ADVANCED TECHNOLOGY GROUP (ATG)

Accelerate with ATG Webinar:

IBM Cyber Vault Introduction 101

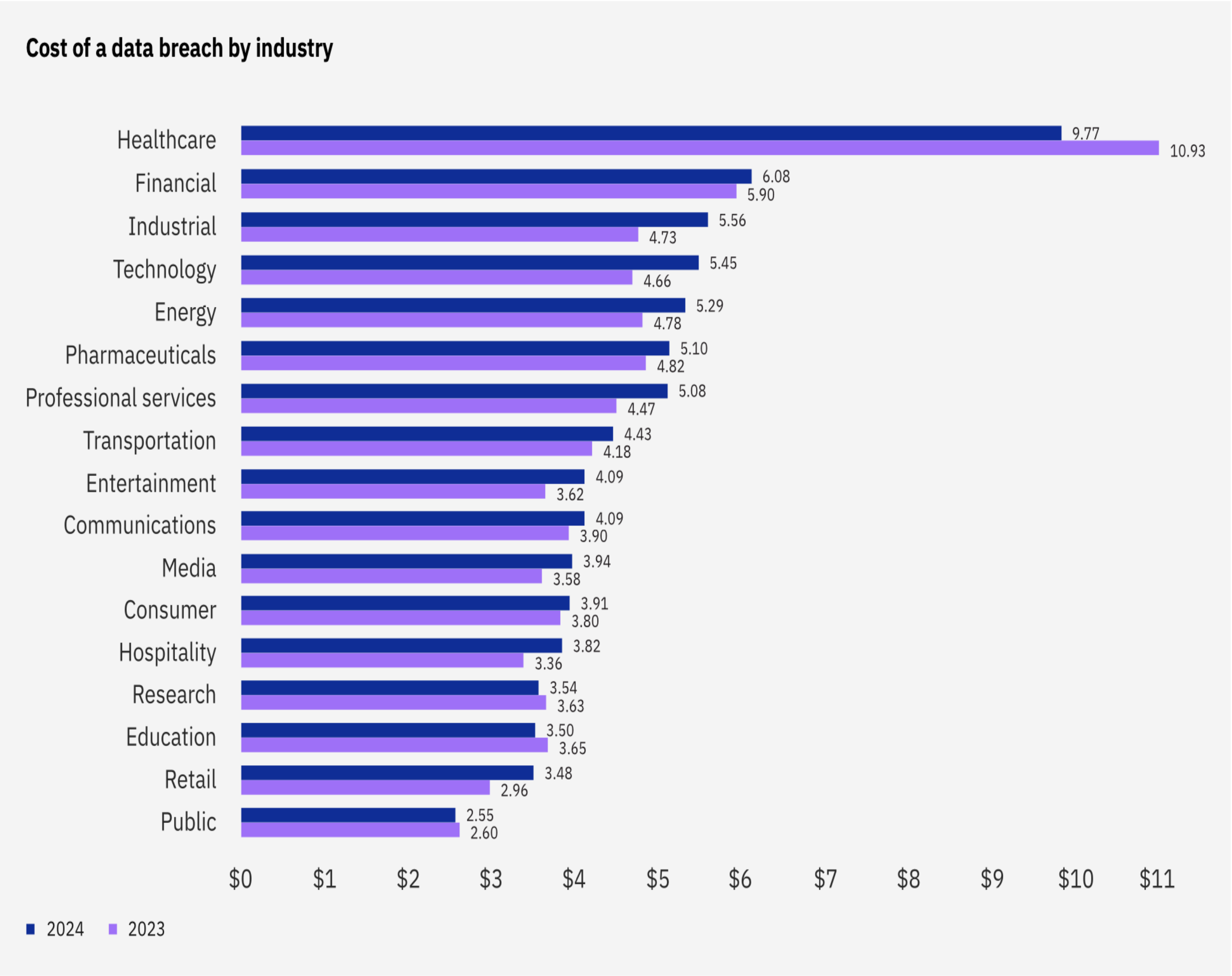
Thomas Bish
STSM - Storage Technical Specialist
IBM Advanced Technology Group
tbish@us.ibm.com

Meet the Speakers

Tom Bish has been with IBM for 35 years and is an IBM Senior Technical Staff Member, Principal Architect, and Master Inventor. Tom was in IBM storage product development and architecture for 25 years, and then joined IBM Global Technology Services to define their software define storage strategy. Tom is currently within IBM Advanced Technology Group (ATG) within technical sales to help clients and sellers best utilize IBM storage technologies.

Average cost of a US data breach

$9.36 million



Cost of a data breach by industry

Measured in USD millions

Source: IBM Cost of a Data Breach report 2024

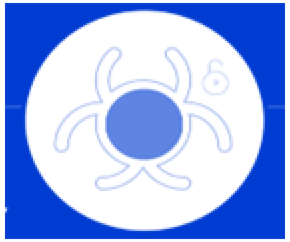
Destructive attacks that left systems inoperable accounted for one out of every four attacks, and another 24% involved ransomware.[1]

$5.24M

The average cost of a destructive attack. [1]

12%

Share of data breaches originated from a software supply chain attack.[1]



$1.76M

Lower data breach costs compared to organizations that didn't use security AI and automation capabilities. [1]

25%

Share of malicious attacks that rendered systems inoperable. [1]

Share of total breaches by type of malicious attack

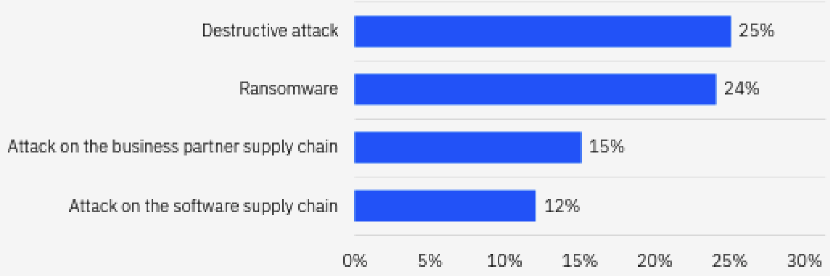


Figure 19. Percentages for each attack type shown are out of total breaches; bars will not sum to 100%

Cost of a ransomware or destructive attack

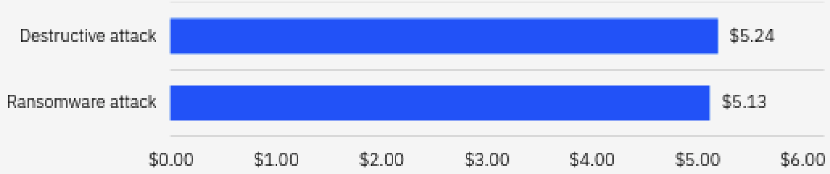
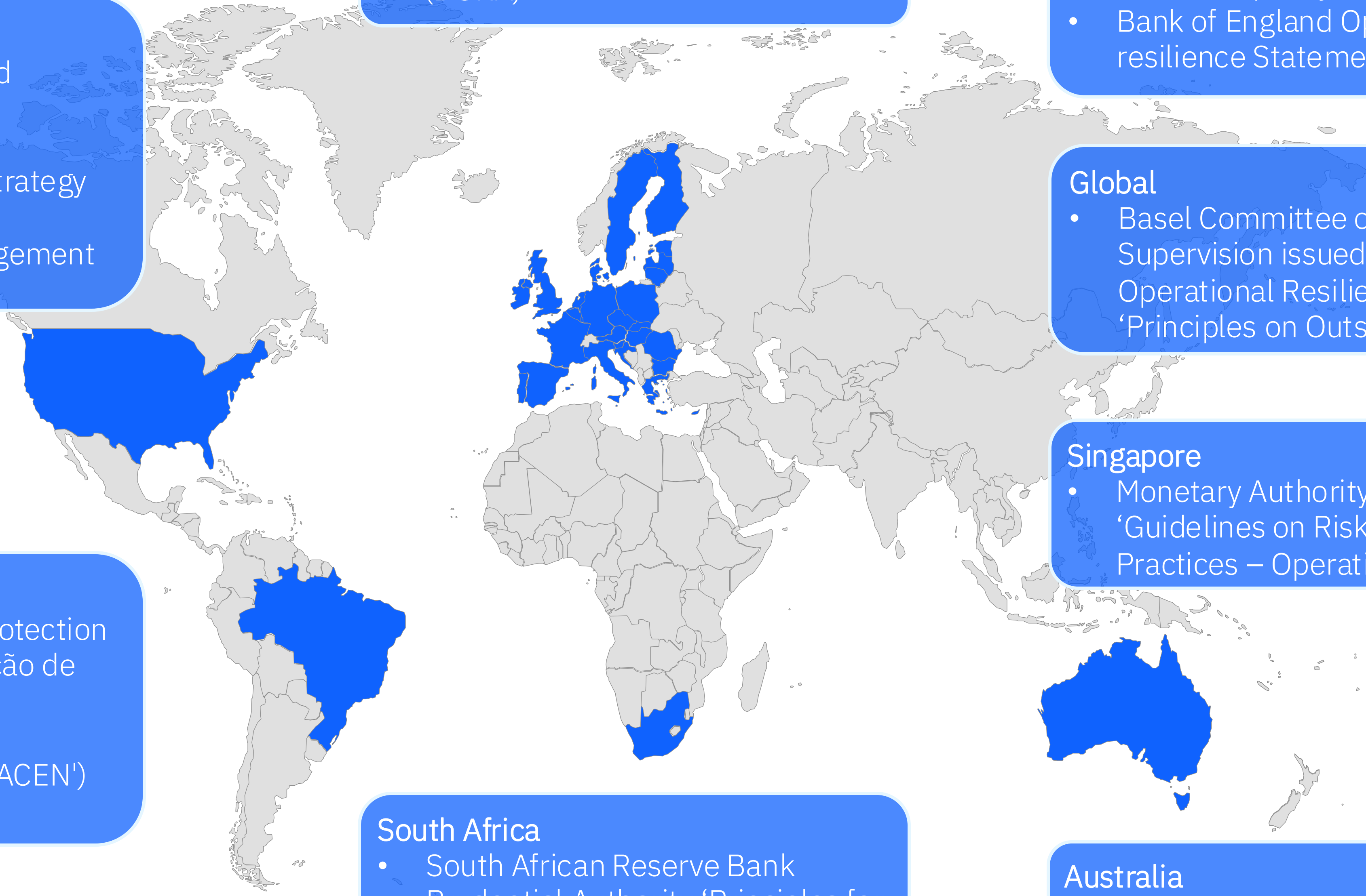


Figure 20. Measured in USD millions

[1] Cost of a Data Breach Report 2023 (https://www.ibm.com/reports/data-breach)

Worldwide regulation



United States

- Interagency paper ‘Sound Practices to Strengthen Operational Resilience’
- National Cybersecurity Strategy
- SEC Proposed Ruling for Cybersecurity Risk Management Rule 10

Europe

- Digital Operational Resiliency Act (DORA)

United Kingdom

- FCA PS21/3 Building operational resilience policy statement
- Bank of England Operational resilience Statement of policy

Global

- Basel Committee on Banking Supervision issued ‘Principles for Operational Resilience’ and ‘Principles on Outsourcing’

Singapore

- Monetary Authority of Singapore ‘Guidelines on Risk Management Practices – Operational Risk’

Brazil

- Brazilian General Data Protection Law (“Lei Geral de Proteção de Dados” or “LGPD”)
- Resolution 4.502/2016
- Central Bank of Brazil ('BACEN') Resolution 4.893/2021

