Ensuring Mainframe Data is Safe in a World of Increasing Cyber Attacks

Monica Bennet, Corporate account sales
monica.bennett@dell.com

Paul Scheuer, Mainframe Storage Marketing
paul.scheuer@dell.com

Carol Elstien, Principal Solutions Partner
carol.elstien@dell.com

Gary Smoak, Mainframe division storage SE
gary.smoak@dell.com

DELL Technologies

The world under cyber attack – a mainframe perspective

DELL Technologies

Cyber threats 2021: the facts

39s

Every 11 seconds

a cyber or ransomware attacks occur.*

71%

86%

of breaches are financially motivated.

verizon

$13M

$24.7M

Avg. cost of cybercrime for an organization.

accenture

$1T

$6T

Total global impact of cyber crime in 2021.

Cybersecurity Ventures

43%

48%

of breaches involved small business.

verizon

Banking	$18.4M
Utilities	$17.8M
Software	$16.0M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*Source: Cybersecurity Ventures

DELL Technologies

Why Should We Be Worried?

Its all about the money

It's your data (in fact. It's YOU in in binary form)

There are teams of people who make a fortune (millions) from stealing data and selling it

And they have a marketplace to go and sell it!

Slide courtesy of BMC Software

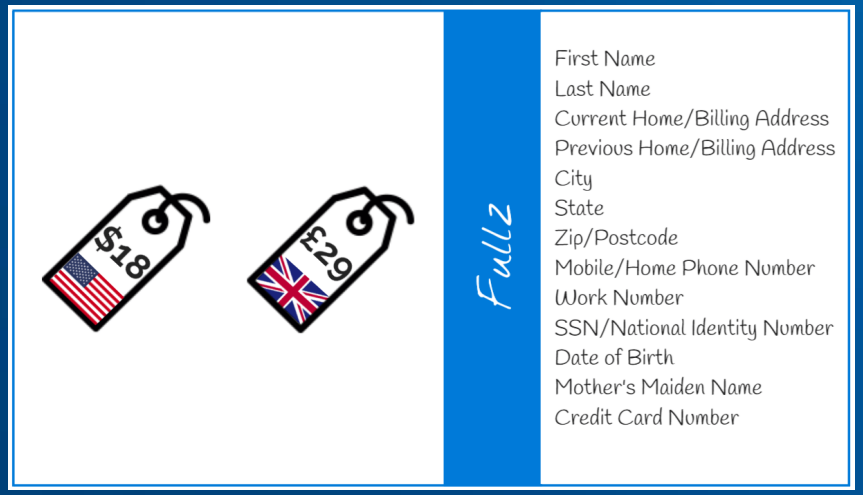
DELL Technologies

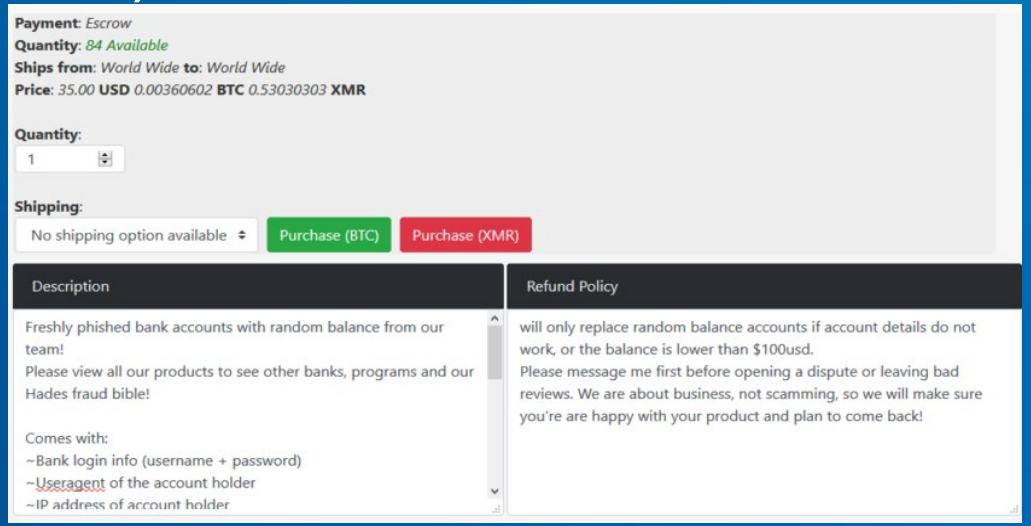
The Dark Web – In A single Picture

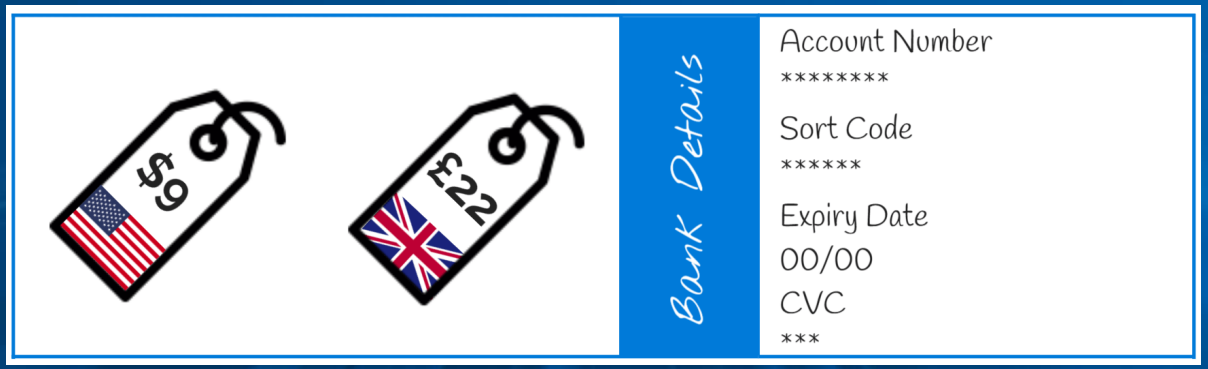
Slide courtesy of BMC Software

DELL Technologies

The value of YOU (your data) on the Dark Web!







Slide courtesy of BMC Software

DELL Technologies

Look at what's happening!

June 3, 2021

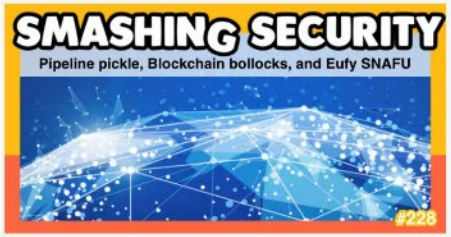
Smashing Security podcast #230: Flash card f-up and energy pipe pilfering

May 21, 2021

Cyber insurance giant CNA paid out $40 million to its ransomware attackers

May 20, 2021

Qlocker ransomware gang shuts shop after extorting owners of QNAP NAS drives



May 20, 2021

Smashing Security podcast #228: Pipeline pickle, Blockchain bollocks, and Eufy SNAFU

May 31, 2021

US Army tells remote workers to switch off their IoT devices (and then withdraws advice)

May 19, 2021

Fake Microsoft Authenticator extension discovered in Chrome Store

May 18, 2021

Apple rejected 215,000 iOS apps due to privacy concerns last year

May 17, 2021

Cyber insurance giant AXA hit by ransomware attack after saying it would stop covering ransom payments

Slide courtesy of BMC Software

DELL Technologies

What's is the wider security industry saying?

