Ransomware protection for your Mainframe Data

Dell EMC

December 2019

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

* By cartoonist John Klossner – May 2016

156 million phishing emails sent WW every day

↓

16 million make it through filters

↓

8 million are opened

↓

800,000 LINKs are click'd

↓

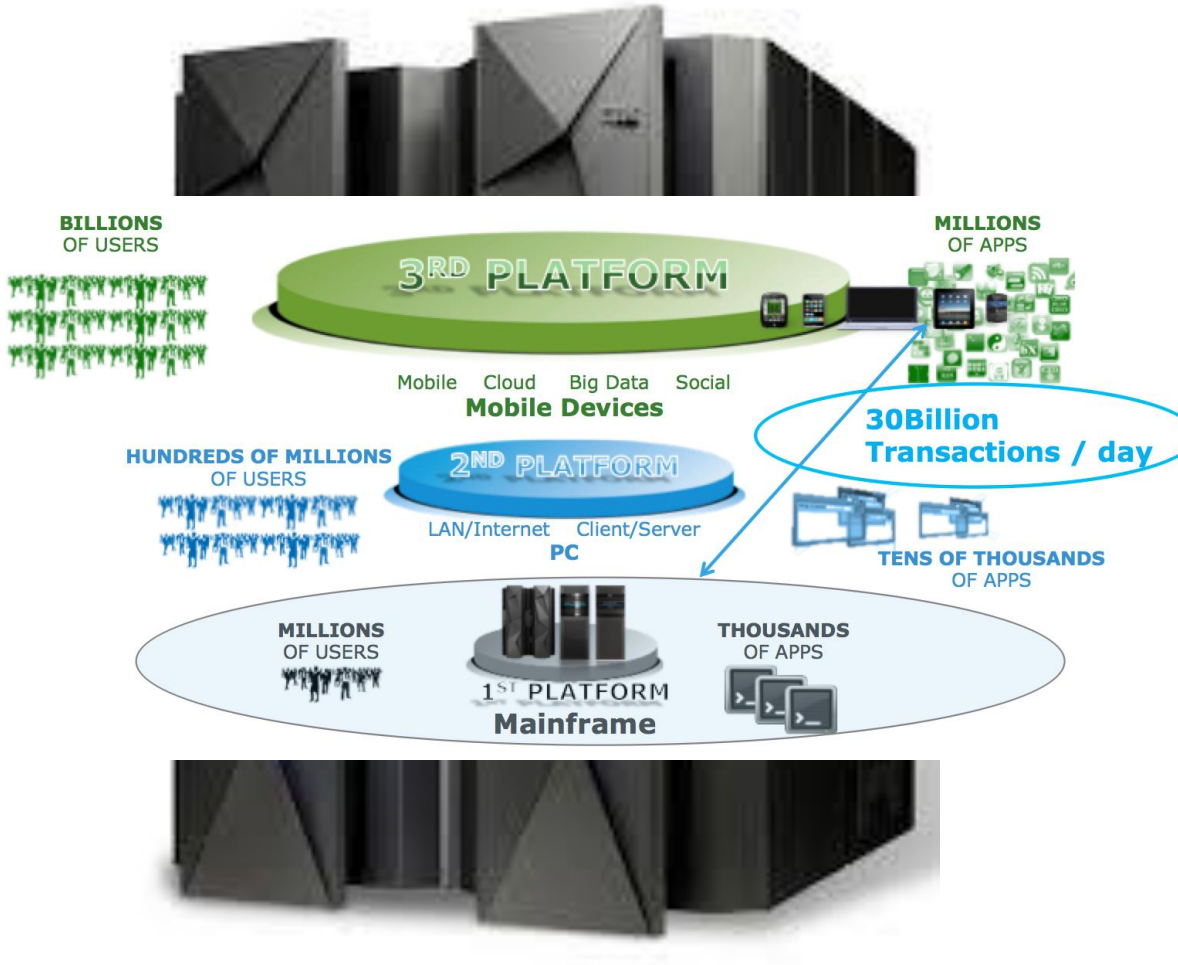
IF 12% click on phishing emails

↓

All it takes is **ONE**

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



Source: 2013 IBM zEnterprise Technology Summit

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.bigendiansmalls.com/files/ransomware_share_2017.mp4

What questions are the board of directors asking?

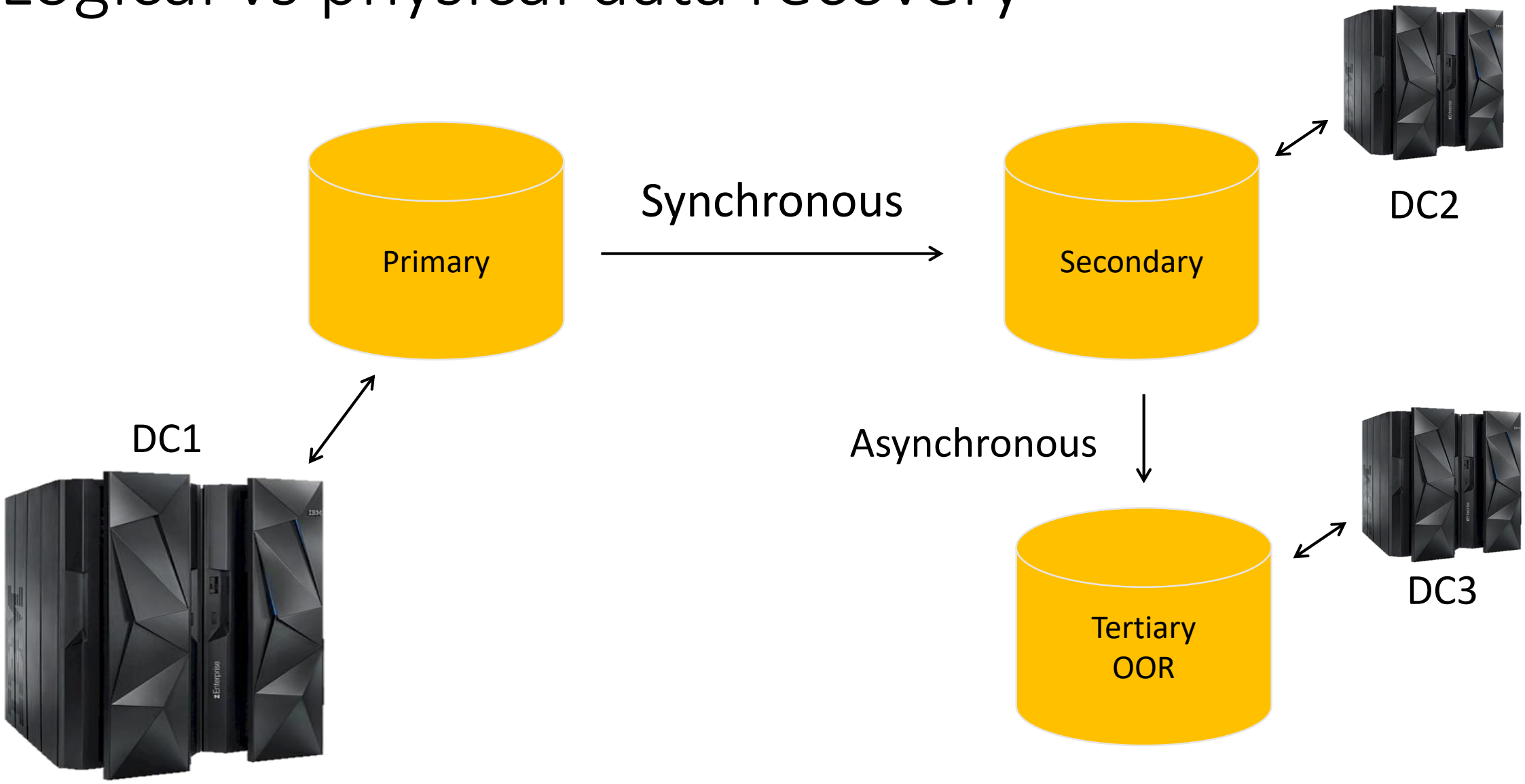
- Are we at risk of a destructive Hacktivist Attack?
- Do we have the cyber security protections in place to guarantee our business is safe?
- What would be the impact to our customers, shareholders, employees if our information was lost ?

- 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?

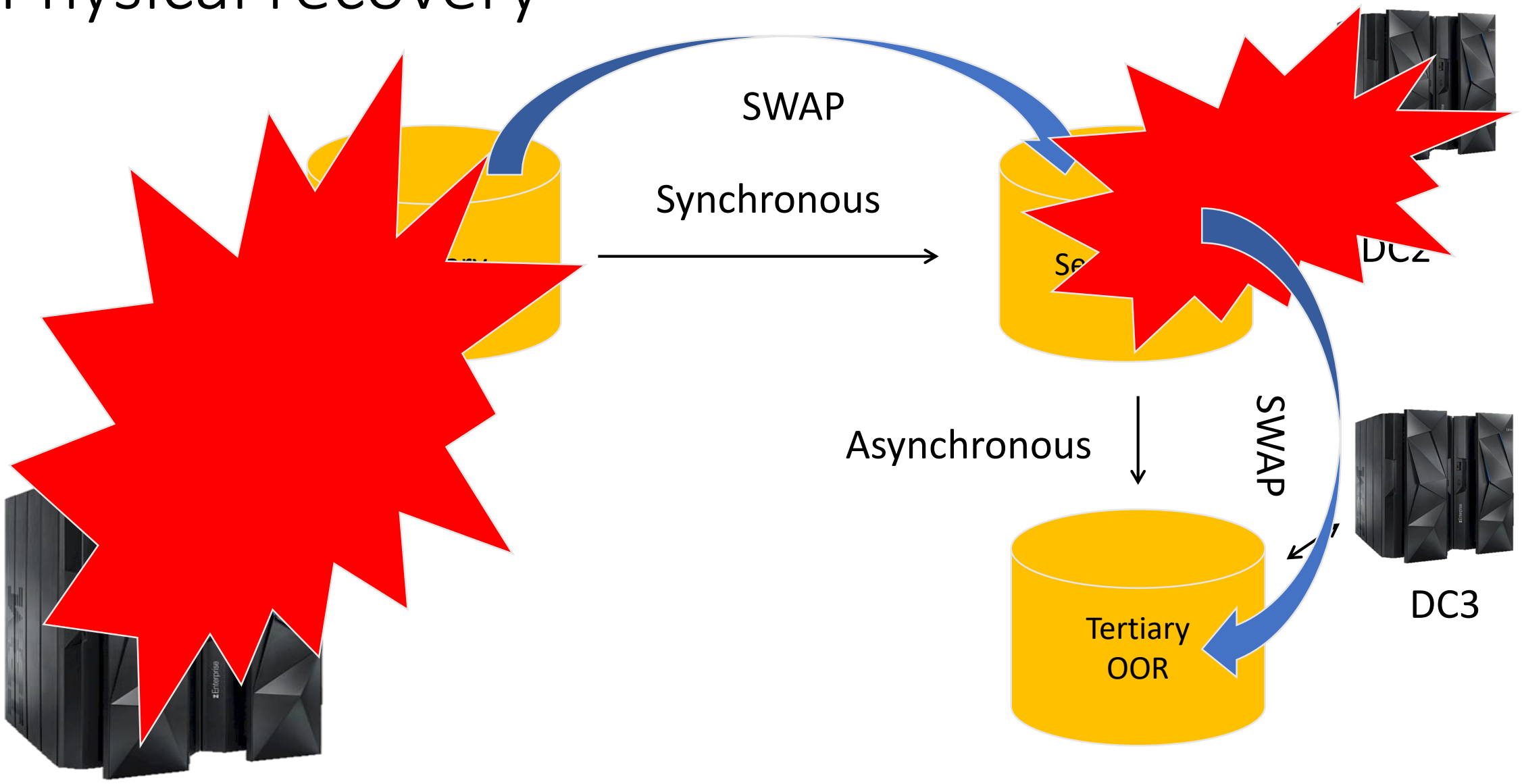
WHO IS PAYING FOR THIS EXTRA PROTECTION??

