IBM Z Cyber Vault Explained: Soup to Nuts and Nose to Tail

Aleksander Mieczkowski
IBM - GDPS Developer

Cost of a Data Breach

Average total cost of a data breach in 2024 (Worldwide)

$4.44 million

Average total cost of a data breach in 2024 (USA)

$10.22 million

+9%

"Cybercriminals are most often breaking in without breaking anything – capitalizing on identity and access management gaps proliferating from complex hybrid cloud environments. Compromised credentials offer attackers multiple potential entry points with effectively no risk."

Mark Hughes,

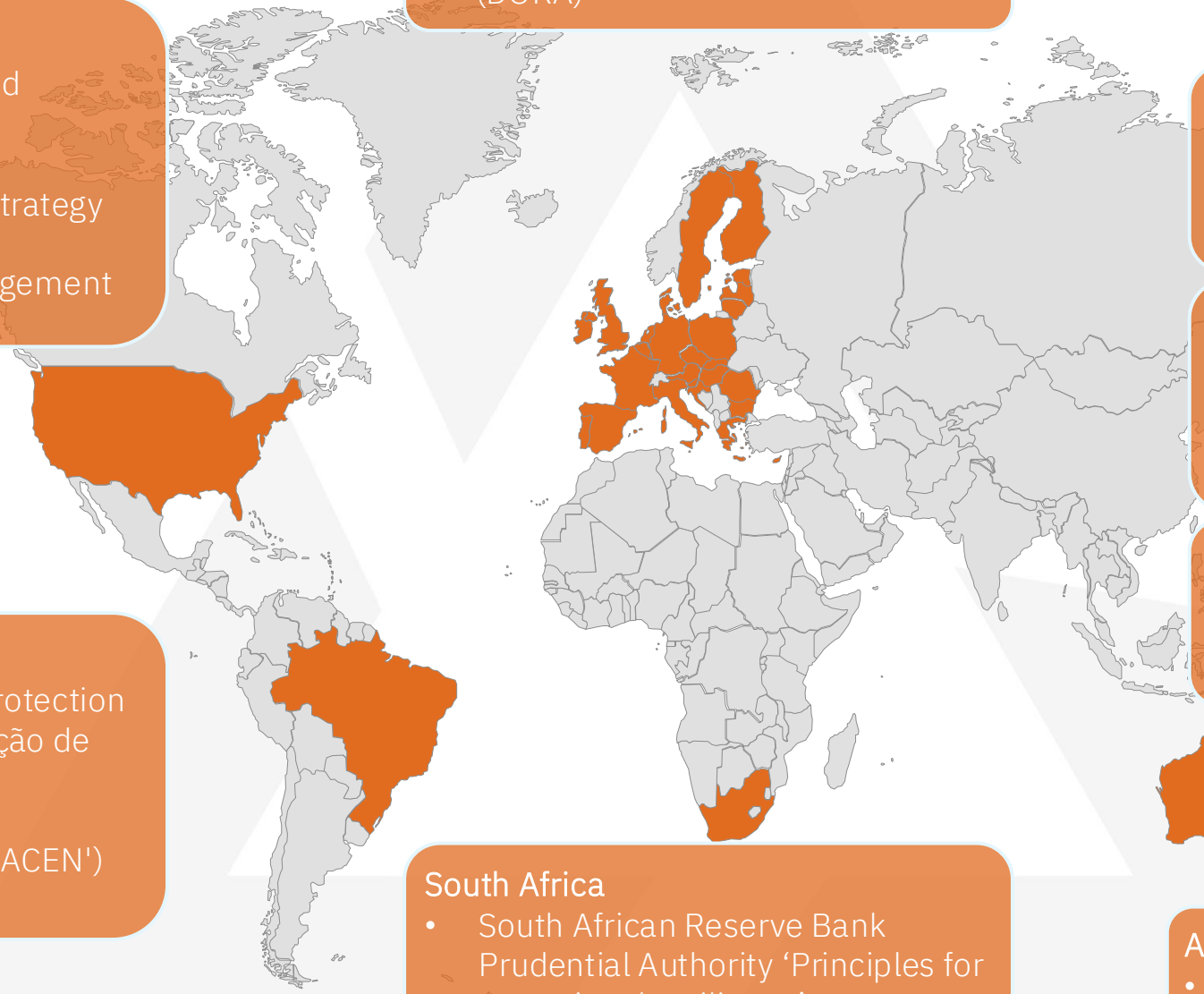
Global Managing Partner for Cybersecurity Services, IBM

Source: IBM X-Force 2025 Threat Intelligence Index

Worldwide regulation

Europe
- Digital Operational Resiliency Act (DORA)

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



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

Global
- Basel Committee on Banking Supervision issued 'Principles for Operational Resilience' and 'Principles on Outsourcing'

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

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

South Africa
- South African Reserve Bank Prudential Authority 'Principles for operational resilience'

