Logical Corruption Protection and Cyber Resiliency for Z

Nick Clayton
Distinguished Engineer,
Enterprise Storage Development
claytonn@uk.ibm.com

IBM

The question is not IF you will be attacked but WHEN

$170 B

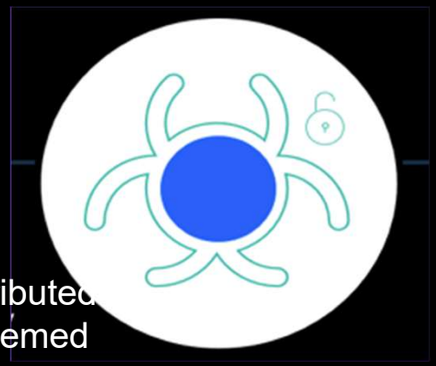
Predicted global ransomware demands WW forecast [6]

2000%

Explosive growth of attacks on enterprise operations 2019 compared to 2018 [1]

$8 Billion

Estimated global cost of WannaCry attack [3]



+ 50+

Unique malware distributed in various Covid-19 themed campaigns [4]

67%

Average increase in ransomware destructive attacks in 2019 [1]

$230 Million

GDPR fine for one data breach [5]

111K

Average ransomware cost up from 6700 in 2018 [2]

1. X- force intelligence index report 2020
2. Forbes Aug 18,2020
3 ReInsurance news May 23 2017
4,XF IRIS internal data analysis IBM 2020
5 Compliance Week July 8, 2019
6. MSSP Alert Feb 13,2020

solarwinds

Orion: More US government agencies hacked

BBC NEWS

HONDA

Honda Hackers May Have Used Tools Favored by Countries

The New York Times

REUTERS

'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals

GARMIN

The Garmin Hack Was a Warning

As ransomware groups turn their attention to bigger game, expect more high-profile targets to fall.

WIRED

The Register

Major bank-logic bomber jailed for eight years

Real-life BOFH ordered to pay $3.1m restitution

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

“If our cyber defenses fail ....
.... how could we recover our 300 most critical services within 24 hours?”

Focus

How do we reduce outage time as a result of corruption or destruction of data and systems ?

Problem

Existing HA/DR protects from physical infrastructure outages.
Traditional backups are specific to individual databases and do not allow re-creation of a consistent system image.

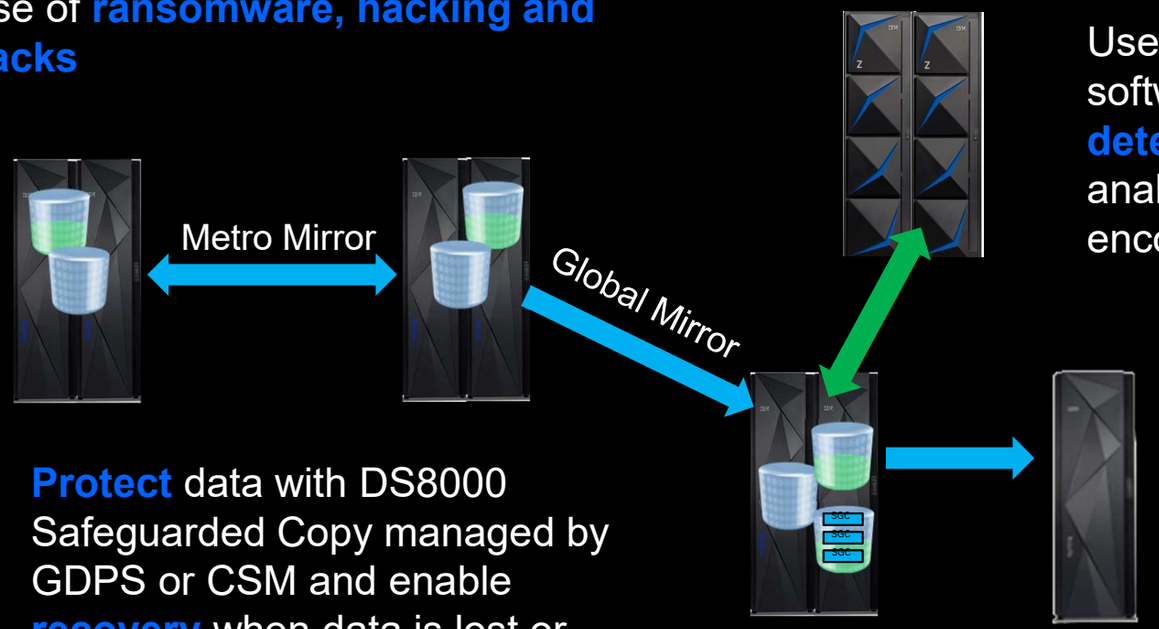
Solution

Establish a set of recent ‘point in time’ copies of the entire system, with ability to regularly inspect quality of data in the isolated vault, and test recovery scenarios.

Cyber Vault for IBM Z

Logical corruption can happen for a wide range of reasons and in many ways. As well as malicious activity, user error or application issues can cause corruption or destruction of data.