Physical vs Logical Recovery

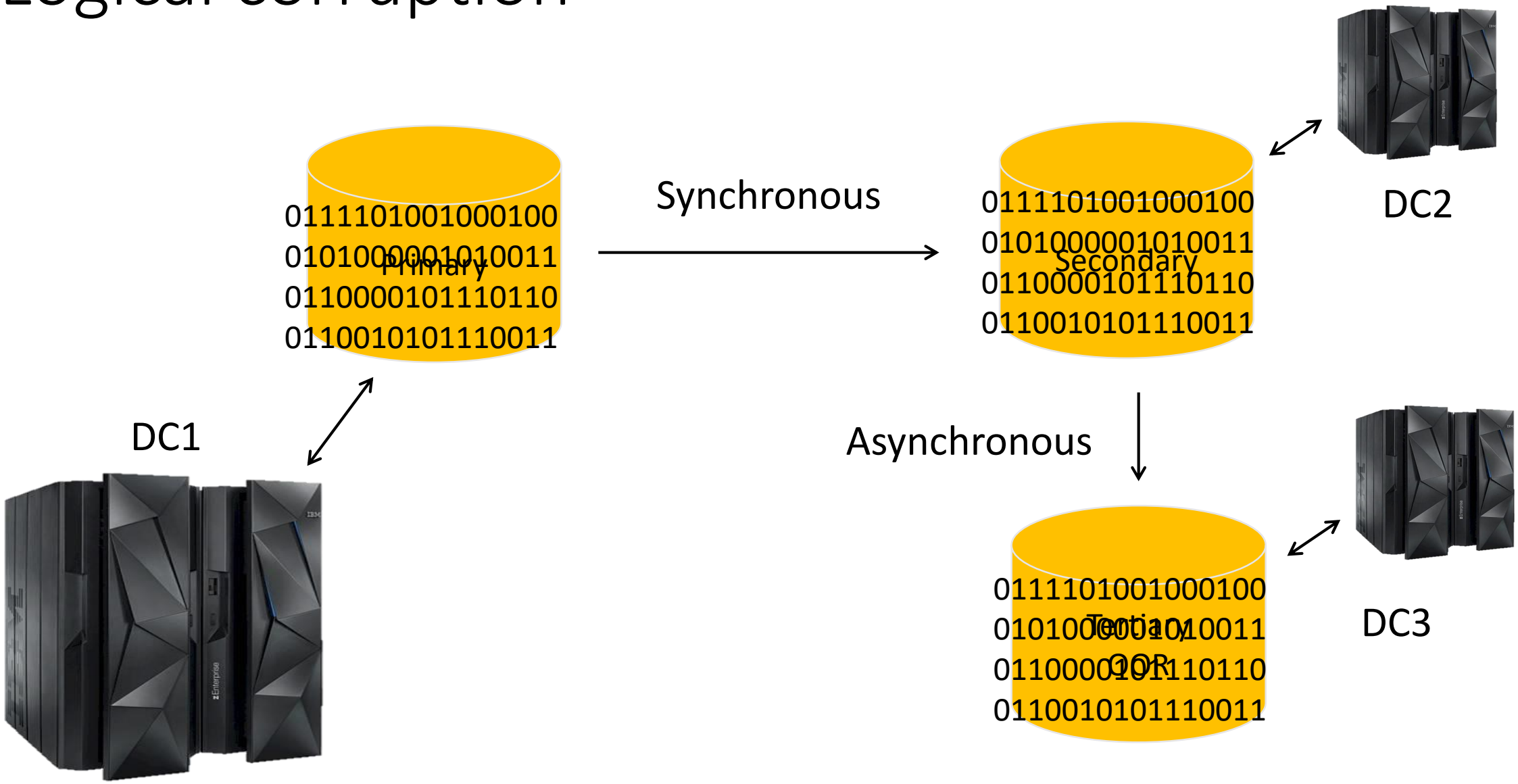
Logical vs physical data recovery



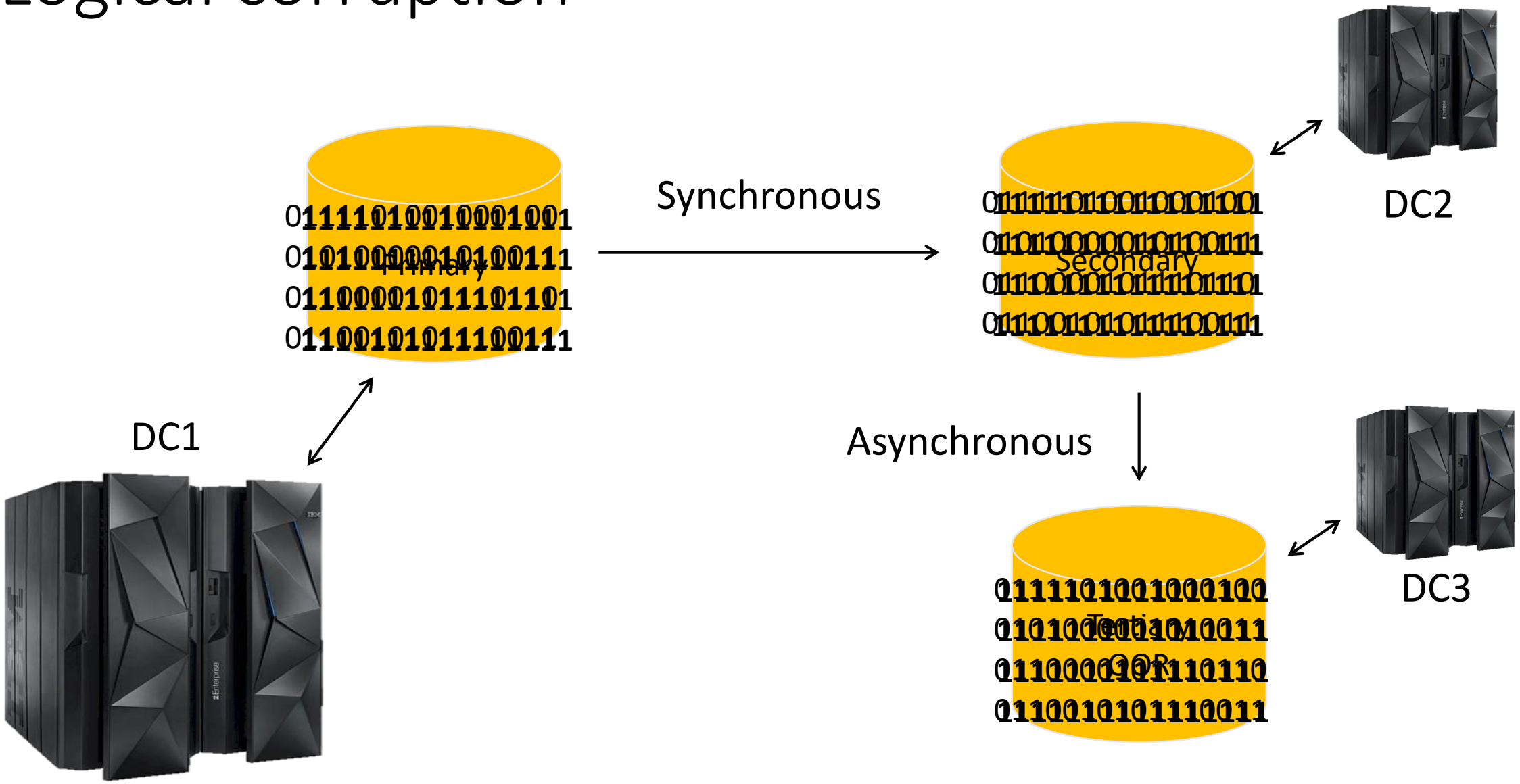
Physical recovery



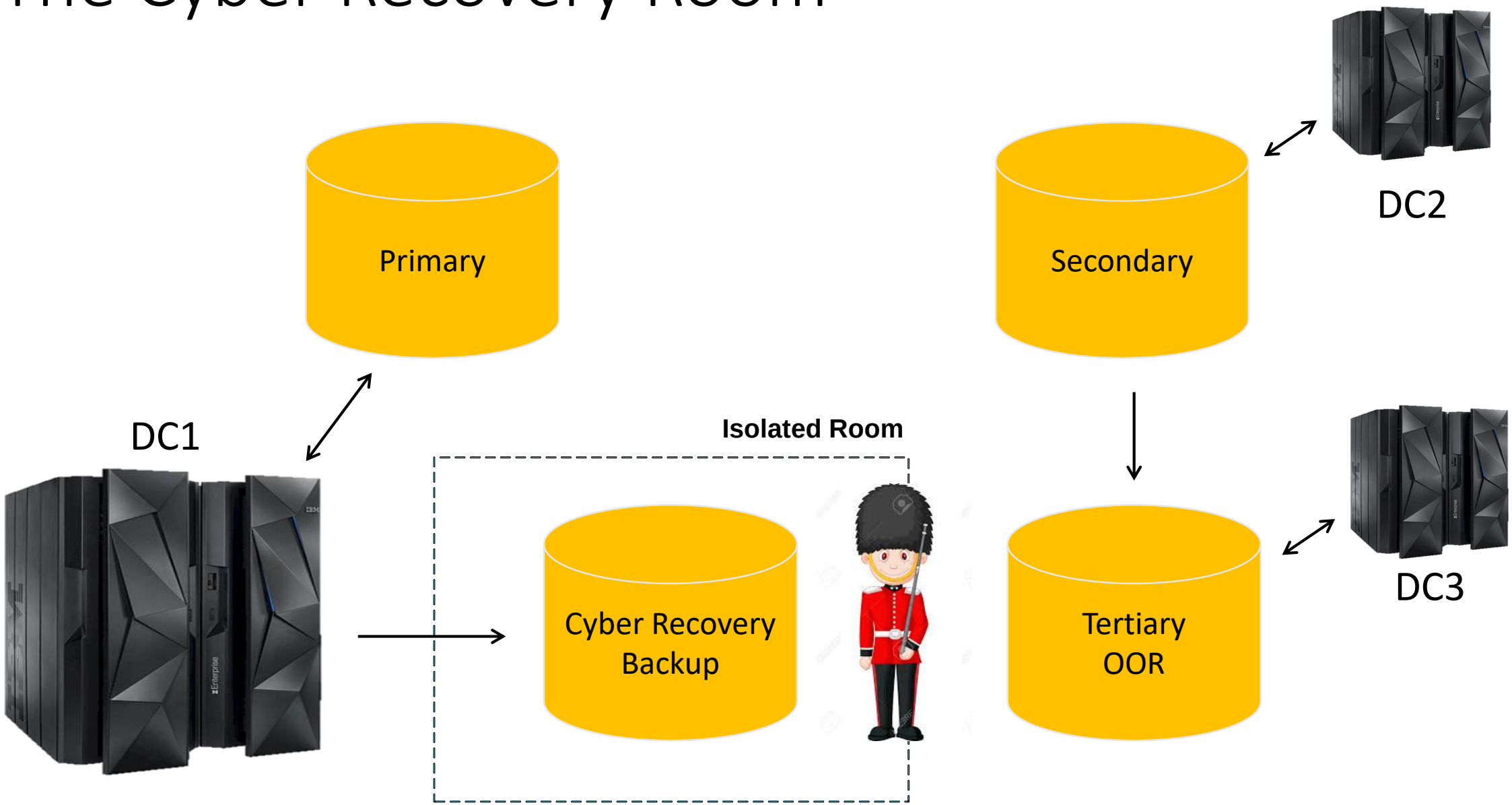
Logical corruption



Logical corruption



The Cyber Recovery Room



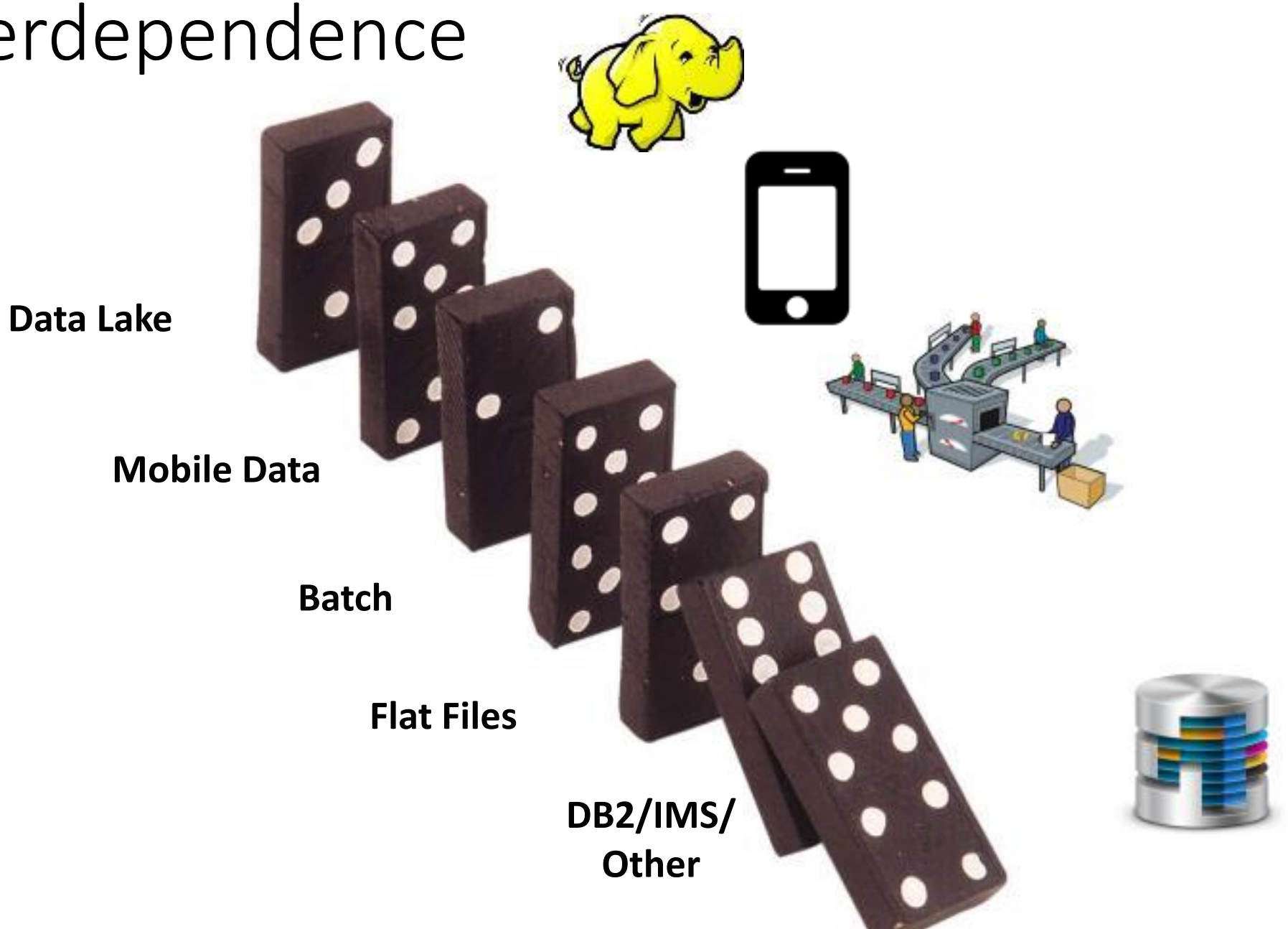
Cyber RECOVERY IS NOT TRADITIONAL BC/DR

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



