Elevate your Data Resiliency Framework

Orlando, Florida 2026
Session IBM_copy230

Glenn Wilcock
IBM z/OS DFSMS Chief Product Owner
wilcock@us.ibm.com

Notices and disclaimers

This document is distributed "as is" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

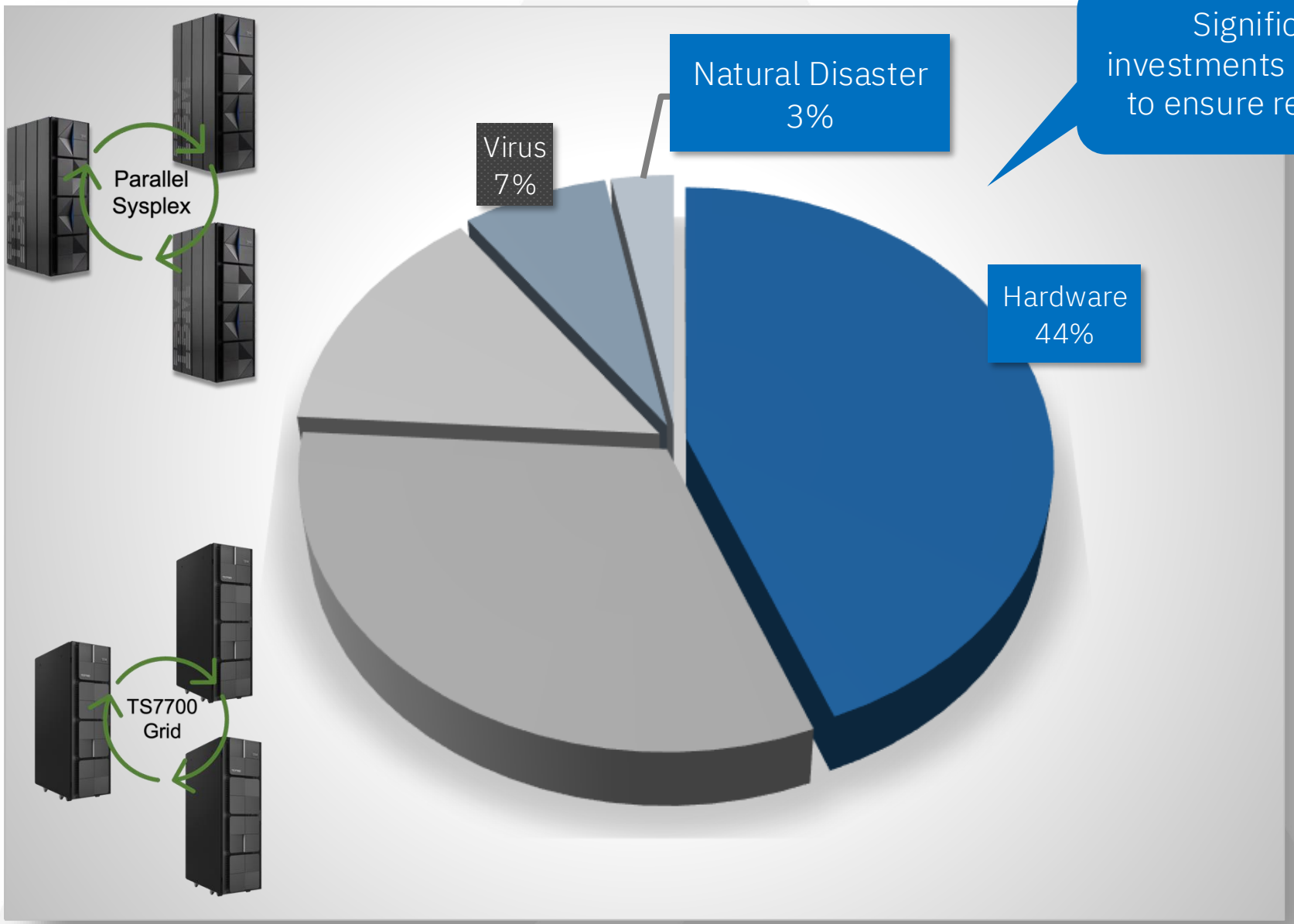
Certain comments made in this presentation may be characterized as forward looking under the Private Securities Litigation Reform Act of 1995.

Forward-looking statements are based on the company's current assumptions regarding future business and financial performance. Those statements by their nature address matters that are uncertain to different degrees and involve a number of factors that could cause actual results to differ materially. Additional information concerning these factors is contained in the Company's filings with the SEC.

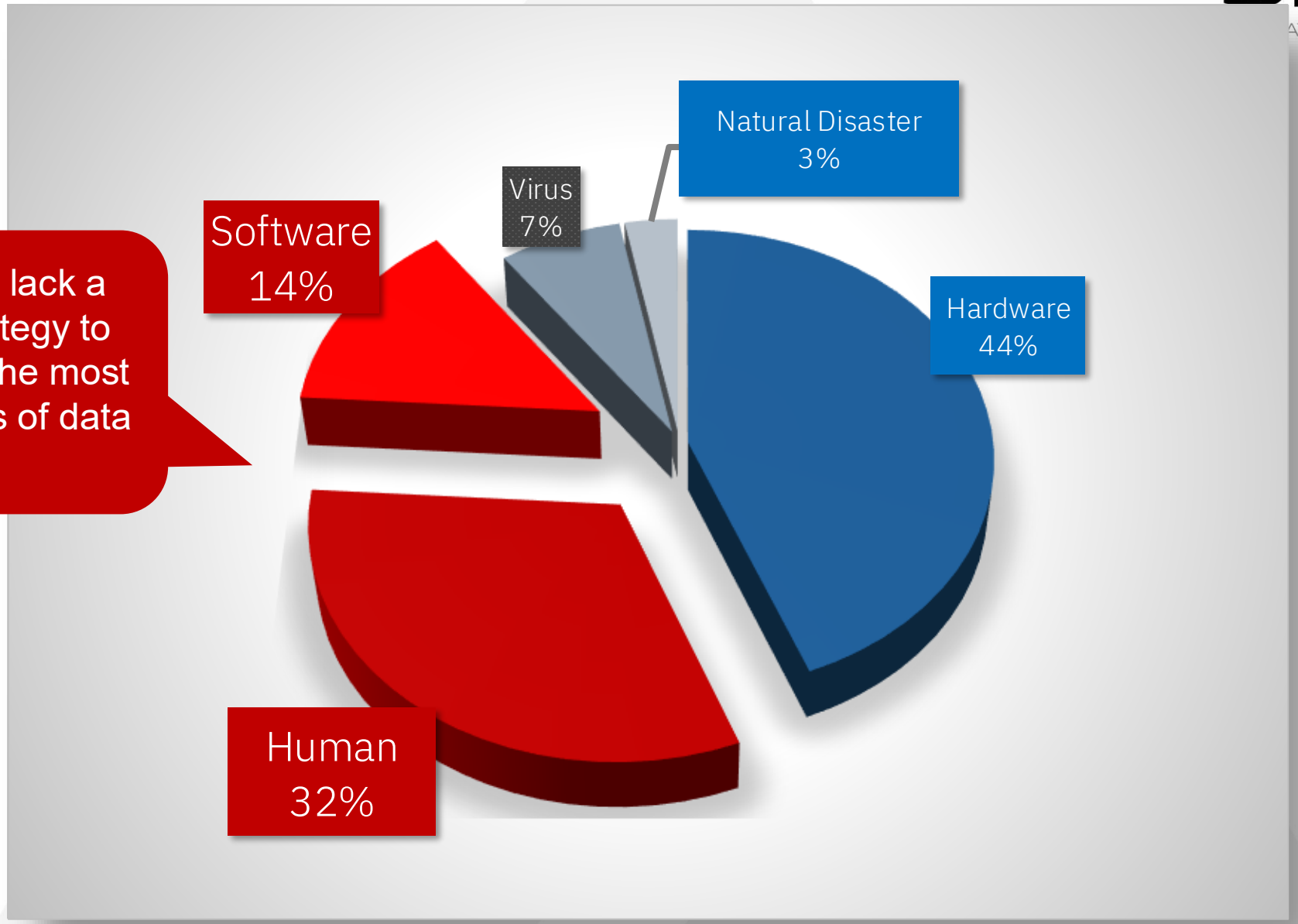
Copies are available from the SEC, from the IBM website, or from IBM Investor Relations.

Any forward-looking statement made during this presentation speaks only as of the date on which it is made. The company assumes no obligation to update or revise any forward-looking statements except as required by law; these charts and the associated remarks and comments are integrally related and are intended to be presented and understood together.

Industry Causes of Data Loss



Industry Causes of Data Loss



Many clients lack a wholistic strategy to recover from the most common types of data loss

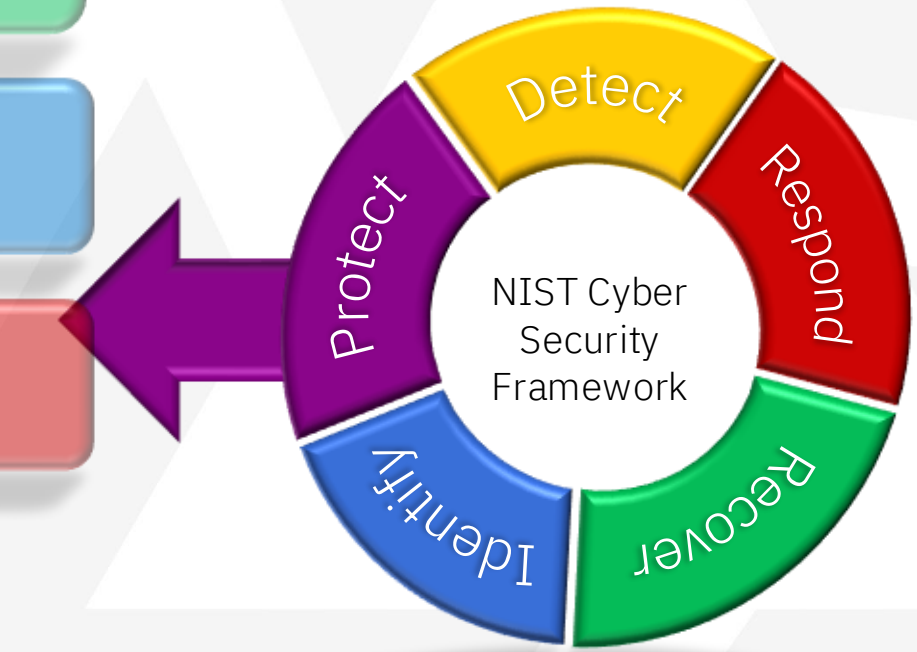
Zero Trust – It's not just for Data Protection!

Pervasive Encryption

Zero Trust Architecture: Least Privilege, Dual Controls, Immutability, etc

Trust but Verify: Multi-Factor

Trust: USERID / Password



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

Zero Trust Data Protection

Key Components

Zero Trust Security

- No user or device is assumed trusted and verification is enforced with every access
- Role-based, 2-person authentication

Encryption

- When data is exfiltrated, it is unusable

Immutable Storage

- Read Only data (such as backup and archive data) is guaranteed to be on unalterable storage and eventual access is guaranteed (e.g. WORM tape, Object Lock feature of object storage, DS8K Safeguarded Copy)

Air-Gapped

- Backup copies have logical or physical isolation from production environment to prevent malicious actors from altering or destroying

Key Benefits

Ransomware Resiliency

- Backup copies ensured to be unaltered and available for recovery without having to pay a ransom

Protection from Insider Threats

- Protects against malicious *or accidental* data corruption and destruction

Data Integrity and Compliance

- Immutable storage ensures data is unalterable, which is required for regulatory compliance

Zero Trust – It's not just for Data Protection!

Pervasive Encryption

IBM Threat Detection for z/OS

Ensure that your business can recover from user / software data loss / corruption!

