

# Ransomware protection for your Mainframe Data

Dell EMC

November 2018

Session **FJ**



# Topics

- The threat and external agencies that have taken notice
- Logical vs physical recovery
- Storage based solutions: SnapVX and zDP
- Examples of Cyber Recovery for IBM Z

# The Threat and Who's Taking Notice

# Evolution of cyber threats

## Traditional Threats

Cyber  
Theft



Denial of Service  
Attacks



## Emerging Threats

Cyber  
Extortion

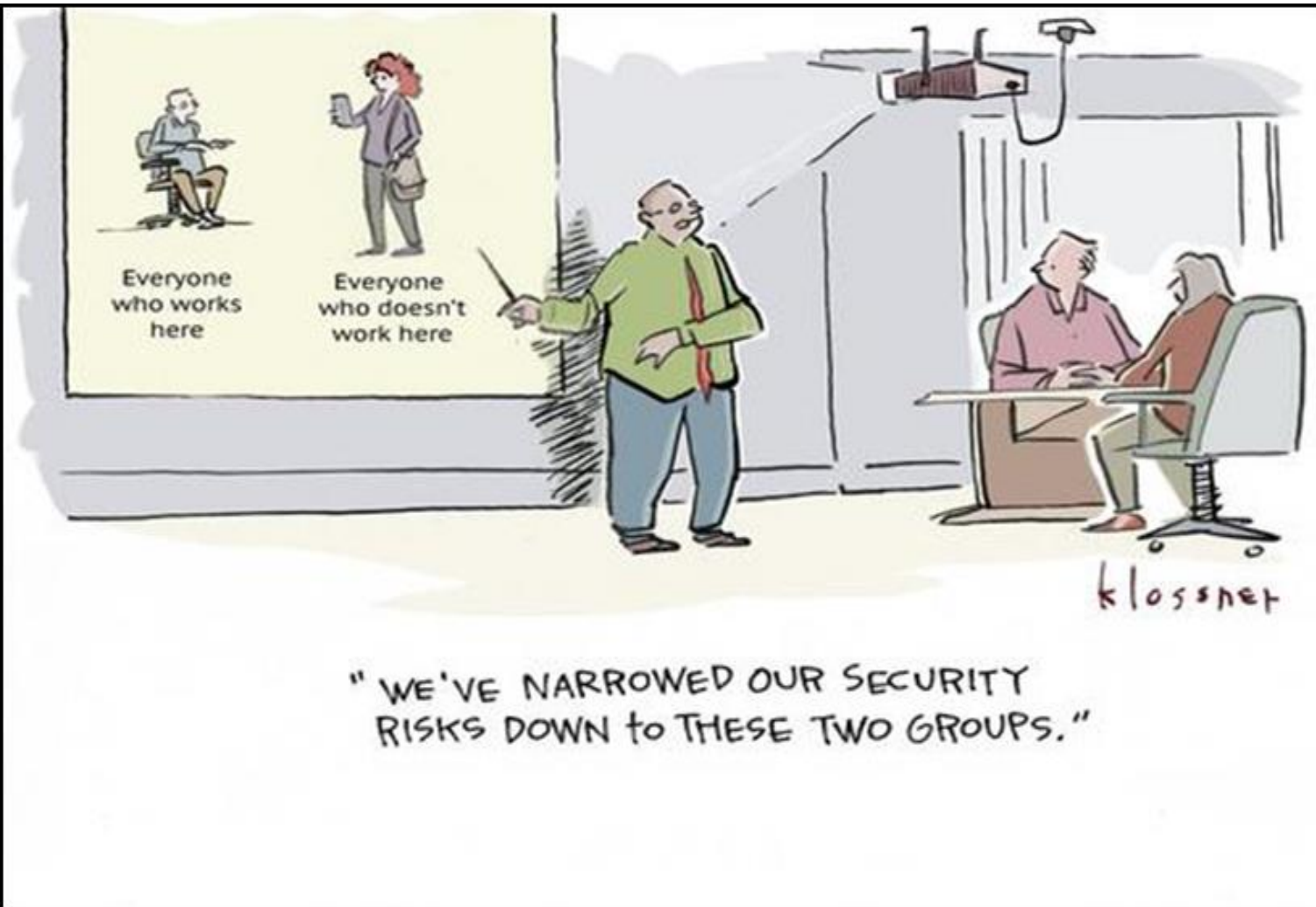


Cyber  
Destruction



Cyber Recovery Solutions protect  
against these types of attacks

# Threat vectors are increasing



156 million phishing emails sent WW every day



16 million make it through filters



8 million are opened



800,000 LINKs are click'd



IF 12% click on phishing emails

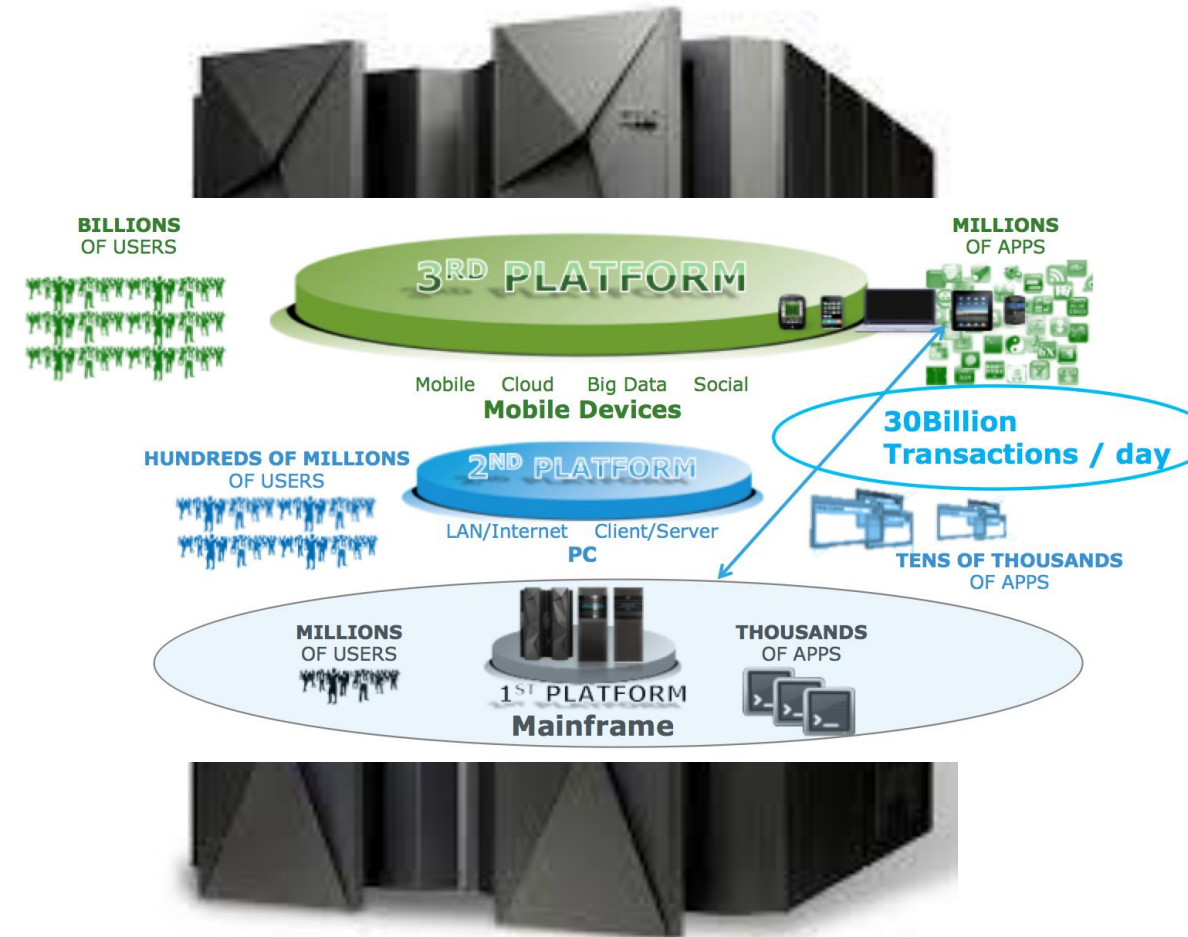


All it takes is **ONE**

\* By cartoonist John Klossner – May 2016

# MAINFRAME THE MOST DESIRABLE TARGET

- Mainframe is system of record for their organizations
- 80% of all active code runs on mainframe
- 80% of enterprise data is housed on mainframe
- Today technologies have eliminated mainframe isolation



# The next wave of cyber attacks are here now

## *DESTRUCTION*

### Prominent Entertainment Company

“It erased everything stored on 3,262 of the company’s 6,797 personal computers and 837 of its 1,555 servers. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.”

- Fortune, July 2015

## *RANSOMWARE*

### Prominent Health Care Provider

“The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.”

- Letter from CEO, February 2016

# Regulatory cybersecurity guidance



**FFIEC:** “Data Or Systems Destruction and Corruption... Another control for consideration is an "air-gap," a security measure in which a computer, system, or network is physically separated from other computers, systems, or networks. ***An air-gapped data backup architecture limits exposure to a cyber attack*** and allows for restoration of data to a point in time before the attack began.”



**Federal Reserve System:** “financial institutions should consider ... ***logical network segmentation, hard backups, air gapping [and] physical segmentation*** of critical systems”



**European Banking Authority:** “Competent authorities should assess whether the institution has ***comprehensive and tested business resilience and continuity plans*** in place”



**National Security Agency:** “best practices to protect information systems and networks from a destructive malware attack include... ***Segregate network systems***”



**National Association of Insurance Commissioners:** “... it is vital for state insurance regulators to provide ***effective cybersecurity guidance*** regarding the protection of the insurance sector’s data security and infrastructure..”



# Ransomware is a real threat

- See SHARE Live San Jose 2017 Security project presentation:

- “Ransomware on the Mainframe...Checkmate!

[https://www.bigdiansmalls.com/files/ransomware\\_share\\_2017.mp4](https://www.bigdiansmalls.com/files/ransomware_share_2017.mp4)



**SHARE**   

**San Jose 2017** 

**Ransomware on the Mainframe  
Checkmate!**

*Chad Rikansrud*



#SHAREsjc    

SHARE is an independent volunteer-run information technology association  
that provides education, professional networking and industry influence.

Copyright © 2016 by SHARE Inc.   Content where otherwise noted. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license  
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

**SHARE**  
EDUCATE • NETWORK • INFLUENCE

# What questions are the board of directors asking?

- Are we at risk of a destructive Hacktivist Attack?
- Do we have the cyber security protections in place to guarantee our business is safe?
- What would be the impact to our customers, shareholders, employees if our information was lost ?
- If we assume we have been compromised and our data was destroyed could we recover the business and how long would it take?
- Will my Errors and Omissions Insurance cover me if we lose customer assets due to a Cyber Attack?

