

Advanced Technology Group



Accelerate with ATG: Protect your business with IBM Z Cyber Vault

David Petersen

IBM Distinguished Engineer

petersen@us.ibm.com

Accelerate with ATG Technical Webinar Series

Advanced Technology Group experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to accelerate-join@hursley.ibm.com.

2023 Upcoming Webinars – click on the link to register for the live event:

November 14 – [IBM TS7700 R5.4 Update](#)

December 5 – [What is IBM Storage Defender?](#)

Important Links to bookmark:



ATG Accelerate Support Site: <https://www.ibm.com/support/pages/node/1125513>

ATG MediaCenter Channel: <https://ibm.biz/BdfEgQ>



ATG-Storage Offerings

CLIENT WORKSHOPS

- **IBM DS8900F Advanced Functions: December 6-7, 2023 (Virtual)**
- IBM Storage Point of View on Cyber Resiliency
- IBM FlashSystem and Storage Virtualize
- IBM Storage Scale System and Storage Scale
- IBM FlashSystem 9500 Deep Dive & Advanced Functions
- IBM Storage Fusion

Please reach out to your IBM Rep or Business Partner for future dates and to be nominated.

TEST DRIVE / DEMO'S

- North America ATG Storage - IBM Storage Scale and Storage Scale System GUI
- North America ATG Storage - IBM Storage Virtualize Test Drive
- North America ATG Storage - IBM DS8900F Storage Management Test Drive
- North America ATG Storage - Managing Copy Services on the DS8000 Using IBM Copy Services Manager Test Drive
- North America ATG Storage - IBM DS8900F Safeguarded Copy (SGC) Test Drive
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (Appliance based)
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (VMware based)
- North America ATG Storage - IBM Storage Protect Live Test Drive
- North America ATG Storage - IBM Storage Ceph Test Drive - (VMware based)

Please reach out to your IBM Rep or Business Partner for more information.

Accelerate with ATG Technical Webinar Series - Survey

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

You can access this 6-question survey via [Menti.com](https://www.menti.com) with code 2243 3599 or

Direct link <https://www.menti.com/albneqj15g57>

Or

QR Code



Advanced Technology Group



Accelerate with ATG: Protect your business with IBM Z Cyber Vault

David Petersen

IBM Distinguished Engineer

petersen@us.ibm.com

Meet the Speakers



Mr. Petersen is an IBM Distinguished Engineer in the IBM Z platform. He has over 20 years of experience with IBM and responsible for the overall IBM Z Platform continuous availability, disaster recovery, and cyber resiliency strategy. David is the chief technologist / program manager of the GDPS continuous availability / disaster recovery / cyber resiliency solution, is responsible for the overall strategy, and leads the worldwide development organization. He is recognized throughout the IT industry as a resiliency expert.

GDPS Level-set

IBM GDPS is installed in several of the largest enterprises in the world.



83% of the top **40** banks around-the-world use GDPS¹

Over **25** years of experience

+98% of the new GDPS deployments are with DS8K

Over **1100** licenses in **51** countries and dozens of references

2 MLOC in GDPS

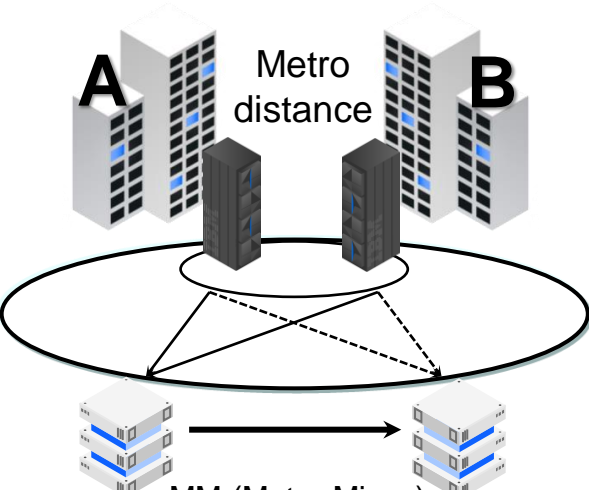
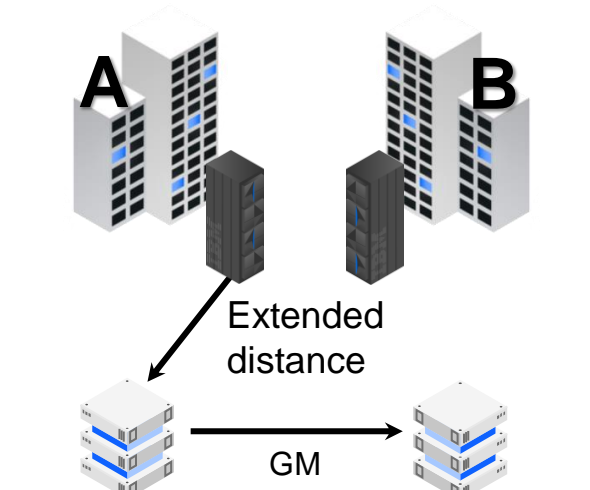
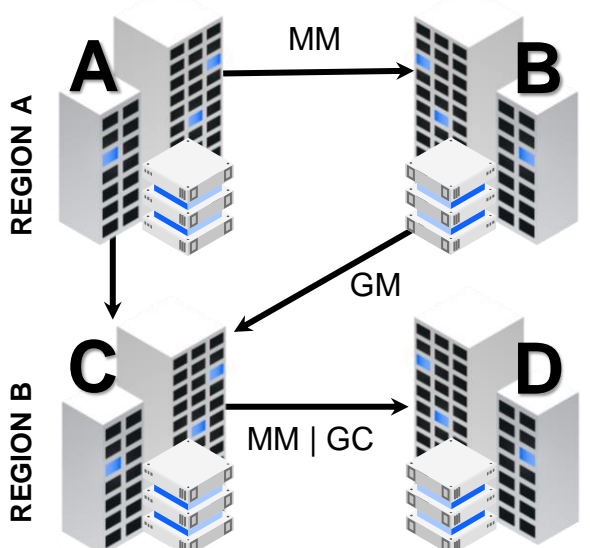
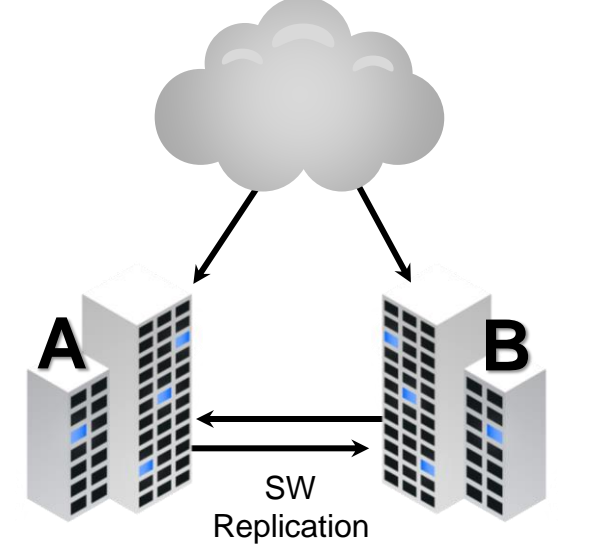
+50 people work on GDPS



¹Based on offering engagement data and the [The Top 50 Banks in the World](#) listing by relbanks.com, February 2016

