

IBM zSystems Client Engineering Workshop

## IBM Z Cyber Vault Overview Session

# IBM Client Engineering for Systems

Thomas Bish  
[tbish@us.ibm.com](mailto:tbish@us.ibm.com)  
Principle Solution Architect

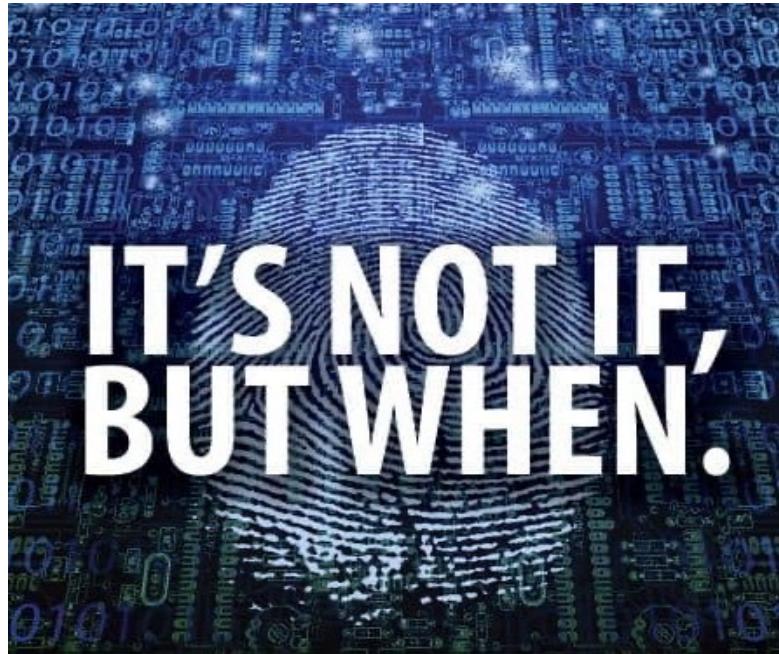


# Agenda

- Cyber Resiliency Introduction
- IBM Z Cyber Vault Overview
- Protecting Your Data
- Validating and Recovering Your Data
- Next Steps

# Cyber Resiliency

# Absolute resiliency or security is impossible



## *Systems need to be built for Cyber Resiliency*

- ✓ The ability to continuously deliver the intended outcome despite any adverse event or attacks
- ✓ Do everything you can to prevent downtime and attacks, plus minimize the impact and potential loss when an event does happen

# Sixty percent of businesses victimized by a cyber attack go out of business within six months.<sup>1</sup>

**CLOSED  
FOR BUSINESS**

**\$4.54M**

Average cost of a ransomware attack, not including the cost of the ransom itself.<sup>2</sup>



**\$1M**

Average difference in cost where remote work was a factor in causing the breach versus when it wasn't.<sup>2</sup>

**29 Days**

Savings in response time for those with extended detection and response (XDR) technologies.<sup>2</sup>

**83%**

Of organizations studied have had more than one data breach.<sup>2</sup>

Average cost of a data breach for ransomware and destructive attacks



<sup>1</sup>CNBC (<https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>)

<sup>2</sup>Cost of a Data Breach Report 2022 (<https://www.ibm.com/reports/data-breach>)

# Cyber resiliency solutions should handle a wide range of possible scenarios to reduce the risk of financial losses.

Cyber threats to enterprise data are increasing from a range of different sources including:

Depending on the platform different risks are seen as more or less likely. For core systems running on IBM Z, many organizations believe the greatest risk is a threat from a:

Similar loss or corruption of data is still also possible from other causes such as:

*External Malware Infection  
External Hacking  
Insider Threats*

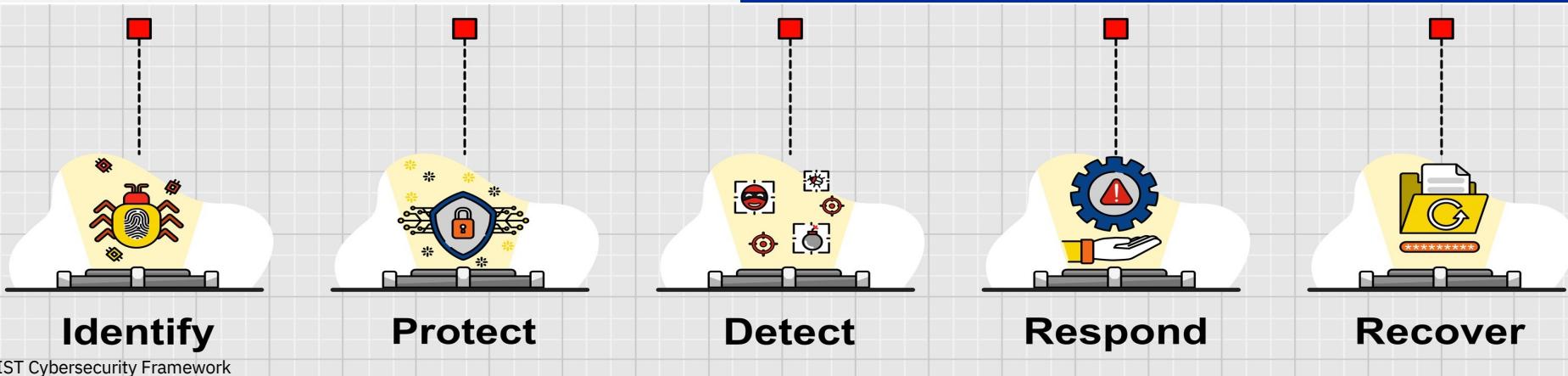
*Privileged Insider*

*Application error  
Operational error*

Furthermore, the pandemic and massive increase in remote working changes some of the risk vectors as access to mainframe systems is more likely from outside the organization controlled networks.