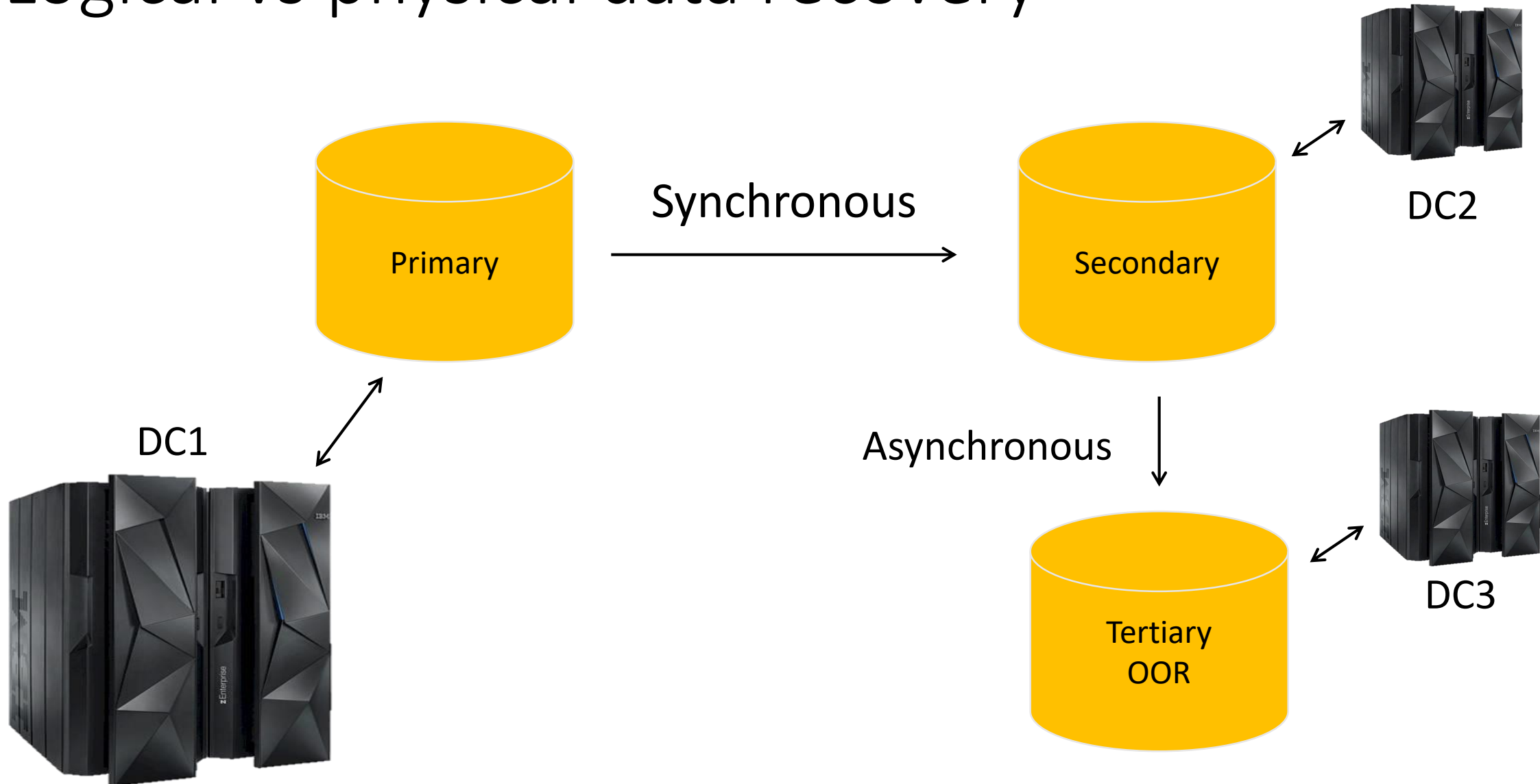


***WHO IS PAYING FOR THIS EXTRA PROTECTION??***

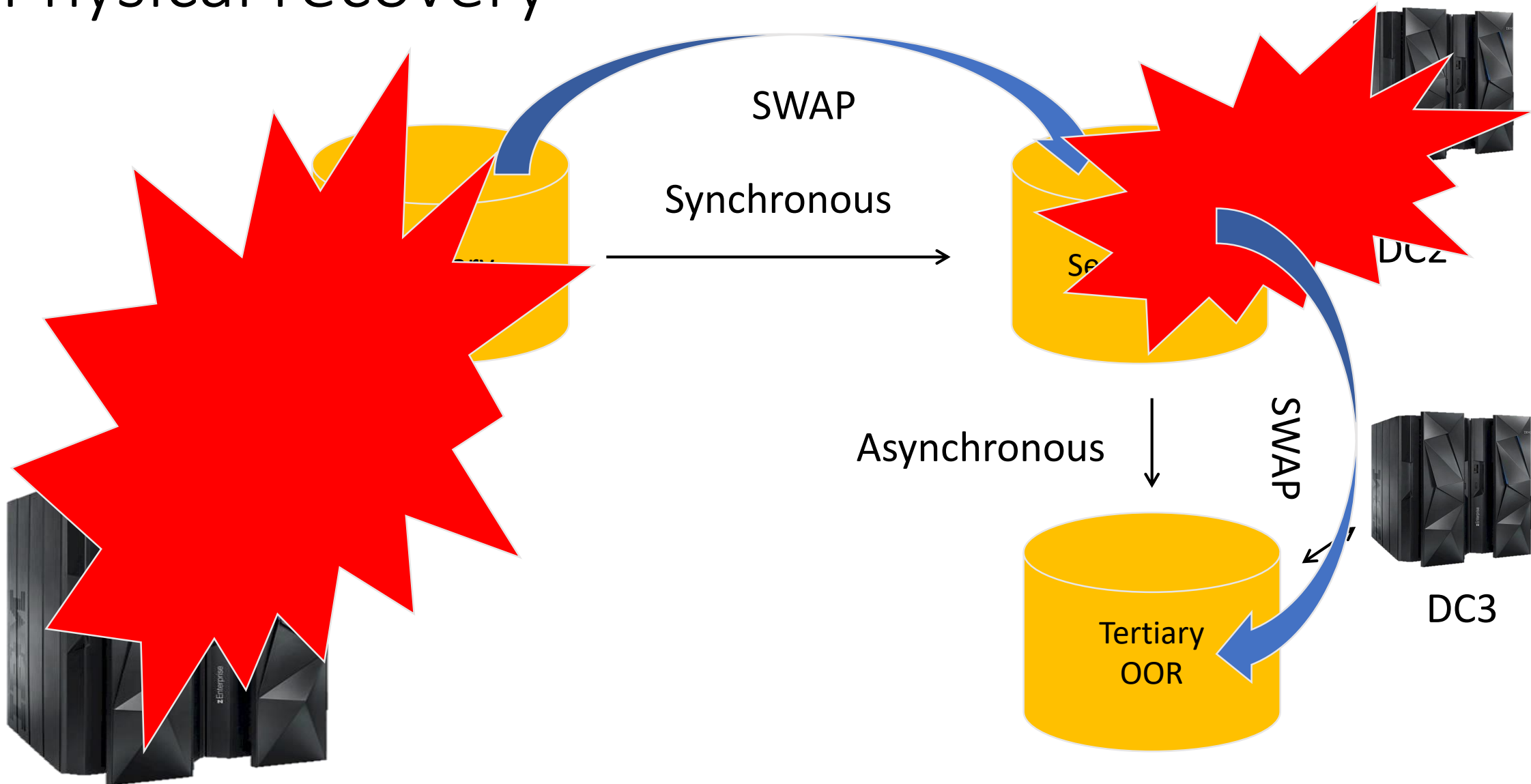


# Physical vs Logical Recovery

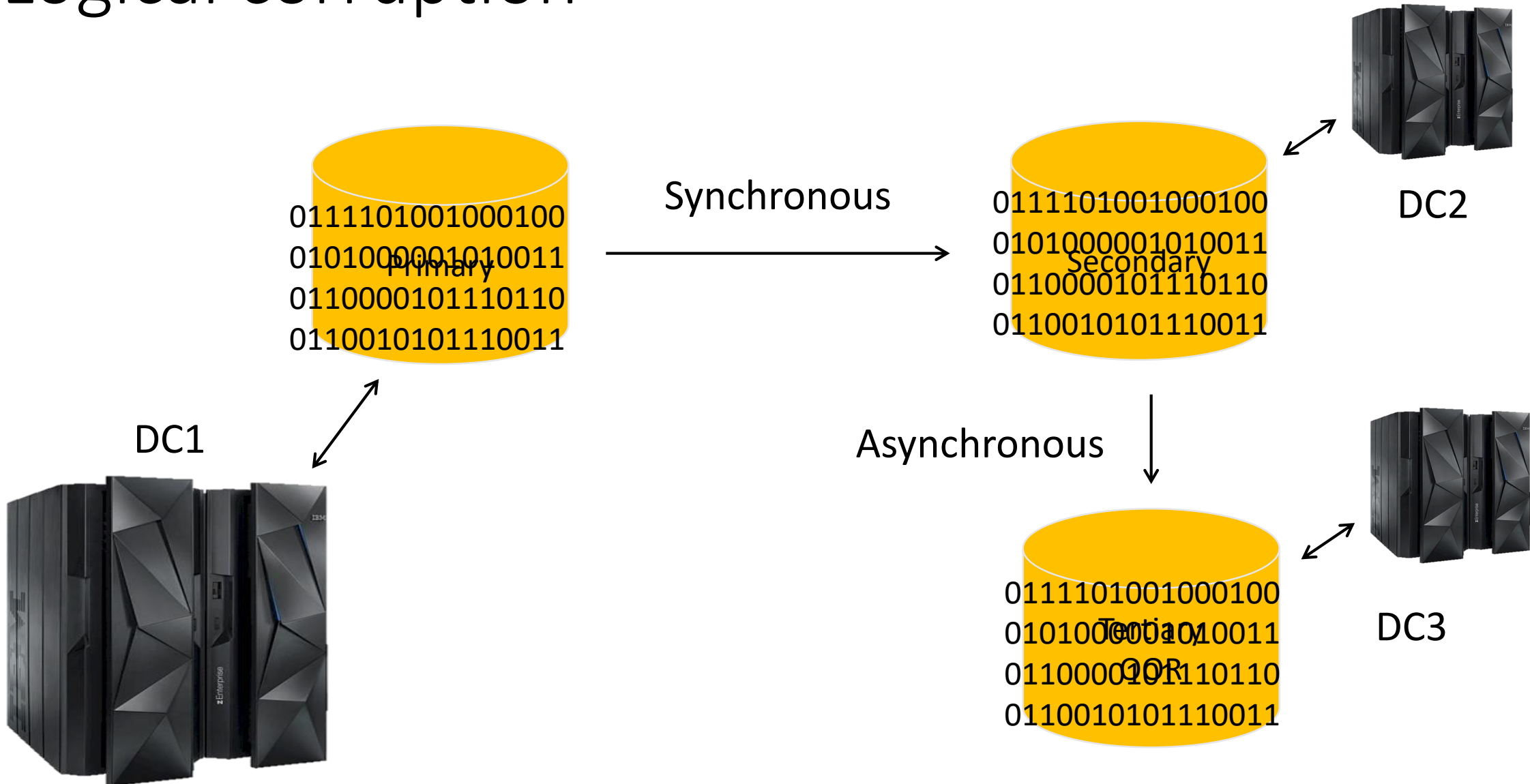
# Logical vs physical data recovery



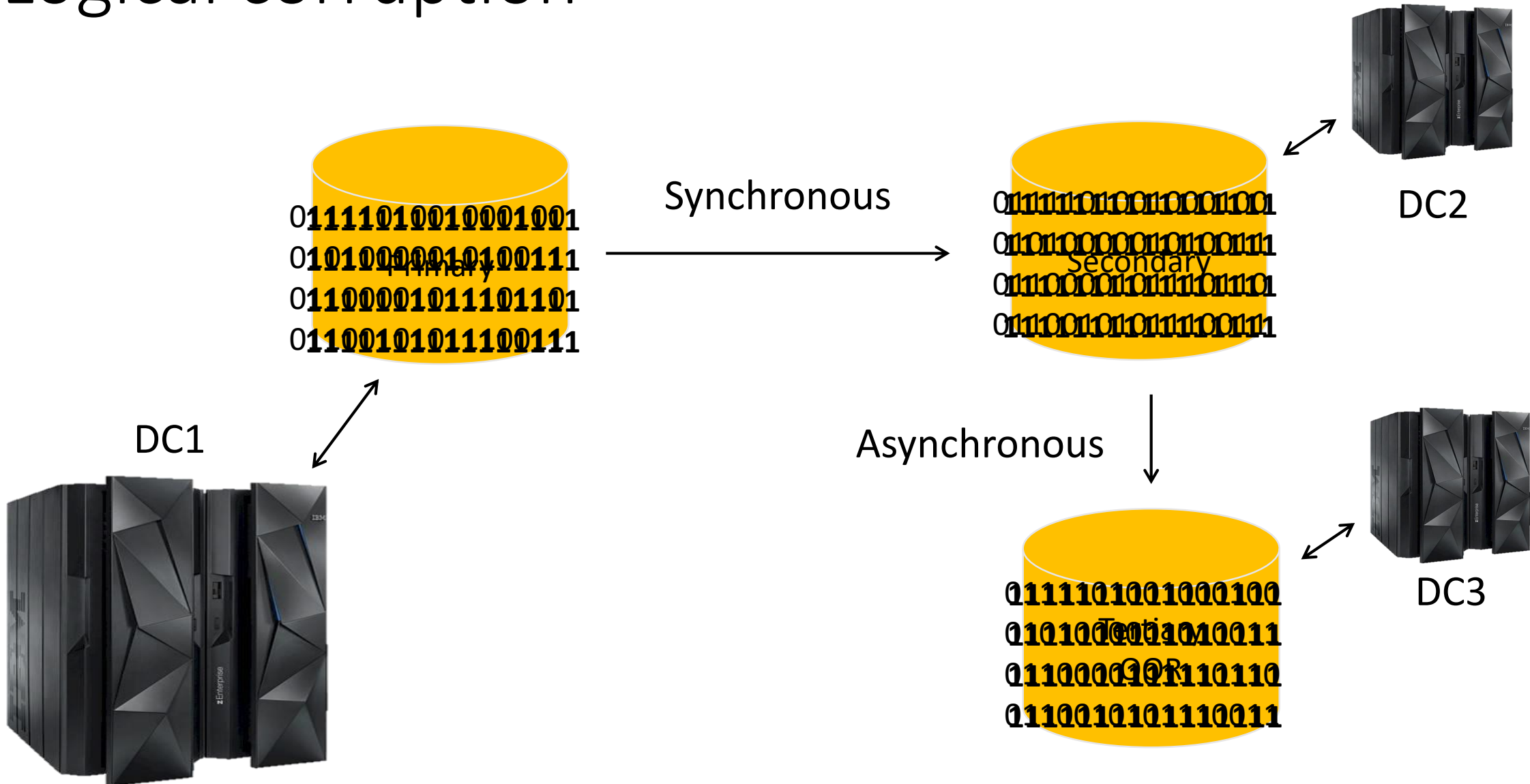
# Physical recovery



# Logical corruption

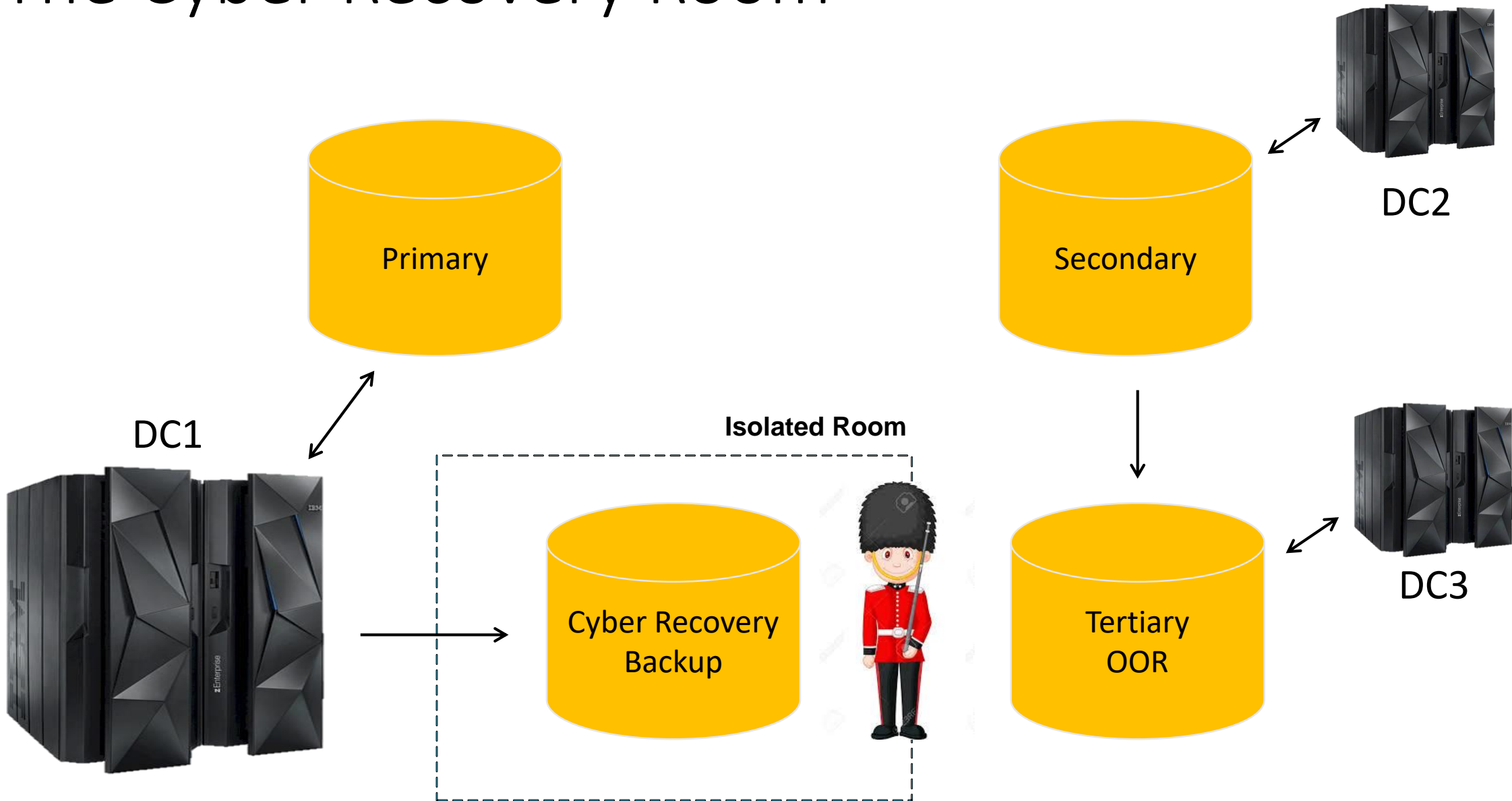


# Logical corruption





# The Cyber Recovery Room



# Cyber RECOVERY IS NOT TRADITIONAL BC/DR

WHY YOU NEED BOTH a Cyber AND A Disaster Recovery SOLUTION

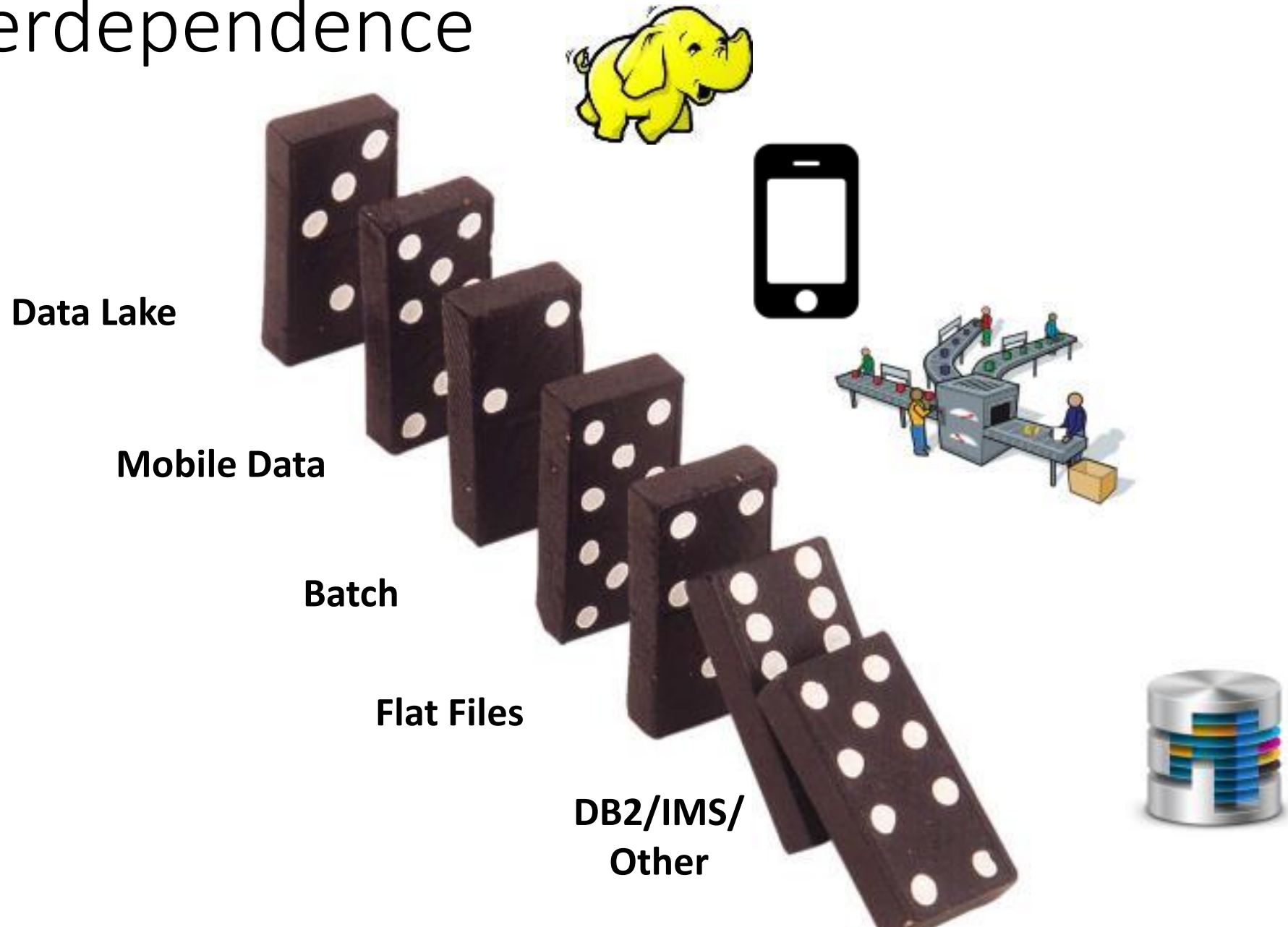
- **Cyber Recovery Systems are Isolated**
  - An isolated data center environment that is disconnected from the network and restricted from users other than those with proper clearance.
- **Data Copies Periodically Scheduled**
  - Software to export data copies to targets in the cyber recovery area.
- **Integrity Checking & Alerting**
  - Workflows to stage copied data in the cyber recovery zone and perform periodic integrity checks
- **Recovery & Remediation**
  - Procedures to perform recovery / remediation after an incident.