Zero Trust Architecture:
Least Privilege, Dual Controls, Immutability, etc

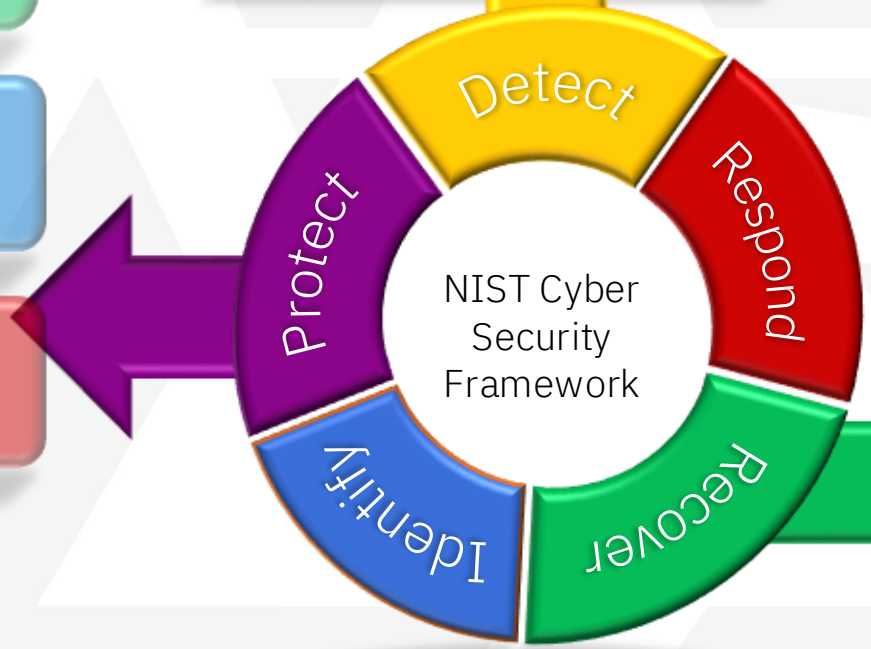
Zero Trust Architecture:
Safeguarded Copy / Cyber Vault and IZBR

Trust but Verify:
Multi-Factor

Trust but Verify:
IBM Z Backup Resiliency (IZBR)

Trust:
USERID / Password

Trust:
Each Application Owner Manages Backup Copies



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

Zero Trust Data Recovery

Key Components

Zero Trust Backups

- Backup copies are created at an enterprise level in addition to application driven creation
- *No application owner is assumed to be infallible at creating and maintaining backup copies*

Iterative, Changed Data Only, Immutable Backups

- Safeguarded Copy fundamentally changes how we backup and recover data sets
- *Grow the return on your safeguarded copy investment by extending scope to day-to-day recovery*

Single Source

- All available backup copies of all types are presented in a single dashboard

Key Benefits

Guaranteed Data Recovery

- Because backups are created at an enterprise level on immutable storage, there is a guarantee that all data may be recovered to some point in time

Compliance

- Demonstrating the ability to recover data is required for regulatory compliance

Gartner Predicts 2026

[1] Gartner “Predicts 2026: Cybersecurity Program Rebrands to Cyber Resilience”

SHARE
EDUCATE • NETWORK • INFLUENCE

What

“By 2028, half of CISOs will formally rebrand their cybersecurity program as cyber resiliency programs” [1]

Why

“Increasingly stringent regulations around cyber resilience are driving cybersecurity leaders to rapidly ramp up their capabilities after years of underinvestment” [1]

How

“Cybersecurity leaders must immediately realign their cybersecurity strategy to prioritize

- ✓ limiting business harm,
- ✓ minimizing operational impact,
- ✓ and ensuring continuity

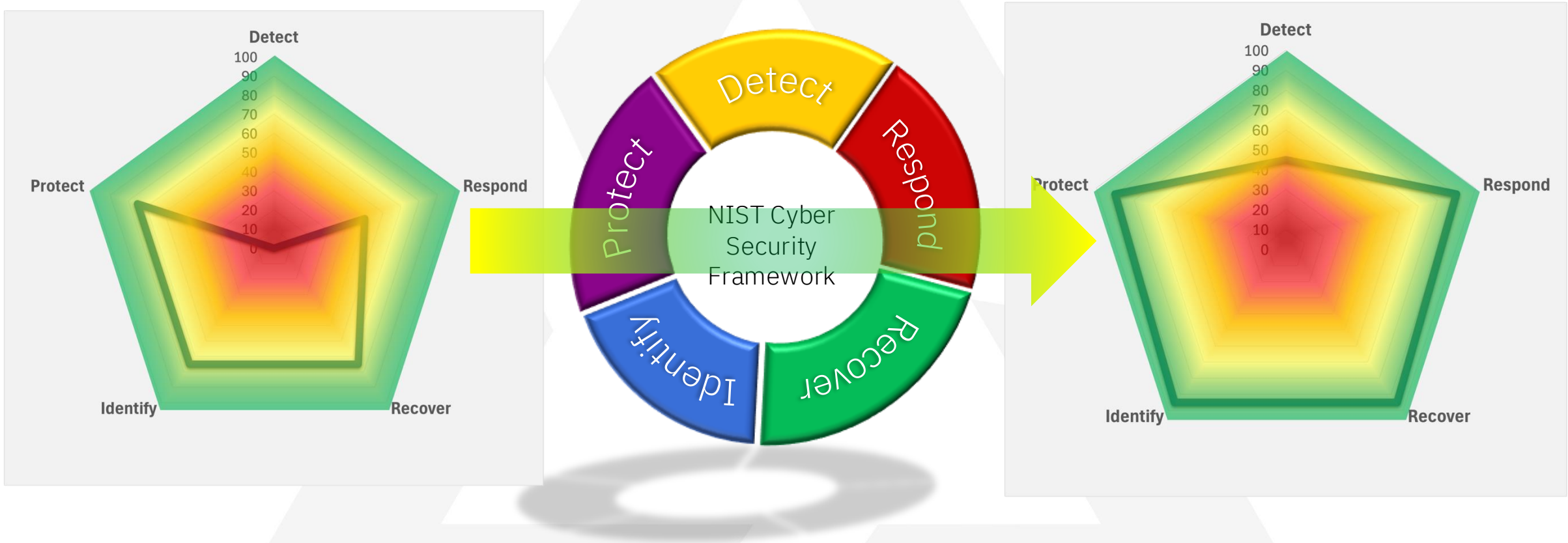
rather than pursuing the unattainable goal of total protection” [1]

Risk

“Failure to act will expose organizations to

- × regulatory penalties,
- × increased recovery costs,
- × and prolonged business disruptions” [1]

Elevate your Data Resiliency Framework



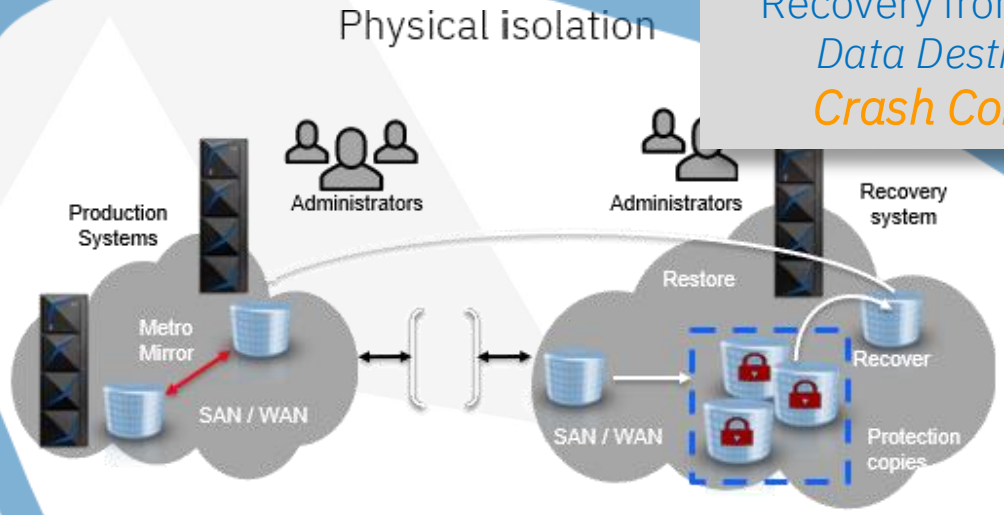
Protecting against Software and Human Caused Data Loss – Point in Time Captures

Classic

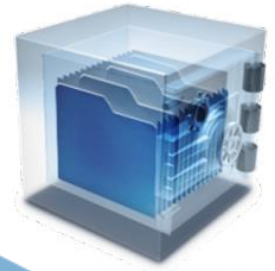
Optimized for Granular Recovery from *Accidental Data Corruption* - *Data Consistent*

FlashCopy & Cloud Backup

Optimized for Large Scale Recovery from *Malicious Data Destruction* – *Crash Consistent*



Safeguarded Copy
Managed by GDPS LCP or CSM



IBM Z Cyber Vault

- ✓ Data Validation
- ✓ Forensics Analysis
- ✓ Catastrophic Recovery
- ✓ Offline Backup

GDPS LCP - Logical Corruption Protection
CSM – Copy Services Manager

Classic Data Set Backup

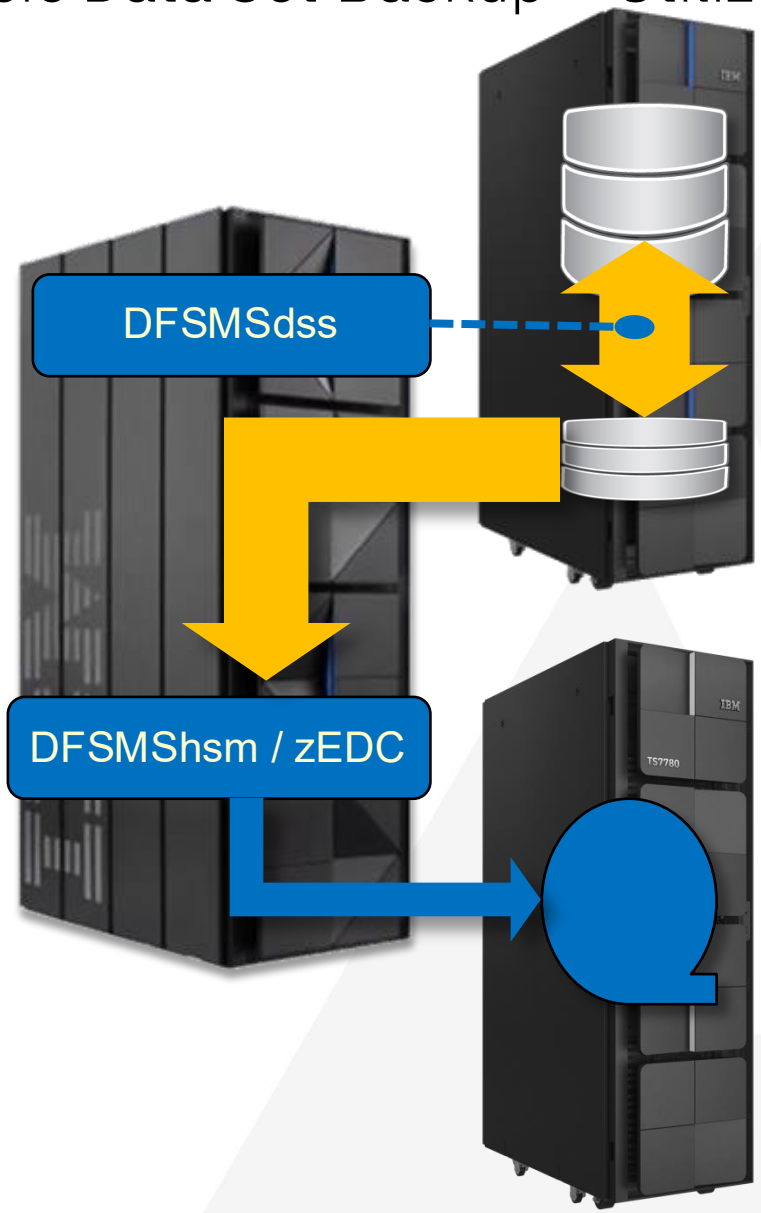
Backup

- Quiesce: High
- Elapsed Time: High
- MIPS: High
- Storage Low (Tape Compression)

Recover

- Recovery Point Objective (RPO): Low
  24+ hours
- Recovery Time Objective (RTO): Low
  For multiple data sets on same tape, recovery is sequential

Classic Data Set Backup – Utilize FlashCopy



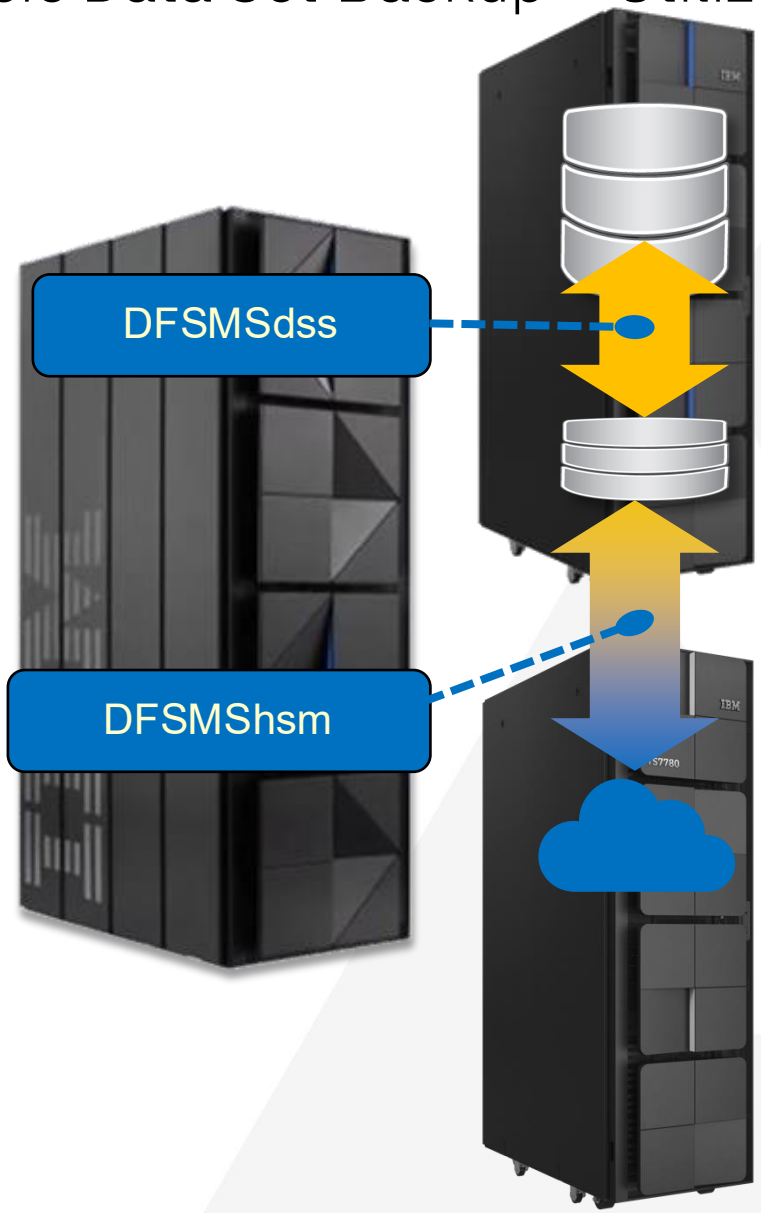
Backup

- Quiesce: Low
  - Only during time to create FlashCopy
- Elapsed Time: Low / High
  - *Low for FlashCopy,* High for Tape offload
- MIPS: Low / High
  - *Low for FlashCopy,* High for Tape offload
- FlashCopy Storage: High / Low
  - High for Full
  - Very Low for Space Efficient
- Tape Storage: Low

