zSystems **Resiliency**

Maintaining Operations under Unplanned Outages

Diego Bessone
Director, IBM zSystems Global Sales

Reduce risk for business resiliency

Secure your data and systems to protect against current and future threats

Take the complexity and ambiguity out of compliance audits

Proactively reduce the impact of downtime

Increased protection and privacy and simplified compliance

Quantum-safe cryptography to help protect your business against “harvest now, decrypt later” quantum attacks

Industry first quantum-safe system

Protect sensitive data

Create crypto inventory

Reduce number of skilled resources needed for audit preparation functions and increase the confidence in your security positioning

Optimize resources

Assess compliance posture

Identify compliance drift

Business continuity is a key aspect of cyber resiliency

Avoid service disruptions proactively by managing capacity across locations and transferring workloads on demand

Greater flexibility

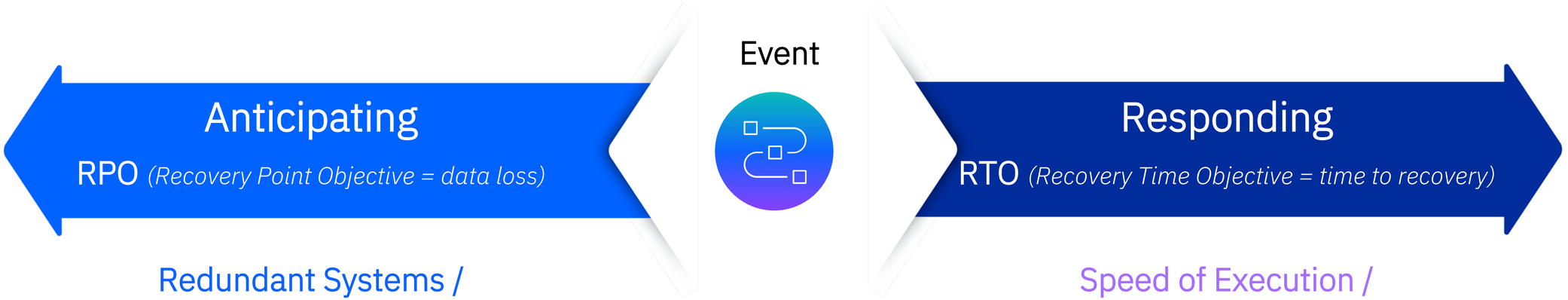
Complete client control

Simplified compliance

IBM z16 A02 systems, with GDPS, IBM DS8000 series storage with HyperSwap, and running a Red Hat OpenShift Container Platform environment, are designed to deliver 99.99999% availability. [2]

[1] see disclaimer chart for claims

Anticipating and responding to an event is increasingly complex, and the speed and precision of response is increasingly critical



Redundant Systems / Redundant Data

Synchronous Replicated Copy
Asynchronous Replicated Copy
Point-in-Time Copy

Parallel Sysplex®
Recovery Systems / MIPS Availability

HA
DR
Cyber

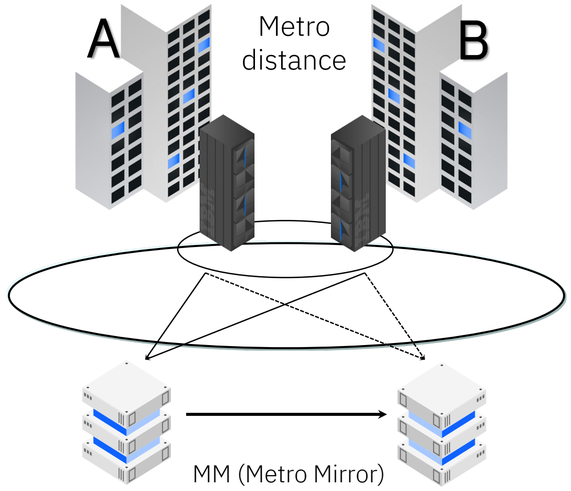
Speed of Execution / Restoration of Service

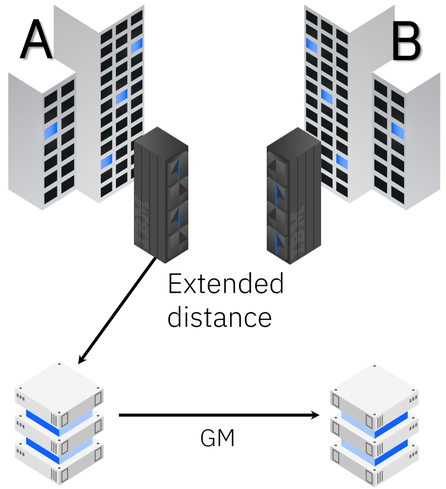
HA Recovery Procedure / Runbook
DR Recovery Procedure / Runbook
Cyber Recovery Procedure / Runbook