Australia
- Prudential Standard CPS 230 - Operational Risk Management

Cyber Security verses Cyber Resilience

SHARE
EDUCATE • NETWORK • INFLUENCE

Cyber Security

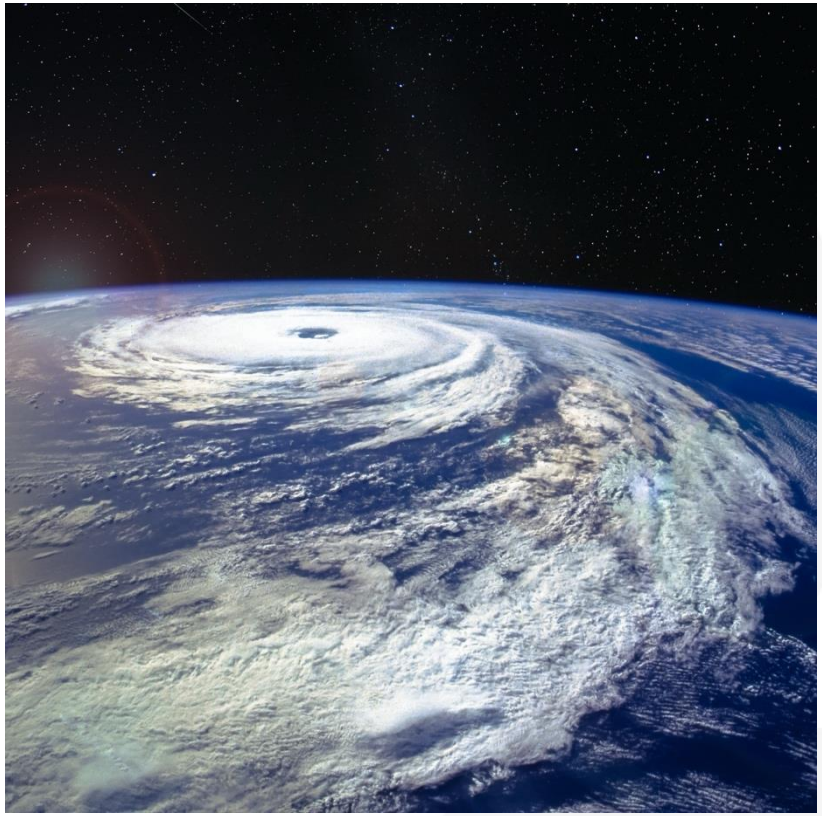
Cyber security is about prevention; it's about trying to keep the bad actors out of your environment

Cyber Resilience

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

Organizations need to be both cyber secure and cyber resilient

Traditional resiliency solutions will not protect you from cyber attack



	Traditional resiliency for HA/DR	What's required for Cyber Resiliency
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 with IBM Solutions

- ✓ IBM Z Cyber Vault Storage
  - ➢ DS8000 with Safeguarded Copy
  - ➢ TS7700 with LWORM Retention

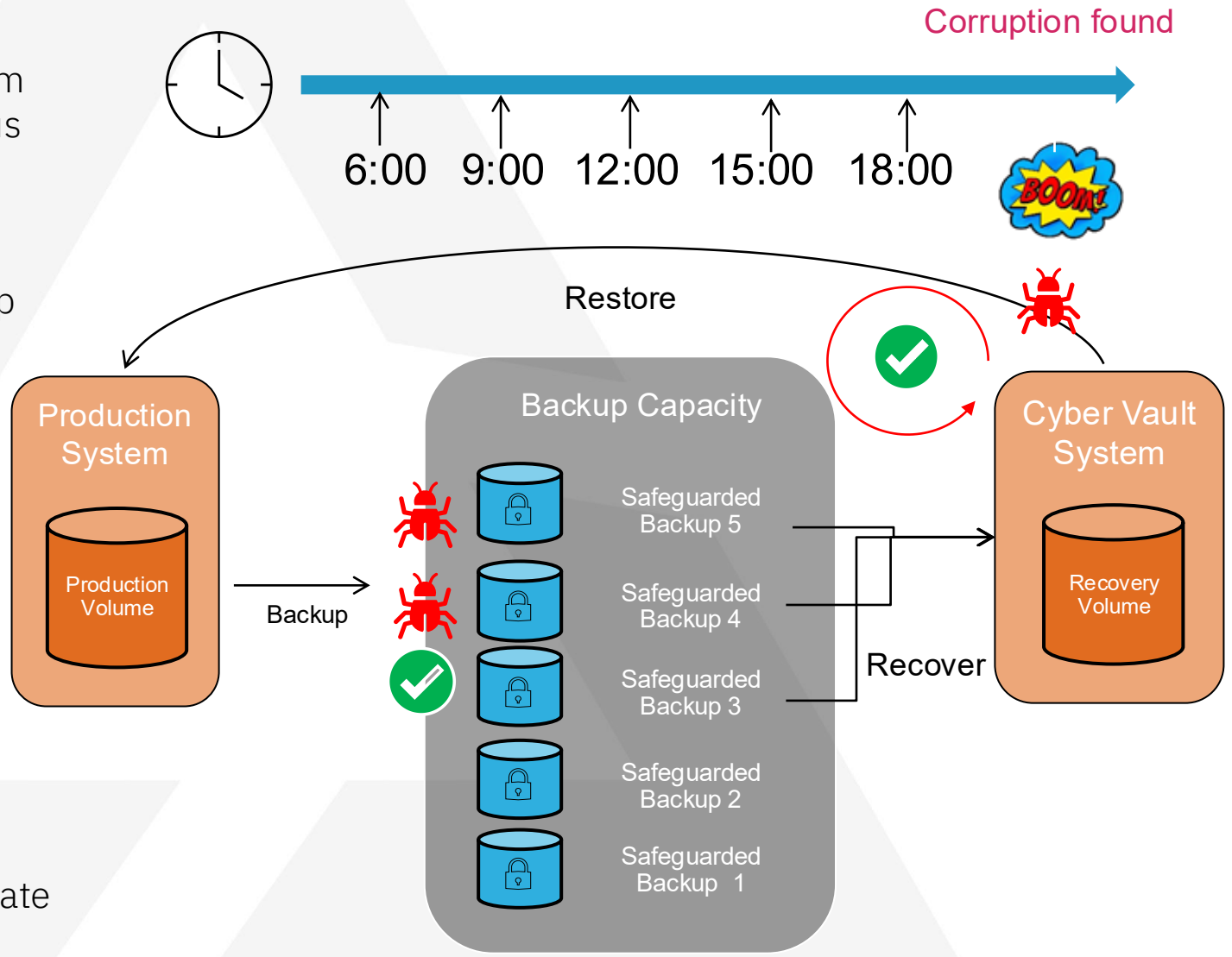
- ✓ IBM Z Cyber Vault Automation
  - ➢ GDPS Logical Corruption Protection (LCP) Manager
  - ➢ IBM Technology Expert Labs Z Cyber Vault validation services assets to drive three types of validation:
    1. Infrastructure
    2. Data Structure
    3. Data Content

