IBM Z Cyber Vault

Matthias Bangert
Executive IT-Specialist,
Worldwide Technical Sales, IBM Z
matthias.bangert@de.ibm.com

December 2020

IBM

The question is not IF you will be attacked, but WHEN

$53 Billion

Predicted economic losses of the next global cyber attack

$3.86 Million

Average total cost of a data breach*

$8 Billion

Estimated global cost of WannaCry attack*

+ $137,000

Increase in data breach and incident response time costs due to remote work during COVID-19*

280 Days

Average amount of time hackers spend inside IT environments before discovery*

$230 Million

GDPR fine for one data breach*

- Cost of a Data Breach Report 2020, Ponemon Institute
- Riensirce news May 23 2017

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

UBS 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.

What are we protecting against ?

1.) Ransomware **attacks**, cyber threats, external malicious activities (Honda, APMM, Software AG, ...)

2.) **Insider threats**. People with admin rights for example could damage databases etc. before leaving the company (2 clients I know of)

3.) **Mistakes**, people are making. For example: wrong data used in production, wrong fields in database deleted etc. (3 companies I know of)

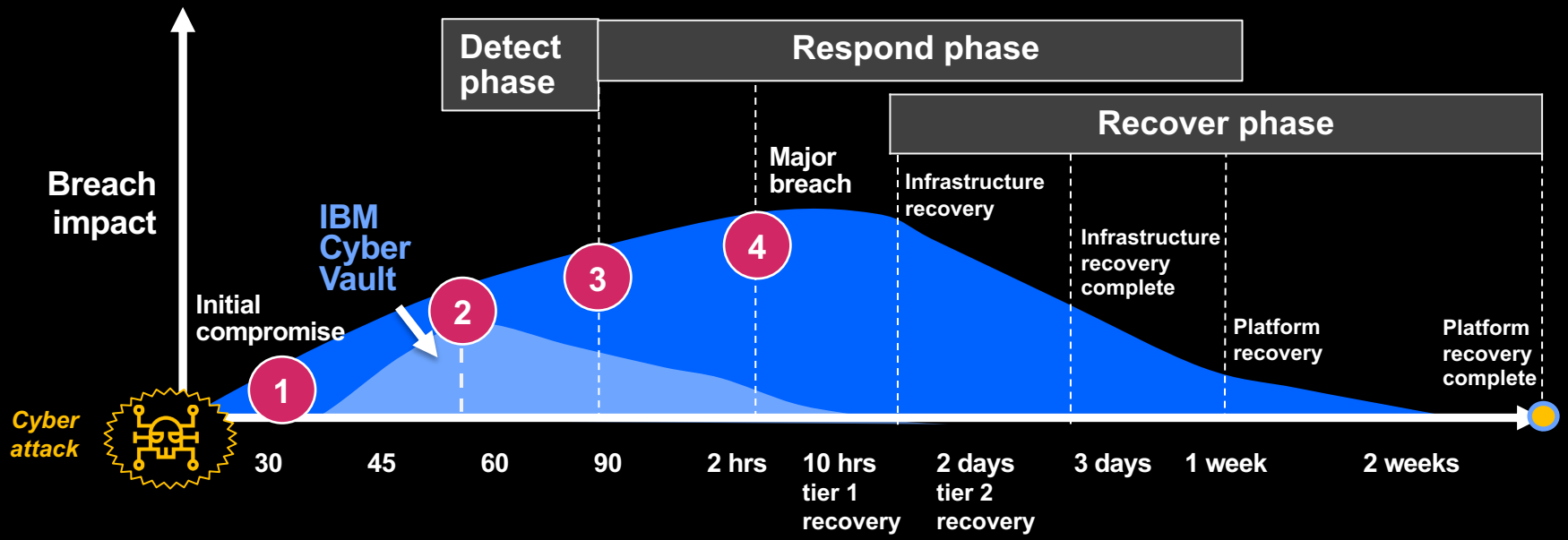
Why should you care?

Many clients might say “we have tape backups” – but tape access can’t be shared, which means recovery will take long, for many too long.

And by the way – single database backups will not be consistent across applications, which leads to unforeseeable problems once you restore.

And finally – have you ever tried to test a complete system recovery from single database image copies?

Speed recovery to significantly reduce the impact of breaches



1. Corruption of data occurs – but not yet detected
2. Due to the Cyber Vault environment and the use of SafeGuarded Copy technology, data is continuously checked and corruption is found and corrected
3. Without the Cyber Vault environment corruption is detected much later and has a greater chance to spread
4. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

Why traditional resiliency solutions won't protect you from logical data corruption

	You have	What is required
Replication	Data is being replicated continuously but logical errors are also replicated instantaneously	Scheduled point in time copies stored in an isolated, secure location
Error detection	Immediate detection of system and application outages	Regular data analytics on point in time copies to validate data consistency
Recovery points	Single recovery point that likely will be compromised	Multiple recovery points
Isolation	All systems, storage and tape pools participate in the same logical system structure	Air gapped systems and storage so that logical errors and malicious intruders can not propagate
Recovery scope	Continuous availability and disaster recovery	Forensic, surgical or catastrophic recovery capabilities

IBM Z Cyber Vault solution

IBM storage

Data volumes and active copies generated and maintained

DS8000 SafeGuarded Copy

Immutable backups

TS7700 Virtual Tape with Encryption and/or WORM

Secure air-gapped data vault

IBM Z and Software

The only System with a 99.99999% availability

EAL 5+ certified IBM Cyber Vault for Z LPAR for validation, testing and forensics

Data monitoring, consistency and anomaly detection

Management Software

IBM Security solutions

IBM Services

IBM GDPS provides services, clustering technologies, and server and storage replication and automation

Logical Data Corruption (LCP) and Copy Services Manager (CSM) enhancements manage the entire recovery environment

IBM Lab Services risk assessment and deployment services

Challenges with using FlashCopy for logical corruption protection

(... and the reason why we needed to improve it and come out with something new)

Addressing requirements of multiple FlashCopy target devices

- Each FlashCopy target consumes a volume on the DS8K restricting the number of copies that can be created
- FlashCopy target devices could also consume UCBs although planned LCP enhancements remove this requirement
- Limit of 12 copies also an issue although other considerations probably mean this limit is not reached in practice

Space requirements using thin provisioned devices

- The 21cylinder allocation unit used for Extent Space Efficient devices is optimised for host and FlashCopy performance and is not as efficient as a smaller (e.g. track level) allocation unit especially for sparse updates

Performance impact of maintaining large number of FlashCopy relationships

- Updates to the production volume are copied to all FlashCopy target devices increasing the impact as more FlashCopies are created

Securing the FlashCopy target volumes

- FlashCopy volumes are normal production volumes and can be mapped to a host so extra efforts need to be made to secure these

IBM Z Cyber Vault (principal idea)

IBM Z & Storage are introducing a joint play that will enhance the data and operations security of your clients.