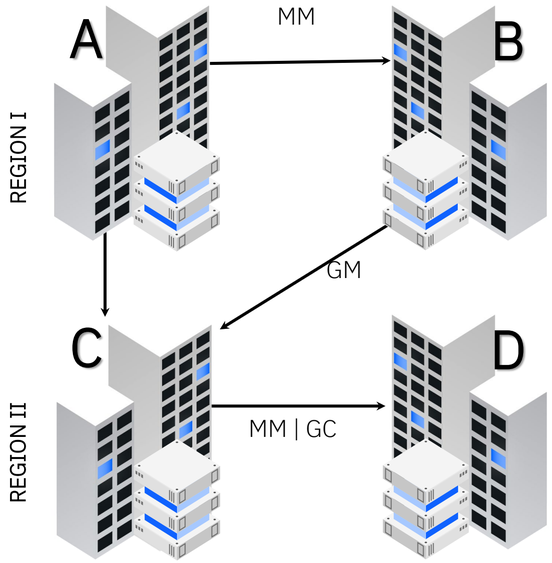
Risks:
Human Error
Lost Data Consistency
Difficulty Returning to Normal Operations

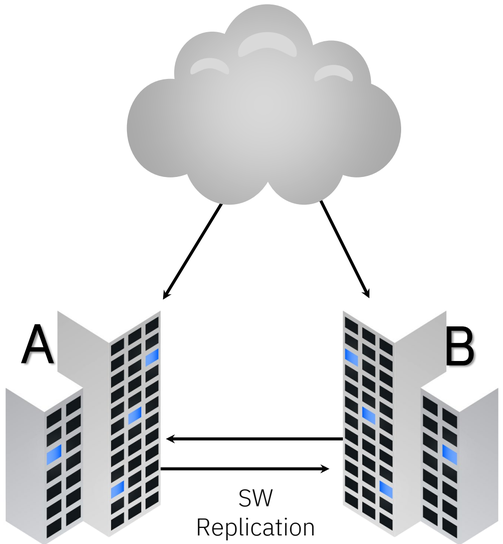
GDPS: Balanced HA/DR solutions designed to address different client requirements

GDPS Metro	GDPS Global	GDPS Metro Global	GDPS Continuous Availability
Near-continuous availability and recovery at metro distances	Disaster recovery at extended distance	Near-continuous availability regionally & recovery for 3-4 sites	Near-continuous availability, recovery & workload balancing
Systems remain active Multisite workloads can withstand site and storage failures	Rapid systems DR with “seconds” of data loss	Metro near-continuous availability and out of region disaster recover	Continuous availability at unlimited distances









Business continuity **The landscape is changing**

Regulators around the globe are introducing more stringent policies in relation to business continuity and disaster recovery requiring more comprehensive and extended testing mandating clients switch over full production loads and operate for **30 days up to 6 month** out of their secondary data center.

FFIEC / NY DFS

Institutions should demonstrate, through testing that their business continuity arrangements can sustain the business until permanent operations are reestablished.

Involve a sufficient volume of all types of transactions to ensure adequate capacity and functionality of the recovery facility.

Exercises generally extending over a longer period to allow issues to fully evolve as they would in a crisis and to allow realistic role-playing of all the involved groups.

EU NIS 2 Directive

EU regulators are clearly indicating the emergence of new requirements that surpass prior legislation like Operational Resiliency (ex Basel III), dealing from component failure to acknowledge risks associated to cyber attacks.

When the service is Cross-European (ex Real Time Gross Settlement, EU Securities Settlements et cetera) ECB and EBA will supervise directly meaning companies must adhere to a “Resiliency testing framework”.

Regulators are asking to prove that a secondary Site (DR) is fully functional and can run production for a long time.

NIST Special Publication 800-53

CP-2(6) Plan for the transfer of mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

CP-4(4) Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

CP-7(6) Plan and prepare for circumstances that preclude returning to the primary processing site.

Preventive maintenance strategies

Enterprises need operations to continue uninterrupted while maintenance is performed, an issue is addressed, or a new component is installed

Be proactive not reactive

Often, major outages, data interruptions, and downtimes are directly caused because simple, physical maintenance and care haven’t been properly established

Equipment repairs are costly

Emergency equipment repairs come at a high cost—especially if you add in the ancillary costs of business disruption, downtime and reputational damage

By managing equipment with the right maintenance strategies, at the right time, data center operators can reduce capital and operating expenses, and—most important—improve uptime