Recover

- RPO: Low/High
  - High when multiple space efficient FlashCopies created on disk
- RTO: High/Low
  - High from FlashCopy
  - Low from Tape

Classic Data Set Backup – Utilize Transparent Cloud Tiering



Backup

- Quiesce: Low
- Elapsed Time: Low / High
  - *Low for FlashCopy,* High for Object offload
- MIPS: Low / Low
  - Low for FlashCopy, Low for Tape offload
- FlashCopy Storage: High / Low
  - High for Full
  - Low for Space Efficient
- Object Storage: Low (TCT Compression)

Recover

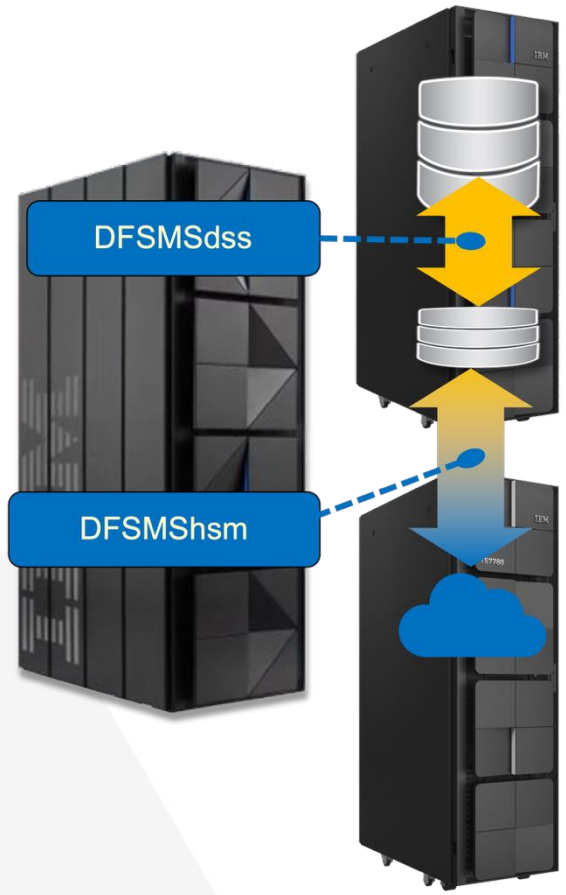
- RPO: Low/High
  - High when multiple space efficient FlashCopies created on disk
- RTO: High/Low
  - High from FlashCopy
  - Low from Object

Note:

- DFSMShsm manual recall required before DSS restore

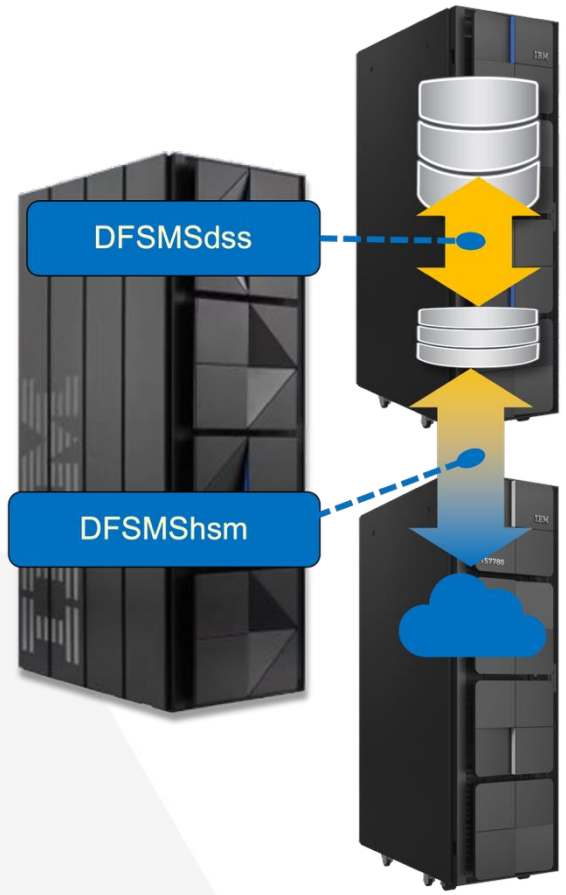
Classic Data Set Backup Comparison

Backup	Classic	Enhanced
Quiesce	High	Low
Elapsed Time	High	Low
MIPS	High	Low
Storage	Low	High/Low
Recover	**Classic**	**Enhanced**
RPO	Low	High/Low
RTO	Low	High/Low



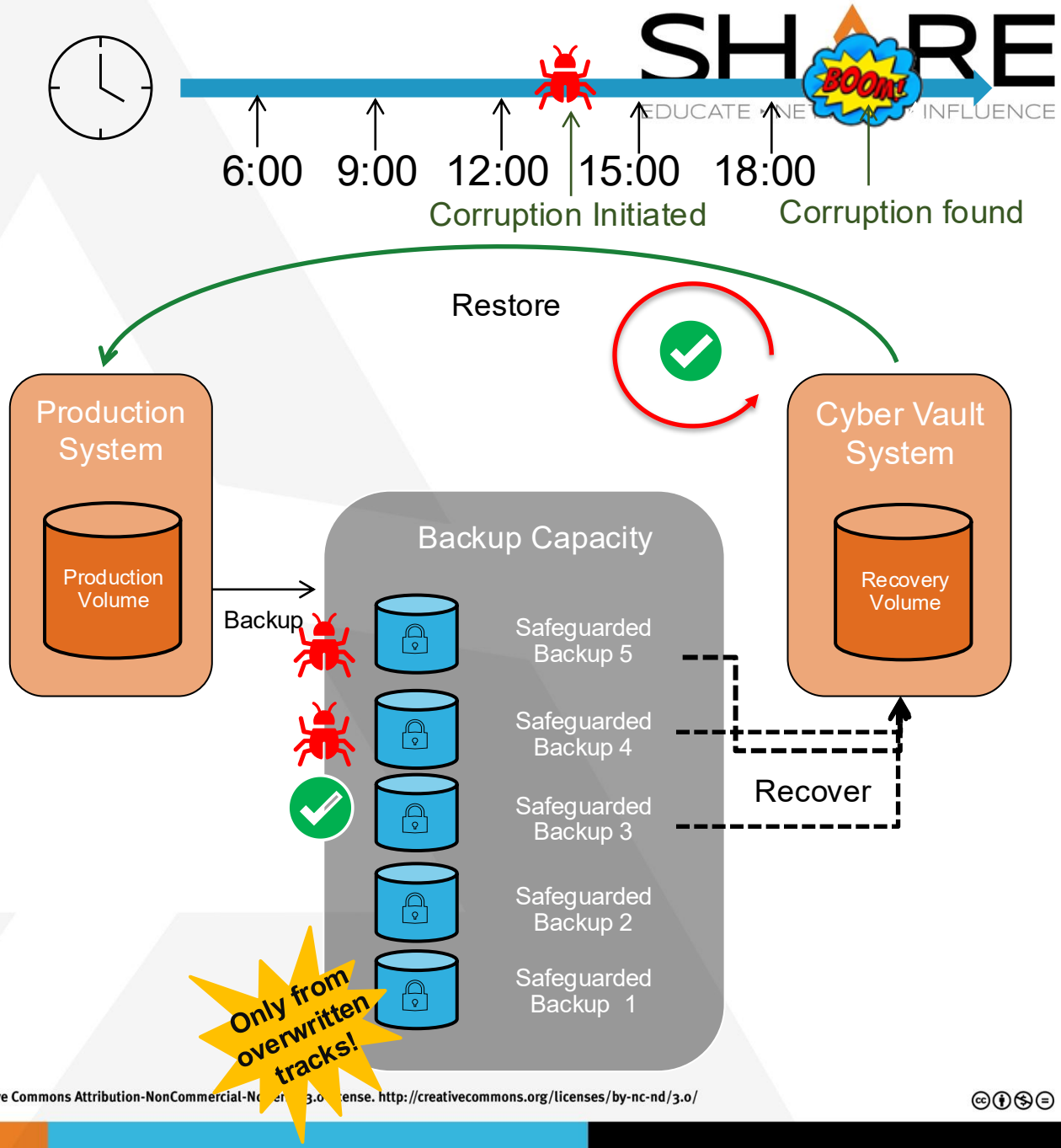
Classic *Full Volume Dump* Comparison

Dump	Classic	Enhanced
Quiesce	High	Low
Elapsed Time	High	Low
MIPS	High	Low
Storage	Low	High/Low
Restore	**Classic**	**Enhanced**
RPO	Low	High/Low
RTO	Low	High/Low



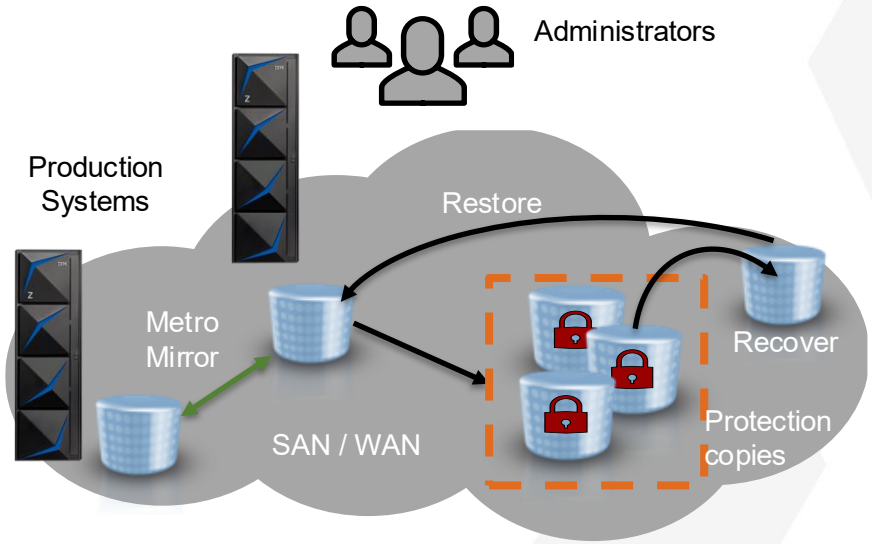
DS8000 Safeguarded Copy

- Each backup (capture) is only of the overwritten tracks!
- Create 1000 Safeguarded Backups for a production volume stored in Safeguarded Backup Capacity, which is not accessible to any server.
  - Thinly provisioned
- Prevent sensitive point in time copies of data from being modified or deleted due to errors, malicious destruction or ransomware attacks.
- Recovery volumes are used with a data recovery system for:
  - Data validation
  - Forensic analysis
  - Restore production data
- IBM GDPS or CSM are required to create and manage the Safeguarded Backups