- Assume that the “Bad Actors” are already in your network
- Detection and Response are where we should be focusing?
- Ask yourself, could you really recover in the event of a Cyber/Ransomware Attack?
- Client Quote: “It’s OK I have all of my data replicated in 3 locations”
- We need to think more like a “Time Machine” solution that you see on Apple Mac’s

Slide courtesy of BMC Software

Our Perspective

This is the most difficult time in history to protect the integrity of data.

DELL Technologies

Our Perspective

Dell EMC has been protecting the integrity of over 1/3 of the world's most essential data for over 30 years.

We invent and apply technology to ensure integrity of data; technology that as little as four years ago wasn't even a thought.

DELL Technologies

“69% of global IT decision-makers lack confidence their organizations could reliably recover all business-critical data in the event of a cyber attack. “

source: Dell Technologies Global Data Protection Index Survey 2020 Snapshot

DELL Technologies

Modern Ransomware

- No longer just ‘fire and forget’
  - Larger coordinated efforts are now more common
- Three major stages of illegal capture of data:
  1. Access (Phishing campaign, social engineering, watering hole, vendor compromise, etc.)
  2. Discovery (what is available for us to steal/encrypt)
  3. Selling of the data (back to the owner!)
     - Sell the decryption Key
     - Sell copies of a company’s data or, for an additional fee, destroy (*that sensitive*) data

07/26/2020 00:24:03

Support

Hello! Can I help you?

You

07/27/2020 03:27:33

Hello? What do we need to do to get our data deleted from your servers and unlock our files?

07/27/2020 07:43:08

Support

Hello !

You have 30.000 infected and locked devices from different countries.

Our price is consists of two services, decryption software and deleting all downloaded data from our servers.
If you need both of them you have to pay 10.000.000$ in Bitcoins, before the timer on main page will ends.

As a bonus we will provide you with the details about how we breach your security perimeter and give you recommendations about improving security measures to help your admins avoid such issues in future!

07/27/2020 07:43:35

Support

For sure we understand your worries about this deal, that's why we will decrypt two your random files for Free, just to prove that our decryptor is working properly!

Cyber Insurance

Your network has been infected!

CYBERCRIME FEATURED PEOPLE TECHNOLOGY

‘I scrounged through the trash heaps… now I’m a millionaire:’ An interview with REvil’s Unknown

By Dmitry Smilyanets · March 16, 2021

DS: Do your operators target organizations that have cyber insurance?

UNK: Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

But what does that have to do with the mainframe?

Mainframe Security Myths!

- Mainframes have long been assumed secure:
  - Because: The mainframe was designed to be secure
  - Because: “Specialized skills” would be needed to compromise them
  - Because: It’s not public facing, it’s behind a firewall
  - Because: I don’t hear about mainframes being hacked in the news

Slide courtesy of BMC Software

Common Mainframe Attacks (from very private discussions)

- Password Spraying
  - Trying one password across every account
- Credential stuffing
  - Using known compromised username/passwords collected on one website and used / tried on others.

But, that's TOO NOISY

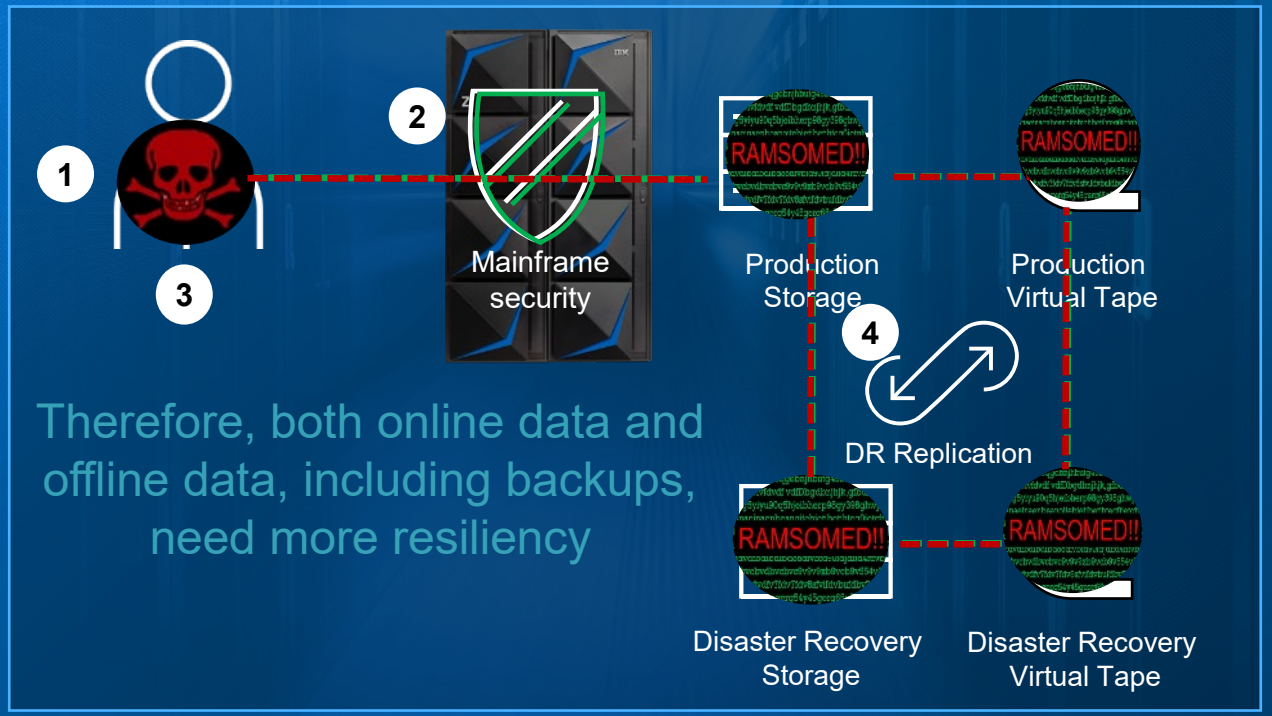
- So, steal user credentials with a key logger

Mainframe Cyber Attack Target: storage infrastructure

Attackers exploit controls, then infiltrate storage which replicates the corruption

How to hack a mainframe

1. Install a keylogger via a phishing email to a Sys Admin.
2. Sniff the network & find open ports or FTP-in
3. Via a browser, send your malicious payload
4. Malicious intent is replicated and 100% of storage is corrupted and, potentially ransomed



Click to watch the details of the security breach

What you will learn

Data corruption, extortion and theft is real, the mainframe is not immune; obscurity does not ensure security; for many companies it's a matter of when, not if

Dell Technologies CR solution uses space efficient, secure snapshots for superior protection using less storage.

Time To Protection (TTP) is shorter based on the ability to leverage existing Dell mainframe storage technology while implementing a seamless solution into an and existing infrastructure.

Time To Recovery (TTR) from a CR event is shorter based on the ability to leverage extremely fast Dell CR technology

Dell Technologies Professional Services shortens the implementation timeframe while adding insight and value

DELL Technologies

Protect and restore mainframe data

DELL Technologies

NIST Cybersecurity Framework

DELL Technologies

Cyber resiliency for mainframe – why?