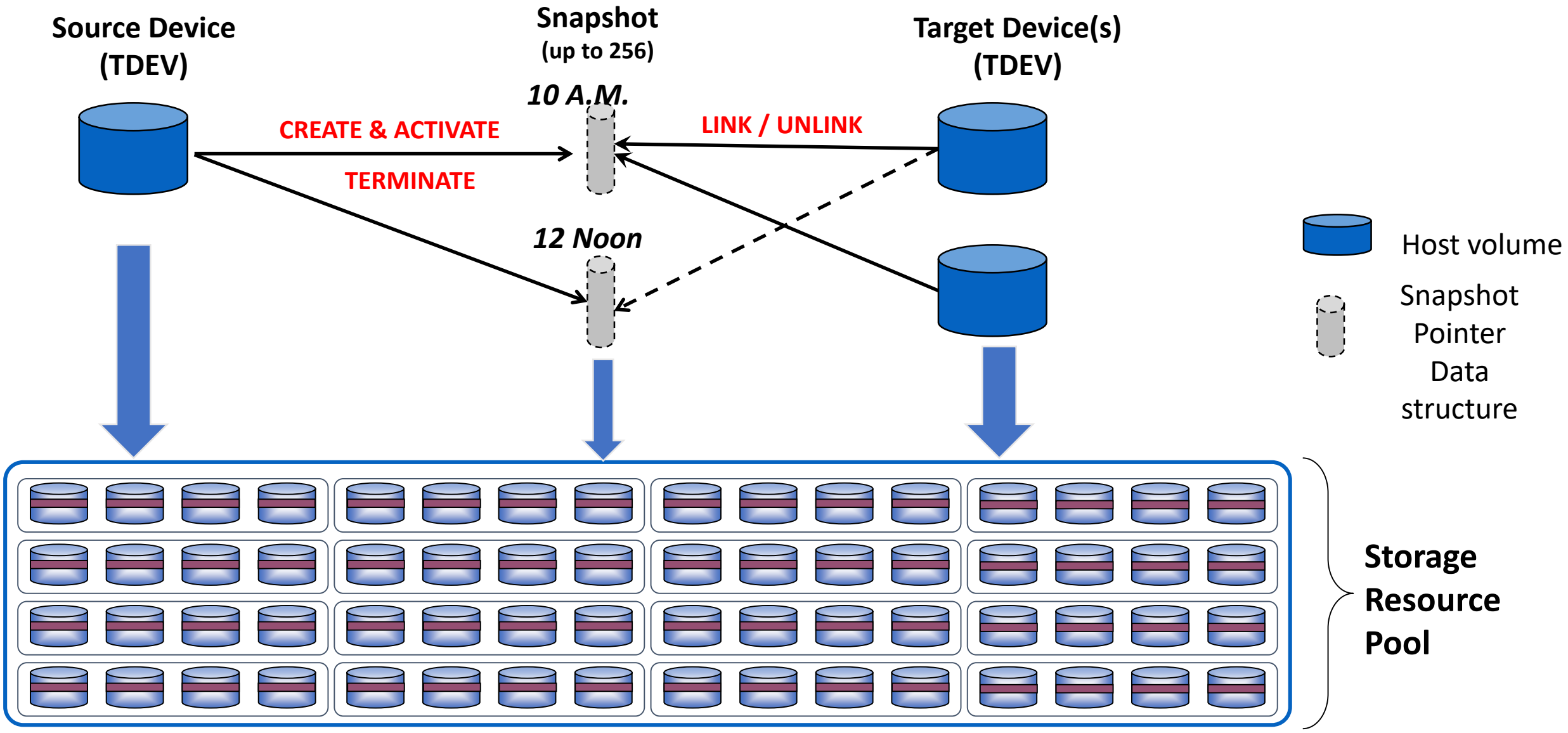
SnapVX and zDP

Incorporate snaps for data copies

New TimeFinder SnapVX™

REDUCED IMPACT	INCREASED AGILITY	EASE OF USE
• Target-less Snapshots	• Up to 256 Snapshots per source • Up to 1024 Linked Targets (snaps and/or clones) per source	• User-defined name/version number • Automatic expiration if desired • Secure Snapshots