Description:

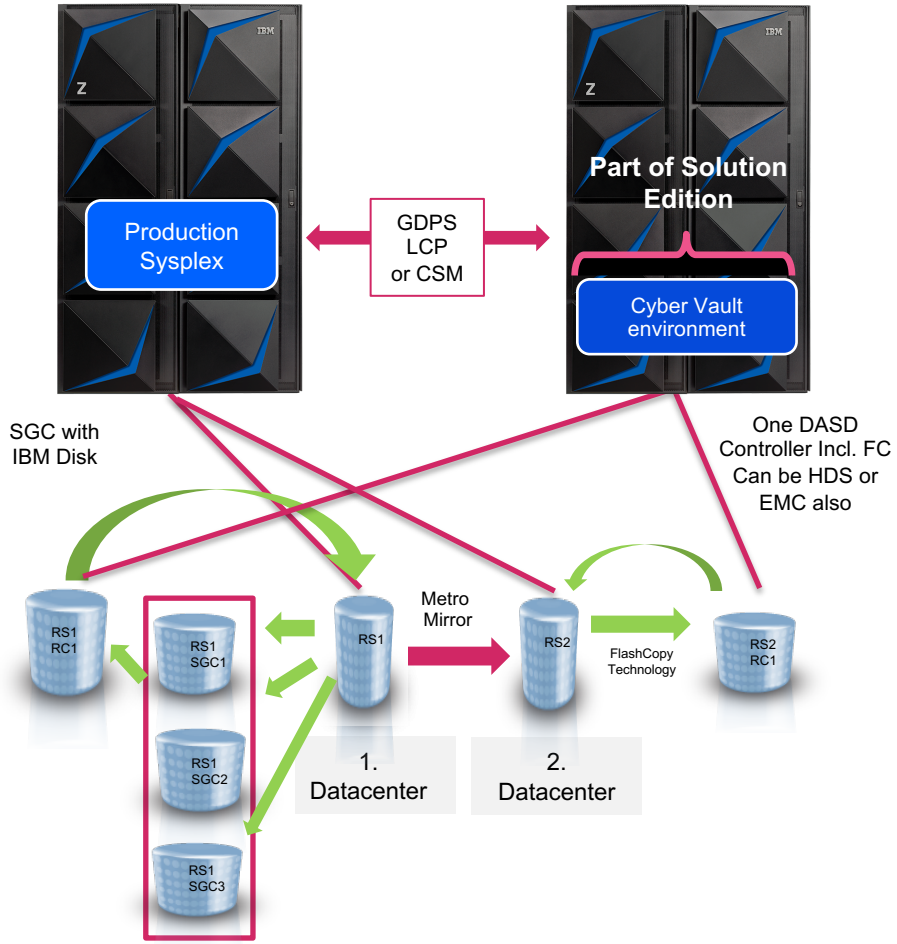
Reduce the time to recovery from days to minutes, by implementing a Data Corruption Protection solution as part of your D/R strategy

Concept:

1. Start by implementing a Cyber Vault environment
2. Add storage to allow for consistent copies
3. Manage solution with GDPS/LCP or CSM
4. Add software for enhanced validation

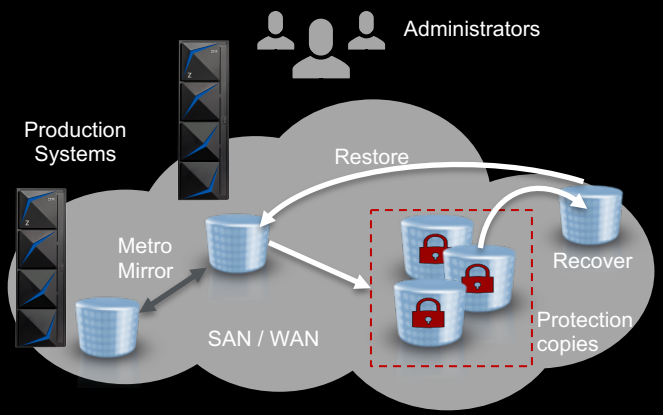
Benefit to the client:

- Data Validation
- Forensic Analysis
- Surgical Recovery
- Catastrophic Recovery
- Offline Backup



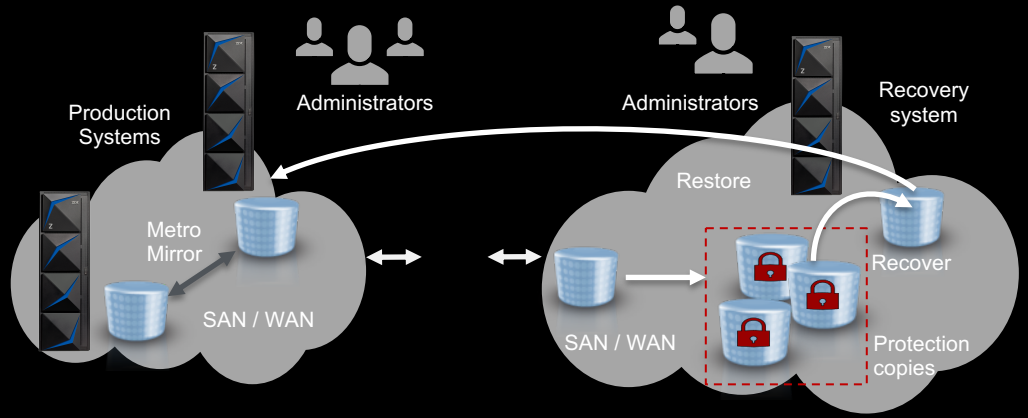
Air gap: Virtual and physical isolation of protection copies

