistent point-in-time copy without the need to perform a freeze. The ShadowImage at-time split feature applies to small as well as very large configurations. Based on timestamps, it allows consistency across different controllers to be achieved.

The consistent ShadowImage copies of the production data can be used as a basis to restore data, disk to disk, but more likely will be used in a disk-to-disk-to-virtual-tape or cloud paradigm.

Full copies and snapshot copies reside on the same array as the production data, which does not protect against physical array failure. Moreover, snapshots like FlashCopy space-efficient volumes require the production data as source to recreate the full data.

Regular checking of the backup data is not an easy process, so this generally does not address the requirements for a cyber resiliency solution.

Organizations usually create a data protection level by using replication to a different location, with two, three or even four different locations. Unfortunately, replication propagates the logical corruption to all sites and is not meant to recover from cyber attack or from logical corruption.

In the case of cyber attack, backups would need to be restored to validate that the data is healthy before recovering production data. Regular checking of the backup data is not an easy process, so this generally does not address the requirements for a cyber resiliency solution.

Hitachi Vantara and our partners offer a solution for virtual tapes using appliances (Luminex or Secure Agent), or not (Rocket Software, BMC AMI Cloud, VTFM New Gen). The current trend is to copy data to Amazon S3 storage (over IP with S3 interface to cloud or object storage like Hitachi Content Platform, for example). One of the advantages of the cloud/object storage solutions is the immutability of the data, as the object storage is acting like a write once, read many (WORM), with a pre-set expiration date.

Hackers are targeting backups (to infect or destroy them) to be very sure to lock down organizations and put more pressure on them for the ransom. The other advantage of these solutions is reduction of MSU consumption by using zIIP to move data (BMC AMI Cloud or Log-On Software VTFM New Gen, which are also very competitive to IBM's Transparent Cloud Tiering and IBM Cloud Tape Connector for z/OS.

While all these solutions have their utility in a mainframe production environment, none of these are protecting companies from a cyber attack with minimal data loss. Therefore, Hitachi engineered a mainframe cyber resiliency solution to address this specific need.

Hitachi Mainframe Cyber Resiliency

Requirements of an Effective Cyber Resiliency Solution

- Capability to make multiple copies of the whole production data without impacting production.
- Isolation from the mainframe storage to avoid 1) unwanted access to data 2) modification to production images.
- Possibility to recover data to a different storage unit than the main one (the one used to create the fortress images), should the primary mainframe storage be unavailable or considered as a crime scene by authorities (kept as is for further investigations).
- Capability of having more than a single primary storage source for the fortress.
- Immutable production images — no possibility to access, modify or delete the fortress data within retention period.
- No possibility given of removing the fortress copies retention period, as this would allow data to be modified or deleted within the fortress.
- Automated process, with alerting mechanisms.
- Possibility to give solution management outside of the mainframe team for complete isolation.
- Capability to protect mainframe storage locally or remotely.
- Capability to have multiple plans/schedules for taking the images.
- Capability to do on-demand backups and manage them independently of the regular images.
- Any critical management action protected with dual acknowledgement.
- High-availability solution.
- Fortress may reside on a different site than the primary storage.
- Enough consistent images to achieve business goals.

Elements of the Hitachi Solution

- **ShadowImage at-time split feature,** which can provide a consistent incremental copy of production, without the need to freeze I/Os, and can be combined with Hitachi Remote Replication to provide a remote point-in-time copy.
- **Storage virtualization,** which allows use of an open external storage connected via Fibre Channel.
- **Hitachi Thin Image Advanced snapshot capability,** which takes advantage of the advanced data reduction and redirect on write technology features. It also secures snapshot data, protecting it from any modification/deletion.
- **Hitachi Dynamic Provisioning for Mainframe** 38Mb pages on-demand.
- **Hitachi Business Continuity Manager** (BCM).
- **Proven high availability.**
- **Linux for IBM Z** (running on a Z series server)
- **Ansible templates,** used to synchronize images, triggering scripts to capture the modifications, or mounting images.

Image-Storing Process

Hitachi Mainframe Cyber Resiliency solution uses the unique capabilities of Hitachi storage to provide an advantageous image-storing process.

At regularly scheduled intervals, the image-capture process is triggered, creating consistent I/O ShadowImage copy using the at-time split feature. The copy is a point-in-time consistent copy, often referred to as "crash consistent." Administrators can define multiple cycles.