Modern recovery plans MUST reduce the risk of data loss

Historically, mainframe recovery had a DR focus: unavailability (system / site disasters)

Modern threats: intentional data corruption or destruction; threats not immediately identified or understood

Cyber Recovery protects data and provides for recovery from data disasters

	Disaster Recovery	Cyber Resiliency
Recovery Time	Zero to minutes	Varies based on time to locate recovery points
Recovery Point	Zero to 10s of seconds	As little as 5 minutes
Nature of Disaster	Flood, power outage, weather	Intentional attack, human error
Impact of Disaster	Regional; typically contained	Widespread organizationally
Topology	Geographic	Systemic
Amount of Data	Physically bounded	Organizationally bounded
Recovery	Well-understood “run book” (procedural)	Attack-dependent, iterative, complex

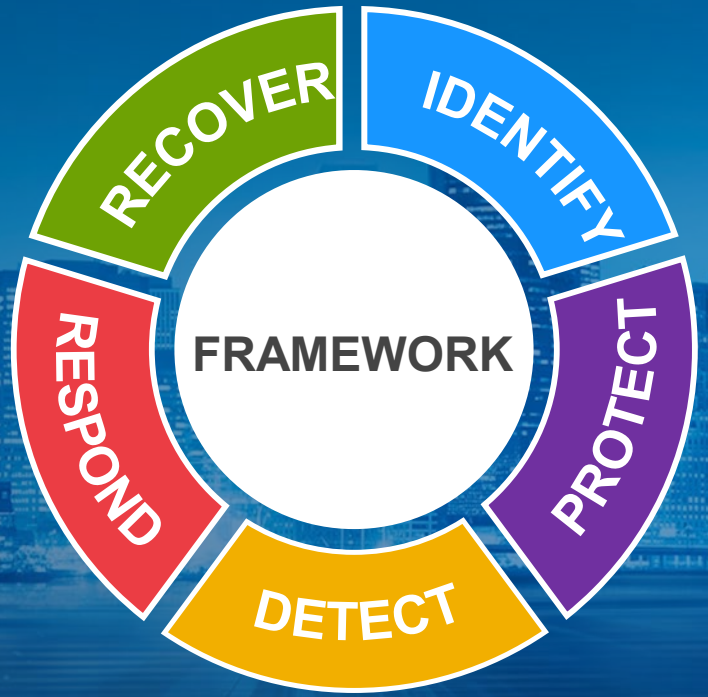
DELL Technologies

Cyber Resilience is a Strategy | Cyber Recovery is a Solution

Cyber Resilience

- *"The ability (for a business / organization) to continuously deliver the intended outcome despite adverse cyber events."* *
- A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions
- Example: NIST Cybersecurity Framework

*https://en.wikipedia.org/wiki/Cyber_resilience



Cyber Recovery

- Cyber Recovery is a critical component of an overall Cyber Resilience strategy
- Cyber Recovery is a data protection solution that isolates business-critical data away from attack surfaces
- Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality

DELL Technologies

Dell Cyber Recovery Mainframe

Immutability

- A capability, not a solution
- Data can’t be deleted or changed
- No admin or security overrides
- Single point of failure / platform dependence

Isolation

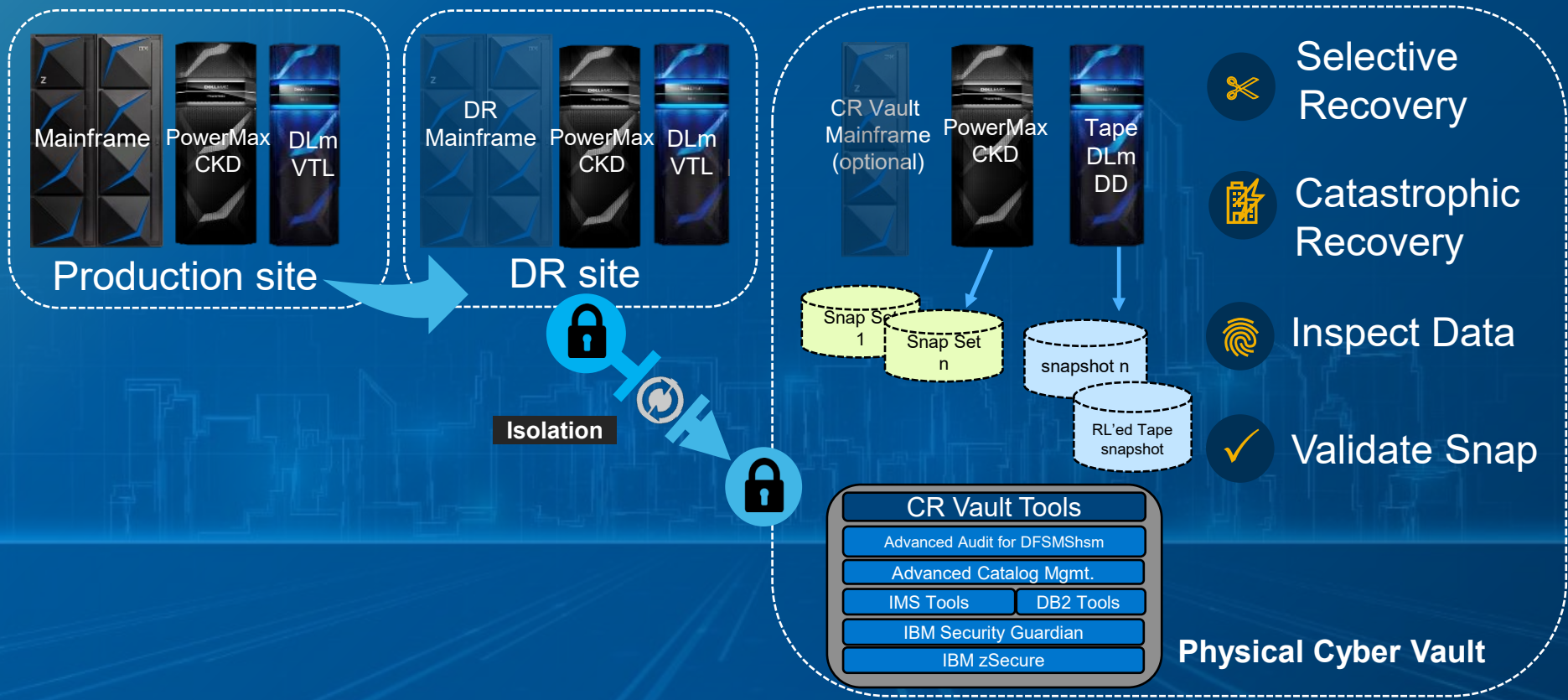
- Offline Copy
- Air gap with isolation
- Logical isolation – not just separate from production
- Automation and control from secure side
- Secure during “unlock” phase
- Certification to a standard (Sheltered Harbor)

Intelligence

- Intelligent about how data is protected and recovered
- Flexibility in data protection, retention and granularity
- Answers the question: “Could this data be used for recovery?”
- Resides and operates in the vault for security