# 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



NIST Cybersecurity Framework

Cyber Security – *Minimize Risk through prevention*

Cyber Resiliency – *Minimize Impact with IBM Cyber Vault*

# 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

Encryption  
zSecure  
Guardium  
QRadar

### Continuous Operations

Parallel Sysplex  
System Recovery Boost  
Datasharing  
Hyperswap

### Disaster Recovery

GDPS  
Automation  
System Recovery Boost  
Disk Replication

### Cyber Vault

IBM Z Cyber Vault  
DS8K Safeguarded copy  
GDPS LCP  
TS7700

Minimize the risk by preventing access, ensuring immediate detection, and providing rapid response.

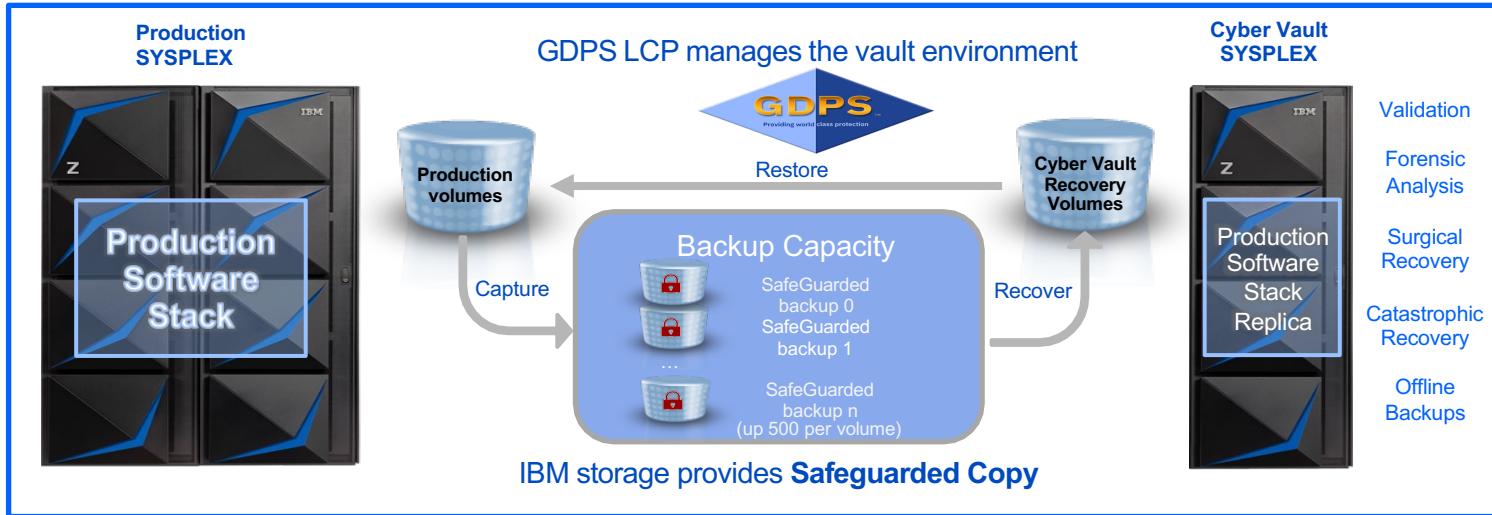
Minimize the risk and recover from outages caused by unplanned system failures and planned maintenance.

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.*



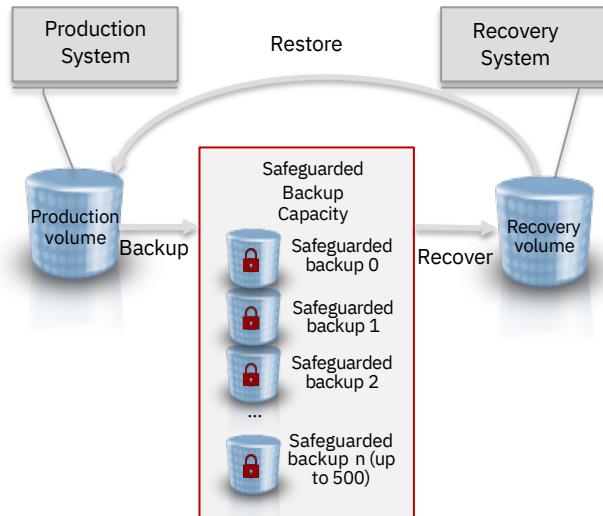
*IBM DS8K* with Safeguarded Copy provides immutable, consistent point-in-time copies of data.

*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.

# Traditional resiliency solutions don't protect you from logical data corruption.... more is needed.

Protect your data with immutable point in time copies



+

Detect, Respond, and Recover faster with these critical capabilities



#### Data validation

Regular analytics on the data copy to provide early detection of a problem, or reassurance that everything is OK



#### Forensic analysis

Start a copy of the production systems from the copy and use it to investigate the problem and determine the recovery action



#### Surgical recovery

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



#### Catastrophic recovery

Recover the entire environment back to the point in time of the copy as this is the only recovery option