- ✓ IBM Z Cyber Vault Environment
  - ➢ IBM Z Hardware including CPs, zIIPs, ICF, memory and required infrastructure
  - ➢ IBM Z Cyber Vault Environment Licensing (5770-ZCV) - the full IBM Z SW production Stack (MLC & OTC) in the CV environment
  - ➢ IBM Z Software Tools

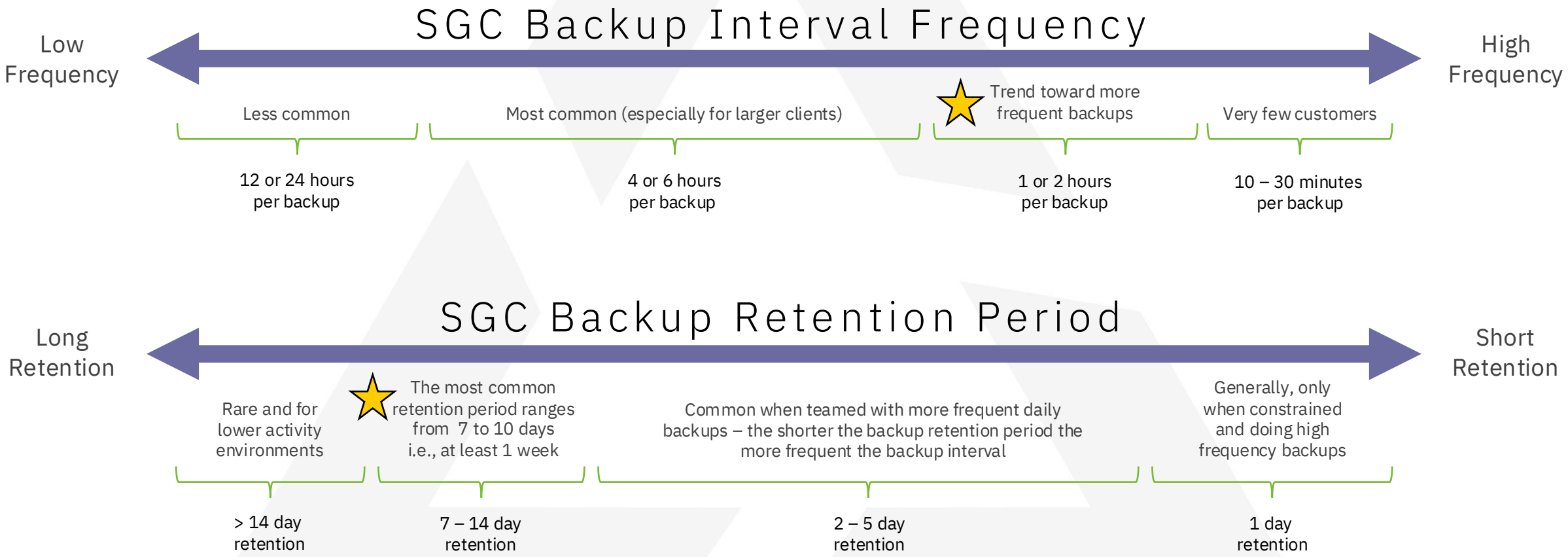
Customers can start their journey at any of these entry points, and progress based on their specific requirements.
Third party tools must be licensed and priced independently of the IBM Z Cyber Vault PID.

Protect your data with IBM 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 1024 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
- IBM GDPS or IBM CSM is required in order to create and manage the Safeguarded Backups