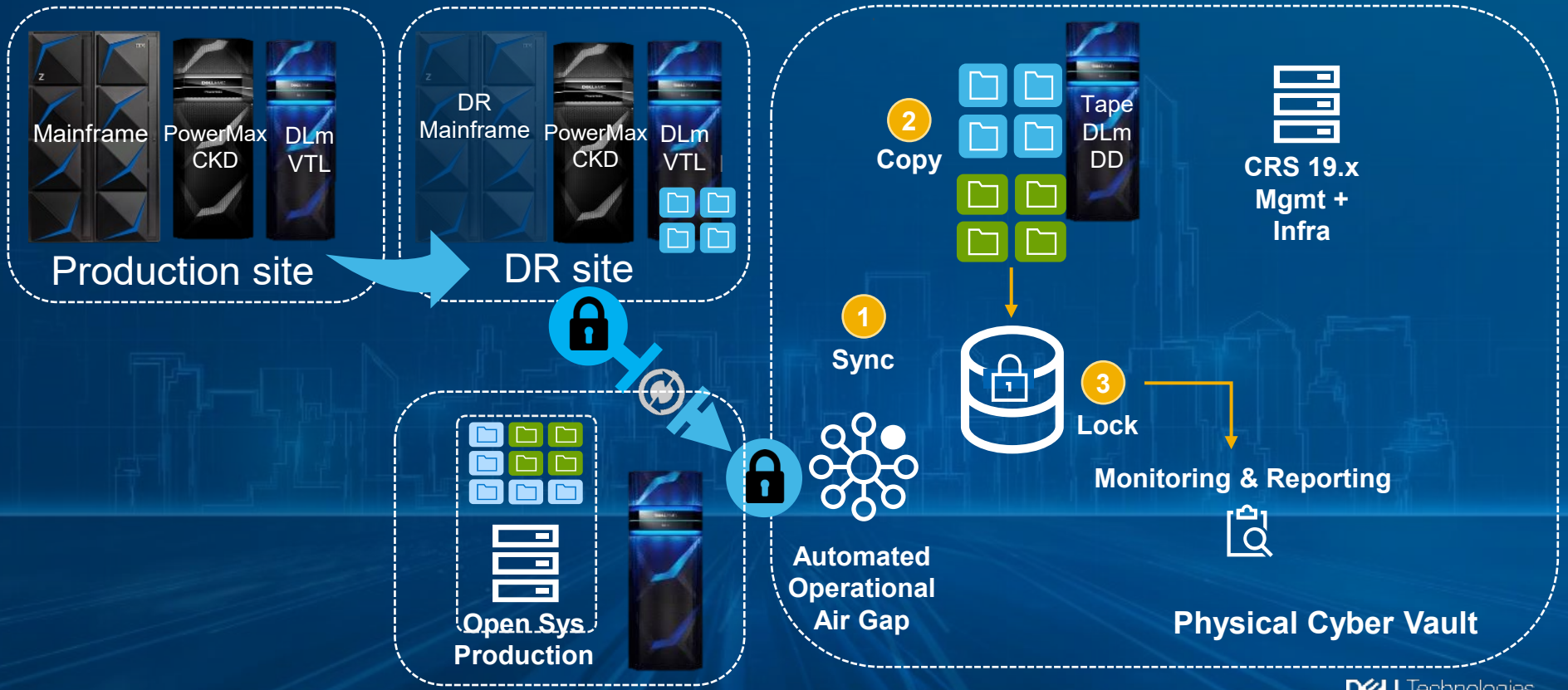
DELL Technologies

Dell Technologies mainframe physical cyber vault

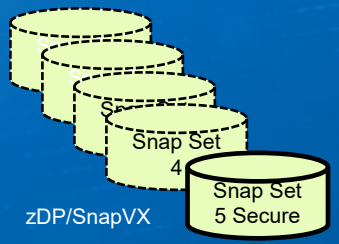


Dell Technologies mainframe physical cyber vault

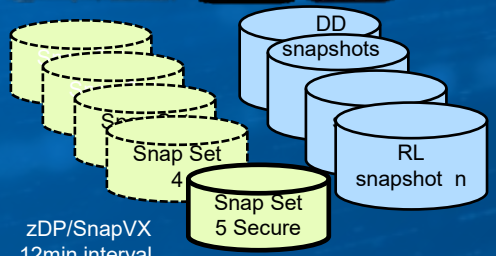
PowerProtect Cyber Recovery – Leveraging Data Domain as a Data Protection Platform



Dell Technologies Virtual Cyber Vault



Production Site



- Selective Recovery
- Catastrophic Recovery
- Inspect Data
- Validate Snap

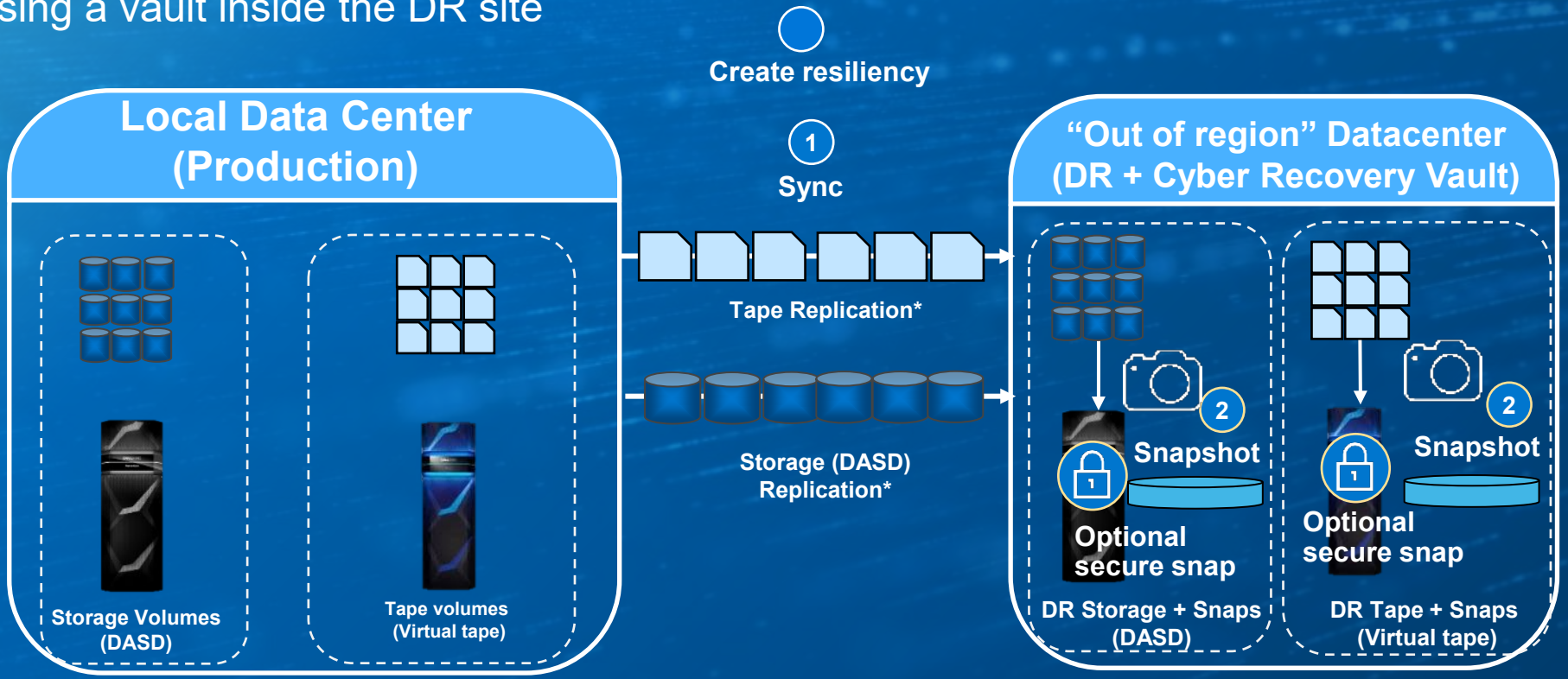
CR Vault Tools

- Advanced Audit for DFSMShsm
- Advanced Catalog Mgmt.
- IMS Tools | DB2 Tools
- IBM Security Guardian
- IBM zSecure