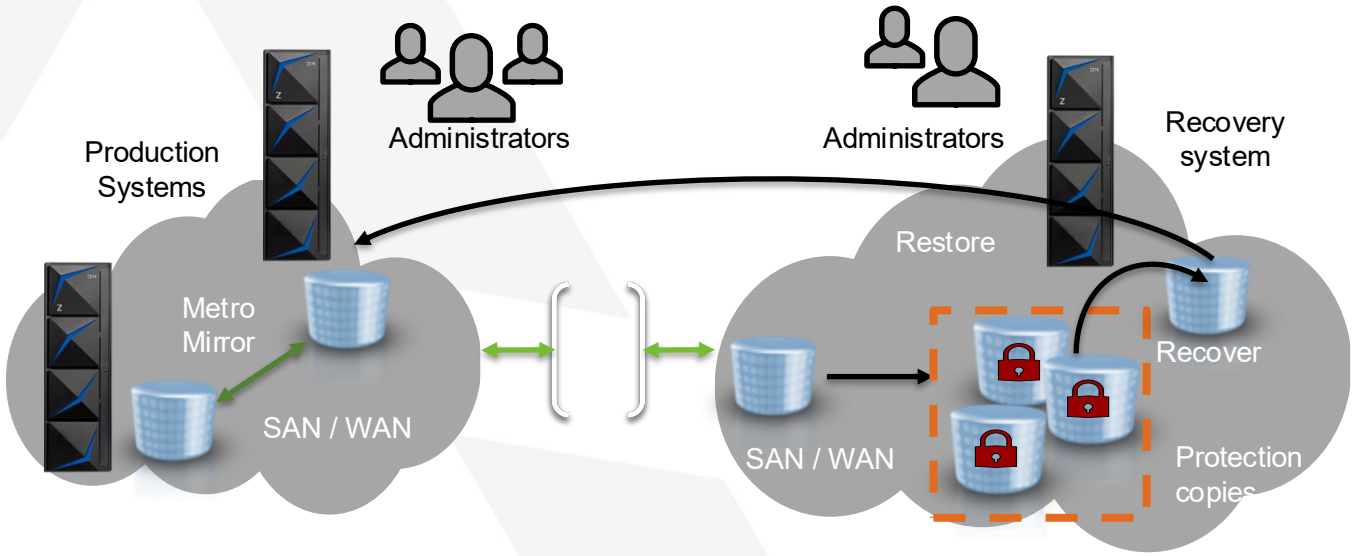
Two Environments: Virtual and Physical

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

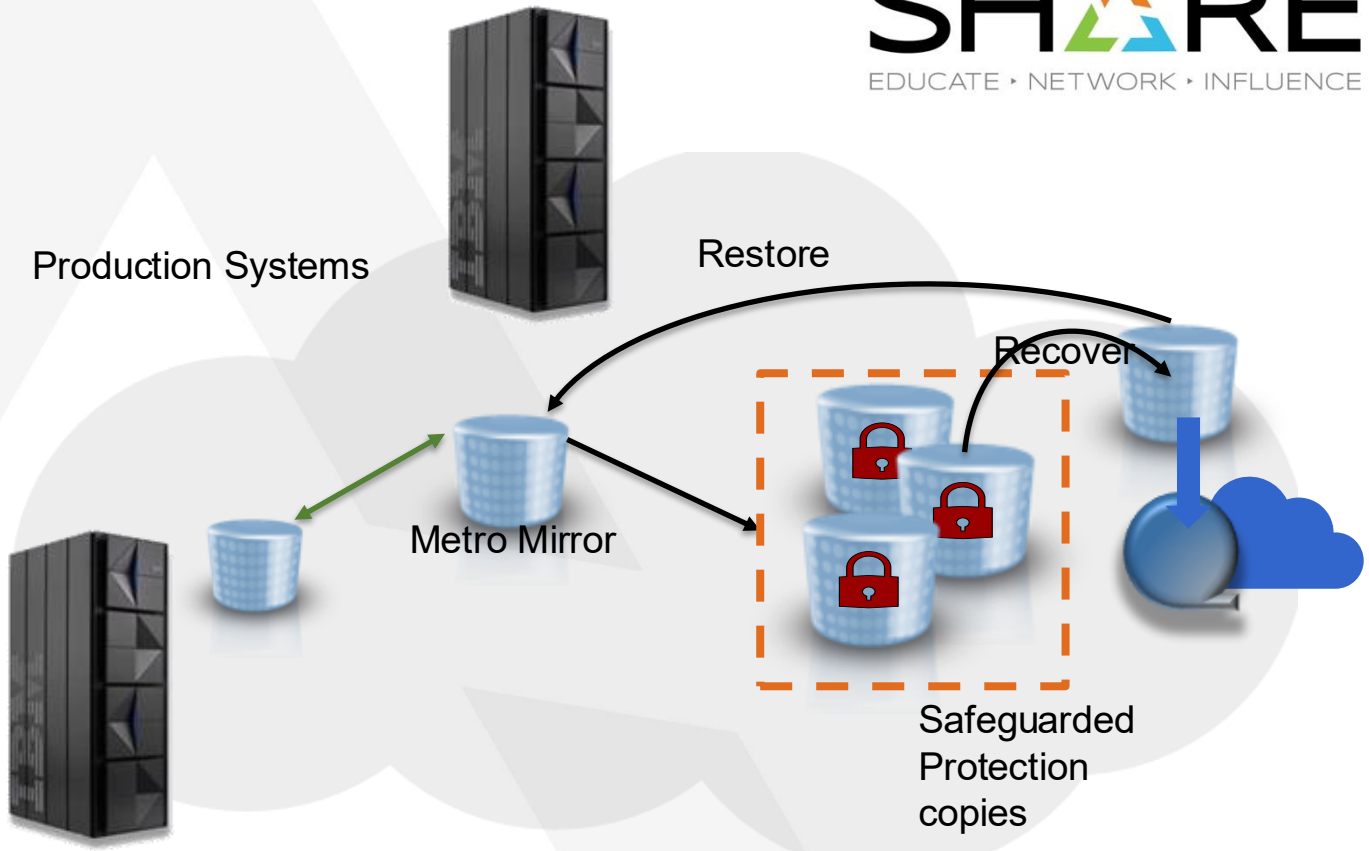
Physical isolation



- 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 Aware’ Data Resiliency

DFSMS and IZBR
integrate backup methodologies to enable clients to leverage their Cyber Vault investments to *significantly enhance*
‘Data Aware’ Data Resiliency

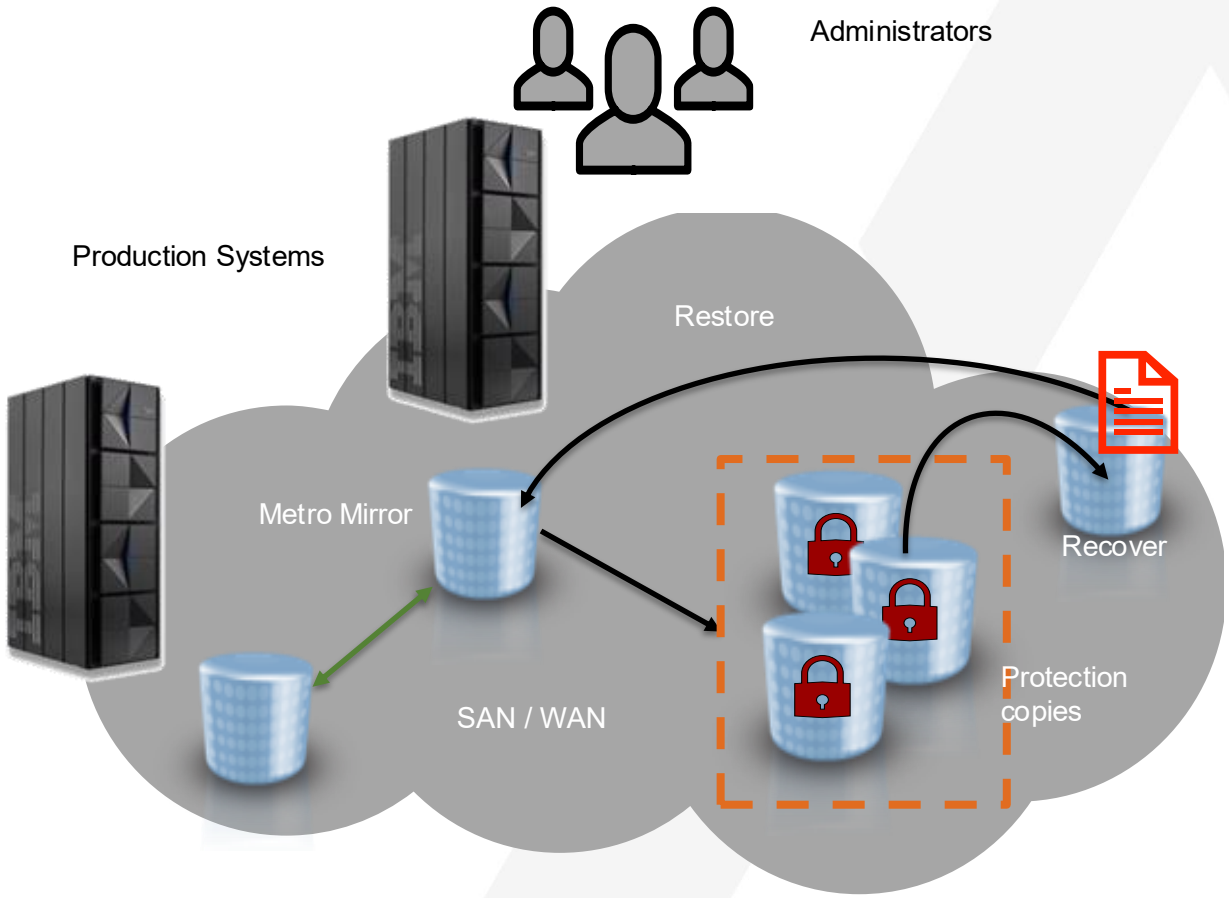


Discrete, individual backup copies optimized for *Granular Recovery* from *Accidental Data Corruption*

Discrete, individual backup copies *and* surgical recovery from Safeguarded Copy / Cyber Vault environments

Many, enterprise-wide undo logs, optimized for *Large Scale Recovery* from *Malicious Data Destruction*

Surgical Recovery from a Safeguarded Copy

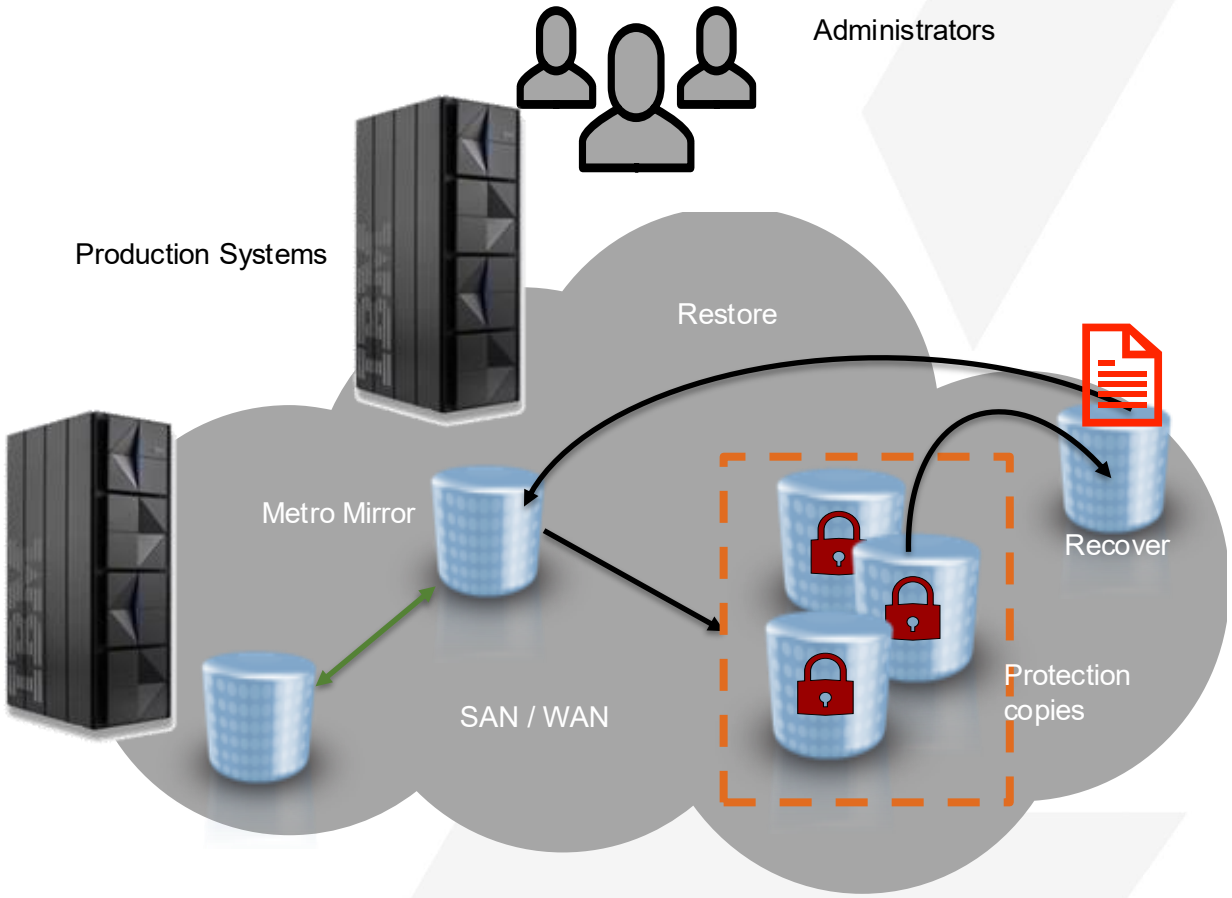


Backup	Classic	Enhanced	SGC
Quiesce	High	Low	Crash Consistent
Elapsed Time	High	Low	Extremely Low
MIPS	High	Low	Extremely Low
Storage	Low	High/Low	Low
Restore	**Classic**	**Enhanced**	**Surgical**
RPO	Low	High/Low	High
RTO	Low	High/Low	High

Notes:

- Because backup is crash consistent, to have a valid recovery, the data must be closed at the time of the safeguarded copy capture or the data set validated
- You need to get the data set back to production from a Cyber Vault system

Surgical Recovery from Safeguarded Copy



Non 'Data Aware' Method

- Initiate GDPS / CSM Recovery
- IPL Recovery System to a Crash Consistent Point
- Select data sets
  - Were data sets open-for-update during the capture (Fuzzy Backup)?
    - CI/CA Split, extend processing, KSDS data/index, …
    - Run data set validation

IZBR 'Data Aware' Method

★ ~~IPL~~

★ Select data sets

IZBR shows SGC Capture Points & if *data sets were open-for-update! This addresses the crash consistency*