SGC Capture Frequency

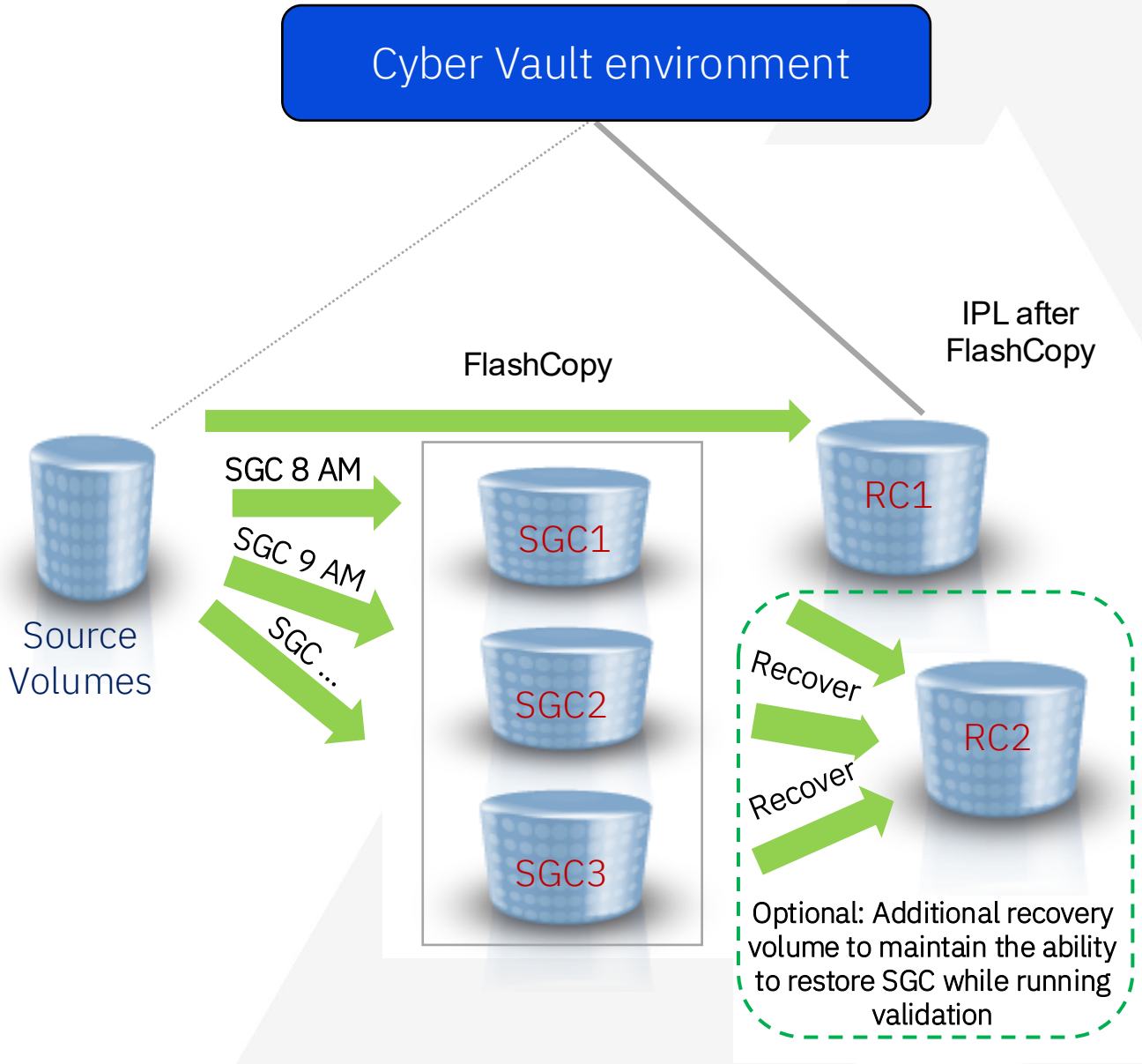


Data validation

Detect data corruption early or validate that the copy is clear

- Data validation is the process of executing regular analytics to identify a data corruption situation and determine the most convenient recovery action.
- Performing corruption detection and validation processes against a copy of data is more practical than doing this in the live production environment.
- Valid data can be sent to offline media to have a reliable and isolated point-in-time copy.

Data validation



Early identification of potential issues

Type 1: Infrastructure Validation
- IPL off FlashCopy of production sysplex to Recovery Copy set (RC1)
- Check sysplex infrastructure & subsystem restart

Type 2: Data Structure Validation
- Db2 Utilities (CHECK DATA/INDEX, Log analysis)
- IMS Utilities (Pointer checker)
- Catalog tools (Tivoli, IDCAMS, ISV products)
- VSAM Indexcheck, Datacheck
- DFSMShsm, DFSMSrmm tools
- RACF (IRRUT200), zSecure-Audit
- ISV software (CA1, CA7, ...)

Type 3: Data Content Validation
- Customer application program

Forensic analysis

SHARE
EDUCATE • NETWORK • INFLUENCE

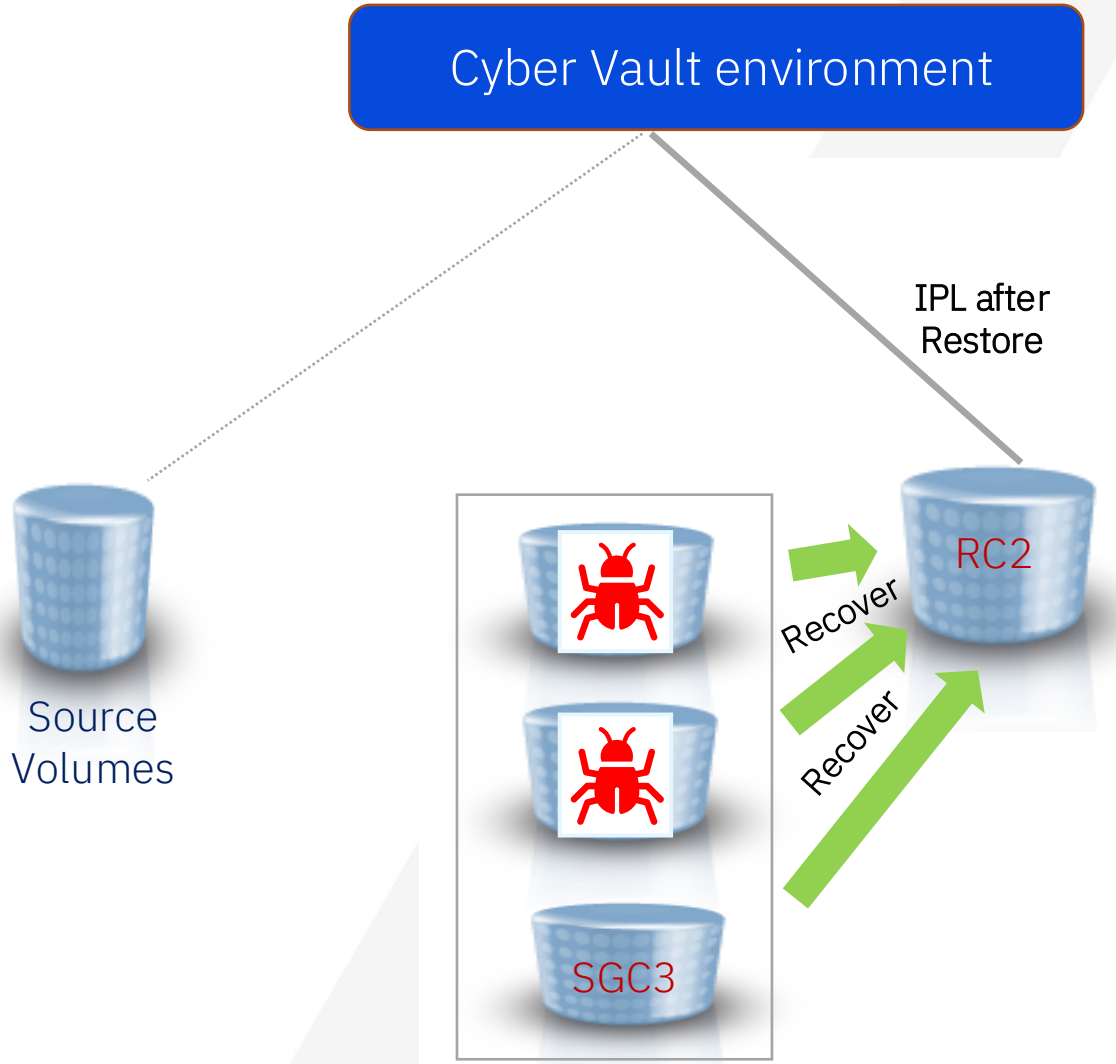
Investigate the problem and determine the best recovery action