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

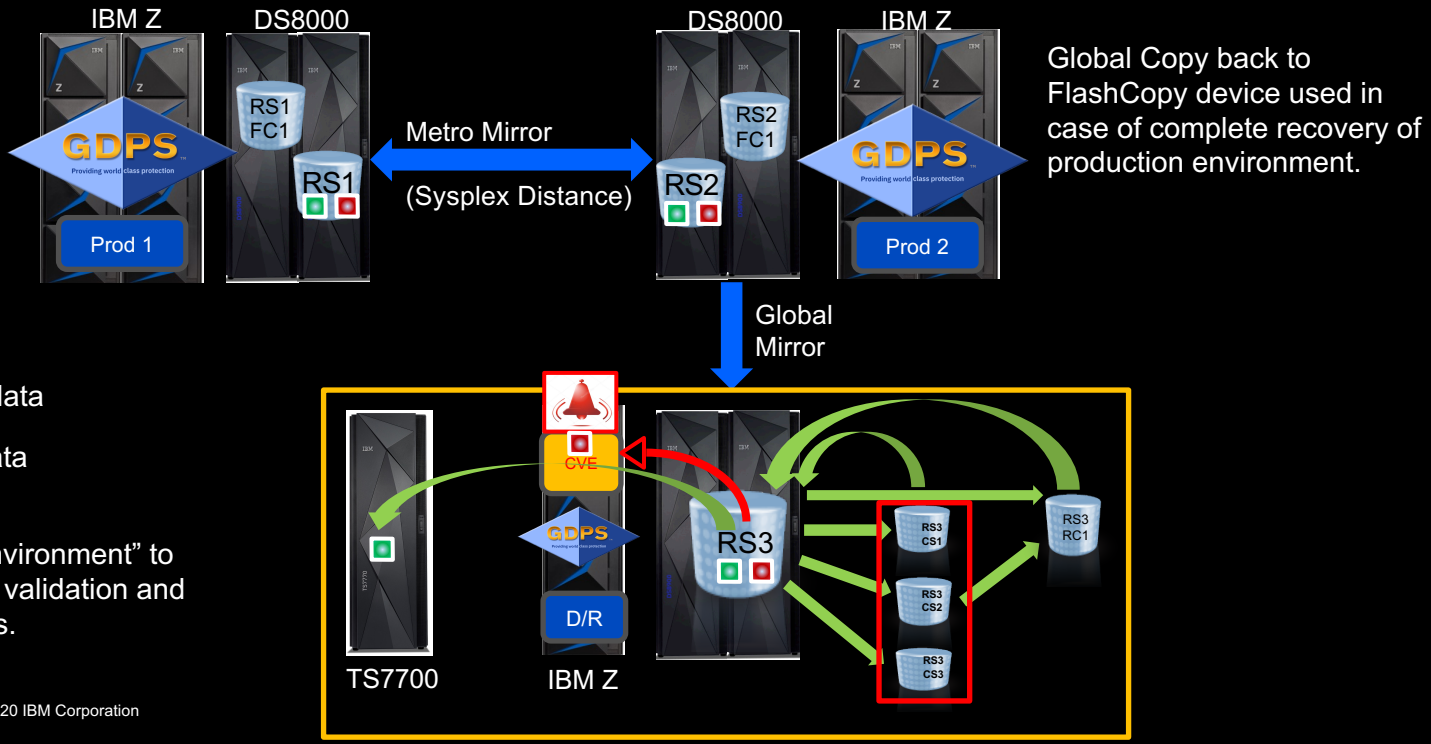
Physical isolation



- 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

Cyber Vault deployment example
Physical Airgap (and Isolation) with Global Mirror

Metro Mirror managed by GDPS Metro with FlashCopy for isolated DR testing.



Global Copy back to FlashCopy device used in case of complete recovery of production environment.

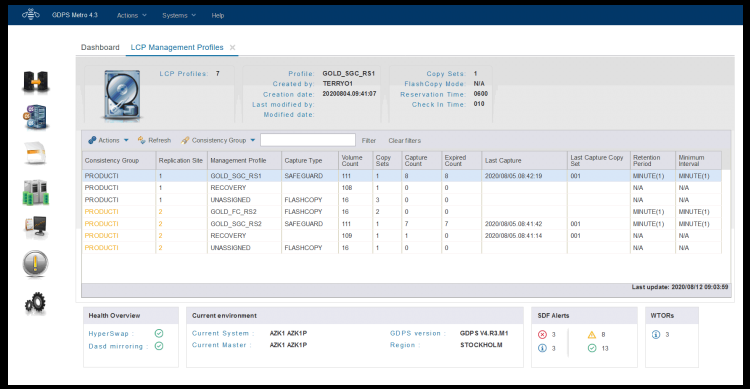
= “Good” copy of data

= “Bad” copy of data

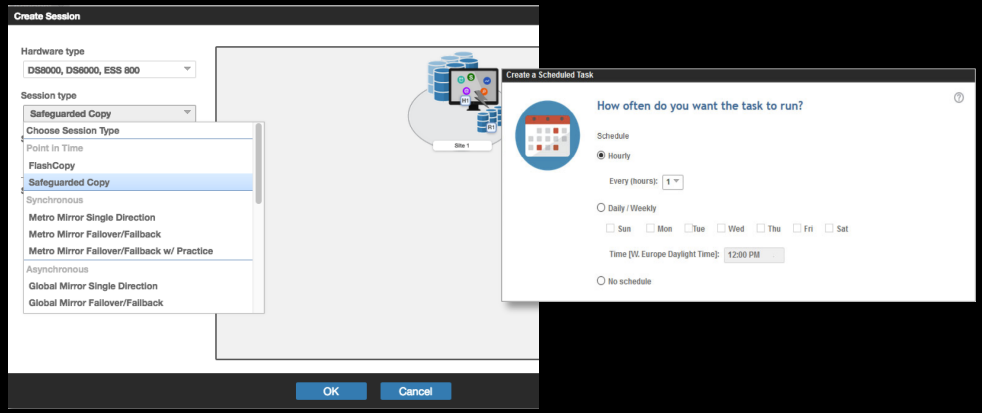
CVE = “Cyber Vault Environment” to enable ongoing validation and recovery actions.

GDPS/LCP or CSM is needed to 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

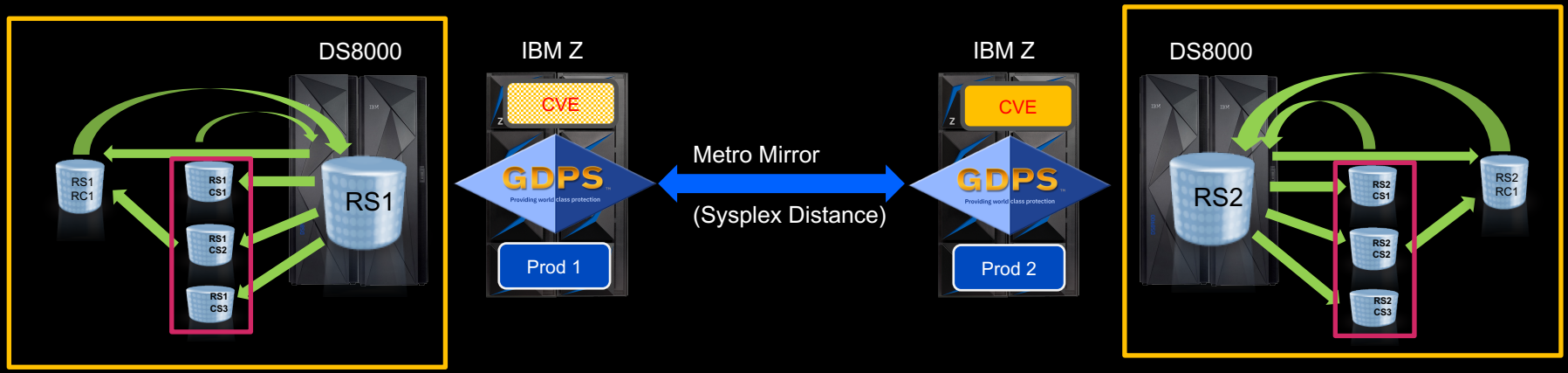
Customer has GDPS installed ?:
GDPS/LCP to manage the data corruption protection solution is preferred

Customer has CSM installed ?:
Integrate the data corruption protection solution (CSM price based on TB)

If customer has neither GDPS nor CSM: GDPS is the more comprehensive, CSM the cheaper solution.

SafeGuarded Copy deployment (examples)
Logical Airgap (virtual isolation) with Metro Mirror