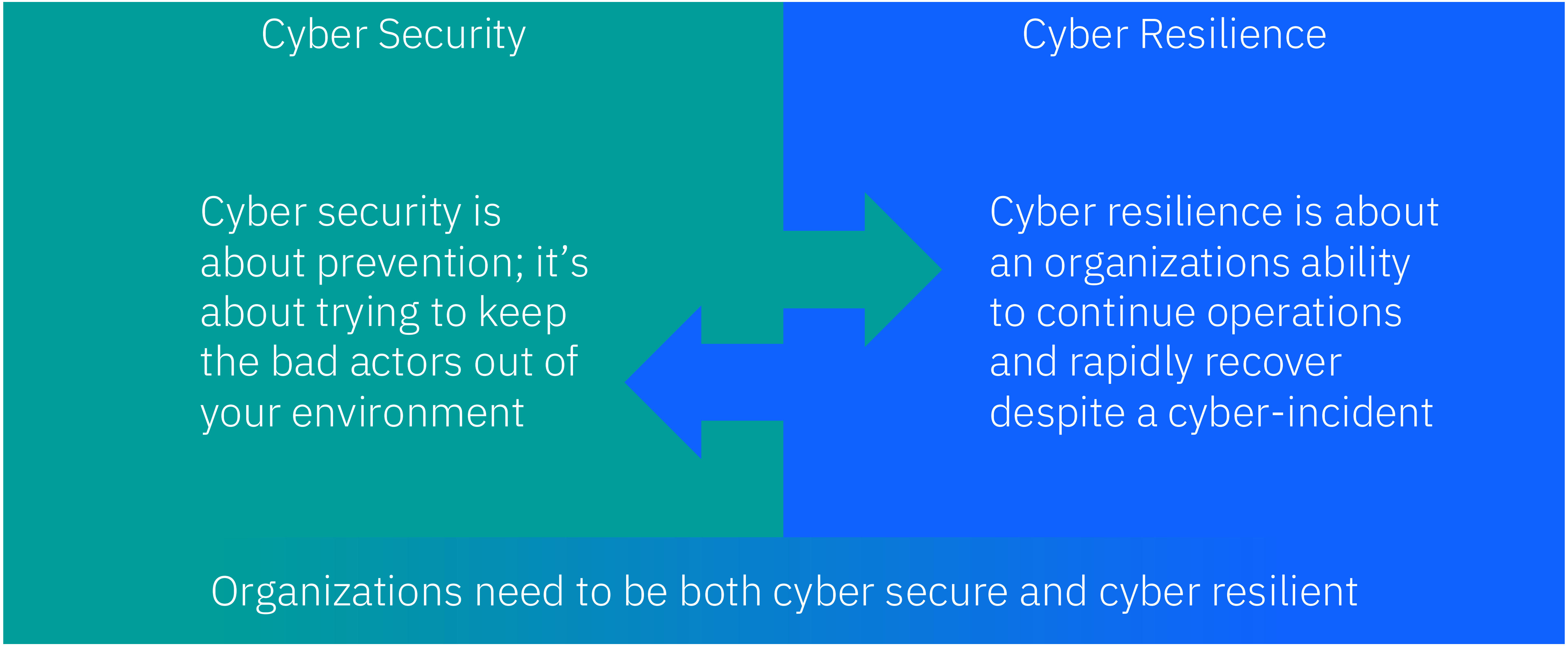
South Africa

- South African Reserve Bank Prudential Authority ‘Principles for operational resilience’

Australia

- Prudential Standard CPS 230 - Operational Risk Management

Cyber Security and Cyber Resilience



Cyber Security

Cyber security is about prevention; it’s about trying to keep the bad actors out of your environment

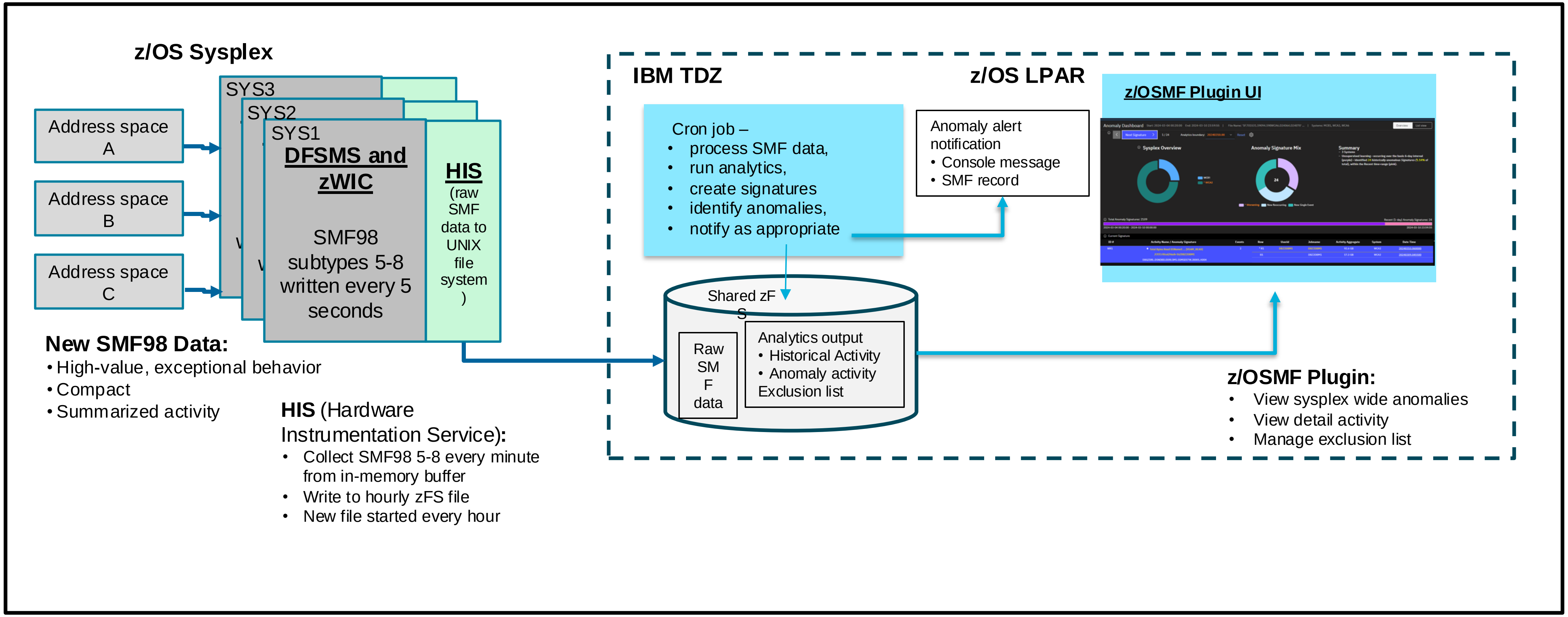
Cyber Resilience

Cyber resilience is about an organizations ability to continue operations and rapidly recover despite a cyber-incident

Organizations need to be both cyber secure and cyber resilient

IBM Threat Detection for z/OS

Architecture flow



Cron job –

- process SMF data,
- run analytics,
- create signatures
- identify anomalies,
- notify as appropriate

Anomaly alert notification

- Console message
- SMF record

Analytics output

- Historical Activity
- Anomaly activity Exclusion list

New SMF98 Data:

- High-value, exceptional behavior
- Compact
- Summarized activity

HIS (Hardware Instrumentation Service)**:**

- Collect SMF98 5-8 every minute from in-memory buffer
- Write to hourly zFS file
- New file started every hour

z/OSMF Plugin:

- View sysplex wide anomalies
- View detail activity
- Manage exclusion list

IBM Z Cyber Vault Overview

Robust Cyber Resiliency requires Cyber Security, traditional Business Continuity, and Corruption Protection.

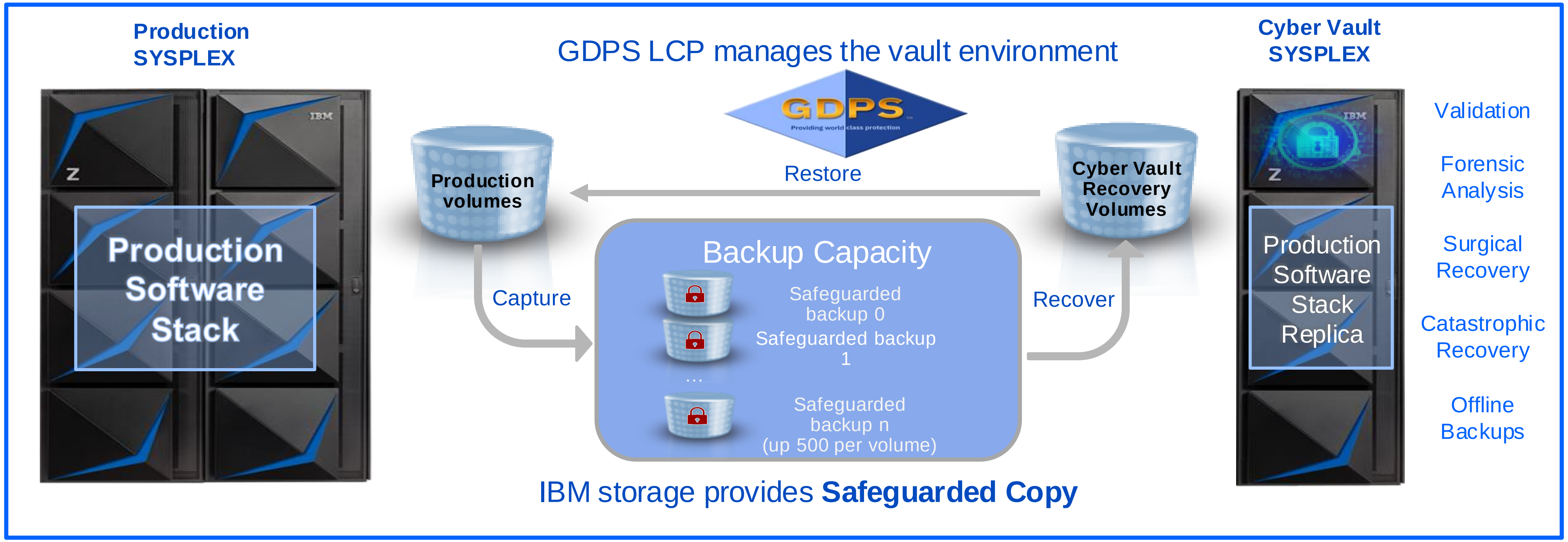
Cyber Resiliency

The ability to *anticipate, withstand, adapt to, and recover* from adverse conditions, events, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Cyber Security	*Continuous Operations*	*Disaster Recovery*	*Cyber Vault*
Encryption zSecure Guardium Qradar	Parallel Sysplex System Recovery Boost Datasharing Hyperswap	GDPS Automation System Recovery Boost Disk Replication	IBM Z Cyber Vault DS8K Safeguarded copy GDPS LCP TS7700
Minimize the risk by preventing access, ensuring immediate detection, and providing rapid response.	Minimize the risk and recover from outages caused by unplanned system failures and planned maintenance.	Minimize the impact of disaster level events by providing fast failover.	Minimize the impact of corruption events by protecting data, detecting corruption, responding quickly, and providing fast recovery.

IBM Z Cyber Vault

Reduce the time to recover from days to minutes.


Production SYSPLEX
GDPS LCP manages the vault environment
Cyber Vault SYSPLEX
GDPS
Providing world class protection
Production Software Stack
Production volumes
Restore
Cyber Vault Recovery Volumes
Capture
Backup Capacity
Safeguarded backup 0
Safeguarded backup 1
…
Safeguarded backup n (up 500 per volume)
Recover
Production Software Stack Replica
Validation
Forensic Analysis
Surgical Recovery
Catastrophic Recovery
Offline Backups
IBM storage provides Safeguarded Copy

IBM DS8K with Safeguarded Copy provides immutable, consistent point-in-time copies of data.

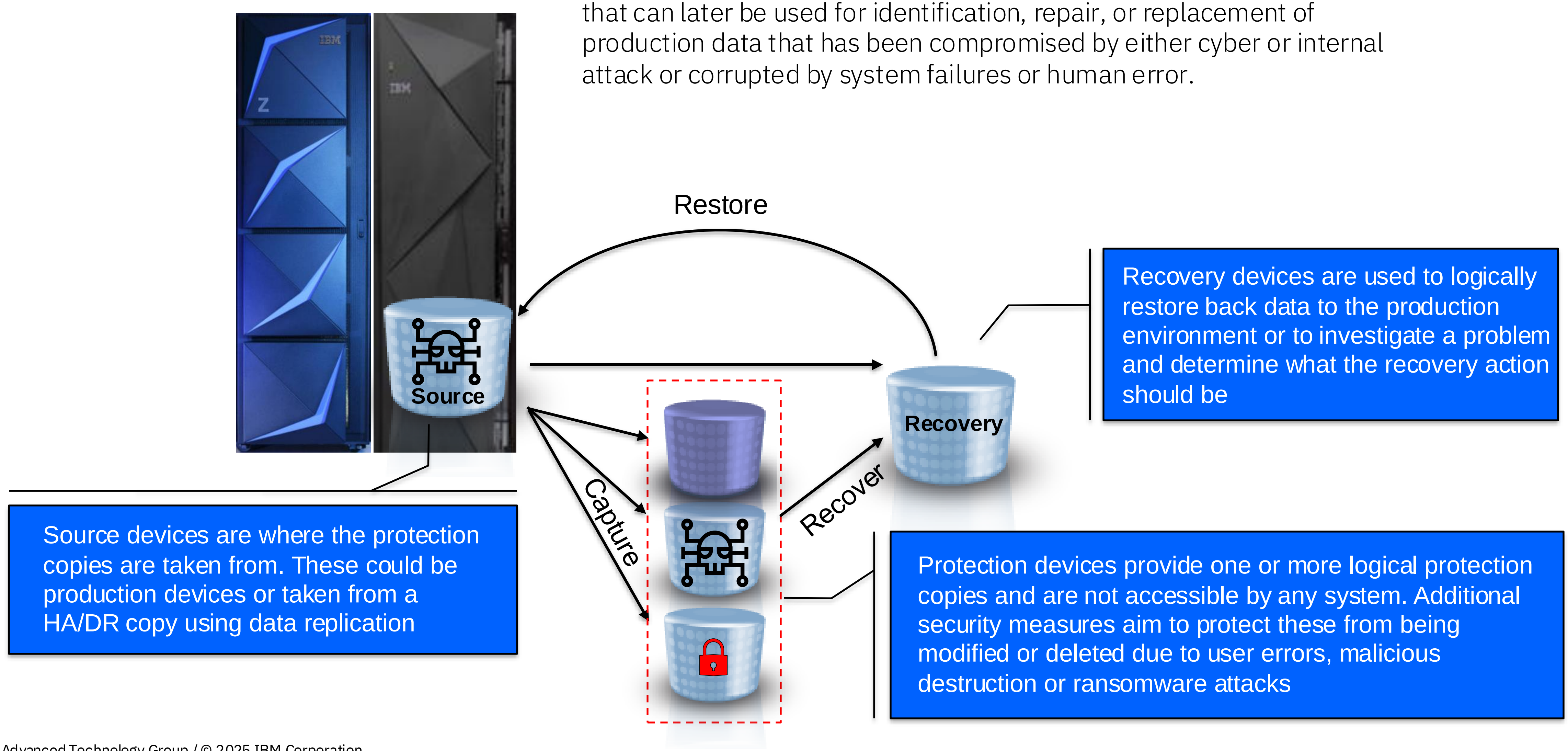
GDPS LCP manages the creation, recovery, and restoration of the copies and provides automation to manage those processes.