Metro Mirror and HyperSwap provide HA and DR but do not protect against **logical corruption** which is a significant concern given the rise of **ransomware, hacking and insider attacks**



Use a **recovery system** and IBM Z software to perform data validation to **detect** issues and perform forensic analysis to **respond** when a problem is encountered

Protect data with DS8000 Safeguarded Copy managed by GDPS or CSM and enable **recovery** when data is lost or corrupted

Optionally perform **offline backup** from the data vault to TS7700 to enable longer retention and greater isolation

Implement a **virtual isolation** or **physical isolation** configuration depending on security requirements and budget

Cyber Vault structure

Batch resiliency

Surgical recovery

Automated validation

500 Immutable DISK copies

Isolated Environment for Analysis

Tape Logical WORM and expire hold

Application dependency visualization

Tape Flashcopy for D/R

Integrated in known D/R management tools

Cyber Vault is a "Project" not a feature

Cyber Resiliency lifecycle (based on "*NIST Cybersecurity Framework*")

IDENTIFY

Risks and vulnerabilities

PROTECT

Your critical applications and data

DETECT

Data corruption and configuration anomalies

RESPOND

To changes in configuration and data

RECOVER

Access to critical applications and data

Production Environment:

- RACF two Factor authentication
- Guardium
- zSecure
- Qradar
- .....

Cyber Vault Environment:

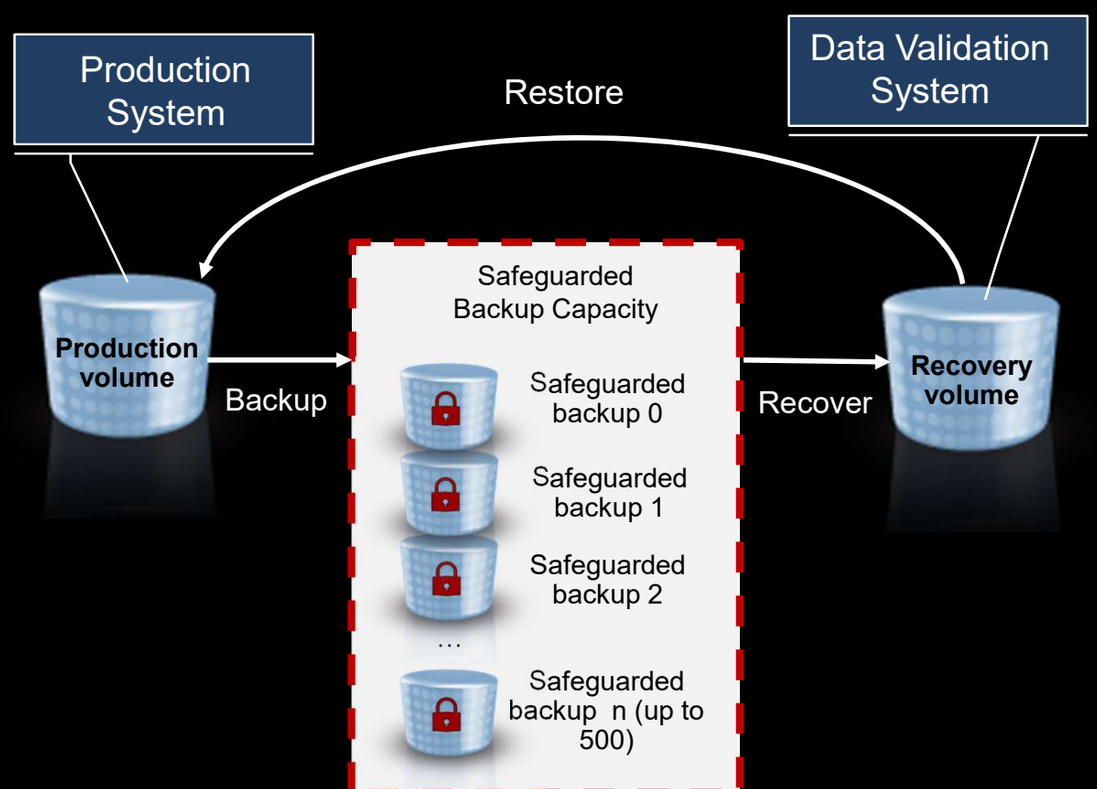
- Separated Hardware, Storage and Network
- Db2 Utilities, IMS Utilities, DFHSM Audit, Catalog check, etc.
- Ability to try out "forward fixing" and "surgical recovery" without risk
- Recovery of data to production after fixing has been done