Remote management

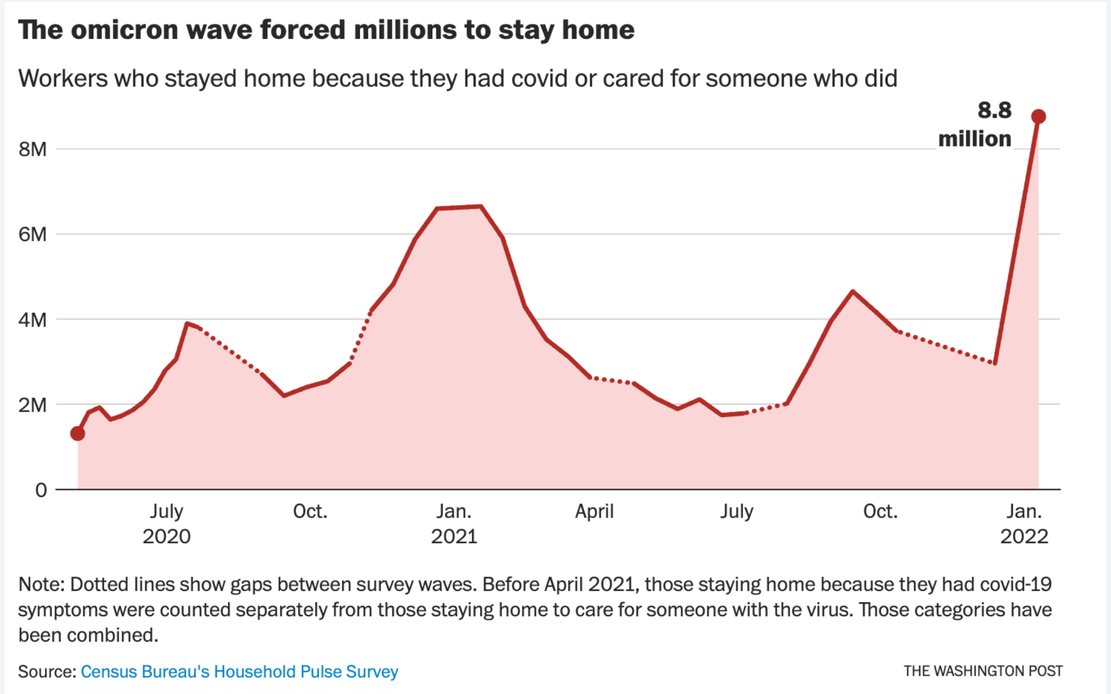
According to a report released by Honeywell, nearly all respondents (96%) indicate remote management is (or would be) important to their facility, yet only 34% of those surveyed currently have such a system in place

- Rethinking Data Centers as Resilient, Sustainable Facilities

Avoidance of natural disasters, climate change, and COVID-19 impact

Texas Deep Freeze
Extreme cold shuts down data centers in Texas

Unprecedented weather conditions caused data center outages for bus carriers, healthcare companies, insurance providers, credit unions and the city of Austin



COVID-19 continues to challenge data center industry

Strategic capacity planning is more critical than ever

More people than ever, especially with the recent omicron variant, are staying home and consuming data from video conferencing to streaming services

IBM z16 is built to build

We built a powerful and secure platform for business. Let’s build the future of yours.

Predict and Automate for Increased Decision Velocity

Apply insights at speed and scale to create new value in every client interaction

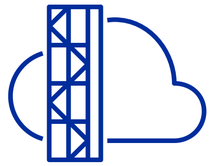
Increase productivity and lower operational costs with automation and AIOps

Secure with a Cyber Resilient System

Secure data and systems now and in the future with quantum-safe protection

Address ever-increasing regulations with automation for compliance

Plan and mitigate risk of potential future outages



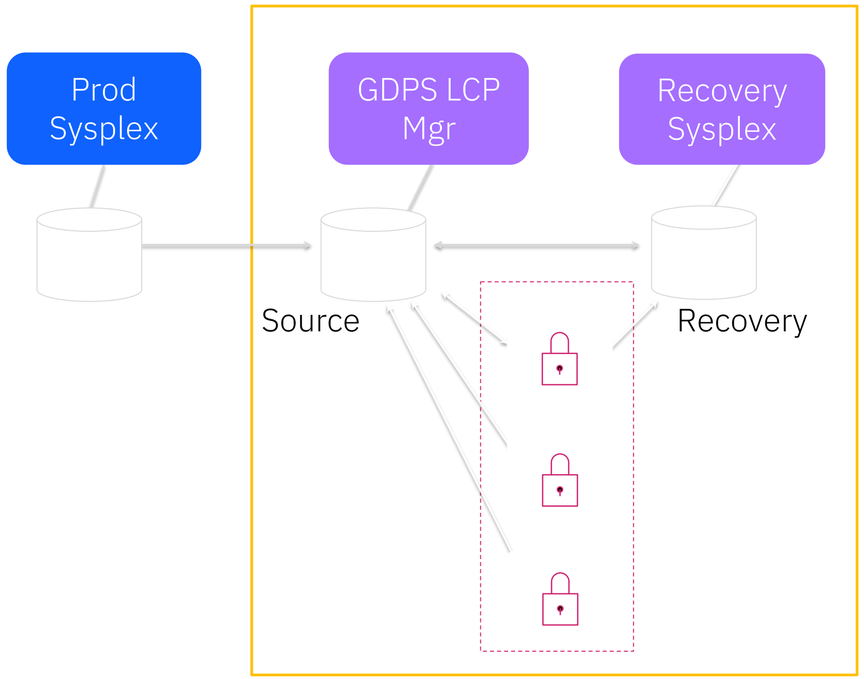
Modernize with Hybrid Cloud

Empower developers with agility to accelerate modernization of existing workloads