TimeFinder SnapVX – pointer-based snaps

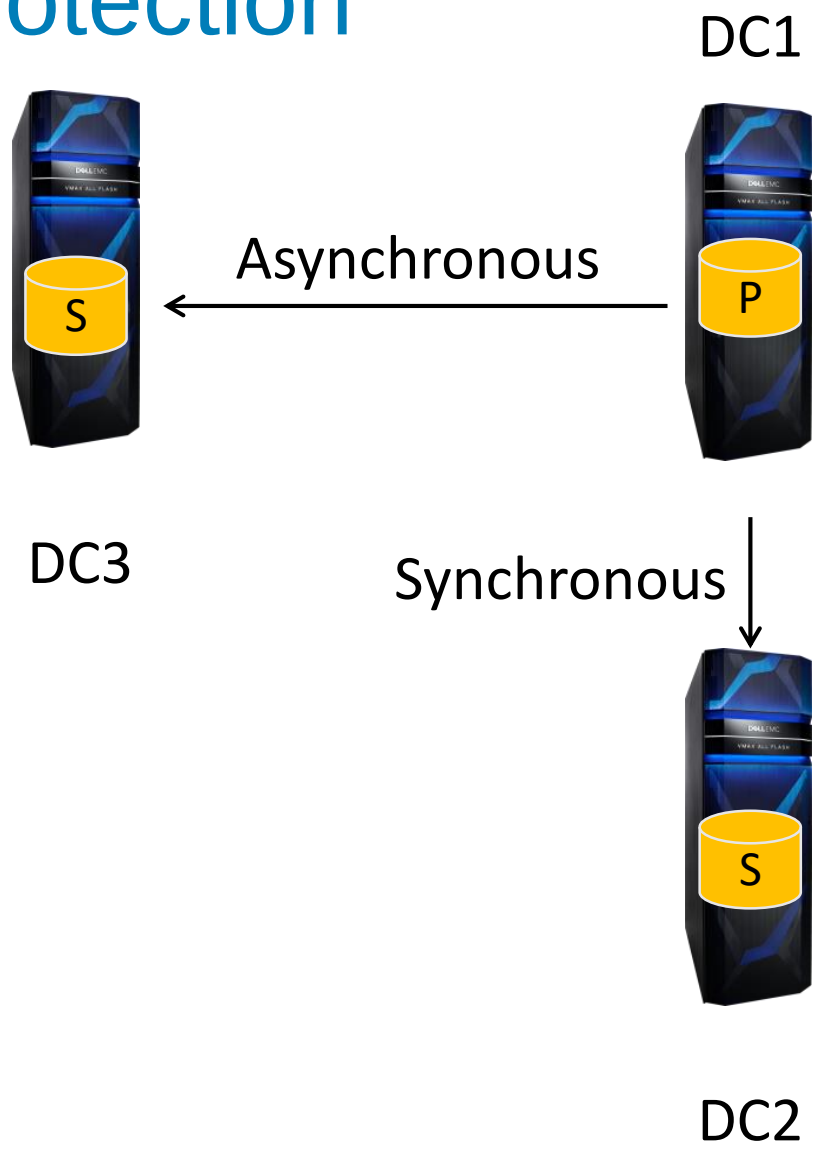


zDP: Data Protector for Z Systems

- 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’

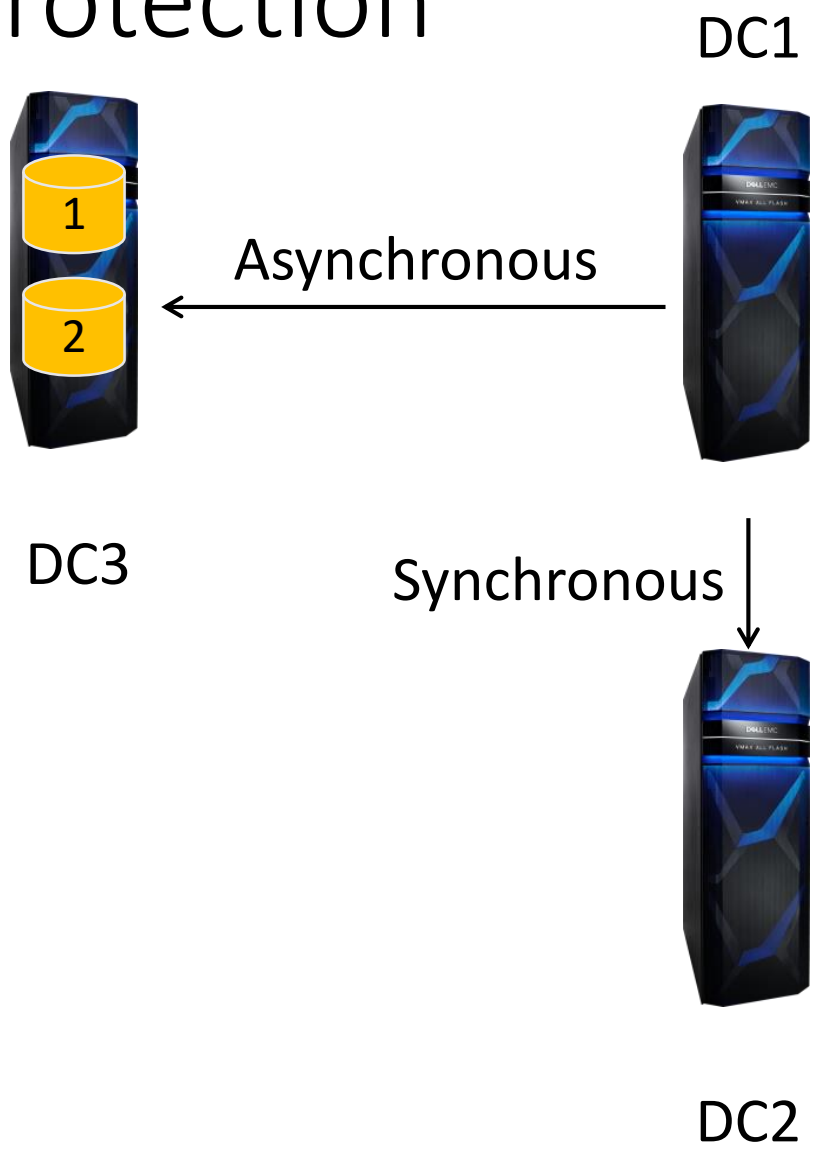
Why zDP? – logical vs physical protection

- 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!



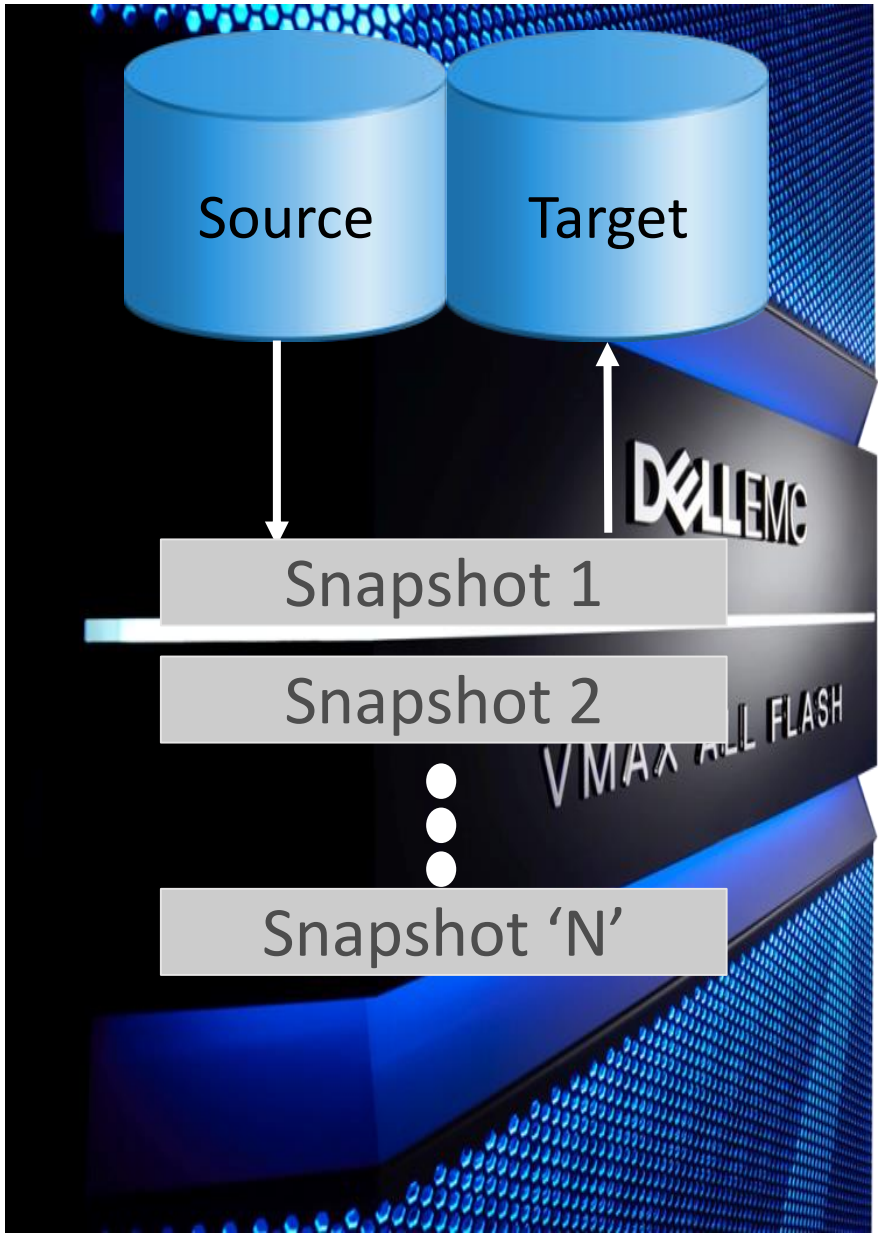
Why zDP? – logical vs physical protection