NIST = National Institute of Standards and Technology of the USA Government

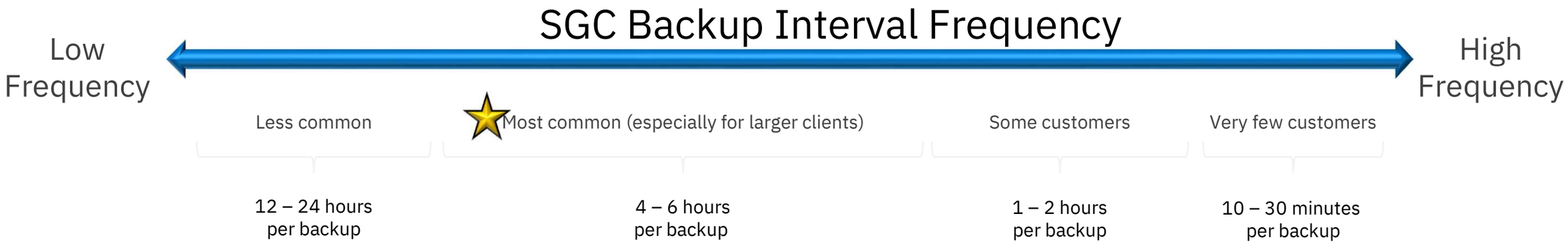
Safeguarded Copy for data corruption protection

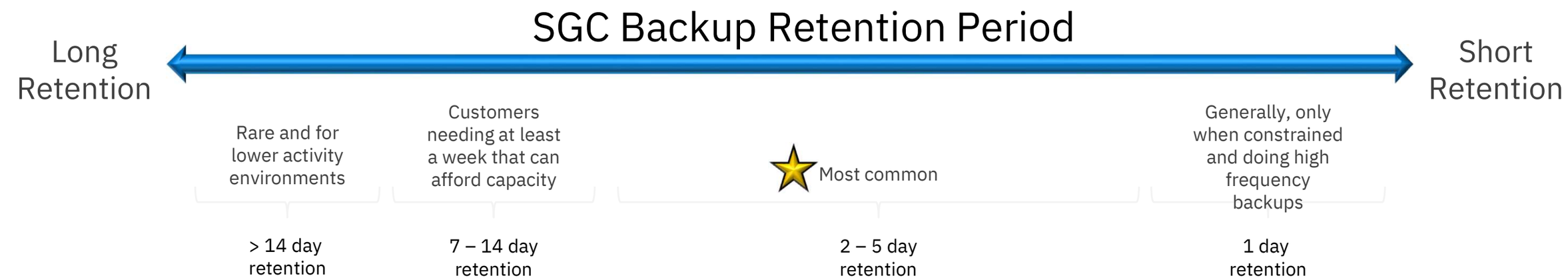
- Safeguarded Copy provides functionality to create up to 500 Safeguarded Backups for a production volume
- They are stored in a storage space that is called Safeguarded Backup Capacity which is hidden and not accessible by any server
- The data can only be accessed after a Safeguarded Backup is recovered to a separate recovery volume.
- Recovery volumes can be used with a data recovery system to perform data validation, forensic analysis or to restore production data.

IBM DS8000 Safeguarded Copy prevents sensitive point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks

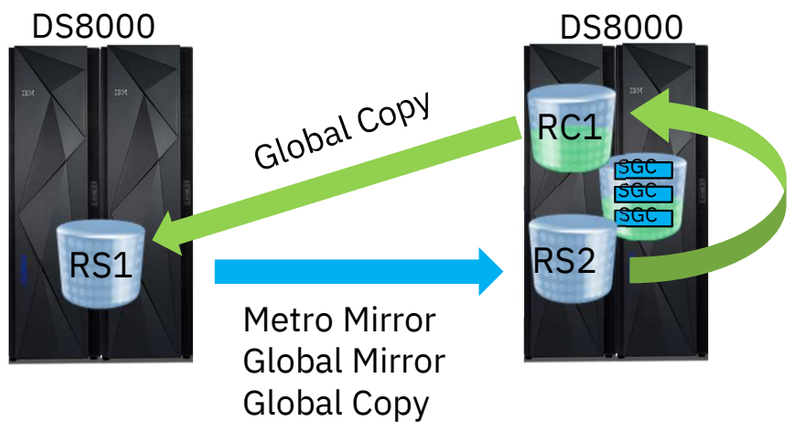


Typical Backup Interval Frequency & Retention Periods





Safeguarded Copy Incremental Restore to Production – new with DS8900 R9.2



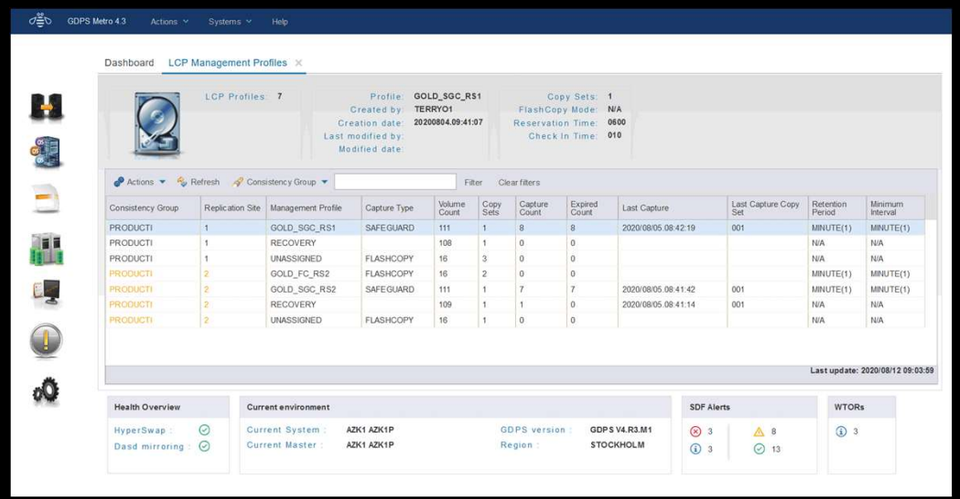
Enable a user to restore a recovered Safeguarded Copy back to a Production copy of data using an incremental Global Copy rather than the full Global Copy required today.