# Storage Hardware to the Rescue!



# Why take a storage hardware based approach?

## Data interdependence



# SnapVX and zDP

# Incorporate snaps for data copies

## New TimeFinder SnapVX™



### REDUCED IMPACT

- Target-less Snapshots

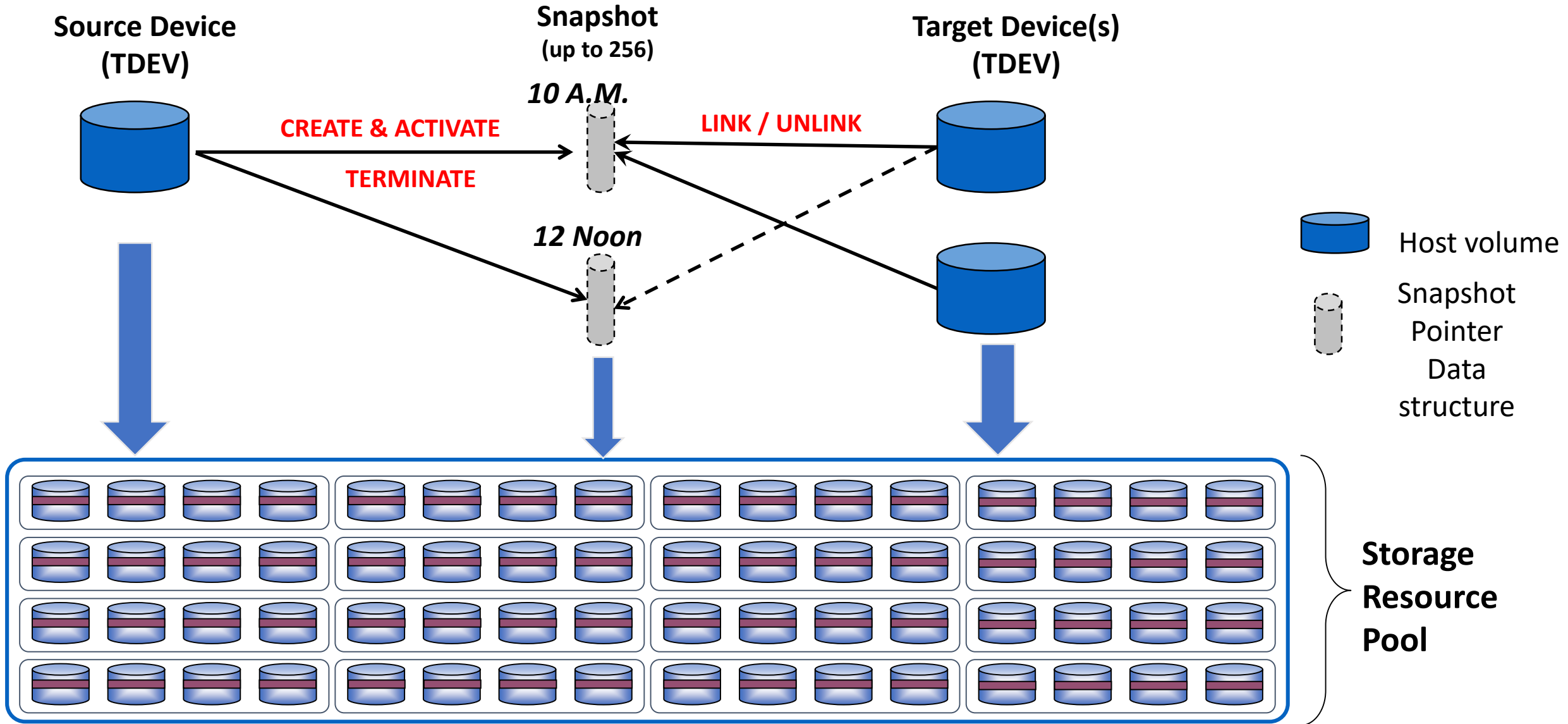
### INCREASED AGILITY

- Up to 256 Snapshots per source
- Up to 1024 Linked Targets (snaps and/or clones) per source

### EASE OF USE

- User-defined name/version number
- Automatic expiration if desired
- Secure Snapshots

# TimeFinder SnapVX – pointer-based snaps



# zDP: Data Protector for Z Systems

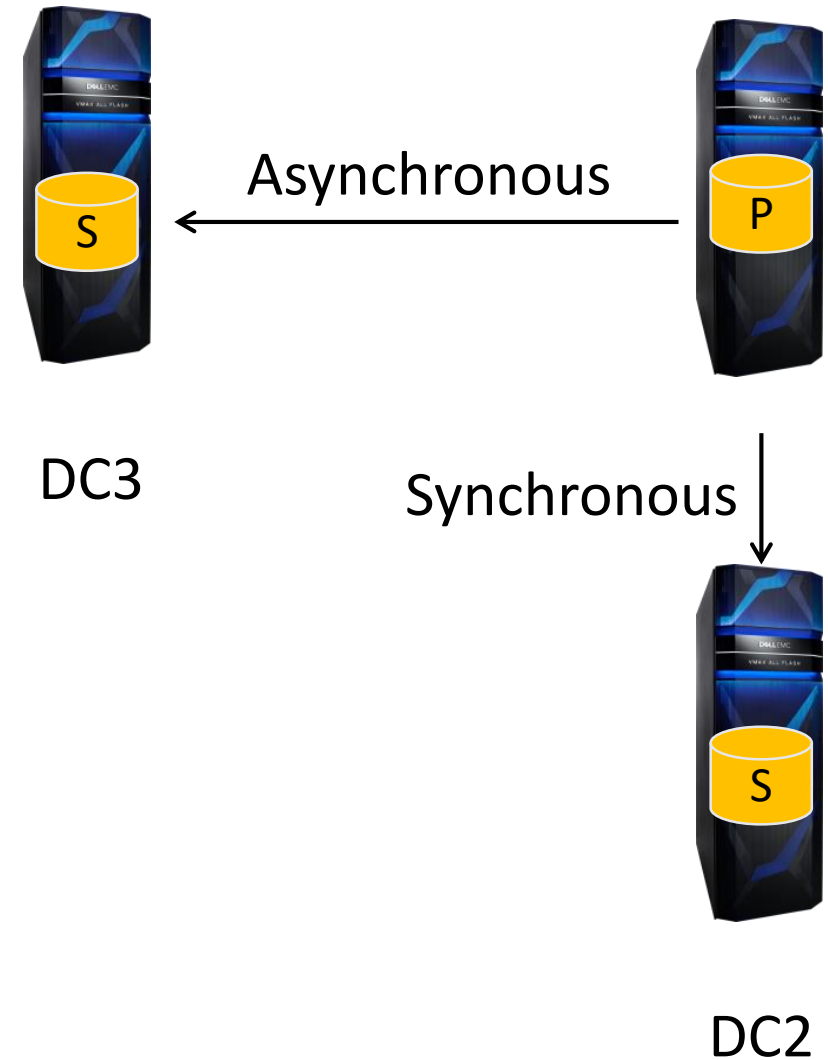
- A z/OS-based solution that automates SnapVX snapshot creation/deletion
- Enables rapid recovery from a spectrum of risks to data
  - Processing error
  - Human error
  - Malicious intent
- Think: 'a time machine for the mainframe'





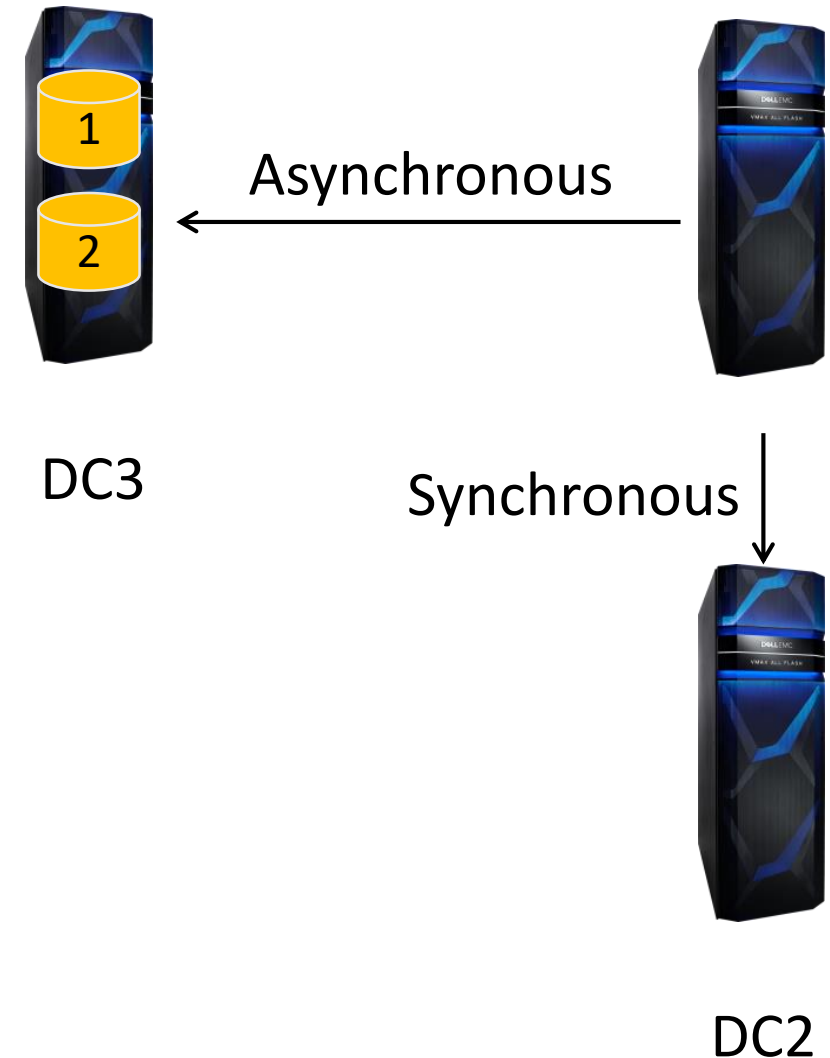
# Why zDP? – logical vs physical protection

- Replication solutions focus on the physical:
  - **“availability with data integrity”**
  - Planned and Unplanned outage events
  - Multiple copies
  - EVERYTHING gets physically replicated
    - Even the logical corruptions!



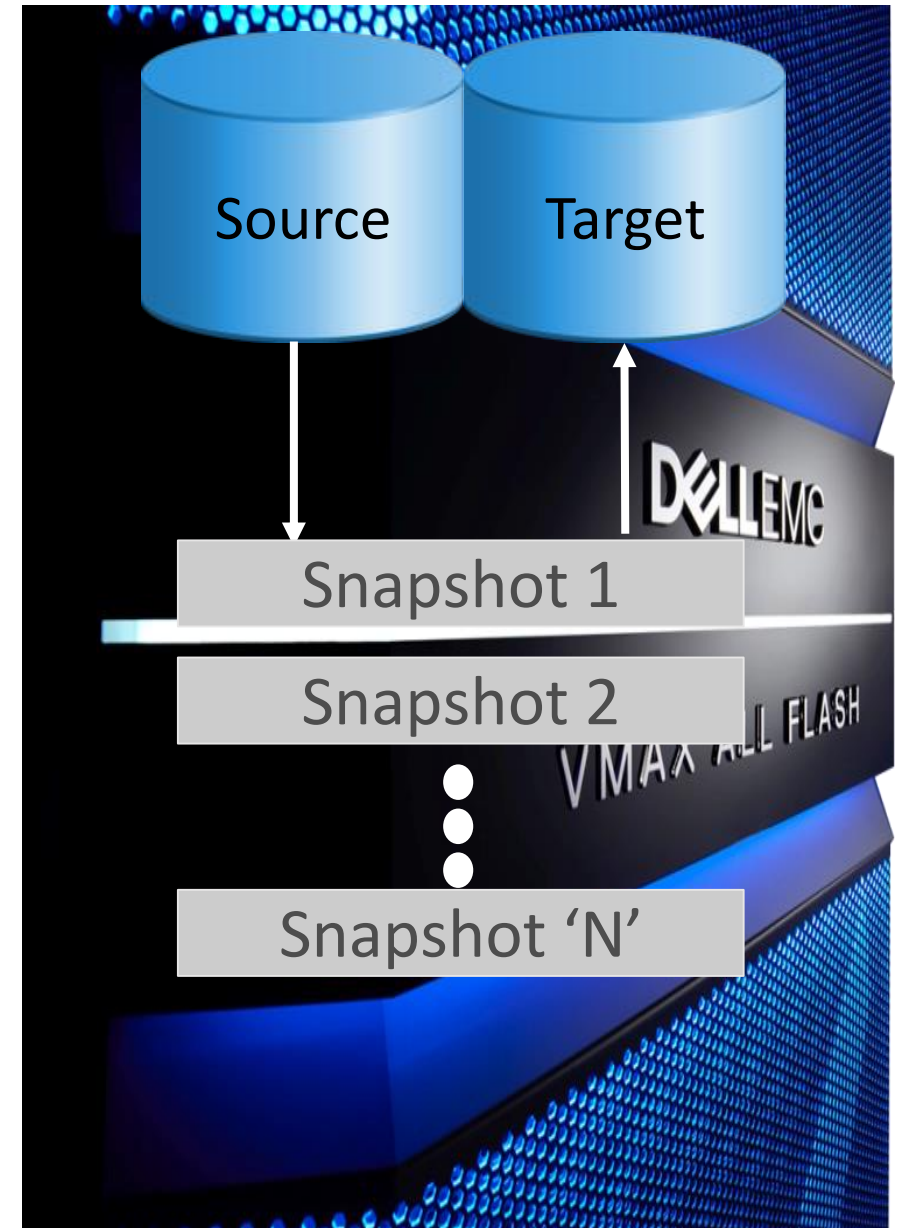
# Why zDP? – logical vs physical protection