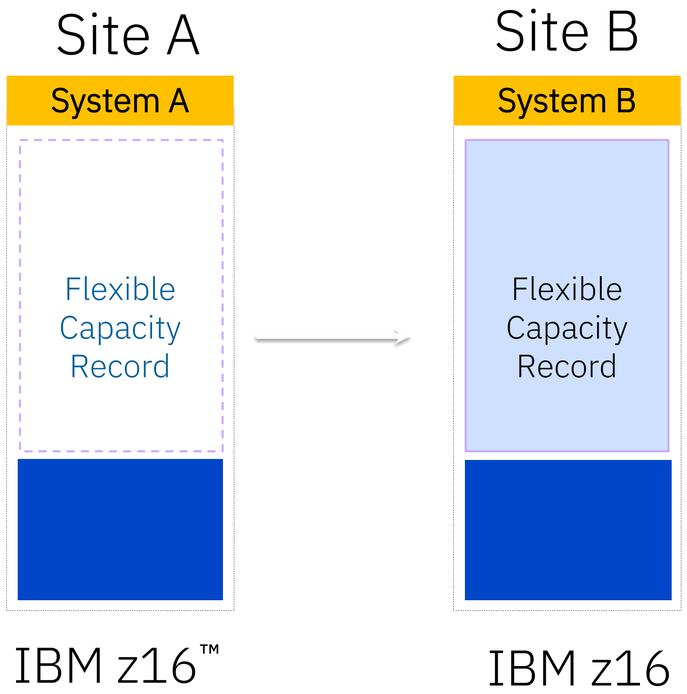
Enable integration of IBM z16 workloads with new digital services across the hybrid cloud

Important GDPS features that expand and enhance resilience capabilities

Logical Corruption Protection (LCP) **Manager** automates your cyber resiliency capabilities



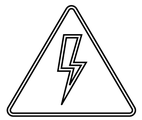
For **Flexible Capacity**: GDPS can automate the transfer of flexible capacity from one site to another



IBM Z Flexible Capacity for Cyber Resiliency

Use Cases

Disaster Recovery & DR Testing



Transfer the capacity you need at your DR site to continue to run your business workloads. Automate and test recovery procedures for unplanned outages, including cyber attacks to provide near-continuous availability and disaster recovery.

Frictionless Compliance

Meet the ever-evolving stringent requirements of global regulators, allowing a highly automated and fast process to demonstrate a production site swap.

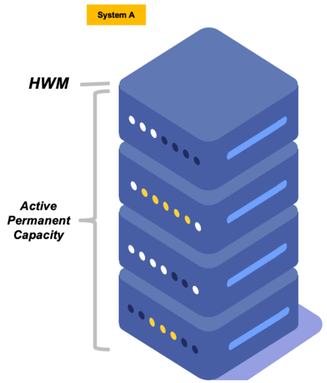
Facility Maintenance

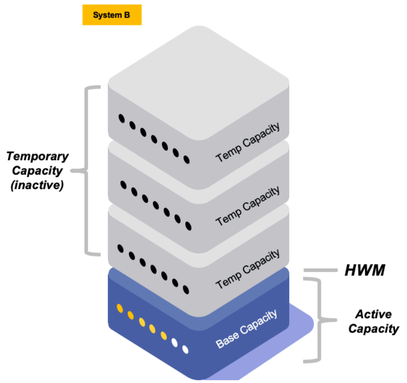
Run your production workload from your alternate site while you perform maintenance at your primary site with the capacity you need.

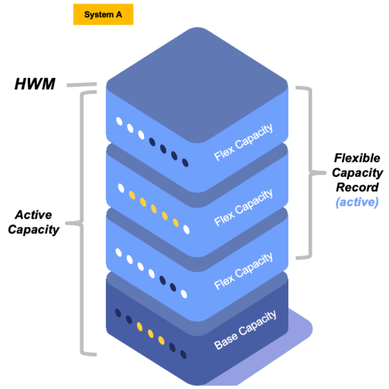
Pro-active Avoidance

Protect your critical business services from natural disasters. Avoid rolling power outages. Migrate your critical workloads to an alternate site before your business gets impacted and stay there for up to one year.

Technical Overview

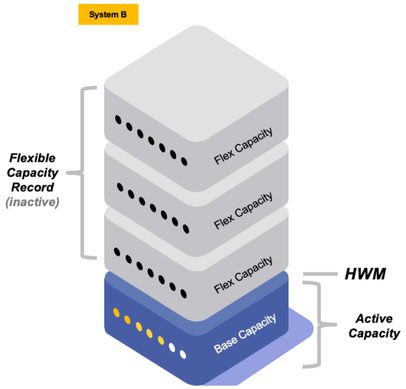






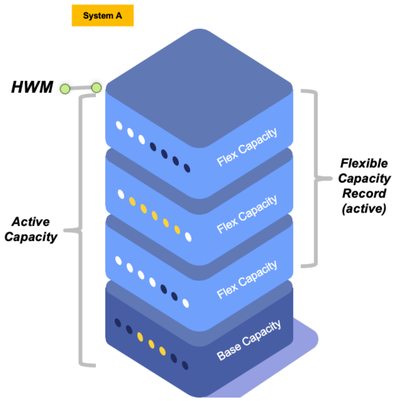
New Flexible Capacity temporary capacity record

All Engine Types supported (GPs, zIIPs, ICFs, IFLs)