The Global Copy is performed back to the PPRC pair of the Safeguarded Source device (RS1 in the picture) enabling this to be done both in physical isolation and virtual isolation scenarios.

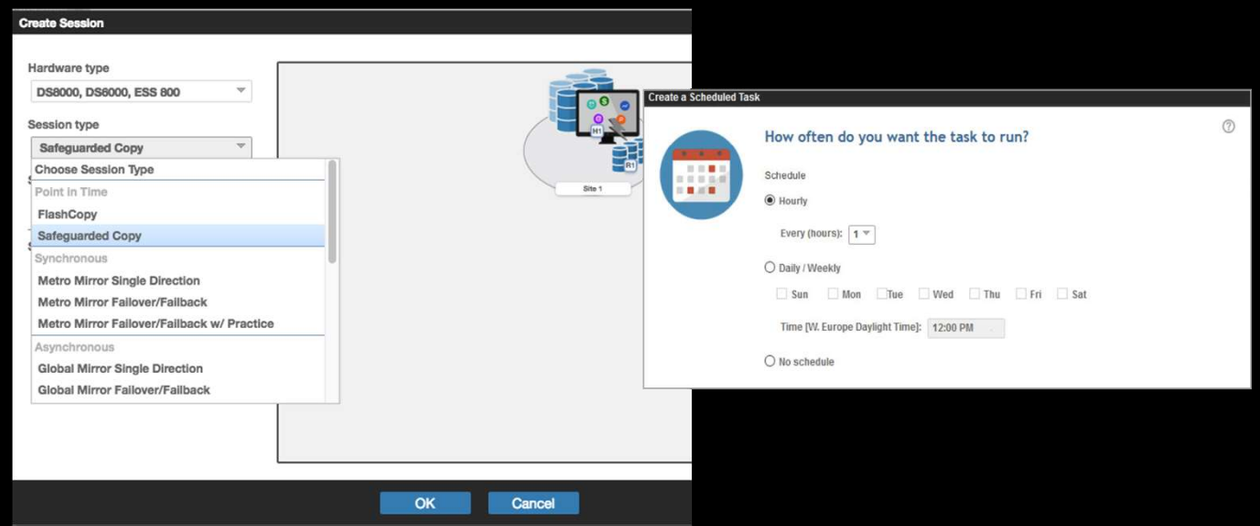
The amount of data copied back and time to copy will depend on the time and changes since the particular backup that is being restored

GDPS/LCP or CSM can both manage SafeGuarded Copy

Manage the whole Data Corruption Protection lifecycle with the same tool you manage your CA and DR environment with – GDPS/LCP is an enhancement to existing GDPS implementations. CSM can manage all DISK copy services.