- Replication solutions focus the physical: **“availability with data integrity”**
  - Planned and Unplanned outage events
  - Multiple copies
  - EVERYTHING gets physically replicated
    - Even the logical corruptions!
- Today– 1 additional full PIT copy
  - Copy 1: near real time
  - Copy 2: new PIT created every 24 hrs.
  - 24 hours to find corruption
  - Up to 24 hours of data loss

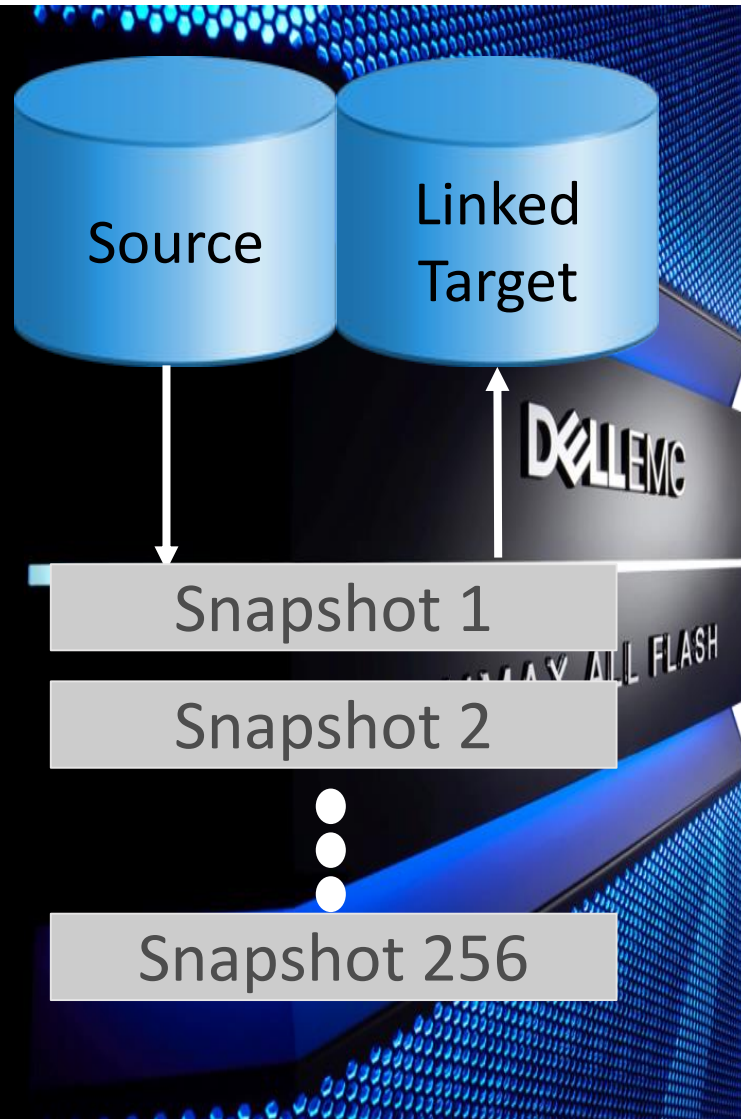


# Why zDP? – logical protection

- zDP focuses on the logical:
  - **“recovery from loss of data integrity”**
    - Continual consistent point in time copy creation
    - Automated
    - Selectable recovery points
- Brings Point in Time recovery capability to database and non-database systems
- Provides applications with recovery capability when not ‘designed-in’
- Provides cross-application recovery point
- Supports both FBA and CKD data

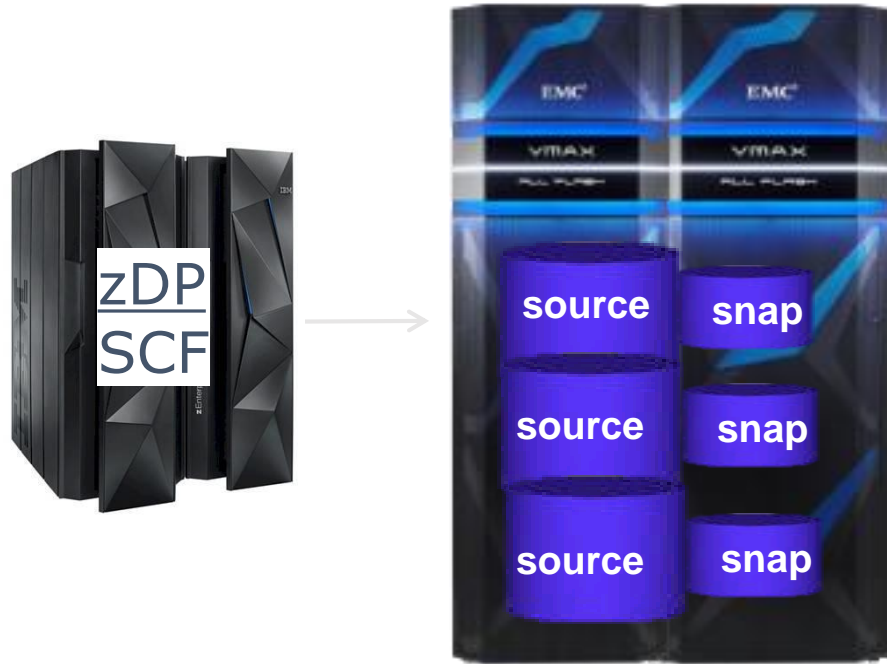


# zDP summary



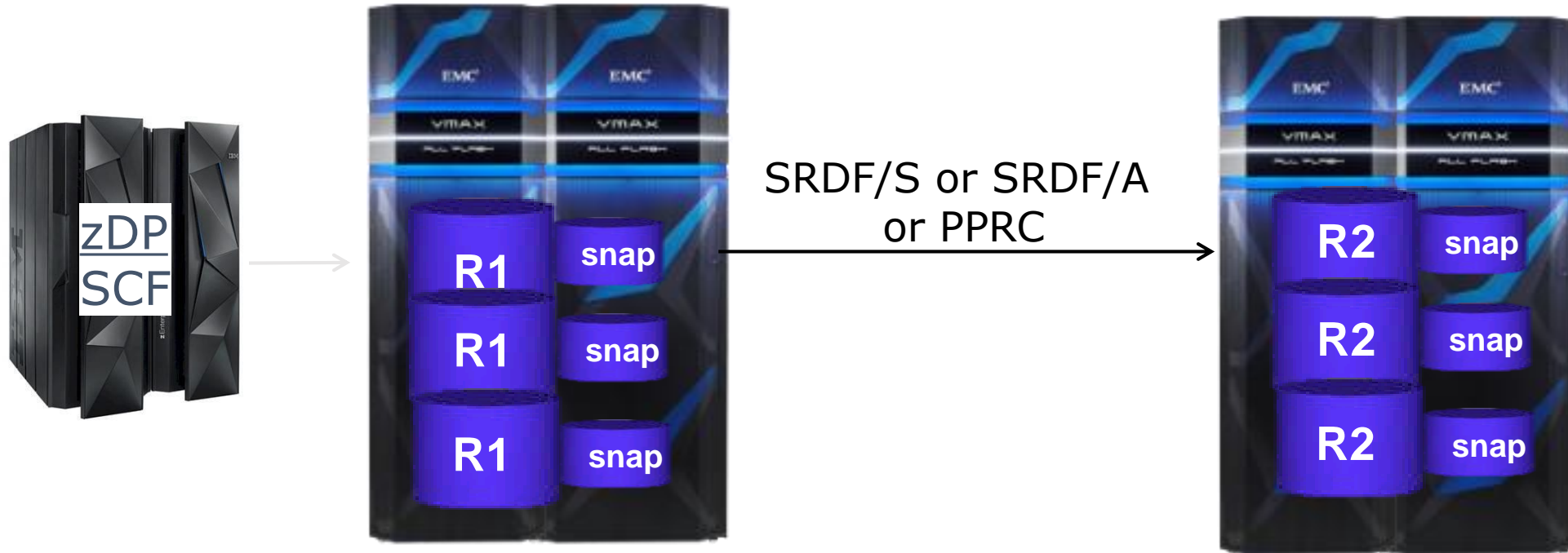
- Host automation solution
  - Frequent creation/deletion of snapshots
  - Benefit: Fast recovery from logical corruption
- Features at-a-glance
  - Up to 144X more recovery capability compared to a daily snapshot (10 min intervals)
  - Keep up to 256 versions of each volume
  - Select snapshots to LINK by timestamp
  - Automatic 'roll-off' of aged snapshots
  - Space estimation and monitoring
  - Consistent scale (32,000 volumes)

# zDP – deployment options



zDP supports snapshot creation:  
Locally attached to VMAX3

# zDP – deployment options



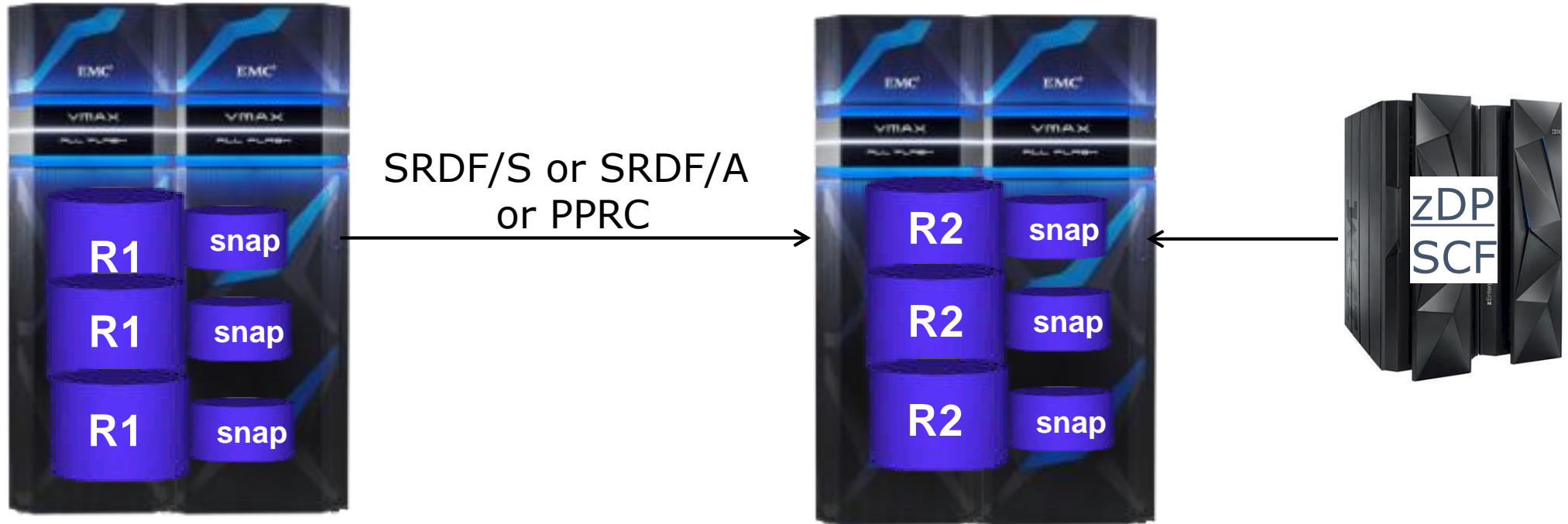
zDP supports snapshot creation in:

Locally attached VMAX3

Remote to VMAX3 via SRDF/S or SRDF/A (up to 4 hops)

R1 array can be VMAX2 for sending SnapVX commands to a VMAX3 for remote execution

# zDP – deployment options



## zDP supports snapshot creation in:

Locally attached VMAX3

Remote to VMAX3 via SRDF/S or SRDF/A (up to 4 hops)

R1 array can be VMAX2 or VMAX3

Direct attached to SRDF target array

# zDP Structures and Operations

- Version Data Group (Source Volumes)
  - DEFINE, DELETE, QUERY, MODIFY, ADD/REMOVE
- Target Set (Target Volumes for Linking)
  - DEFINE, DELETE, QUERY, MODIFY, ADD/REMOVE
- SNAPSET (Snapshots of VDG)
  - QUERY, LINK, UNLINK, TERMINATE
- Operations
  - START,STOP,PAUSE,RESUME
  - Modify
  - Set Persistent
  - Set Secure
  - Set SMF



# zDP XFACILIT RESOURCES

Function	Class	Resource	Attribute
Start	XFACILIT	EMC.ADMIN.CMD.ZDP.START	Update
Stop	XFACILIT	EMC.ADMIN.CMD.ZDP.STOP	Update
Pause	XFACILIT	EMC.ADMIN.CMD.ZDP.PAUSE	Update
Resume	XFACILIT	EMC.ADMIN.CMD.ZDP.RESUME	Update
Query VDG	XFACILIT	EMC.ADMIN.CMD.ZDP.QUERY.VDG	Read
Query target	XFACILIT	EMC.ADMIN.CMD.ZDP.QUERY.TGT	Read
Query status	XFACILIT	EMC.ADMIN.CMD.ZDP.QUERY.STATUS	Read
Query devices	XFACILIT	EMC.ADMIN.CMD.ZDP.QUERY.DEVICES	Read
Query snapshot	XFACILIT	EMC.ADMIN.CMD.ZDP.QUERY.SNAPSHOT	Read
Define VDG	XFACILIT	EMC.ADMIN.CMD.ZDP.DEFINE	Update
Define target	XFACILIT	EMC.ADMIN.CMD.ZDP.DEFINE	Update
Delete VDG	XFACILIT	EMC.ADMIN.CMD.ZDP.DELETE	Update
Delete target	XFACILIT	EMC.ADMIN.CMD.ZDP.DELETE	Update
Add device	XFACILIT	EMC.DEVC.12digitserialnumber.ssid.dev# <sup>a</sup>	Update
Remove device	XFACILIT	EMC.DEVC.12digitserialnumber.ssid.dev# <sup>a</sup>	Update

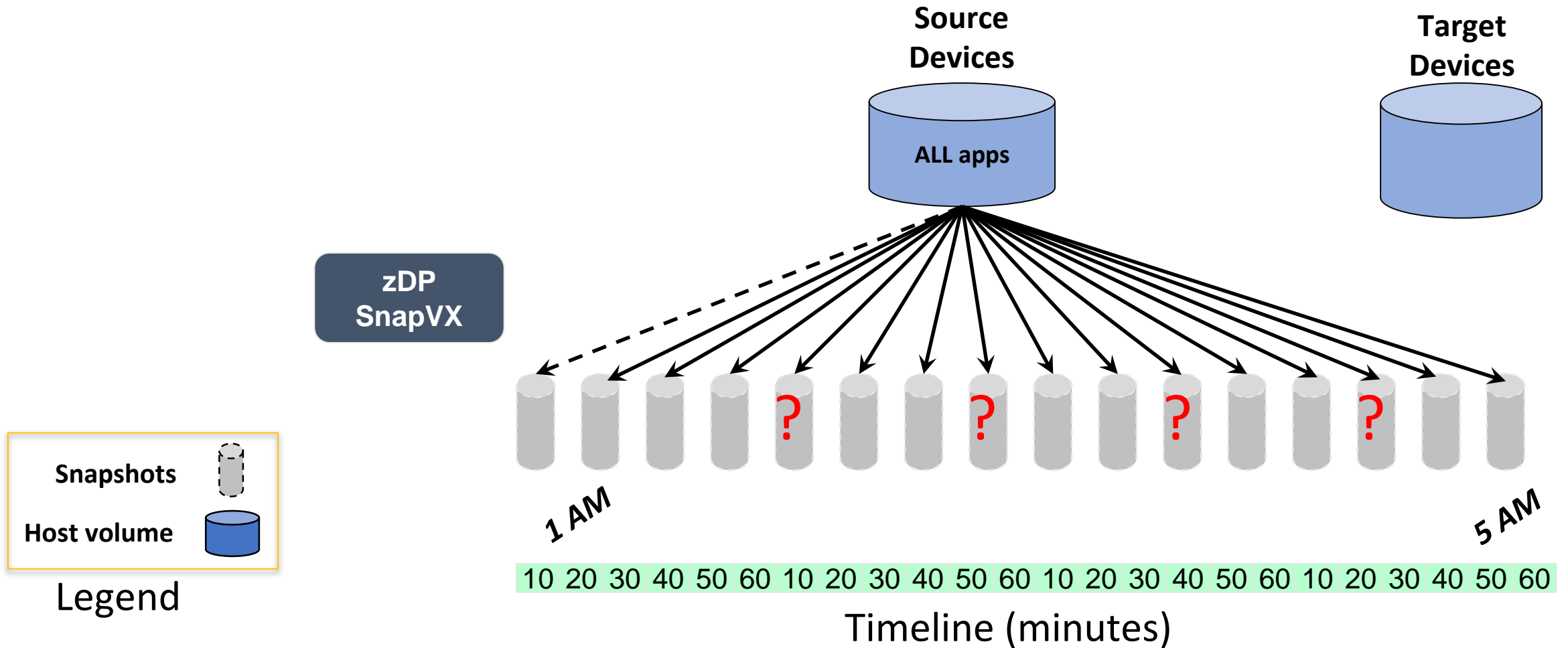
Function	Class	Resource	Attribute
Release device lock	XFACILIT	EMC.ADMIN.CMD.ZDP.RELDLOCK	Update
Modify options	XFACILIT	EMC.ADMIN.CMD.ZDP.MODIFY.OPTIONS	Update
Set up SMF recording	XFACILIT	EMC.ADMIN.CMD.ZDP.MODIFY	Update
Set persistent attribute	XFACILIT	EMC.ADMIN.CMD.ZDP.PERSISTENT	Update
Make snapshot secure	XFACILIT	EMC.ADMIN.CMD.ZDP.SECURE	Update
Terminate snapshot	XFACILIT	EMC.ADMIN.CMD.ZDP.TERMINATE	Update
Terminate snapshot by date/time range	XFACILIT	EMC.ADMIN.CMD.ZDP.TERMINATE.RANGE	Update
Link snapshot	XFACILIT	EMC.ADMIN.CMD.ZDP.LINK	Update
Unlink snapshot	XFACILIT	EMC.ADMIN.CMD.ZDP.UNLINK	Update
Debug	XFACILIT	EMC.ADMIN.CMD.ZDP.DEBUG	Update
Link/Restore	XFACILIT	EMC.ADMIN.CMD.ZDP.BYPASS-ONLINE-CHECK	Read