The image is stored on a virtualized open systems storage attached to the mainframe disk array using Fibre Channel connectivity. Or, it can be stored in the same storage, under format of open system LUN/s, which aggregate the multiple mainframe volumes.

The virtualization layer of the VSP One Block High End systems allows multiple mainframe volumes to be aggregated into a single open systems LUN. This approach helps to reduce management overhead on the virtualized array. Ansible triggers the process of taking consistent image from the primary storage.

As soon as the delta image of the production is stored on the open systems LUN/s, Ansible triggers a secure snapshot on the virtualized array, capturing the current delta image in the fortress and informing the mainframe host when the process is over.

The fortress protects the snaps from any access so that no change is possible to the stored images. Each point-in-time copy has a retention period associated to it that cannot be removed. The end of the retention period corresponds to the date and time this image will be deleted from the fortress.

The Mainframe Cyber Resiliency solution is then ready for the next image cycle.

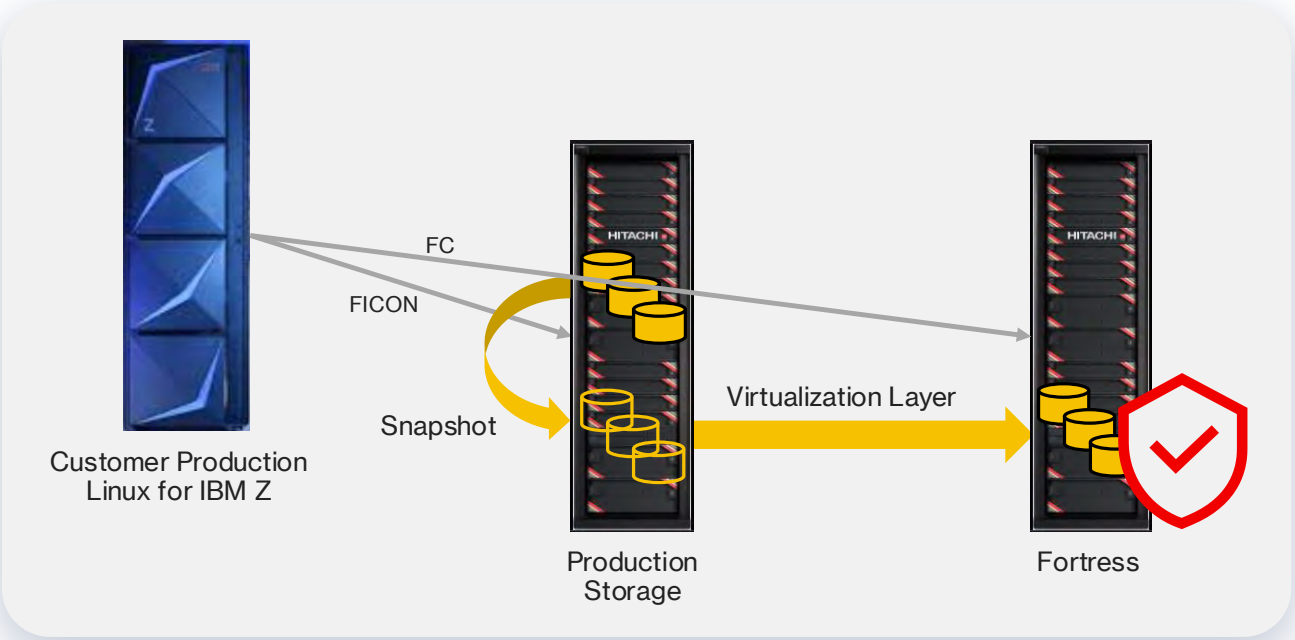

Figure 1. Hitachi Mainframe Cyber Resiliency Solution on primary site with external storage.