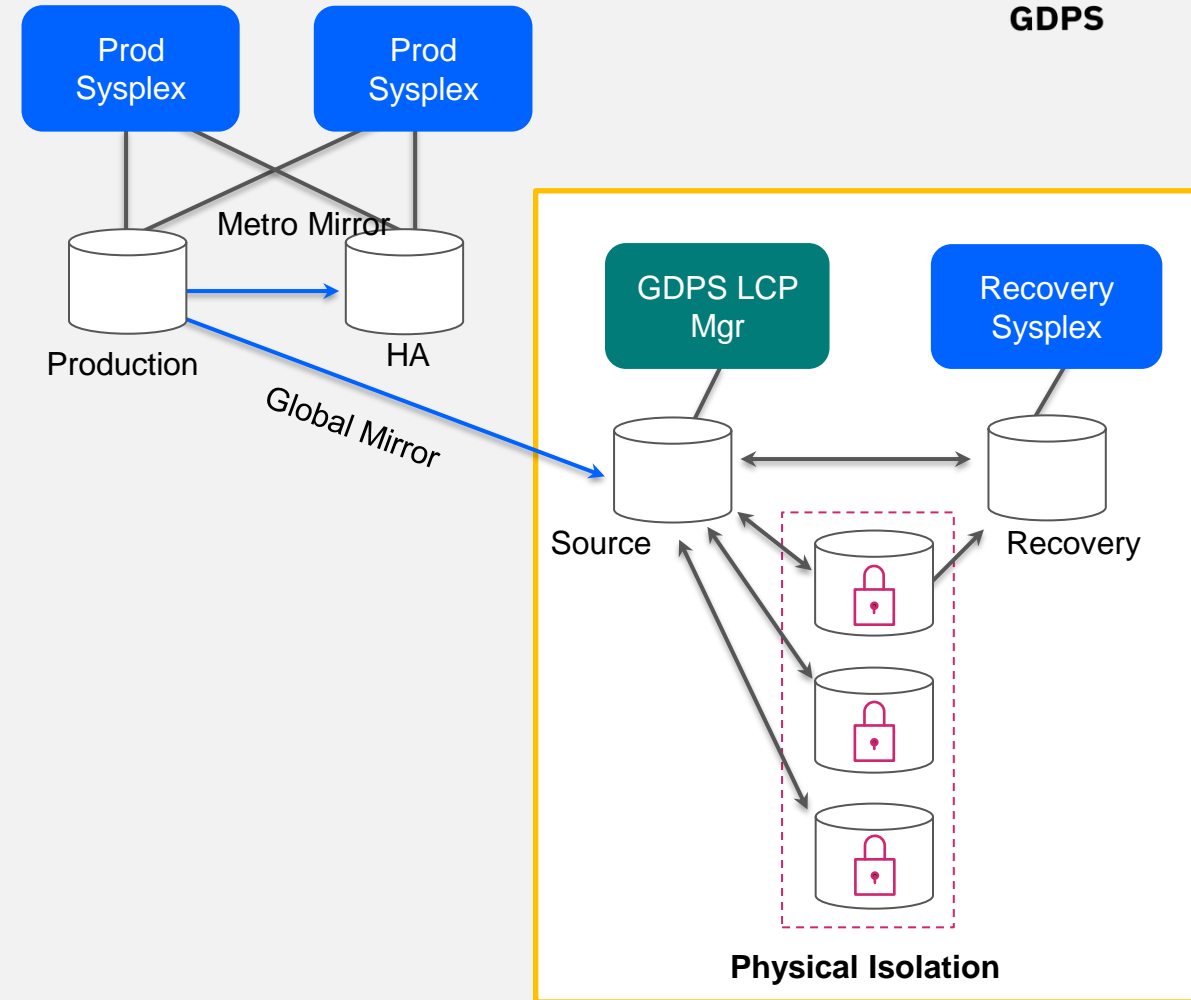
Balanced solutions designed to address different requirements



GDPS Metro	GDPS Global	GDPS Metro Global	GDPS Continuous Availability
<p>Near-continuous availability and recovery at metro distances</p>	<p>Disaster recovery at extended distance</p>	<p>Near-continuous availability regionally & recovery for 3-4 sites</p>	<p>Near-continuous availability, recovery & workload balancing</p>
<p>Systems remain active Multisite workloads can withstand site and storage failures</p>	<p>Rapid systems DR with “seconds” of data loss</p>	<p>Metro near-continuous availability and out of region disaster recover</p>	<p>Continuous availability at unlimited distances</p>
 <p>RPO 0 & RTO <60 min</p> <p>© Copyright IBM Corporation 2023</p>	 <p>RPO 3-5 sec & RTO <60 min</p>	 <p>RPO 3-5 sec & RTO <60 min</p>	 <p>RPO 3-5 sec & RTO <60 sec</p>

Logical Corruption Protection (LCP) Manager for cyber resiliency

- Automates the policy-based capture and vaulting of a point-in-time (PIT) copy (either Safeguarded Copy or FlashCopy) for each GDPS-managed sysplex
- Automates the movement of a chosen PIT copy into the recovery sysplex for analysis, testing, or full recovery
- Initiates the IPL of a chosen PIT copy in the recovery sysplex
- Automates the movement of a chosen PIT copy back to the production sysplex, when ready
- Can be integrated to provide this robust automation capability within a broader zCyberVault solution



LCP Manager supports both physical and virtual vault isolation.

IBM Z Cyber Vault Overview

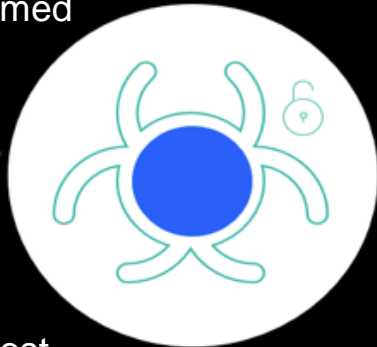
The question is not IF you will be attacked but WHEN

\$265B

Predicted global ransomware demands WW forecast ⁶

+ 50+

Unique malware distributed in various Covid-19 themed campaigns ⁴



\$1.54M

Average ransomware cost in 2023, almost double 2022 and 10x 2020²

\$4 Billion

Estimated global cost of WannaCry attack ³

49%

Increase in publicized attacks in 1H23 over same period in 2022¹

\$1.3 Billion

GDPR fine for one data breach ⁵

solarwinds

Orion: More US government agencies hacked

BBC NEWS

Meta

Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules

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

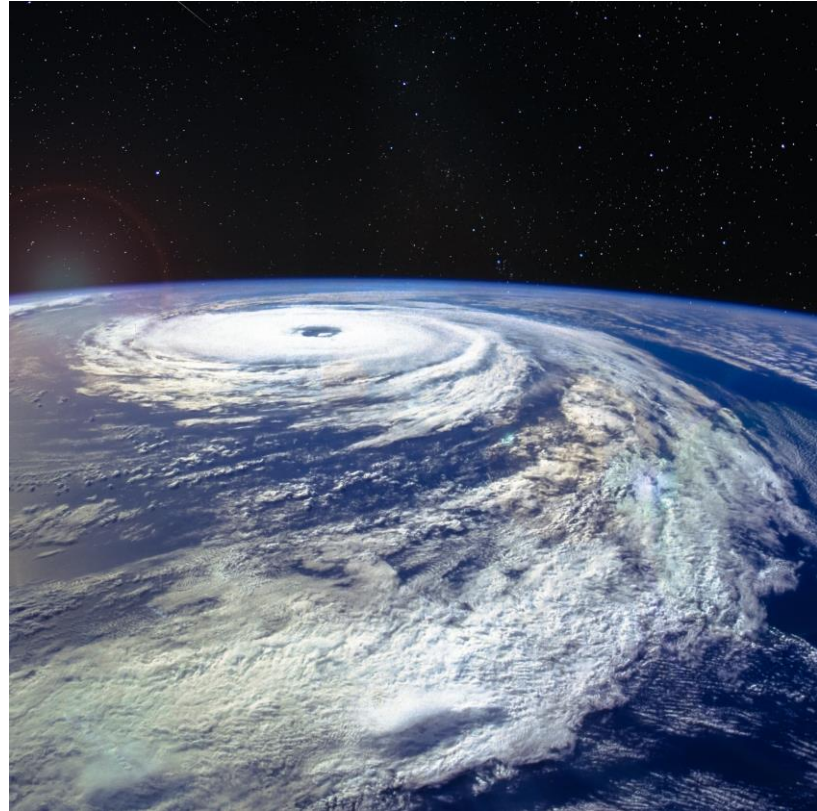
Real-life BOFH ordered to pay \$3.1m restitution

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.

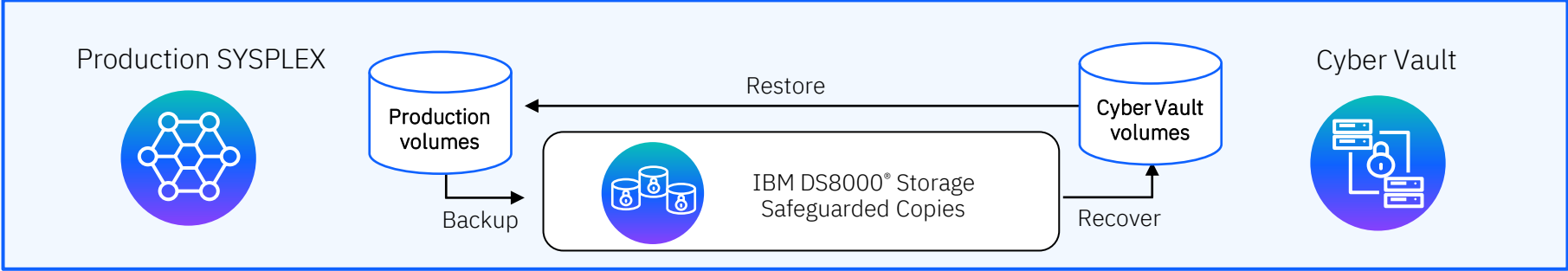
1. BlackFog Most Impactful Ransomware Attacks of 2023
2. The Sophos State of Ransomware 2023 report
3. ReInsurance news Sept 24, 2017
4. XF IRIS internal data analysis IBM 2020
5. dataprivacymanager.net/blog 19 Sept, 2023
6. Cybercrime magazine July 7, 2023

Traditional resiliency solutions will not protect you from cyber attack



	Traditional resiliency	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



Data Validation
Detect data corruption early or validate that the copy is clear



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 Cyber Vault capabilities are supported by