# Automating Recovery using zDP Snapsets:

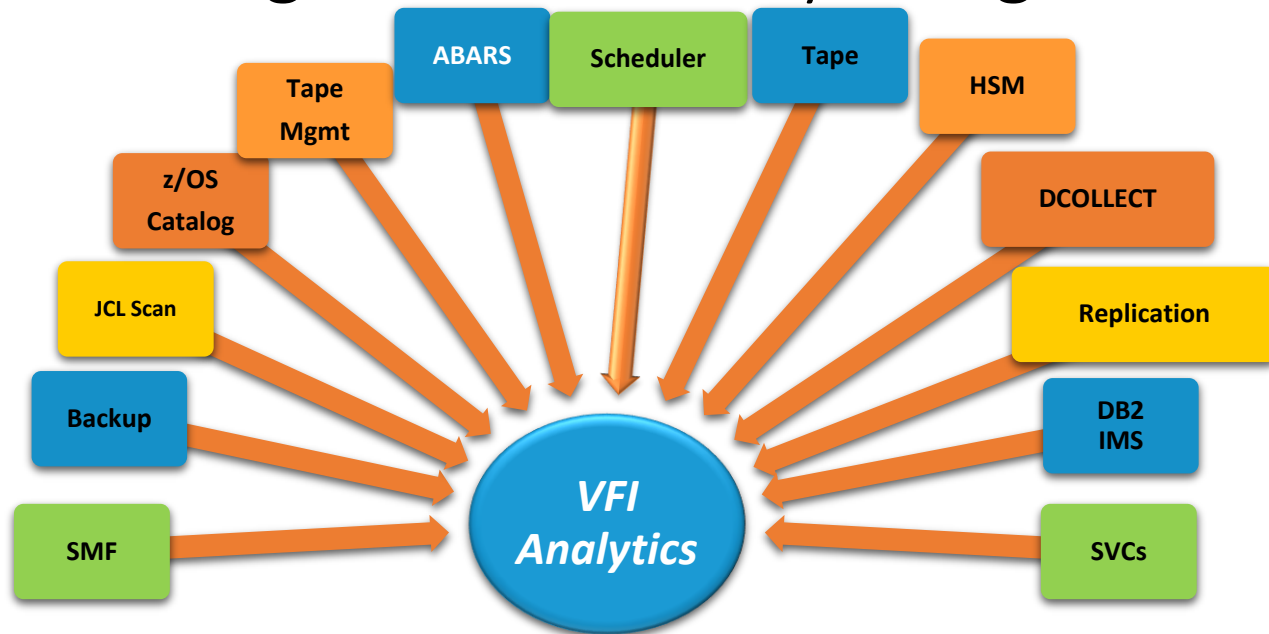


- Vital File Identifier (VFI)
- Timeliner

# VFI / TimeLiner Application Awareness: Enabling faster recovery using zDP



# VFI / TimeLiner Application Awareness: Enabling faster recovery using zDP

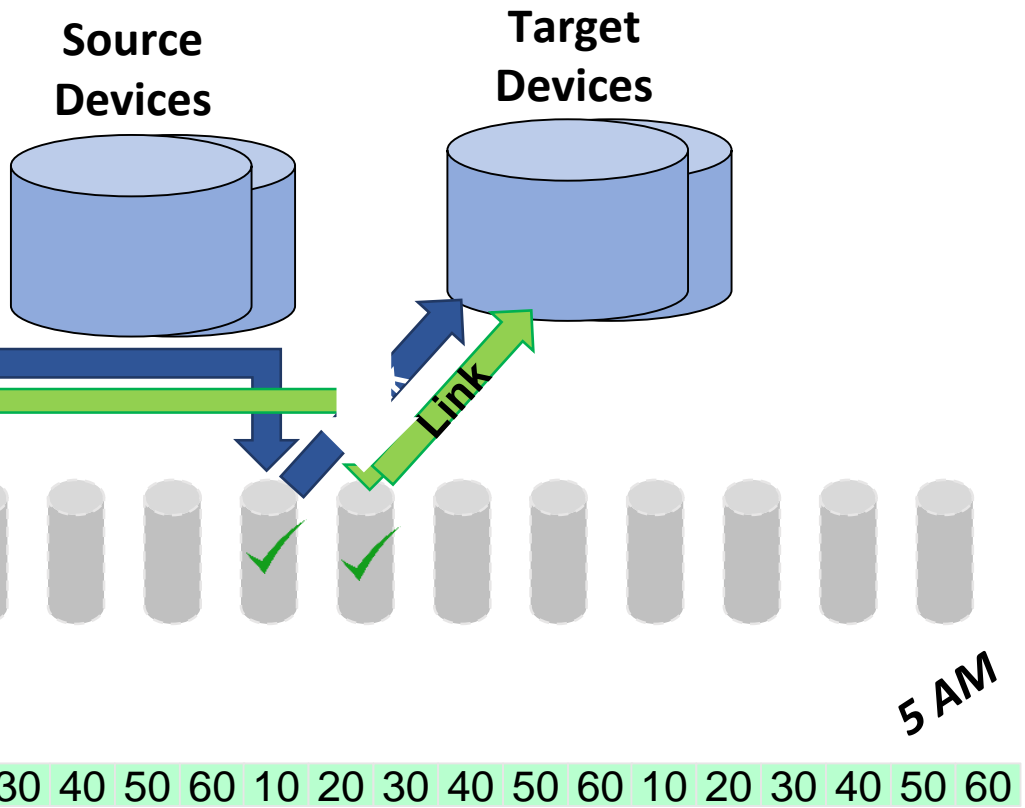


Cascade Impact Report for STEP

Job name : ATMJD010  
 Job id : JOB11235  
 Step name : ATM00UPD  
 Step start : 2017/09/25 02:58:25.36  
 Step end : 2017/09/25 03:08:26.52

Dataset name	Affected D/T	Jobname	Jobid	Stepname
PROD.TESTING.ATM.DDATXS.PS.G0011V00	2017/09/25 02:58:28.46	ATMJD010	JOB11235	ATMJD010
PROD.TESTING.DDA.TXSHST.VSAM	2017/09/25 03:22:26.38	DDAJD004	JOB11259	DDA00ACT

TOTAL DATA SETS IMPACTED: 2



**Snapshots**

**Host volume**

**Legend**

# NIST Cyber Security Framework Whitepaper

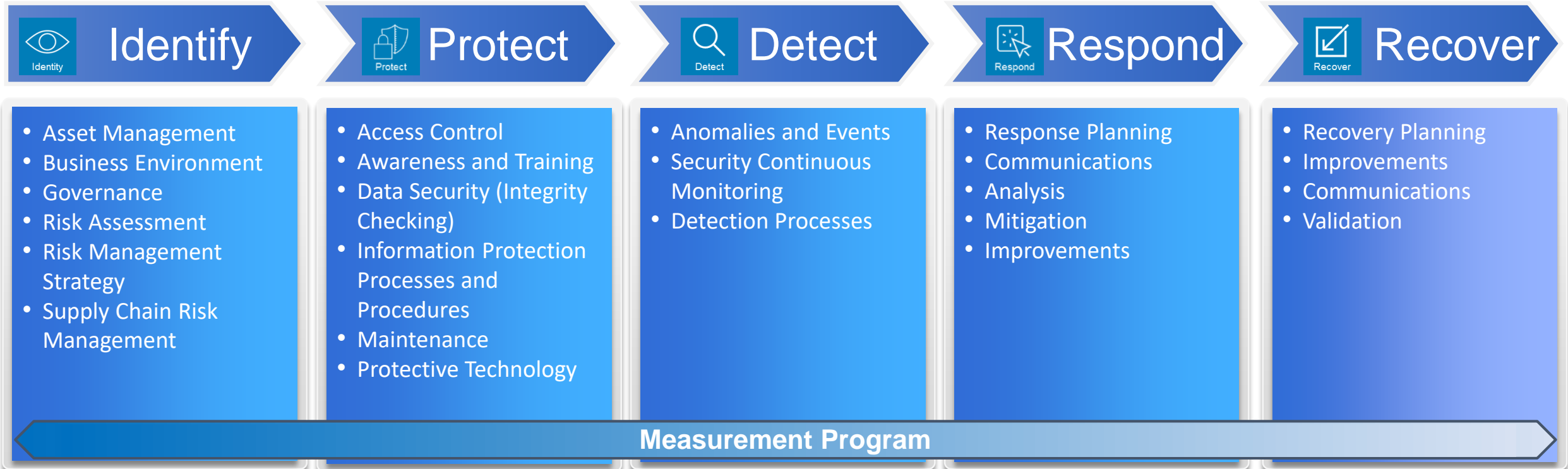
## **Framework for Improving Critical Infrastructure Cybersecurity**

Version 1.1

National Institute of Standards and Technology

April 16, 2018

# NIST Cybersecurity Framework



## Dell Technologies Aligned Solutions and Services

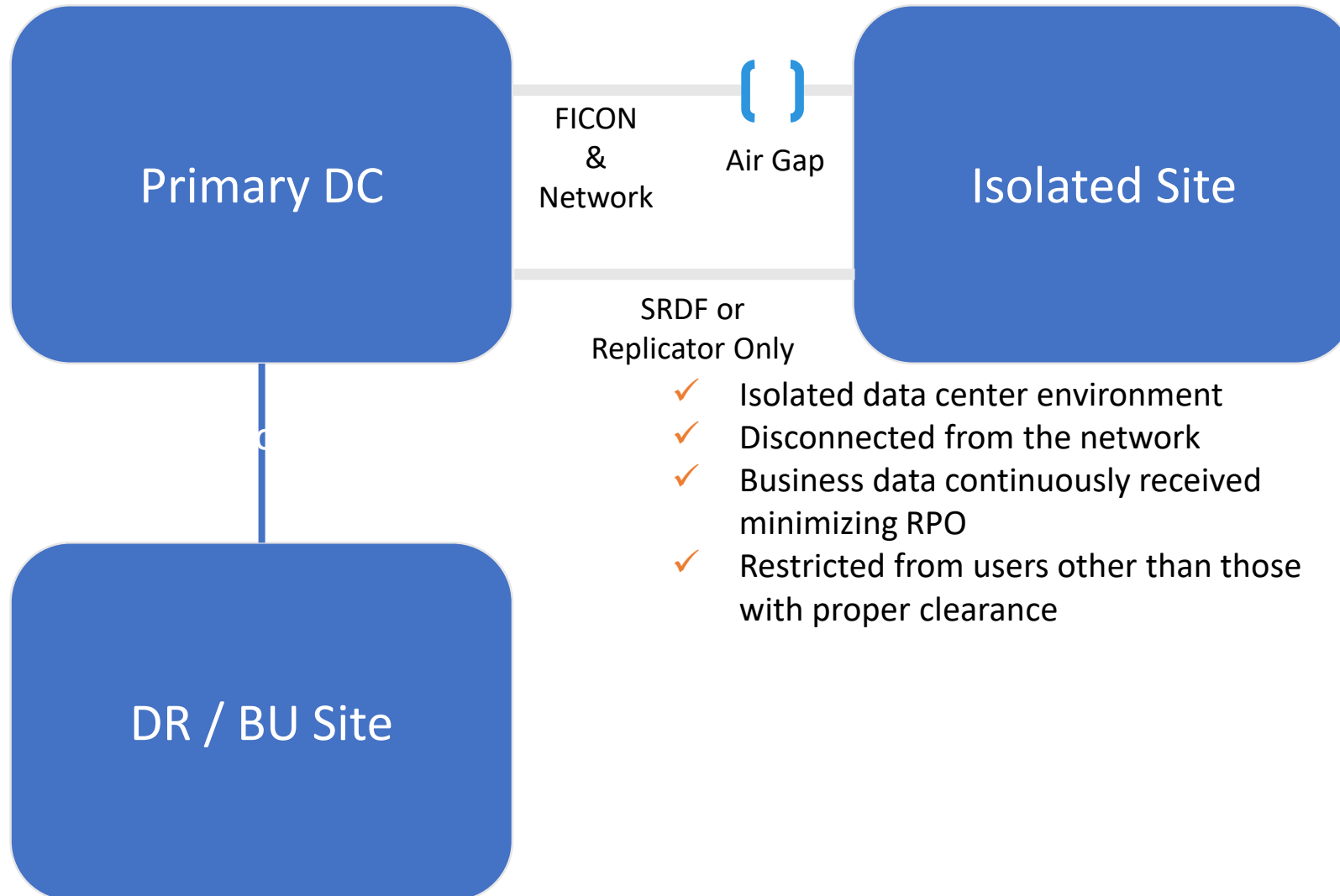
# zDP: What's New?

- Functional Enhancements to zDP in MFE 8.3:
  - Secure Snapsets
    - cannot be deleted via zDP or EMCSNAP
    - are instead deleted by the ucode only at the expiration date, and no longer at the MAX\_SNAPSETS value
  - Copy Once Attribute
    - attribute saves SRP space by including the device only in the first snapset of a VDG
  - Define VDG by RDF Group
    - Allows RDF Group to be used in definition of VDG and Target sets
  - 5 minute minimum Cycle Time

# Example of Z Systems Cyber Recovery



# Mainframe Cyber Recovery solution overview



- ✓ Isolated data center environment
- ✓ Disconnected from the network
- ✓ Business data continuously received minimizing RPO
- ✓ Restricted from users other than those with proper clearance

1

## Planning:

- Business Critical Systems
- RPO/RTO
- Throughput Requirements

2

## Isolation:

- Isolated DC Environment
- Dedicated Link SRDF or Replicator Only
- FICON & Network Air Gap
- Hidden Local Copies that cannot be deleted

3

## Validation:

- Maintain gold copy
- Compare to incoming copy
- Tools application dependent
- Rate of Change
- Sentinel Record Injection