DR & Virtual Vault Site

Basic Cyber Resiliency illustration: protect the data

Using a vault inside the DR site

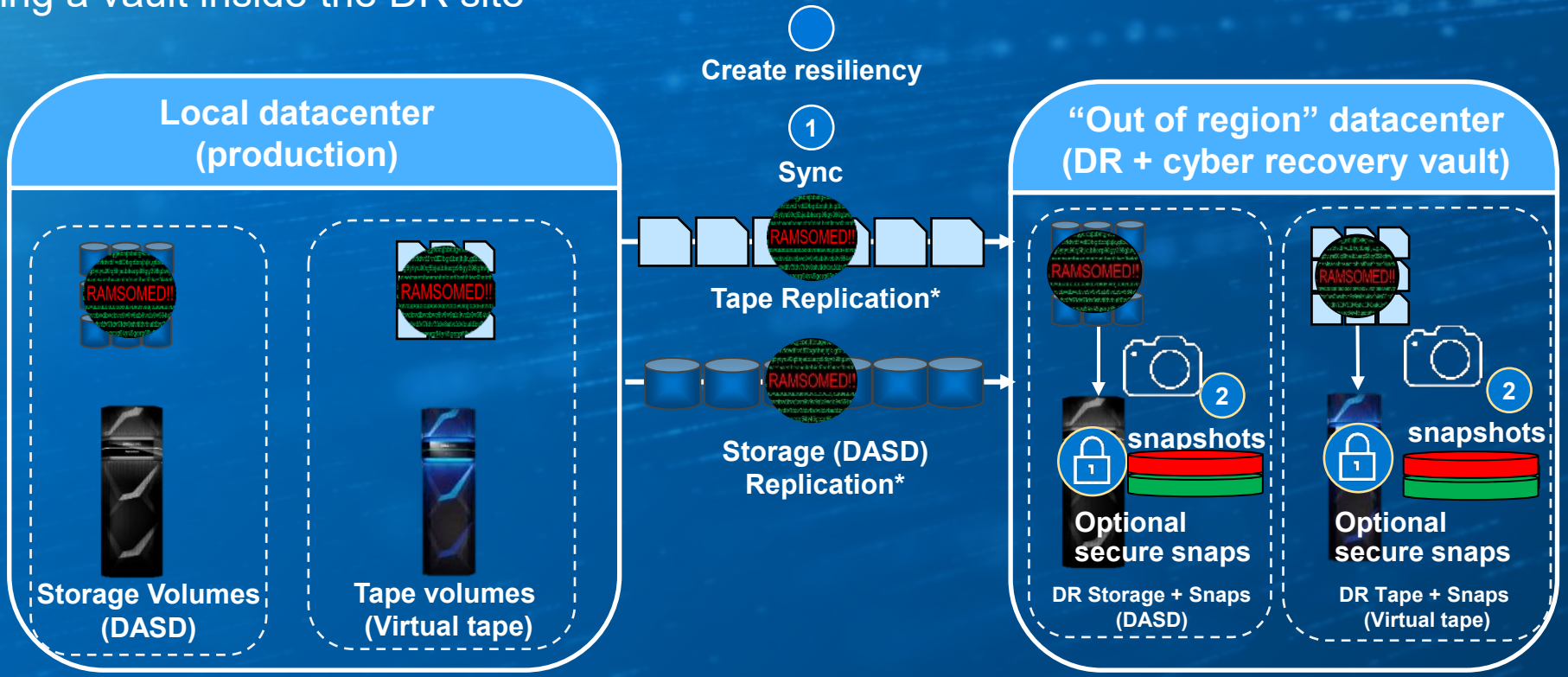


*use a private, isolated, non-discoverable network

DELL Technologies

Basic Cyber Resiliency Illustration: corruption event

Using a vault inside the DR site

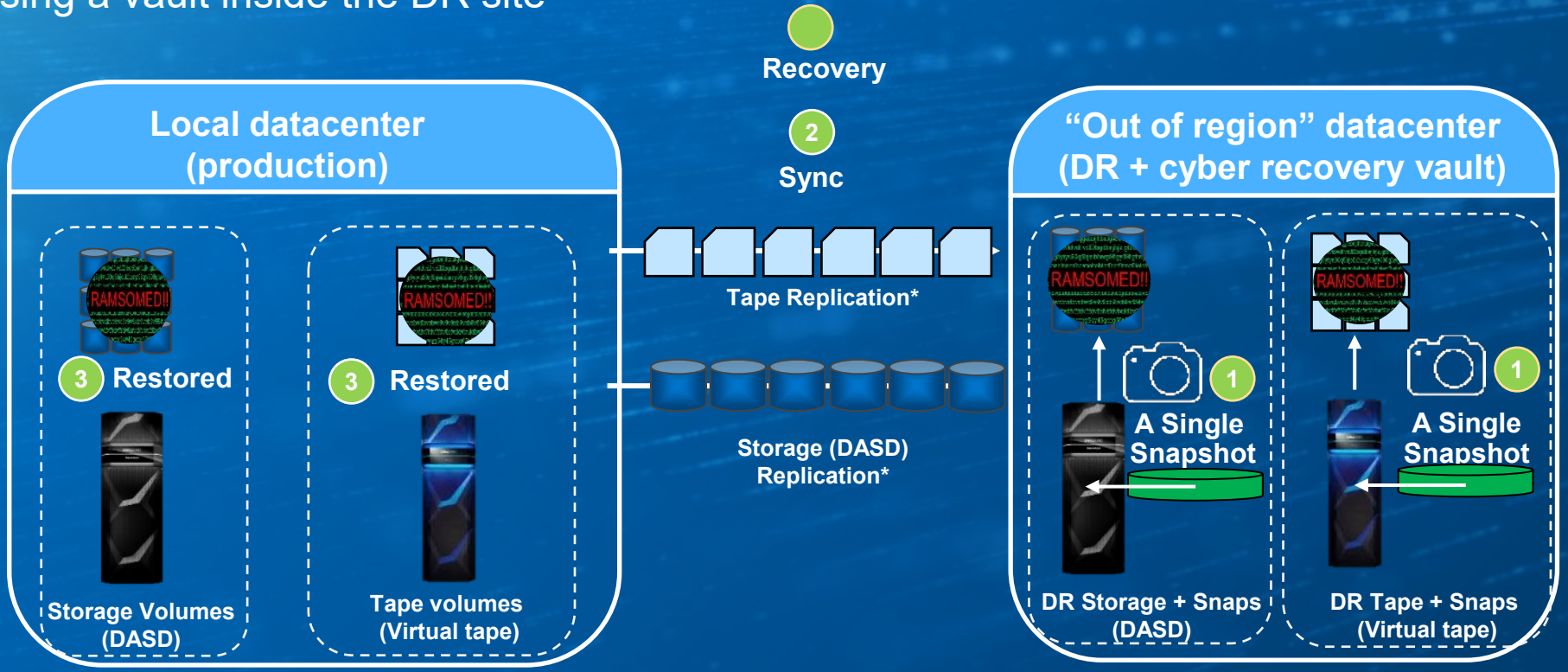


*Replication network is private, isolated, and non-discoverable

DELL Technologies

Basic Cyber Recovery: restore the data

Using a vault inside the DR site



*Replication network is private, isolated, and non-discoverable

Dell Mainframe Cyber Data Protection Technology

DELL Technologies

Dell EMC addresses the mainframe storage challenges

Simplify operation, reduce complexity; do more with less staff