#### Offline backup

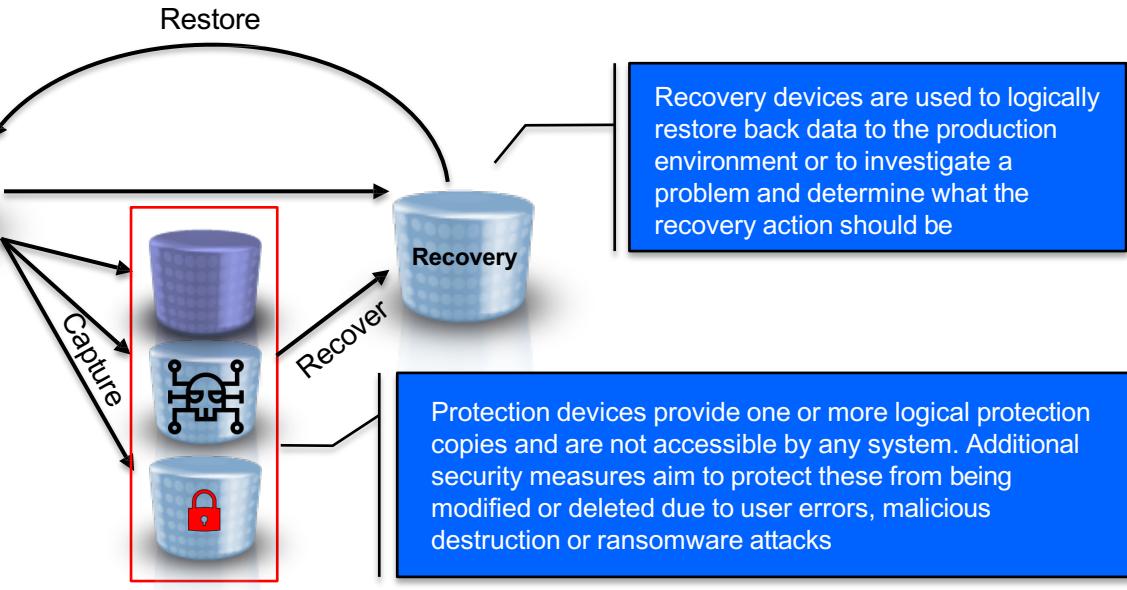
Copy the copy of the environment to offline media to provide a second layer of protection

# Protecting Your Data

# Logical corruption protection copies (Safeguarded Copy)

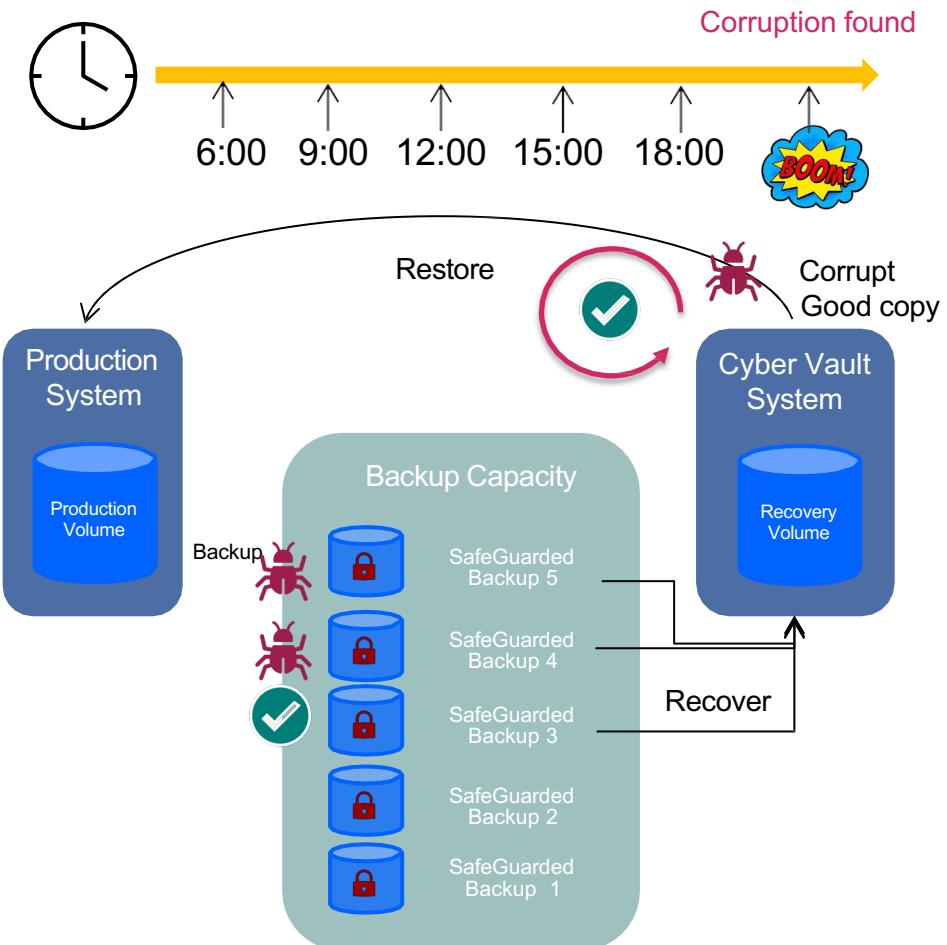


Safeguarded Copies are secure, point-in-time copies of production data that can later be used for identification, repair, or replacement of production data that has been compromised by either cyber or internal attack or corrupted by system failures or human error.



