HITACHI
Inspire the Next

WHITE PAPER

Hitachi Mainframe Cyber Resiliency Solution

Protect Your Mainframe Data and Adapt to Any Adverse Conditions

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

By Hitachi Vantara

Table of Contents

Executive Summary

Data is the fuel of today's economy and mainframe environments still power and process huge volumes of corporate data that needs to be protected against malicious attacks or logical corruptions. As one of the major storage providers in the mainframe arena, Hitachi Vantara has developed a solution that helps customers ensure resiliency against cyberattacks. The mainframe environment has been the most secure environment for several decades, with security has always at the heart of its developments.

Here are some mainframe initiatives examples:

- Mainframe resource control access security products have been around for decades and are being adapted to the today's world security requirements.
- Data-at-rest encryption, 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 level 2.
- IBM FICON® with Encryption of Data in Flight (eDiF) encrypts data between the host and storage over the SAN network. At the time of this writing, Hitachi Vantara expressed its intent to support this functionality.

Rise of cyberattacks on strategic targets has dramatically increased in recent years. For example, hospitals and the vaccine supply chain itself have been targeted, using their need to address Covid-19 as a means of pressuring them into quickly paying the requested ransom. A more vicious attack, which is showing the highest increase, steals insurance lists of companies covered against ransomware payment and targets them.

Some analysts' reports indicate that despite paying the ransom, some companies did not recover their data, and some recovered only partial data. At the same time, according to CBS News, 80% of organizations that previously paid ransom demands confirmed they were exposed to a second attack. Today, only 14% of the companies attacked did recover 100% of their data after paying ransomware, according to ESG study, "2022 Ransomware landscape". In one example from 2022 where the ransom was paid, the decrypting tool provided by the attackers was so slow that the payee had to continue restoring systems from company backup. Another study showed that paying the ransom cost double what a company not paying the ransom would spend to recover from the attack.

The cybercriminals are using techniques that are more and more sophisticated, such as aiming to destroy or corrupt backup data to prevent recovery. The World Economic Forum Global Risks Report from 2019 ranks cyberattack risk 5th out of 10 and forecasts a potential cost of up to 90 trillion in net economy impact by 2030.

Emerging regulations regarding cybersecurity and eases of recovery are either guidelines already in place (US Federal Financial Institutions Examination Council -FFIEC-, US National Association of Insurance Commissioners -NAIC-, European Banking Authority -EBA-, Hong Kong Association of Banks – HKAB- with Secure Tertiary Data Backup (STBD) Guideline, ...) or will have to be implemented before Jan 17, 2025 per the European Commission: Digital Operational Resilience Act ('DORA').

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

Physical separation from the 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.

These images are mountable on a logical partition (LPAR), giving the customer the capability to validate the data, to do forensic analysis, and eventually used them for surgical restore or full restore of data should a disaster occur.

For multivendor environments, Hitachi Vantara and our partner Model9 offer a solution that meets the requirements for cyber resiliency. The data stored on Hitachi Content Platform allows organizations to make their 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 a 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. All midrange to high-end Hitachi storage platforms can be encrypted. The data on Hitachi Virtual Storage Platform (VSP) 5000 series can be encrypted using AES 256-bit keys, with each internal drive having a different key. Keys can be generated, stored, and backed up on a customer key management server or self-created by the storage.

Hitachi Vantara offers two different family solutions to make disk to disk or snapshot copies: IBM FlashCopy® and FlashCopy® space efficient compatibility, 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 such as IBM DB2®. FlashCopy® is not perfectly fit to take a consistent image of a large configuration as, to get data consistency, FlashCopy® must freeze the I/Os, during a period of time, in order to add all the volumes 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 writes timestamps from source volumes. This allows a consistent point-in-time copy without the need for a freeze. The ShadowImage at-time split feature applies to small as well as very large configurations. Based on timestamps, consistency across different controllers can 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.

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 such as FlashCopy® space efficient volumes require the production data as source to create the full data.

Usually, customers do also have a data protection level 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 cyberattack or from logical corruption. In the case of cyberattack, backups would need to be restored to validate that the data is healthy before recovering production data. Regular check of the backup data is not an easy process, so it does not address the requirements of a cyber resiliency solution.

Hitachi Vantara and our partners offer a solution for virtual tapes using appliances (Luminex or Secure Agent), copying data to the cloud (over IP with Amazon S3 interface to Hitachi Content Platform, for example) while reducing the MSU consumption by using zIIP to move data (Model9, which is also very competitive to Transparent Cloud Tiering and Virtual Tape Connector). Eventually, the backup data could potentially be infected or destroyed, as hackers are now targeting the backups to be very sure to lock down customers.

While all these solutions have their utility in a mainframe production environment, none of these protect companies from a cyberattack 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 unwanted access to data and any modification to production images.
- Possibility to recover data to a different storage than the main one used to create the fortress images, should the primary mainframe storage be unavailable or considered as a crime scene—kept as is for further investigations.
- Capability to do have more than a single source primary storage for the fortress.
- Immutable production images, no possibility to access, modify or delete the fortress data within retention period.
- No possibility of removing fortress copies retention period, as this would allow data to be modified or deleted in the fortress.
- Automated process, with alerting mechanisms.
- Management of the solution outside of the mainframe 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.
- Any critical management action protected with dual acknowledgement.