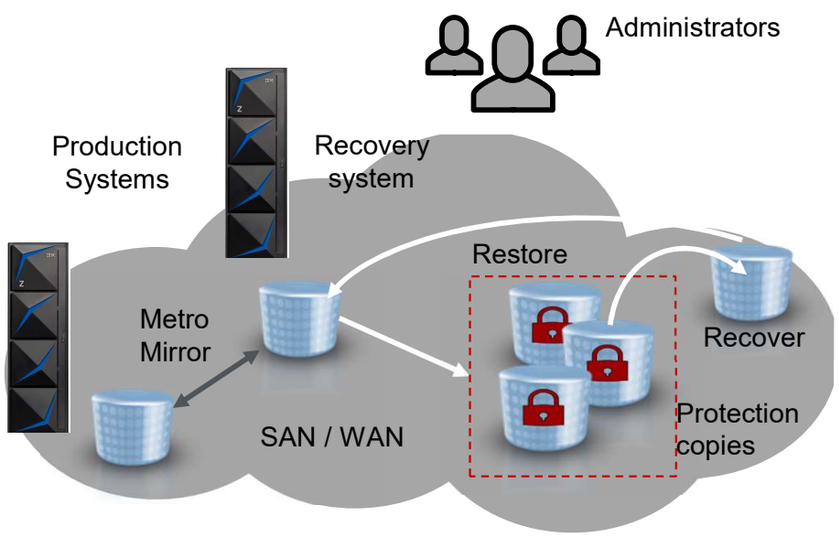
GDPS / LCP



CSM

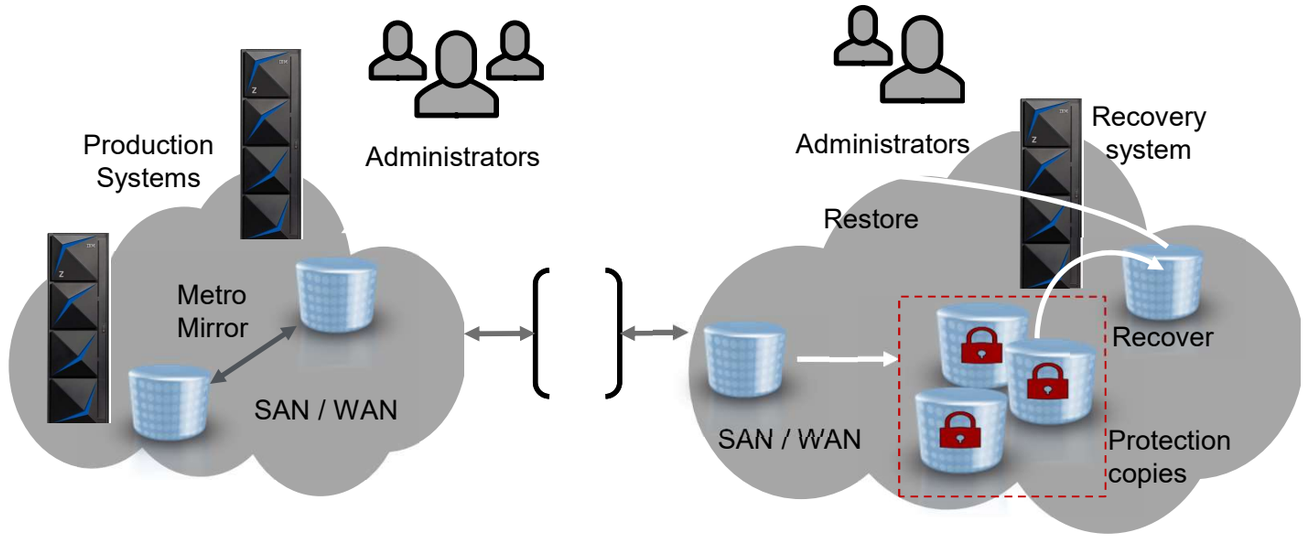
Different levels of isolation

Virtual Isolation



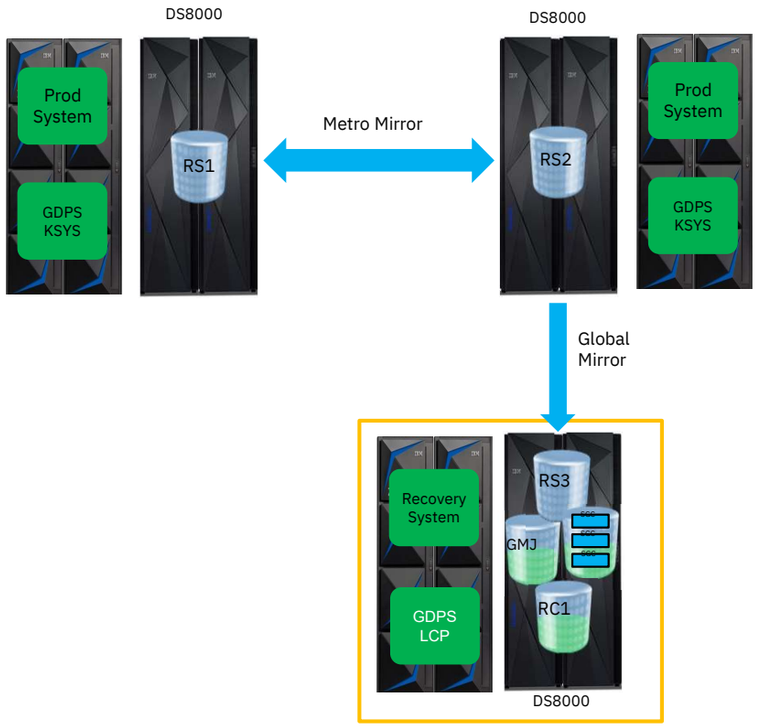
- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

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

Example LCP Topology
Metro Mirror Physical Isolation



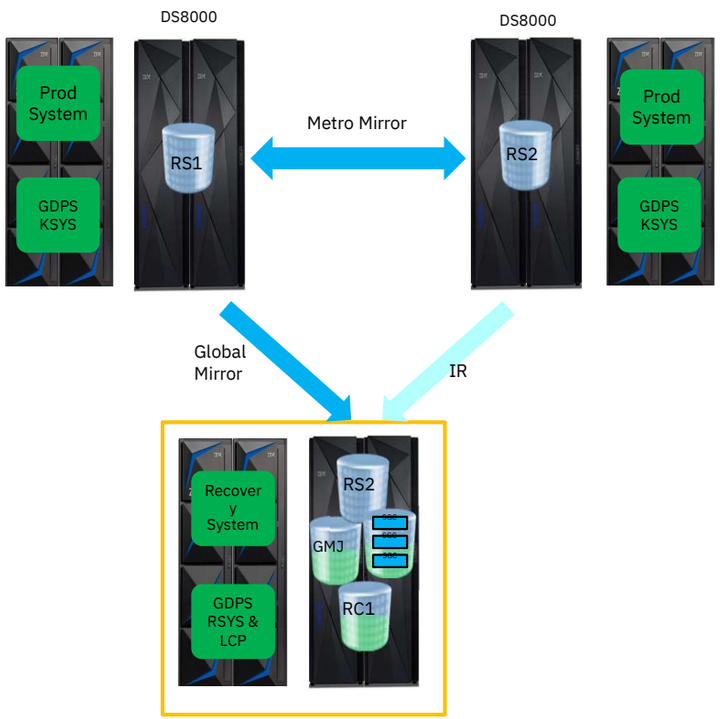
Safeguarded Copy on Global Mirror secondary device