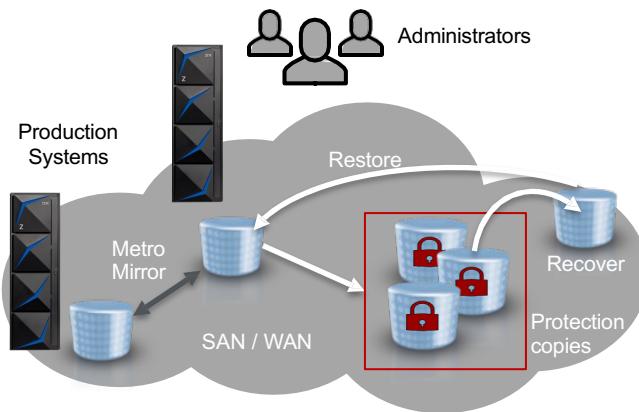
# IBM Storage provides SafeGuarded Copy

- 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

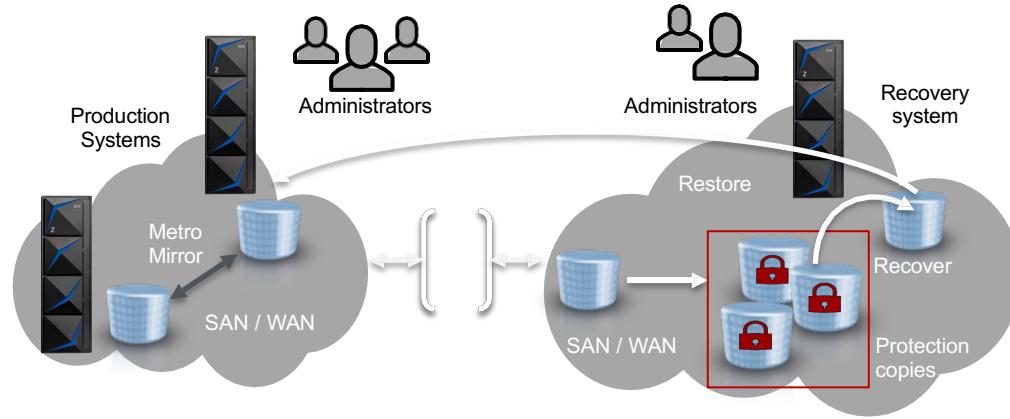


# Air gap: Virtual and physical isolation of protection copies

## Virtual isolation



## Physical isolation

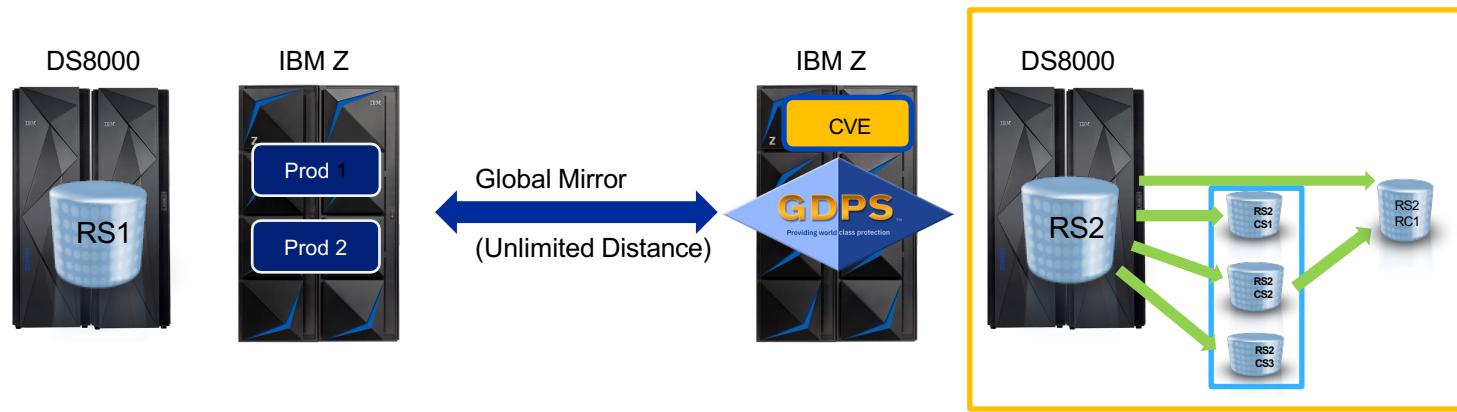


- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

- 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

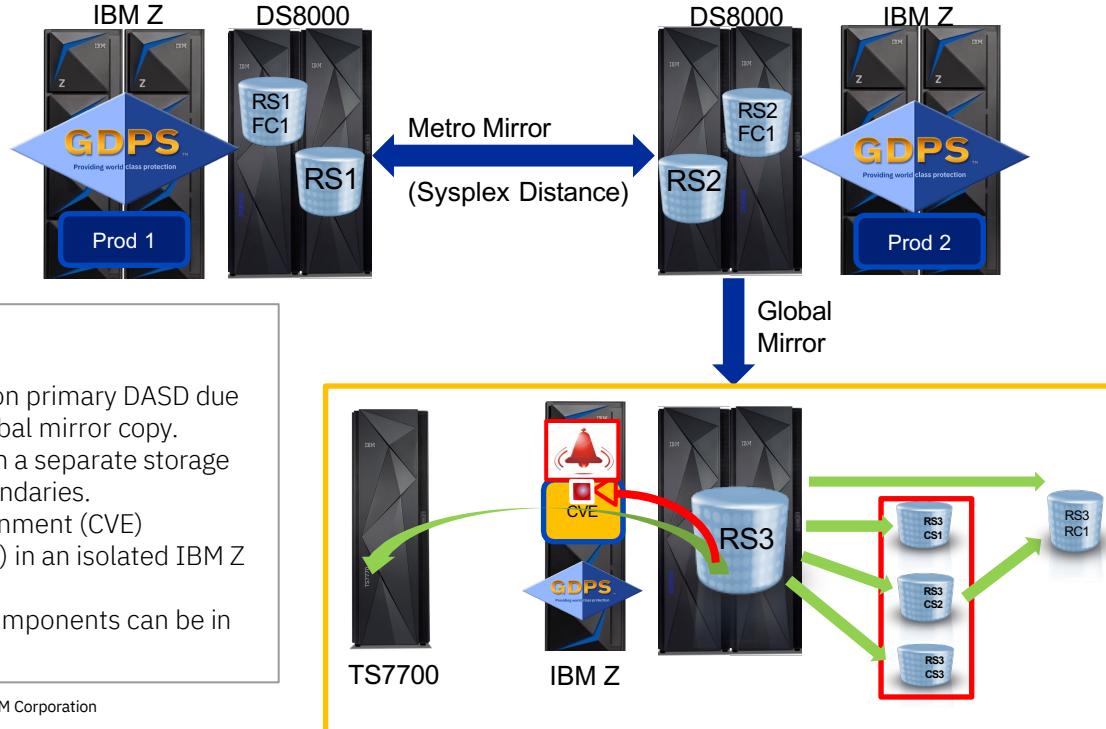
## Safeguarded Copy on DR site



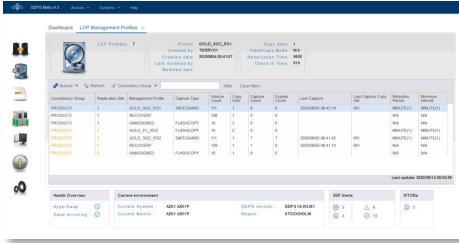
### Description:

- 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



# Management Solutions for Cyber Vault and Safeguarded Copy

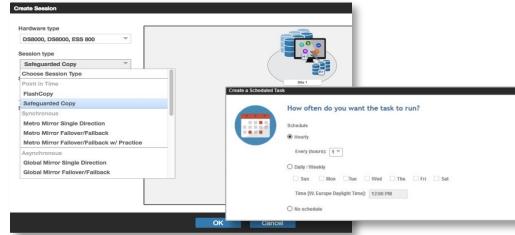