IBM GDPS® LCP Manager

IBM z/OS® Utilities

IBM Security zSecure™

IBM Z® Catalog management tools

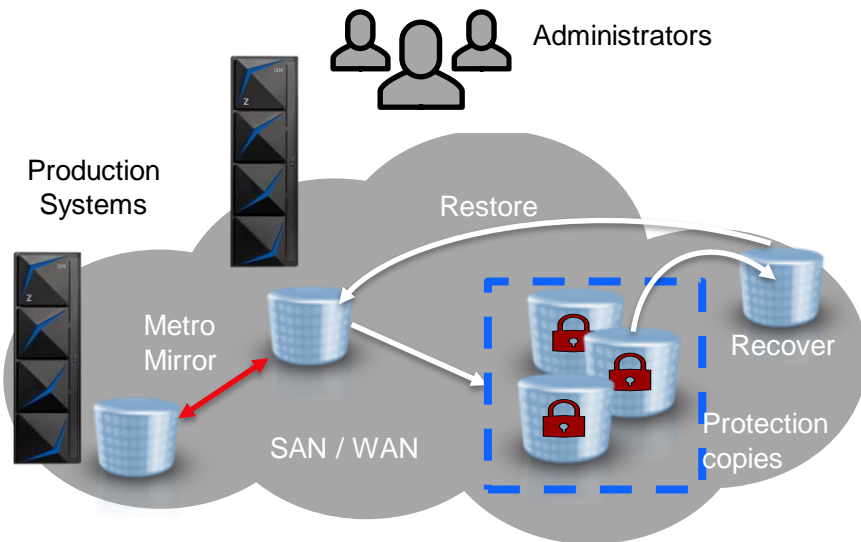
IBM Z Batch Resiliency (IZBR)

IBM DFSMSHsm™ tools

Db2® and IMS™ Tools

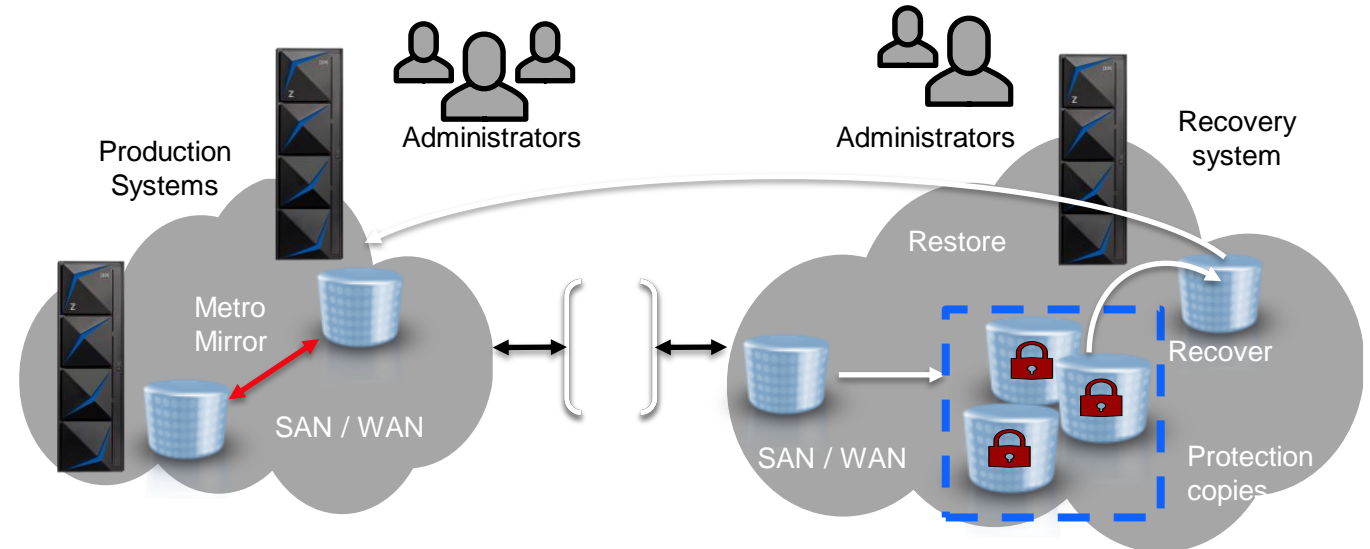
Air gap: Virtual and physical isolation of protection copies

Virtual isolation



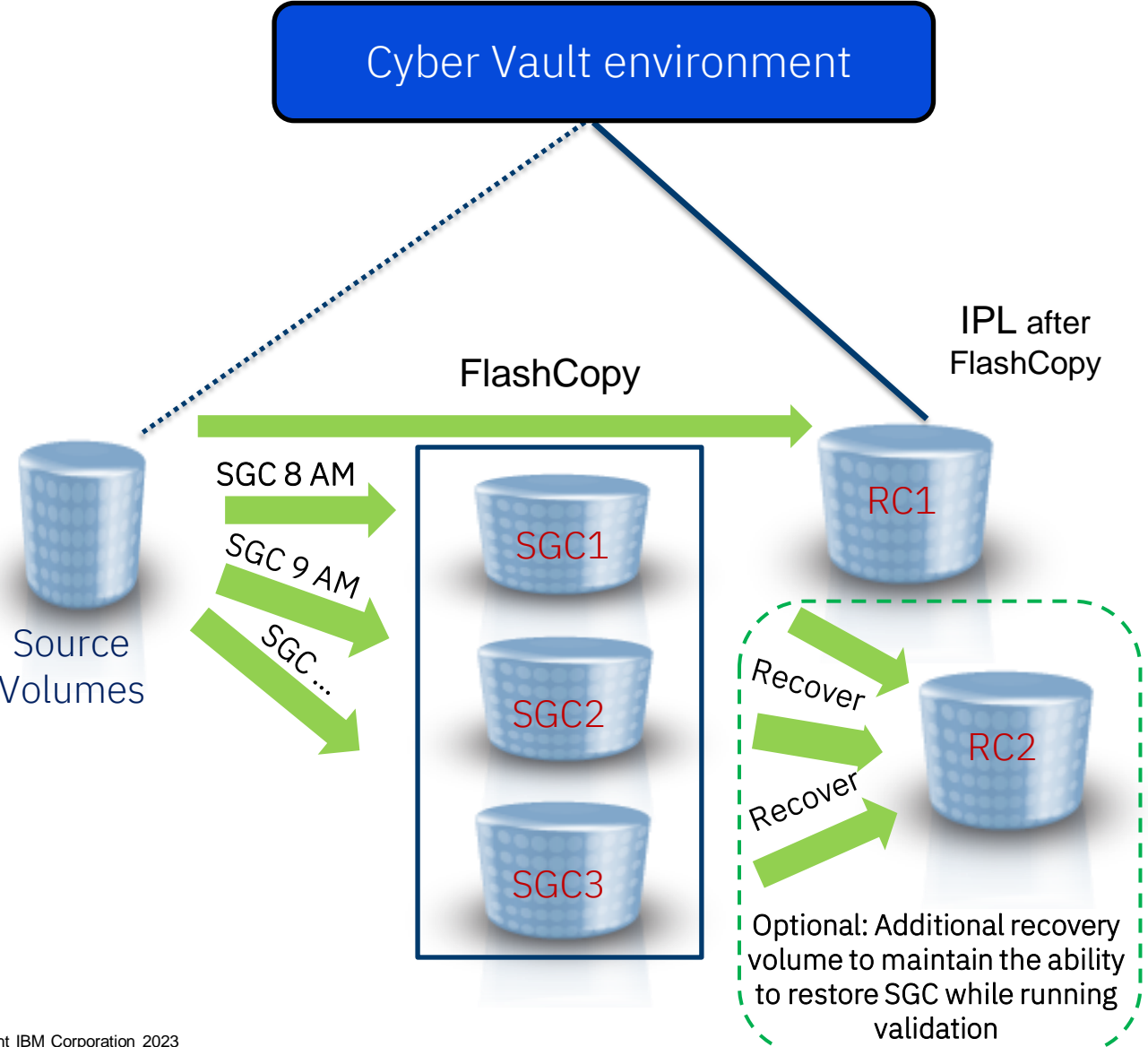
- The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- The storage systems are typically in the same SAN or IP network as the production environment

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

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
- DFSMSshm, DFSMSrmm tools
- RACF (IRRUT200), zSecure-Audit
- ISV software (CA1, CA7, ...)