IBM z Systems hardware and software provides a secure, isolated environment to perform data validation, forensic analysis, and create offline backups.

Protecting Your Data

Logical corruption protection copies (Safeguarded Copy)

Safeguarded Copies are secure, point-in-time copies of production data that can later be used for identification, repair, or replacement of production data that has been compromised by either cyber or internal attack or corrupted by system failures or human error.



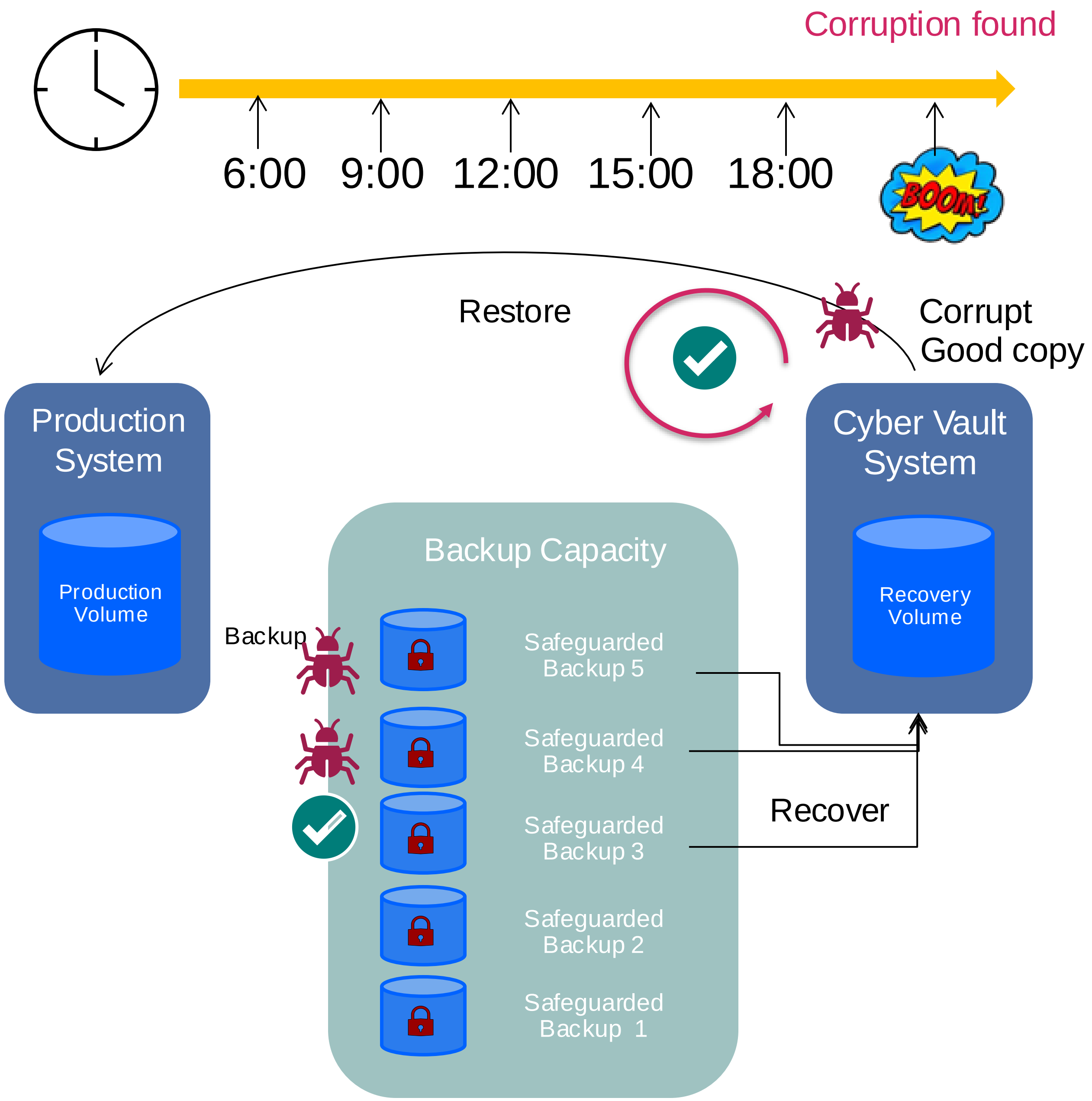
Recovery devices are used to logically restore back data to the production environment or to investigate a problem and determine what the recovery action should be

Source devices are where the protection copies are taken from. These could be production devices or taken from a HA/DR copy using data replication

Protection devices provide one or more logical protection copies and are not accessible by any system. Additional security measures aim to protect these from being modified or deleted due to user errors, malicious destruction or ransomware attacks

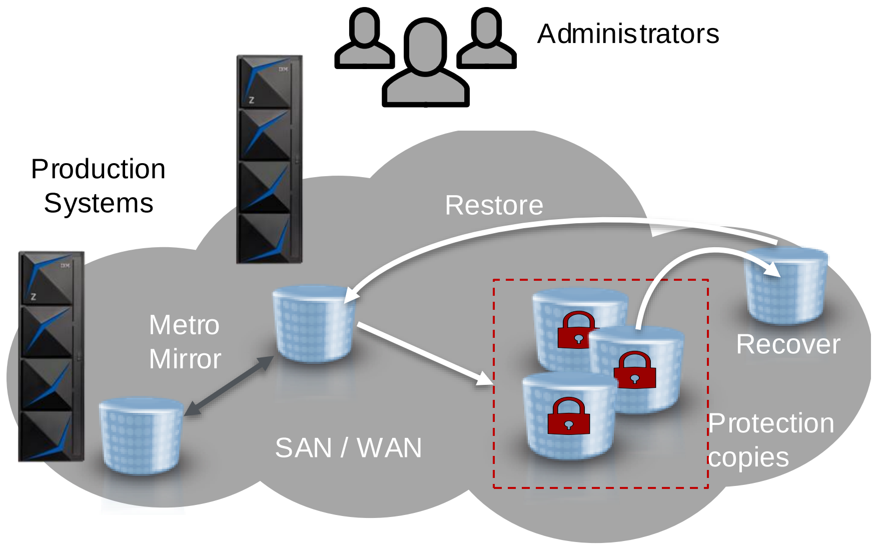
IBM Storage provides Safeguarded Copy

- Prevent sensitive point in time copies of data from being modified or deleted due to errors, malicious destruction or ransomware attacks.
- Create up to **500** Safeguarded Backups for a production volume stored in Safeguarded Backup Capacity, which is not accessible to any server.
- The data is accessible only after a Safeguarded Backup is recovered to a separate recovery volume.
- Recovery volumes are used with a data recovery system for:
  - Data validation
  - Forensic analysis
  - Restore production data



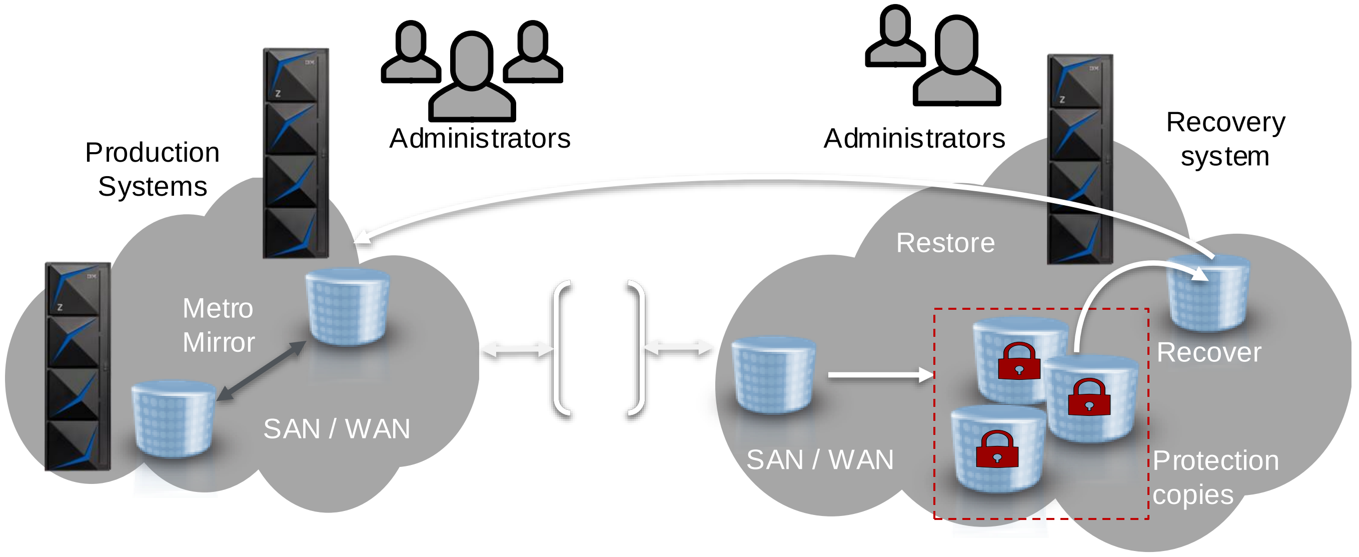
Air gap: Virtual and physical isolation of protection copies

Virtual isolation



- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

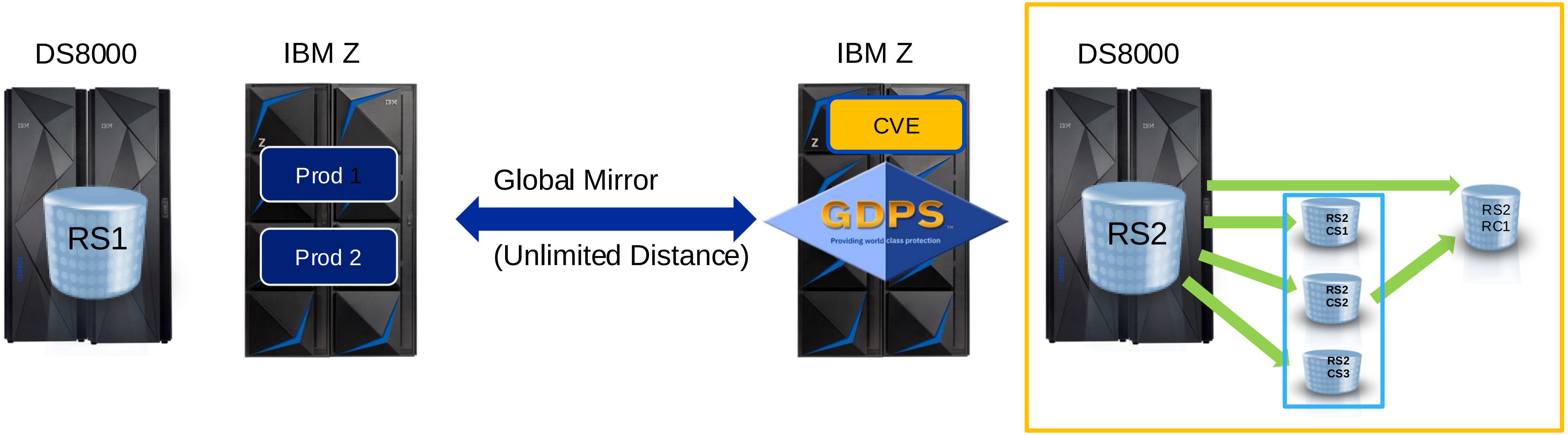
Physical isolation



- Additional storage systems are used for the protection copies
- The storage systems are typically not on the same SAN or IP network as the production environment
- The storage systems have restricted access and even different administrators to provide separation of duties

Safeguarded Copy Deployment example:
Logical Airgap (virtual isolation) with Global Mirror