GDPS LCP Manager

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

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

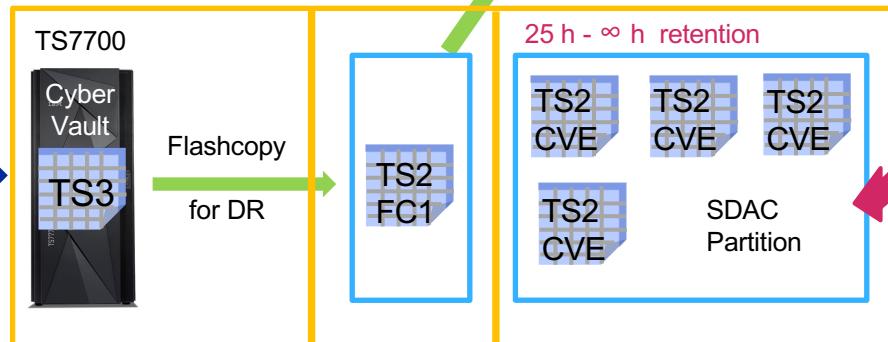
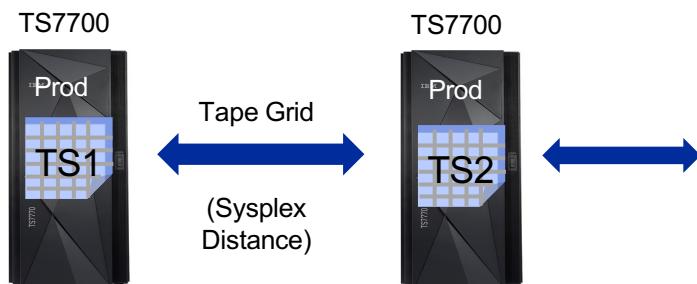
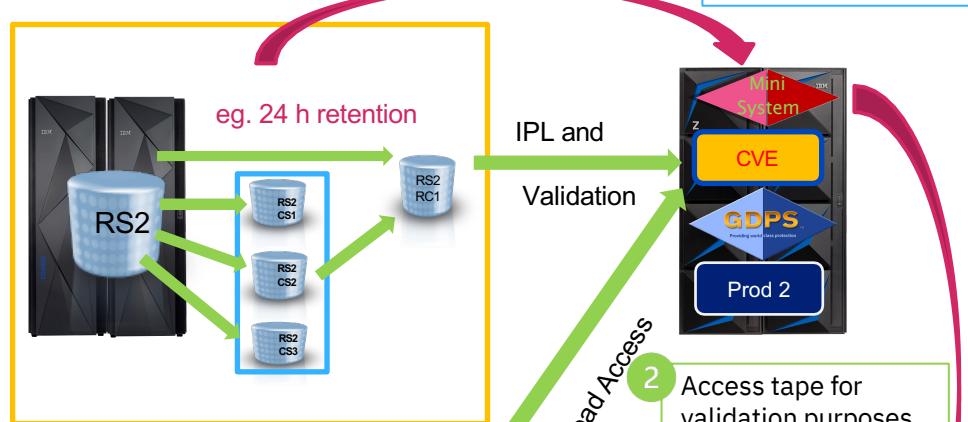


Copy Services Manager (CSM)

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

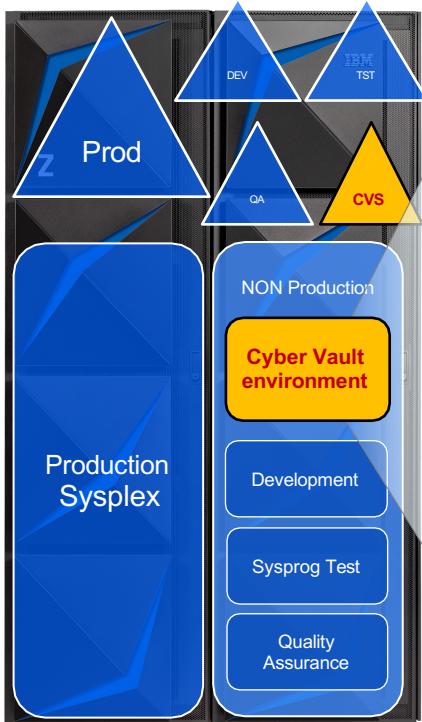
- Manage and monitor Safeguarded Copy sessions
  - *Create Safeguarded Copy Backups*
  - *Expire Safeguarded Copy Backups*
  - *Recover a Safeguarded Copy Backup*
  - *Display Volumes of a Safeguarded Copy Backup*
  - *Terminate a Safeguarded Copy session*
- Provides dual authentication control capability