Workload Transfer

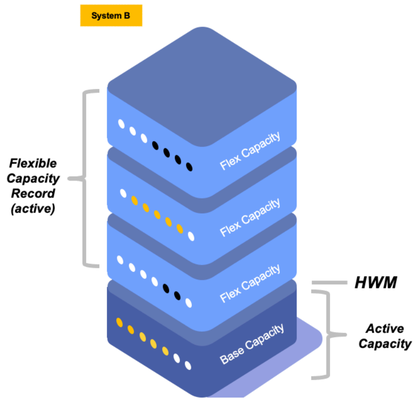
Site A



Fully automatable using IBM GDPS

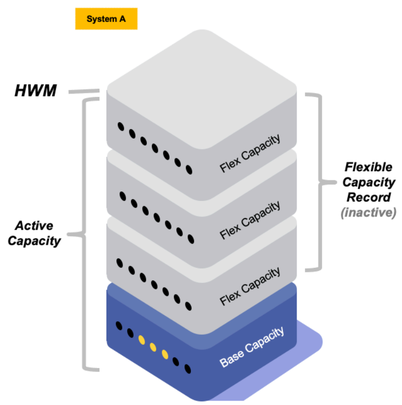
Up to 24 hours overlap period for workload transfer

Site B



Swap completed

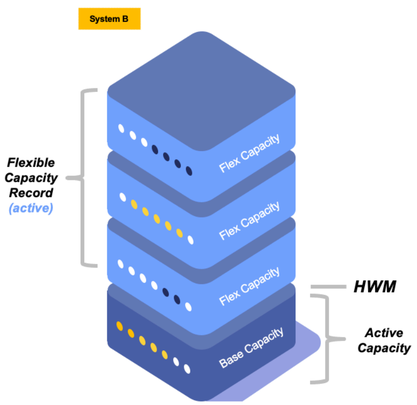
Site A



Run production from your alternate site for up to 12 months

Transfer your production up to 12x a year

Site B



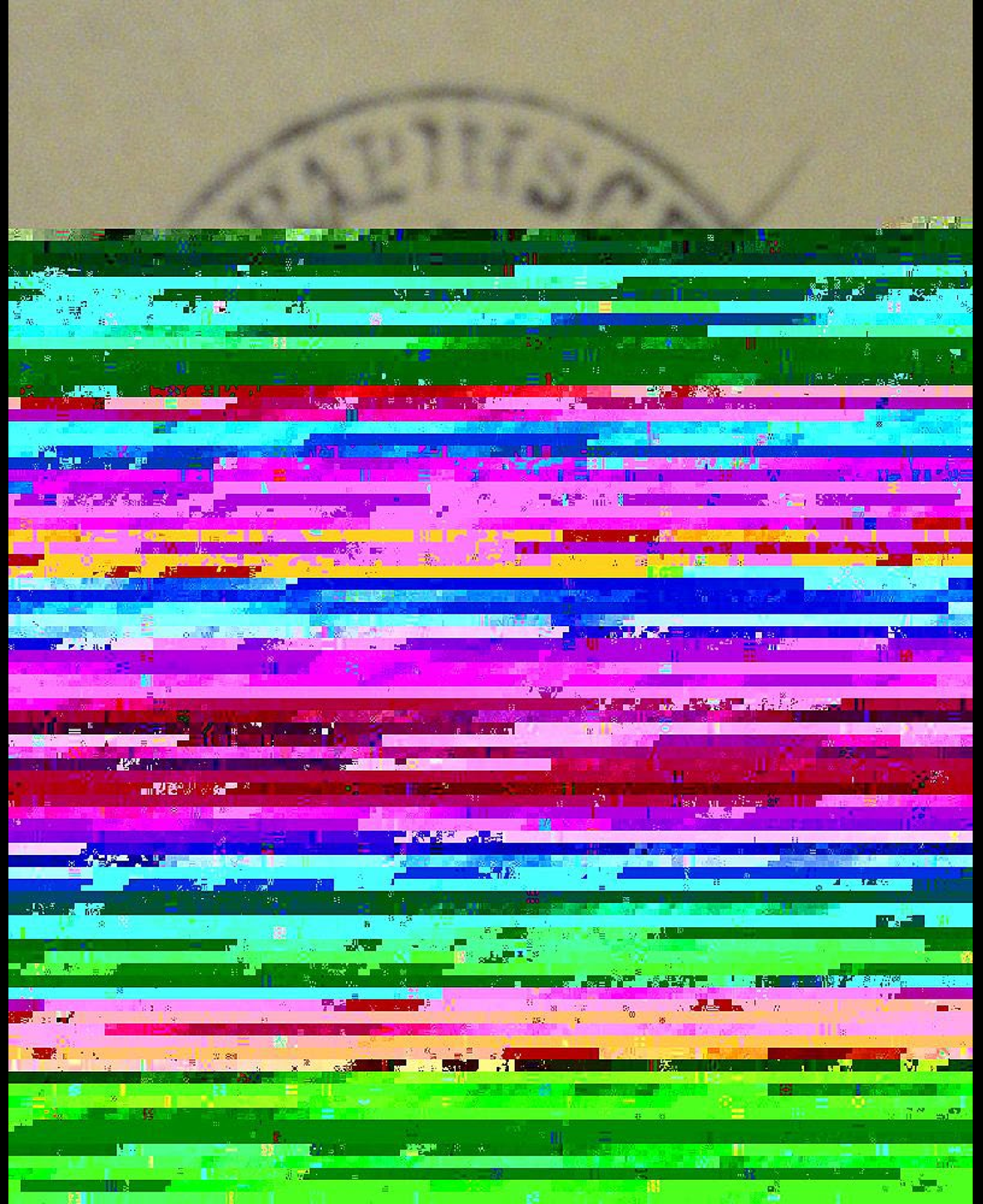
Logical data corruption

Data corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

There are two types of data corruption associated with computer systems: **undetected** and **detected**.