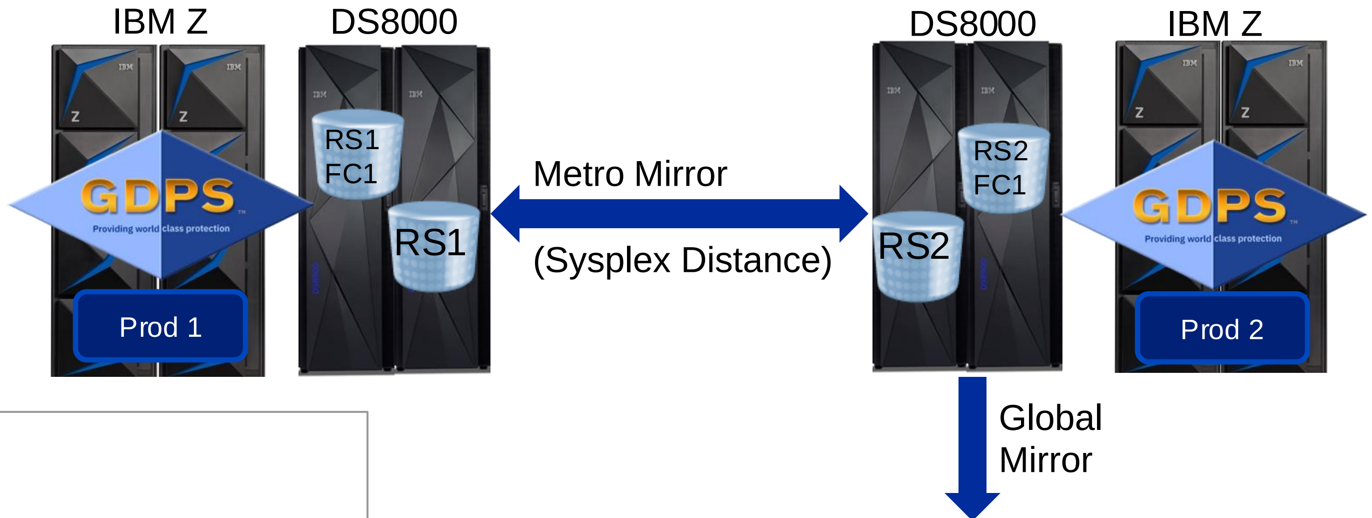
Safeguarded Copy on DR site

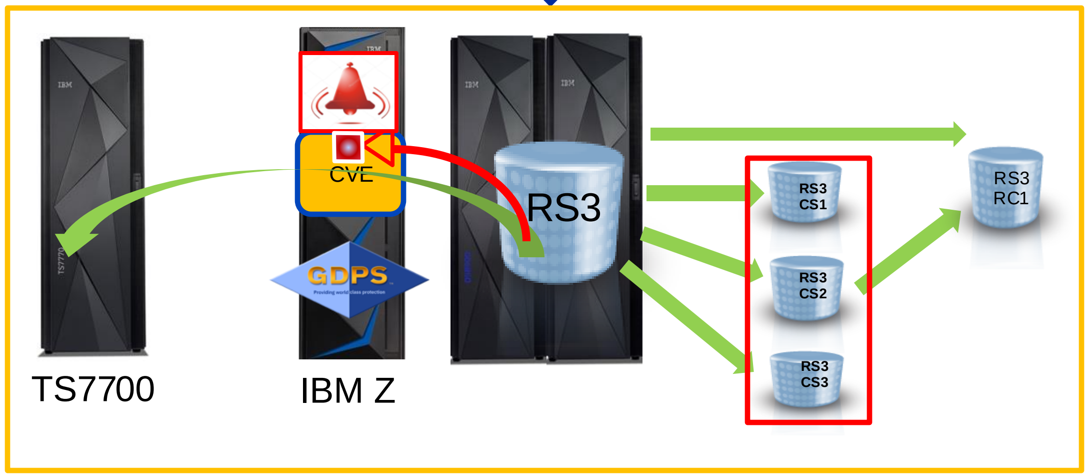


Description:

- Unlimited Distance
- No performance impact on primary DASD due to asynchronous copy mechanism.
- Safeguarded copies are in the same storage box as GM secondaries.
- IBM Z Cyber Vault Environment (CVE) leverages active capacity (MIPS) in DR site.

Safeguarded Copy Deployment example:
Physical Airgap (and Isolation) using Global Mirror

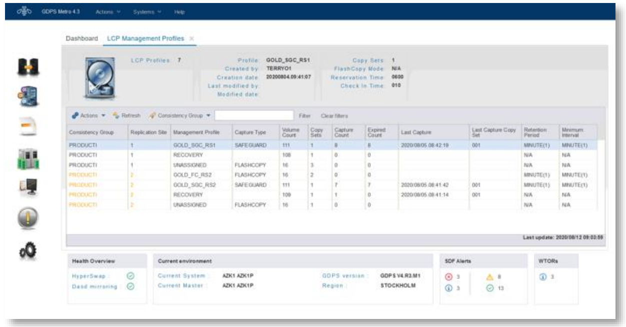




Description:

- Synchronous Distance
- No performance impact on primary DASD due to asynchronous new global mirror copy.
- Safeguarded copies are in a separate storage device with new GM secondaries.
- IBM Z Cyber Vault Environment (CVE) leverages capacity (MIPS) in an isolated IBM Z environment.
- The IBM Z Cyber Vault components can be in any datacenter.

Management Solutions for Cyber Vault and Safeguarded Copy



LCP Profiles: 7

Profile: GOLD_SGC_RS1
Created by: TERRYO1
Creation date: 20200804.09:41:07
Last modified by:
Modified date:

Copy Sets: 1
FlashCopy Mode: N/A
Reservation Time: 0600
Check In Time: 010

Consistency Group	Replication Site	Management Profile	Capture Type	Volume Count	Copy Sets	Capture Count	Expired Count	Last Capture	Last Capture Copy Set	Retention Period	Minimum Interval
PRODUCTI	1	GOLD_SGC_RS1	SAFEGUARD	111	1	8	8	2020/08/05 08:42:19	001	MINUTE(1)	MINUTE(1)
PRODUCTI	1	RECOVERY		108	1	0	0			N/A	N/A
PRODUCTI	1	UNASSIGNED	FLASHCOPY	16	3	0	0			N/A	N/A
PRODUCTI	2	GOLD_FC_RS2	FLASHCOPY	16	2	0	0			MINUTE(1)	MINUTE(1)
PRODUCTI	2	GOLD_SGC_RS2	SAFEGUARD	111	1	7	7	2020/08/05 08:41:42	001	MINUTE(1)	MINUTE(1)
PRODUCTI	2	RECOVERY		109	1	1	0	2020/08/05 08:41:14	001	N/A	N/A
PRODUCTI	2	UNASSIGNED	FLASHCOPY	16	1	0	0			N/A	N/A

Last update: 2020/08/12 09:03:59

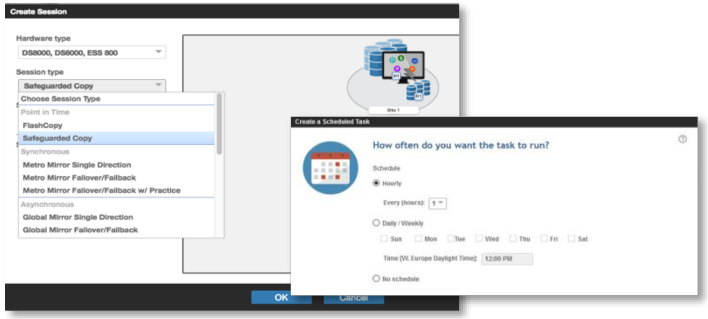
Health Overview
HyperSwap: ✓
Dasd mirroring: ✓

Current environment
Current System: AZK1 AZK1P
Current Master: AZK1 AZK1P
GDPS version: GDPS V4.R3.M1
Region: STOCKHOLM

SDF Alerts
⊗ 3 ⚠ 8
ⓘ 3 ✓ 13

WTORs
ⓘ 3

GDPS LCP Manager


Create Session
Choose Session Type
Point in Time
FlashCopy
Safeguarded Copy
Synchronous
Metro Mirror Single Direction
Metro Mirror Failover/Failback
Metro Mirror Failover/Failback w/ Practice
Asynchronous
Global Mirror Single Direction
Global Mirror Failover/Failback
Site 1
H1
R1
OK
Cancel
Create a Scheduled Task

Hardware type: DS8000, DS6000, ESS 800

Session type: Safeguarded Copy

How often do you want the task to run?

Schedule

● Hourly

Every (hours): 1

○ Daily / Weekly

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time [W. Europe Daylight Time]: 12:00 PM

○ No schedule

Copy Services Manager (CSM)

GDPS LCP is a feature of GDPS that provides continuous data protection by managing Safeguarded Copies and automating validation and recovery.

- Manage and monitor Safeguarded Copies
  - Supports Safeguarded Copy in DS8K
  - Captures multiple, secure point-in-time copies of critical production data (referred to as protection copies)
  - Expire Safeguarded Copy Backup
  - Recover Safeguarded Copy Backup
  - Display Volumes of a Safeguarded Copy Backup
- Provides enhanced security features to protect Safeguarded Copies
- Automates data validation and recovery processes

IBM Copy Services Manager provides highly secure and efficient capabilities to manage Safeguarded Copy

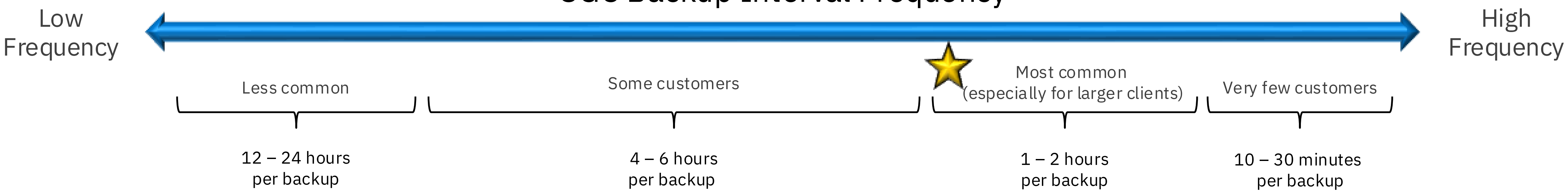
- Manage and monitor Safeguarded Copy sessions
  - Create Safeguarded Copy Backups
  - Expire Safeguarded Copy Backups
  - Recover a Safeguarded Copy Backup
  - Display Volumes of a Safeguarded Copy Backup
  - Terminate a Safeguarded Copy session
- Provides dual authentication control capability

GDPS and GDPS LCP is the more comprehensive resiliency and cyber resiliency solution

IBM DS8000 Safeguarded Copy – Backup Interval Frequency & Retention Period

★ Safeguarded Copy Backup Interval Frequency & Retention Period should be determined by *business requirements* to ensure that the frequency and retention period are relevant for business recovery. Safeguarded Copy can be complemented with offline backup to virtual tape for longer term retention. e.g., create an offline backup after data validation of an online copy.