- 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

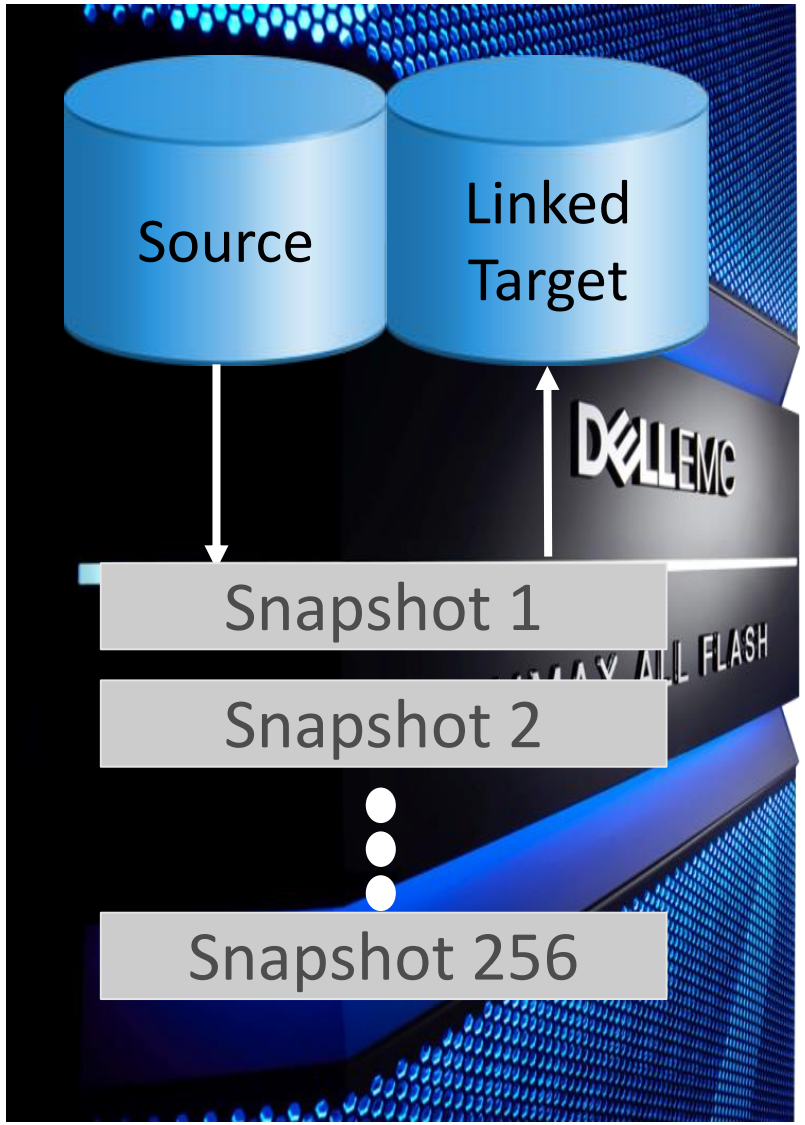


Why zDP? – logical protection

- 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



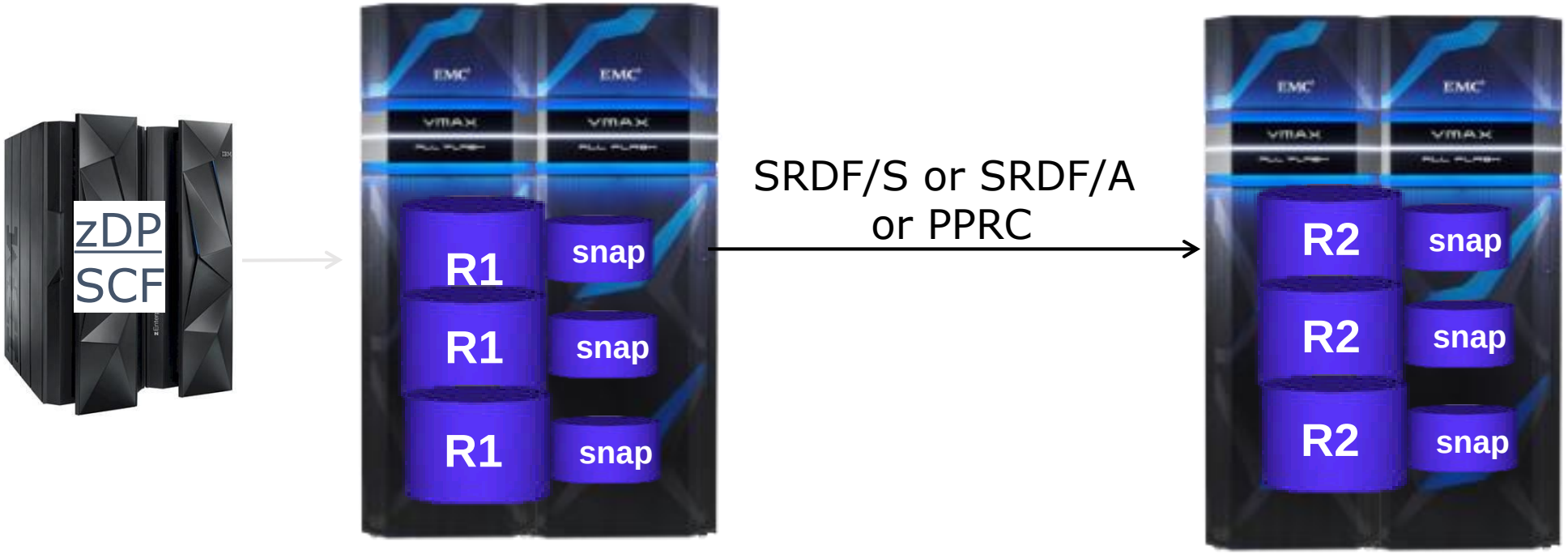
- Host automation solution
  - Frequent creation/deletion of snapshots
  - Benefit: Fast recovery from logical corruption
- Features at-a-glance
  - Up to 288X more recovery capability compared to a daily snapshot (5 min intervals)
  - Keep up to 1024 versions of each volume
  - Select snapshots to LINK by timestamp
  - Automatic ‘roll-off’ of aged snapshots
  - Space estimation and monitoring
  - Consistent scale (32,000 volumes)

zDP – deployment options

zDP supports snapset creation:

- Locally attached to VMAX3

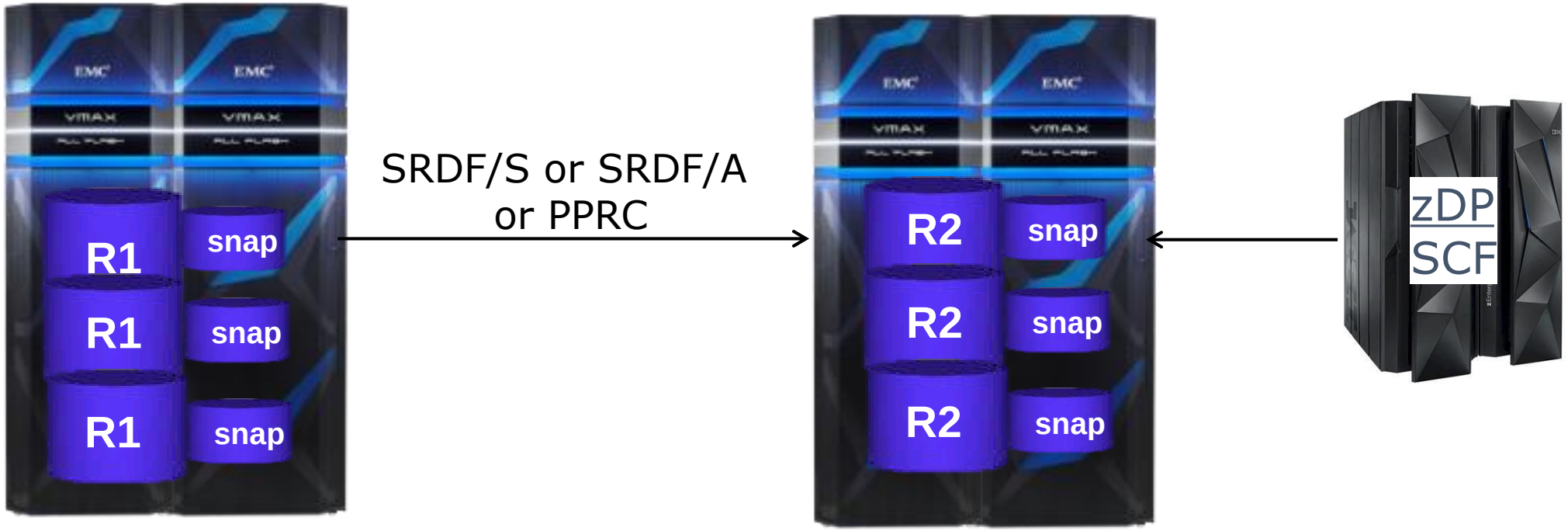
zDP – deployment options



zDP supports snapset 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



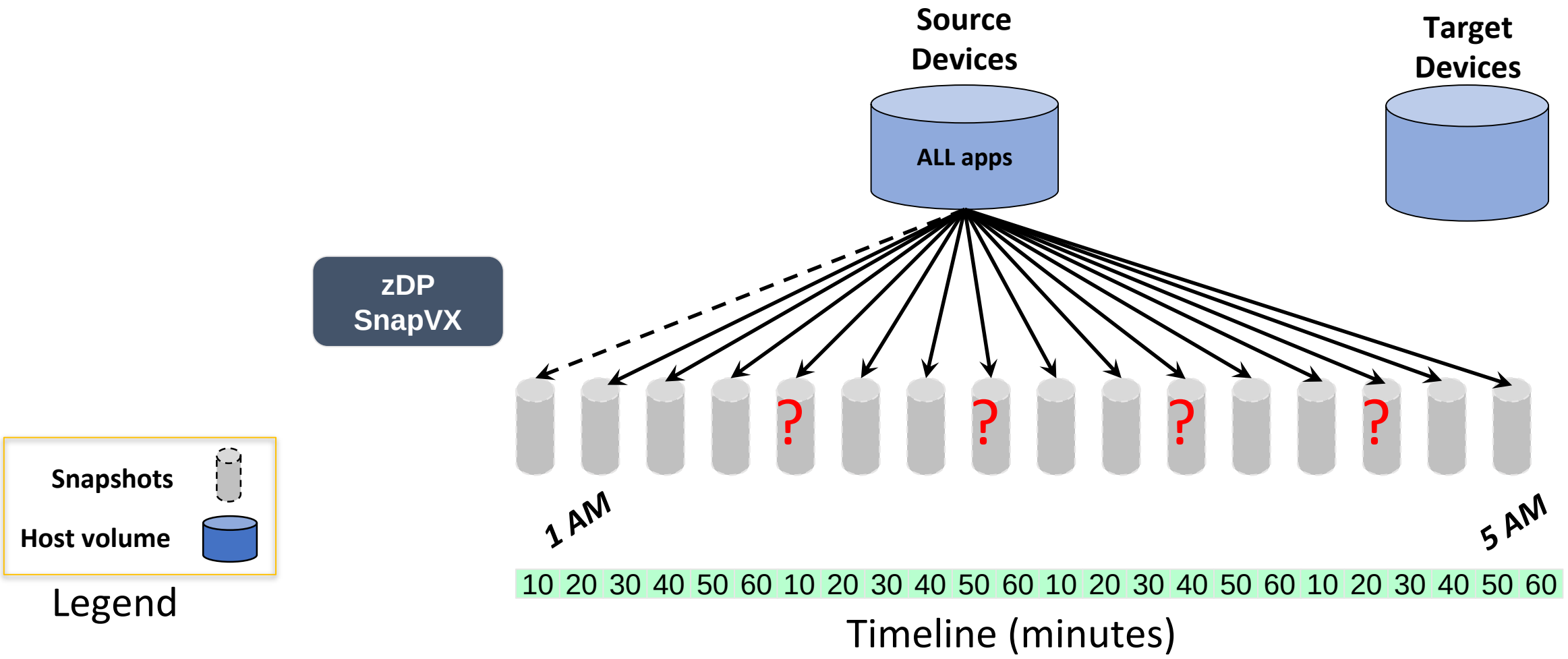
zDP supports snapset creation in:

- 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

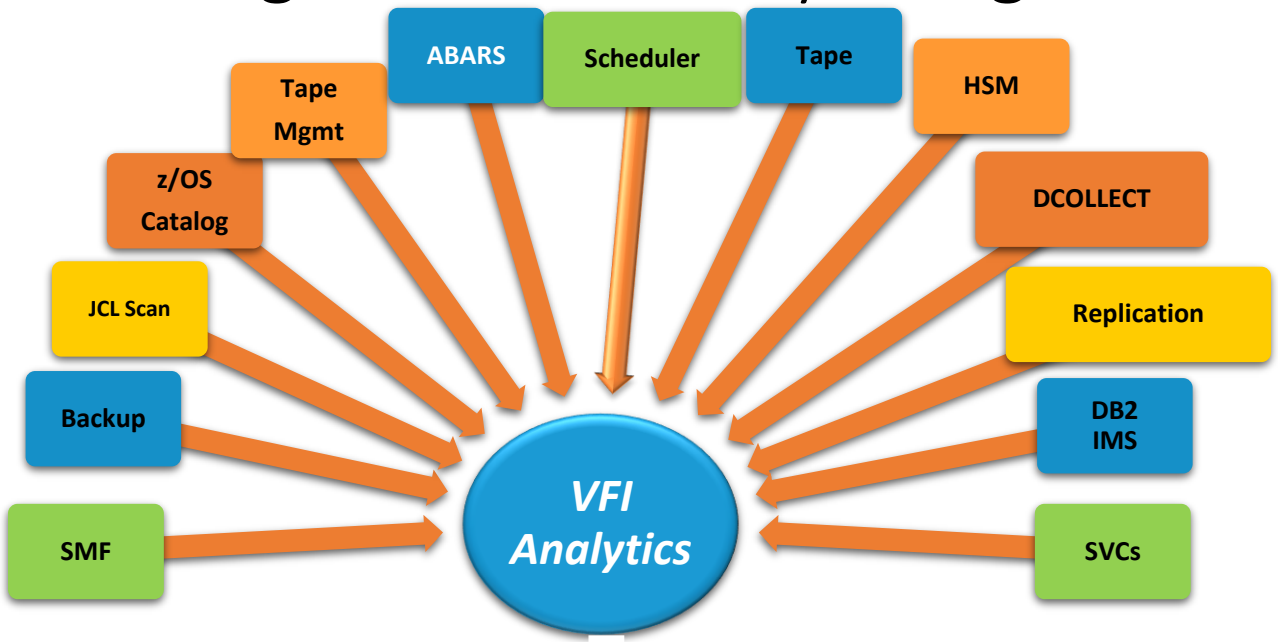
Automating Recovery using zDP Snapsets:

- Vital File Identifier (VFI)
- Timeliner

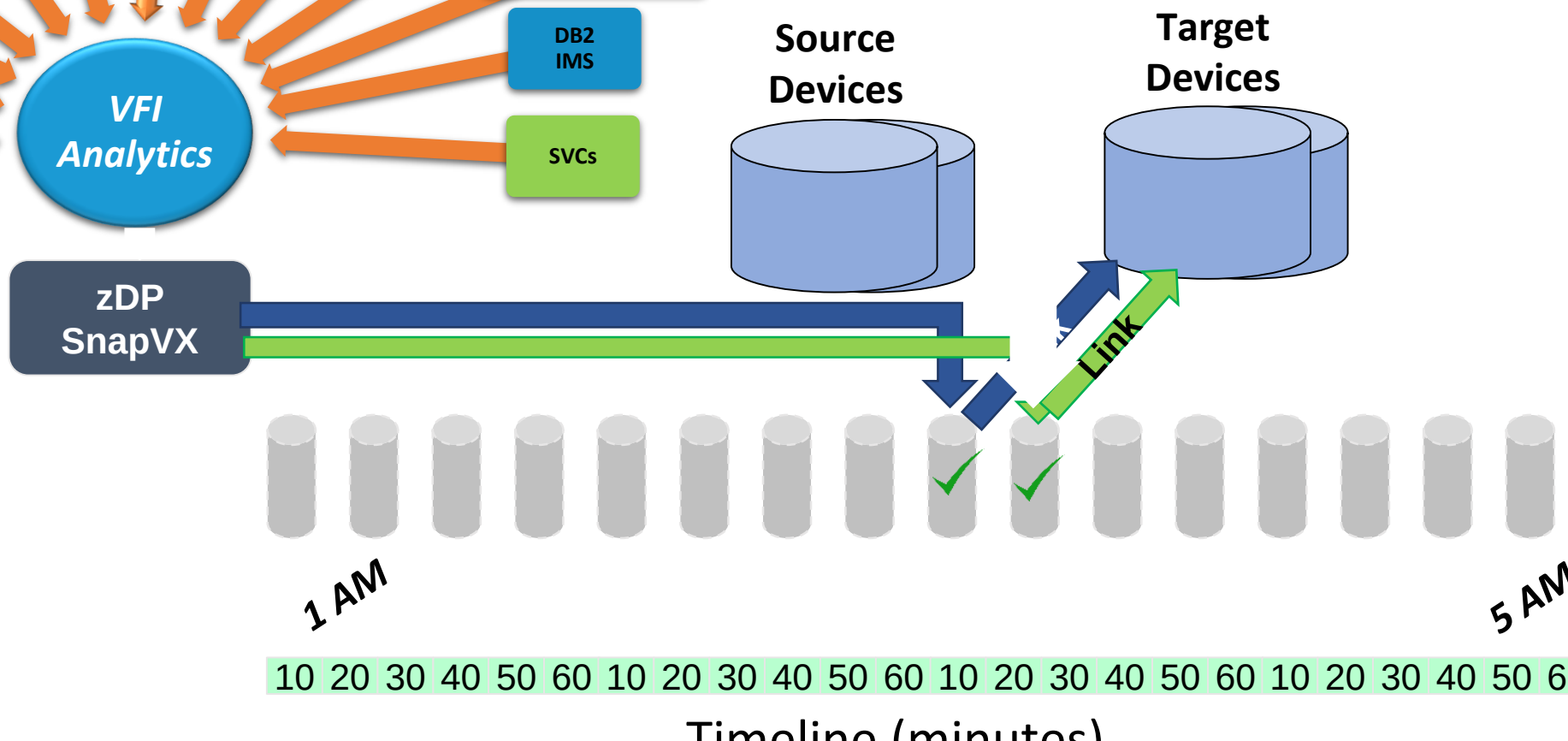
VFI / TimeLiner Application Awareness: Enabling faster recovery using zDP

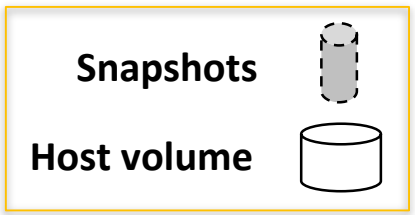


VFI / TimeLiner Application Awareness: Enabling faster recovery using zDP



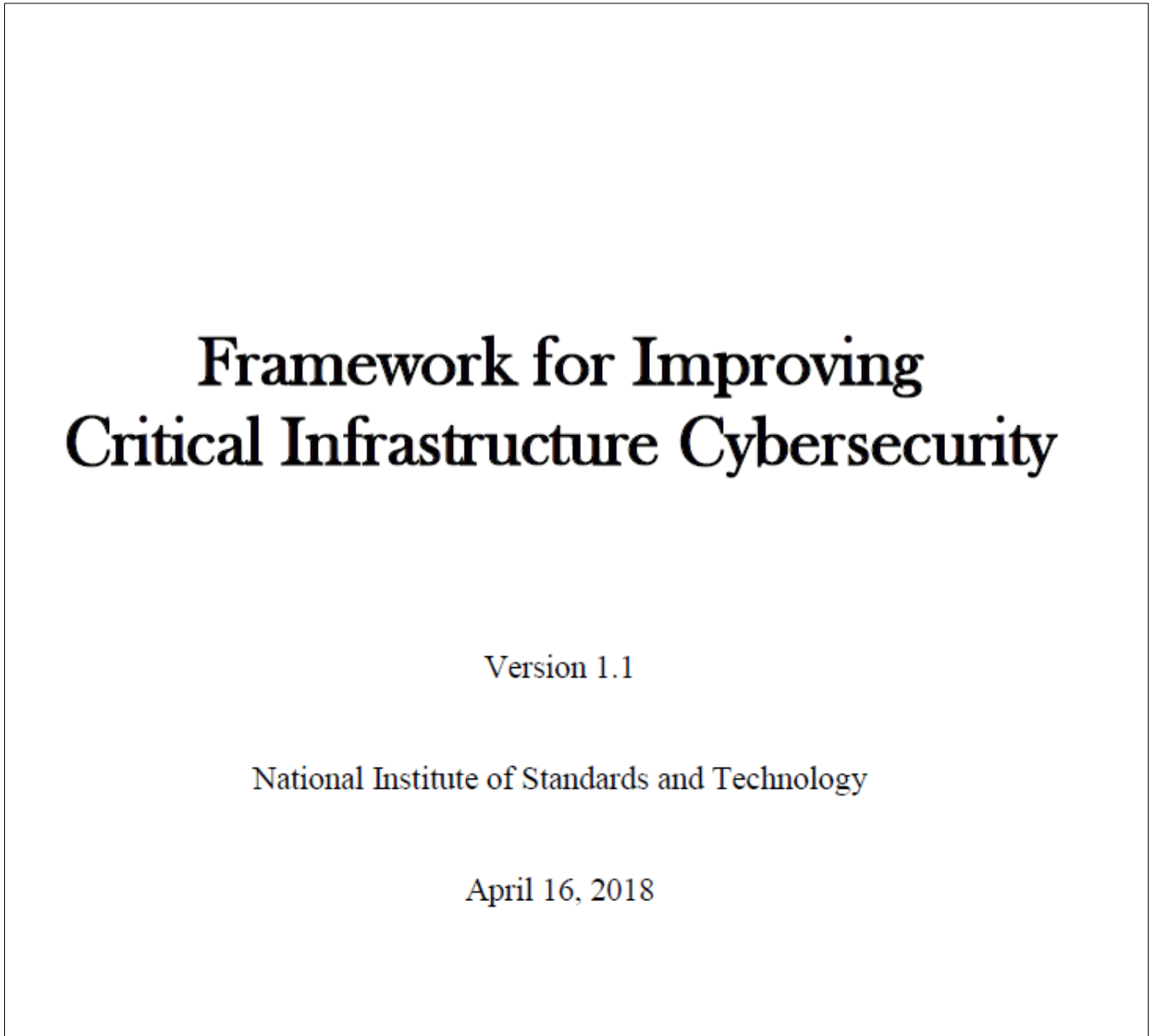

```
Cascade Impact Report for STEP

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
=============================================================================================
```





Legend

NIST Cyber Security Framework Whitepaper



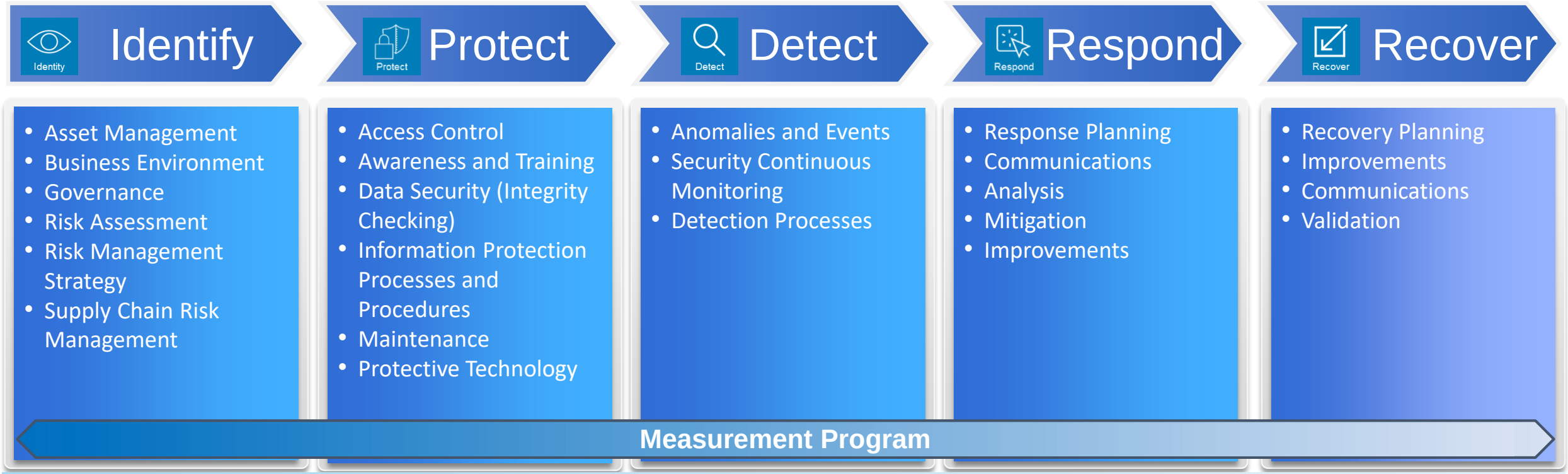
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