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

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

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

Forensic analysis



Determine start of data corruption …

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

Surgical recovery

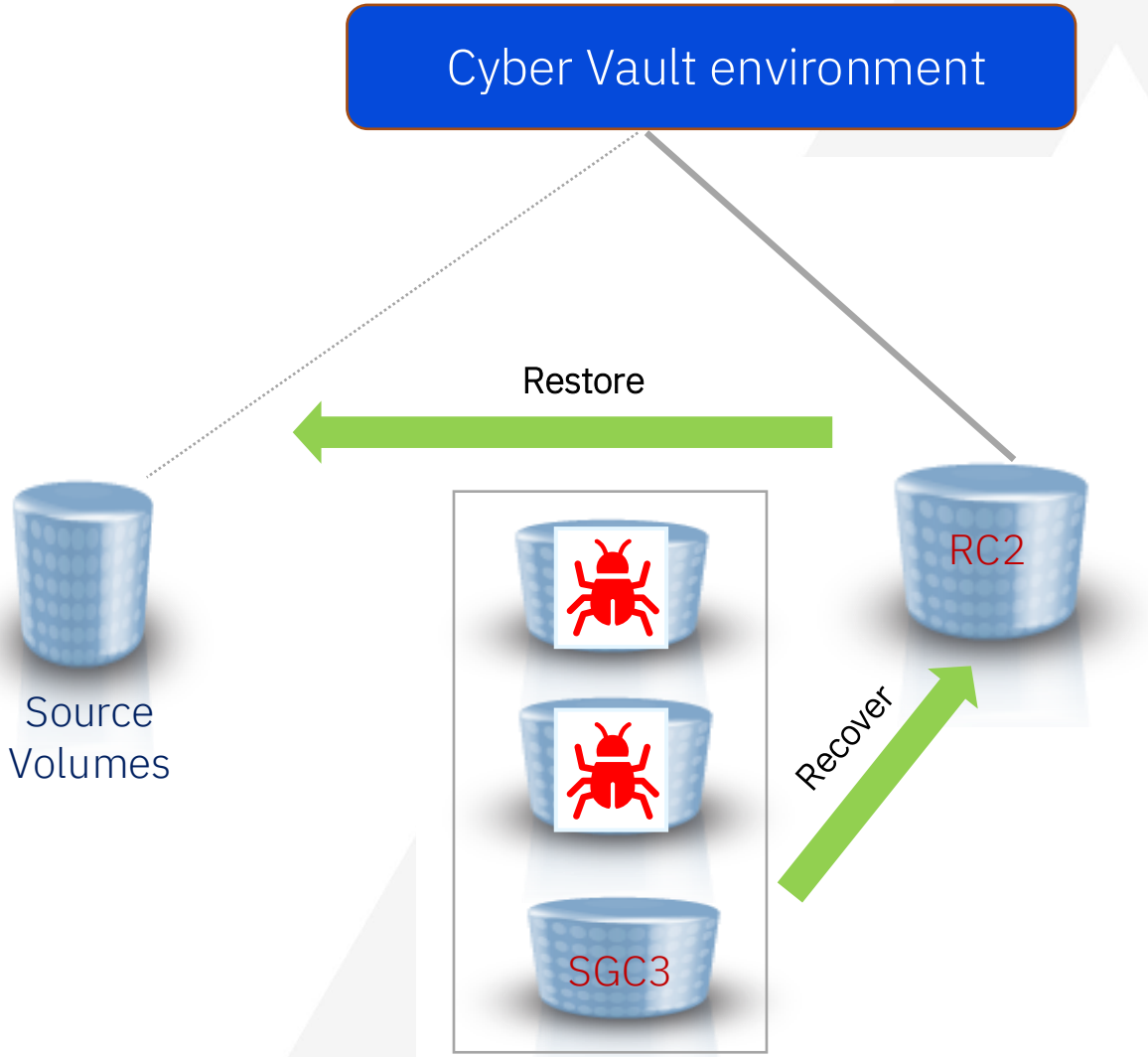
SHARE
EDUCATE • NETWORK • INFLUENCE

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

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

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

Surgical recovery



Restore confirmed ‘good’ copy

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

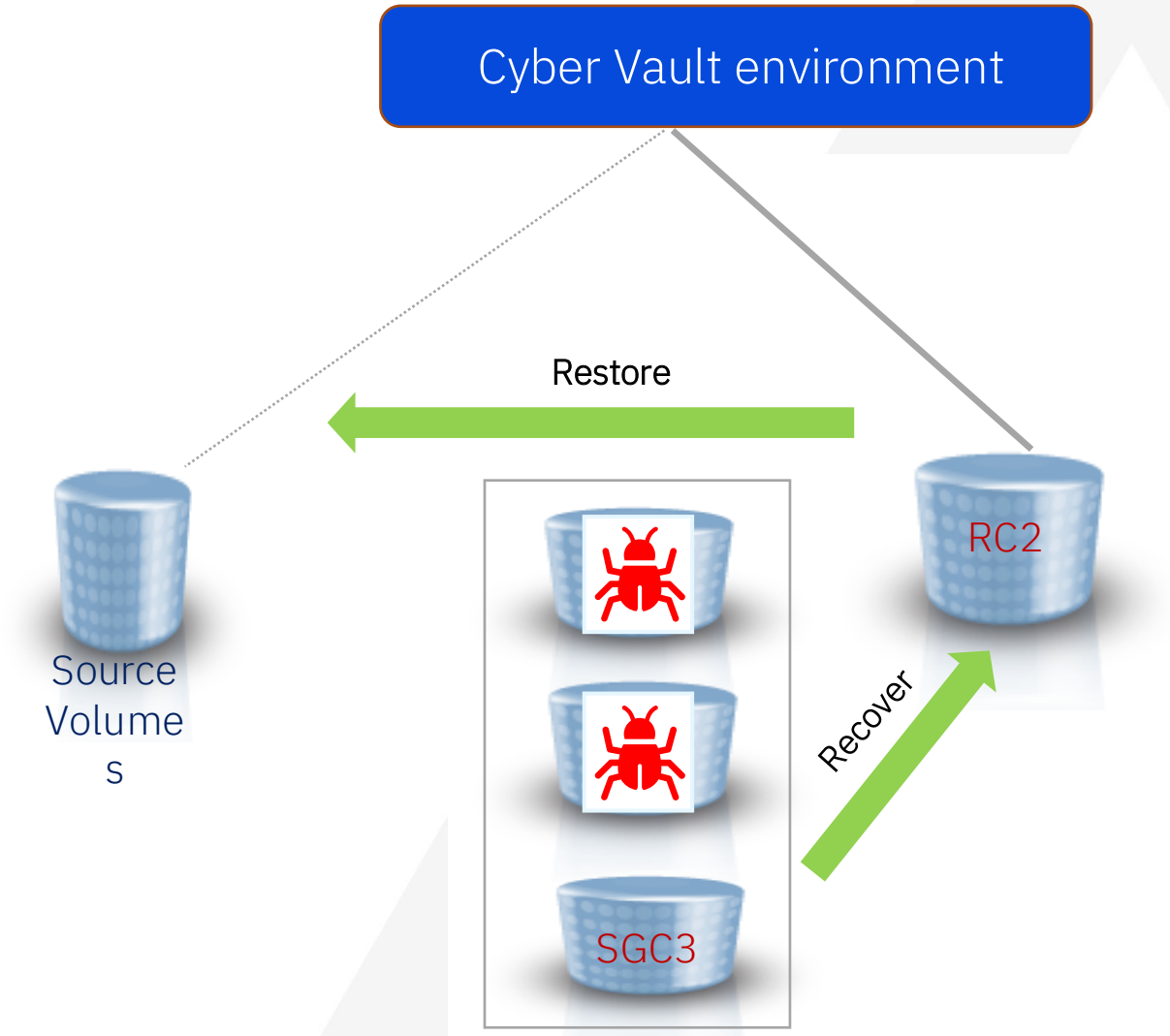
Catastrophic recovery

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Recover the entire environment back to a point in time copy

- In the case of massive corruption to all or most of the data in the environment, a 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