SGC Backup Interval Frequency



Low Frequency

High Frequency

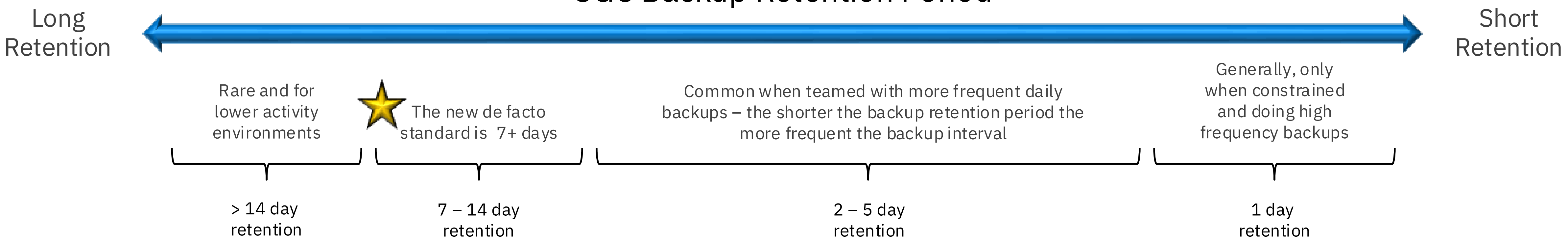
Less common: 12 – 24 hours per backup

Some customers: 4 – 6 hours per backup

★ Most common (especially for larger clients): 1 – 2 hours per backup

Very few customers: 10 – 30 minutes per backup

SGC Backup Retention Period



Long Retention

Short Retention

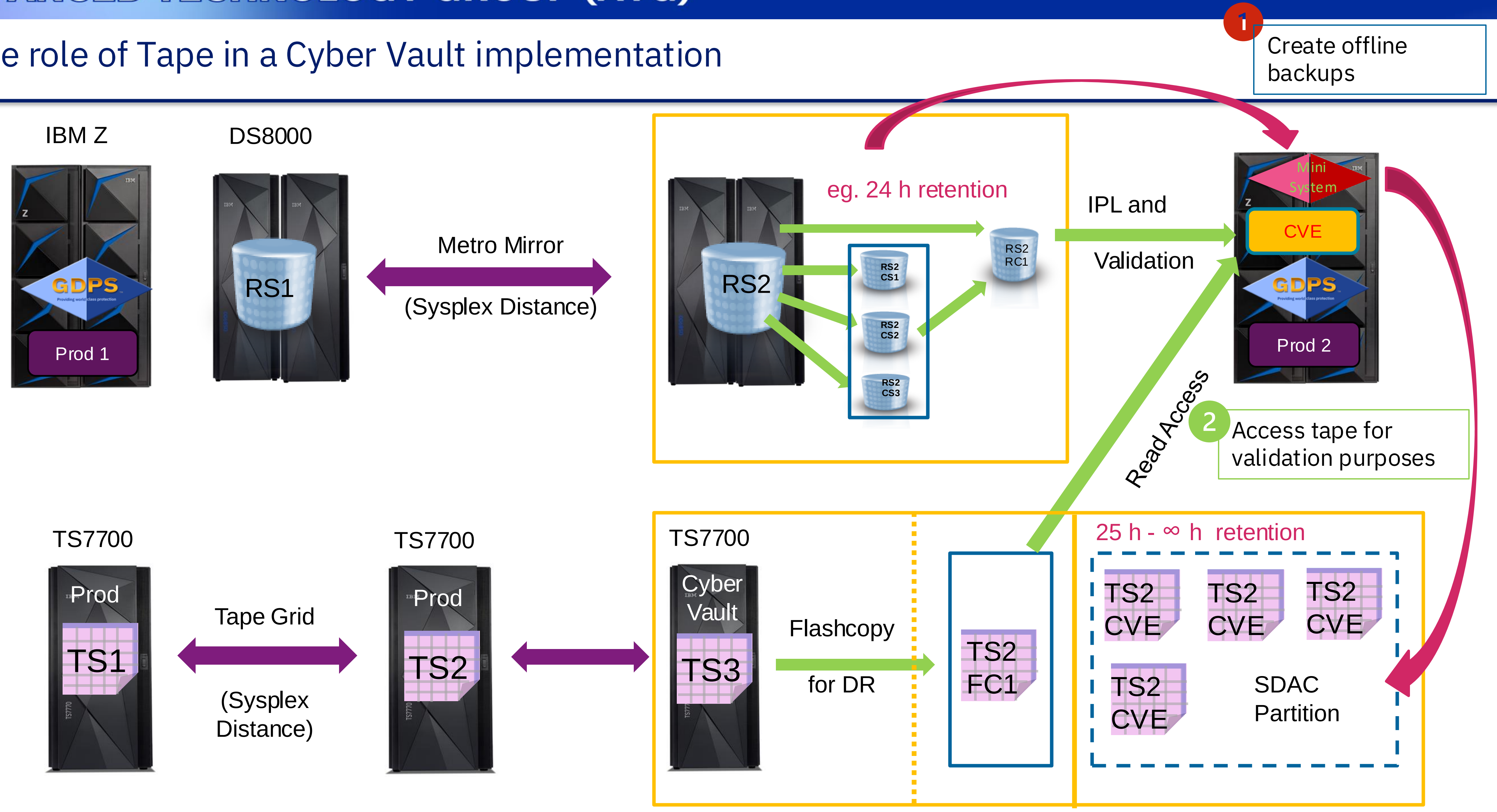
Rare and for lower activity environments: > 14 day retention

★ The new de facto standard is 7+ days: 7 – 14 day retention

Common when teamed with more frequent daily backups – the shorter the backup retention period the more frequent the backup interval: 2 – 5 day retention

Generally, only when constrained and doing high frequency backups: 1 day retention

The role of Tape in a Cyber Vault implementation



Validating and Recovering your data

Data validation

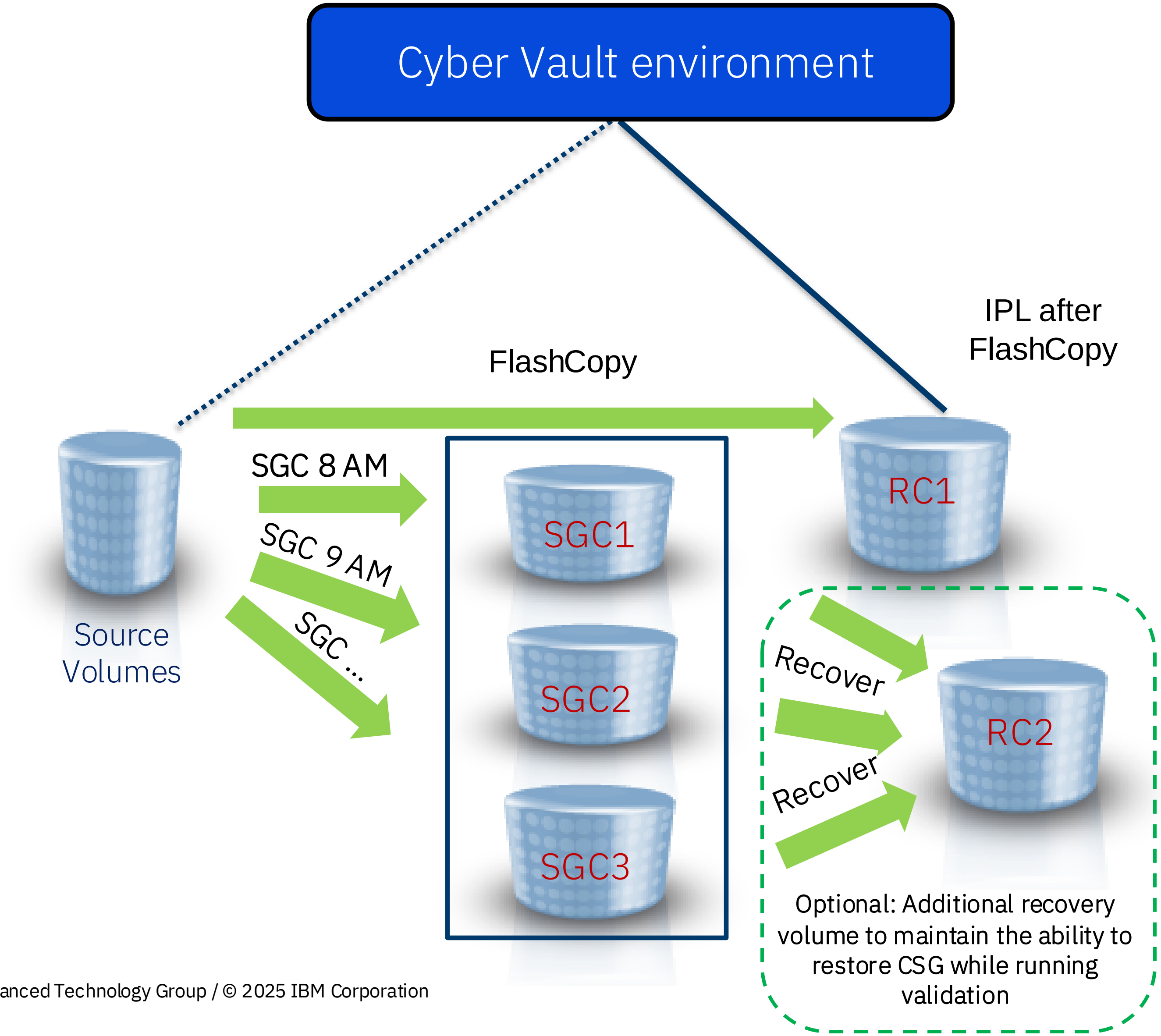
Detect data corruption early or validate that the copy is clear

Data validation is the process of executing regular analytics to identify a data corruption situation and determine the most convenient recovery action.

Performing corruption detection and validation processes against a copy of data is more practical than doing this in the live production environment.

Valid data can be sent to offline media to have a reliable and isolated point-in-time copy.

Data validation



Early identification of potential issues

Type 1: Infrastructure Validation

- IPL off FlashCopy of production sysplex to Recovery Copy set (RC1)
- Check sysplex infrastructure & subsystem restart

Type 2: Data Structure Validation

- Db2 Utilities (CHECK DATA/INDEX, Log analysis)
- IMS Utilities (Pointer checker)
- Catalog tools (Tivoli, IDCAMS, ISV products)
- VSAM Indexcheck, Datacheck
- DFSMShsm, DFSMSrmm tools
- RACF (IRRUT200), zSecure-Audit
- ISV software (CA1, CA7, ...)

Type 3: Data Content Validation

- Customer application program

Forensic analysis

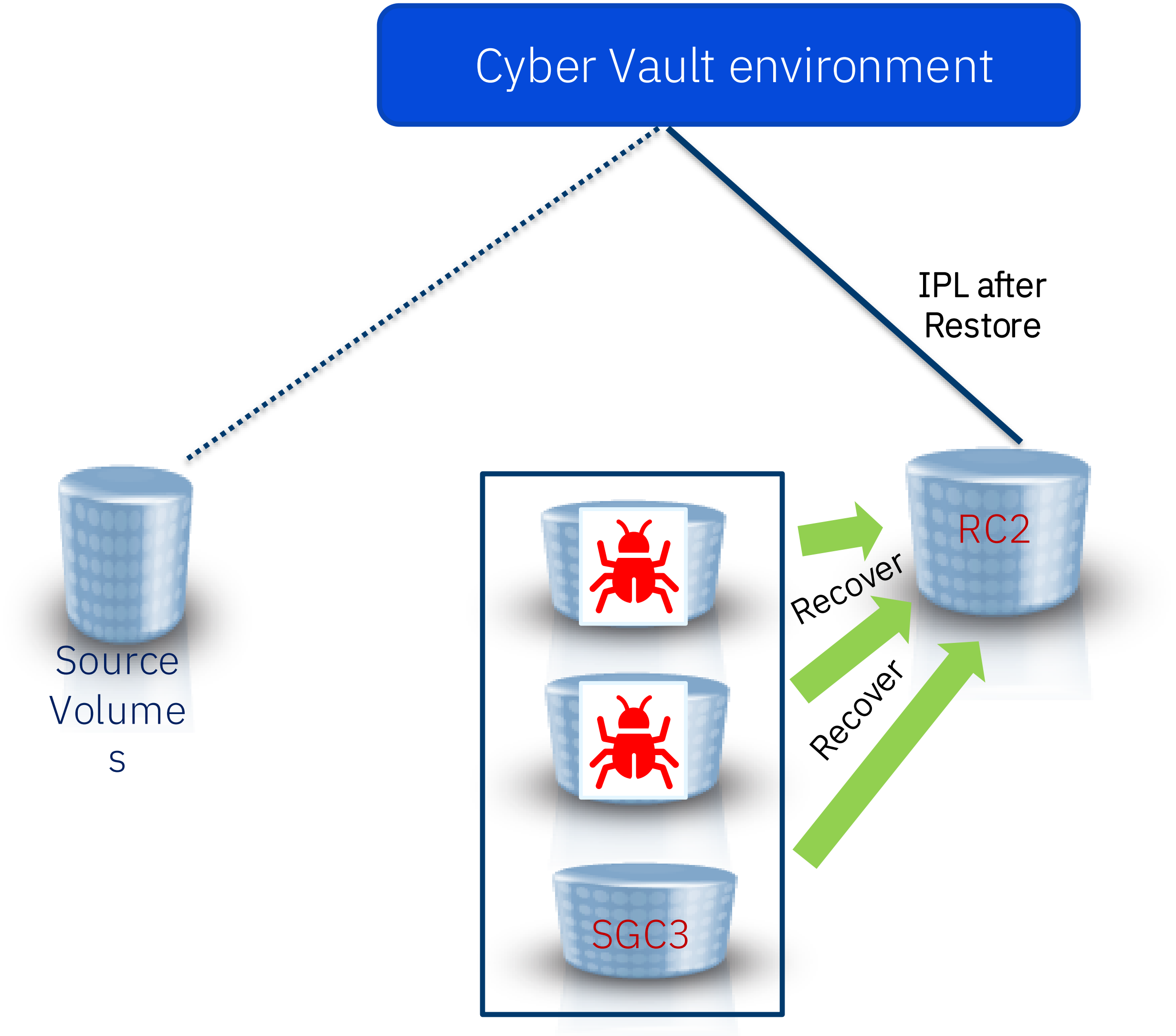
Investigate the problem and determine the best recovery action

The forensic analysis determines what data is corrupted, when the corruption occurred, and which of the available protection copies is the last good one.

Based on this analysis, it can be determined how to proceed:

- Fix the corruption from within the production environment
- Extract and recover certain parts of the data from a valid backup copy (Surgical Recovery)
- Restore the entire environment to a point in time that is known to be unaffected by the corruption (Catastrophic Recovery)

Forensic analysis



Determine start of data corruption …

- IPL one Safeguarded Copy after the other to the Cyber Vault Recovery Copy set (RC2) to find the last clean copy.
- Understand the problem
  - Run specific data structure and data content analysis on all stored Safeguarded Copies until a “clean” copy is found.
  - Use database tools to analyze databases and logs to fully embrace the scope of the problem
  - Use IZBR to identify open datasets and create cascade report for rapid analysis
- Identify steps forward
  - Create strategy for recovery dependent on availability of database image copy files.