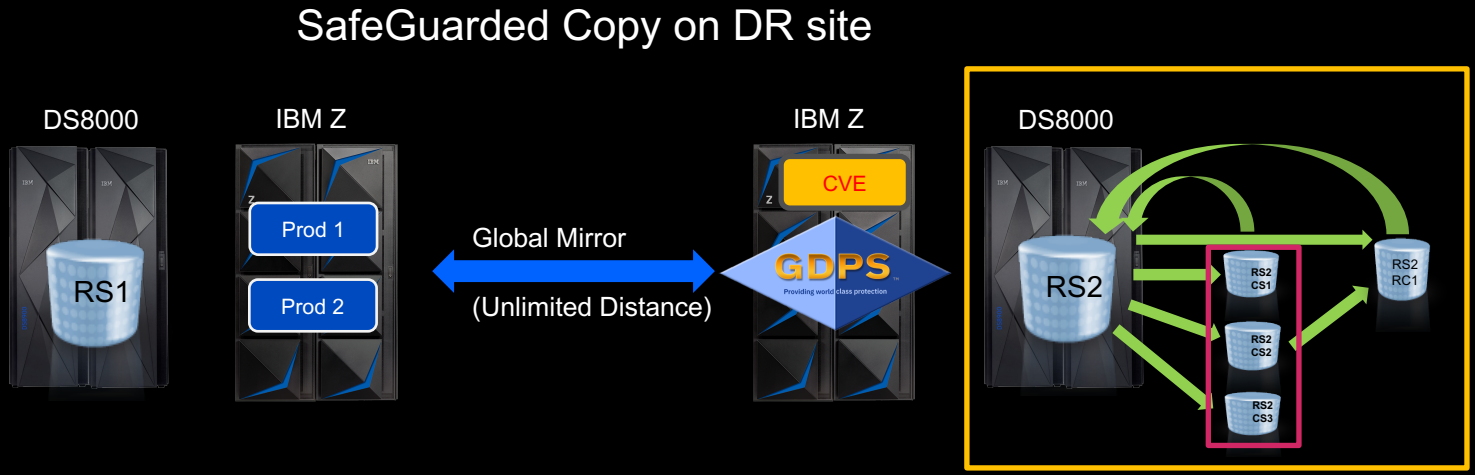
SafeGuarded Copy on both sites



Attention must be given to performance:
- To establish a consistent copy, the write IO's need to be stopped for 2-3 seconds once a SafeGuarded Copy is established (latest DS8K µCode required).
- There is no "general rule" if this acceptable or not. Every business needs to assess this.

Additional Remark:
- It is not required to run SafeGuarded Copy on both DASD controllers – but it provides additional security.
- The "Cyber Vault environment" needs to e active only on one server, with a backup environment on the other server.

SafeGuarded Copy deployment (examples)
Logical Airgap (virtual isolation) with Global Mirror

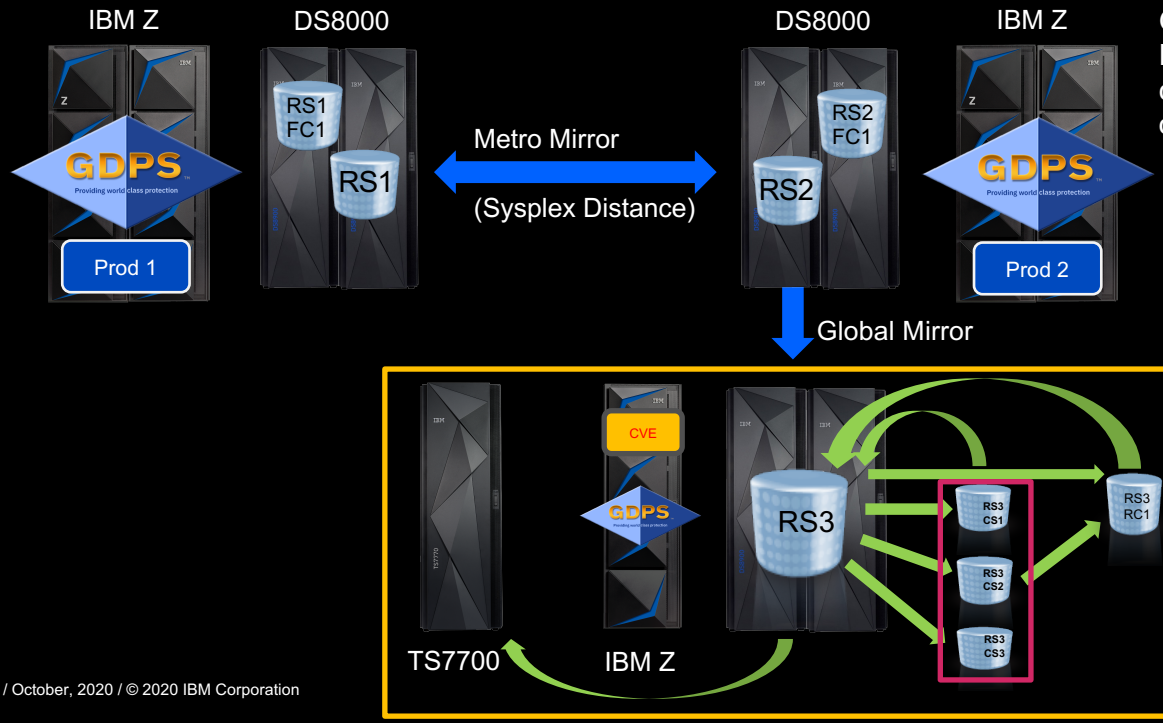


Description:
- Unlimited Distance.
- No performance impact on primary DASD due to asynchronous copy mechanism.
- Cyber Vault environment in the same box as GM secondaries.

Additional Remark:
- In this example the Cyber Vault environment is shown in the DR site. This is advantageous from a performance point of view (no stop of IO's to create consistent copies).
- It also makes use of the MIPS in the DR site.
- BUT: The DR site becomes a "HOT" site (not Cold or Warm any more).

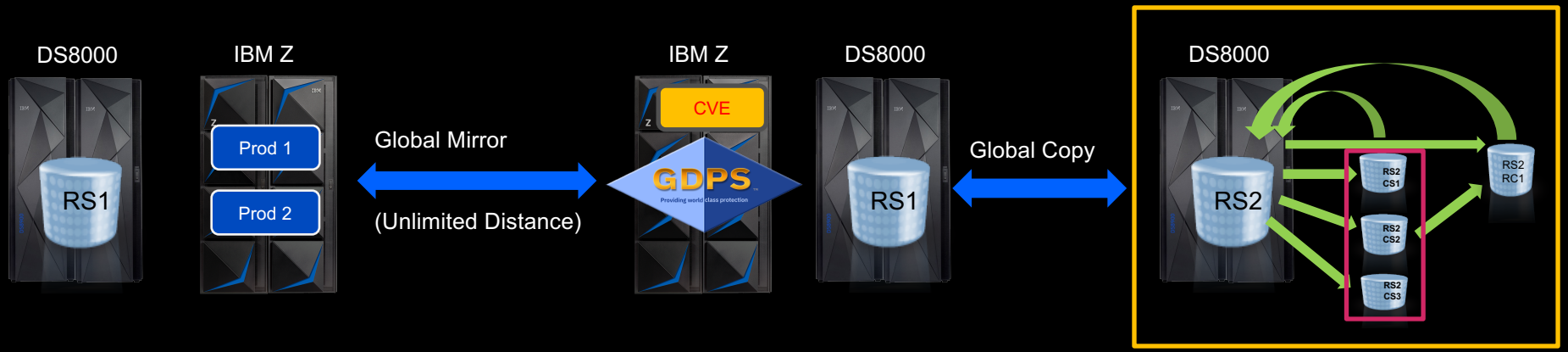
SafeGuarded Copy deployment (examples)
Physical Airgap (and isolation) with Global Mirror

Metro Mirror managed by GDPS Metro with FlashCopy for isolated DR testing



Global Copy back to FlashCopy device used in case of complete recovery of production environment.