Restore identified ‘good’ data

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

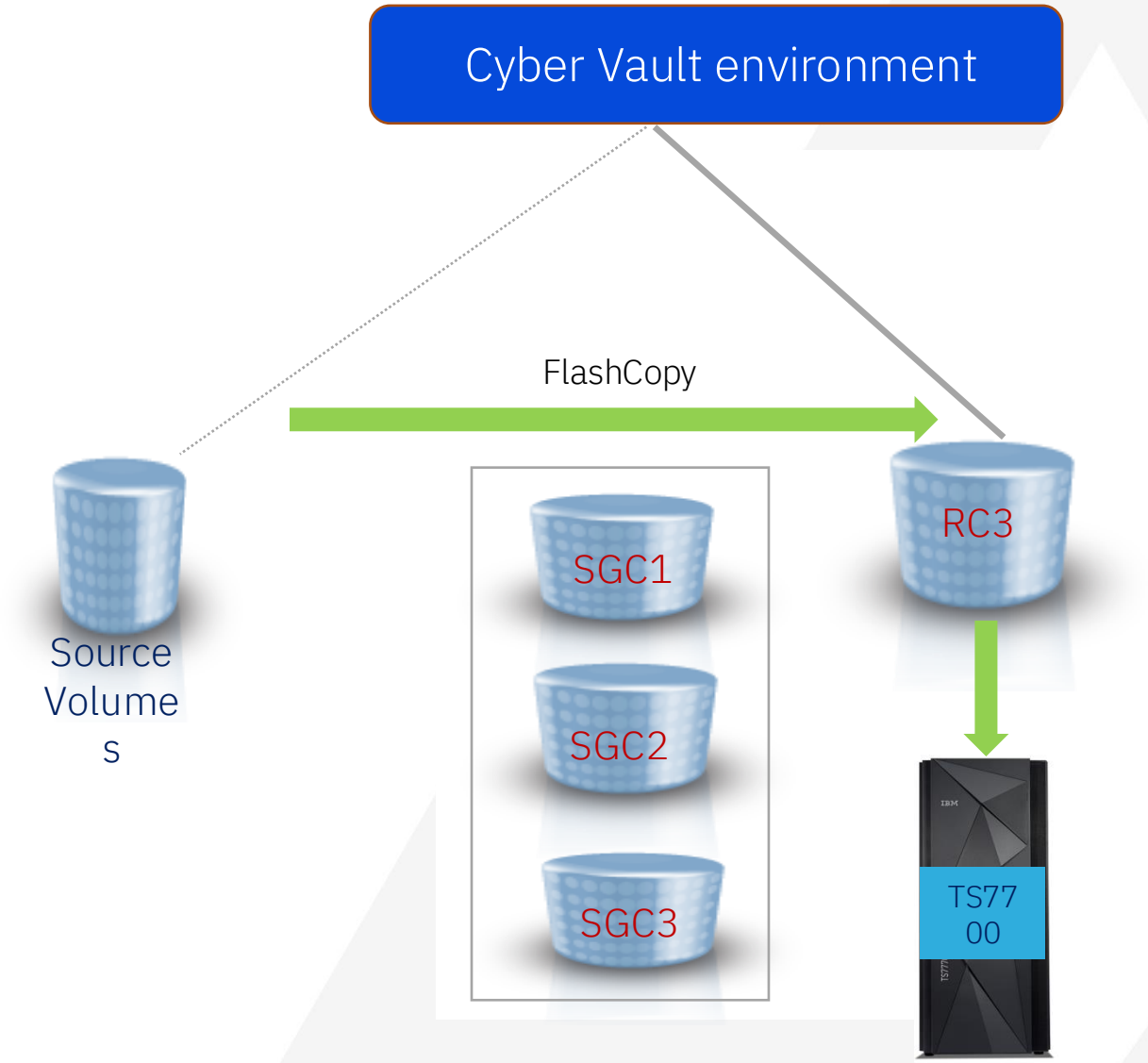
Offline Backup

Backup copy of the clean environment to offline tape media

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

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