Undetected data corruption, also known as **silent data corruption**, results in the most dangerous errors as there is no indication that the data is incorrect.

From Wikipedia, the free encyclopedia



Why traditional resiliency solutions will not protect you from logical data corruption

	You have	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

Asia Pacific

2 minute read · September 26, 20224:36 PM EDT · Last Updated 2 days ago

Australia flags privacy overhaul after huge cyber attack on Optus

Reuters

SYDNEY, Sept 26 (Reuters) - Australia plans to toughen privacy rules to force companies to notify banks faster when they experience cyber attacks, Prime Minister Anthony Albanese said on Monday, after hackers targeted the country's second-largest telecoms firm.

Optus, owned by Singapore Telecoms Ltd (STEL.SI), said last week that home addresses, drivers' licences and passport numbers of up to 10 million customers, or about 40% of the population, were compromised in one of Australia's biggest data breaches.

Summary of EU's Digital Operational Resilience Act (DORA)

The EU regulation proposal is a legislative attempt to streamline information security risk management processes to increase digital operational resilience across the Financial Services sector

What does it focus on?

Introduce a comprehensive framework to mitigate cybersecurity risks and **improve operational resilience across the Financial Sector**

Who does it apply to?

- Traditional financial entities
- „Fintech" companies
- **Third party service providers** of financial entites

When will it apply?

- Expected to become **EU wide regulation in 2022**
- Allowing grace period of 12-18 months

Why should I care?

- **Avoid penalties**
- Mitigate impact of cyber threats
- Reduce time and costs of incident recovery

What can I do?

- **Take early action** to prepare for DORA's compliance obligations

A penalty of 1% of the average daily worldwide turnover of the impacted critical ICT third-party service provider in the preceding business year may be imposed. Other administrative penalties are advised by Member state authorities based on the nature of the breach.

THE WALL STREET JOURNAL.

RISK & COMPLIANCE JOURNAL

Merck's Insurers On the Hook in $1.4 Billion NotPetya Attack, Court Says

A court rejected arguments by insurers that they shouldn't have to cover Merck's losses from the Russia-linked attack

By *Richard Vanderford* Follow

May 2, 2023 at 3:42 pm ET

Thousands of Merck computers were damaged six years ago after malware entered the company's systems through accounting software. PHOTO: ANDREW KELLY/REUTERS

Insurers for Merck & Co. must help cover losses from a $1.4 billion cyberattack that the U.S. blamed on Russia, a court said, rejecting the insurers' argument that the attack was akin to an act of war normally excluded from coverage.

Cyber resiliency on IBM Z

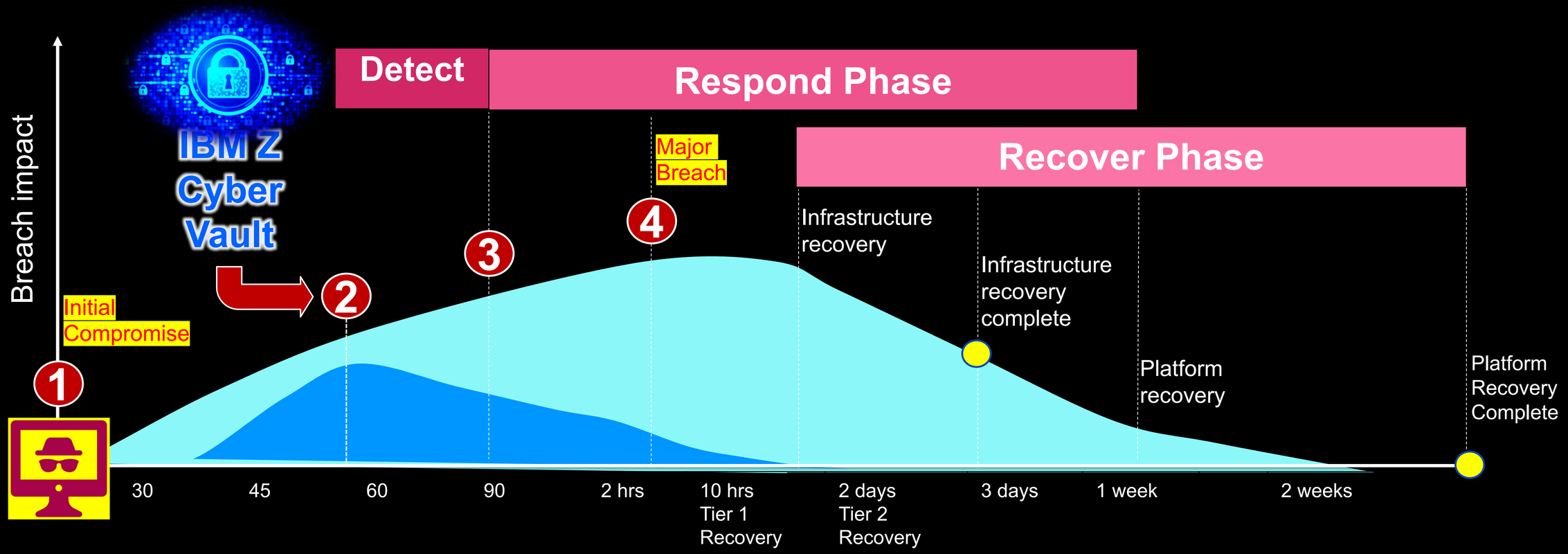
Cyber resilient systems must have the ability to anticipate, withstand, and recover from adverse conditions, stresses, or attacks.