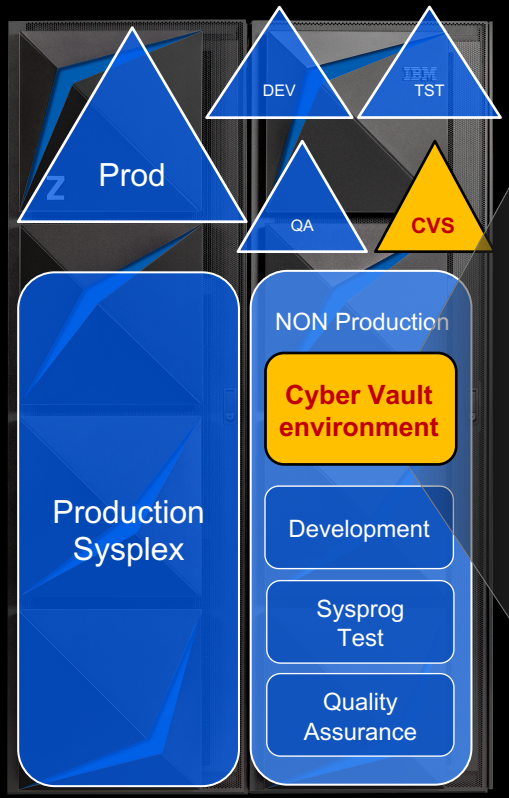
SafeGuarded Copy deployment (examples)
Physical Airgap with Global Mirror



Description:
- Unlimited Distance.
- No performance impact on primary due to asynchronous copy mechanism.
- Physical protection due to separated Cyber Vault DASD controller.

IBM Z Cyber Vault environment
Setup and usage

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

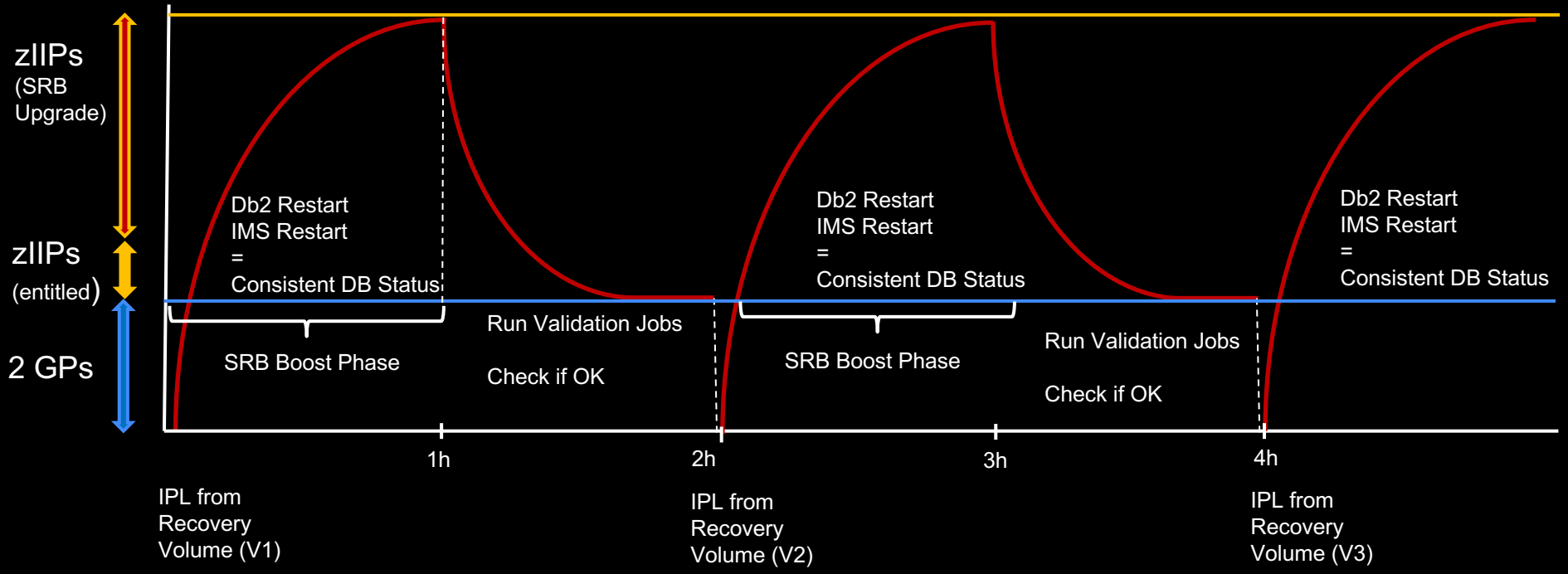


Cyber Vault environment

1. Prepare
   - Leverage Solution Edition pricing for SW, HW, Services, GDPS
   - Use System Recovery Boost to speed up IPL
   - Provide enough MIPS to run data structure and data content analysis
2. Establish Analysis Environment
   - Establish a new z/OS LPAR outside the production Sysplex
   - Provide a Coupling Facility LPAR for Sysplex structures
   - Create a recovery copy to be accessed only by the newly created LPARs with strictly limited user access
3. Usage patterns
   - Data Validation (IPL, data structure and data content check)
   - Forensic Analysis (Db2, IMS, VSAM, Catalog etc. tools)
   - Surgical recovery (DSS data restore)
   - Catastrophic Recovery (Global Copy to production device)
   - Offline Backup (DSS to tape)

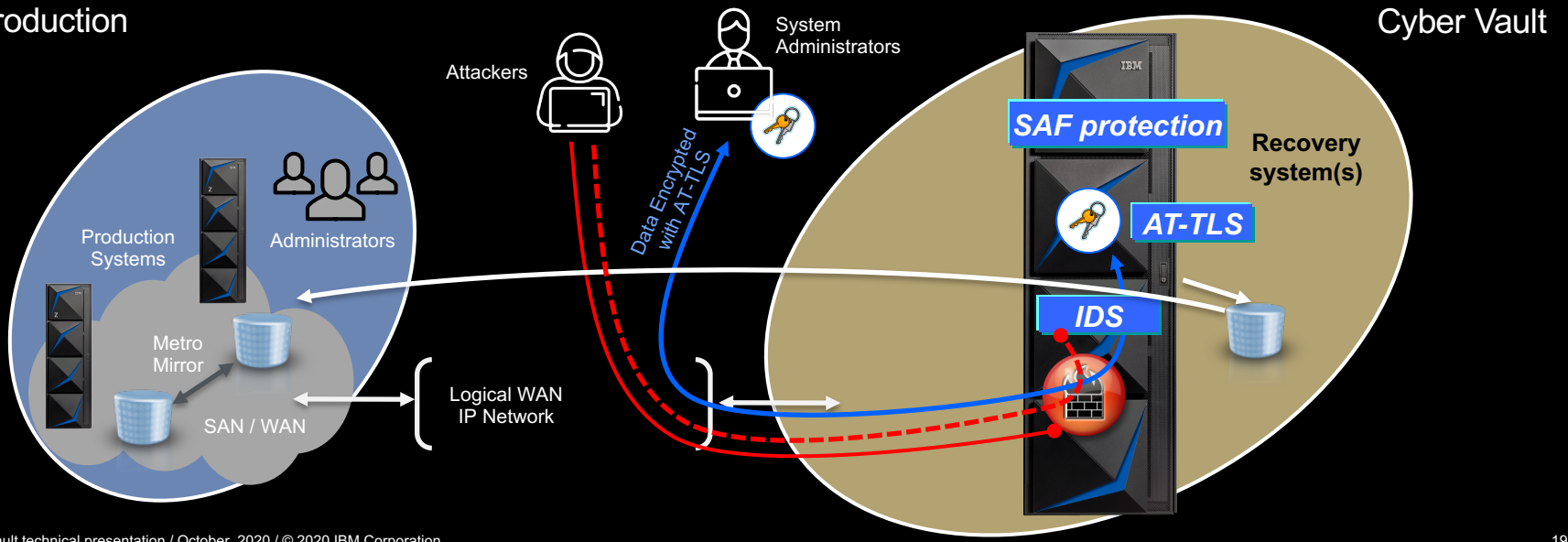
System Recovery Boost usage for IBM Z Cyber Vault