Separate GDPS Metro and GDPS Global with LCP license

Direct connectivity for LCP system to Global Mirror source DS8000

Safeguarded capture taken using Global Mirror pause with consistency with no impact to production IO

Example LCP Topology
Metro Global Mirror Virtual Isolation



Safeguarded Copy on Global Mirror Secondary in Disaster Recovery location

Global Mirror suspended with consistency to perform captures

No production impact with LCP capture process but Global Mirror will be paused for some seconds each time a Safeguarded Backup is taken

LPAR(s) for Recovery System in Disaster Recovery location on same Z server also typically used for DR and GDPS RSYS

GDPS LCP Capture Process

```
13:54:36  $$_SGC1RS2_CAPTURE PLANNED/STANDARD ACTION STARTED FROM STEP 1
13:54:36  LCP=CAPTURE PROFILE(SGC1RS2) STARTED
13:54:36  SCHEDULING LCP CAPTURE FOR MANAGEMENT PROFILE SGC1RS2
13:54:36  SEQUENCE NUMBER 610A9C1C HAS BEEN GENERATED FOR THIS SAFEGUARD CAPTURE
13:54:36  GEO2772I SAFEGUARD CAPTURE PHASE 1 RESERVATION STARTED
13:54:38  GEO2773I SAFEGUARD CAPTURE PHASE 1 RESERVATION ENDED SUCCESSFULLY
13:54:38  GEO2772I SAFEGUARD CAPTURE PHASE 2 RESERVATION SCAN STARTED
13:54:59  GEO2773I SAFEGUARD CAPTURE PHASE 2 RESERVATION SCAN ENDED SUCCESSFULLY
13:54:59  GEO2772I SAFEGUARD CAPTURE PHASE 3 CHECKIN STARTED
13:55:01  GEO2957I THE USER IMPACT TIME (UIT) FOR THIS SAFEGUARD CAPTURE WAS 0.911 SECONDS
13:55:01  GEO2773I SAFEGUARD CAPTURE PHASE 3 CHECKIN ENDED SUCCESSFULLY
13:55:01  GEO2775I LCP SAFEGUARD CAPTURE ENDED SUCCESSFULLY
```

Safeguarded Copy Backup
with GDPS Metro

Safeguarded Copy Backup
with GDPS Global

```
14:28:58  AAA_CAP_GOLD_SGC_RS1 PLANNED/STANDARD ACTION STARTED FROM STEP 1
14:28:58  LCP='CAPTURE PROFILE(GOLD_SGC_RS1)' STARTED
14:28:58  SCHEDULING LCP CAPTURE FOR MANAGEMENT PROFILE GOLD_SGC_RS1
14:29:00  SEQUENCE NUMBER 5F96CF1B HAS BEEN GENERATED FOR THIS SAFEGUARD CAPTURE
14:29:00  GEO2772I SAFEGUARD CAPTURE PHASE 1 RESERVATION STARTED
14:29:00  GEO2773I SAFEGUARD CAPTURE PHASE 1 RESERVATION ENDED SUCCESSFULLY
14:29:00  GEO2772I SAFEGUARD CAPTURE PHASE 2 RESERVATION SCAN STARTED
14:29:22  GEO2773I SAFEGUARD CAPTURE PHASE 2 RESERVATION SCAN ENDED SUCCESSFULLY
14:29:22  GEO2949I SCHEDULING CGPAUSE FOR SESSION PRODUCTI
14:29:23  GEO2950I MONITORING COMPLETION OF CGPAUSE FOR SESSION PRODUCTI
14:29:23  GEO2951I SESSION PRODUCTI HAS BEEN SUCCESSFULLY CGPAUSED
14:29:23  GEO2772I SAFEGUARD CAPTURE PHASE 3 CHECKIN STARTED
14:29:25  THE CHECKIN TIME FOR THIS SAFEGUARD CAPTURE WAS 0.760 SECONDS
14:29:25  GEO2773I SAFEGUARD CAPTURE PHASE 3 CHECKIN ENDED SUCCESSFULLY
14:29:25  GEO2949I SCHEDULING RESUME FOR SESSION PRODUCTI
14:29:27  MONITORING SESSION PRODUCTI FOR 'RUNNING' STATE
14:29:28  SESSION PRODUCTI WAS RETURNED TO 'RUNNING' STATE IN 3.064 SECONDS
14:29:28  GEO2951I SESSION PRODUCTI HAS BEEN SUCCESSFULLY RESUMED
14:29:30  GEO2775I LCP SAFEGUARD CAPTURE ENDED SUCCESSFULLY
14:29:30  LCP='CAPTURE PROFILE(GOLD_SGC_RS1)' ENDED RC=0
14:29:30  AAA_CAP_GOLD_SGC_RS1 PLANNED/STANDARD ACTION ENDED
```