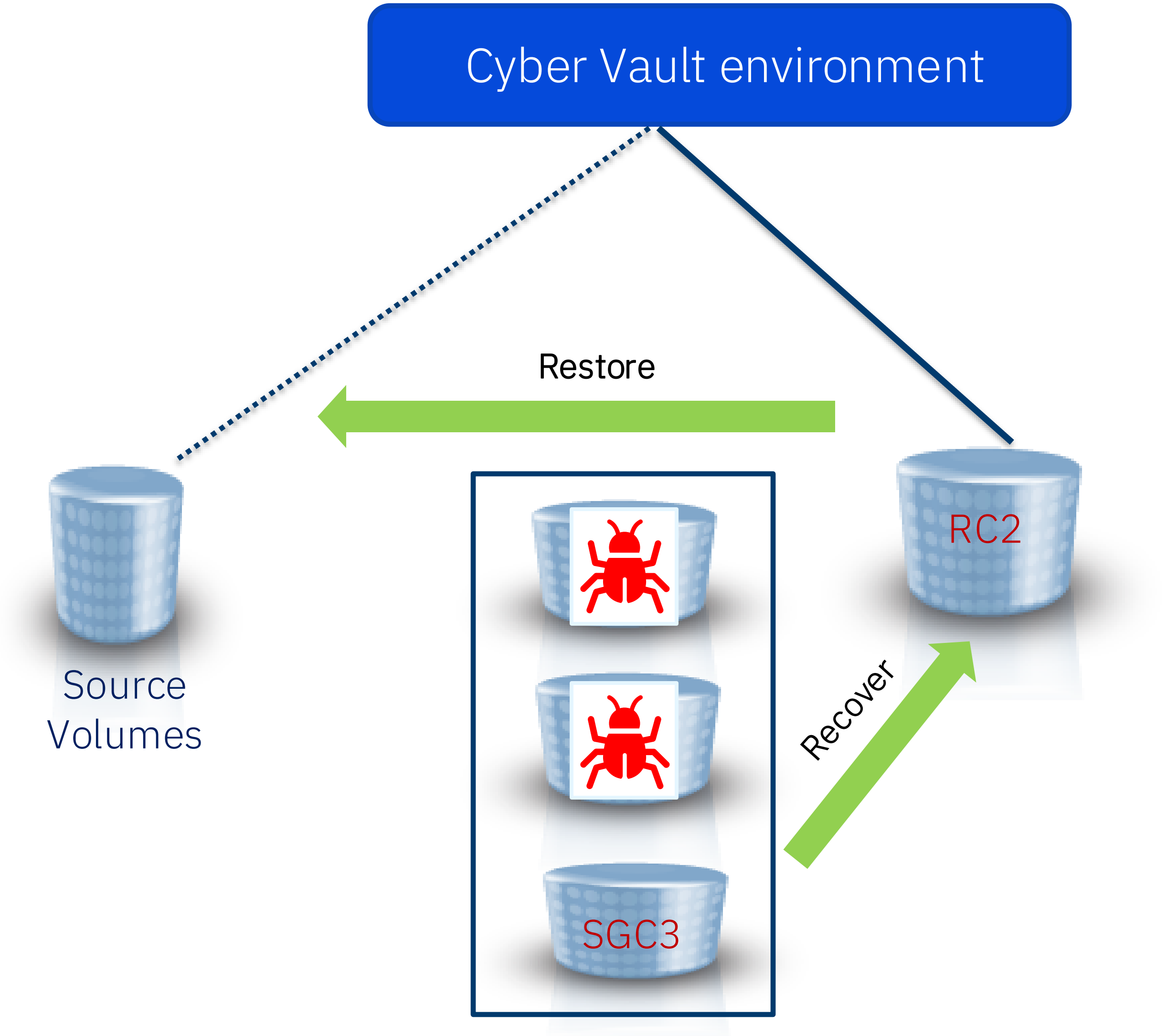
Surgical recovery

Extract data from the copy and logically restore back to production environment

Surgical Recovery may be a faster method if only a small portion of the production data is corrupted and if consistency between current production data and the restored parts can be re-established.

Another case for this kind of recovery may occur if the last known good backup copy is too old to restore the complete environment. It may then be desirable to leave most of the production volumes in its present state, and just copy replacement data to correct corrupted data.

Surgical recovery



Restore confirmed ‘good’ copy

- **Identify** specific point-in-time backup to be used as the restore point
- **Recover** the backup in the Cyber Vault environment (RC2)
- **Analyze** backup to determine what data is required.
- **Extract and copy** only the required data back into the running production environment using IZBR
- **Resolve** any inconsistency between backup data and production data

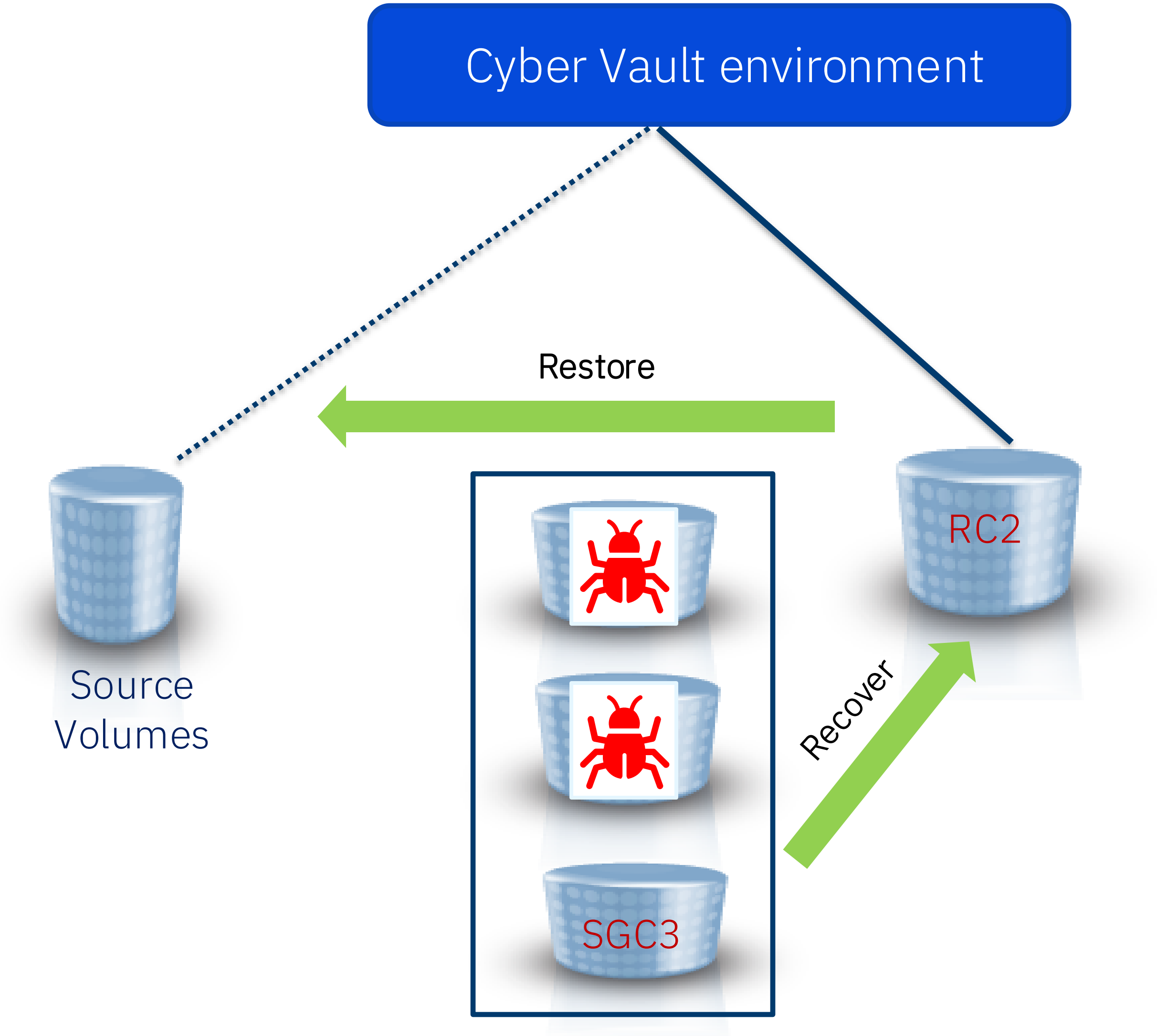
Catastrophic recovery

Recover the entire environment back to a point in time copy

In the case of massive corruption to all or most of the data in the environment, a castastrophic recovery needs to take place.

This means a full restore of a “clean” copy from Safeguarded Copy into the production environment needs to be done.

Catastrophic recovery



Restore identified 'good' data

- Identify specific point-in-time backup to be used as the restore point
- Recover the backup in the Cyber Vault environment (RC2)
- Incrementally restore the backup into the production environment
- Resolve any inconsistency between new production environment at T-X hours and any external dependencies

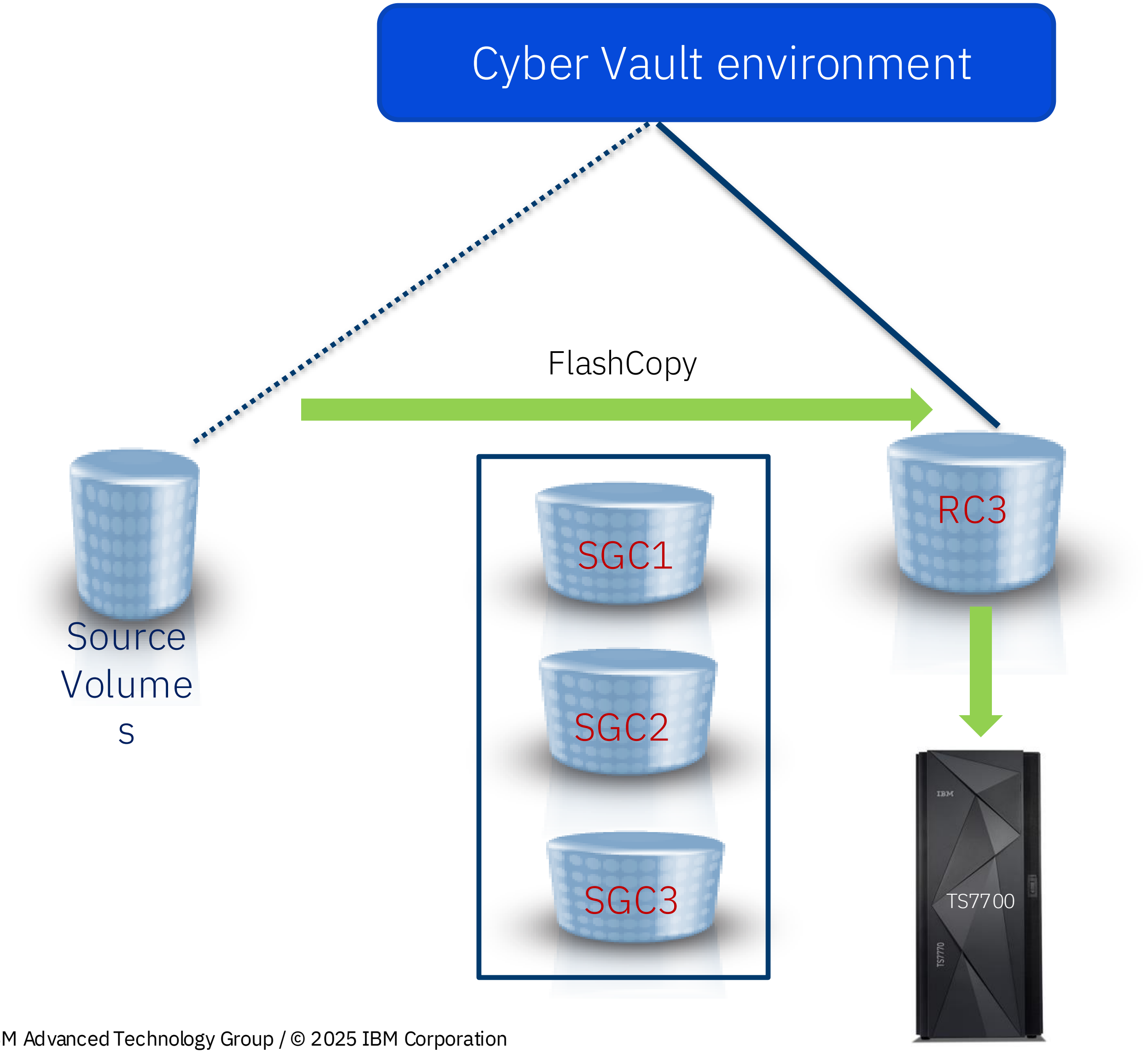
Offline Backup

Backup copy of the clean environment to offline tape media

In the context of Cyber Resiliency and Cyber Vault, additional offline copies provide additional protection. Safeguarded copy gives you the ability to capture and retain upto 500 copies for recovery and restoration from disk. However, you may need to retain some copies for longer.

Storing validated point-in-time copies on media like virtual tape or cloud object storage gives you a lower cost solution for longer term retention.