★ IZBR will initiate GDPS / CSM Recovery and then only access required volumes

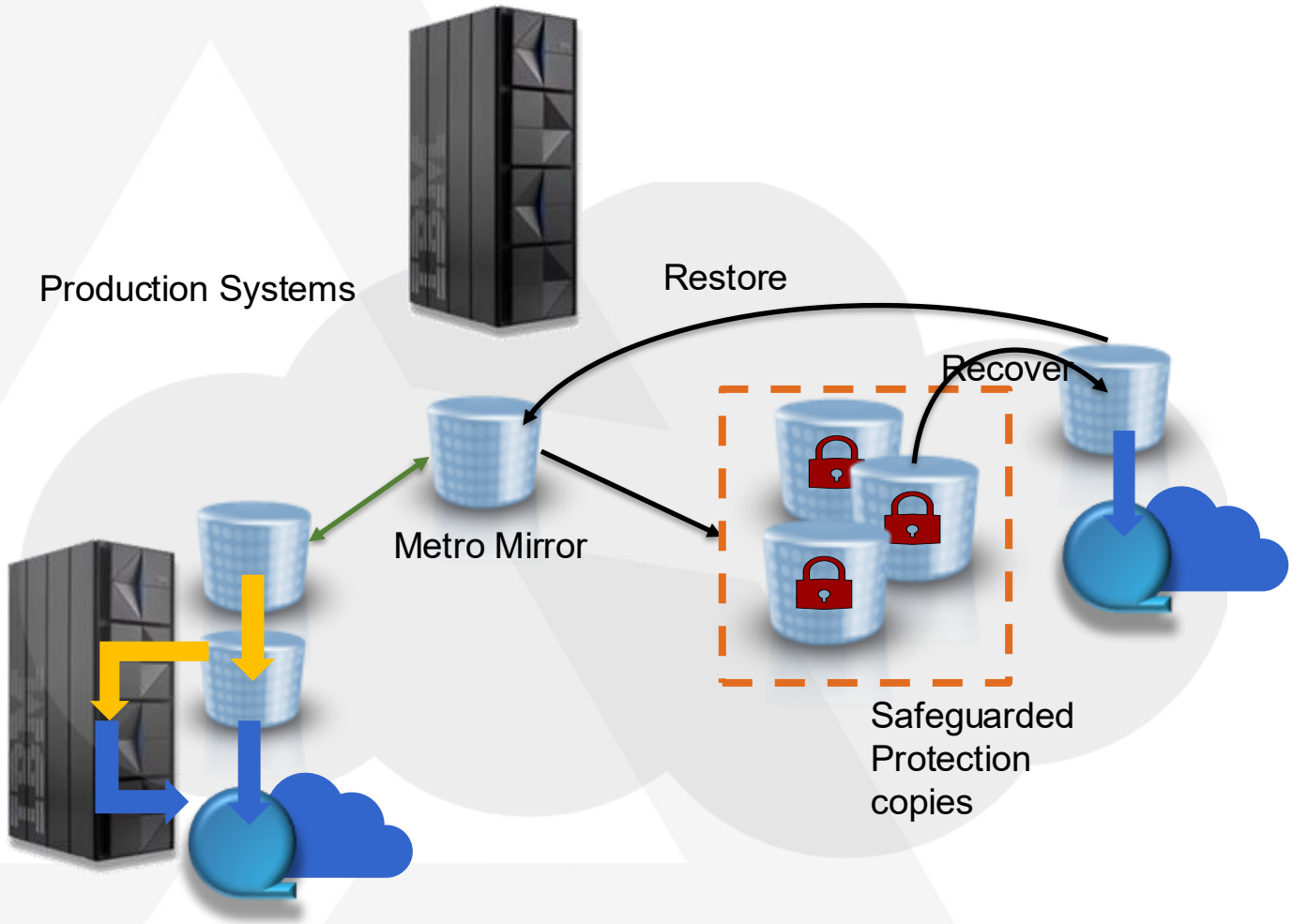
The Magic? IZBR 3DVK

z/OS Strategy: Provide Industry Leading Data Resiliency

As an Infrastructure Architect,
I can provide...

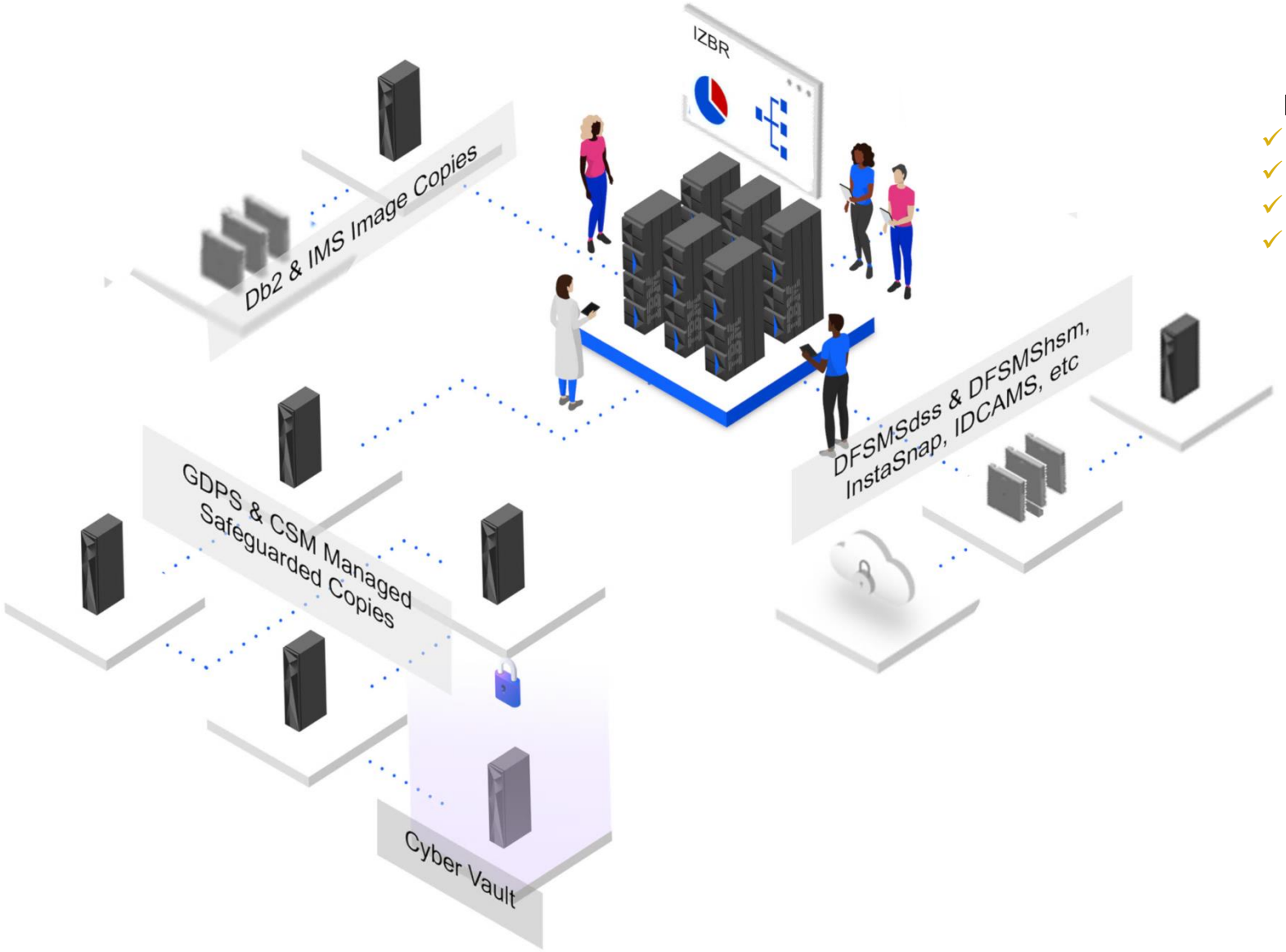
- ✓ Recovery at any scale from malicious or accidental data corruption
- ✓ Regulatory compliance
- ✓ Cost reductions
- ✓ Simplified procedures and processes

...to deliver industry leading Data Resiliency to my Business.



IZBR – z/OS "Data Aware" Data Resiliency Manager

Simplified, Centralized, Persona-Driven Data Resiliency

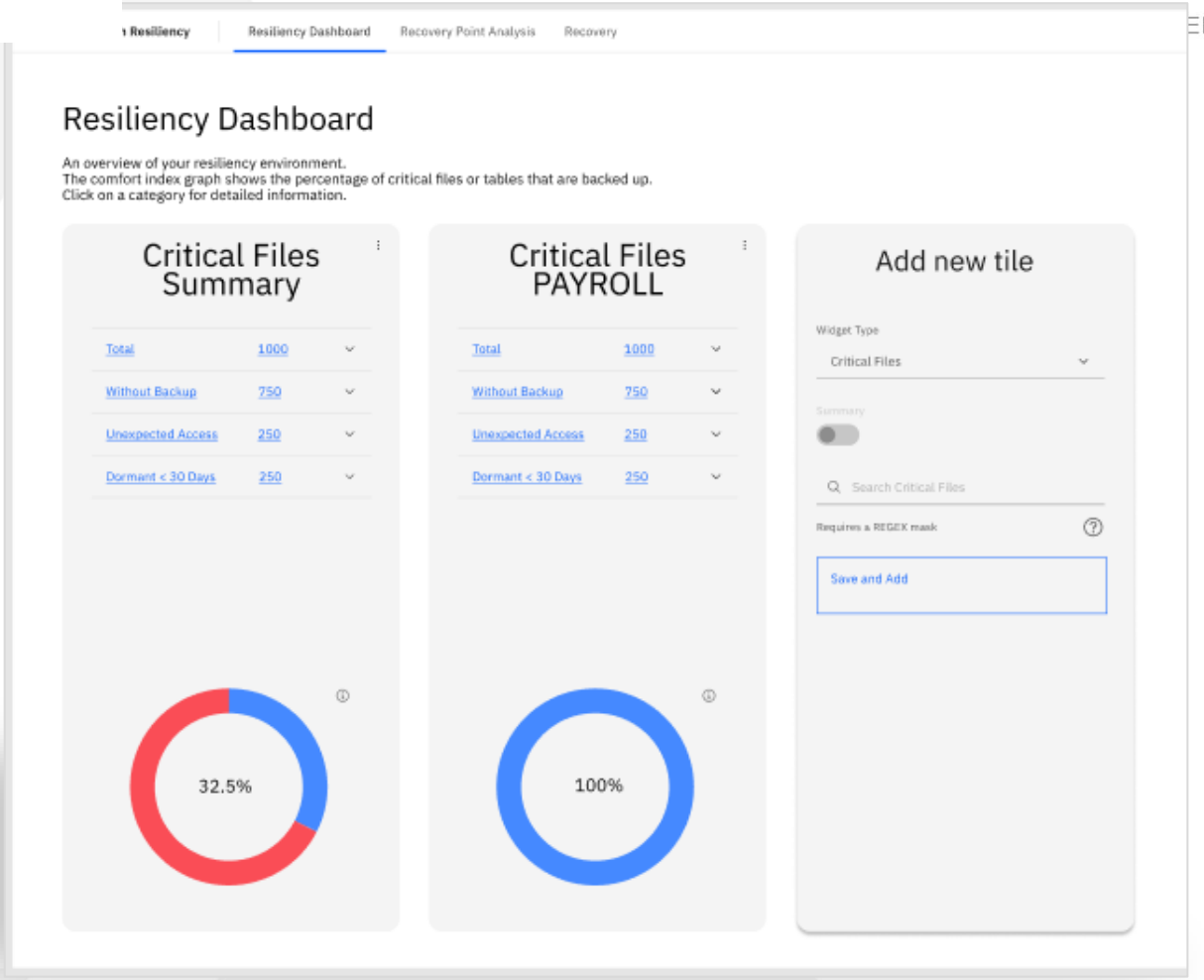


Single source of truth leveraged by *All Personas*

Persona based dashboards:

- ✓ LOB Owner
- ✓ Compliance Team
- ✓ Application Owners
- ✓ Storage Admins

IZBR Persona-Based Dashboards



Single source of truth leveraged by *All Personas*

Persona based dashboards:

- ✓ LOB Owner
- ✓ Compliance Team
- ✓ Application Owners
- ✓ Storage Admins

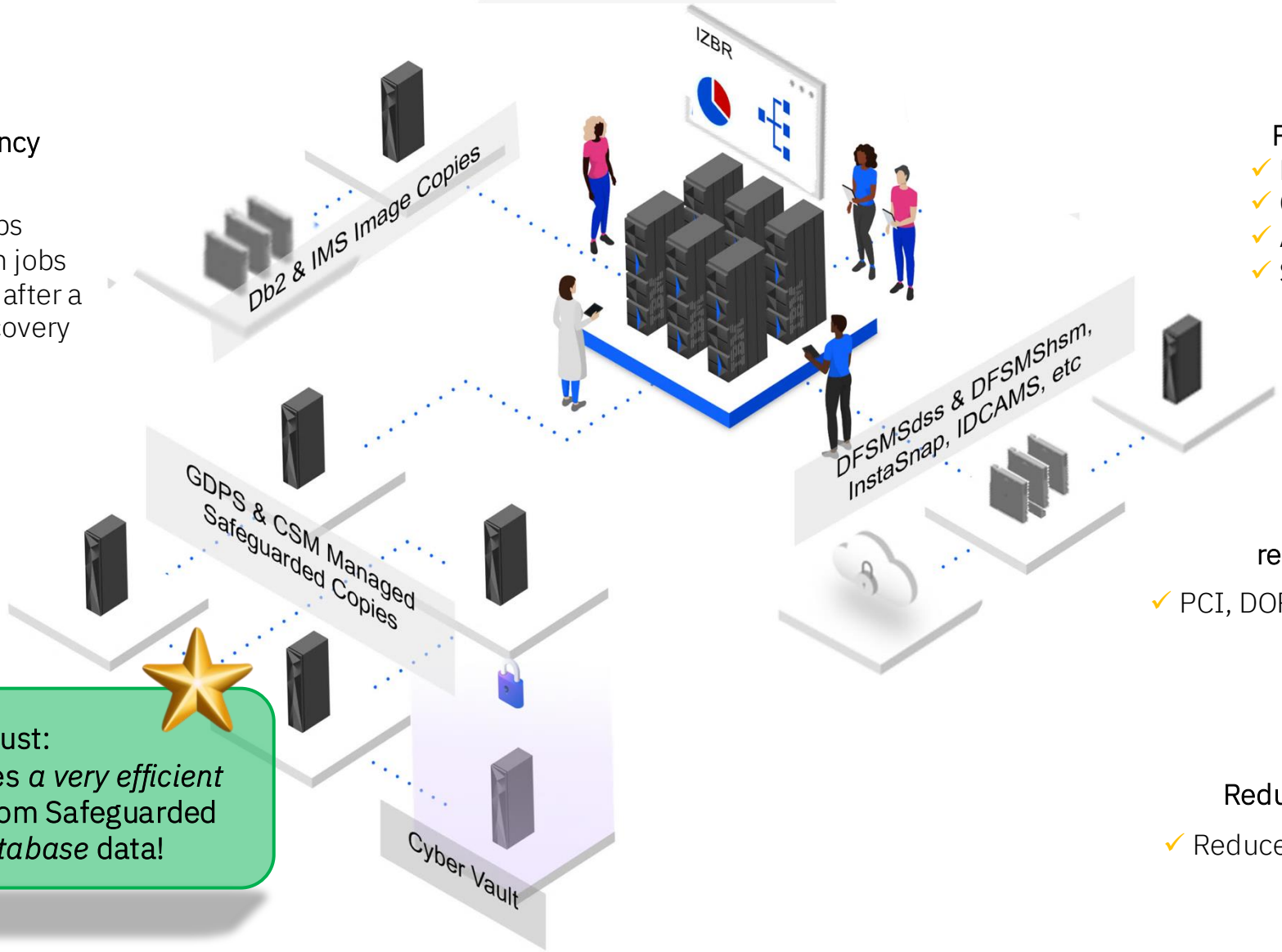
IZBR – z/OS "Data Aware" Data Resiliency Manager

Simplified, Centralized, Persona-Driven Data Resiliency

SHARE
EDUCATE • NETWORK • INFLUENCE

Robust Data Resiliency

- ✓ Identify critical data
- ✓ Identify missing backups
- ✓ Identify all downstream jobs that may need to rerun after a restore to complete recovery
- ✓ Forensics aids



Zero Trust:
Today, IZBR provides *a very efficient* surgical recovery from Safeguarded Copy for *nonDatabase* data!