z15 Machine with SRB enabled for the Cyber Vault environment

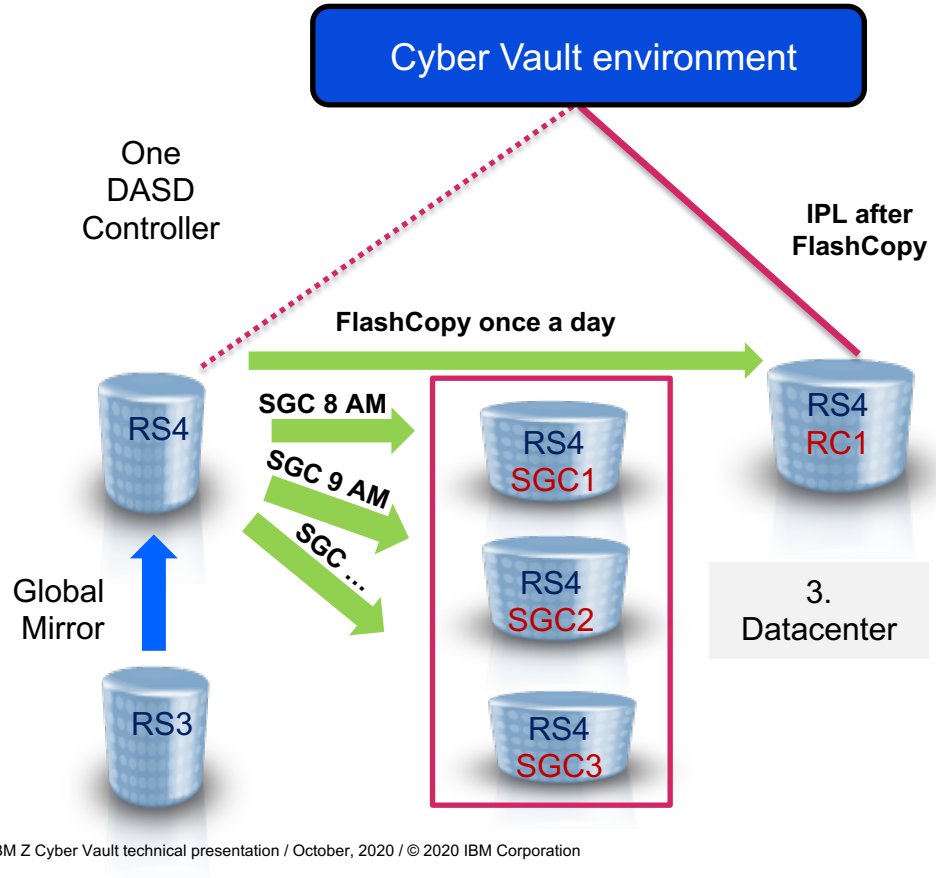


Network considerations – Security

- Cyber Vault environment LPAR(s) are protected using built-in z/OS Communications Server Security Features.
- IP filtering (e.g. Firewall) blocks out all IP traffic that this system doesn't explicitly permit within its defined IP Filter Policy. Intrusion Detection Services (IDS) protect against Attacks of various types on the system's legitimate (open) services. Application Transparent Transport Layer Security (AT-TLS) provides SSL/TLS encryption services at the TCP transport layer to protect and secure "in-flight" sensitive application data. AT-TLS is transparent to the application.
- SAF (e.g. RACF, Top Secret, ACF2) authenticate users and prevents unauthorized access to system resources and datasets.



IBM Z Cyber Vault – Data validation concept



At least once a day …

Phase 1: IPL with production image

At least one LPAR per Sysplex is necessary

- System Recovery Boost Upgrade record used for one IPL per day
- Check Sysplex infrastructure

Phase 2: Data Structure Validation

- Db2 restart (all data sharing group members), Utilities, Log analysis
- IMS restart, Utilities
- Catalog tools (Tivoli, IDCAMS, ISV products)
- VSAM Indexcheck, Datacheck
- SMShsm, SMSrmm tools
- RACF (IRRUT200), zSecure-Audit
- ISV software (CA1, CA7, ...)

Phase 3: Data Content Validation

- Customer Application Program

If no issue found: Create tape copy

Data validation activities (1)

Catalog / VTOC / VVDS

- IDCAMS Diagnose (BCS and VVDS)
- IDCAMS Examine (VSAM KSDS)
- ICKDSF, DITTO, IEHLIST
- VSAM Indexcheck / Datacheck
- Tivoli Advanced Catalog Management for z/OS

DF/SMS

- Audit HSM, IBM Advanced Audit for DFSMShsm
- OAM (CATDB2CP Rexx)
- RMM - Use EDGUTIL VERIFY(ALL) and EDGUTIL VERIFY(SMSTAPE)

Sysplex Infrastructure

- IPL Production System in New LPAR (incl. CF Structures)
- SRB during IPL (SRB upgrade record)
- At least 2 additional CPs
- One CF LPAR

z/OS

- RACF (IRRUT200)
- zSecure-Audit
- z/OS Command Output
- Syslog and EREP review
- z/OS Health Check

Db2

- Db2 Log Analysis
- Db2 Utility Suite
- Execute IBM IVPs to test Db2 functionality
- Execute application IVPs to test application functionality and data integrity
- Restart all Db2 stand-alone subsystems or all members which are part of the data sharing group(s)
- Review all start-up messages for any critical messages
- Check local and remote connectivity
- Use the Db2 Utilities Suite to check system and application object integrity as needed

z/OS Connect

- Initialize server
- Review system logs for critical startup messages
- Verify connection status

ISVs

- CA1, CA7, ...
- Adabas .....
- Others

Text in YELLOW marks the additional products from software or hardware which IBM recommends using.

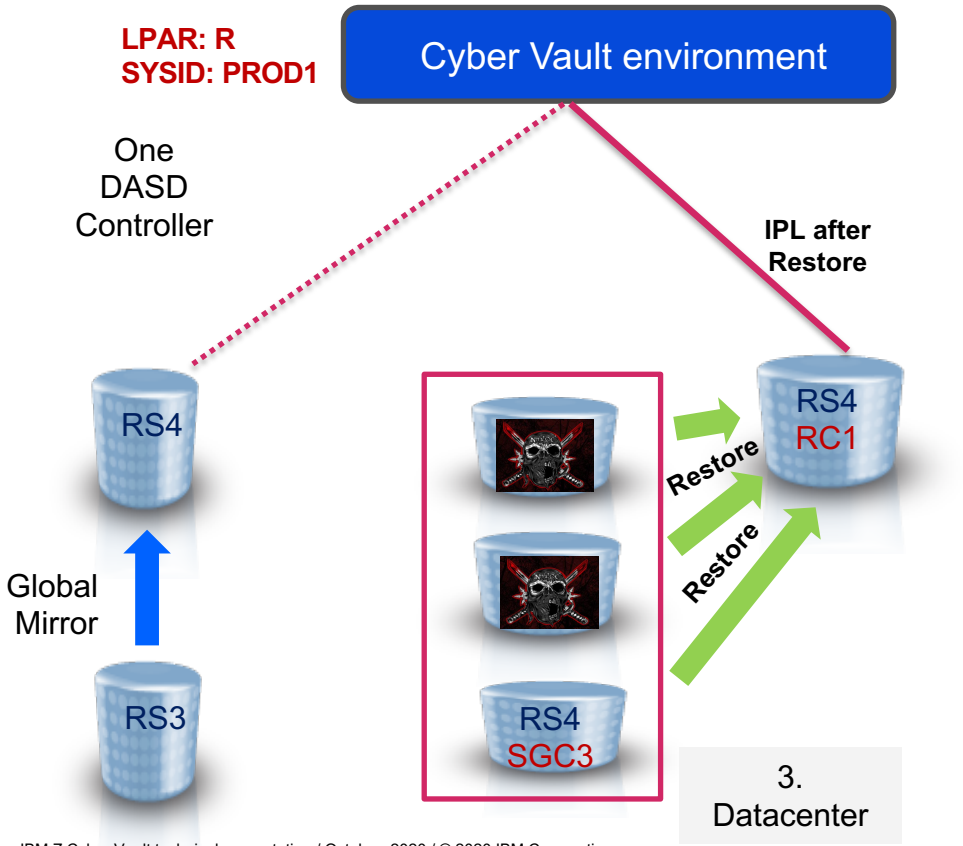
Data validation activities (2)