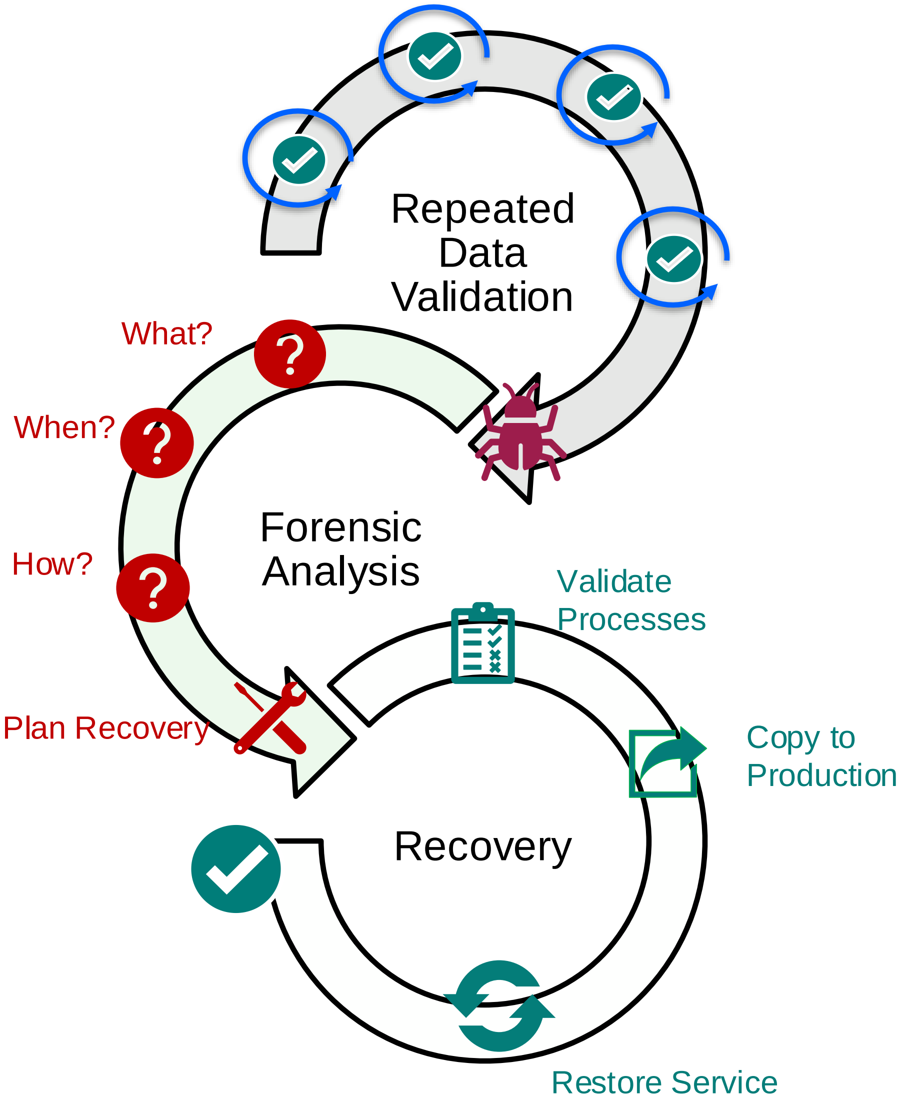
Offline backup



Longer term storage

- Backup a FlashCopy to tape (likely to take a significant amount of time)
- Safeguarded Copies are typically held for a few days or weeks
- Copy of production stored on tape that can be held indefinitely for longer term storage

Process summary



Backup and Validation

- Repeatable and Automated
- Time Consistent Copy is clean
- System is operational

Forensic Analysis

- What, when and how data was corrupted?
- Can’t be automated
- Tools may help, application knowledge is required

Recovery

- Execute Recovery Actions - Surgical or Catastrophic.
- Use existing templates and predefined procedures

Z Software

IBM Z Cyber Vault
Protect & Thrive with Security and Resiliency

Good News!

You have what you need today for Type 1 and basic Type 2 validations.

More robust Type 2 validations, forensic analysis and surgical recovery can be enhanced with additional tools.

Data validation

Forensic analysis

Surgical recovery

Catastrophic recovery

Offline backup

Catalog/VTOC/VVDS	
IBM Advanced Catalog Mgmt for z/OS	Enhanced checks on catalog integrity, runs faster than standard IDCAMS utilities, has extensive repair capabilities.
DFSMS	
Advanced Audit & Reporting for DFSMShsm	Faster than standard HSM audit, has a connection to RMM to cross check tapes. Auto correct HSM errors.
Security	
zSecure Audit	Potential identification of malicious database activities to help identify starting point of corruption.
Guardium	Can check unauthorized update of static libraries (load libraries, JCL, ...).
Datasets/Batch	
IZBR	Fast identification and recovery of all datasets open/closed during the Safeguarded copy.
Db2 Subsystem	
Db2 Log Analysis & Recovery Tools	Creation of data value change reports and fast recovery of changes recorded in the Db2 log.
Db2 Utilities Suite	Data structure check for all Db2 databases.
IMS Subsystem	
IMS High Performance Pointer Checker	Data structure check for all IMS databases.
IMS Recovery Solution Pak	Speeds up backup and recovery processes.
CICS VSAM Recovery Tool	Determines which CICS logs and VSAM backups are needed and constructs the recovery job

IBM Z Cyber Vault Environment Licensing

Full z/OS **Production** Software Stack

Licensed at full capacity for the IBM Z Cyber Vault Environment using a single PID: **5770-ZCV**

zHW Restricted Use pricing available for IBM Z Cyber Vault Environments.

New zSW PID 5770-ZCV is available as MLC and provides IBM software licensing entitlement for IBM zSW already licensed in the client’s production environment.

5770-ZCV GA’ed on January 19th, 2024

For more information, please see the announcement letter.

IBM Z Cyber Vault Software Recommendations – z/OS

Here are the recommended tools to manage and provide resiliency capabilities to the z/OS environment, including the z/OS catalog, DFSMShsm backup subsystem, and security related aspects to identify unauthorized activity.

Solution	P	CV	Capability
IBM Tivoli Advanced Catalog Management for z/OS Pointer checking for the catalog. Recovery of a catalog, including forward recovery to specific point in time.	✗	✓	Data Validation
IBM Tivoli Advanced Reporting and Management for DFSMShsm Verify inventory data set records are in sync with migration and backup copies. Compare reports between safeguarded copies taken at different times and find differences.	✓	✓	Recovery
IBM Tivoli Advanced Audit for DFSMShsm Conduct trouble-free audits and automate corrective actions.	✗	✓	Data Validation
IBM Security zSecure Audit Potential identification of malicious database activities to help identify starting point of corruption.	✗	✓	Forensic Analysis
IBM CICS VSAM Recovery CICS VSAM Recovery (CICS VR) is used to recover lost or damaged VSAM datasets. It determines which CICS logs and VSAM backups are needed and constructs the recovery jobs.	✗	✓	Recovery

IBM Z Cyber Vault Software Recommendations – Db2

These are the products that, following IBM Best Practices, provide resiliency capabilities for your Db2 databases.

IBM Db2 Utilities Suite

- The Db2 Utilities Suite is at the core of managing DB2 for z/OS. Helps minimize downtime associated with routine DB2 data maintenance, while ensuring the highest degree of data integrity. It provides Db2 data operations such as REORG, LOAD, UNLOAD and more.

IBM Db2 Log Analysis Tool

- Provides the ability to pinpoint who did what and when to business critical Db2 data. It enables the flexibility required to track data changes by automatically building reports of changes made to database tables, as well as isolate accidental or undesired changes made to data, and optionally undo or redo changes made to data.

IBM Db2 Recovery Expert

- Analyzes data and conditions to drive the necessary Db2 backup recovery processes to meet Recovery Time Objectives. Recovery plans provide cost and time estimations. with recovery jobs are built and validated PRIOR to execution. Supports point-in-time, dropped object, transaction, redirected, application, system level and disaster types of recovery operations.

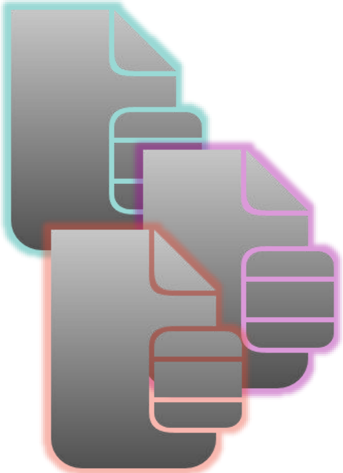
IBM Z Cyber Vault Software Recommendations – IMS

These are the products that, following IBM Best Practices, provide resiliency capabilities to your IMS database and transaction processing subsystems.

Solution	P	CV	Capability
IBM IMS High Performance Pointer Checker Pointer checking IMS full function databases	✗	✓	Data Validation
IBM IMS Fast Path Solution Pack Pointer checker function for Fast Path databases, aka DEDBs	✗	✓	
IBM IMS Recovery Solution Pack Database Recovery Facility component to validate all assets needed for recovery are available and can get to all of them	✗	✓	
IBM IMS Connect Extensions Collect and write data about IMS transactions coming in through IMS Connect	✓	✗	Forensic Analysis
IBM IMS Problem Investigator Deep dive analysis of IMS logs and IMS Connect Extensions journals	✗	✓	
IBM IMS Performance Analyzer Report on transactions that occurred during a specified period	✗	✓	
IBM IMS Recovery Solution Pack Recover specific IMS systems or databases based on the volume level backups	✓	✓	Surgical Recovery
IBM IMS High Performance Pointer Checker Repair specific segments in IMS full function databases without requiring full recovery	✗	✓	
IBM IMS Fast Path Solution Pack Repair specific segments in IMS Fast Path databases without requiring full recovery	✗	✓	
IBM IMS Queue Control Facility Recover and/or replay specific transactions	✓	✓	

IBM Z Cyber Vault Software Recommendations – non-database managed files

Database managers keep track of database activity (logs) and provide tools to recover to a consistency point

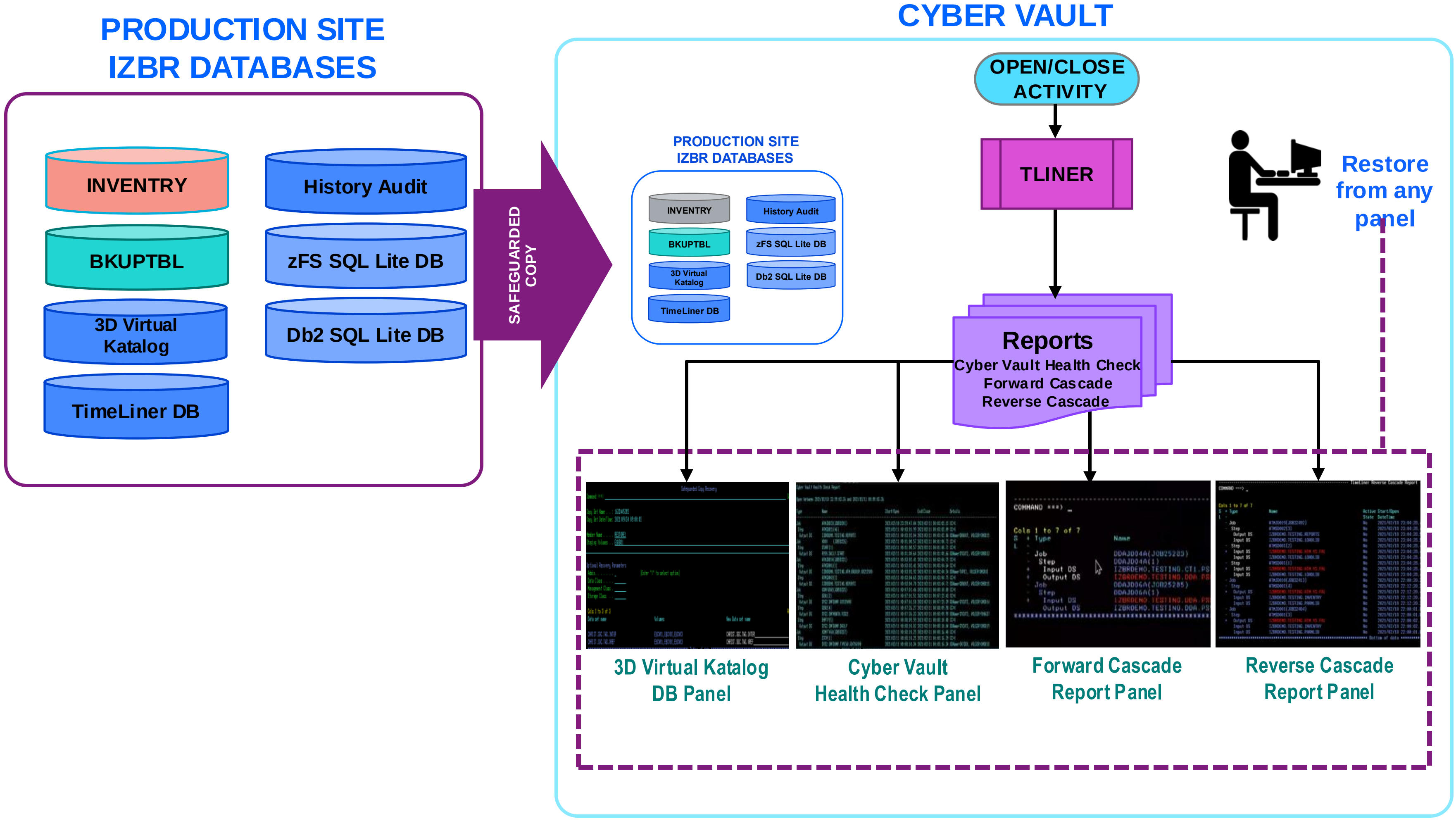


IBM Z Batch Resiliency v1.2 provides *log* and *recover* capabilities for non-database managed data, such as libraries, flat files, PDSes, and VSAM datasets.