# The role of Tape in a Cyber Vault implementation

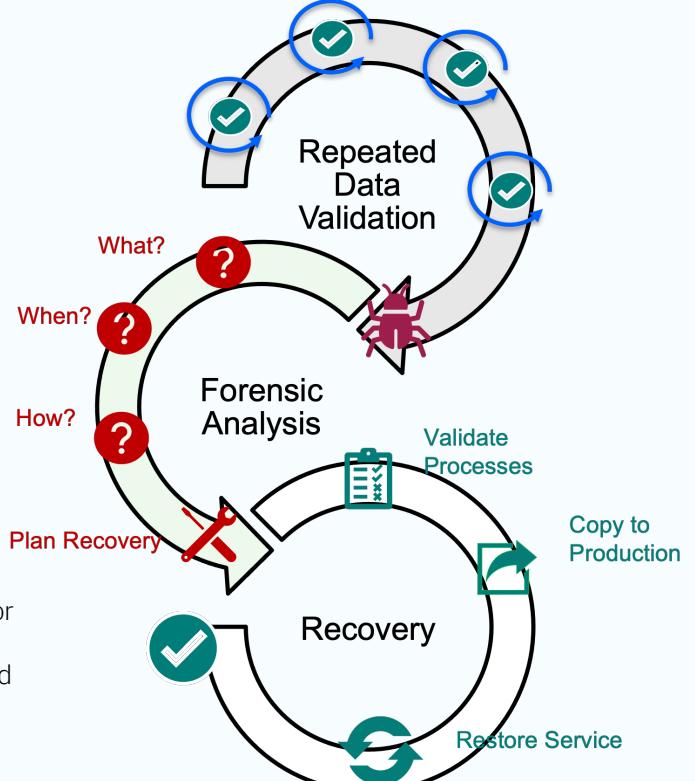


# Validating and Recovering your data

# The sooner you identify a problem, the smaller the impact will be.



- Repeatable and Automated
  - Time Consistent Copy is clean
  - System is operational
- 
- What, when and how data was corrupted?
  - Can't be automated
  - Tools may help, application knowledge is required
- 
- Execute Recovery Actions - Surgical or Catastrophic.
  - Use existing templates and predefined procedures



# Stay one step ahead with continuous data validation

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

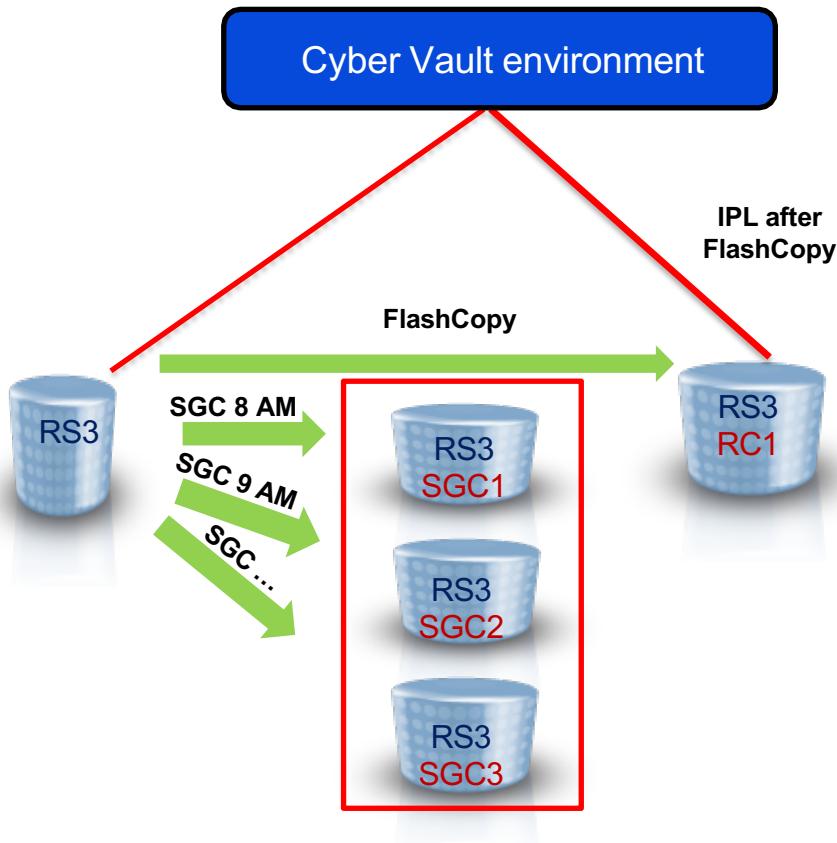
Performing corruption detection and validation processes against a copy of data is more practical than doing this in the live production environment.

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

Continuous data validation allows the early detection of a problem or reassurance that a given protection copy is uncorrupted.