Single source of truth leveraged by *All Personas*

Persona based dashboards:

- ✓ LOB Owner
- ✓ Compliance Team
- ✓ Application Owners
- ✓ Storage Admins

Comply with regulations and audits

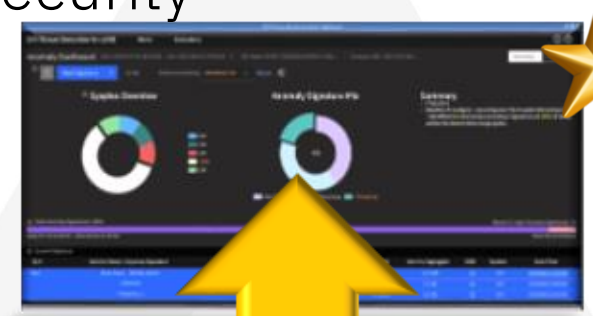
- ✓ PCI, DORA, Bank of England , etc

Simplification

Reduce processing cost

- ✓ Reduce excessive backups, etc

IZBR & TDz Amplify your Cyber Security

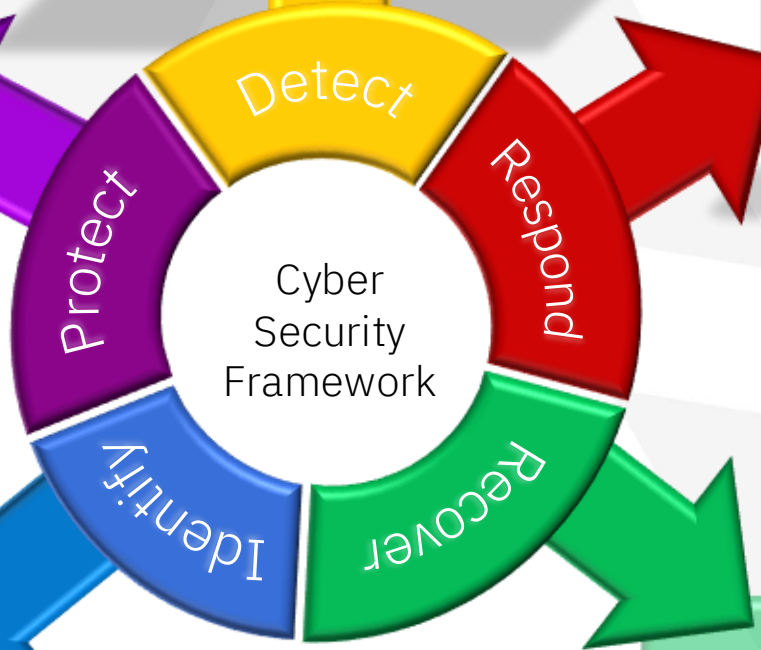


IZBR Foundation

Identify and report on classic and *immutable backup copies* (Safeguarded Copy, WORM tape, Object Storage[1])
Identify unprotected data

New IZBR Foundation

Integration with TDz to respond to Cyber Events[1]



IZBR Foundation

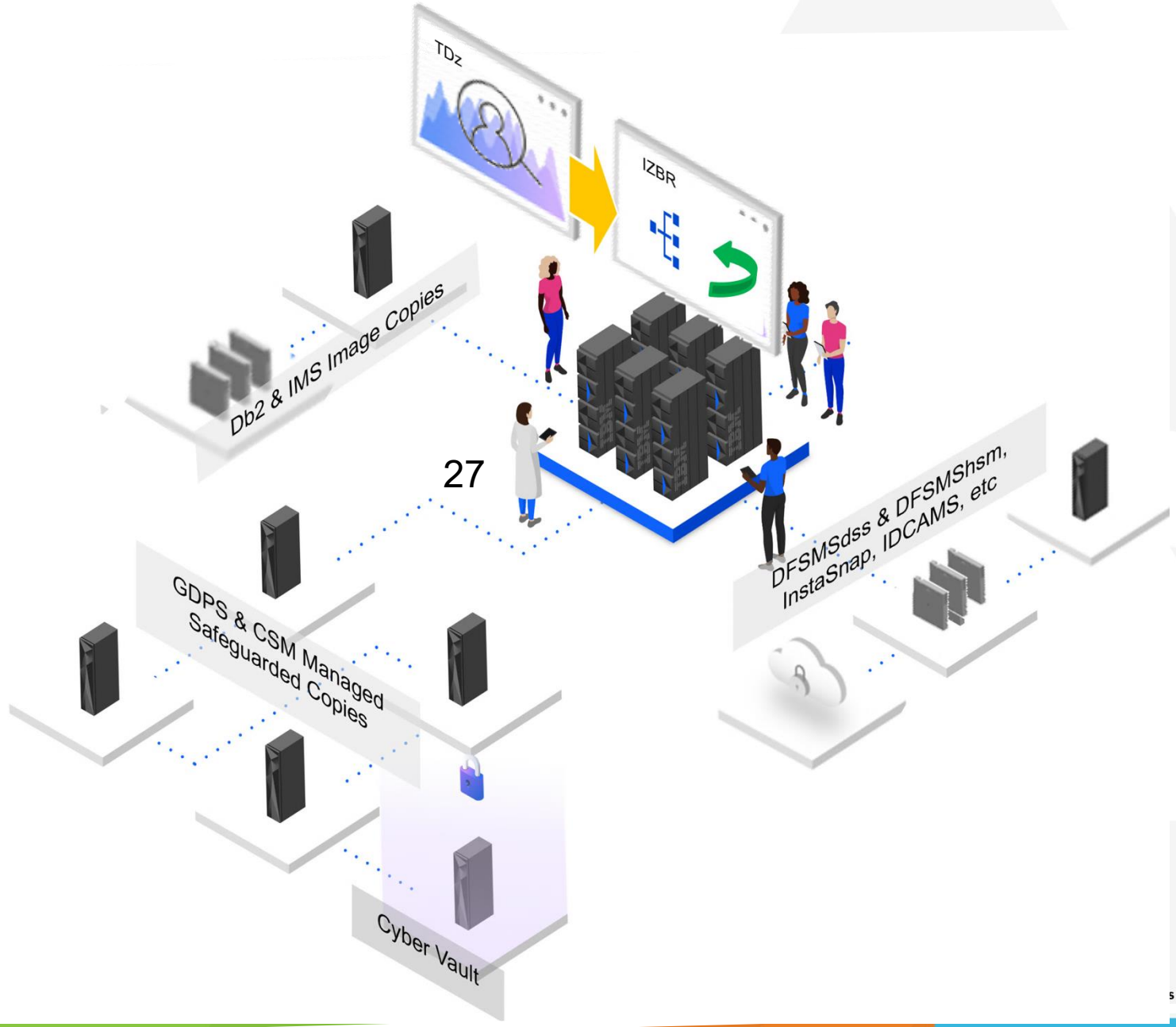
Identify critical data and its flow
Identify data relation with Db2

IZBR Foundation

Simplified, *Meaningful* Recovery

[1] Statement of Direction AD25-0976 8 Apr 2025

IZBR and IBM Threat Detection



IBM Threat Detection for z/OS uses AI to identify anomalies in data access, enhancing security and compliance with emerging regulations like DORA for IBM Z systems.

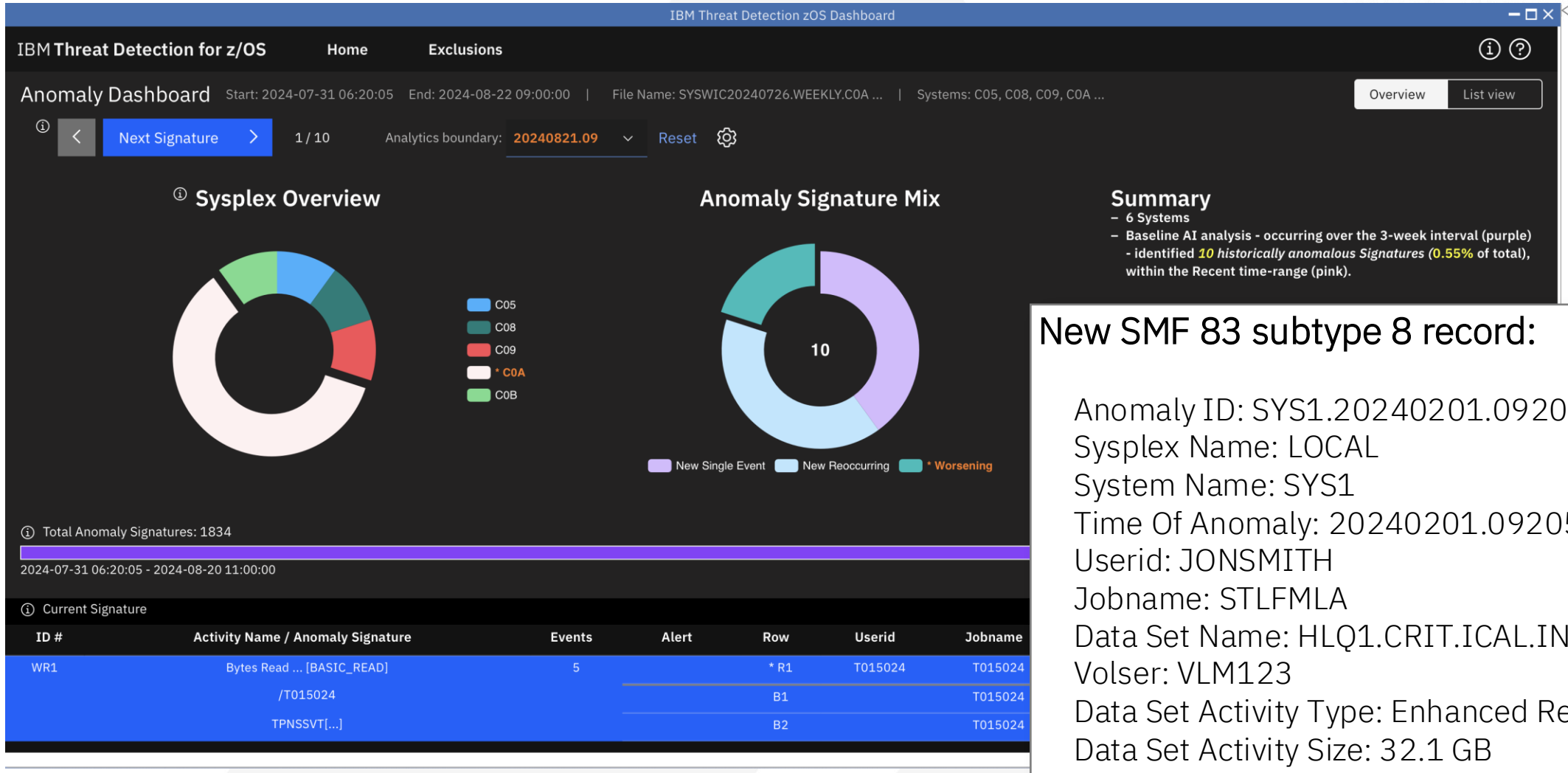
TDz identifies anomalies by *user, job and data set.*

IZBR provides forensics capabilities via job and data sets.