- Cyber Vault health check report for Safeguarded copies
- TimeLiner reverse cascade report for forensic analysis
- TimeLiner forward cascade report to create recovery plan
- Panel driven surgical recovery

Capabilities to benefit recovery in IBM Z Cyber Vault deployments

- Surgical recovery of ***any data set*** using 3DVK database, automatically generating accurate restore JCL
- Cyber Vault Health Check report identifies “at risk” non-database managed data in air gapped copy
- Additional forensic capability is created through HISTORY, AUDIT and INVENTRY including identification of critical input tape data
- Reverse Cascade report assists forensic investigation of corruption by identifying jobs and steps that updated the corrupted files, and when
- Forward Cascade Report assists in developing a forward recovery plan for the applications that use the data that is recovered



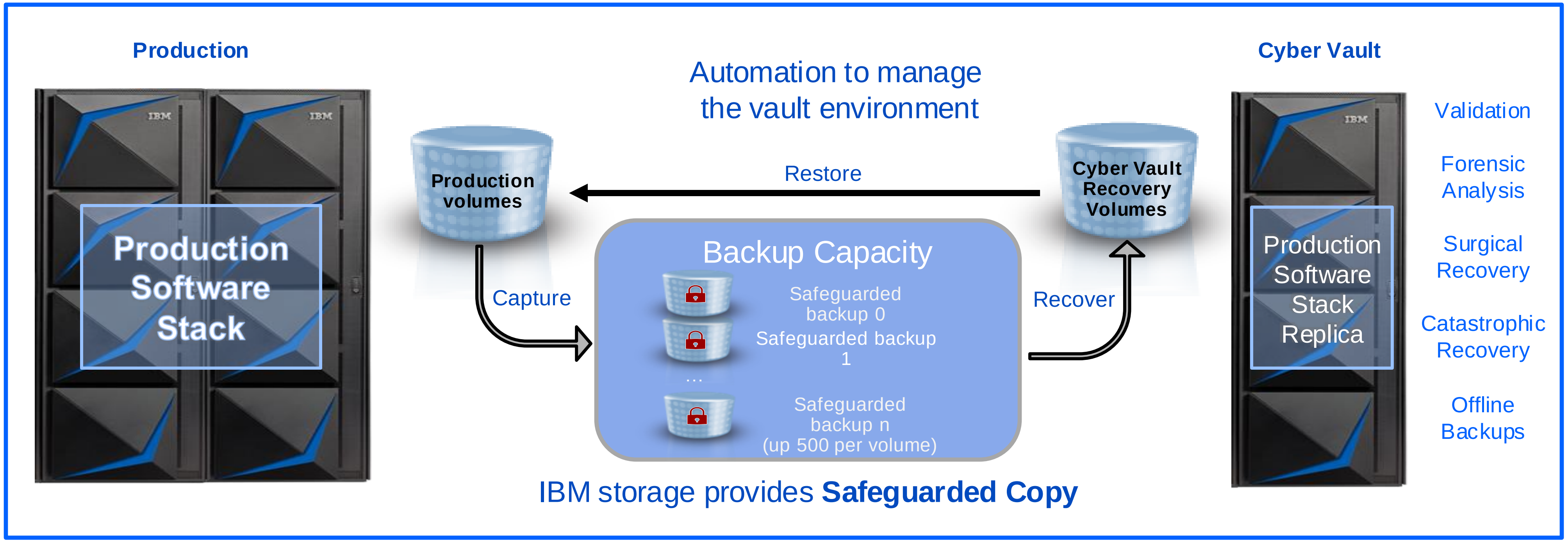
** Watch this APAR!*

APAR PH47869 – ‘Implement GDPS/LCP recovery support in IZBR’

IBM i Environments

IBM Cyber Vault

Reduce the time to recover from days to minutes.



Production
Cyber Vault
Automation to manage the vault environment
Production volumes
Restore
Cyber Vault Recovery Volumes
Production Software Stack
Capture
Backup Capacity
Safeguarded backup 0
Safeguarded backup 1
…
Safeguarded backup n (up 500 per volume)
Recover
Production Software Stack Replica
Validation
Forensic Analysis
Surgical Recovery
Catastrophic Recovery
Offline Backups
IBM storage provides **Safeguarded Copy**

IBM DS8K with Safeguarded Copy provides immutable, consistent point-in-time copies of data.

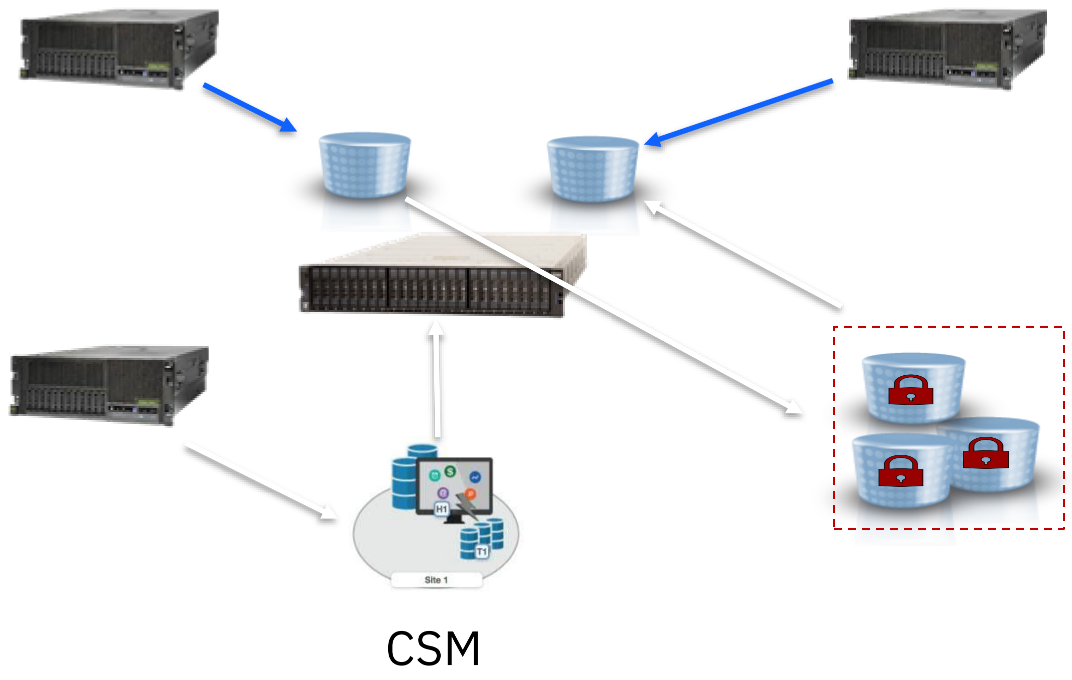
IBM Expert Labs – has automation for the creation, recovery, and restoration of the copies and provides automation to manage those processes.

IBM i hardware and software provides a secure, isolated environment to perform data validation, forensic analysis, and create offline backups.

The **Cyber Vault offering** is based on the **IBM Safeguarded Copy solution**

Safeguarded Copy prevents point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks

IBM i Cyber Vault automation



Production partition

Recovery partition
Automatically fixes TCP/IP and other resources per configuration

- Validation
- Forensic analysis
- Surgical recovery

Management partition
Orchestration of Safeguarded copy actions

- Start
- End
- Recover
- Restore
- Monitor

PowerHA Tools for IBM i with CSM

- PowerHA tools HA has integrated with CSM (TPC-R) for over 10 years

- Uses RestAPIs to mange sessions
- Manages CSM HA for the customer.
  - Performs automated takeover is the primary is unavailable
  - Performs automated reconnect or define secondary once after a failure
- Supports Dual Control via 2 separate profiles entered into the IBM i credentials list
  - When Dual Control is enabled, potentially malicious tasks like expiring copies is disabled

Management Partition(s)

PowerHA tools credentials list

USER *CSM
USER2 *CSMAUTH (only for dual control)

RestAPI

PowerHA Tools for IBM i configuring SGC for Flash Systems

- ➢ A Volume group is created in the Flash System
- ➢ A policy is assigned to the volume group
- ➢ Flash System is configured to use CSM as the scheduler

- ➢ IBM i customers can use the scheduler as configured or disable the schedule and use PowerHA tools to issue the Safeguarded Copies

- ➢ STRSGCPY will use a default expiration configured in the tools, or allow a custom expiration interval.

```
Environment name . . . . . . :    SGCPROD
Storage Type . . . . . . . . :    SVC

Primary ASP  . . . . . . . . .    *SYSTEM                    33 - 255,
*SYSTEM

CSM Safeguarded copy /
  FlashCopy  . . . . . . . . .    *YES                       *YES, *NO
  CSM Primary server . . . . .    10.10.1.50                 IPv4
  CSM Secondary server . . . .    10.10.1.51                 IPv4
  CSM Safeguard session name
    SVCPRDSG_CTCLABSVC                                       Name,
*NONE
  CSM FlashCopy session name      *NONE                      Name,
*NONE
  Default retention period        2                          1-365

Flash SVC IP Address . . . . .    10.10.1.60                 IPv4
GMCV Source SVC IP Address
```

Next Steps

Deployment Services for IBM Z Cyber Vault

Discovery and Architecture Workshop	Cyber Vault Installation and Configuration	Cyber Vault Data Recovery System Validation
• Validate Cyber Vault use case & understanding • Design technical solution • Create inputs to produce customized implementation services scope and size	• Install Cyber Vault components • GDPS LCP • Safeguarded Copy • Cyber Vault environment • Validate installation completeness • Basic CV knowledge transfer	• Validate selected system component copy restore capability and use • Understand operational processes required for CV operation • Prepare for Cyber Event Usage

No Cost

Co-requisite services

Cyber Vault forensics and recovery assistance can be provided in support of cyber incidents on a time & materials basis

Workshop Objective

IBM Advanced Technology Group will conduct two 2-hour sessions.

Identify high-level current state and gain insights into the Cyber Resiliency risks and challenges. Define the desired state and next steps for achieving it.

- Define cyber resiliency objectives including data retention and recovery time.
- Understand the current state and gain insights into cyber resiliency gaps and risks.
- Define success criteria.
- Design a future state Cyber Vault architecture.
- Develop and document an approach and roadmap to achieve the future state.

Session Agendas

Discovery Session

- ❑ Introductions and Workshop Objectives
- ❑ IBM Z Cyber Vault Overview
- ❑ Current Environment Discussion
- ❑ Requirements and Scope

Architecture Session
(scheduled one week after Discovery session)

- ❑ Future State Topology Options
  - Storage Topology Options
  - IBM Z Environment Capabilities
  - Software
  - Compare Options
- ❑ Next Steps

Prepare for discussions on the following topics

- ❑ Existing Architecture – datacenters, IBM Z, Parallel Sysplex, Storage (disk and tape), Replication, DR, Software

- ❑ Required use cases – examples:
  - ▪ Catastrophic Recovery
  - ▪ Surgical Recovery
  - ▪ Forensic Analysis

- ❑ Resiliency and Cyber Resiliency Requirements – SLAs, Recovery Time Objectives, Recovery Point Objectives

- ❑ Resiliency and Cyber Resiliency Regulatory requirements

- ❑ Recent outages caused by data corruption or cyber attacks – severity, recovery

- ❑ Current Cyber Resiliency strategy and direction

Client Workshop Participants

Role	Description
Resiliency, Cyber Resiliency Focal Point	Understands the resiliency and cyber resiliency business requirements. Can discuss things like Recovery Time Objectives and Recovery Point Objectives.
Security Architect, Compliance	Understands the cyber resiliency requirements, regulations, and compliance challenges. Can describe any regulatory requirements that need to be considered.
Chief Architect	Understands solutions from both an infrastructure and application perspective, may be an Enterprise Architect.
System Infrastructure Architect, Storage Infrastructure Architect	Understands Infrastructure and why certain architectural decisions were made, understands the platform and storage environment well.
Application Architect(s) and/or Middleware and Database (IMS, VSAM, Db2, etc) Experts	Understands the data that needs to be recovered. Can explain current backup and recovery processes. Has an understanding of what data validation would be required and how to determine success after recovery.

The following information is required to prepare sizings and estimates prior to the architecture session.

□ Storage Capacity and change rate data. See “IBM ATG - DS8000 Safeguarded Copy Sizing - Data Request Form - RMF Data - 20220620.pdf” (sent separately)

□ Software Information:

1. List of ISV products in the environment. We are particularly interested in any DB2, IMS, Storage, and Catalog Management tools.
2. List of current IBM SW products. This can be the last Workload Pricer (WLP) configuration file updated with new software versions. The list has 2 parts: MLC and IPLA software.
3. For Value Unit Edition (VUE) products, what does the current contract say in terms of adding capacity?

□ IBM Z Capacity and Architecture Information:

1. Previous month’s SCRT report for all machines.
2. Architecture diagram of the environment – how many Parallel Sysplexes? Where are they located?
3. How many MSUs does the client have in total and how many are used?

IBM local team will work with client team as needed

Accelerate with ATG Survey

Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 5151 0447 or

Direct link https://www.menti.com/alhsf3bgvxu6
Or

QR Code

Thank you!