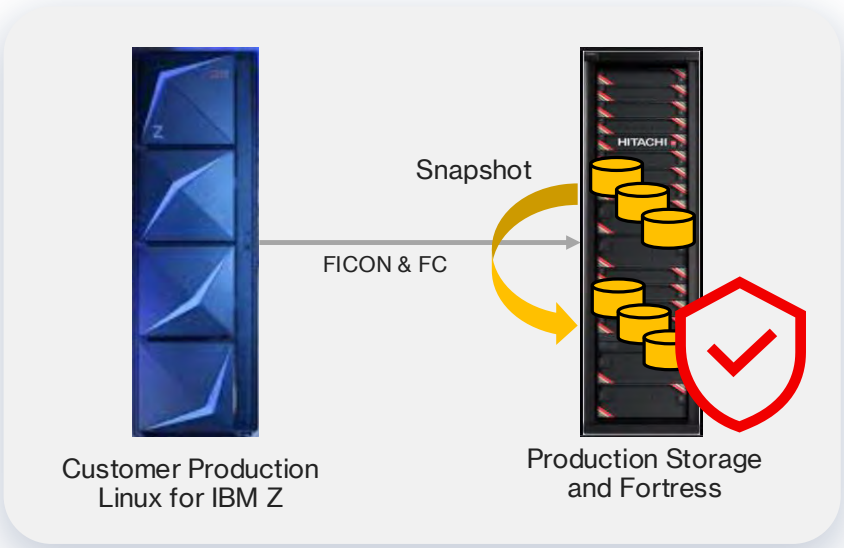

Figure 2. Hitachi Mainframe Cyber Resiliency Solution on primary site.

It is possible to store up to 1,022 generations of a single volume in the fortress.

The fortress is not necessary on the same site as the source mainframe storage, which provides another airgap (up to 100km).

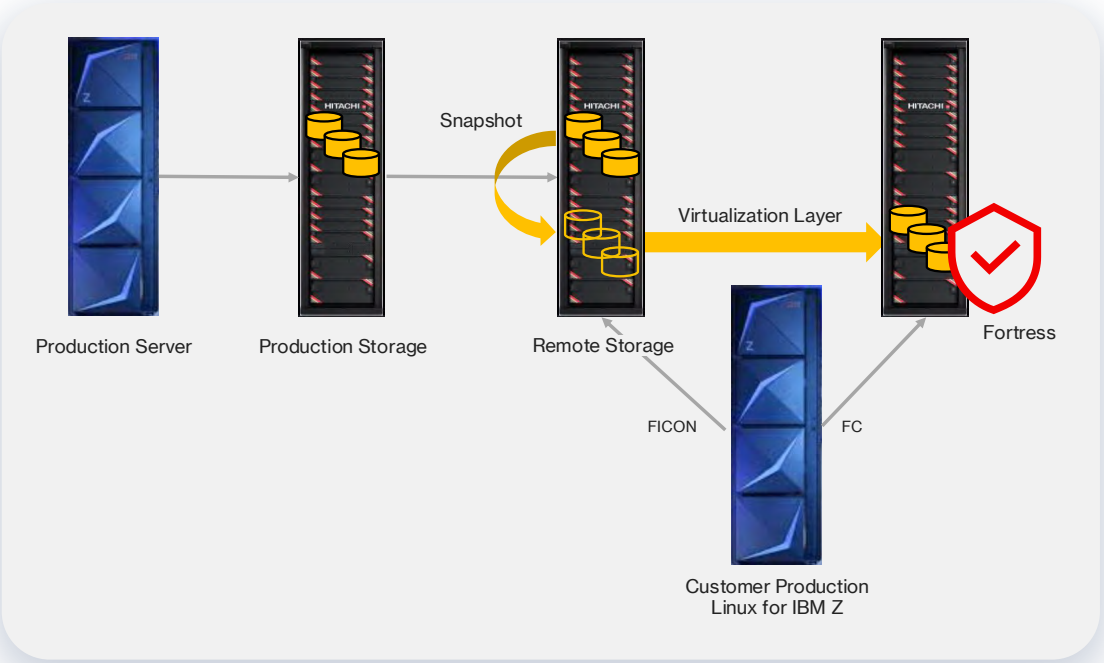

Figure 3. Hitachi Mainframe Cyber Resiliency Solution on a remote site.

In Figure 3, the fortress is on the remote site. BCM script running on the IBM Z series server on primary site triggers the new generation capture on the remote site using in-band commands.