Increase storage capacity while meeting budgets

Recover from cyber attacks & insider threats

Ensure business continuity

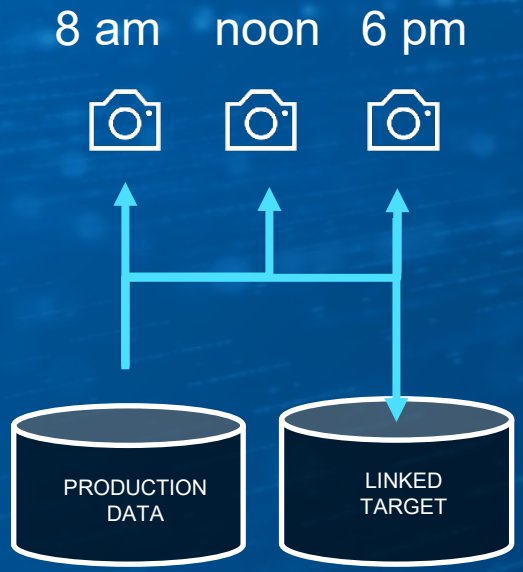
Ensure Z compatibility & performance for successful consolidations

DELL Technologies

SnapVX: Space Efficient Snapshots

Each snapshot is ~ 99.9% smaller than the actual data it points to

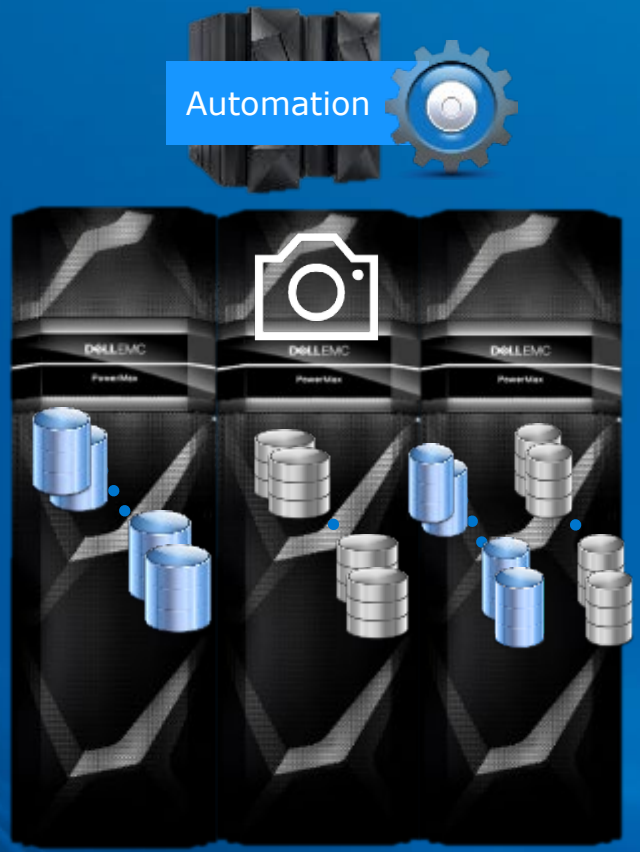
- Simple to make and manage
- No performance impact
- Two flavors
  - “non-secured” for read-only continuous data protection while saving space
  - “Secure” for further protection against accidental or malicious deletion



Dell EMC mainframe exclusive: “2nd copy NOT required” for restoration of data

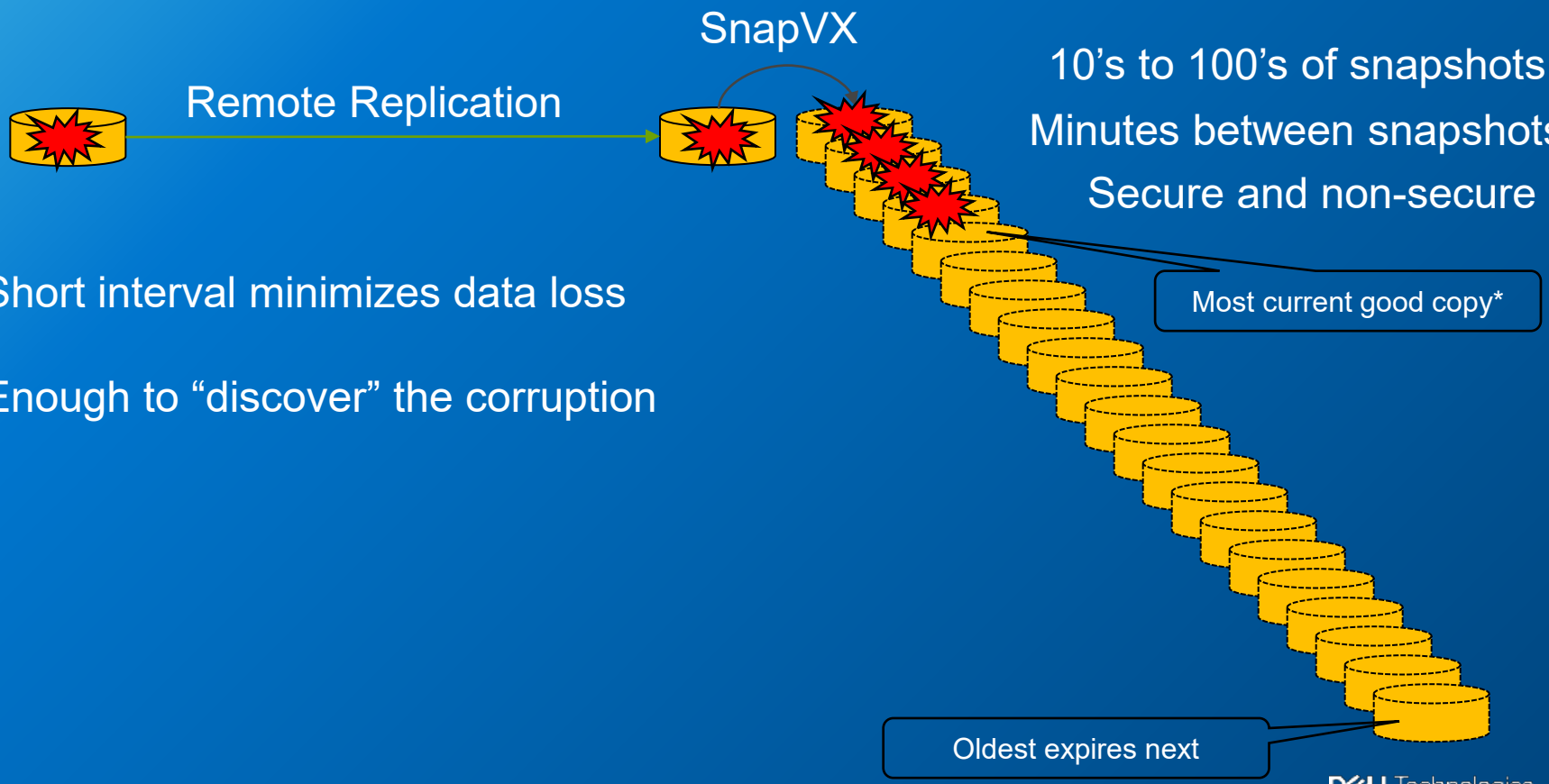
zDP: The key to Mainframe Cyber Resiliency