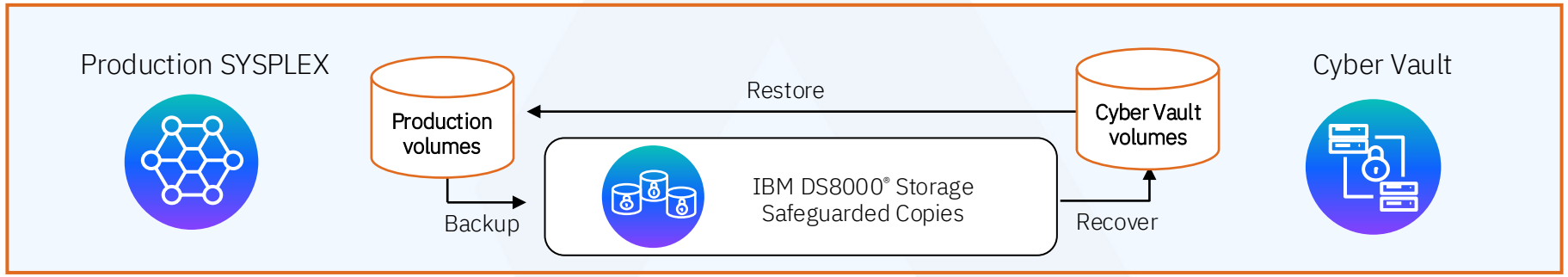
Offline backup



Longer term storage

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

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

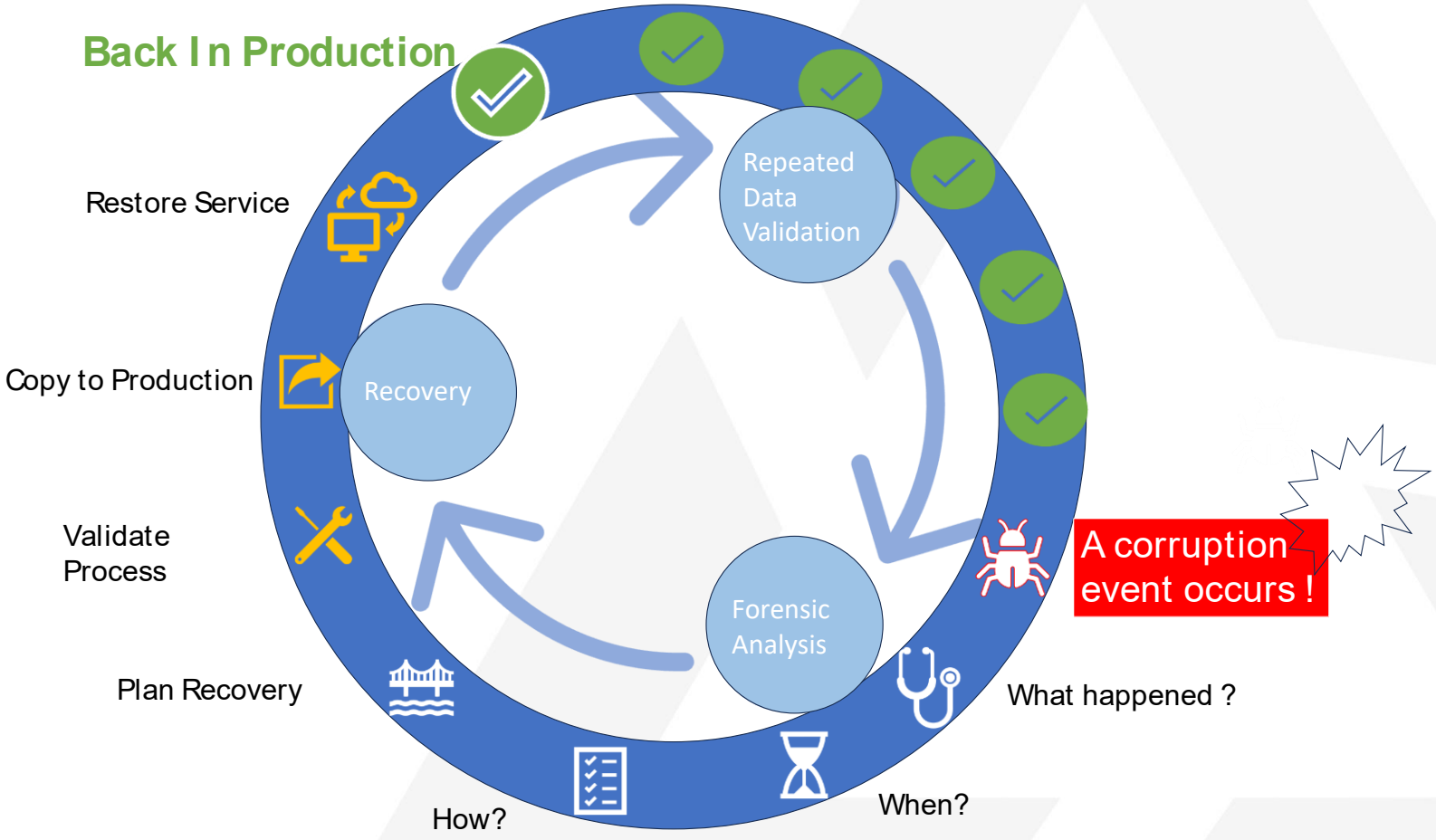
Catastrophic Recovery
Recover the entire environment back to a point in time copy