Support announced to enhance IZBR to provide user-based forensics such as user data set access before and after the anomalous event to help determine if the event was malicious and if needed, perform a meaningful recovery. [1]

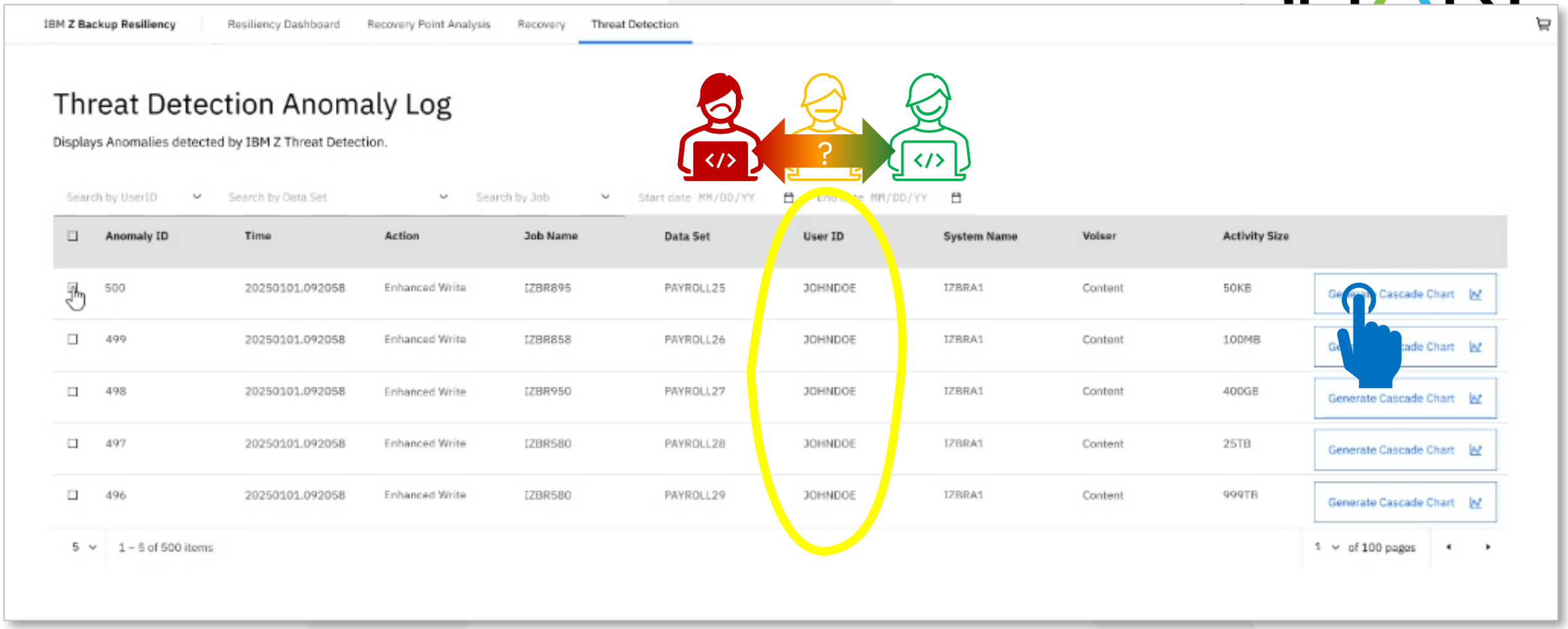
[1] Statement of Direction AD25-0976 8 Apr 2025

Integration with IBM TDz *(Threat Detection)*

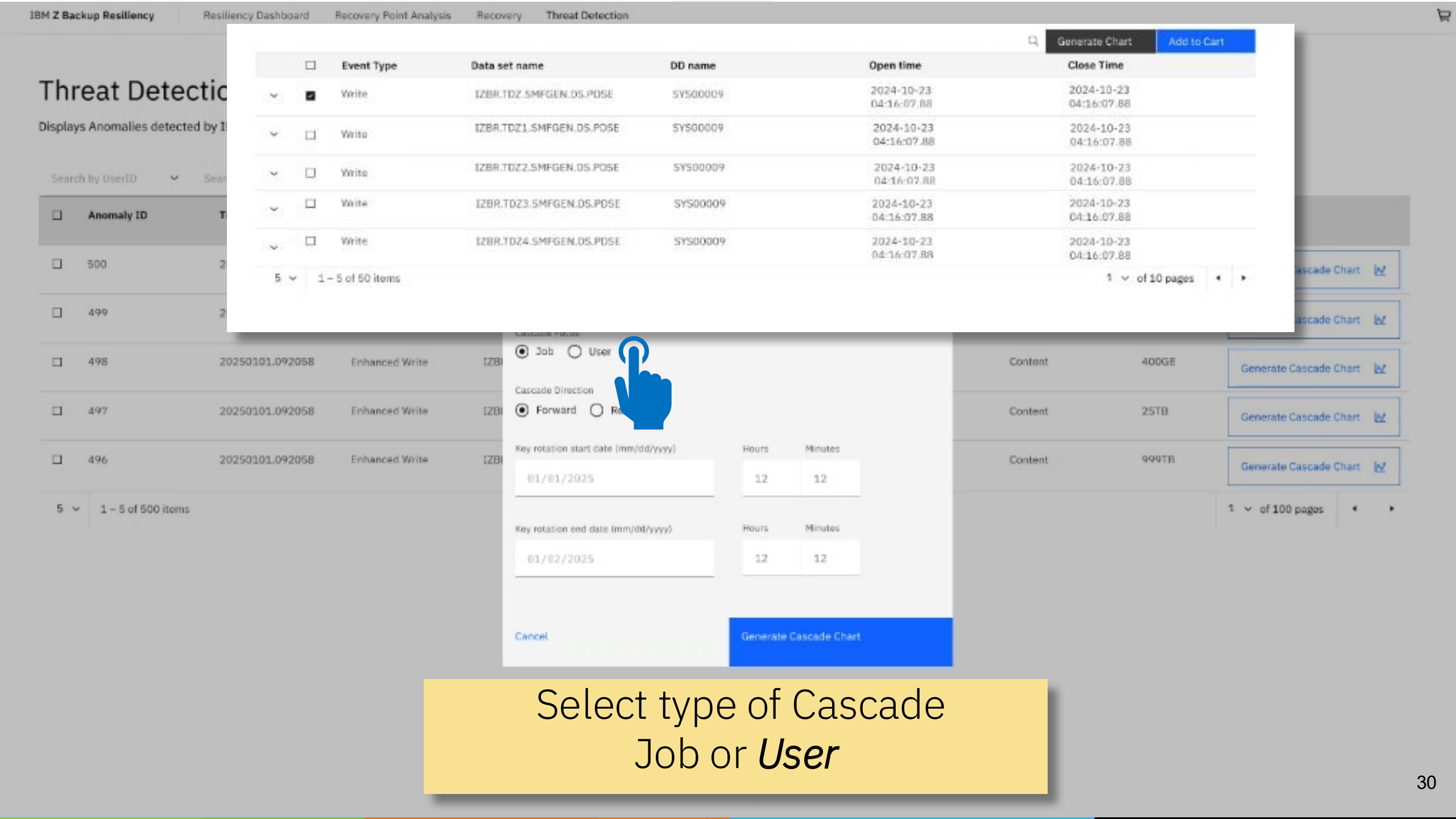


New SMF 83 subtype 8 record:

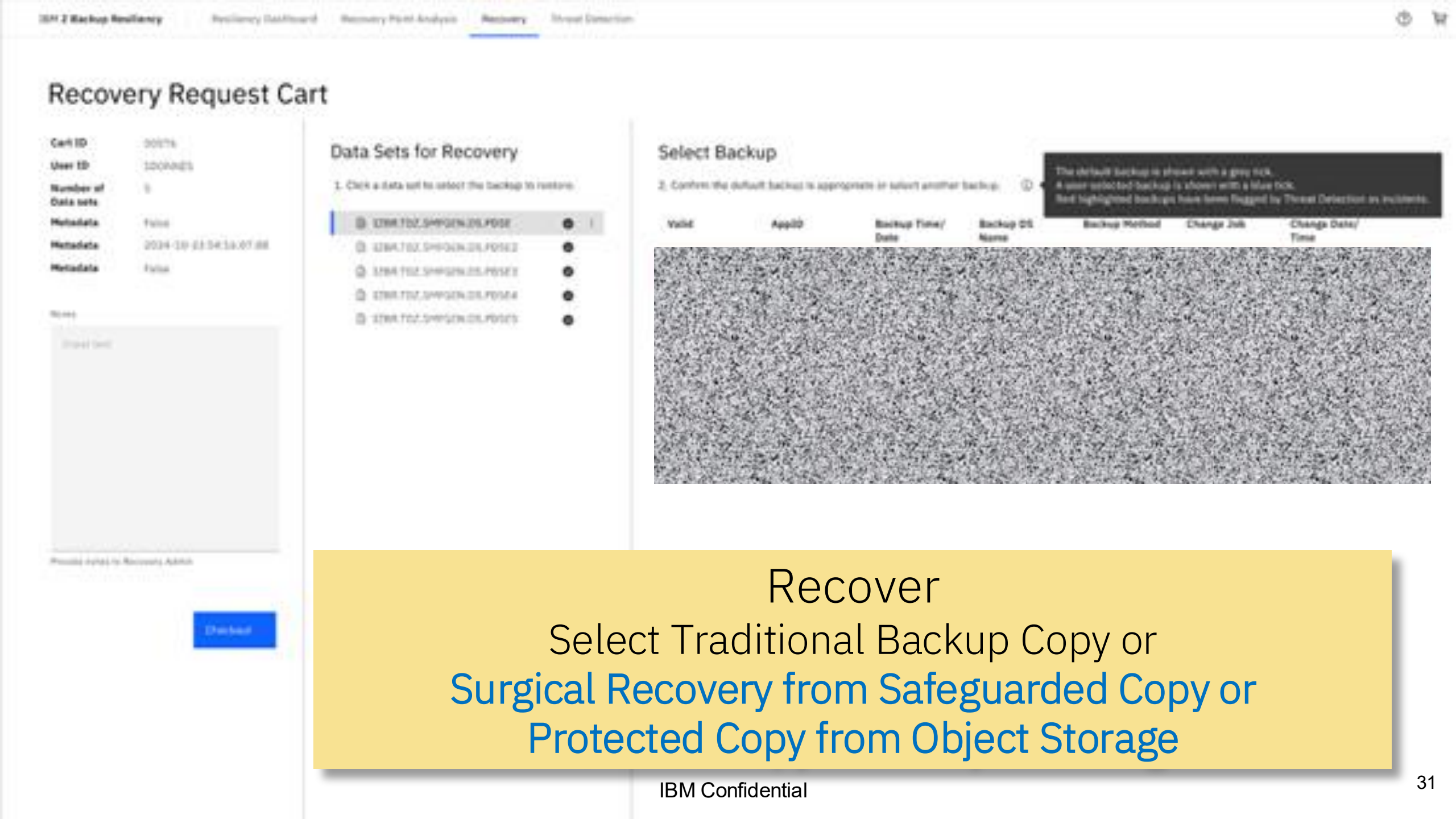
Anomaly ID: SYS1.20240201.092058
Sysplex Name: LOCAL
System Name: SYS1
Time Of Anomaly: 20240201.092058
Userid: JONSMITH
Jobname: STLFMLA
Data Set Name: HLQ1.CRIT.ICAL.INFO
Volser: VLM123
Data Set Activity Type: Enhanced Read
Data Set Activity Size: 32.1 GB



View / Sort *Anomalies*



Select type of Cascade
Job or ***User***



Recover

Select Traditional Backup Copy or

Surgical Recovery from Safeguarded Copy or

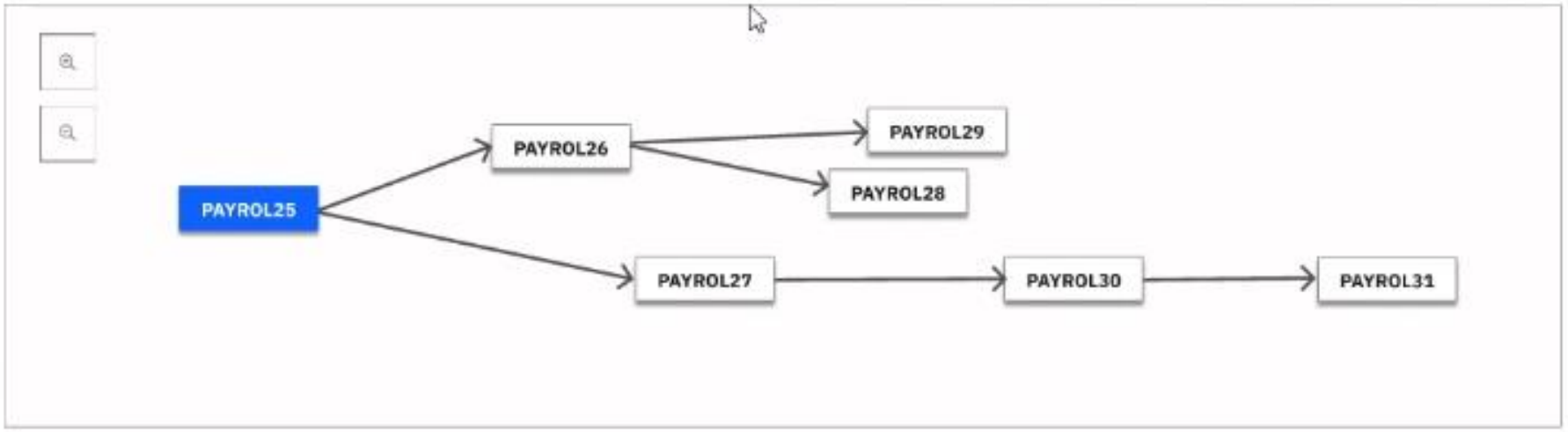
Protected Copy from Object Storage

Search Results / PAYROLL25

Job Viewer for Job **PAYROL25**

Timeline Selector

- PAYROL25
  - Step1(1)
    - Output DS (DEMO.8)
  - Step2(2)
    - Input DS (DEMO.9)



Data Set Events for Job Step 1 (DEMO.8)