Use cases for logical corruption protection copies

Data Validation
Regular analytics on the copy to provide early detection of a problem or reassurance that the copy is a good copy prior to further action

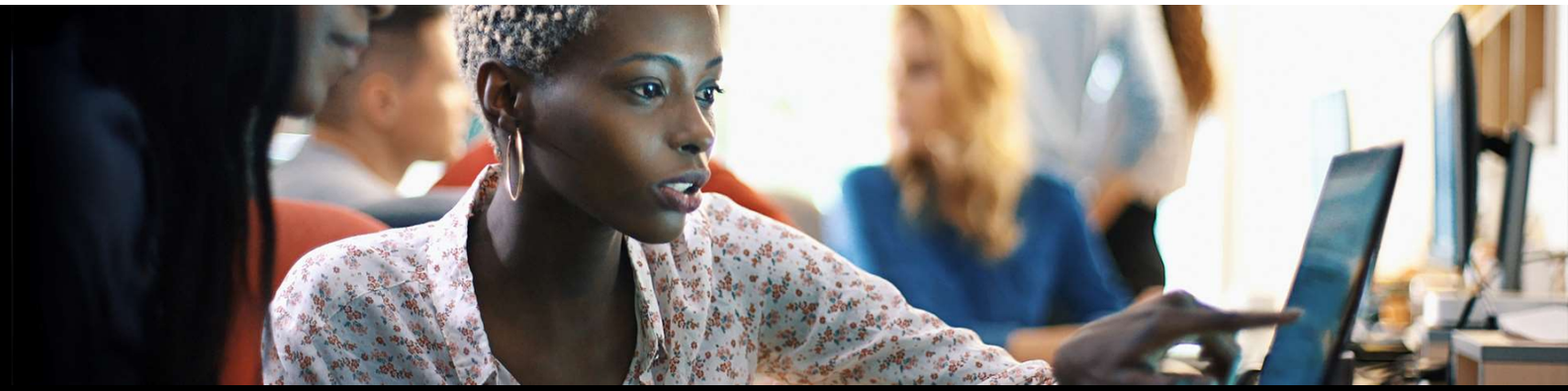
Forensic Analysis
Start a copy of the production systems from the copy and use this to investigate the problem and determine what the recovery action is

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 if this is the only recovery option

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

Data validation steps



Phase 1 (IPL)

- The production system will be IPLed from a recovery volume, but in a separated LPAR
- During the IPL, basic infrastructure functionality will be tested (Sysplex, Data sharing, Logger, JES2, etc.)
- Once all subsystems have been restarted successfully (with no connectivity to the outside world of course, see network considerations earlier in this presentation) phase 1 can be considered being finished successfully

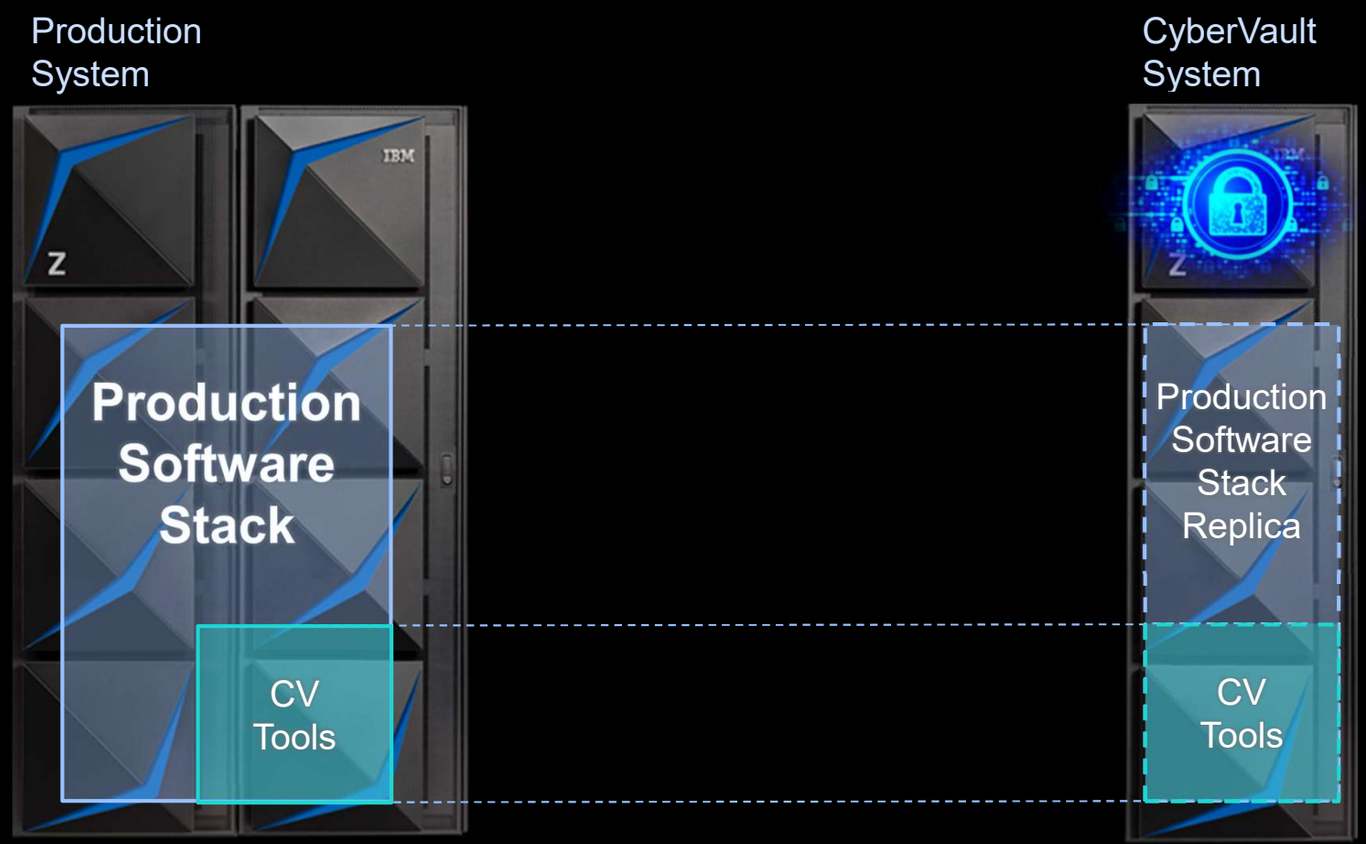
Phase 2 (Data Structure Validation)