Type 3: Data Content Validation

- Customer application program

LCP Topologies - update

Supported

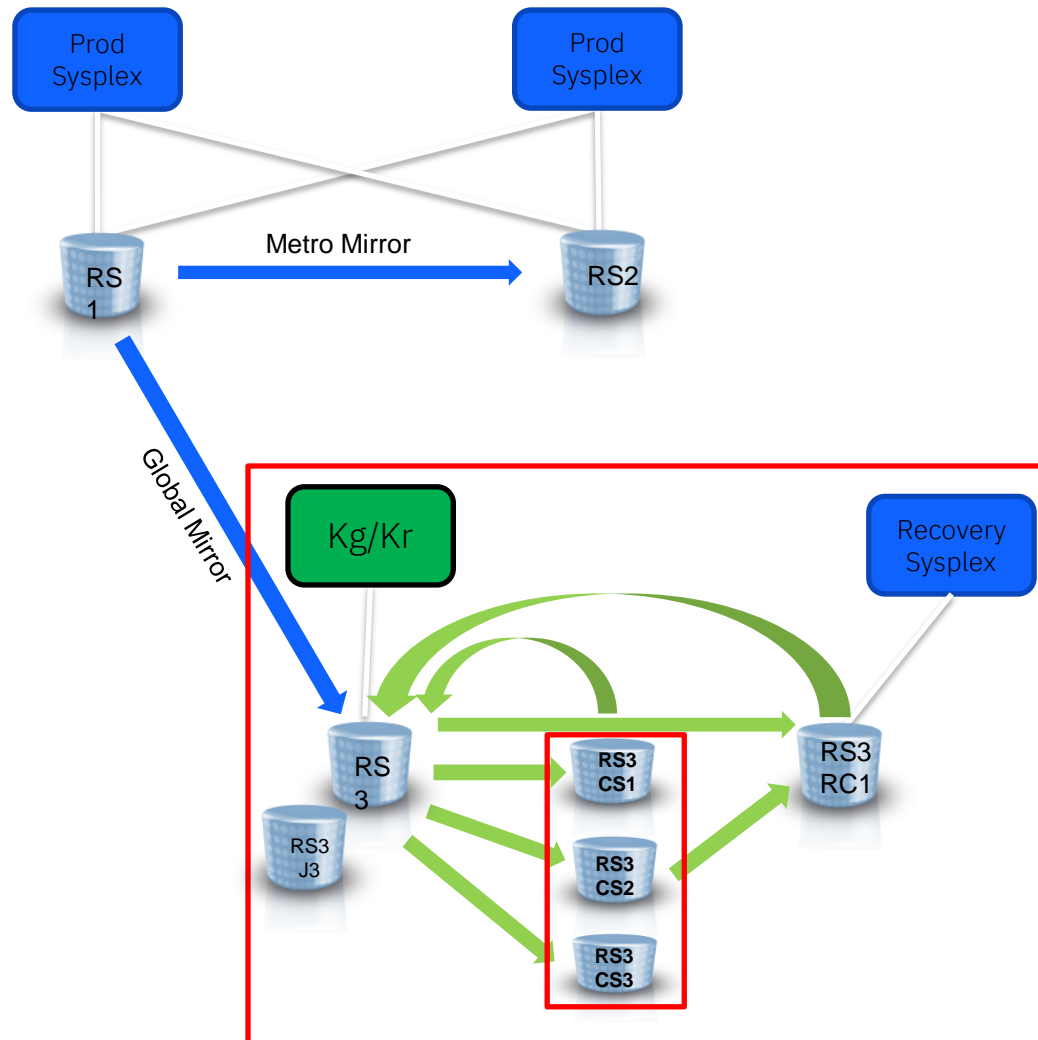
MM2SITE	Virtual
MM2SITE	Physical
MM3SITE	Virtual
MM3SITE	Physical
GM2SITE	Virtual
GM2SITE	Physical
MGM3SITE	Virtual-M
MGM3SITE	Virtual-G
MGM3SITE	Physical
MGM4SITE	Physical
MGM4SITE	Virtual*
MZGM3SITE	Virtual*
MZGM4SITE	Virtual*

Not Currently Supported

MGMnSITE	Combo	Virtual plus Physical isolation
MMnSITE	Combo	Virtual plus Physical isolation
GMnSITE	Combo	Virtual plus Physical isolation
MGM4SITE	Virtual	On the Global Mirror replication leg
MGM4SITE	Virtual	On the Global Copy replication leg
MZGM4SITE	Virtual	On the recovery region Metro Mirror replication leg
MZGMnSITE	Physical	Not supported

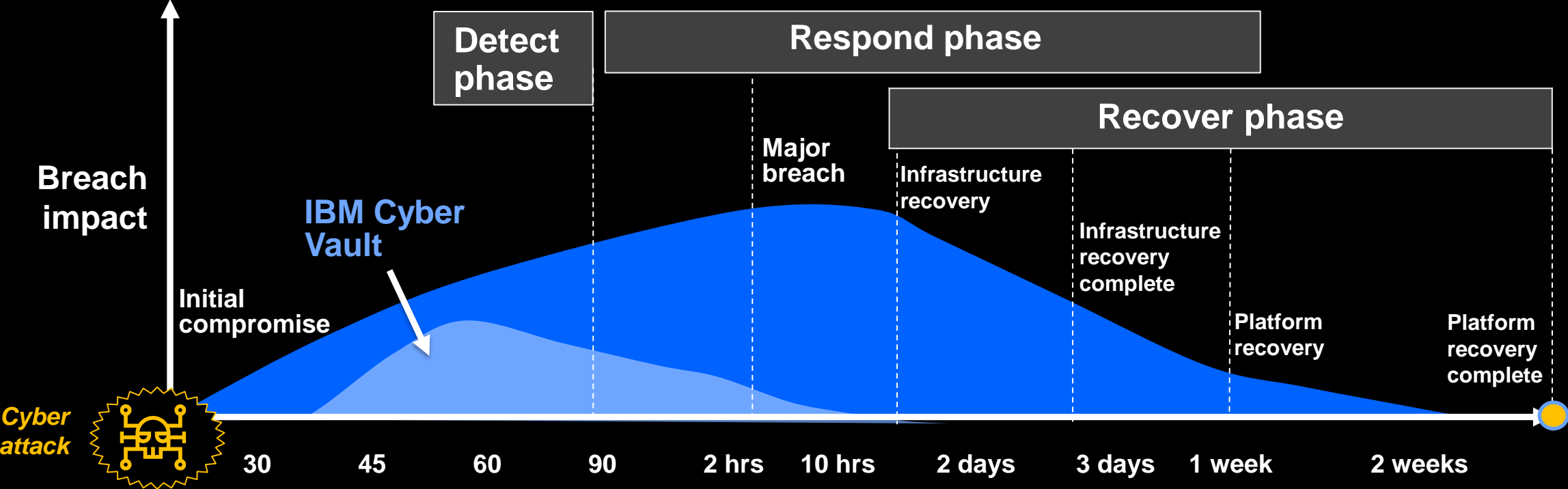
* Production region Metro Mirror leg only

GDPS Metro (MM2SITE) – Physical airgap



Logical Corruption Protection Environment physically isolated in Global Mirror secondary site – can be from RS1 or RS2 but needs to be MT capable

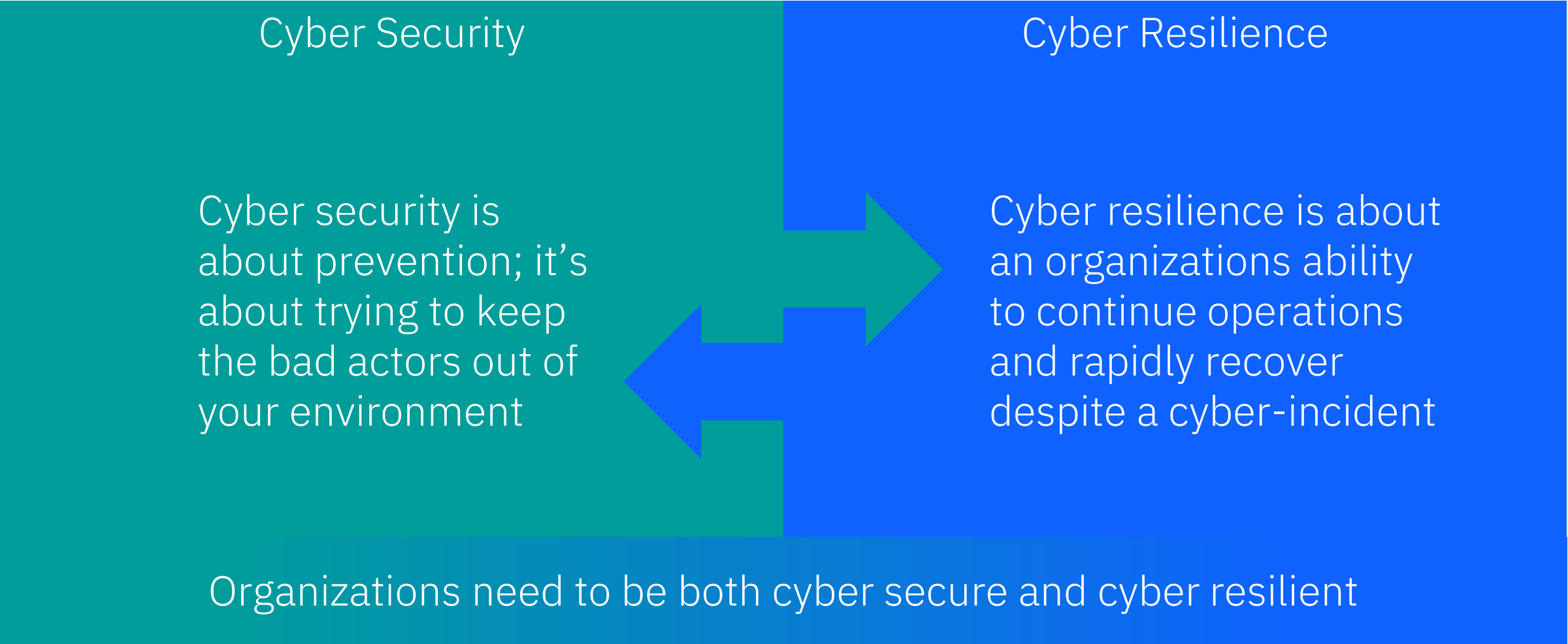
Speed recovery to significantly reduce the impact of breaches