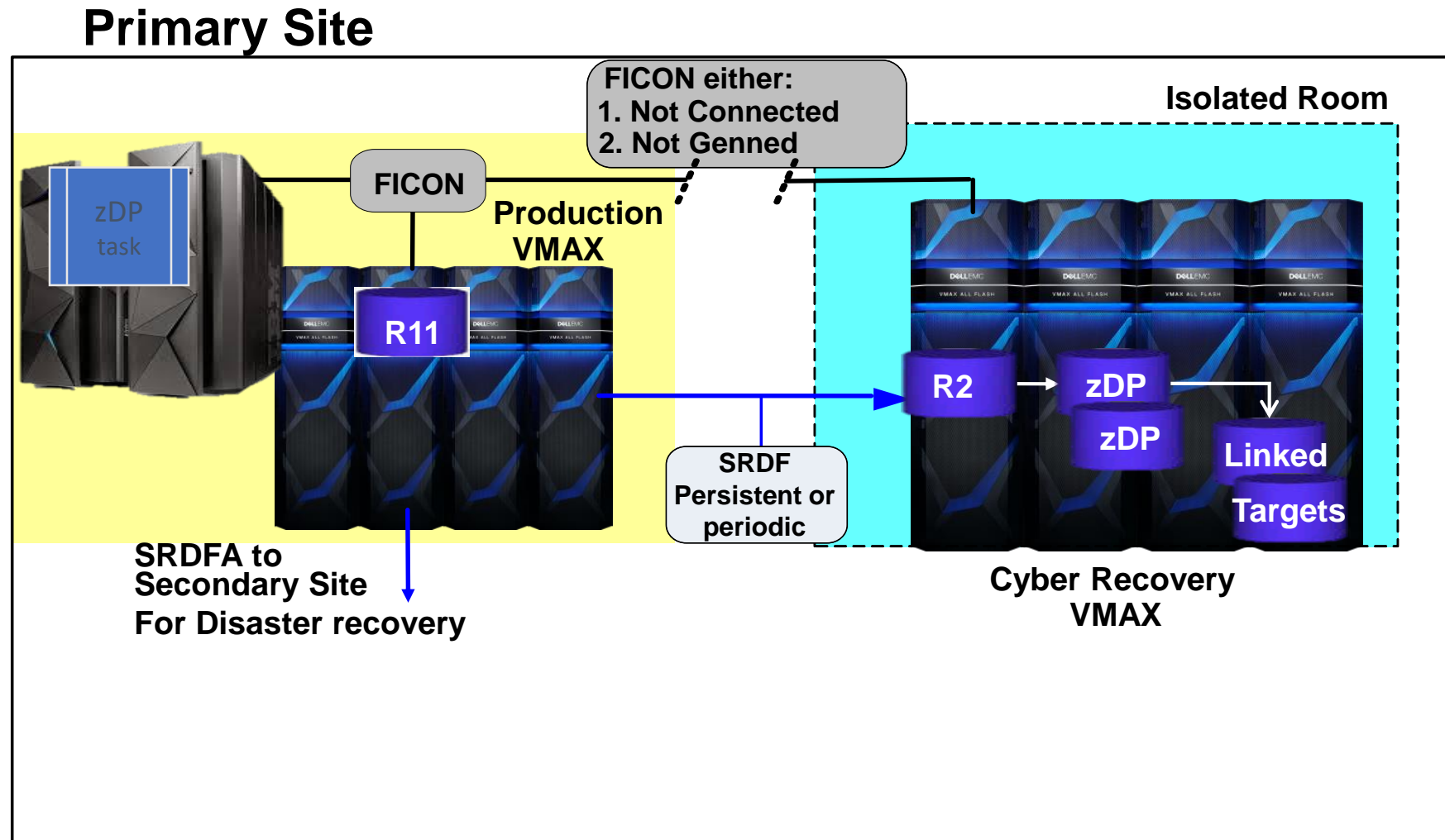
4

## Recovery:

- Standard failback mechanisms
- Additional remediation / validation

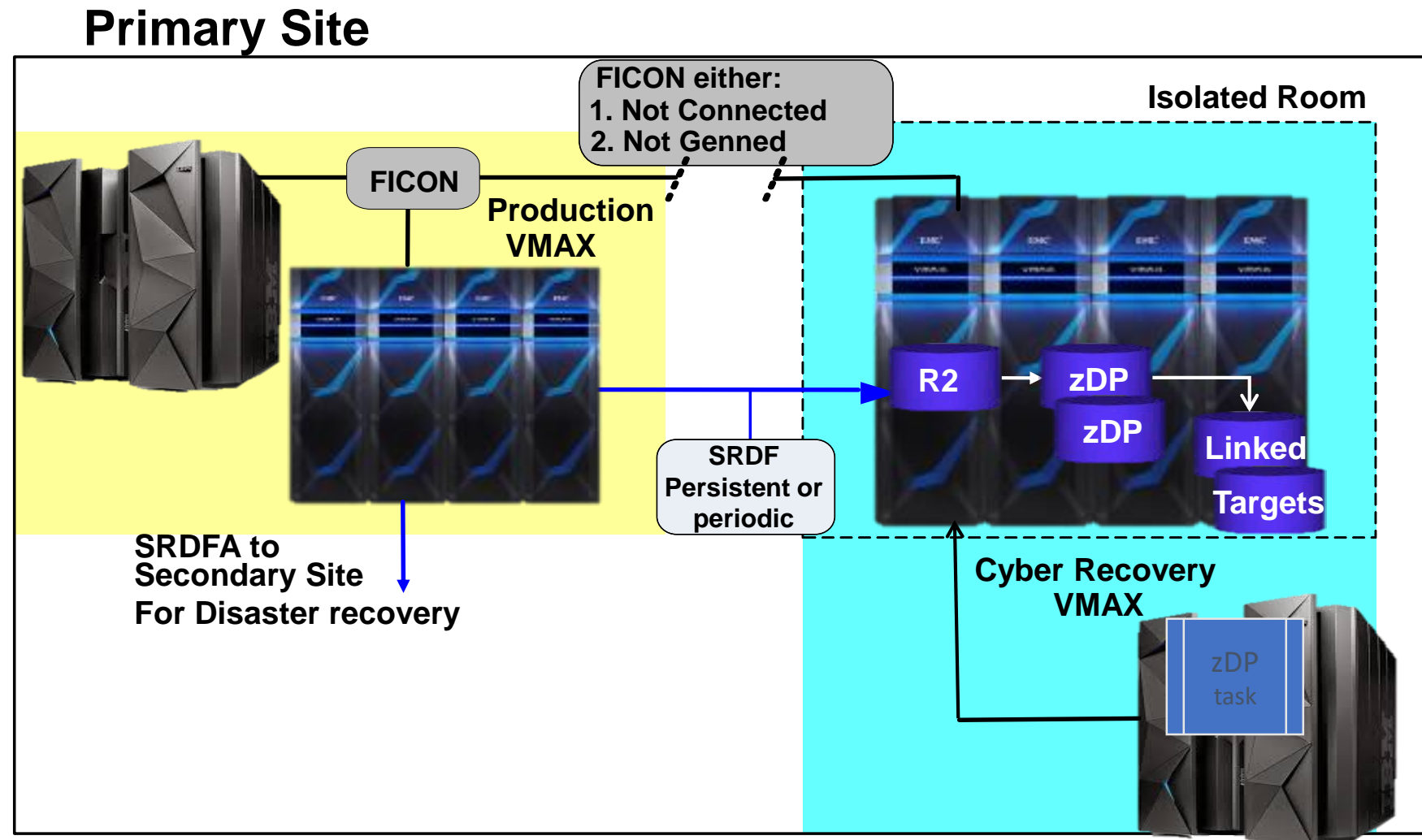
# MF isolated “air-gapped” Cyber Recovery system example

- Preserves PiT copies on physically isolated VMAX
- Isolation from:
  - Personnel
  - Networks
- Ensures recoverability from catastrophic large scale data corruption or deletion
- Enhanced security for PiT copy
  - Secure snapsets

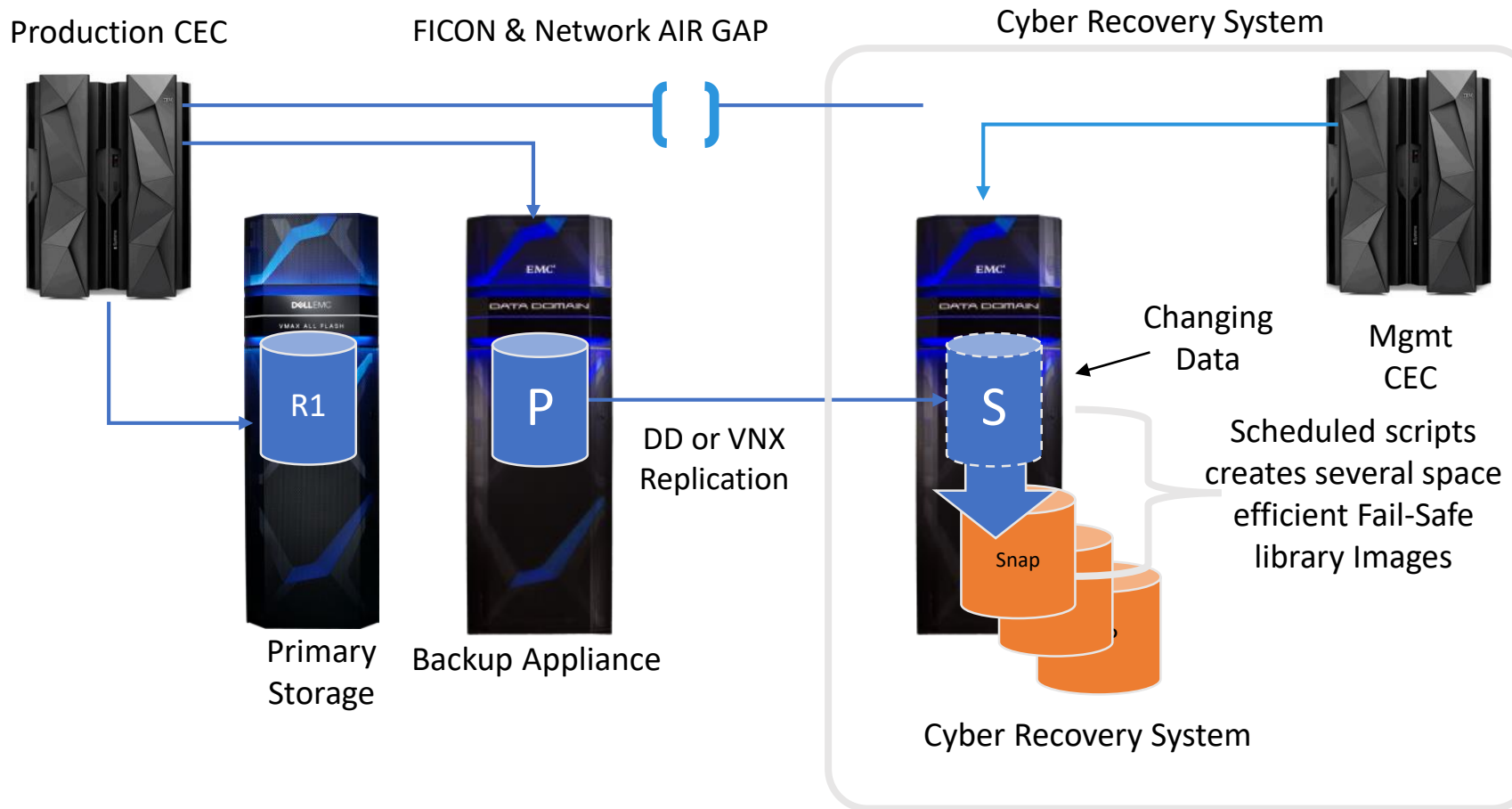


# MF isolated “air-gapped” Cyber Recovery system example

- Preserves PiT copies on physically isolated VMAX
- Isolation from:
  - Personnel
  - Networks
- Ensures recoverability from catastrophic large scale data corruption or deletion
- Enhanced security for PiT copy
  - Secure Snapsets



# DLM Cyber Recovery solution components



- All TCP/IP Sockets Closed on DLM storage except Replicator
- Separate dedicated storage replication ports
- Separate Dedicated Replication Network
- Backup / Archive Volumes / Restore Points
- Instant Access\*\*\*
- Retention Periods / WORM



Cost Effective



RPO = Hours to 1 Day\*



RTO = Hours to Days\*\*

\* Adjustable based on desired security window

\*\* Depends on # of Volumes, Data etc.

\*\*\*Lower Performance

- Can co-exist with and enhance an existing BC/DR Solution
- Tape Data is continuously periodically copied in to IRS environment
- File System Snapshot multiple space efficient Fail-Safe Library images
- Management CEC is "hardwired" to IRS Solution
- Un-addressable Snapshot Copies allow multiple restore points
- Management CEC can be used used to periodically validate data

# Summary

- Recovery from Logical corruption is the next wave of Business Continuity planning
- Both operational errors and malicious attacks are current and emerging threats to data integrity and availability .
- Organizations need to be organized to properly plan and implement their response to these threats
- Tools and procedures must be developed based on perpetual and persistent data copy technologies
- Consider the applicability of Cyber Recovery Solutions for your enterprise

# We want your feedback!

- Please submit your feedback online at ....
  - <http://conferences.gse.org.uk/2018/feedback/nn>
- Paper feedback forms are also available from the Chair person
- This session is **FJ**