- In this phase INDEX and DATA structures of a database are checked. IMS pointer chains for example, Catalog pointers, DFSMShsm control datasets etc.
- In order to do the structure validation several tools like Db2 Utility Suite are available to speed up processing

Phase 3 (Data Content Validation)

- During the last phase of the validation procedure we will run customer provided application programs to get an application view of the data
- This is the only way to check the quality of the data in the databases

IBM **Z Cyber Vault** Software Stack



Surgical Recovery - Scenarios

Surgical Recovery is rather complex and the execution is dependent mainly 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

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

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

Data Types on z/OS

Primary Storage resident data and its replicated copies

- This data would be protected in the first instance by Safeguarded Copy
- A further offline backup of this data to Virtual Tape can be taken within the Cyber Resilience environment

Backup data on Virtual Tape

- Already a copy of data which is also being copied on the disk based PiT copies
- This is likely the first line of defence for any limited scope corruption event so still important to secure it

Master data on Virtual Tape (DFHSM ML2, OAM, batch input/output data)

- This data needs to be protected as it only exists on virtual tape
- There is no guaranteed consistency today of this data with the replicated copies of primary storage and this would be the same for any copies made for LCP purposes

Logical WORM and Expire Hold with TS7700

Most use cases for tape can exploit logical WORM including DFHSM, OAM etc

- This requires that a tape is only opened for read or append once it is first written
- If there is a specific application/use that does not support logical WORM it can be separated in its own dataclass

Logical WORM status for a logical volume cannot be changed except by returning to scratch

- Increasing the Expire Hold period can provide a grace period in which the data can still be recovered and custom roles can be used to prevent users from having access to this task.

Previous recover points of the primary data will contain tape catalogs which reflect the content of these tapes and in the case of a restore to this point in time they can be set back to an Active state for the data to be accessed

Tape Grid functionality used for Cyber Vault

Read access to tapes during validation process

- In order to be able to read tapes as input during the validation process, a Flashcopy for DR of the tape environment needs to be created at the same time the Safeguarded Copy is taken.
- Access to the production tape environment is in no case granted to the Cyber vault environment and vice versa.
- Before initiating a new TS7700 Flashcopy for DR supporting a new Cyber Vault validation, the previous TS7700 Disaster Recovery Test must be ended

Partitioning the Tape Grid

- For clients who intend to elongate their retention period of the Safeguarded Copies a copy to tape is possible.
- Using “Selective Device Access Control (SDAC) “ is possible to partition the TS7700 for different LPARs.
- In case a client chooses this option, a sepeate SYSTEM (eg. GDPS K System) is required to manage the copies to tape. TCT can also be used as methodology to create Full Volume Dumps to tape.

Cyber Vault for IBM Z

Logical corruption can happen for a wide range of reasons and in many ways. As well as malicious activity, user error or application issues can cause corruption or destruction of data.

Metro Mirror and HyperSwap provide HA and DR but do not protect against **logical corruption** which is a significant concern given the rise of **ransomware, hacking and insider attacks**

Use a **recovery system** and IBM Z software to perform data validation to **detect** issues and perform forensic analysis to **respond** when a problem is encountered

Protect data with DS8000 Safeguarded Copy managed by GDPS and enable **recovery** when data is lost or corrupted

Optionally perform **offline backup** from the data vault to TS7700 to enable longer retention and greater isolation

Implement a **virtual isolation** or **physical isolation** configuration depending on security requirements and budget