- High-availability solution.
- Fortress may reside on a different site than the primary storage.
- Sufficient number of consistent images.

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 open systems snapshot capability.
- Hitachi Data Retention Utility, which protects data from any modification.
- Hitachi Ops Center Automator, which synchronizes the images and triggers the scripts to capture the modifications.
- Hitachi Dynamic Provisioning for Mainframe, which allows allocations in open, based on a 38MB on demand and returned to the pool if unused or freed up.
- Hitachi Business Continuity Manager (BCM).
- Proven high availability.

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 I/O consistent ShadowImage copies 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 under format of single Open System LUN which does aggregates the multiple Mainframe volumes.

The virtualization layer of the VSP 5000 series 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. Hitachi Ops Center triggers the process of taking a consistent image from the primary storage.

As soon as the delta image of the production is stored on the open systems LUN, Hitachi Ops Center Automator triggers a 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 with it that cannot be shortened or 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.

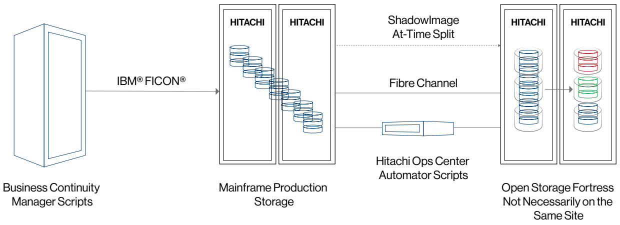

IBM® FICON®
HITACHI
HITACHI
ShadowImage At-Time Split
Fibre Channel
Hitachi Ops Center Automator Scripts
HITACHI
HITACHI
Business Continuity Manager Scripts
Mainframe Production Storage
Open Storage Fortress Not Necessarily on the Same Site

Figure 1. 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.

As mentioned in Figure 1, the fortress is not necessary on the same site as the source mainframe storage, providing another air gap.

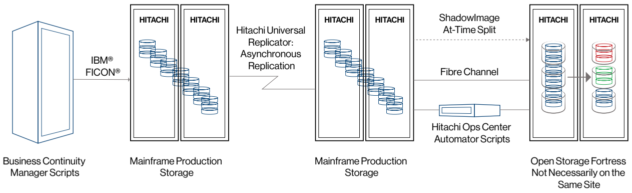

IBM® FICON®
HITACHI
HITACHI
Hitachi Universal Replicator: Asynchronous Replication
HITACHI
HITACHI
ShadowImage At-Time Split
Fibre Channel
Hitachi Ops Center Automator Scripts
HITACHI
HITACHI
Business Continuity Manager Scripts
Mainframe Production Storage
Mainframe Production Storage
Open Storage Fortress Not Necessarily on the Same Site

Figure 2. Hitachi Mainframe Cyber Resiliency Solution on Remote Site

In Figure 2, the fortress is on a remote site. BCM script running on the z-server on primary site does trigger the new generation capture on the remote site using in-band commands.

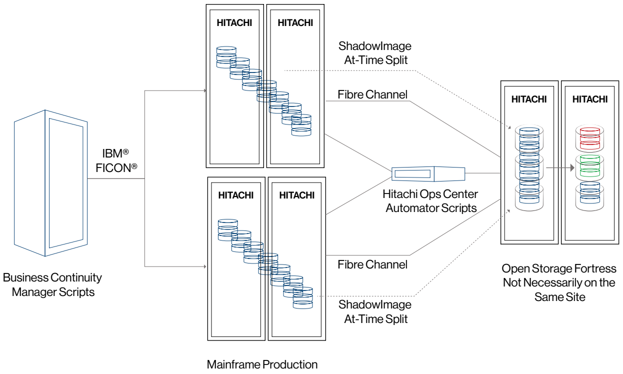

HITACHI
HITACHI
ShadowImage At-Time Split
Fibre Channel
HITACHI
HITACHI
IBM® FICON®
HITACHI
HITACHI
Hitachi Ops Center Automator Scripts
Fibre Channel
ShadowImage At-Time Split
Business Continuity Manager Scripts
Open Storage Fortress Not Necessarily on the Same Site
Mainframe Production

Figure 3. Example of Two Primary Storage to a Single Fortress

Note that there is an integration of Hitachi Business Continuity Manager and a mainframe security product such as IBM RACF® or similar (HBCM extended access control), 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 across the various consistent images stored in the fortress and expose them to a mainframe.

The fortress data volumes cannot be mounted directly to the mainframe. To create another air gap 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 3 shows the complete picture.