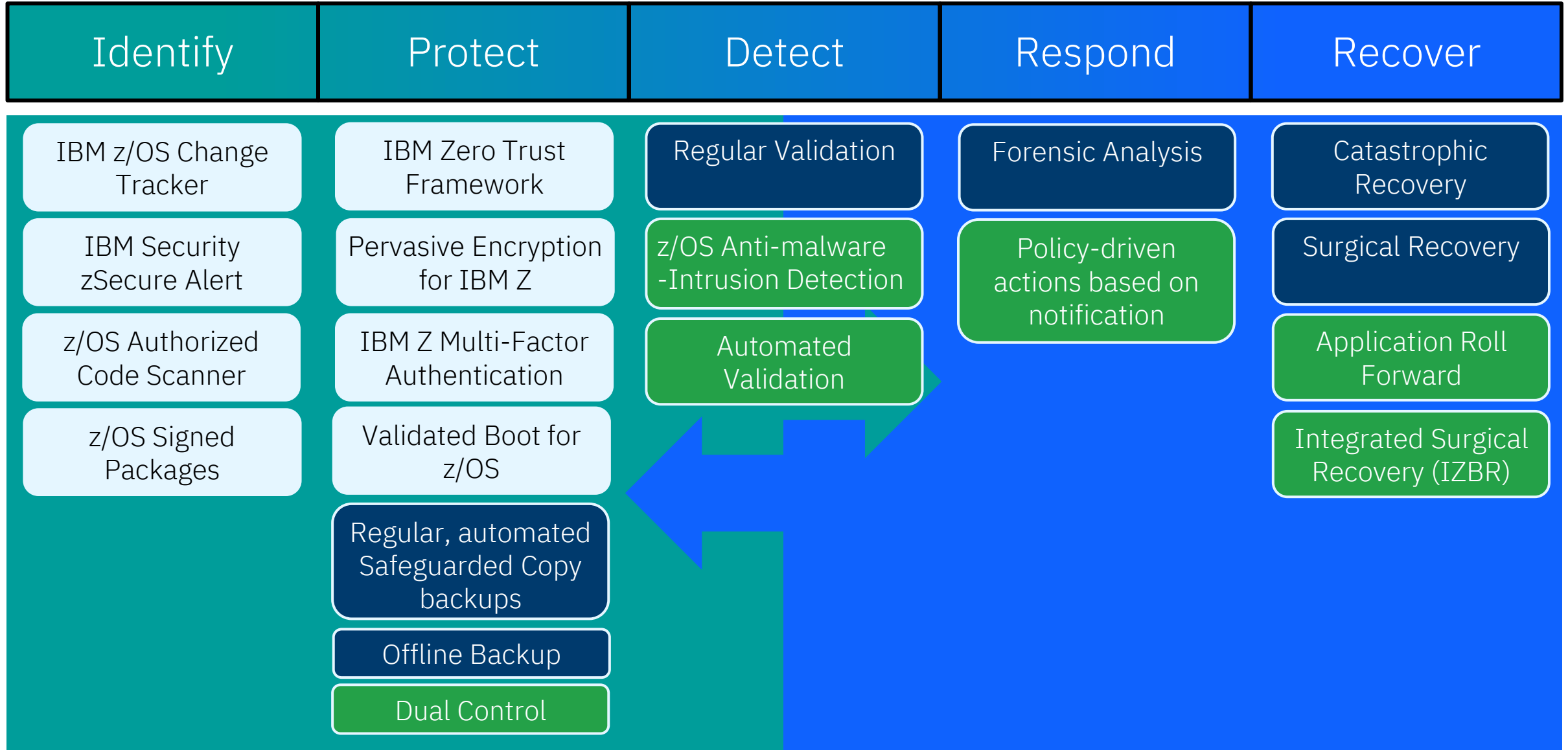
Due to the Cyber Vault environment and the use of SafeGuarded Copy technology, data is continuously checked and corruption is found and can be corrected fast. Leading to a shorter impact time.

IBM Z Cyber Vault Roadmap

Cyber Security and Cyber Resilience



Cyber Security and Cyber Resilience – with NIST framework



Dual Control

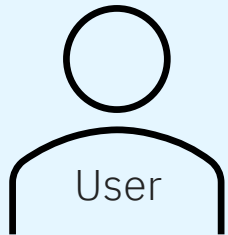
Dual Control

Potentially destructive actions will require additional authorization before they are executed

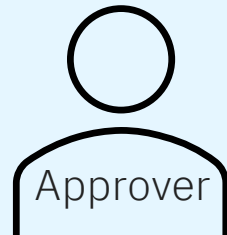
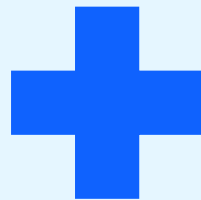
Only a subset of users will be granted “approver” access to be able to reject or approve these pervasive actions

This model will first be rolled out on our Logical Corruption Protection feature and offer further security of FlashCopy and SafeGuarded copy management profiles

Fulfills the “IBM intends to further extend the security in GDPS by providing dual control model for pervasive or potentially destructive actions in the GDPS LCP Manager plus finer grained security controls on the LCP Management Profiles” – Statement of Direction



User attempts a change



Approver reviews & approves the change



Action is executed

Dual Control - Examples

Creating a management profile – A user defines a new profile, and the parameters must be verified before creation

Modifying a management profile – A user wants to make a change to an existing profile and the update must be approved by another user to validate the reason and type of change

Deleting a management profile – A user wants to completely remove a management profile from LCP and before this removal occurs, another user must validate that this is a safe action to take

Flagset in EDIT mode – A user wants to include or exclude a volume from the next capture process. Another user must first verify that this action wouldn't leave out any important copies of data from the next capture before approving this action

Intrusion Detection

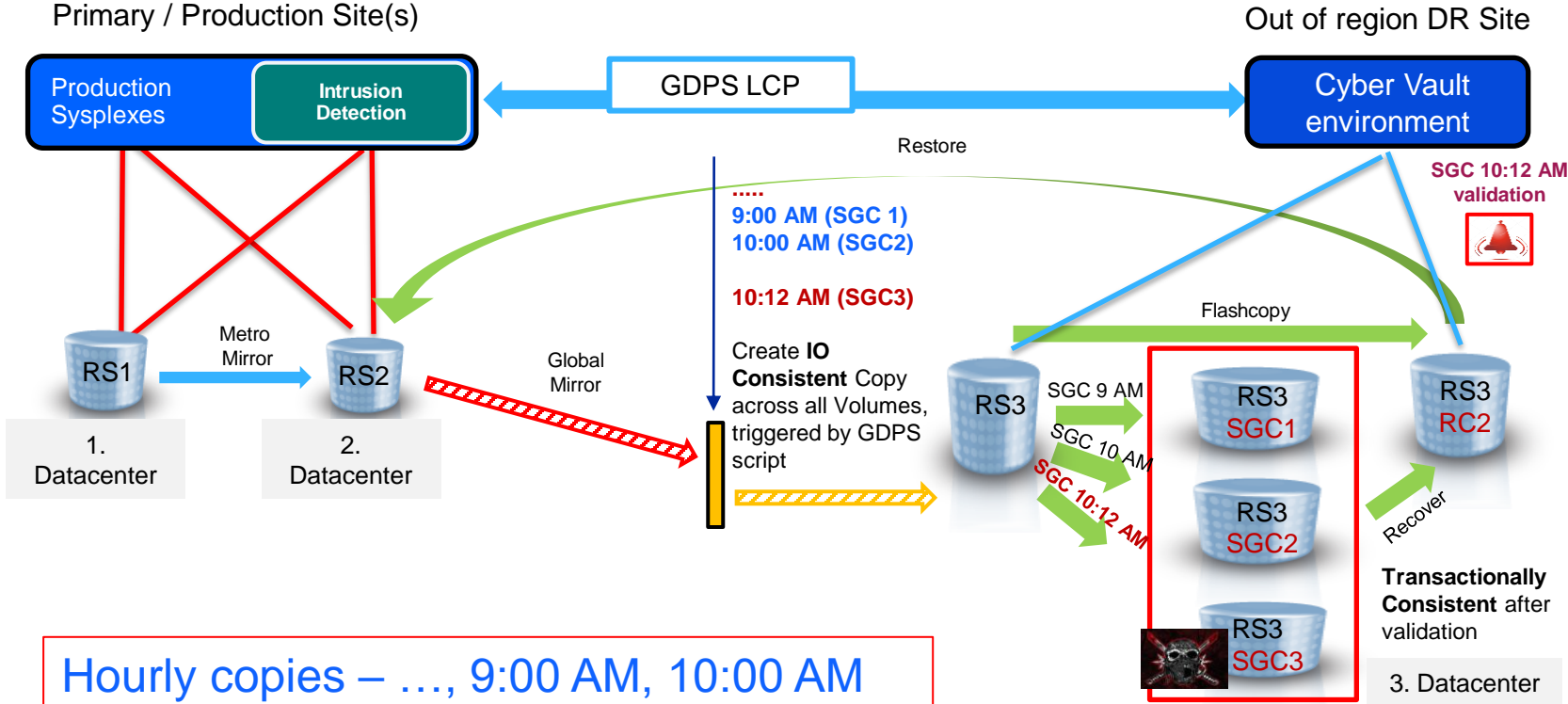
IBM Z Cyber Vault (3-site solution example)

Today's Cyber Vault implementation is focusing on "Detect", "Respond" and "Recover" activities.