IBM MQ	IMS	WebSphere Application Server for z/OS
• Initialize queue manager and channel initiators • Review system logs for critical startup messages • Verify connection status	• Restart all IMS members which are part of the data sharing group • IMS High Performance Pointer Checker to check data structures • IMS Recovery Expert for enhanced database checks	• Initialize application servers and any administrative servers • Review system logs for critical startup messages • Verify connection status

CICS	
• Initialize CICSPLEX, CICS regions, data sharing servers • View CICSPLEX active workloads/regions in WUI/EXPLORER • Review startup messages for subset critical ROR/AORs • View MRO/FILE/Network and DBCONN resources for ENABLED/ACTIVE	• Run sample transactions to verify CICS readiness • ICFRU for forward recovery • Run validation/verification application trans/programs • ICFRU for forward recovery

Text in YELLOW marks the additional products from software or hardware which IBM recommends using.

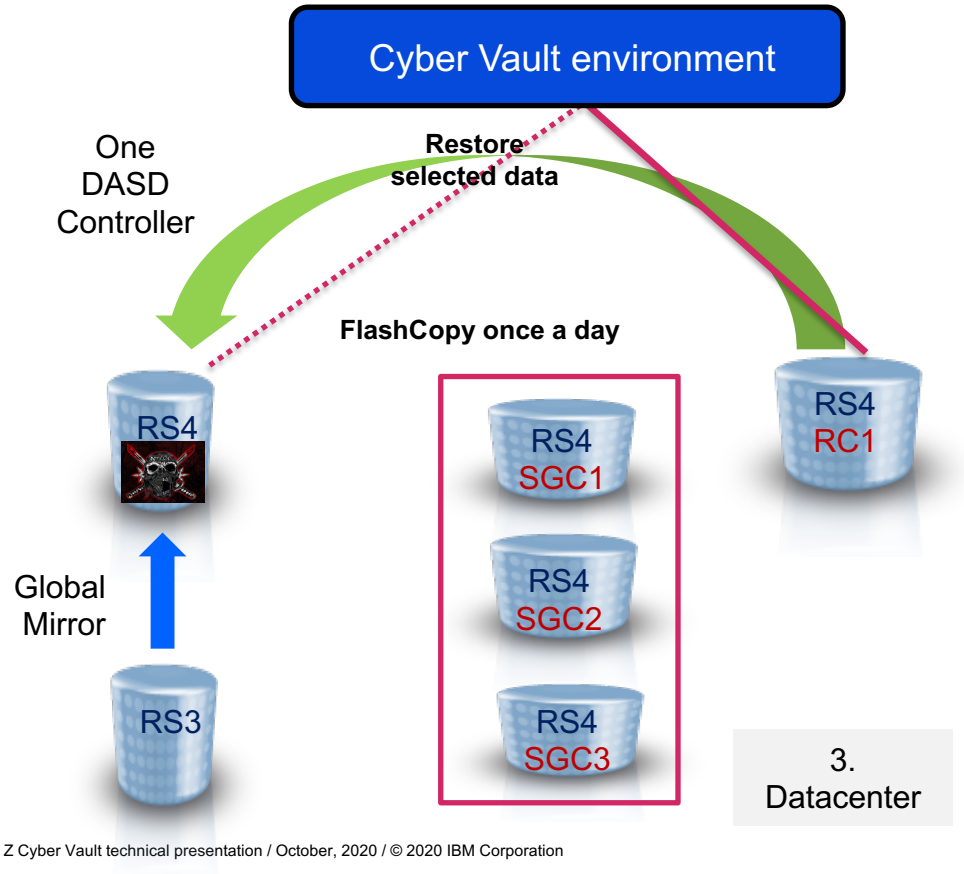
Forensic analysis



Determine start of data corruption …

- **IPL** 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.
- **Identify** steps forward
  - Create strategy for recovery

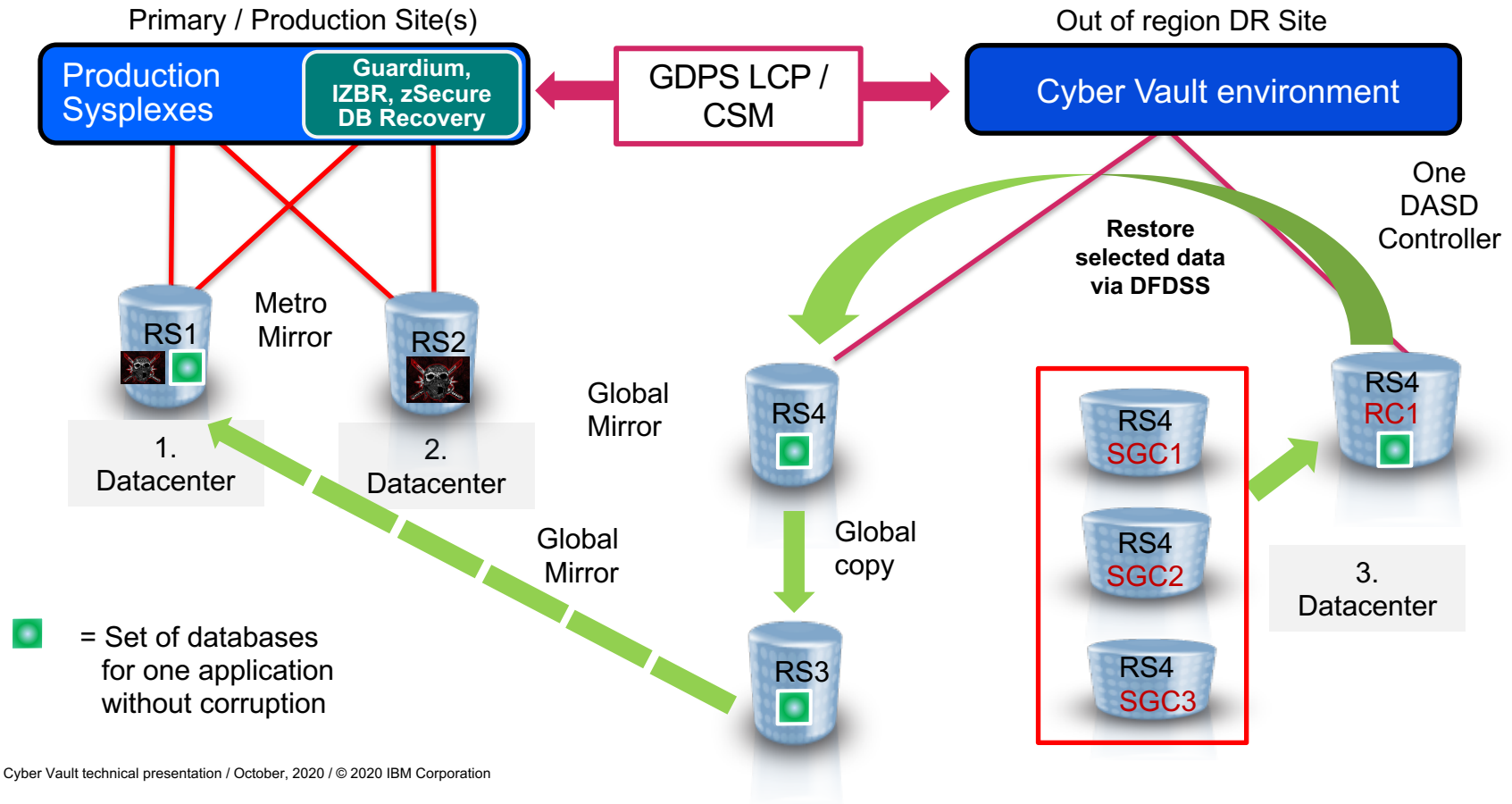
Surgical recovery (3 site solution)