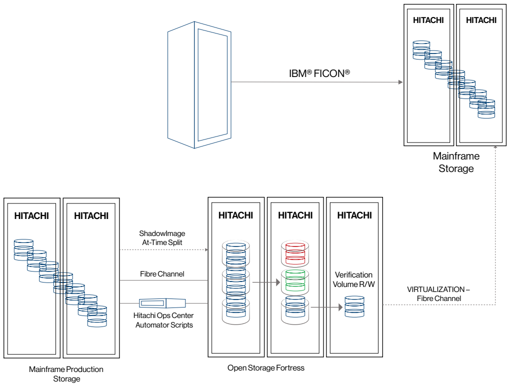


Figure 4. Hitachi Mainframe Cyber Resiliency Solution: Example of Mounting an Image to an IBM z/OS® on Different Storage

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

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.

Should corruption be discovered, customer experts can make a decision regarding production, and start forensic analysis to validate whether the data corruption can be recovered and corrected data brought back into production environment. You may have to mount earlier copies to understand the root of the corruption or to find valid data to restore.

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

For some cases this is not sufficient. It is then possible to restore data from the last valid data from the fortress.

Helping You to Recover From Data Corruption

Hitachi Mainframe Cyber Resiliency provides a lot of advantages to our customers:

- Consistent image created without the need to freeze I/Os.
- Creation of consistent image without burning MSUs.
- Storing the consistent image in fortress without burning MSUs.
- Automated process to create consistent images in the fortress.
- Fortress can be targeted from multiple storage sources.
- Image taken does not reside on the source mainframe storage.
- Source mainframe does not have to manage multiple copies.
- No overhead on the mainframe storage for multiple snap management approaches.
- Images stored in an open system storage create an air gap.
- Management of the fortress outside of mainframe creates an air gap.
- 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 or shortened.
- Administration critical action (on the cycles or the fortress) implies two user acknowledgements.
- 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.
- Customer has 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).

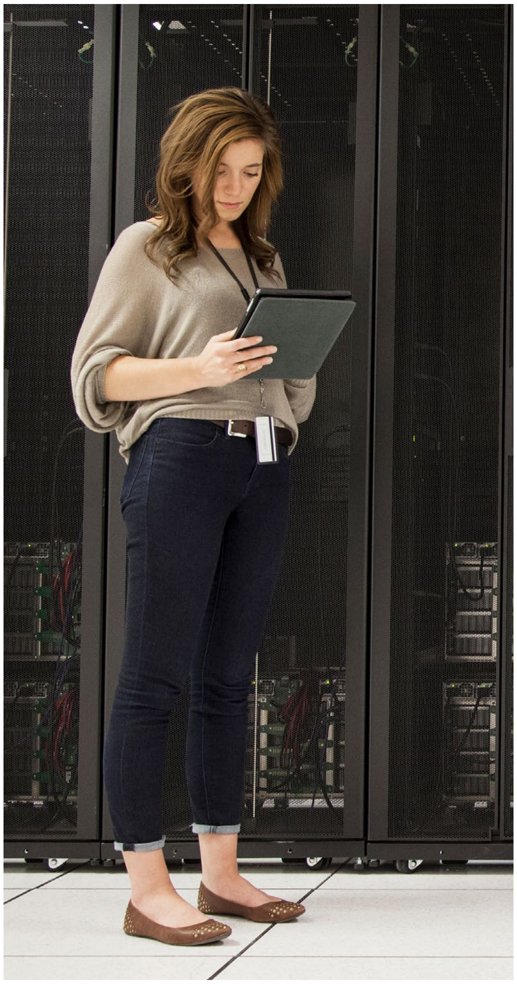
With more than 40 years of experience supporting IBM® mainframe environments, Hitachi Vantara is committed to continued support and innovation for these environments. We provide new innovative storage solutions designed to improve storage processing, performance, availability, recoverability, and management in mainframe environments.

Adding Cyber Security to Cyber Resiliency

To help customers create improved enterprise cybersecurity defenses Hitachi Vantara is partnering with MainTegrity® to bring File Integrity Monitoring to mainframes. MainTegrity's product, FIM+®, detects and alerts customers to unsanctioned changes to system and application software such as Ransomware and Malware. FIM+® also provides continuous monitoring to protect against insider attacks.

This complements the HV Cyber Resiliency Solution by preventing malicious attacks, but also improves resiliency by making recovery from HV snapshots simpler and faster Specifically FIM+® can speed up situational analysis with powerful forensic tools, display available HV snapshots, and perform a surgical recovery of system software to a trusted state. FIM+® can also scan/validate the images in the Fortress.

Please contact your Hitachi Vantara representative for more information.



ABOUT HITACHI VANTARA

Hitachi Vantara, a wholly-owned subsidiary of Hitachi Ltd., delivers the intelligent data platforms, infrastructure systems, and digital expertise that supports more than 85% of the fortune 100. To learn how Hitachi Vantara turns businesses from data-rich to data-driven through agile digital processes, products, and experiences, visit hitachivantara.com.

Learn More →

Find out more about
Hitachi mainframe solutions

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

© Hitachi Vantara LLC 2023. All Rights Reserved. HITACHI is a registered trademark of Hitachi, Ltd. IBM and DB2 are trademarks or registered trademarks of International Business Machines Corporation. All other trademarks, service marks and company names are properties of their respective owners.