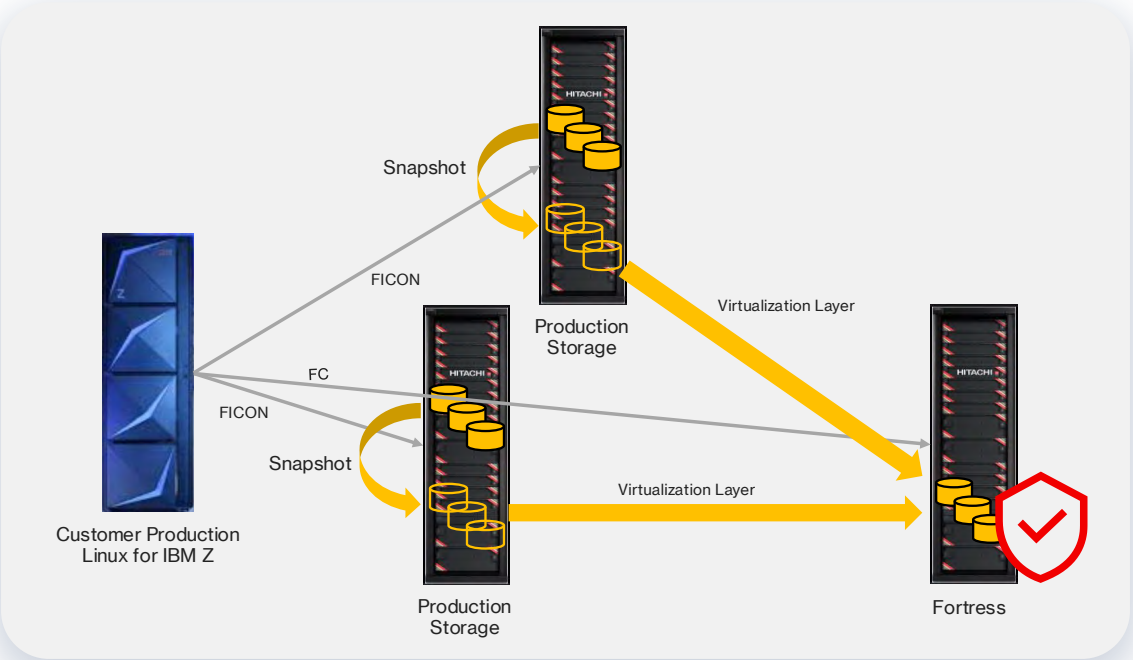

Figure 4. Example of two primary storage virtualized to a single fortress.

Note that there is an integration of Hitachi Business Continuity Manager and a mainframe security product like IBM RACF® or similar, allowing the ShadowImage at-time split pairs to remain unknown unless authorized to be aware of them.

Accessing Stored-Images Process

It is possible for a storage administrator to choose from the various consistent images stored in the fortress and expose their selection/s to a mainframe.

The fortress data volumes cannot be mounted directly to the mainframe. To create another airgap and add another layer to protect the images, the data is mapped on to a verification volume that is shown to the mainframe. This verification volume can be read and written as needed. Figure 5 shows the complete picture.

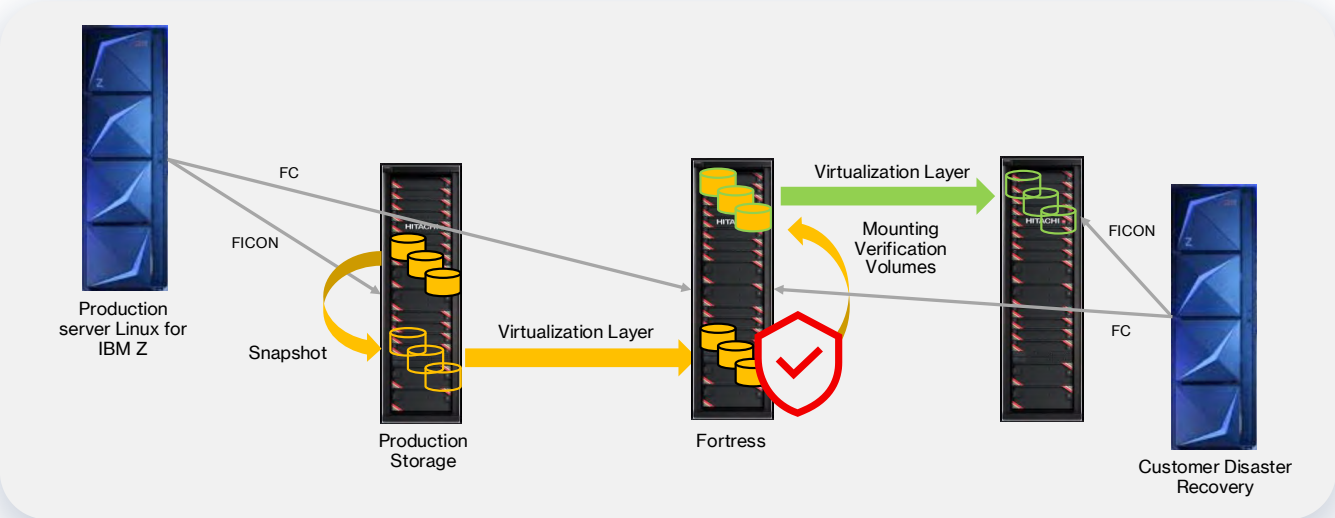

Figure 5. Hitachi Mainframe Cyber Resiliency solution: Example of mounting an image to an IBM z/OS® on different storage.