IO consistent DASD copies in z/OS environments are the cornerstone of the solution.

GDPS/LCP is used to manage the Safeguarded copies and can automate Cyber Vault IPLs.

Intrusion Detection Software complements GDPS/LCP actions, including triggering copies of data and freezing prior snapshots



Hourly copies – ..., 9:00 AM, 10:00 AM
 *Event driven copy – 10:12 AM
 *Intrusion detection finds abnormal activity and signals proactive copy to GDPS – and freeze SGC2 (no overwrite)

- Intrusion Detection
- Reduces RPO since cyber event detected within minutes
- Reduces RTO since there is less archive log to "roll forward"

Automated Capture & Validation

IBM Z Cyber Vault data validation



Types of Data Validation

Type 1

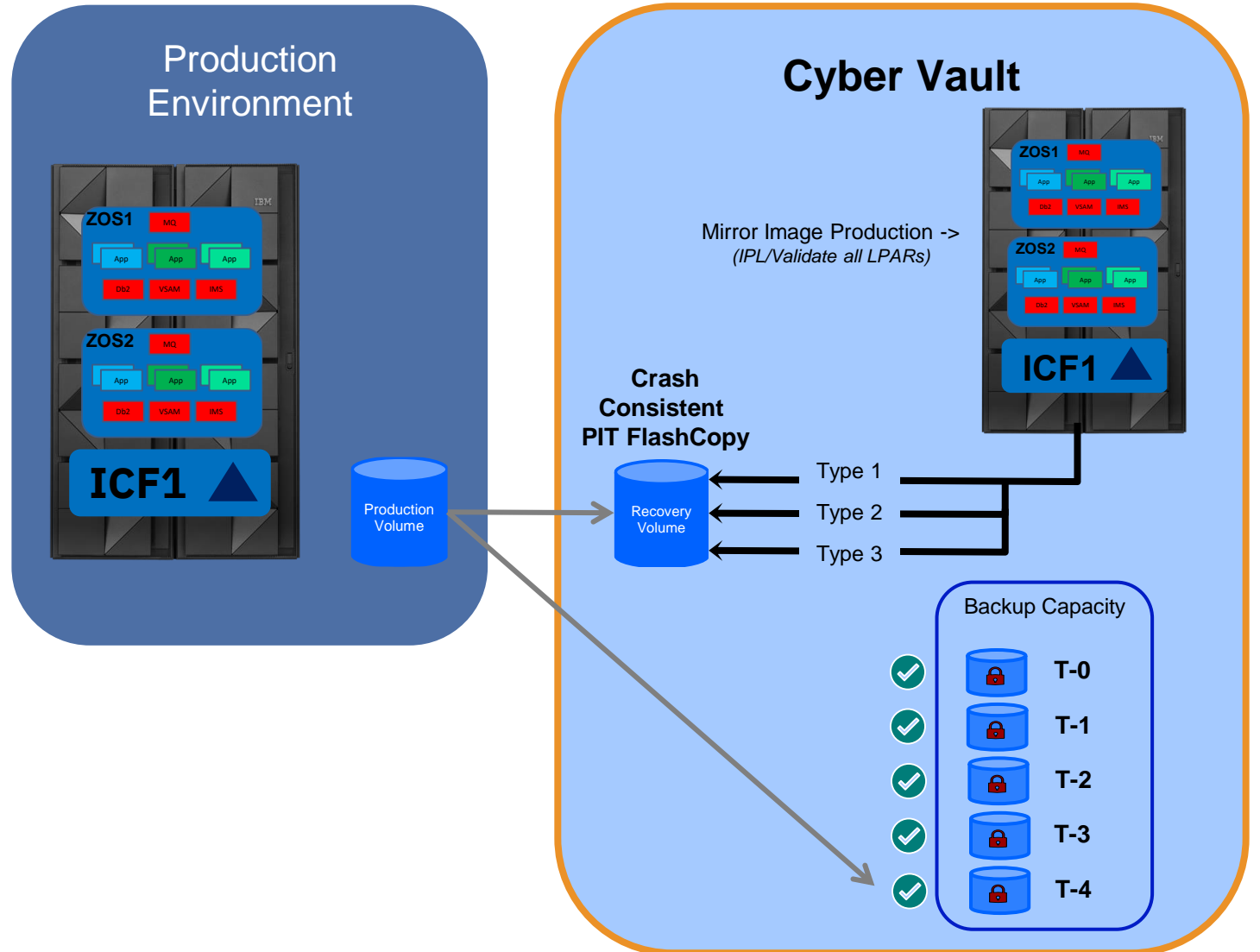
- System Data Validation – IPL, z/OS, subsystems, middleware, database Restart/Recovery

Type 2

- Data Structure Validation – catalogs, VTOCs, database indexes

Type 3

- Application Data Validation
 - *User written validation routines to validate content*



Capture and validation scheduler



- Automated capture and validation operations using a simple scheduler
- New management profile fields to control the scheduled operations
 - **Capture Interval**
 - Time between automated captures
 - A value of NO (default) means automatic capturing is disabled
 - **Capture Base Origin Offset**
 - Offset is applied to the base time of 00:00 when creating the capture schedule
 - **Validation Interval**
 - Minimum amount of time between automated validations
 - When a new capture is taken, the amount of time since the last validation (automatic or on-demand) is calculated. If the time exceeds the validation interval, a direct FlashCopy to RCn is also taken and validation is performed.
 - A value of NO (default) means automatic validation is disabled.
 - **Validation Recovery Copy Set**
 - Specifies the recovery copy set to be used by automated validation

Data Validation (on-demand)



Validation of the current production version of data

- Perform a SGC capture with a direct FlashCopy to RCn in the same window and perform validation
- Flag validity of new capture and older captures
- Used internally when *Validation Interval* is set

```
LCP=CAPTURE PROFILE(mp_name) VALIDATE(validation_type) [RC(n)]
```

Validation of an existing capture

- Recover a tagged SGC to RCn and perform validation
- Flag validity of older captures

```
LCP=RECOVER PROFILE(mp_name) VALIDATE(validation_type) [RC(n)]
```

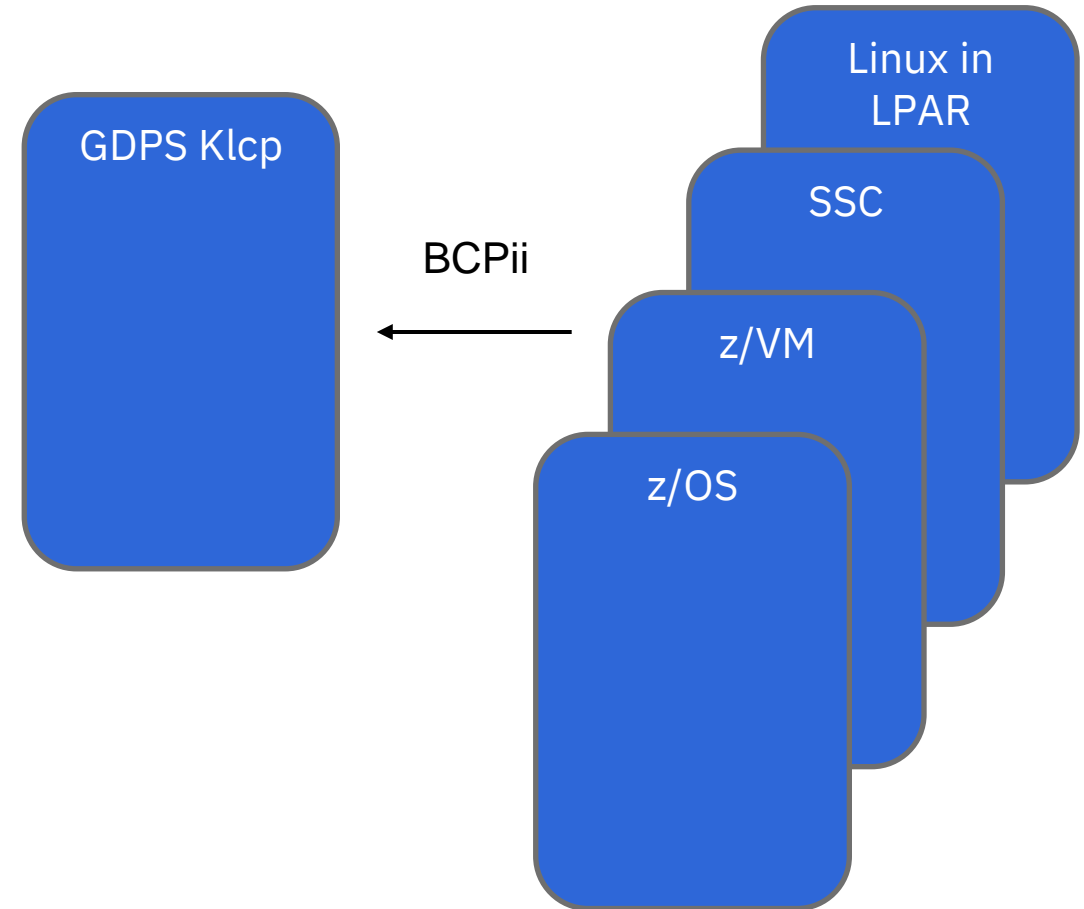
Automated validation support Phase 1



Validate successful IPL of the operating system

Once a validation is triggered (by the validation scheduler or via on-demand request):