- Automates SnapVX snapshot creation/deletion under z/OS
- Rapid recovery from
  - Processing error
  - Human error
  - Malicious intent
- Continual point in time copy creation
  - Granular (5 minutes)
  - Automated
  - Immutable
  - Selectable recovery points
- 2-actor security option



DELL Technologies

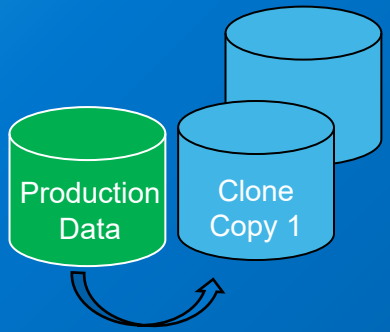
Dell EMC SnapVX / zDP logical protection



Traditional mainframe protection vs. SnapVX protection

space savings + cyber resiliency

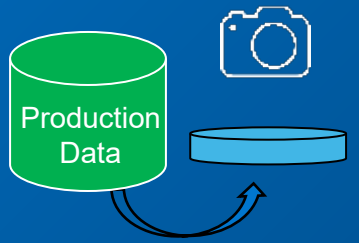
Traditional



- Required array capacity sized as 100% per clone
- RPO = up to 24hrs* of data loss
- Each clone (gold copy) creates a recovery point at the expense of 100% overhead!!

*Single Clone / gold copy

PowerMax



Up to
288 zDP Snaps
Per day

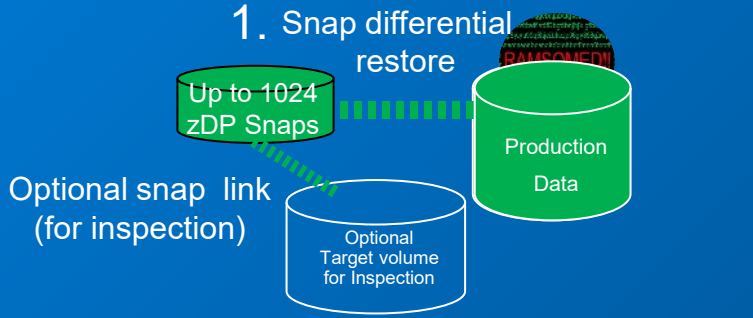
- Total required capacity = small % for each snap
- Smallest RPO = 5 minutes
- Up to 288 Gold copies / day
- Up to 1024 gold copies per volume

DELL Technologies

Dell Technologies simplifies data restoration

Dell Technologies

1 Step (instantly) + 40% of Production data (optionally check before restore)



Selected timestamped snap has all pointers to data needed to restore

- Good data is immediately available after the snap is selected
- Optionally, a “target volume” can be defined for “inspection” of restoration
- Required snap capacity ~40% additional capacity for up to 1,024 Point in time copies

Advisory Services

DELL Technologies

Why Dell Technologies for mainframe Cyber Resiliency and Recovery?

zDP & SnapVX form the most robust, space efficient foundation for CR; the most protection in the least amount of space.

Dell's pointer-based CR use up to 6x Less reserve capacity than other implementations. (40% vs. up to 250%)

Dell CR can create up to 12 inaccessible (non-addressable) protection points vs. a recommendation of a single point. (minimum RPO is based on a 5-minute interval snap vs. minimum RPO of one hour for other implementations.)

Dell's CR for DASD enables 1,024 snaps per volume vs. others.

Dell Technologies single step CR snap recovery makes data immediately available vs. requiring 2 copies and 4 steps, including a mandatory fiber channel connection external to the storage being recovered.

Dell's exclusive use of z/OS System Authorization Facility (SAF) provides a "2-actor security" capability, preventing a single rouge or "company insider" from altering protection. Dell support is required to modify this setting.

Dell Technologies CR implementation is flexible, offering both virtual and physical vault capability

Dell Technologies Professional Services shortens the CR implementation time while adding insight and value.

DELL Technologies

Cyber Recovery Advisory & Implementation

Finalize architecture options while implementing a foundational Cyber Recovery capability

Project Kick-off and Definition

Identify and collect Cyber Security and BCDR background/collateral on potential applications.

Technical Workshop

Discuss cyber vault architecture and operation to create cyber vault architecture, metrics, location and operation considerations

Critical Materials & Data Workshop

Identification of Critical Materials to target for initial implementation of Cyber Vault. Preliminary estimate on application data to be protected.

Infrastructure Configuration

Configure Cyber Recovery Vault Infrastructure, Hardening and Deploy air-gap copy and data immutability capability

Recovery Testing

Develop recovery test plan and conduct knowledge transfer of vault operations, security analytics and restore processes

Deliverables

- Service Overview & Logistics
- Service Tasks Schedule
- Cyber Recovery Overview

- Cyber Recovery Architecture
- Cyber Vault Considerations
- High-Level Vault Design

- Cyber Vault Data Quantity and Copy Stream Recommendations
- Vault Implementation Preparedness

- Vault Configuration Documentation
- Hardening Document
- Air-Gap Copy, Policies & Immutability
- Vault Restore Procedures

- Restore Test Plan & Report
- Data Appropriate Security Analytics Techniques
- Analytics & Operationalization Roadmaps

DELL Technologies

Case Study – Mainframe DASD & Tape

Recover business critical systems associated with mainframe systems

Challenges

- Concerned about emerging Cyber Threats and internal actors
- Mainframe focused

Solution

Cyber Recovery Implementation

- Customer moved to 4-site approach – SRDF-SQAR
- Implemented zDP off the DR side of each site
  - Every 10 min at one site
  - Every day at a second site
- 250 copies over 23,000 volumes and multiple frames

Results

- Developed a comprehensive solution enabling recovery of all mainframe data (DASD and DLm) to enable operations in the event of an extreme Cyber attack.
- Demonstrated key functionality of a Cyber Recovery vault such as data immutability, process integrity and recovery.