The verification volume can be mounted on the same storage as primary storage or on a different storage system.

- Mainframe access to the recovery volume is immediate once mounted, and there is no need to restore the data on the mainframe storage to access that volume.
- As soon as the image is mounted, it is possible to go through a checking phase to validate that no data has been corrupted.
- All modifications made to that mounted image are discarded when the image is unmounted.

Should a corruption be discovered in production, your experts can start forensic analysis to validate whether the corruption can be recovered and corrected with data from the stored images and brought back into production environment. Your staff may have to mount different copies to understand the root of the corruption or to find valid data to restore.

In that situation, your administrators may restore part of the data as valid data on the production system that was corrupted. This helps your organization avoid losing too many data updates and only corrects the infected one.

For some cases this approach is not sufficient for the administrator to use the controls to restore just the infected data. An alternative approach would be to restore the full data set from the last valid fortress data.

The Mainframe Cyber Resiliency solution may be completed by other solutions to restore subsystems like DB2. Some organizations make a copy of the DB2 databases to S3 object storage and store the image copies on S3 storage as well as archive logs. This allows them to restore the DB2 database prior to the corruption and apply the DB2 logs up to the corruption point.

Helping You Recover From Data Corruption

Hitachi Mainframe Cyber Resiliency provides a lot of advantages:

- Create the consistent image without the need to freeze I/Os.
- Create the consistent image without burning MSUs.
- Store the consistent image in the fortress without burning MSUs.
- Automated process creates consistent images in the fortress.
- Fortress can be target of multiple storage sources.
- Images taken do not reside on the source mainframe storage.
- Source mainframe storage does not have to manage multiple copies.
- No overhead on the mainframe storage for multiple snap management approaches.
- Images stored in open system storage creates an airgap.
- Management of the fortress outside of mainframe creates an airgap.
- The fortress can be isolated as it does not need to be physically on the same site as the mainframe storage.
- Up to three different recovery volume sets can be mounted at the same time.
- Any fortress image does not necessarily need to be restored to its source storage.
- Multiple mainframe devices are consolidated into single open system LUN.
- Up to 1,022 different protected consistent images of a set of volumes can be kept in the fortress (up to 1022 images of a single volume).
- The data in the fortress is immutable, protected from being modified or deleted.
- Fortress retention period of the different images cannot be removed.
- Critical administration actions (on the cycles or the fortress content for example) implies two user acknowledgements (changing image cycles or modifying the retention period, for example).

Why a Fortress?

Data inside is immutable, retention period for images cannot be removed, and its management outside of mainframe creates an airgap.

- Any image in the fortress can be exposed to a mainframe (for example for analysis up to restore process).
- The mainframe is not aware of the data copy as it resides on virtualized storage unknown by the mainframe.
- The solution is based on proven robust technology.
- You have the choice in the analysis tools as we provide the repository and the capability.
- The fortress can be used to store on-demand backup (these can be managed by the administrator).
- The Fortress on VSP One Block is taking advantage of the 4:1 compression No Question Ask should the data being not already compressed or encrypted

Cyber Security Partner Solutions

Hitachi Vantara partners with leading cyber security vendors.

Hitachi Partners With MainTegrity for Cyber Security

- Integration with Hitachi Cyber Resiliency Solution to point out the best image to restore from.
- Detects changes in critical libraries.
- Detects unwanted encryption and stop address space before the system has been harmed.
- Detects and stops unwanted data exfiltration.

Hitachi Partners With BMC for AMI Security

- BMC protects Advanced Metering Infrastructure (AMI) from cyber threats.
- BMC ensures integrity of data related to energy consumption and distribution, making sure that it remains confidential and available.
- The BMC solution includes MainTegrity.

Find out more about effective cyber resiliency solutions.

Learn more →

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

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

HV-BTD-WP-Hitachi-Mainframe-Cyber-Resiliency-Solution-13Aug25-A