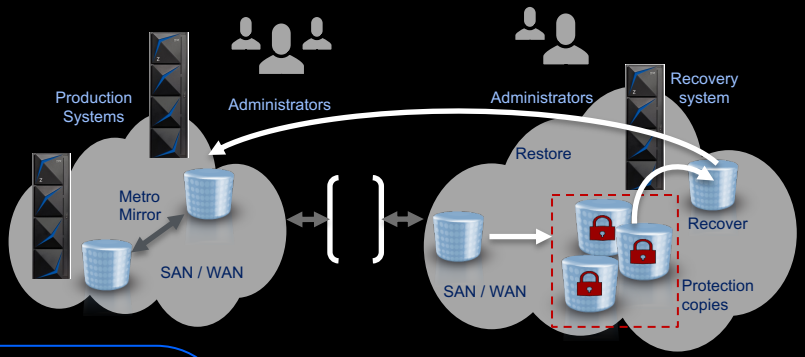
Determine data to restore …

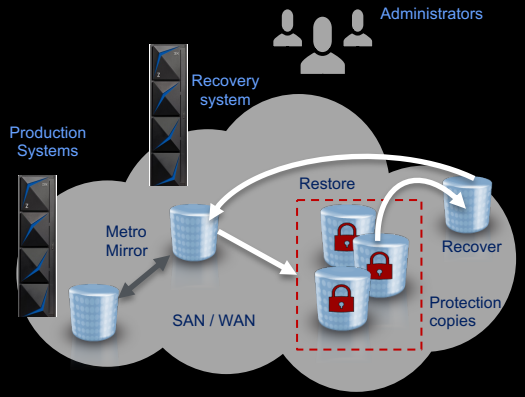
- **Identify** corrupted data
  - Create a list of data to restore
- **Continue** running production degraded on primary site (not all applications active)
- **Restore** partially
  - Run database utilities and DSS copy services to restore individual files and databases to the production environment
- **Update** Databases and Files in production
  - The FlashCopies / SafeGuarded Copies were taken without “knowledge” of the database system.
  - In order to use the selected files special procedures may apply to make these copies known to Db2, IMS, etc.

Surgical recovery (3 site solution)



Catastrophic recovery concept





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

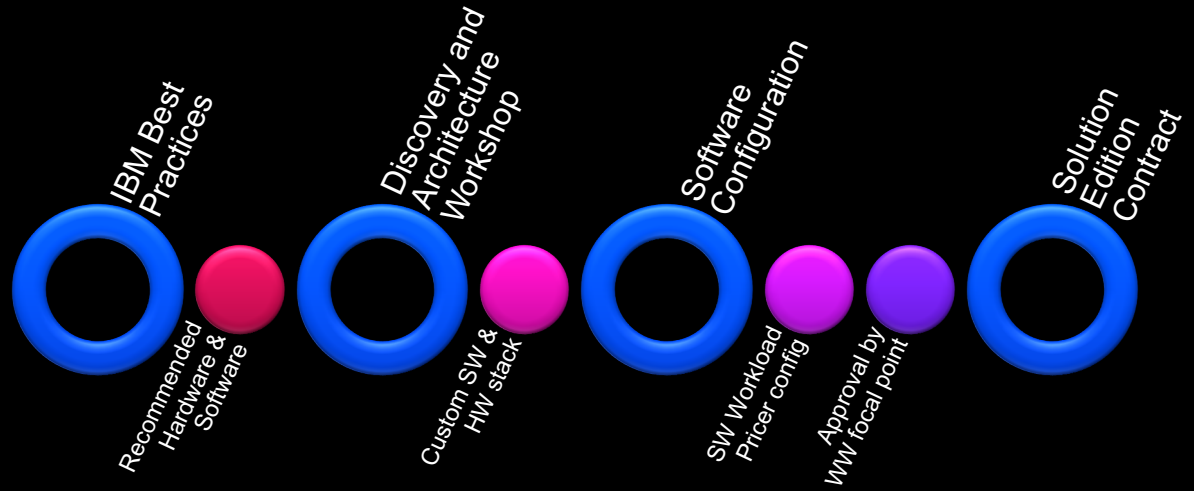
But it is up to the client if, in this case they start production from the DR site, Metro Mirror Site 1 or Metro Mirror Site 2, to name some options

IBM Z Cyber Vault, SW and HW configuration process

The IBM Z Cyber Vault Solution provides air gapped data corruption protection and tools to speed recovery. This isolated environment requires hardware and software that will be configured and priced as a “Solution Edition” in order to provide the best value to customers.

Starting from a recommended Software configuration based on IBM’s best practices for cyber resiliency, our services team will work with customers to identify their specific needs and requirements. This activity is called “Discovery and Architecture Workshop”, and as a result a final software list will be produced.

This list will be used to configure the Software stack and start the process to obtain the solution edition customer price and contract.



Deployment services for the IBM Z Cyber Vault

Z Forward Eligible Services

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
Free of charge
	• 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

Co-requisite services

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

IBM Z and LinuxONE
Quick Reference Guide

Cyber Vault for IBM Z Discovery and Architecture Workshop

Overview

If you need to protect your business from cyber threats, this IBM Garage offering will help you design a Cyber Vault solution that fits your business needs.

IBM Garage

Target Audience

- IBM Z clients who are interested in protecting their systems and business data from cyber threats

Why Use This Service?

- Are you concerned about data corruption caused by cyber attacks?
- Are you concerned about the impact of a ransomware attack?
- Are you confident that you could recover from logical corruption of your data?
- Are your policies and practices aligned with industry best practices?

Benefits

- A Cyber Vault solution protects your data with an air gapped copy.
- This workshop will ensure that you have the architecture and practices in place to be able to recover your systems and data.

Service Provided

- 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 end state.

Deliverables

- Analysis of the existing environment.
- Analysis of data change rates to determine configuration requirements.
- Documentation of the solution as designed.
- Documentation of the roadmap and high-level plan for implementing the solution.

Contacts

- Contact us at SysGarage@us.ibm.com or your local IBM Garage team
- Karen Smolar ksmolar@us.ibm.com
- Tom Bish tbish@us.ibm.com

IBM

Thank you

Matthias Bangert
Executive IT-Specialist, Worldwide Technical Sales, IBM Z
matthias.bangert@de.ibm.com