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 Backup Resiliency	IBM DFSMShsm™ tools	Db2® and IMS™ Tools

Process summary



Backup and Validation

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

Forensic Analysis

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

Recovery

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

IBM Z Cyber Vault Roadmap

2022

CV Automation — GA

Safeguarded Incremental Restore to Production
- LCP Manager (GM) support, MGM3SITE Virtual Isolation support, MGM3SITE & MGM4SITE Physical Isolation support

Monitoring enhancements
- Interval based monitoring, Pool Capacity Monitor, Internal Rolloff Monitor, SGC Backup Expansion Monitor, Capacity Monitoring (Phase 1)

Security enhancements
- LCP Main Panel Security, Role based SAF security

CV Storage — GA

Safeguarded Copy
- Initial SGC support (2018)
- Incrementally restore SGC capture from GM secondary to GM primary
- FlashCopy to Safeguarded Source

2023

CV Automation — GA

Safeguarded Incremental Restore to Production
- GM2SITE Physical Isolation support

Enhanced Cyber Vault support
- Automation & Data Capture Engines. AutoRelease & AllowPartial. Quiesce/Resume LCP operations

CV Environment — GA

Initial IZBR support
- Provide complete inventory of datasets in SGC
- Indication of open datasets at time of capture
- Support for surgical recovery of datasets

2024

CV Automation — GA

Security enhancements
- Dual control support

Additional topology
- MGM4SITE LCP Virtual Isolation in DR region

Standalone LCP Manager
- Enable clients using IBM Copy Services Manager (CSM) for replication management functions to implement GDPS LCP Manager
- Initial support for MM 2-site with physical or virtual isolation and GM 2-site with physical isolation

CV Environment — GA

Dedicated Cyber Vault SW Licensing
- License production SW stack in your Cyber Vault at a differentiated price point
- Enables systems to be started from a point-in-time backup to generate a Cyber Vault environment, with the existing production SW stack

IBM Threat Detection for z/OS
- Detect anomalies in z/OS dataset accesses that could be indicative of a cyberattack

Future

CV Automation - Future

Automated validation
- Automated Infrastructure Validation (Type 1)

Enhanced Cyber Vault support
- Automated action based on anomaly detection
- Automated LCP Surgical Restore and Recover

Automated validation
- Data Structure Validation (Type 2) validation and invocation of Data Content Validation (Type 3)

CV Environment - Future

Enhanced IZBR support
- Initiate communication from Cyber Vault out to production
- Catalog and dataset history retrieved from production

Please note this roadmap reflects IBM's best intension at this time but should not be taken as a commitment we will release any specific capability by a certain date

Adoption of IBM Z Cyber Vault

66

Unique clients have CV deployments

189

LCP Manager licenses now in use worldwide

32%

Of the worlds top 25 banks are using CV

IBM Z Cyber Vault deployment – Banking

Business Challenges	• A large European bank needing to address upcoming regulation to ensure they are compliant with the new Digital Operational Resilience Act (DORA) • The bank were looking for a solution that enables them to recover from a hacking or ransomware attack within a specific recovery time • Any solution needs to detect any data corruption within captured backups
Solution Benefits	• Provide the ability to perform a full system recovery in the event of widespread corruption • Provide the ability to perform a surgical recovery in the event of a cyber attack on a specific application • Validation of backups to ensure useable, corruption free copies
HA/DR Topology	• Existing GDPS client with multiple 3-Site Metro Mirror environments • TS7700 for archive / offline backup
Cyber Vault Solution	• Physically isolated Cyber Vault, extended from 2nd site via Global Mirror • Backup every 4 hours, retention period of 7 days • Automated validation on every copy (Type 1: Infrastructure, and Type 2: Data Structure)
Outcomes	• Solution is deployed in production • Solution supports the banks regulatory requirements

New update! IBM Z Cyber Vault redbook

Download the recently updated Redbook
ibm.biz/IBMZCVRedBook

Other recent items

- Web sites:

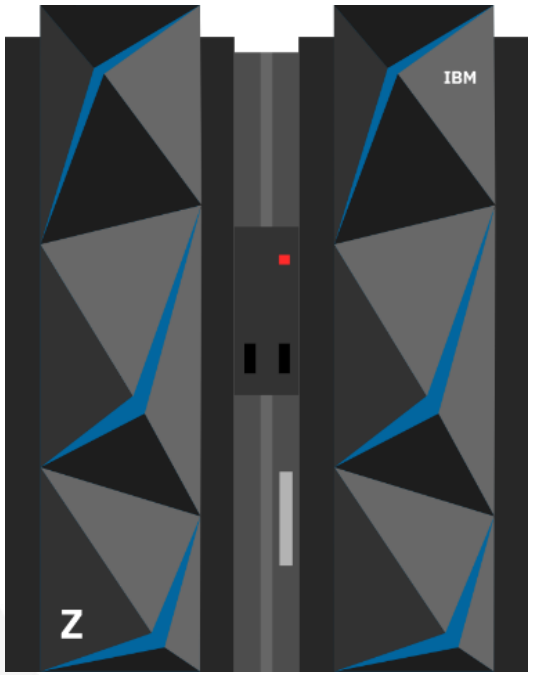
GDPS https://www.ibm.com/products/gdps

IBM Z https://www.ibm.com/z

IBM Z Resiliency https://www.ibm.com/z/resiliency

Storage https://www.ibm.com/storage

Redbook – GDPS Family: An Introduction to Concepts and Capabilities
http://www.redbooks.ibm.com/abstracts/sg246374.html?Open



- GDPS Web site resources

GDPS: The Enterprise Continuous Availability / Disaster Recovery Solution white paper

GDPS pre-requisite information

GDPS training schedule links

GDPS hardware qualification letters

E-mail: gdps@us.ibm.com

Experience more with IBM

Visit us at the IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at **Think 2026**.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation