

IDUG

2026

Sydney | March 16 - 18

AU Db2 TECH CONFERENCE

Db2, IDAA and Safeguarded Copy:
Resiliency Evolution and Integration

Anthony Ciabattoni, IBM

Cuneyt Mehmet, IBM

Session Code: A06

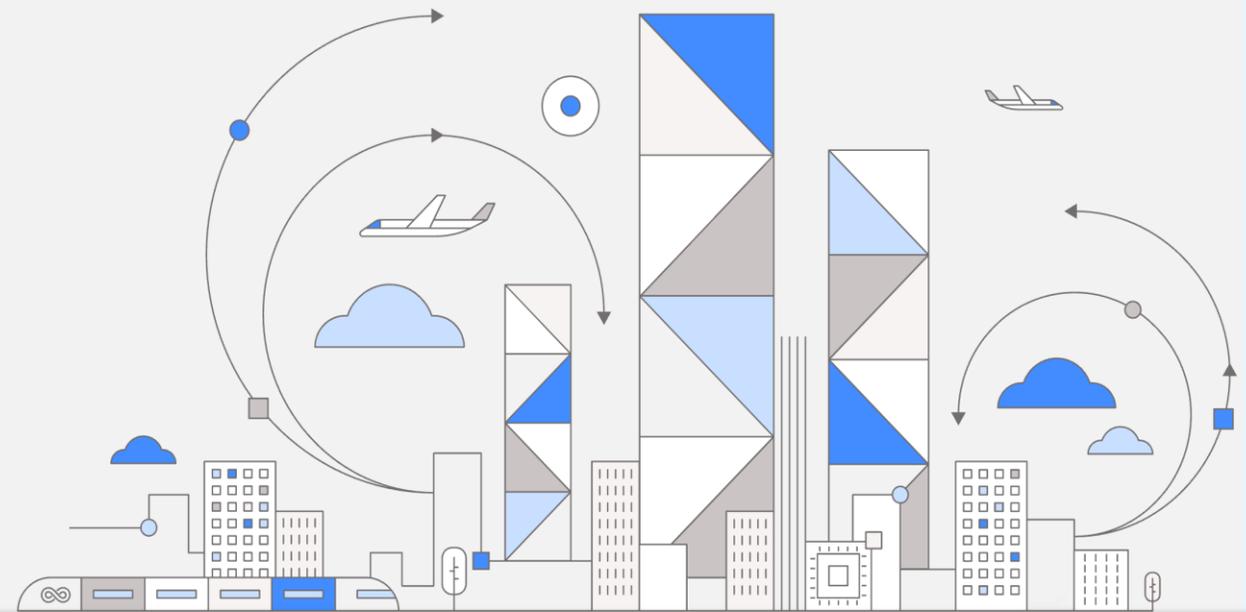


Platform:

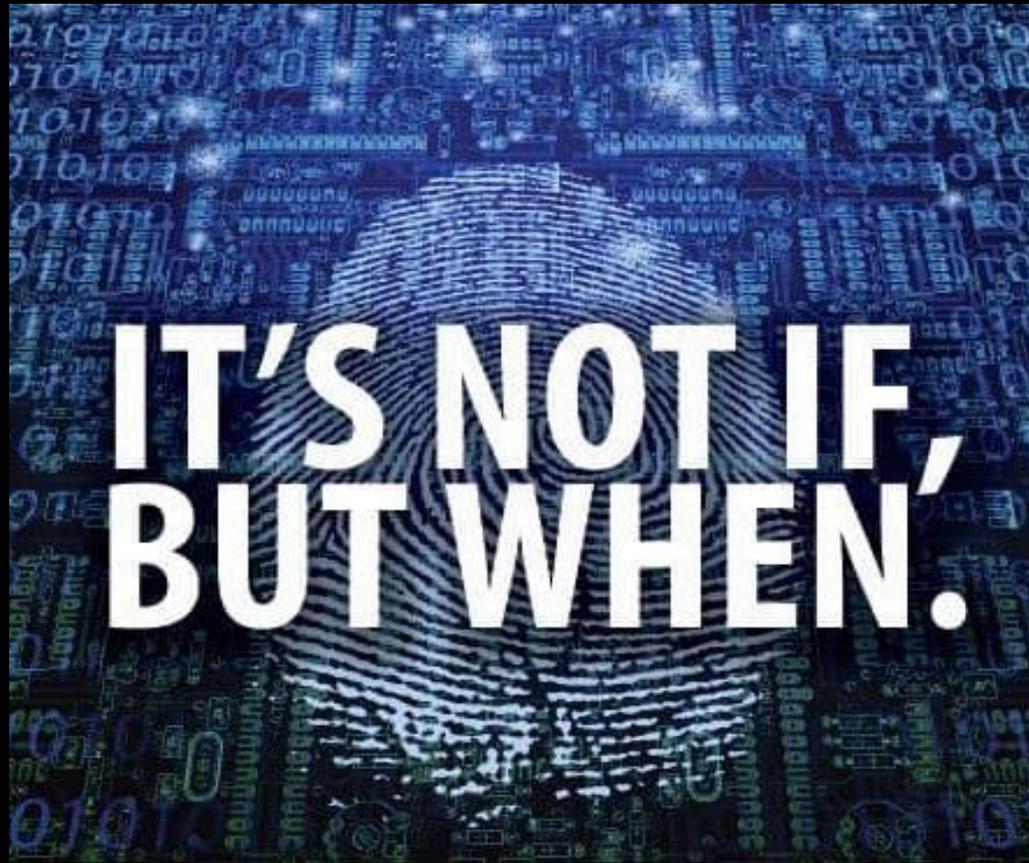
Db2 for z/OS

Agenda

- Cyber Resiliency
- Cyber Vault and Safeguarded Copies
- Db2 Recovery Options
- Additional use cases
- Questions



Guaranteed 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

Ransomware is in the news

Within weeks in September 2023, two of the world's largest casino-hotel companies, MGM Resorts and Caesars, were hit with ransomware attacks

- Caesars met the hacker's demands
- MGM Resort elected to resist

Casino giant MGM expects \$100+ million hit from the hack that led to the data breach

Caesars paid \$15 million in ransom to cybercrime group prior to MGM attack



Ransomware is in the news ...

A third of Americans could have had data stolen in big health care hack



Witty told the committee that cybercriminals accessed Change Healthcare through *a server that was not protected by multi-factor authentication, or MFA, which requires users to verify their identity in at least two different ways.* He said UnitedHealth now has MFA in place across all external-facing systems.

CNN — A third of Americans may have had their personal data swept up in a February ransomware attack on a UnitedHealth Group subsidiary that disrupted pharmacies across the US, UnitedHealth CEO Andrew Witty estimated in testimony to Congress on Wednesday.

It will likely take “several months” before UnitedHealth is able to identify and notify Americans impacted by the hack because the company is still combing through the stolen data, Witty said in written testimony.

In hours of hearings in the Senate and House Wednesday, Witty apologized to patients and doctors, admitted that hackers broke into the subsidiary through a *poorly protected computer server and confirmed that he authorized a \$22 million ransom payment to the hackers.*

Before the Boom

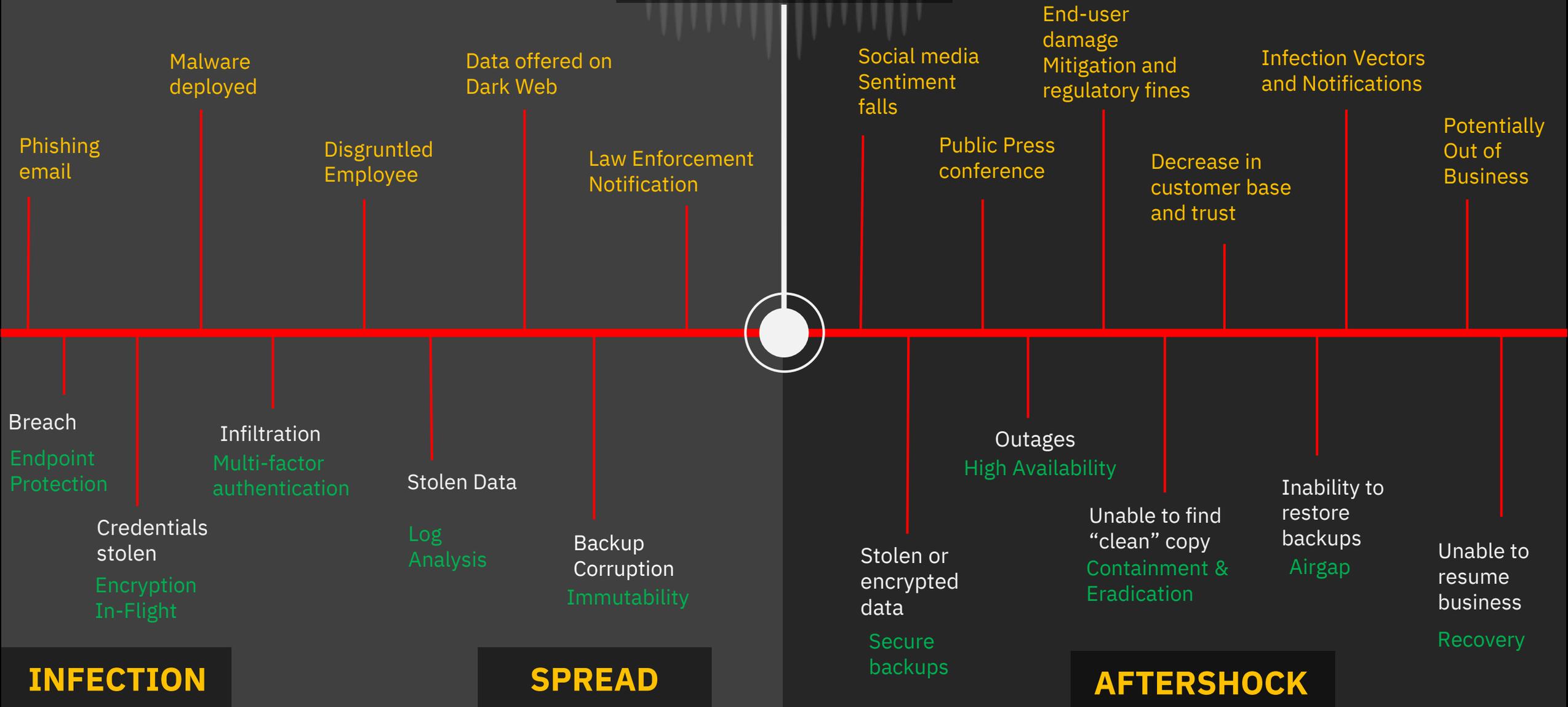
Threat Prevention

After the Boom

Crisis Response

BOOM

Public Notification



INFECTION

SPREAD

AFTERSHOCK

\$4.88M

Average total cost of a breach

\$4.81M

Average cost of a breach when attackers used compromised credentials, which happen in 16% of the breach cases studied

292

Days to identify and contain breaches involving stolen credentials



26.2%

Growth of the cyber skills shortage

\$4.99M

Average cost of a malicious insider attack

46%

Share of breaches involving customer personal data

Data Resilience

Why Act Now?



Cyber Security and Cyber Resilience

Cyber Security

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

Cyber Resilience

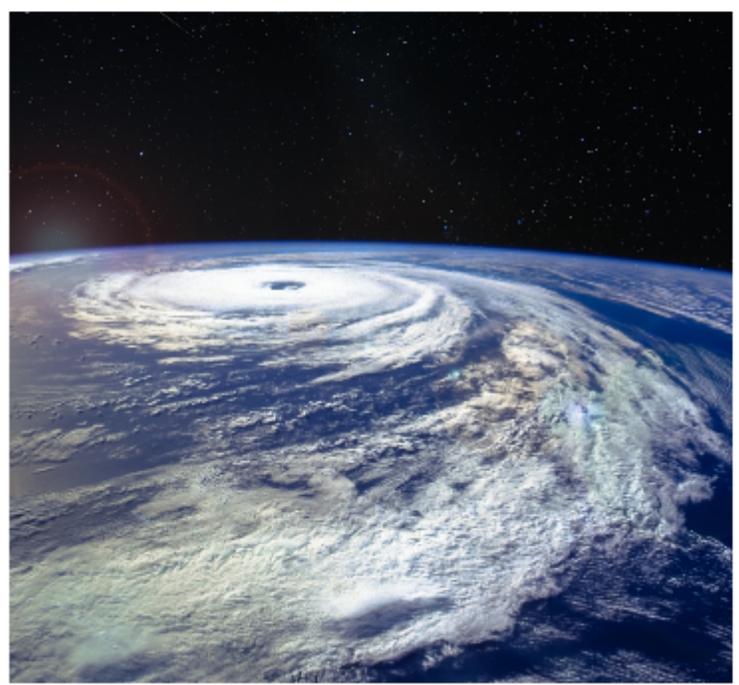
Cyber resilience is about an organizations ability to continue operations and rapidly recover despite a cyber-incident

Organizations need to be both cyber secure and cyber resilient



Cyber Security and Cyber Resilience ...

Traditional resiliency solutions will not protect you from cyber attack

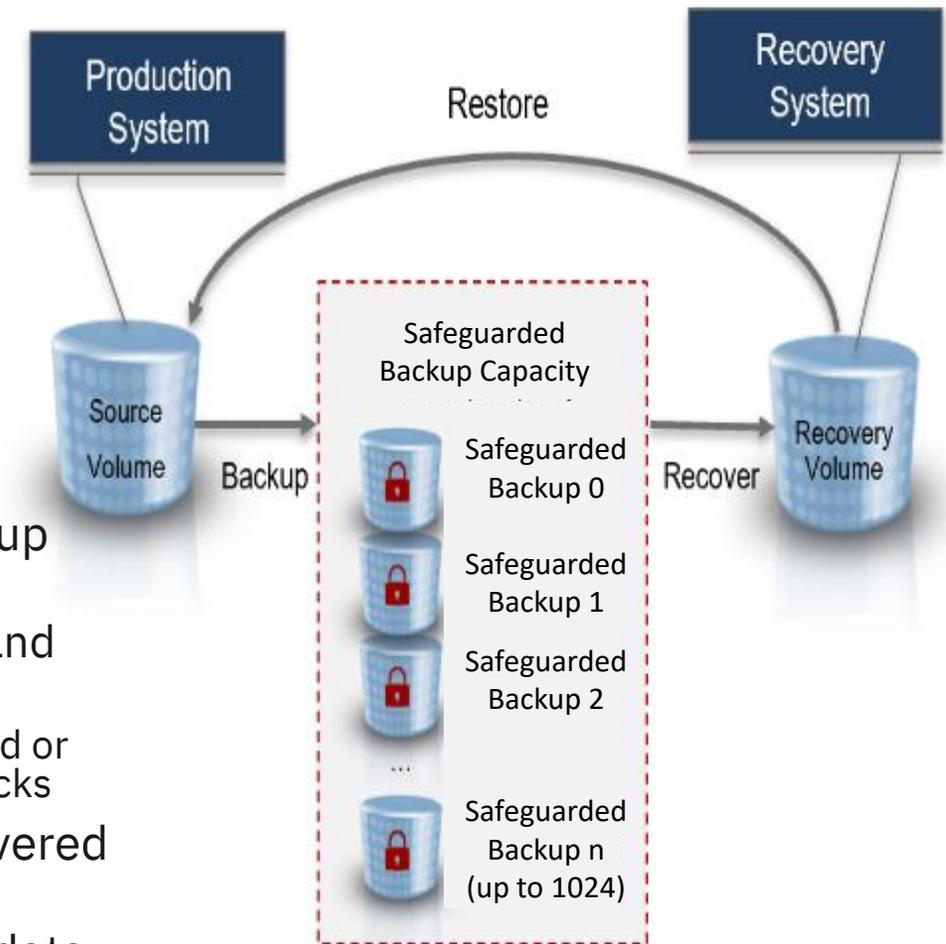


	Traditional resiliency	What is required
Replication	Data is being replicated continuously but logical errors are also replicated instantaneously	Scheduled point in time copies stored in an isolated, secure location
Error detection	Immediate detection of system and application outages	Regular data analytics 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

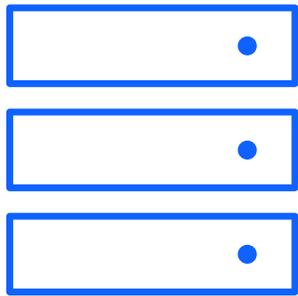


DS8K Series Safeguarded Copy

- 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
 - Provides functionality to create up to 1024 Safeguarded Backups for a source volume
 - Source devices are where the production copies are taken from
 - Production source devices
 - HA/DR copy using data replication
 - They are stored in a storage space that is called Safeguarded Backup Capacity which is hidden and not accessible by any server
 - Protection devices provide one or more logical protection copies and are not accessible by any system
 - Additional security measures aim to protect these from being modified or deleted due to user errors, malicious destruction or ransomware attacks
 - The data can only be accessed after a Safeguarded Backup is recovered to a separate recovery volume
 - Recovery volumes can be used with a recovery system to perform data validation, forensic analysis or to restore production data. It is also possible to restart the production systems directly on the Recovery Volume



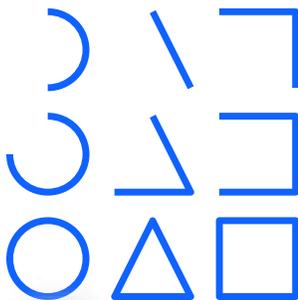
IBM Z Cyber Vault



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



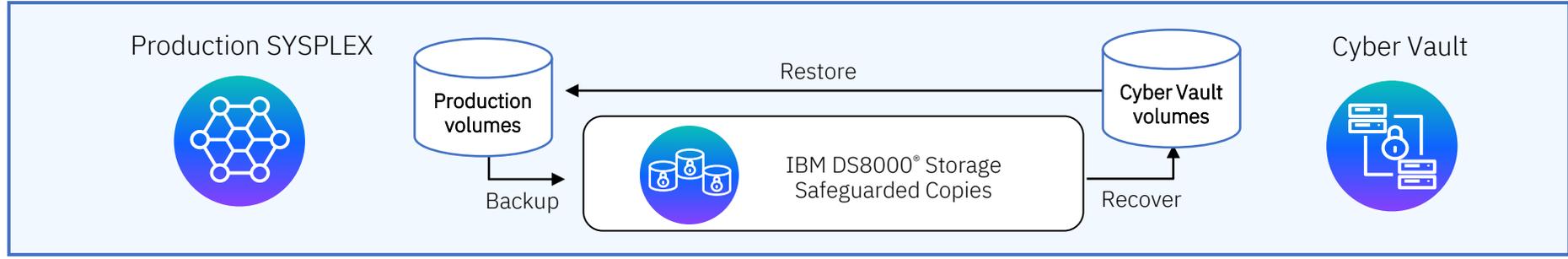
- ✓ IBM Z Cyber Vault **Automation**
 - GDPS Logical Corruption Protection (LCP) Manager
 - IBM Technology Expert Labs Cyber Vault data validation services asset



- ✓ IBM Z Cyber Vault **Environment**
 - IBM Z Hardware including CPs, zIIPs, ICF, memory and required infrastructure
 - IBM Z Cyber Vault Environment pid for SW licensing
 - IBM Z Software Tools including, IZBR, Db2 Recovery Expert, Db2 Tools, etc.



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

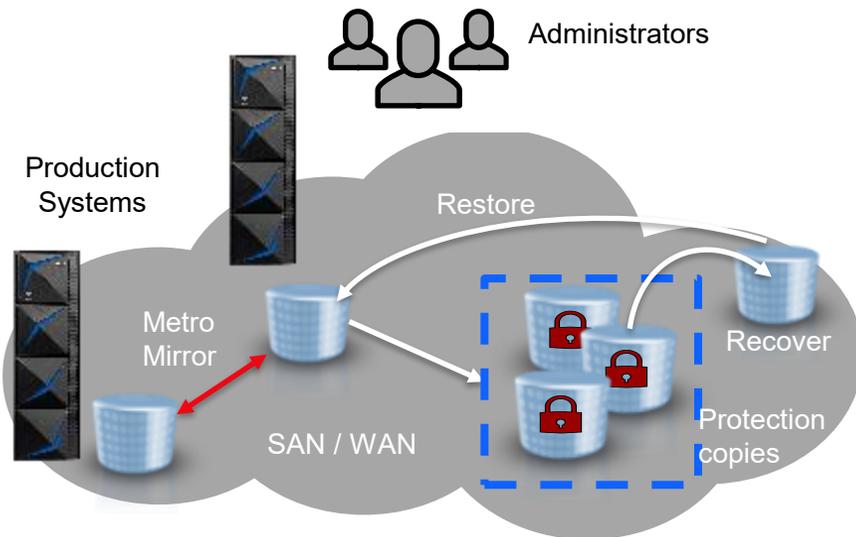
IBM DFSMSHsm™ tools

Db2® and IMS™ Tools



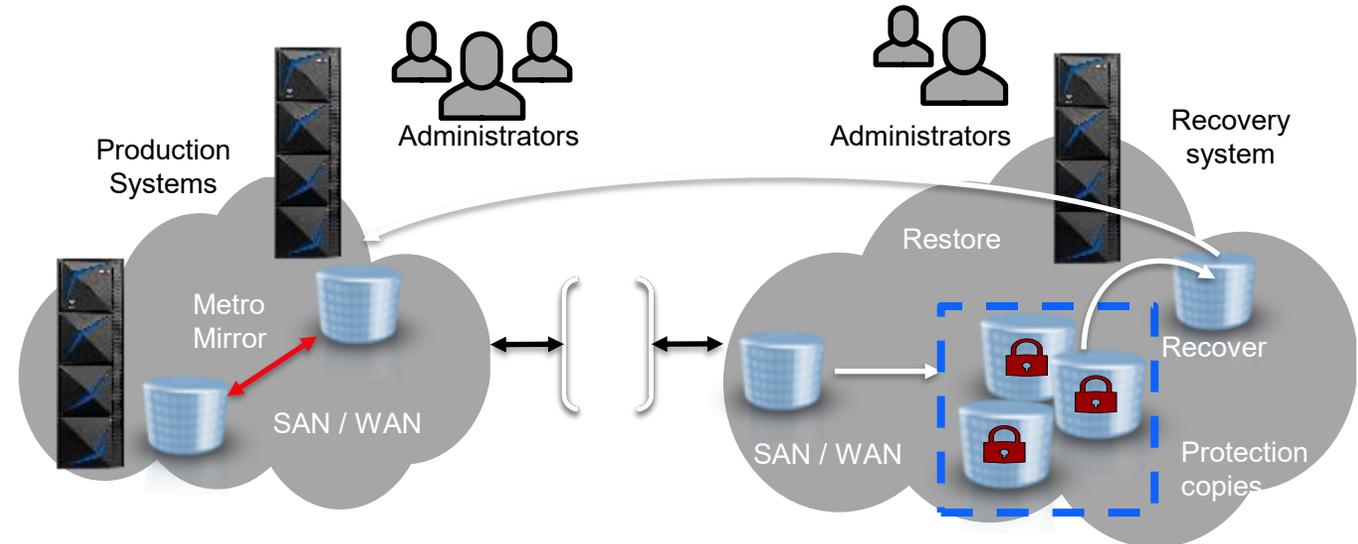
Air gap: Virtual and physical isolation of protection copies

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



TS7700 Security and Air gap Summary



Auditing & Compliancy

- Flash Copy DR Testing
- Event & Task logging (MI/SNMP)
- Rsyslog tamperproof logging
- Upload SSL Certificates or use default
- SP800-131a Compliancy Settings

Management Interface Security

- Granular Roles & Permissions
- Local or LDAP Login
- Dual Control Sensitive Settings



- HTTPS

Secure Data Transfer (AES256)

- DS8K to TS7700 TCT Objects
- Copies between TS7700s
- Exports to cloud storage devices



IBM z/OS

FICON



DS8000

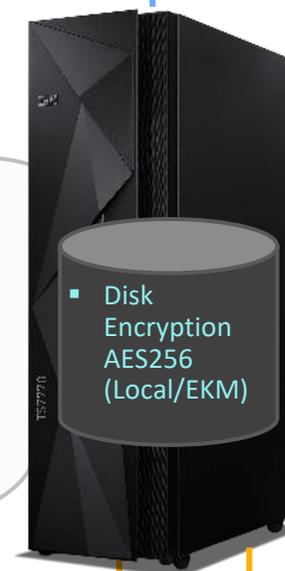
GRID

- TS7700 Grid technology to store multiple copies of data anywhere in the world (up to 8 clusters)
- Fast migrate/recall at disk speeds
- Active/Active...
- Each cluster is an access point



- Disk Encryption AES256 (Local/EKM)

TS7700 Grid



- Disk Encryption AES256 (Local/EKM)

Physical Tape Tier

- Tape Encryption AES256 (EKM)
- Copy Export Secondary Copy
- Copy Export Offsite Airgap
- Copy Export Recovery
- Copy Export Recovery Testing

TS4500



Object Store

Ethernet

Virtual Tape

Fibre Channel

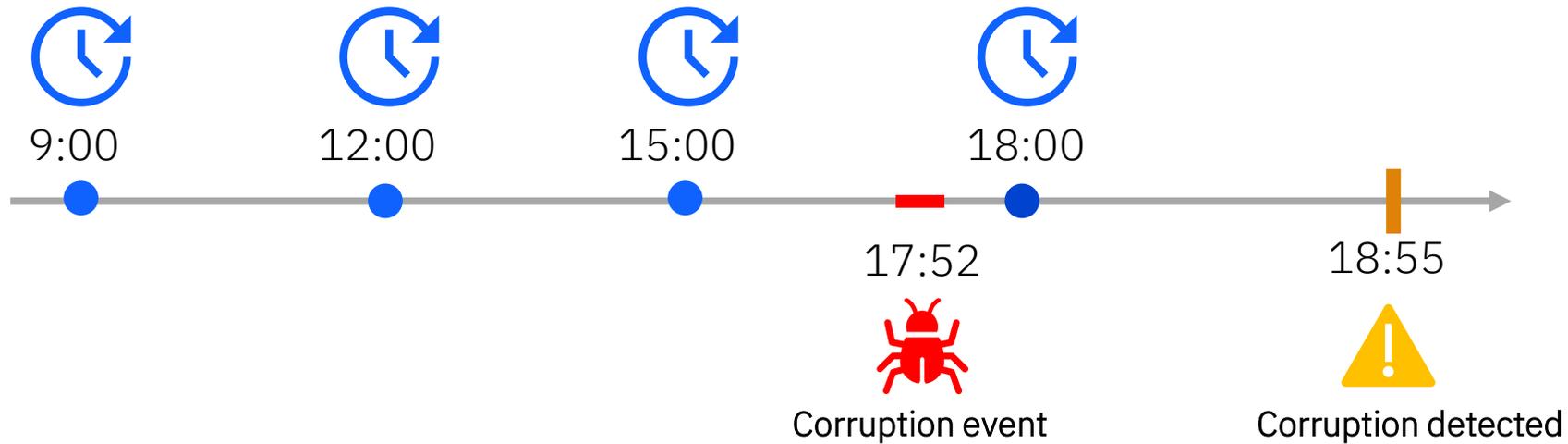
Physical Tape

Extended Retention and Access

- Selective Device Access Control (SDAC)
- Category Retention w/Expire Hold
- LWORM
- LWORM Retention

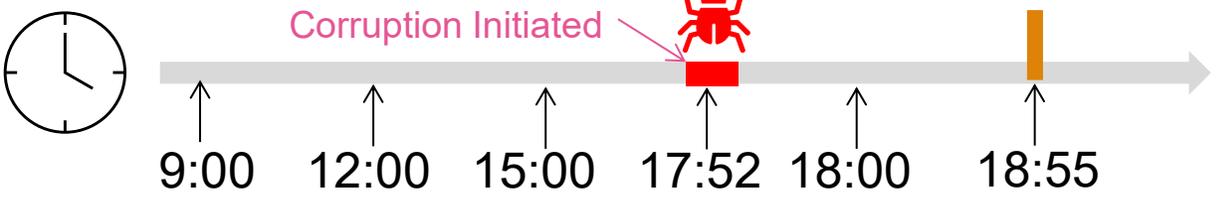
Recovery Point Objective (RPO)

Safeguarded Copy Frequency (3 hours)

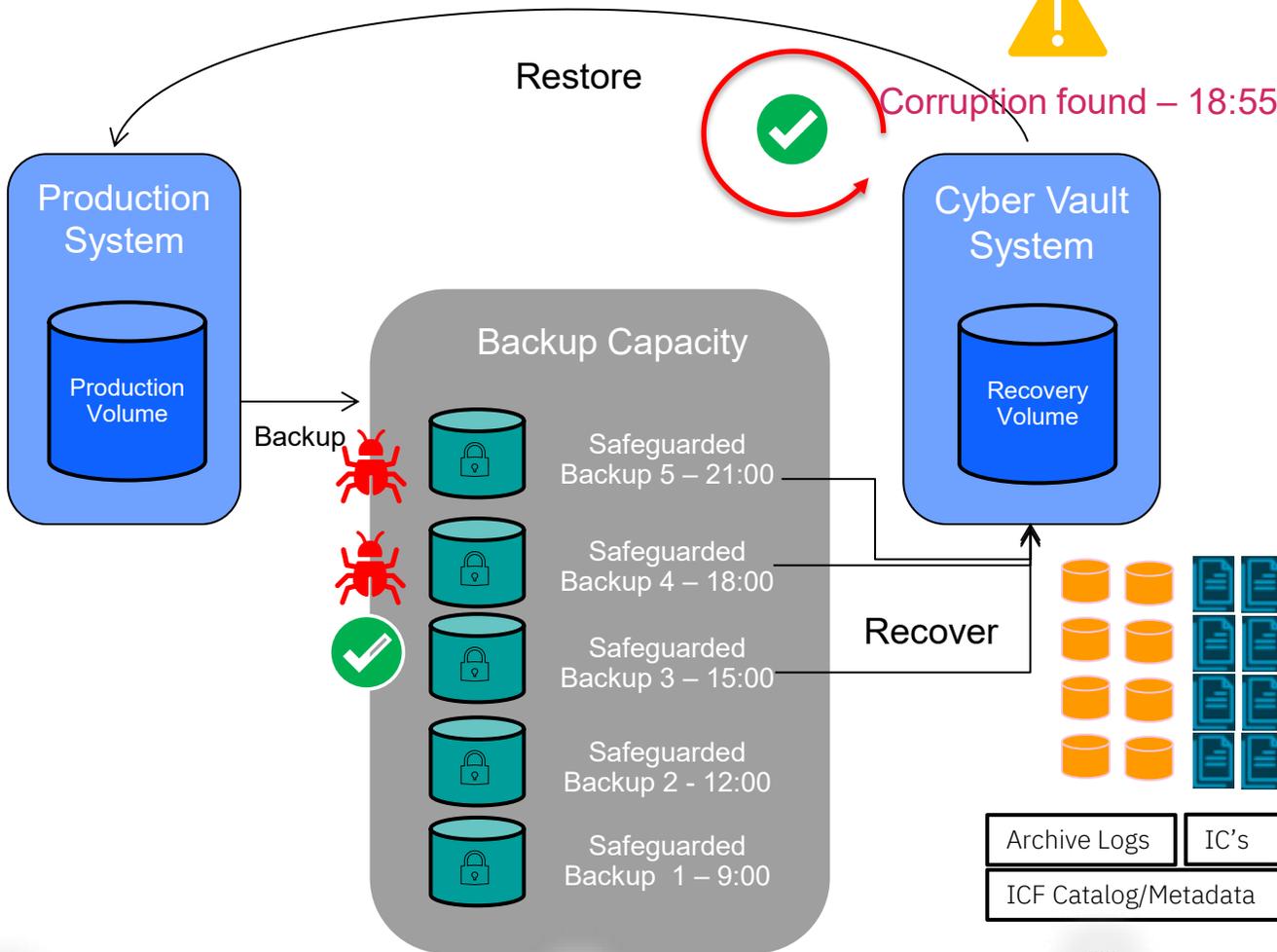


- Safeguarded Copy (SGC) is taken every 3 hours
- Corruption event initiated at 17:52
- Last good SGC prior to corruption was created at 15:00
- Corruption identified at 18:55 in the live production system
- Problem:
 - Last good SGC was taken at 15:00
 - Point-in-Time recovery would result in 2 hours and 52 minutes

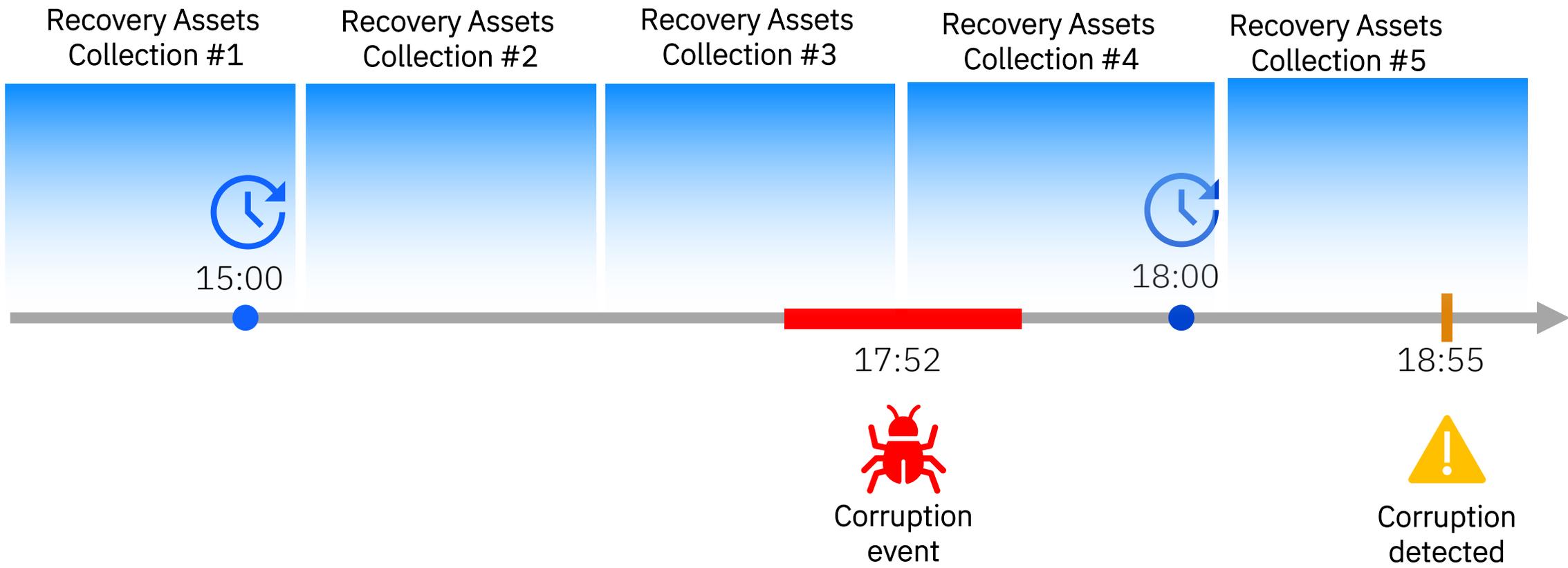
Recovery Point Objective (RPO) Roll Forward



- Additional Recovery Assets are required
 - Db2 archive logs
 - Db2 LOG NO Image Copies
 - ICF Catalog or Metadata
- Advantages
 - Minimize Db2 data loss
 - Use traditionally established reusable disaster recovery/group restart procedures (initial step)
- Operational opportunities
 - Additional procedures and processes
- Operational steps
 - The data is accessible only after a SafeGuarded Backup is recovered to a separate recovery volume IPL Cyber Vault Recovery LPARs
 - Db2 Group Restart
 - Roll forward
 - RESTORE LOGONLY
 - Data Validation



Recovery Point Objective (RPO)



Recovery Assets: Archive Logs, Image Copies, Metadata



Roll Forward Recovery

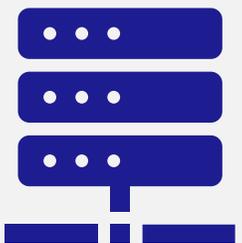
- Db2 13 Recovery Roll Forward
 - Db2 13 RESTORE SYSTEM LOGONLY
 - Recovery starting point and ending point must be established
 - Recovery starting point
 - Recovery Base Log Point (RBLP) continuously being incremented
 - Recovery ending point
 - SYSPITRT
 - SYSPITR
 - *Db2 13 provides additional RESTORE SYSTEM LOGONLY capabilities*
 - *RBLP is updated by Db2 every 5 minutes, starting point always incremented*
 - *RESTORE SYSTEM LOGONLY to point in time is now very appealing*
 - Db2 mass application object level recovery is technically an option but for large, active systems the recovery time will likely be significantly longer than restoring an entire system with one log apply event
 - Lack of planning, intelligent design, optimization and large-scale recovery testing
 - Not optimizing job scheduling based on object size, update rate, number and size of indexes all leading to elongated recovery time
 - Not efficiently using of Db2 Fast Log Apply (FLA)
 - No prioritized list of application objects and inter-dependencies



Resource collection

Production SYSPLEX

Recover technology started task



Archive logs



Image Copies



BSDS



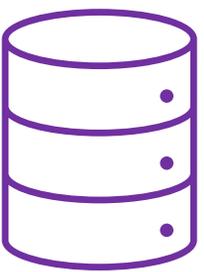
RE Metadata



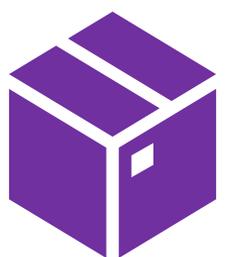
Immutable Storage



Cloud Storage



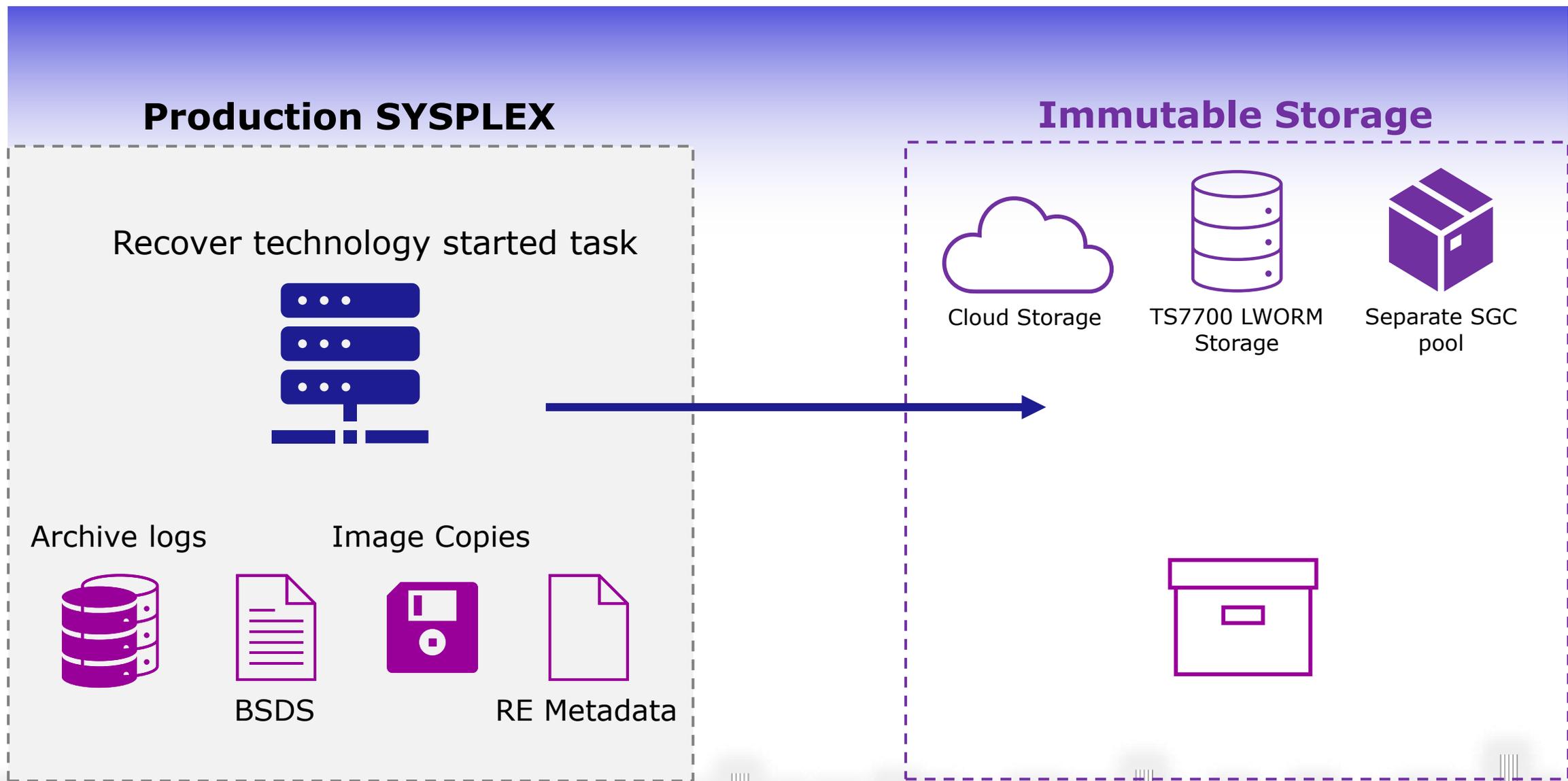
TS7700 LWORM Storage



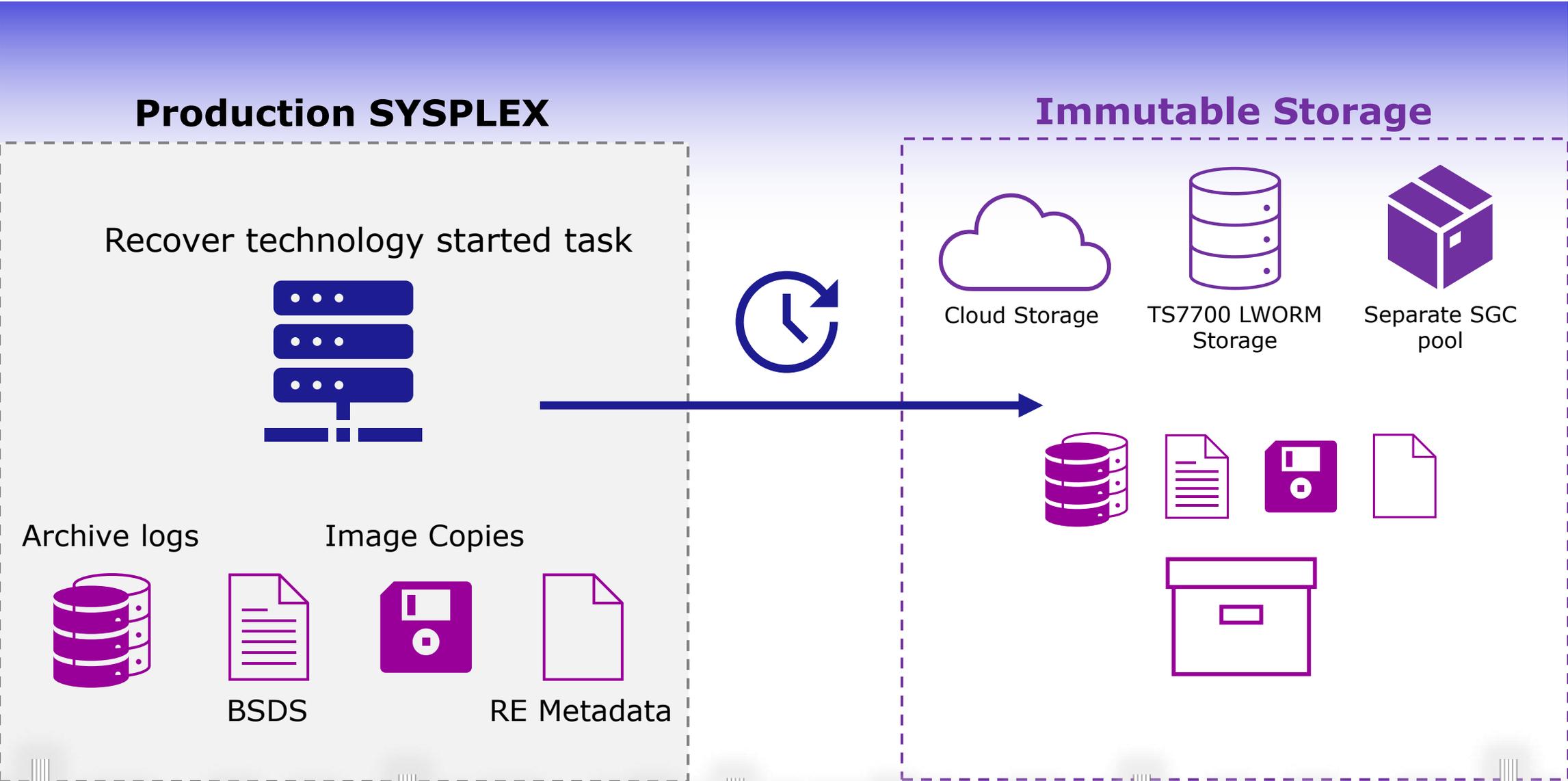
Separate SGC pool



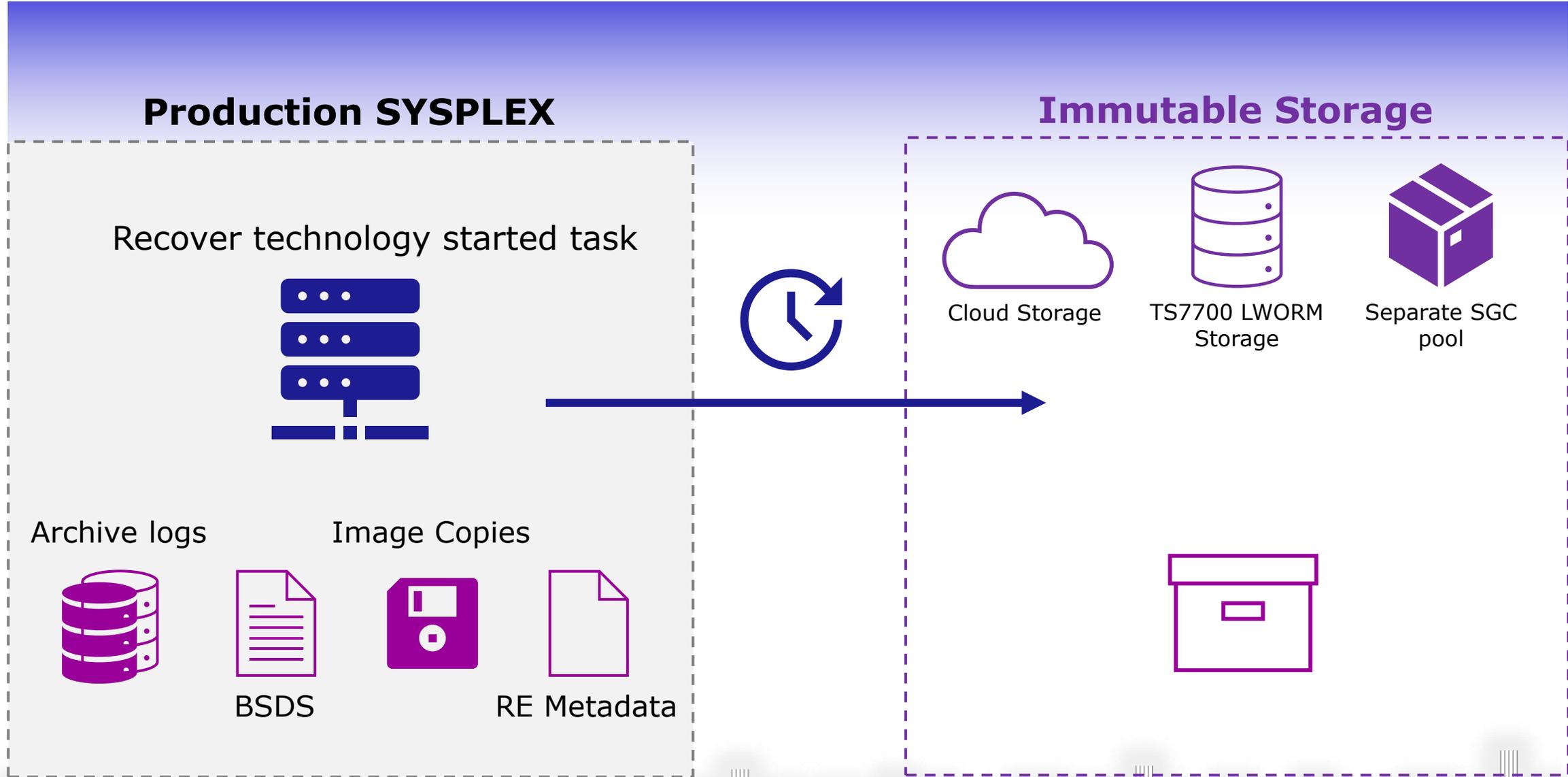
Resource collection



Resource collection



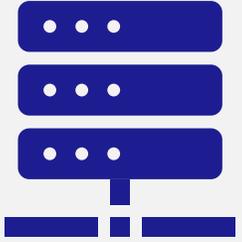
Resource collection



Resource collection

Production SYSPLEX

Recover technology started task



Archive logs



Image Copies



BSDS

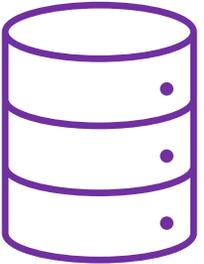


RE Metadata

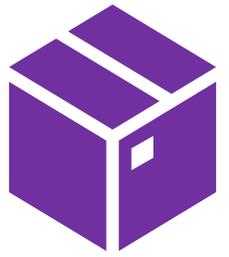
Immutable Storage



Cloud Storage



TS7700 LWORM Storage

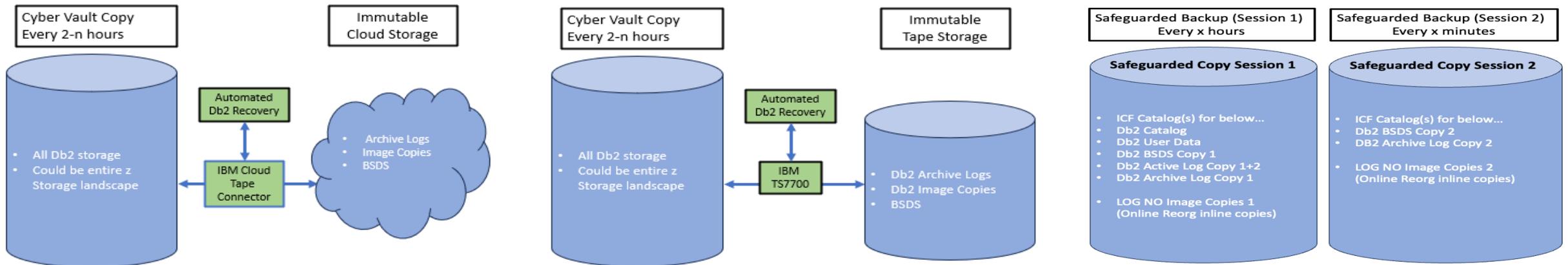


Separate SGC pool



Improve Recovery Point Objective (RPO)

- Write additional Db2 recovery assets to immutable storage at predefined intervals (in minutes) that is accessible to Cyber Vault Recovery LPAR(s)
 - IBM Cloud Tape Connector
 - IBM TS7700 with LWORM Retention
 - An additional Safeguarded Copy Session
- In the event of a cyber attack, user restores storage back to last good Cyber Vault copy
- Restore additional Db2 Archive Logs and LOG NO Image Copies from immutable cloud storage
- Conditions the Db2 environment and rolls forward Db2 to just before the cyber event



End-to-End Cyber Vault Recovery

✓ Preparation and recovery steps

Tower 1

Preparation at the production system

- ✓ Set archive log frequency based on asset collection interval
- ✓ Periodically save recovery assets to immutable storage that is accessible at the recovery system
 - ✓ Archive logs with BSDS
 - ✓ Image copies for table spaces and indexes after LOG NO events
 - ✓ ICF catalog information about the recovery assets

Tower 2

Preparation at the Cyber Vault recovery system after Safeguarded Copy is restored

- ✓ From immutable storage retrieve:
 - ✓ Archive logs, BSDS, and image copies that are more recent than the Safeguarded Copy that was restored.
- ✓ For each Db2 member:
 - ✓ Replace the BSDS with the most recent BSDS.
 - ✓ Run DSN1LOGP on most recent archive log data set.
- ✓ Identify SYSPITR system recovery point - lowest LRSN across the members from the DSN1LOGP output. This is the ending point for the roll forward (log apply).
- ✓ Allow user to override SYSPITR system recovery point

Tower 3

Recovery roll forward at the Cyber Vault recovery system

- ✓ Conditional restart process with SYSPITR
- ✓ Run RESTORE SYSTEM LOGONLY
- ✓ Stop and start Db2
- ✓ Terminate any outstanding utilities
- ✓ Run RECOVER utility on table spaces and indexes in RECOVER-pending status
- ✓ Run REBUILD INDEX on indexes in REBUILD-pending status
- ✓ Validation of data



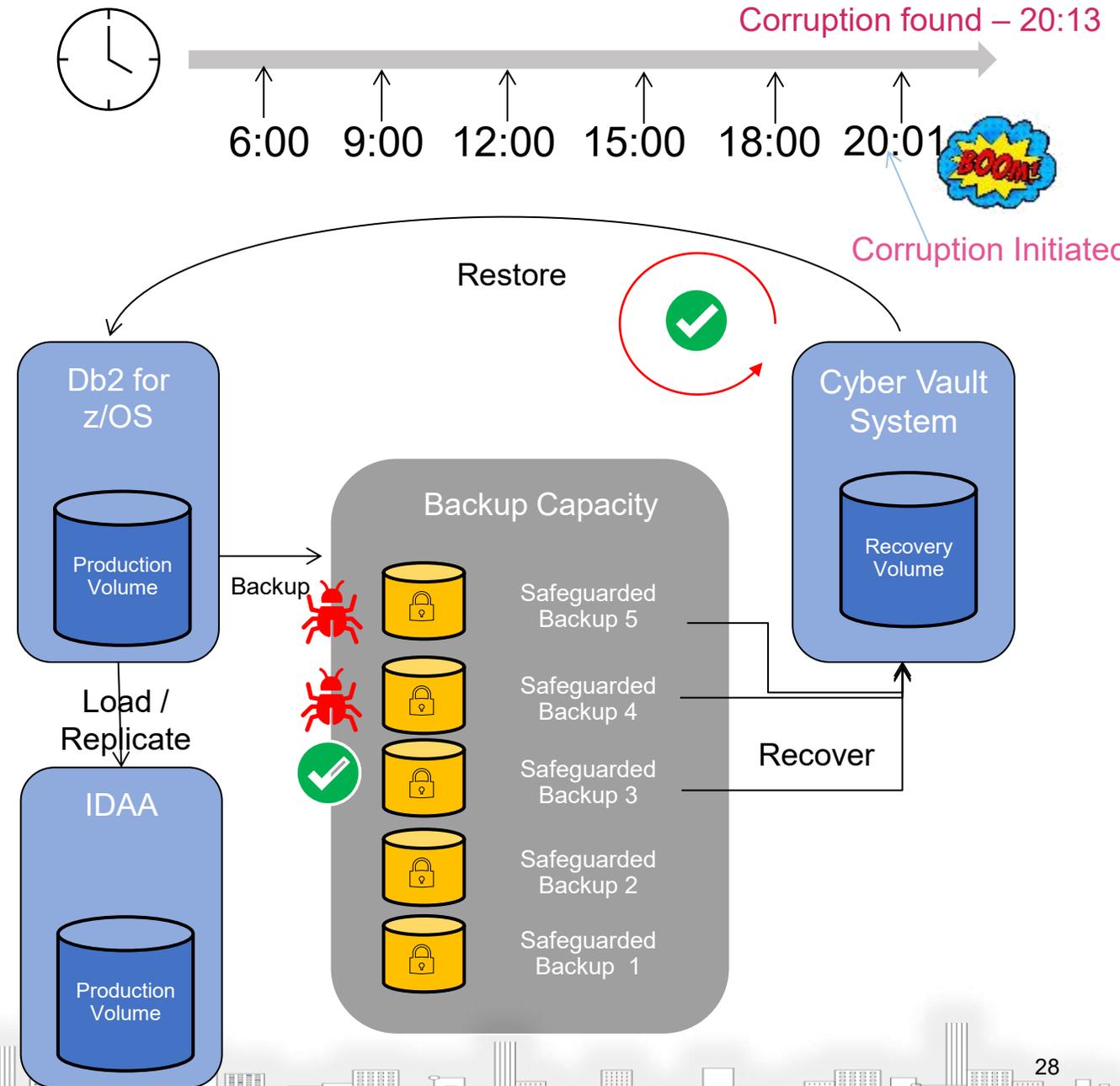
Recovery Point Objective Scenarios with IDAA

- IDAA Pre-Requisites for Safeguarded Copy (SGC)
 - IBM DS8K and GDPS is required
- 1. SGC with NO Roll Forward and IDAA
 - Db2 for z/OS uses DS8K
 - IDAA uses Fibre Channel Protocol (FCP) storage
- 2. SGC with NO Roll Forward and IDAA
 - Db2 for z/OS and IDAA uses DS8K
- 3. SGC with Roll Forward and IDAA
 - 3a - Db2 for z/OS and IDAA uses DS8K
 - 3b - Db2 for z/OS uses DS8K, IDAA uses FCP



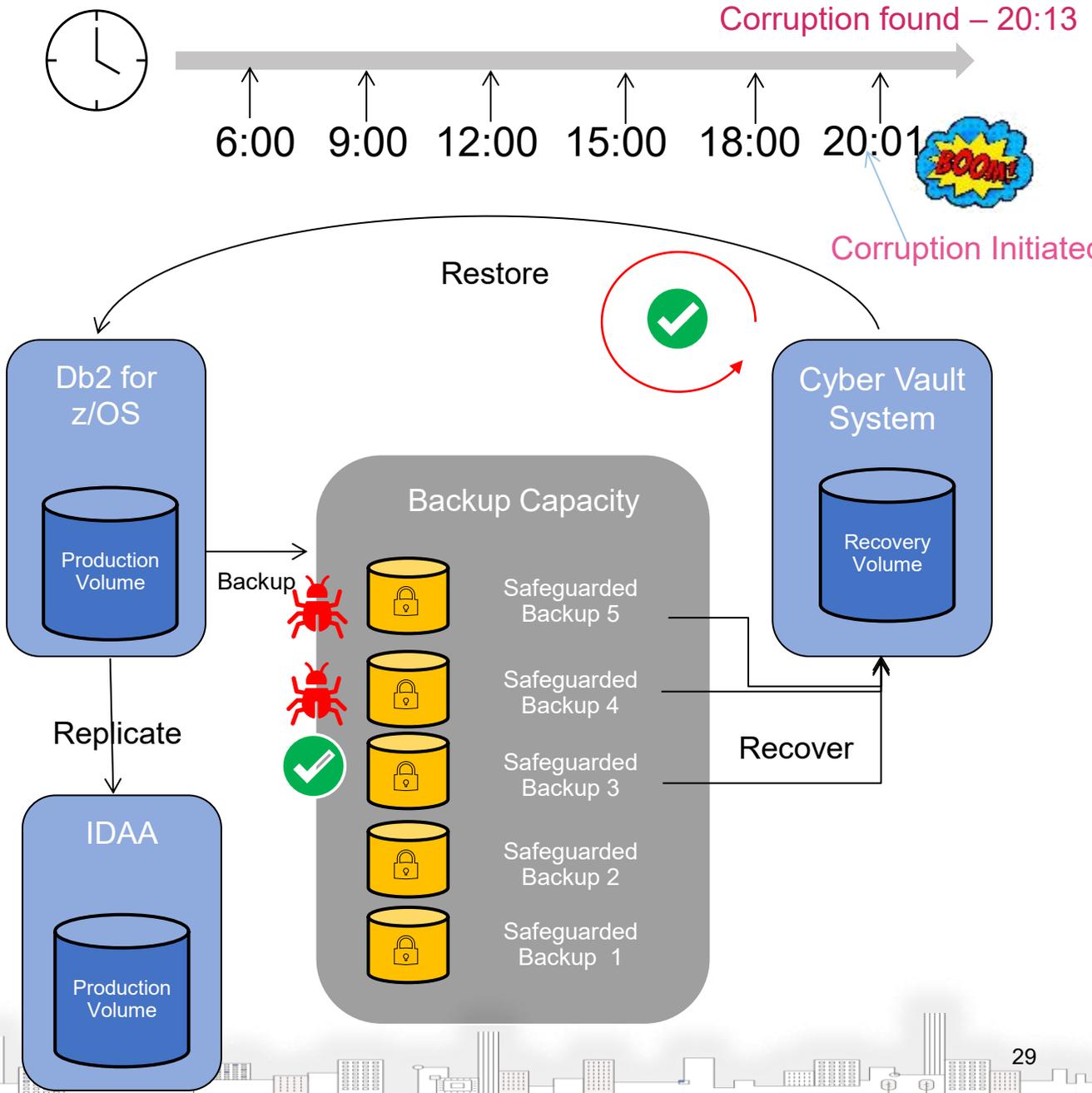
Recovery Point Objective (Scenario 1) (Db2 for z/OS uses DS8K, IDAA uses FCP)

1. Db2 for z/OS volumes will be recovered to Point in Time (PIT) with SGC such as 15:00
2. IDAA volumes will NOT be recovered with SGC since they are FCP
3. Data in IDAA will be more current than Db2 for z/OS
4. To make IDAA and Db2 synchronized
 - All the tables will be reloaded from Db2 for z/OS since the data in Db2 for z/OS is older than IDAA because of PIT Recovery
 - There is data loss for both in Db2 for z/OS and IDAA
 - Both recovered to PIT and synchronized



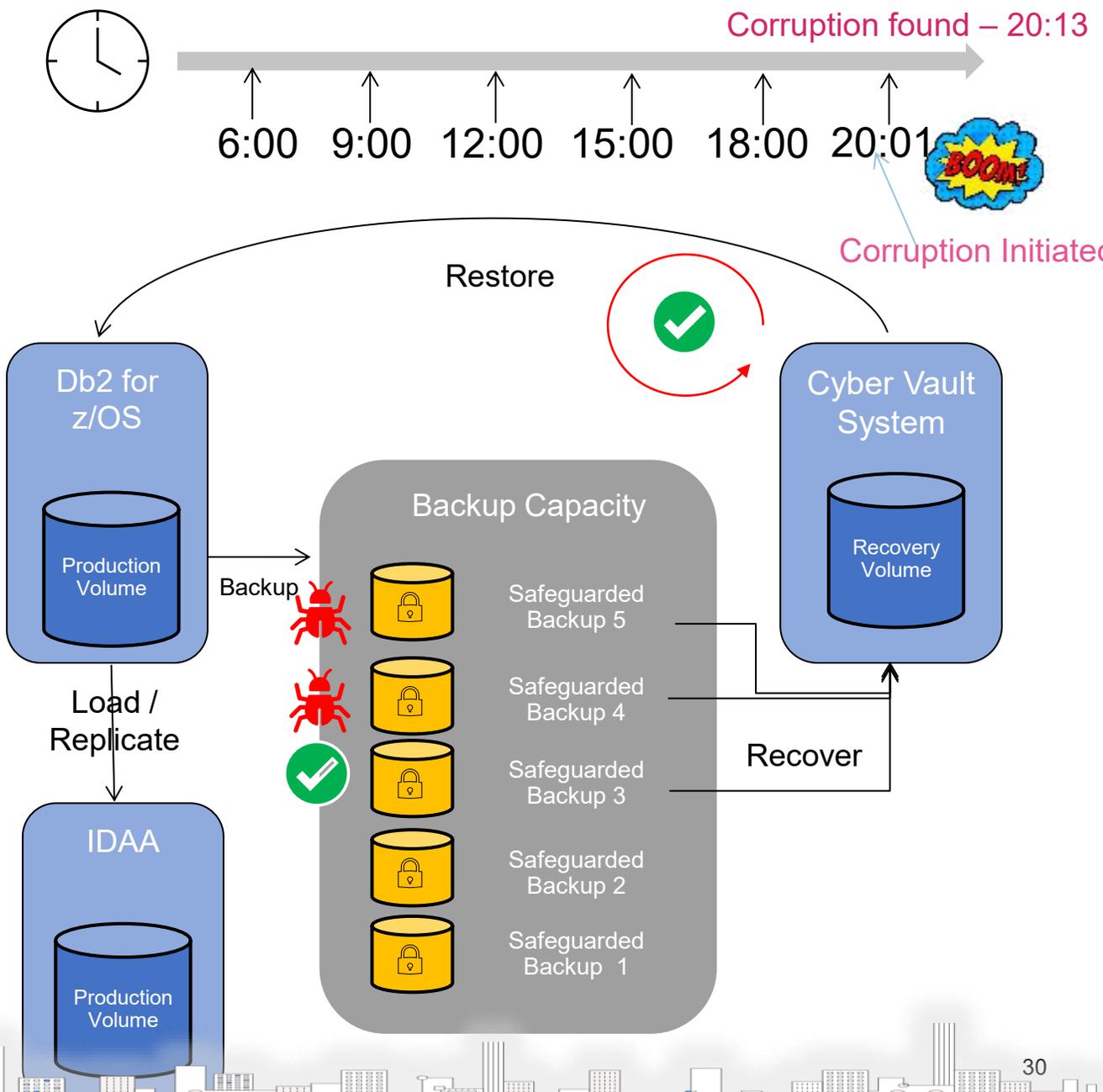
Recovery Point Objective (Scenario 2) (Db2 for z/OS and IDAA uses DS8K)

1. Db2 for z/OS and IDAA volumes will be recovered to PIT with SGC such as 15:00
2. Data in Db2 for z/OS and IDAA will be same to PIT
 - If there is no Integrated Synchronization, no action is required
 - If there is Integrated Synchronization
 - No action required for non-replicated tables
 - Enable Replication for the tables that are in Error status which will be reloaded and enabled for replication
- There is data loss both in Db2 for z/OS and IDAA
- Both recovered to PIT and synchronized



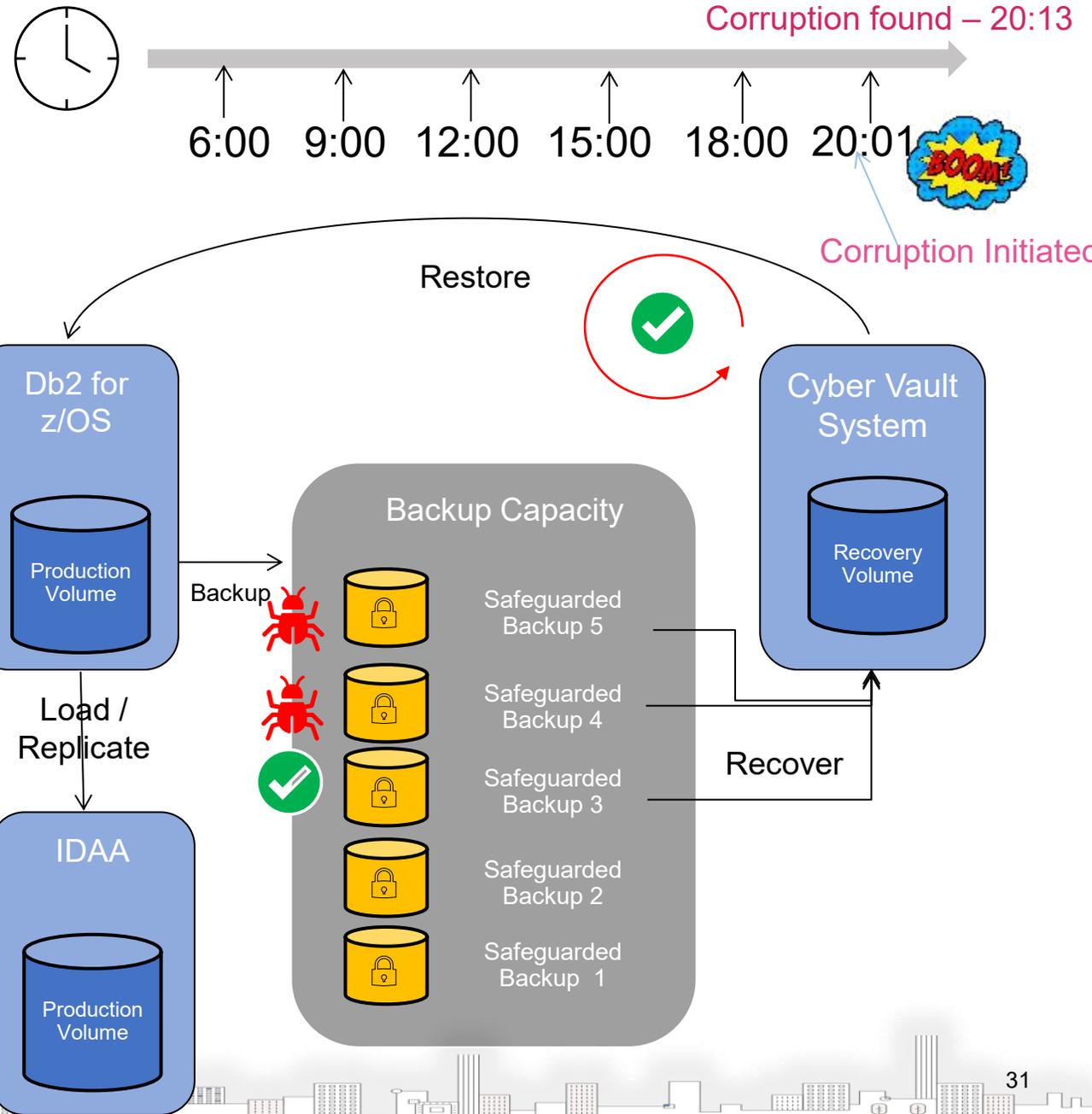
Recovery Point Objective (Scenario 3a) (Db2 for z/OS and IDAA uses DS8K)

1. Db2 for z/OS will be restored from SGC and forward recovered via logs such as 15:00
2. IDAA volumes will be recovered to PIT with SGC
 - If there is no Integrated Synchronization setup, Db2 for z/OS is more current than IDAA because of forward recovery, load tables from Db2 for z/OS to IDAA
 - If there is Integrated Synchronization setup
 - Db2 for z/OS is more current than IDAA because of forward recovery, load non- replicated tables from Db2 for z/OS to IDAA
 - Log Reader Task (Integrated Synchronization) will catch up and apply changes for replicated tables from the Db2 for z/OS log
- Minimum data loss both in Db2 for z/OS and IDAA
- Both recovered to the most current available log point

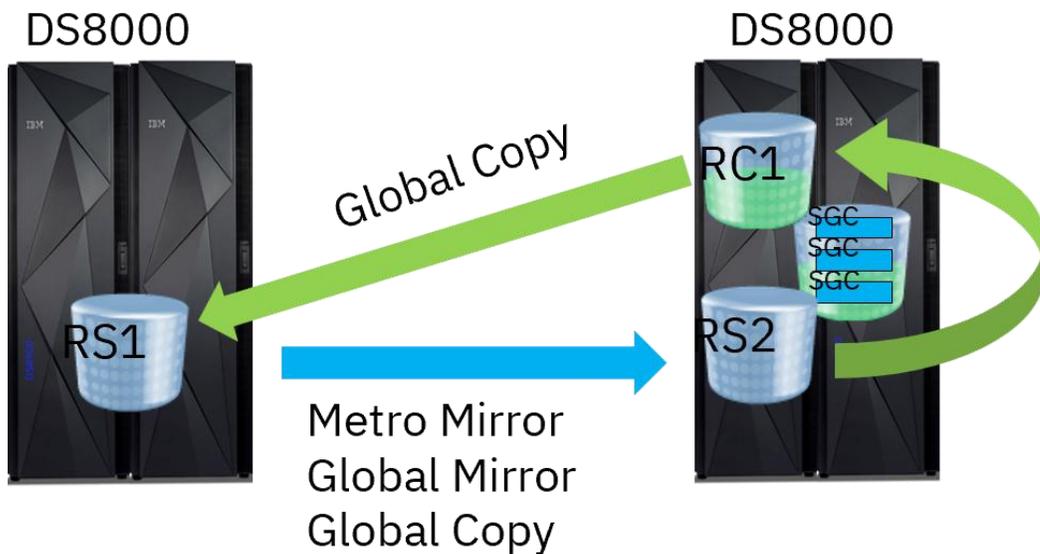


Recovery Point Objective (Scenario 3b) (Db2 for z/OS uses DS8K, IDAA uses FCP)

1. Db2 for z/OS will be restored from SGC and forward recovered via logs such as 15:00
 2. IDAA volumes will be NOT be recovered to PIT with SGC
 3. Data in IDAA will be more current then Db2 for z/OS
 4. To make IDAA and Db2 synchronized
 - All the tables will be reloaded from Db2 for z/OS since the data in Db2 for z/OS is older than IDAA because of PIT Recovery
- Minimum data loss both in Db2 for z/OS and IDAA
 - Both recovered to the most current available log point



Safeguarded Copy Restore to Production



- The majority of DS8000 users are replicating their data with Metro Mirror and/or Global Mirror
- It is possible to restore a recovered Safeguarded Copy back to a Production copy of data using an incremental copy of data
- 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
- It is possible to restart the recovered systems on the RC1 volumes while the copy process is happening. This would typically be done to validate that this is the correct copy and then perhaps for application people to prepare for the restart of the production applications

Continuous Data Validation

- Stay one step ahead with continuous automated data validation
 - Data validation is the process of executing regular analytics
 - Identify a data corruption event and scope of corruption
 - Determine the appropriate 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.



Forensic Analysis

- Back trace a cyber attack by forensic analysis
 - Determine:
 - What data is corrupted (scope)
 - When the data corruption occurred
 - Which available protection copies is the last good one
 - Based on this analysis (corruption scope), it can be determined how to proceed:
 - Fix the corruption from 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)

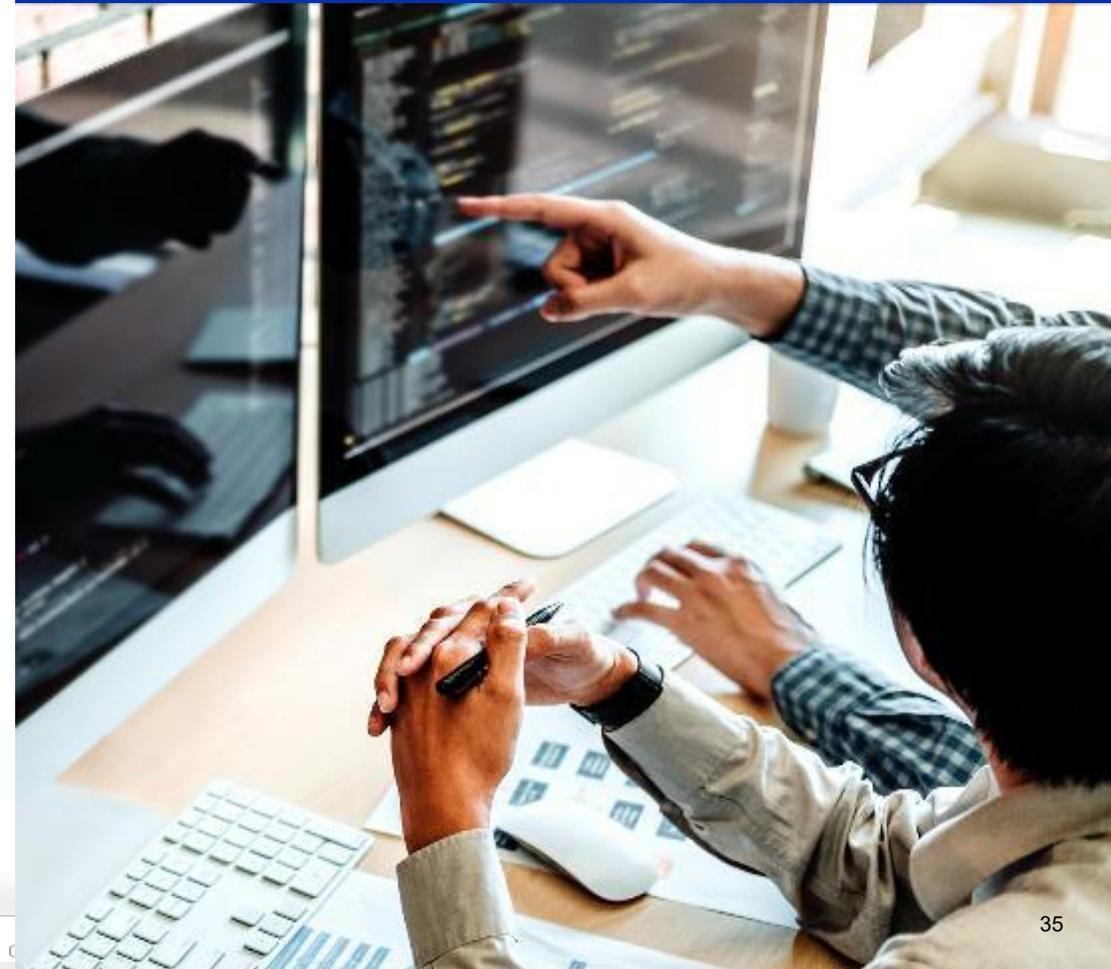
A forensic analysis identifies the cause and scope of a problem before deciding on a recovery action.



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 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
- Must be super confident about understanding application and data dependencies when recovering individual datasets and subset of datasets
- Solutions designed for recovering individual dataset, subset of datasets, whole system and building a “forensic” environment need to be tested, validated and regularly practiced to make sure they are in correct working order

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



IDUG

2026

Sydney | March 16 - 18

AU Db2 TECH CONFERENCE

Db2, IDAA and Safeguarded Copy:
Resiliency Evolution and Integration

Anthony Ciabattoni, IBM

Cuneyt Mehmet, IBM

Contacts: aciabattoni@ibm.com & mehmet.goksu@ibm.com

Session Code: A06



Platform:

Db2 for z/OS

Questions ...



Thank You

The image features the words "Thank You" in a bold, three-dimensional, metallic grey font. The text is positioned centrally and sits on a highly reflective, white surface that creates a clear mirror image of the letters below. The background is a light grey and white geometric pattern consisting of overlapping squares and triangles, some of which are semi-transparent, creating a layered, architectural effect. The lighting is soft and even, highlighting the 3D nature of the text.

An aerial view of Sydney, Australia, at dusk. The Sydney Harbour Bridge is prominent on the left, spanning the water. The city skyline is visible in the background with many skyscrapers lit up. In the foreground, there are many sailboats in the water and a theme park area with a Ferris wheel and roller coaster on the left. The sky is a mix of blue and orange from the setting sun.

IDUG

2026 Australia **Db2** Tech Conference