- ✓ Encryption everywhere
- ✓ Confidential Computing
- ✓ IBM Fibre Channel Endpoint Security
- ✓ IBM Enterprise Key Management Foundation
- ✓ Cryptographic acceleration with Crypto Express7S
- ✓ Cryptographic coprocessor on every core with CP Assist for Cryptographic Function (CPACF)
- ✓ IBM Guardium
- ✓ IBM Security zSecure

- ✓ GDPS
- ✓ High Availability
- ✓ Disaster Recovery
- ✓ IBM System Recovery Boost
- ✓ IBM Z Cyber Vault

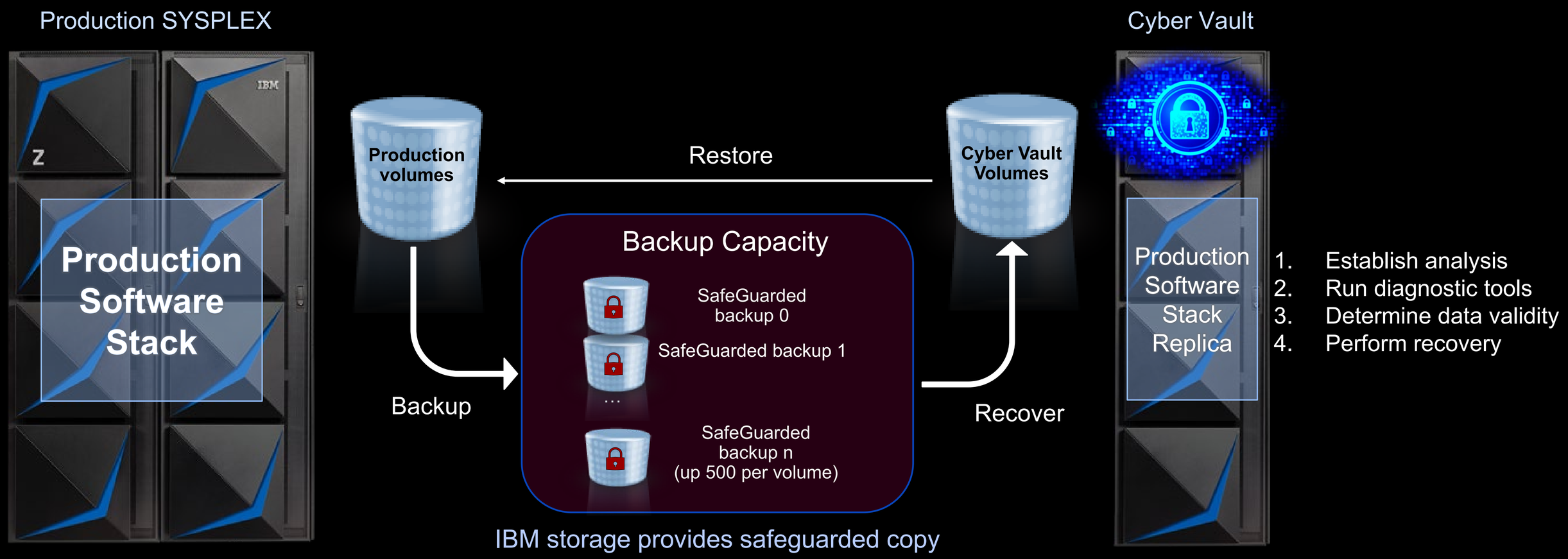
IBM Z Cyber Vault

Speedy recovery to significantly reduce the impact of breaches



1. Corruption of data occurs …
   … but not yet detected
2. Due to the Cyber Vault environment and the use of Safe Guarded Copy Technology, data is continuously checked, and corruption is found and corrected
3. Without the Cyber Vault environment corruption is detected much later and has a greater chance to spread
4. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Z Cyber Vault



IBM **Z** Cyber Vault capabilities

Data Validation
Detect data corruption early or certify 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