- Systems are automatically IPLed in the vault
- BCPii filtering is used to monitor for successful IPL messages (messages differ depending on type of system being IPLed)

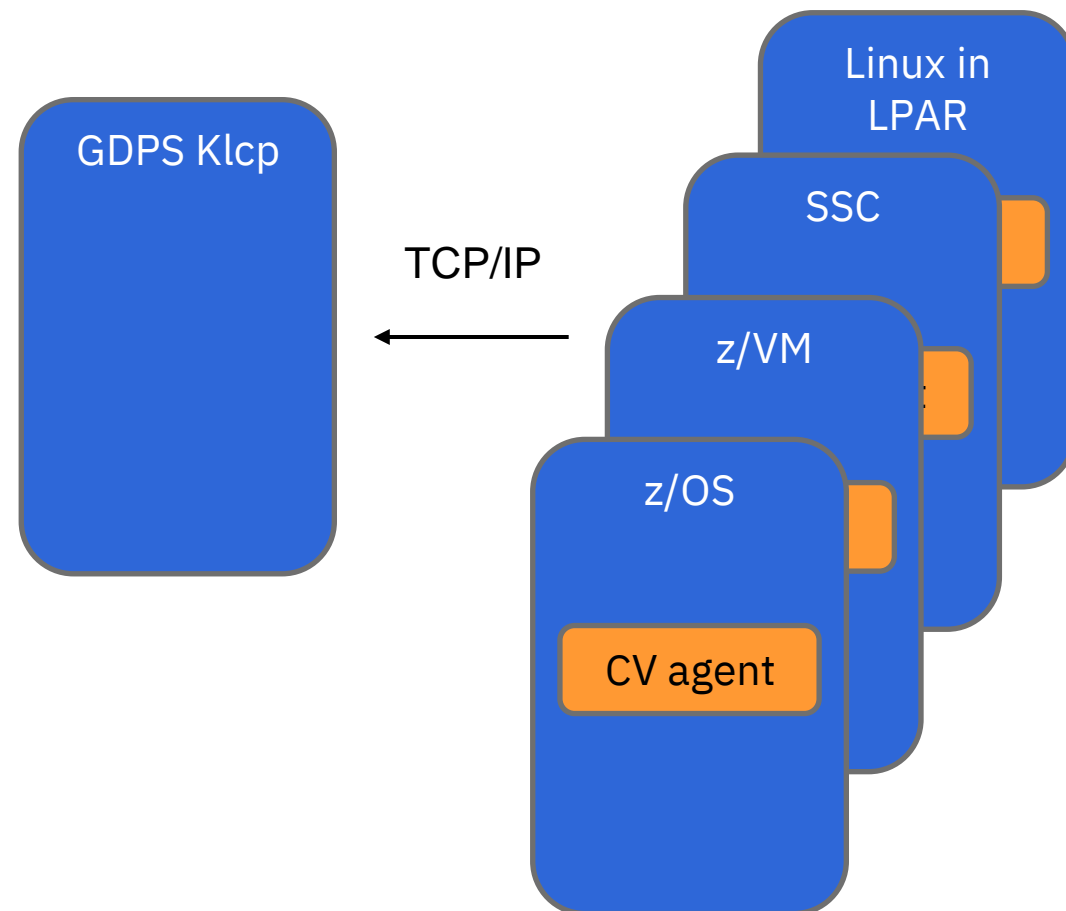


Automated validation support Phase 2



An agent is added to enable deeper IPL validation

- z/OS systems – Subsystems, middleware, database Restart/Recovery
- z/VM systems – virtual machines started



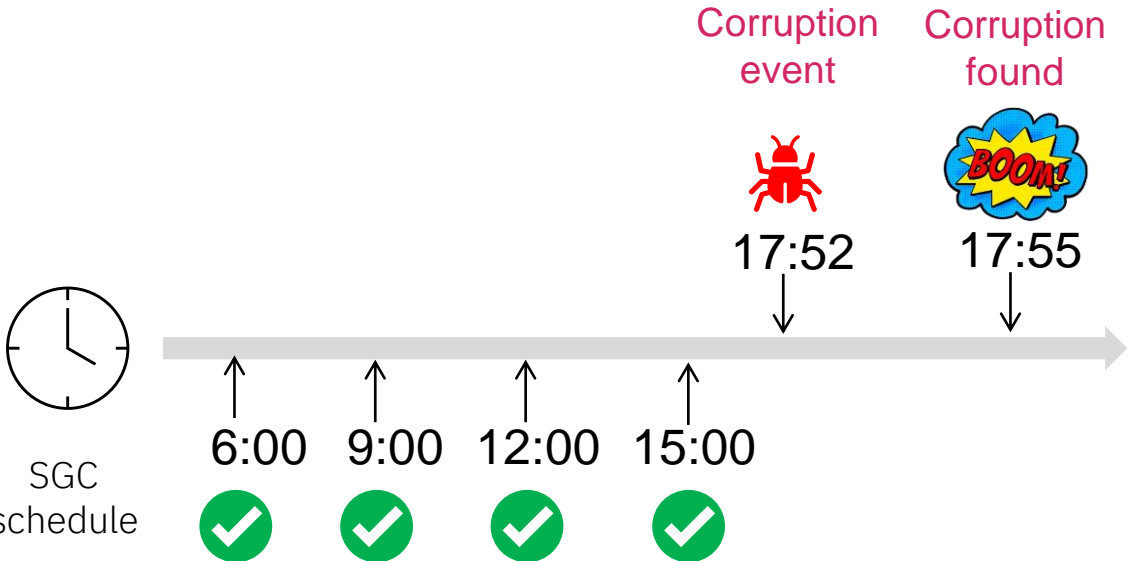
Application Roll Forward

Problem Statement

With a standard approach, there may be minutes or hours of good data that isn't captured in the most recent 'good' Safeguarded Copy (SGC).

Are there any techniques or technology that can make available that good data as close to the point of corruption as possible?

Stage 1: Restore from most recent good Safeguard Copy



- System was corrupted at 17:52
- Most recent good SGC captured at 15:00
- Corruption identified at 17:55 in Production

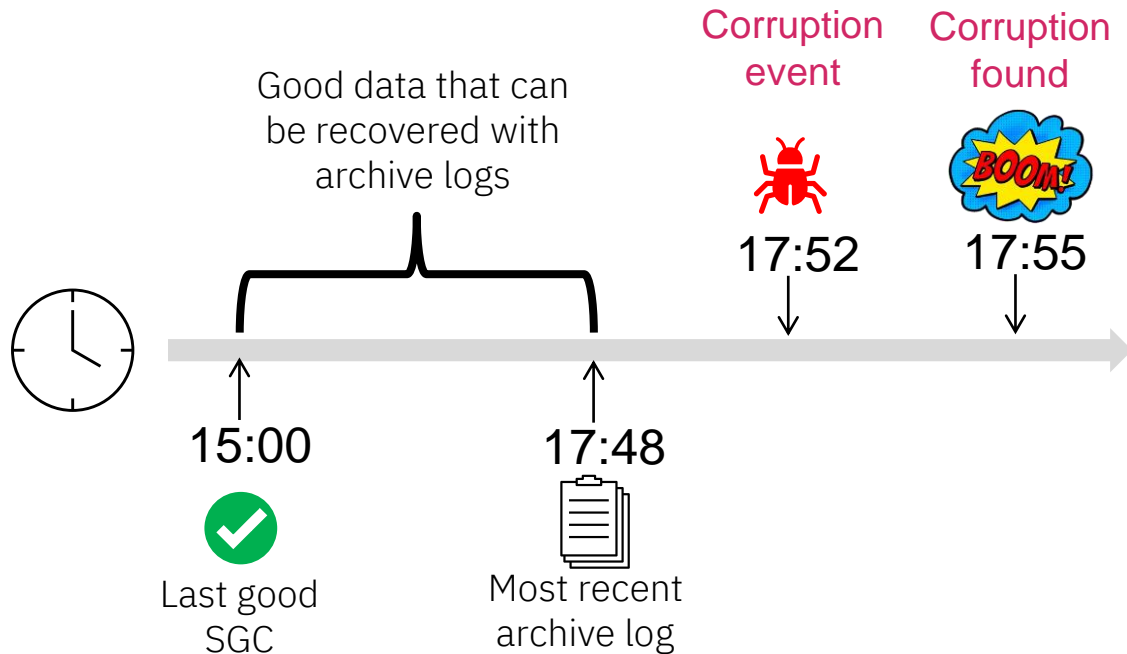
Use Data Validation to identify the most recent good SGC

- When Data Validation was run on the 15:00 SGC it was verified as good

Last good back up is 2 hours and 55 minutes before corruption found in production

However, 2 hour and 52 minutes of that time is before the corruption event and this data could potentially be used if it could be recovered

Stage 2: Capture and Restore Db2 archive logs



- Most recent good SGC at 15:00
- Archive logs available up to 17:48
- An additional 2 hours and 48 minutes of good data are potentially available reducing RPO to minutes