NIST Cybersecurity Framework

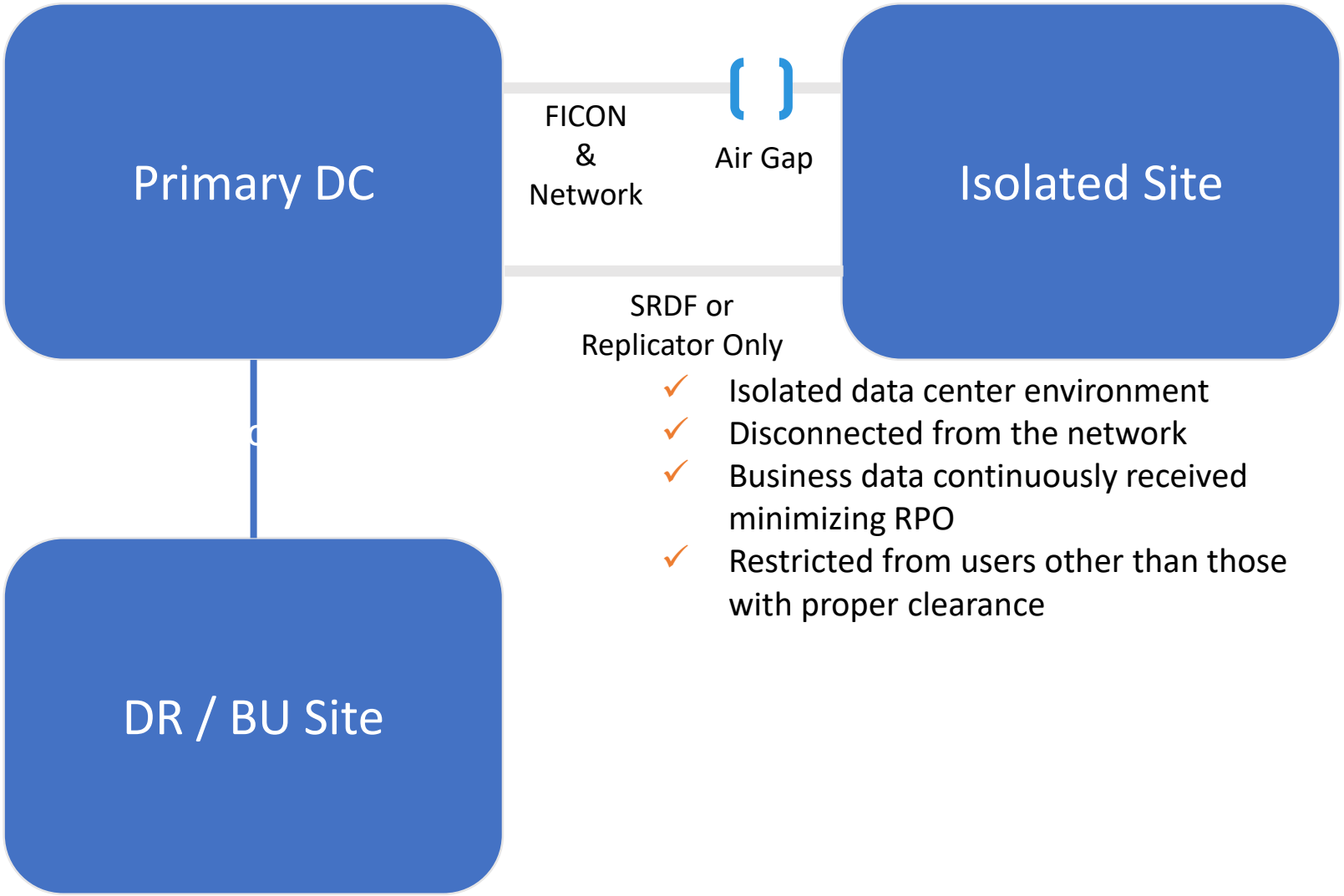


DELL EMC	Cyber Recovery Application/Data Dependency Mapping	Cyber Recovery Data Protection	Cyber Recovery Malware Analytics	Cyber Recovery Destructive Malware Incident Response	Cyber Recovery Solution
RSA	Risk Management RSA Incident Discovery	Identity Management	RSA NetWitness® Security Analytics for Early Detection	Incident Response Retainer Advanced Cyber Defense	RSA NetWitness® Forensics / RSA Archer Recovery Management
Dell Technologies	Secureworks® Cybersecurity Maturity Assessment & Compliance Program Management	Secureworks® Managed Firewall, IDS, IPS	Secureworks® Security Monitoring & Management	Secureworks® Monitoring, Incident Response, Forensics Analysis & Investigation	

Dell Technologies Aligned Solutions and Services

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

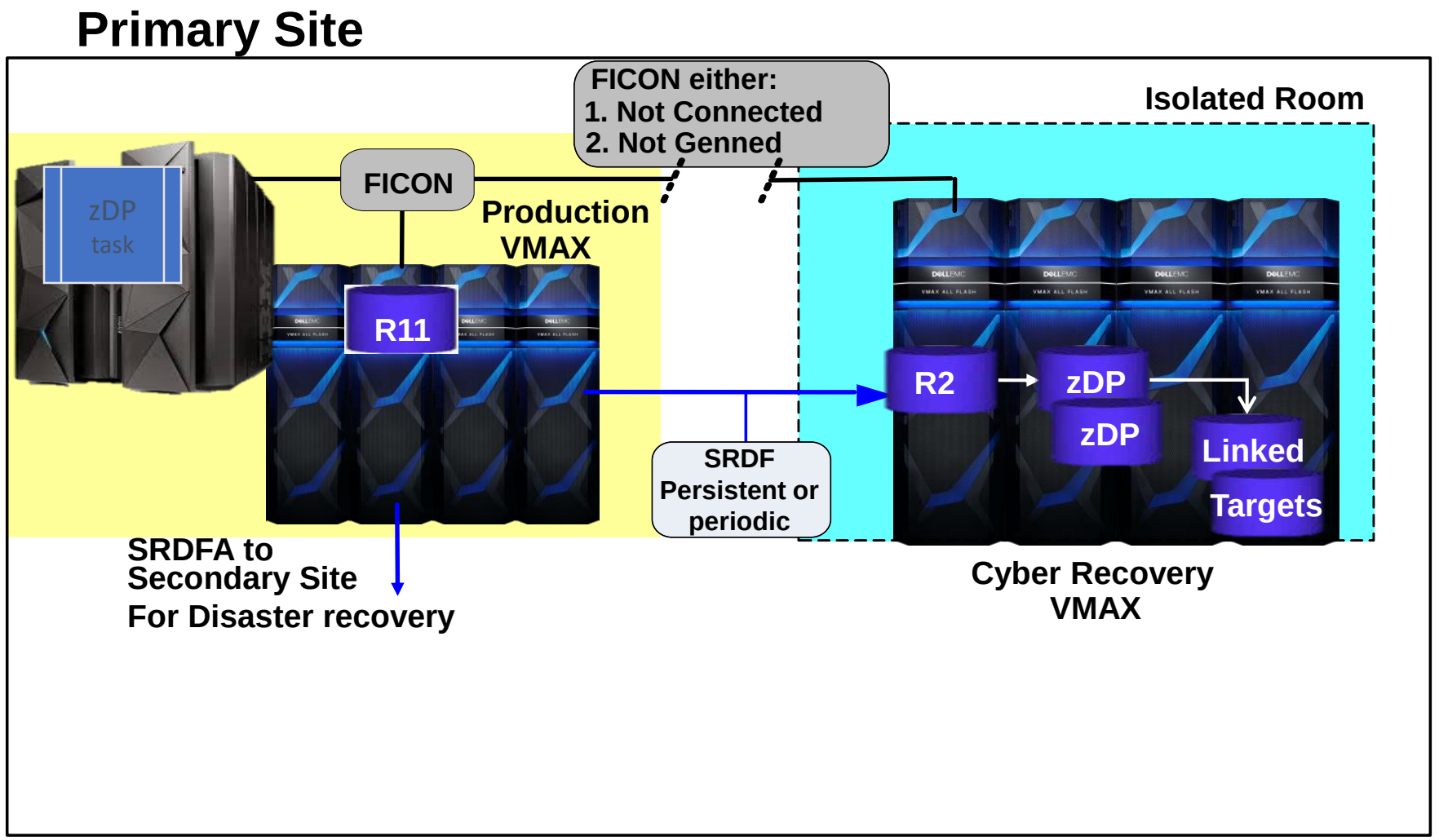
4

Recovery:

- Standard failback mechanisms
- Additional remediation / validation

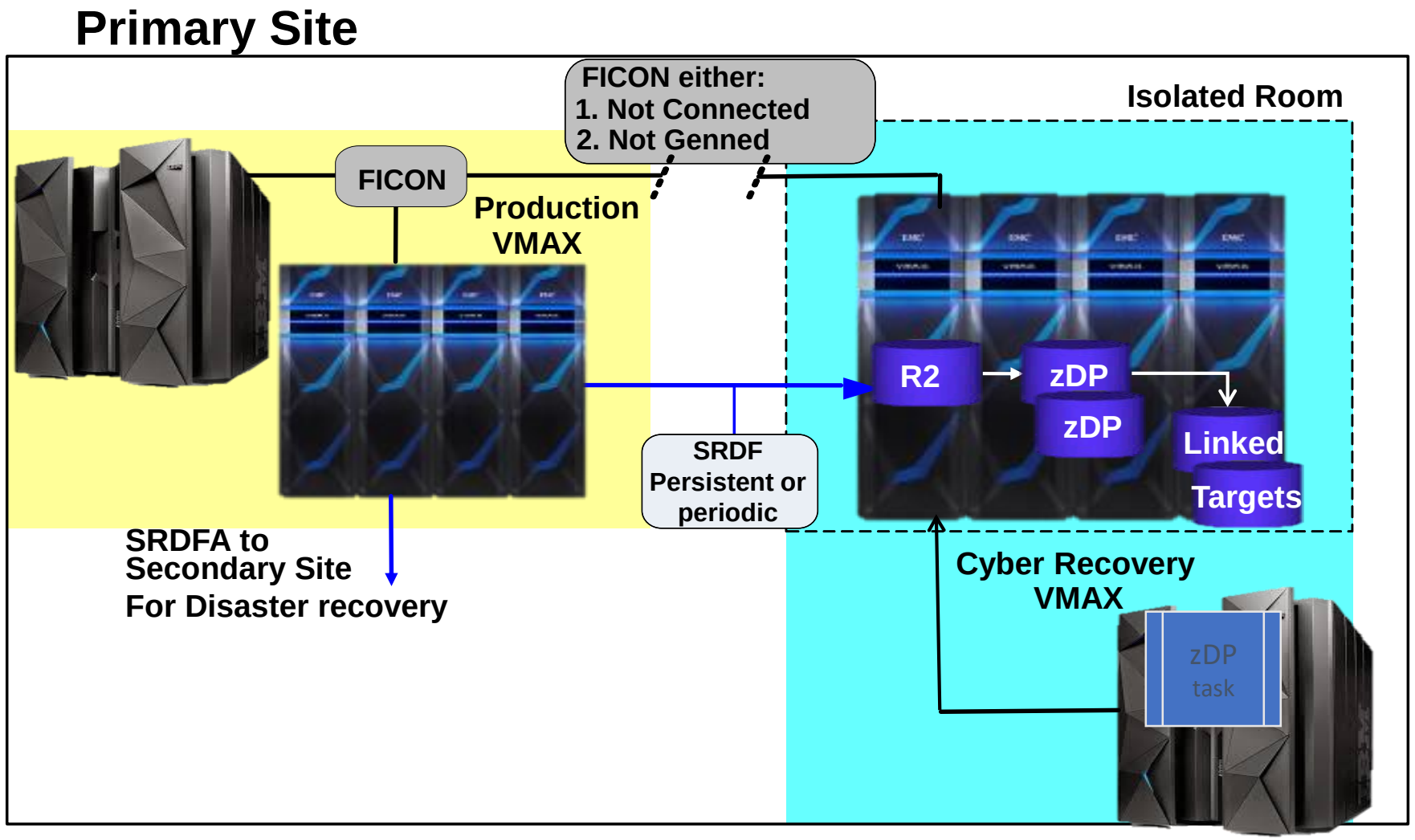
MF isolated “air-gapped” Cyber Recovery system example

- 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

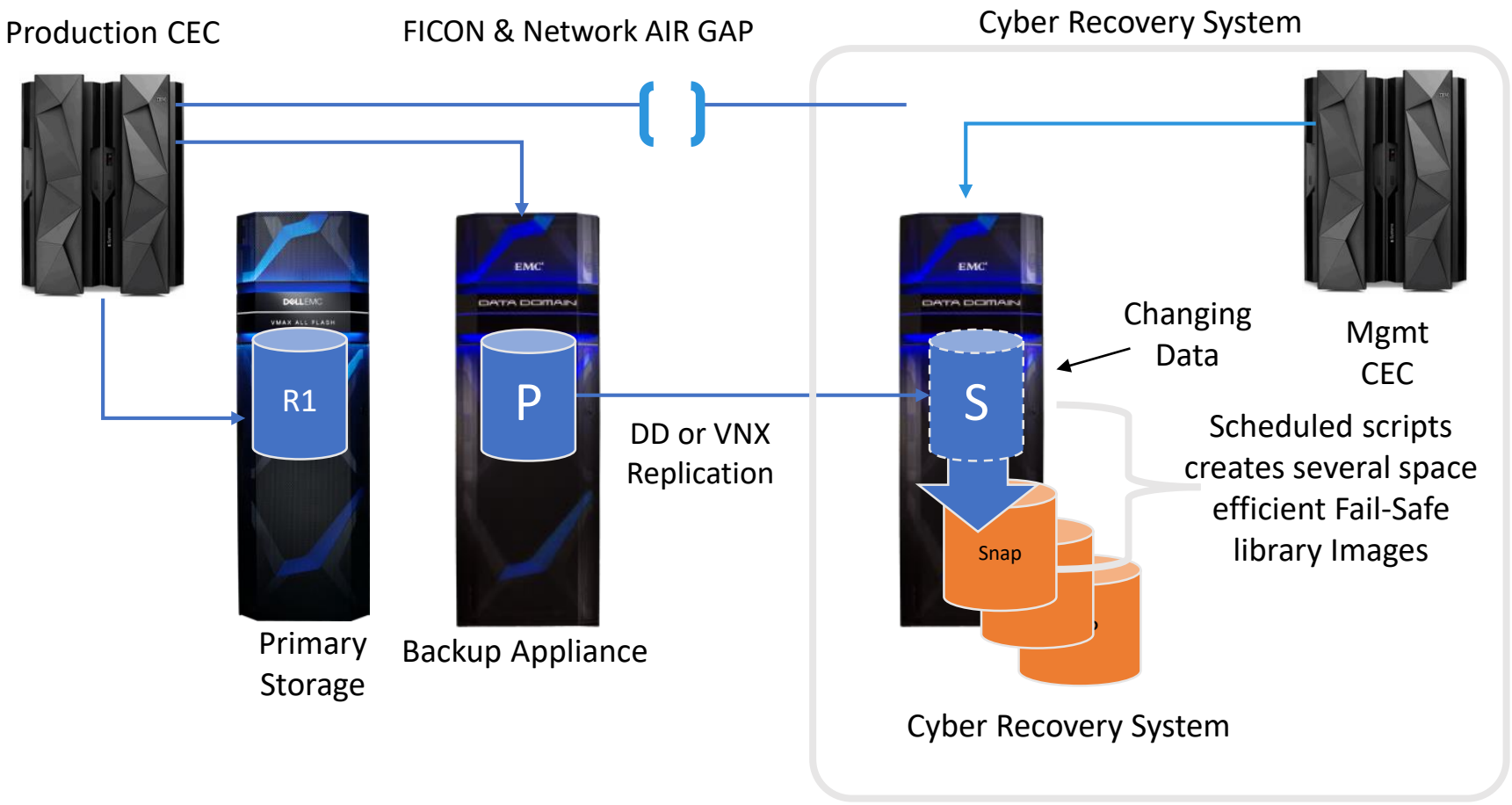


MF isolated “air-gapped” Cyber Recovery system example

- 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 TCPIP 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**

- 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 Llibrary 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

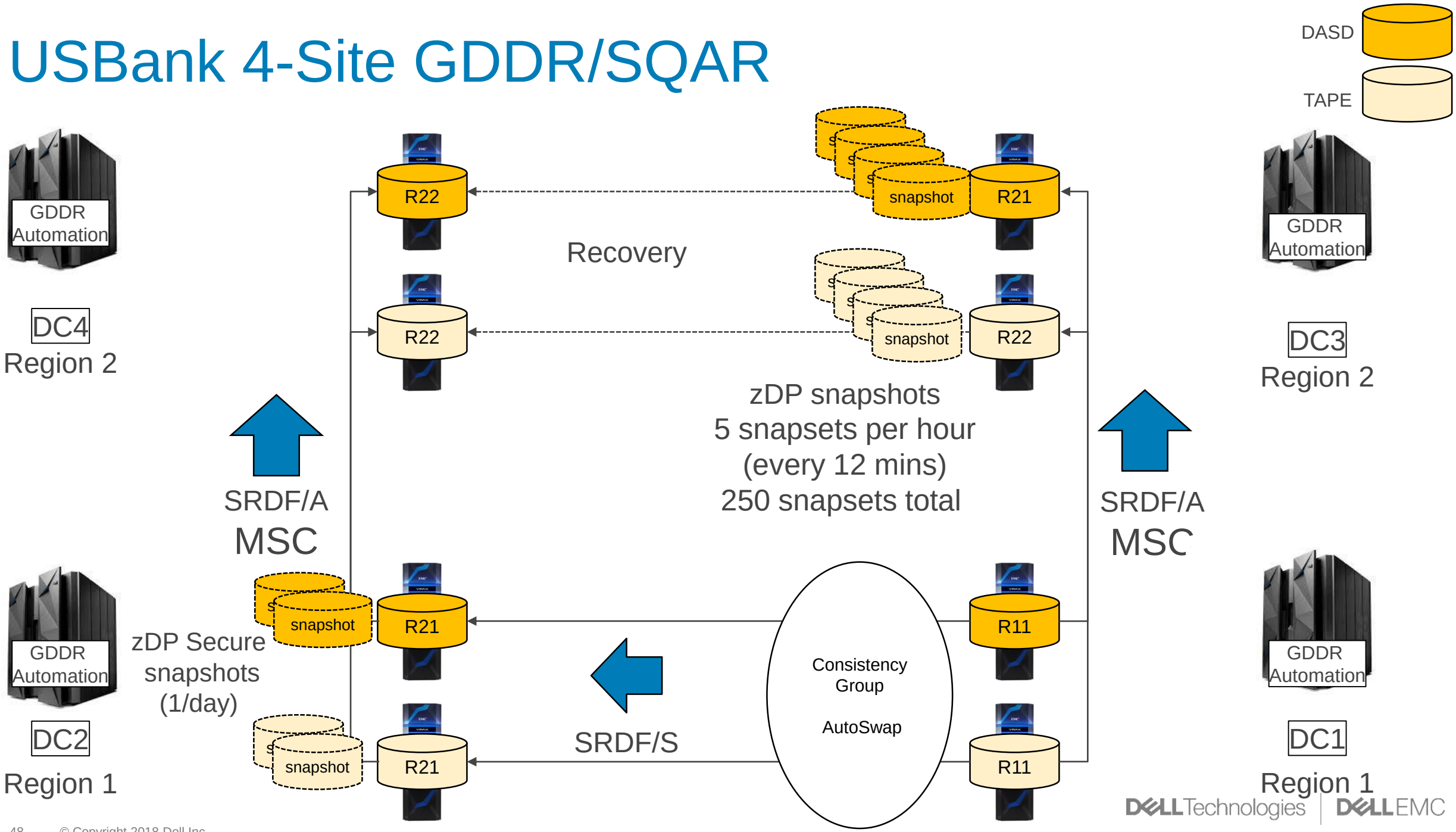
* Adjustable based on desired security window
** Depends on # of Volumes, Data etc.
***Lower Performance

US Bank : A true Technology Partnership

- 5th Largest Bank In The US ($417B In Assets)
- Three Physical Data Centers, Six mainframes per data center, 106,000 MIPS per data center
- 145 TBu of DASD Capacity In Each Data Center
  - ~23,000 CKD Volumes In Each Data Center
- 760 TBu of DLm tape on VMAX
- 3.3M Batch Jobs, 200M CICS Transactions Per Day
- Of note:
  - 3 site GDDR/Star with Autoswap → 4 site GDDR/SQAR
  - Pioneered Universal Data Consistency™ between Tape and DASD using DLm and VMAX under GDDR
  - Drove development of zDP for rapid logical corruption recovery "a Time Machine for the mainframe"
    - zDP in production since July 2016: 10 minute snapshots off 23K SRDF/A R2s across 3 VMAXs, 250 snapshots per volume

Customer comment on zDP:
"I've been waiting over 30 years for this type of recoverability for my data"

USBank 4-Site GDDR/SQAR



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

Thank You!