# IBM Z Cyber Vault – Data validation concept



**As often as possible .....**

## Type 1: IPL with production images

- System Recovery Boost Upgrade record can be used to speed IPL
- Check Sysplex infrastructure
- Database and middleware restart and recovery

## Type 2: Data Structure Validation

- Db2 Utilities, Log analysis, index checking
- IMS Utilities
- 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

# Back trace a cyber attack by forensic analysis

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

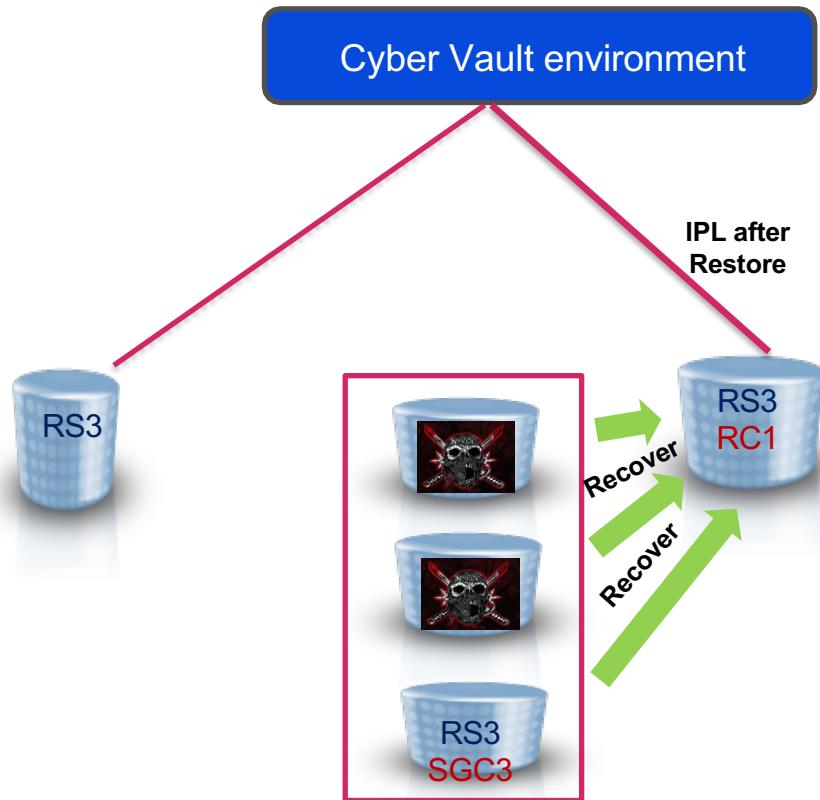
Based on this analysis, it can be determined how to proceed:

- 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)

A forensic analysis identifies the cause and scope of a problem before deciding on a recovery action.



# Forensic Analysis



## Determine start of data corruption ...

- **IPL and validate** one Safeguarded Copy after the other 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
- **Identify** steps forward
  - Create strategy for recovery dependent on availability of database image copy files.

# Surgical data recovery

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 actually corrupted data.

Surgical recovery consists of the extraction of specific data from a valid copy and logically restore it back to the production environment.



# Surgical Recovery - Scenarios

Surgical Recovery can be complex and it is dependent on which data is available where for restore and recovery. In case Surgical Recovery needs to be done, the first step is to identify the actual scenario.

## 1. Backups are available in Production

- Image Copy of database exist in the production environment

Test in Cyber Vault, recover in production (business as usual)

## 2. Backups are available in the Cyber Vault only

- Image Copy of database does not exist in the production environment
- Image Copies exist on DASD in the Cyber Vault environment

Recover and test in Cyber Vault, send to production

## 3. No Backups are available neither in Production nor in the Cyber Vault environment

- Image Copy of database does not exist in the production environment
- Image Copies do not exist on DASD in the Cyber Vault environment

Recover and test in Cyber Vault, send to production, ensure database integrity

# Catastrophic recovery

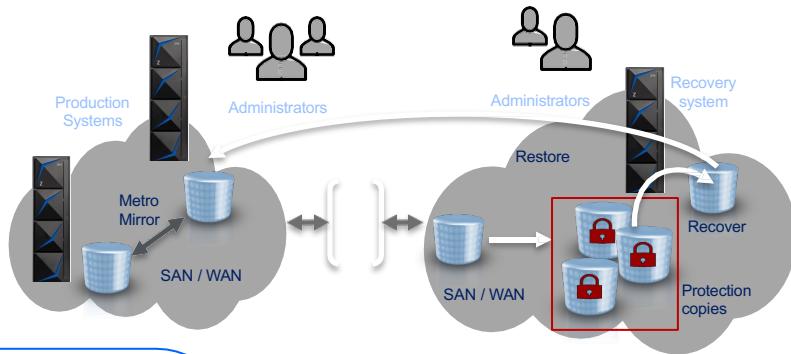
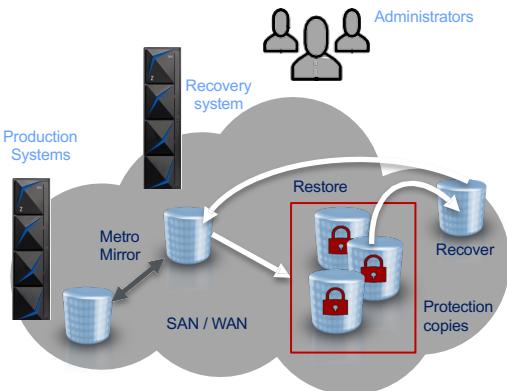
In the case of massive corruption to all or most of the data in the environment, a catastrophic recovery needs to take place.

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

Catastrophic recovery is needed, when forward fixing or surgical recovery is not an option due to the extensive spread of the corruption.



# Catastrophic recovery concept



Catastrophic Recovery solutions will vary from client to client. The unifying concept involves full restore to a defined point in time for the whole environment.