DELL Technologies

Case Study – Heterogeneous Mainframe Environment

Recover business critical systems associated with mainframe & open systems

Challenges

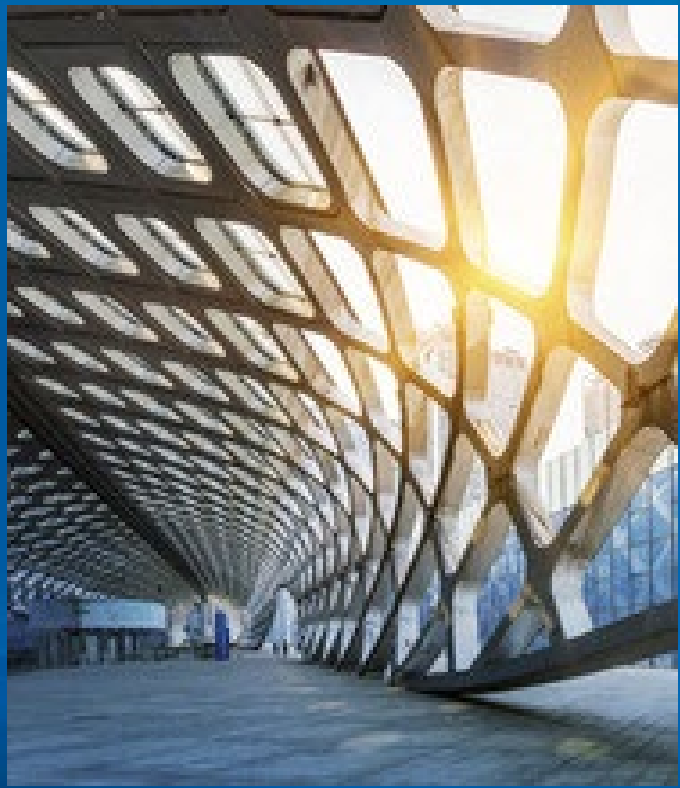
- Security is paramount for this customer, one of the world's largest Banking and financial services institutions
- The Bank identified 426 critical business and IT applications

Strategy

- Engaged an advisory firm to assess the market and identified the Dell Technologies cyber security solution as the solution
- Start small and scale out
- Implemented immediately using agile methodologies.

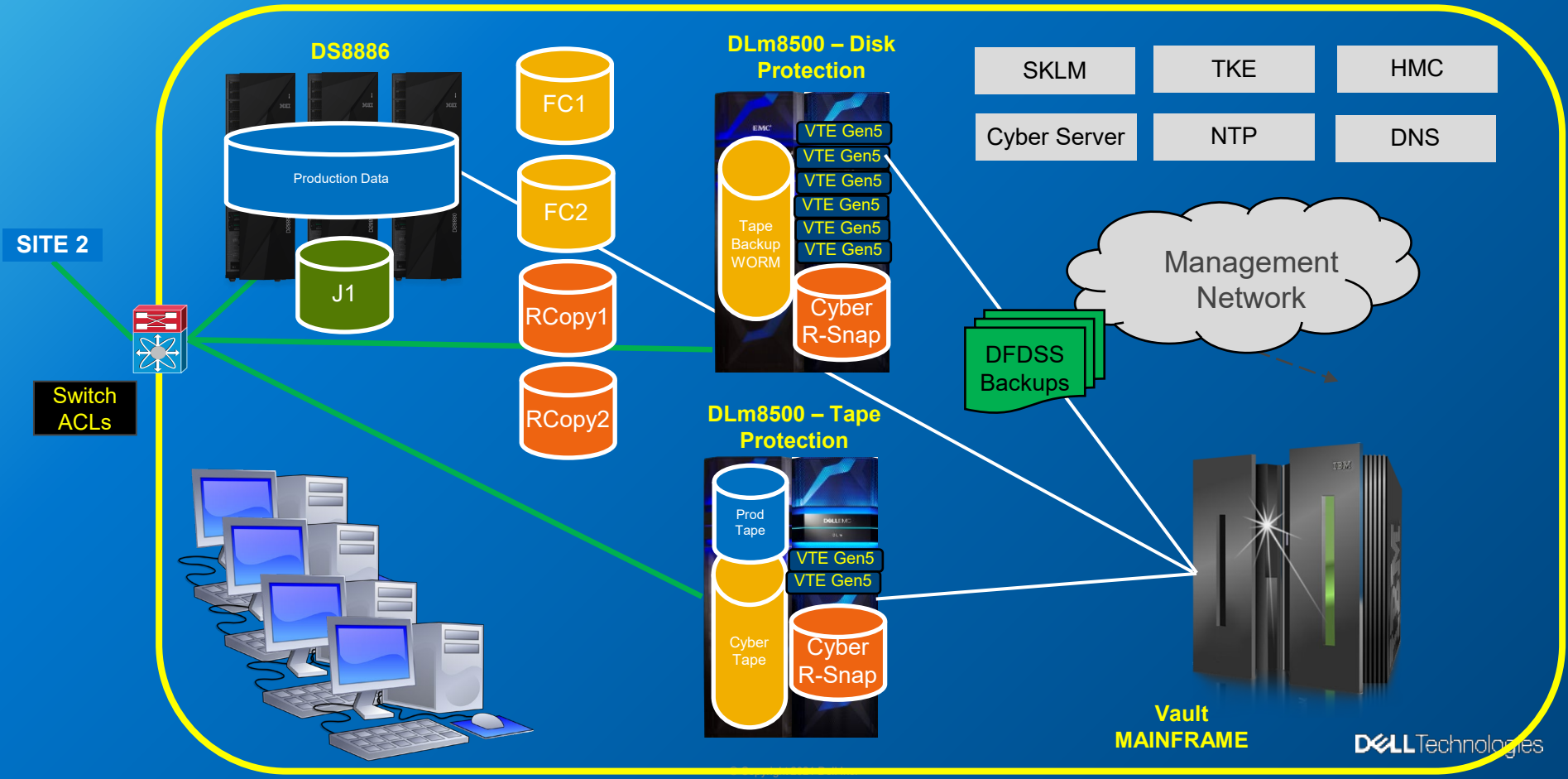
Solution & Benefits

- For open systems, implemented backup domains in the UK, Asia and the U.S. to provide a segregated vault.
- For the mainframe, replaced the existing virtual tape environment in Asia and the U.S. with DLM8500, Data Domain to create efficient off network copies



DELL Technologies

Cyber Recovery Vault



DELL Technologies
Cyber recovery & data protection leadership

2015	First “Isolated” recovery solution with custom deployment
2016	zDP: 1st z/OS implementation of logical corruption protection
2018	Introduced PowerProtect Cyber Recovery solution
2019	First technology vendor in Sheltered Harbor Alliance Partner Program
2020	First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery
2021	Introduced PowerProtect Cyber Recovery for Multi-Cloud
2021	Introduced PowerProtect Cyber Recovery for AWS

900+ **Cyber Recovery Customers**
(includes distributed and mainframe)

#1
Data Protection Appliances & Software*

[1] Based on combined revenue from the IDC 3Q20 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 3Q20 Storage Software and Cloud Services Qview.
[2] IDC 3Q20 Storage Software and Cloud Services Qview

DELL Technologies

Next Steps

DELL Technologies

Next step: Interactive Discovery Session

- Please share the story (in < 24 minutes!): YouTube Dell Mainframe Cyber
- Assess the current Tape and DASD Environment
- CR Design Considerations
  - Review topology
  - Cyber Recovery vault (physical / virtual / both)
    - Air gap considerations
  - Secure copy requirements
  - Required monitoring
  - Recovery process
- Cyber Resiliency & Recovery Expectations
  - Recovery Point Objective
  - Recovery Time Objective
- CR Testing
  - Frequency, personnel, certification
- Define Success Criteria


DELL Technologies