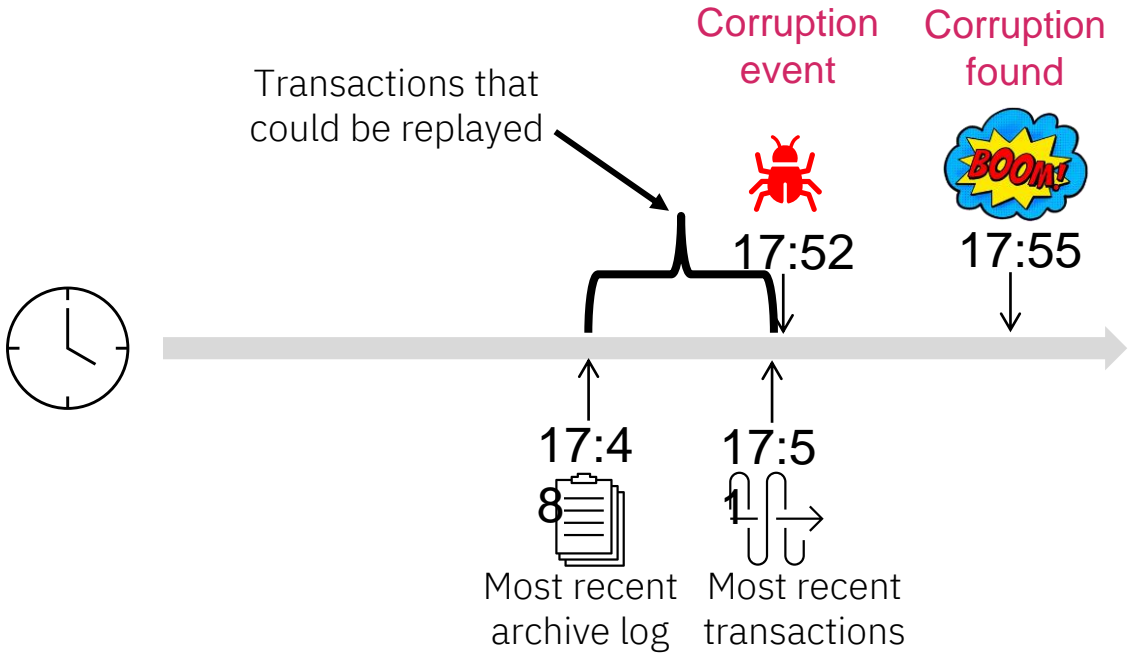
Capture and store Db2 archive logs

- Configure Db2 to archive logs as frequently as possible
- Depending on number of Db2 data sharing members, archive logs should be generated every 4 to 8 minutes
- Decide on an approach to create an immutable copy of the archive logs
 1. Write to WORM on TS7700
 2. Use disk-based replication to an appropriate immutable destination
 3. Move to secured cloud storage

The combination of the restored SGC plus the stored archive logs should bring the RPO down to single digit minute range

NOTE: Db2 used for illustrative purposes. Similar tools/techniques are available for other subsystems

Stage 3 (Optional): Use software replication to replay transactions



- Archive logs available up to 17:48
- Transaction logs available up to several seconds before corruption event
- An additional 4 to 8 minutes of data available reducing RPO to seconds

Capture and store transaction logs

- Stream transaction log in real time to secured environment. This should result in data loss of just several seconds
- After restoration via SGC (Stage 1) and archive logs (Stage 2), use Qrep, or other subsystem equivalent, to replay transactions over remaining few minutes

NOTE: If corruption is identified more than 4-8 minutes after the event, then this approach will not be required as archive logs will be available

Implementation of all 3 stages will result in the minimal possible RPO. However, this is also likely to increase the RTO and it's important to think about the best balance between these two objectives

Integrated Surgical Recovery

IZBR in an IBM Z Cyber Vault environment

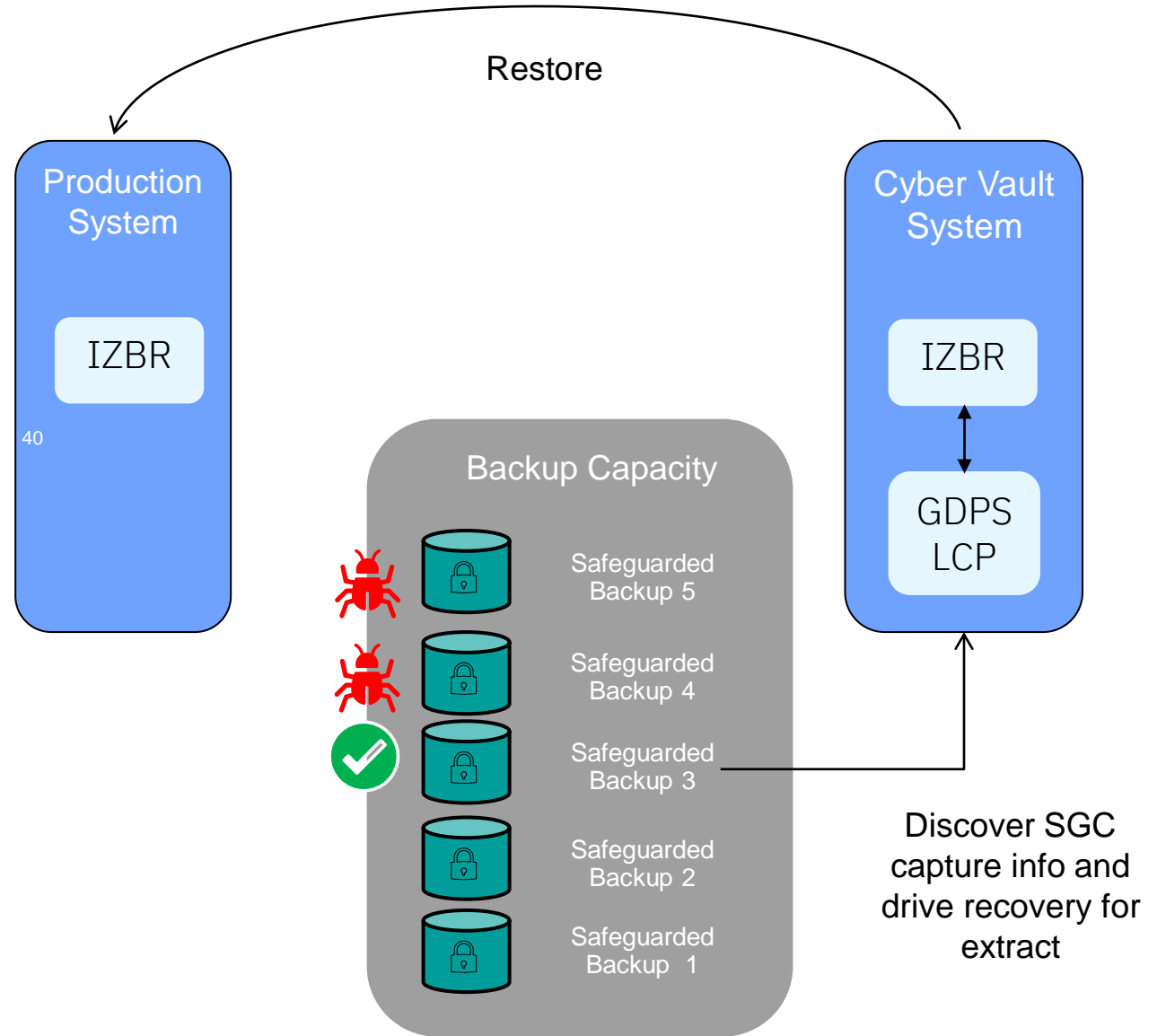
If IZBR is running in the production system, it can provide significant assistance to reduce RTO in the event of a cyber incident

Forensic Analysis

- Complete inventory of datasets in all Safeguarded Copy backups
- Health check of Safeguarded Copy backups, indicating which datasets were open for update at time of capture

Surgical Recovery

- Select identified datasets, and recover to staging volumes with a rename



Typical Cyber Vault Implementation Journey

Typical Cyber Vault Implementation Journey

Provides the foundation to respond to corruption events. Time to restore may be long.

Reduces business impact by reducing the time to detect, respond and recover.

Improves compliance with retention requirements.

Phase 1	Phase 1A	Phase 2	Phase 3	Phase 4
<i>Protect the data</i>	<i>Recover and IPL Type 1 Validation</i>	<i>Restore to Production</i>	<i>Type 2 Validation</i>	<i>Offline Backups (if needed)</i>
<ul style="list-style-type: none"> Implement SGC Implement GDPS LCP (based on timing and topology with standalone LCP) 	<ul style="list-style-type: none"> Create IBM Z Cyber Vault infrastructure Recover SGC to RC1 IPL Sysplex from RC1 Define strategy and processes for forensic analysis Implement and automate Type 1 validation 	<ul style="list-style-type: none"> Design recovery strategy and processes Implement required replication infrastructure and network Restore from SGC to production volumes 	<ul style="list-style-type: none"> Define scope of Type 2 validation Implement Type 2 validation Automate Type 2 validations 	<ul style="list-style-type: none"> Design backup processes Create LPAR to perform backup Perform backup from RC1 to virtual tape or COS



Thank you!

Accelerate with ATG Technical Webinar Series - Survey

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

You can access this 6-question survey via [Menti.com](https://www.menti.com) with code 2243 3599 or

Direct link <https://www.menti.com/albneqj15g57>

Or

QR Code