But it is up to the client if, in this case they start production from the DR site, Metro Mirror Site 1 or Metro Mirror Site 2, to name some options

# IBM Z Cyber Vault capabilities

## Data Validation

Detect data corruption early or certify that the copy is clear



IBM or Comparable ISV tools

IBM z/OS Utilities

## Forensic Analysis

Investigate the problem and determine the best recovery action



## Surgical Recovery

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



## Catastrophic Recovery

Recover the entire environment back to a point in time copy



## Offline Backup

Backup copy of the clean environment to offline tape media



IBM Z Catalog management tools

IBM Z Batch Resiliency

IBM DFSMShsm tools

IBM Security zSecure

Db2 and IMS Tools

# IBM Z Cyber Vault software selection – Start here

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
<b>IBM Tivoli Advanced Catalog Management for z/OS</b> Pointer checking for the catalog.	X	>I	Data Validation
Recovery of a catalog, including forward recovery to specific point in time.	>I	>I	Recovery
<b>IBM Tivoli Advanced Reporting and Management for DFSMShsm</b> 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.	X	>I	Data Validation
	X	>I	Forensic Analysis
<b>IBM Tivoli Advanced Audit for DFSMShsm</b> Conduct trouble-free audits and automate corrective actions.	X	>I	Recovery
<b>IBM Security zSecure Audit</b> Potential identification of malicious database activities to help identify starting point of corruption.			
<b>IBM CICS VSAM Recovery</b> 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.			



# IBM Z Cyber Vault software selection – 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 selection – IMS

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

## Solution

### **IBM IMS High Performance Pointer Checker**

Pointer checking IMS full function databases

### **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

### **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

### **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

P CV Capability

x CV Data Validation

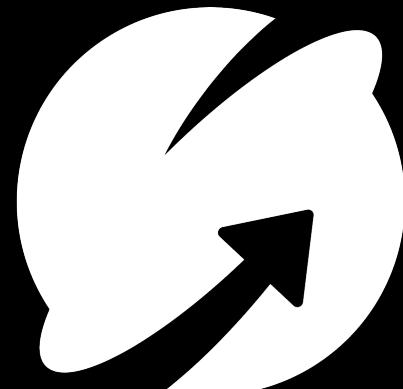
x CV Forensic Analysis

x CV Forensic Analysis

x CV Forensic Analysis

x CV Forensic Analysis

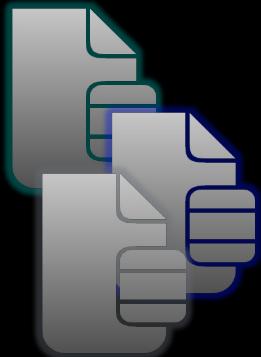
x CV Surgical Recovery



# IBM Z Cyber Vault software – 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

**Schedule an IZBR Cyber Vault soon!**

# Offline Backups

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.

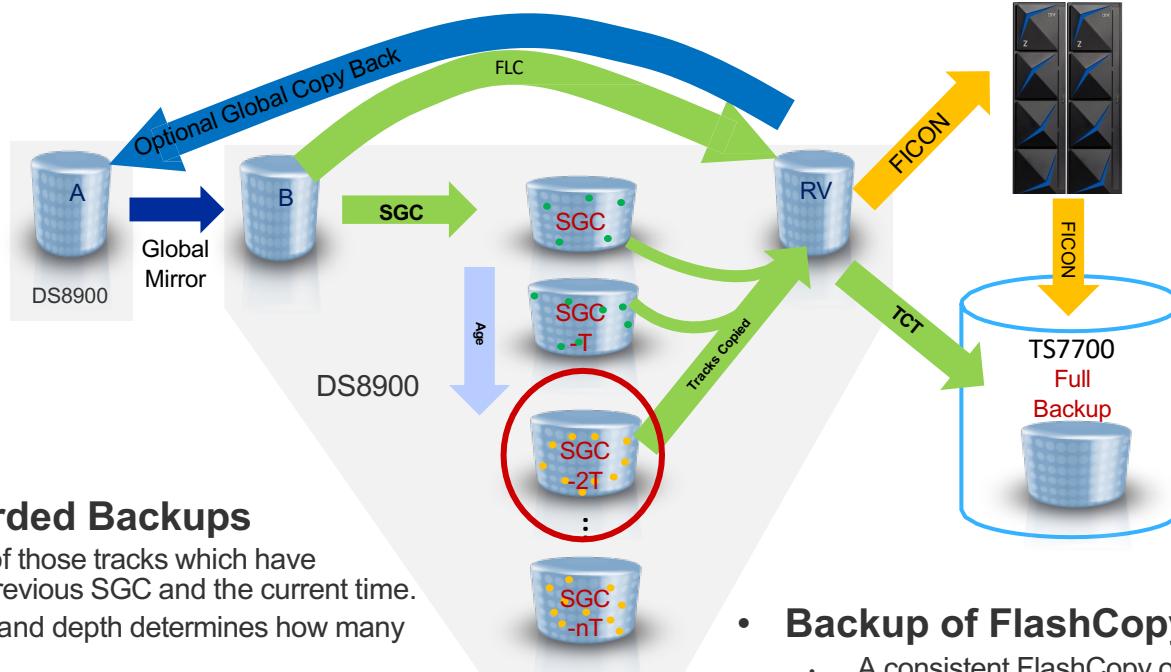
Storing validated point in time copies on media like virtual tape or cloud object storage gives you a lower cost solution for longer term retention.

Creating offline backups from your IBM Z Cyber Vault extends your ability to restore services from older point in copies.



# Option 1 (Today) - Safeguarded Copy and full backups

IBM



## • DS8000 Safeguarded Backups

- Each SGC is made up of those tracks which have changed between the previous SGC and the current time.
- A configured frequency and depth determines how many SGCs are retained
- Instant recovery can be performed to a set of Recovery Volumes
- Incremental restore to production can be done from the Recovery Volumes to a PPRC partner of the Safeguarded Source

## • Backup of FlashCopy

- A consistent FlashCopy or recovered Safeguarded Backup can be backed up to a TS7700 using DSS or other host software
- Full restore can be performed to any volumes on the same or different DS8000

# Next Steps

# IBM Z Cyber Vault

## Discovery and Architecture Workshop

IBM Client Engineering 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.