Generate Chart | Add to Cart

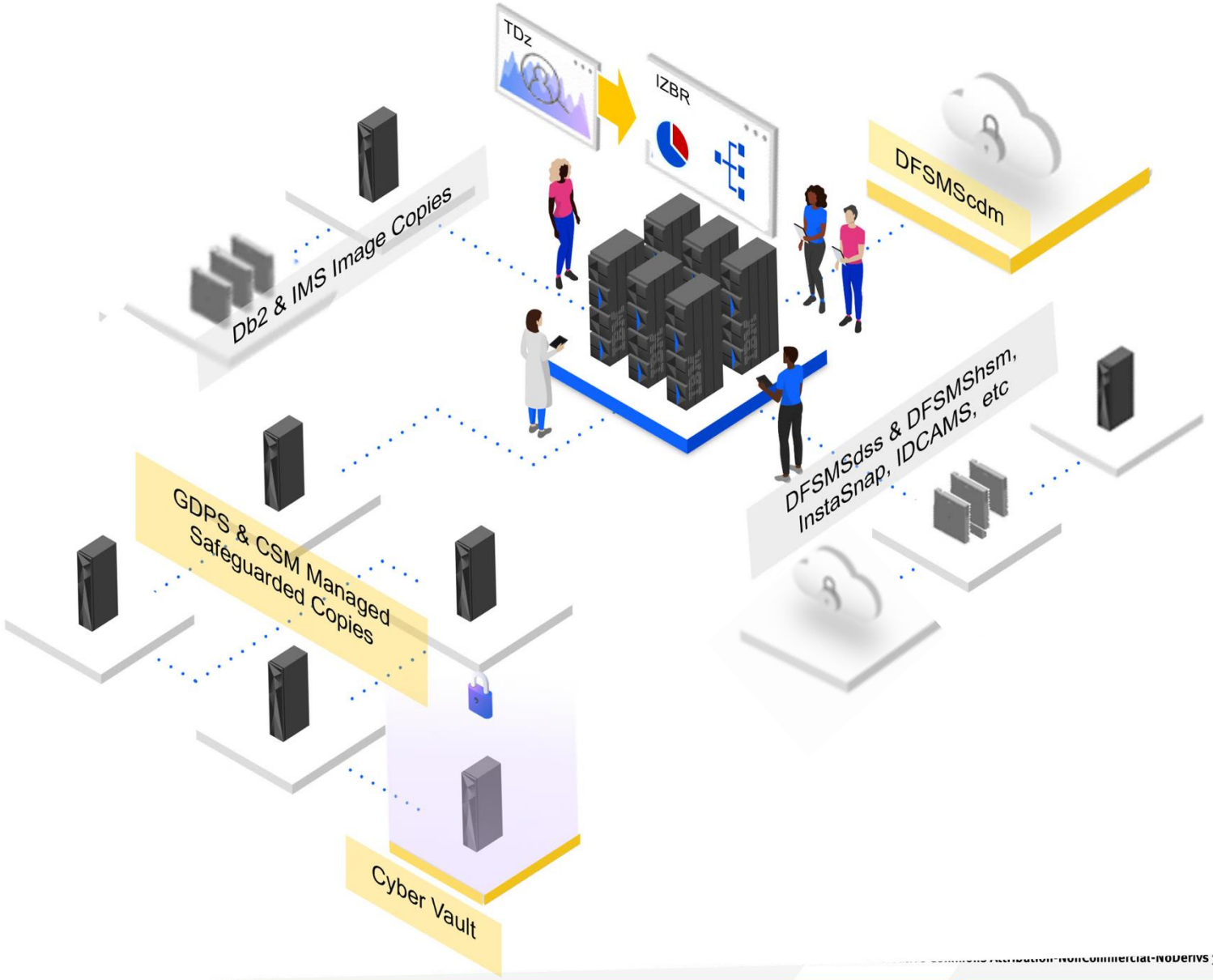
Event Type	Data set name	DD name	Open time	Close Time
Write	IZBR.TDZ.SMFGEN.DS.PDSE	SYS00009	2024-10-23 04:16:07.88	2024-10-23 04:16:07.88
Write	IZBR.TDZ1.SMFGEN.DS.PDSE	SYS00009	2024-10-23 04:16:07.88	2024-10-23 04:16:07.88
Write	IZBR.TDZ2.SMFGEN.DS.PDSE	SYS00009	2024-10-23 04:16:07.88	2024-10-23 04:16:07.88
Write	IZBR.TDZ3.SMFGEN.DS.PDSE	SYS00009	2024-10-23 04:16:07.88	2024-10-23 04:16:07.88
Write	IZBR.TDZ4.SMFGEN.DS.PDSE	SYS00009	2024-10-23 04:16:07.88	2024-10-23 04:16:07.88

5 | 1 – 5 of 50 items | 1 of 10 pages

Identify downstream impact for *meaningful* recovery

Integration by Design for Maximum Data Resiliency

IZBR, DFSMScdm, Safeguarded Copy LCP, Classic DFSMS Backup, TDz

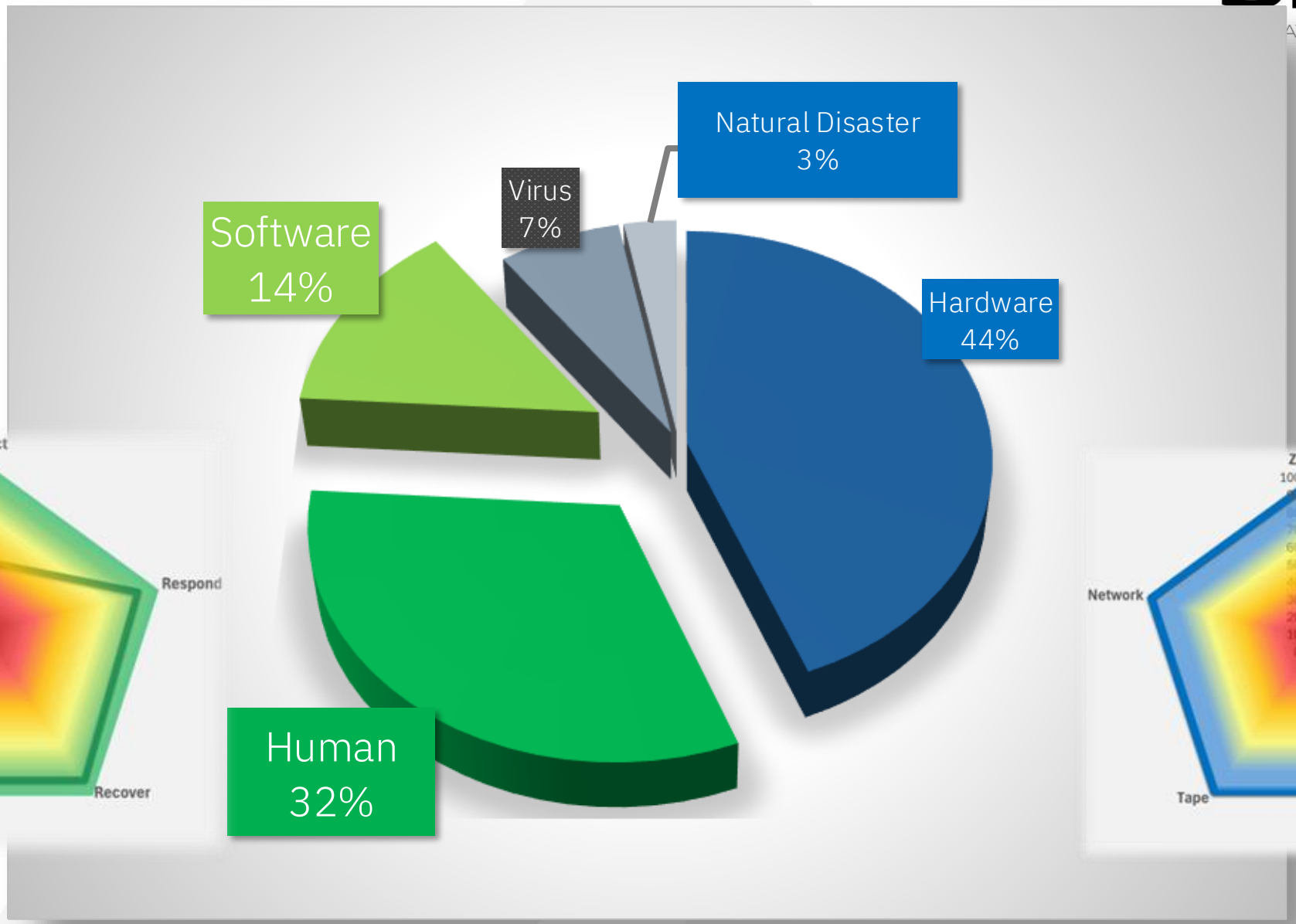


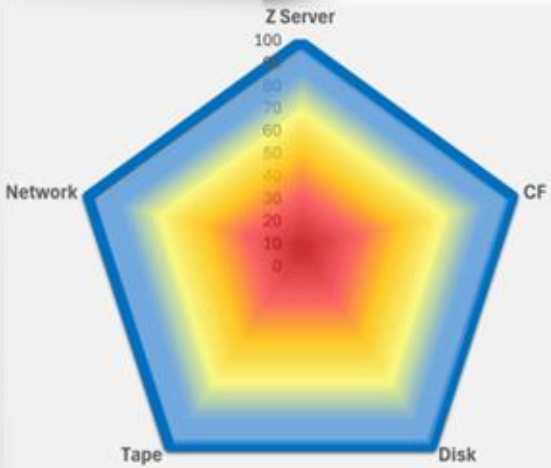
Leveraging IZBR as the z/OS Data Resiliency Manager, provide an integrated data resiliency strategy across all technologies

- ✓ Announced support for **z/OS Threat Detection** for forensics and recovery from malicious data corruption [1]
- ✓ Announced support for **z/OS DFSMScdm** to leverage protected cloud storage as another tier for z/OS data [1]
- ✓ **Surgical Recovery** from a **Safeguarded Copy**, imperative when a cyber attack deletes classic backup copies

[1] Statement of Direction AD25-0976 8 Apr 2025

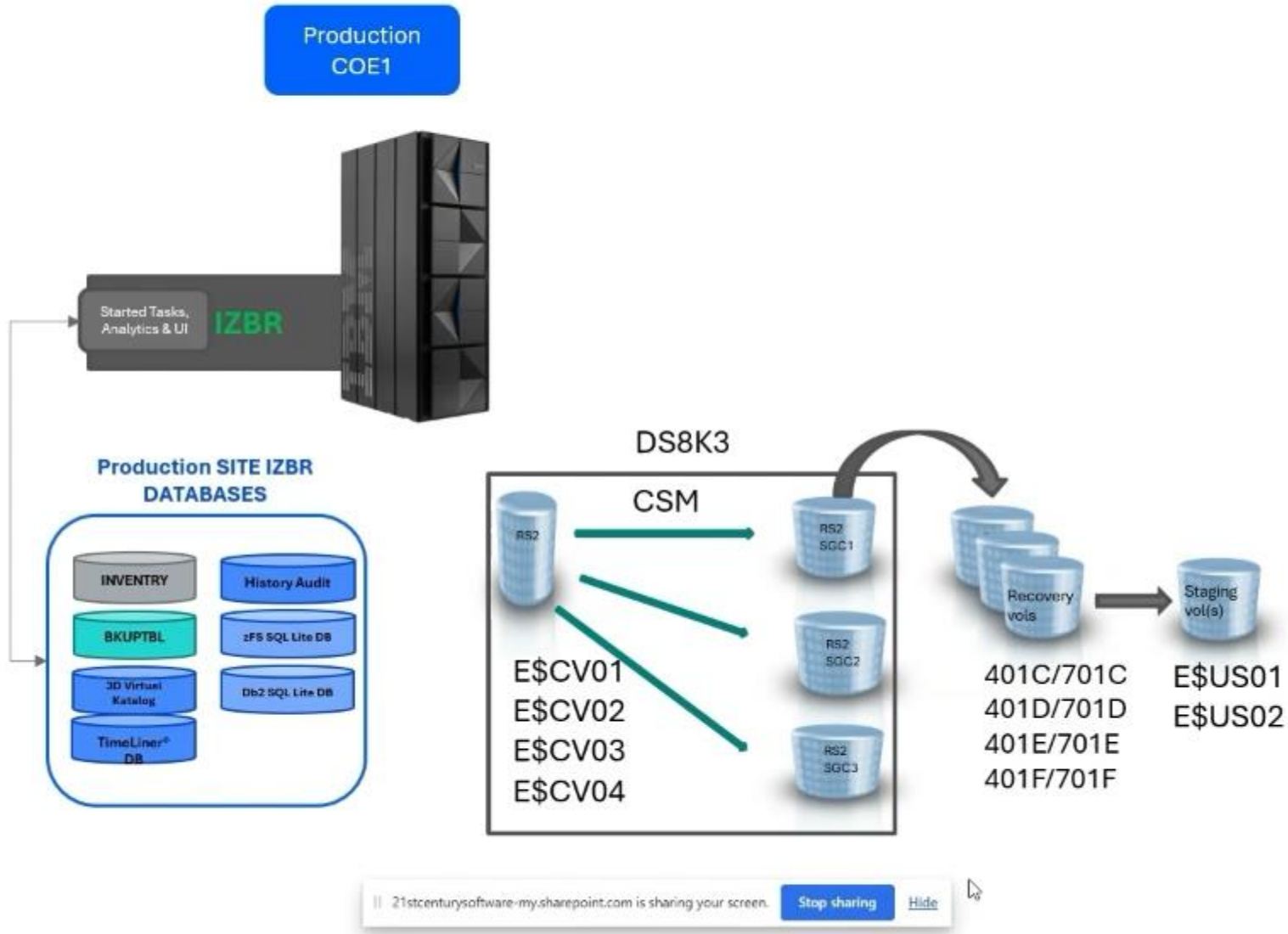
Elevate your Data Resiliency





VIDEO - IZBR SURGICAL RECOVERY

IZBR Cyber Resiliency CSM Demo (Local)



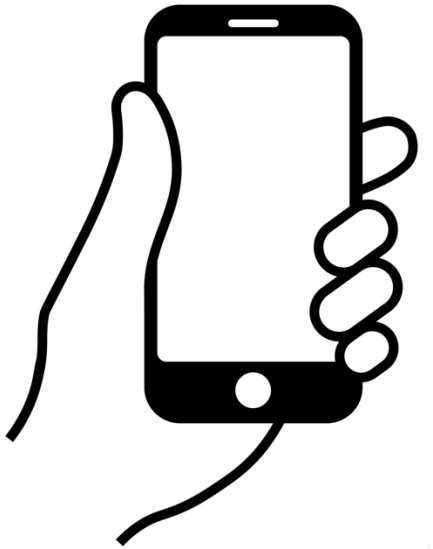
Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation

SHARE mobile app



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.