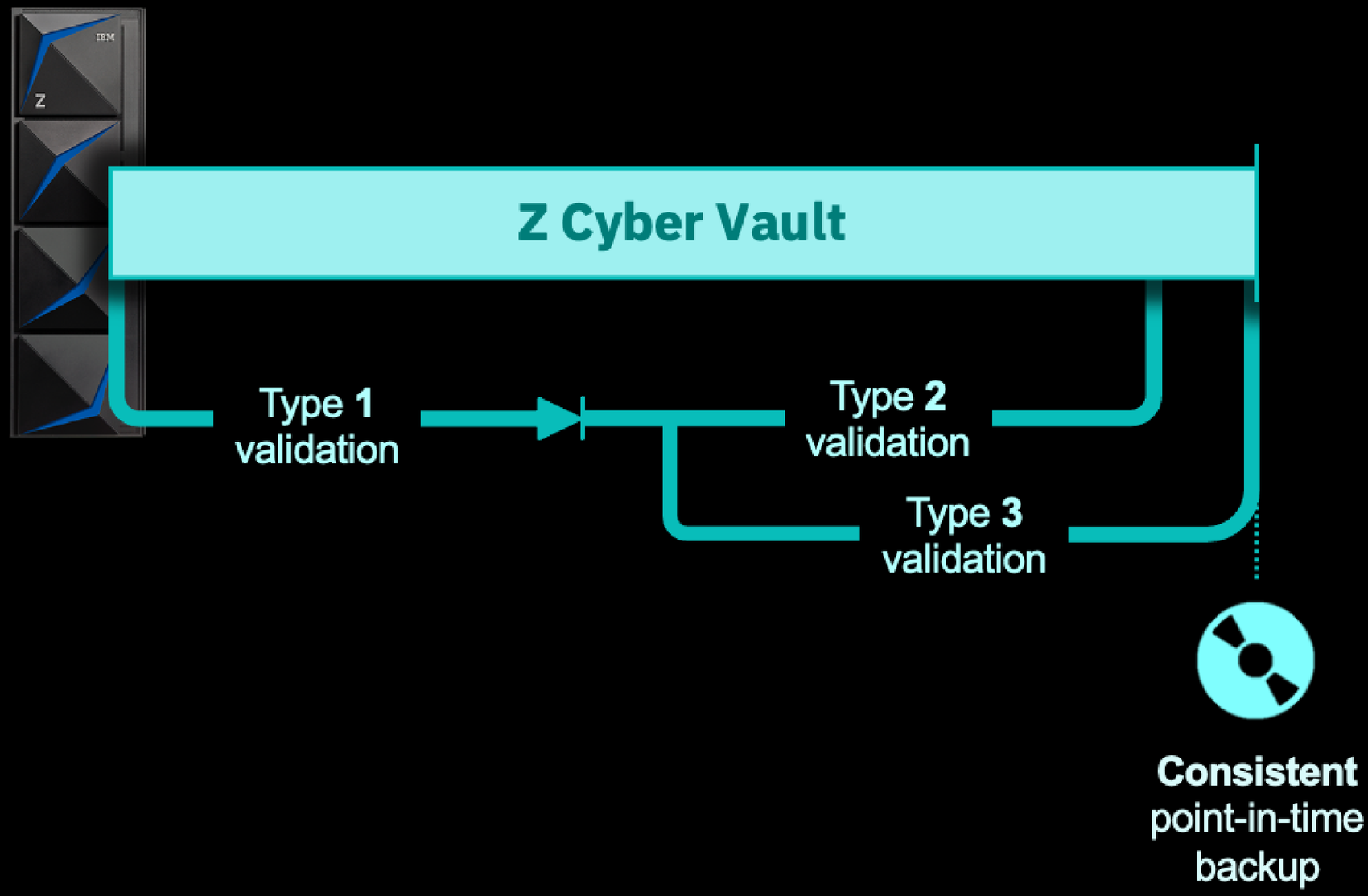
- IBM z/OS Utilities
- IBM Z Catalog management tools
- IBM Z Batch Resiliency
- IBM DFSMShsm tools
- IBM Security zSecure
- Db2 and IMS Tools

IBM Z Cyber Vault data validation

Type 1
z/OS system

Type 2
z/OS subsystems
& data structure

Type 3
Application data



IBM **Z** Cyber Vault as a **sandbox**

- Cyber Range for **Pentesting** and **Ethical Hacking**
- Chaos Engineering experiments

IBM Z Cyber Vault software selection – Start here

Here are the recommended tools to manage and provide resiliency capabilities to the z/OS environment, including the z/OS catalog, DFSMShsm backup subsystem, and security related aspects to identify unauthorized activity.

Solution	P	CV	Capability
IBM Tivoli Advanced Catalog Management for z/OS			
Pointer checking for the catalog.	✗	✓	Data Validation
Recovery of a catalog, including forward recovery to specific point in time.	✓	✓	Recovery
IBM Tivoli Advanced Reporting and Management for DFSMShsm			
Verify inventory data set records are in sync with migration and backup copies.	✗	✓	Data Validation
Compare reports between safeguarded copies taken at different times and find differences.	✗	✓	Forensic Analysis
IBM Tivoli Advanced Audit for DFSMShsm			
Conduct trouble-free audits and automate corrective actions.	✗	✓	Recovery
IBM Security zSecure Audit			
Potential identification of malicious database activities to help identify starting point of corruption.			
IBM CICS VSAM Recovery			
CICS VSAM Recovery (CICS VR) is used to recover lost or damaged VSAM datasets. It determines which CICS logs and VSAM backups are needed and constructs the recovery jobs.			

IBM Z Cyber Vault software selection – Db2

These are the products that, following IBM Best Practices, provide resiliency capabilities for your Db2 databases.

IBM Db2 Utilities Suite

- The Db2 Utilities Suite is at the core of managing DB2 for z/OS. Helps minimize downtime associated with routine DB2 data maintenance, while ensuring the highest degree of data integrity. It provides Db2 data operations such as REORG, LOAD, UNLOAD and more.

IBM Db2 Log Analysis Tool

- Provides the ability to pinpoint who did what and when to business critical Db2 data. It enables the flexibility required to track data changes by automatically building reports of changes made to database tables, as well as isolate accidental or undesired changes made to data, and optionally undo or redo changes made to data.

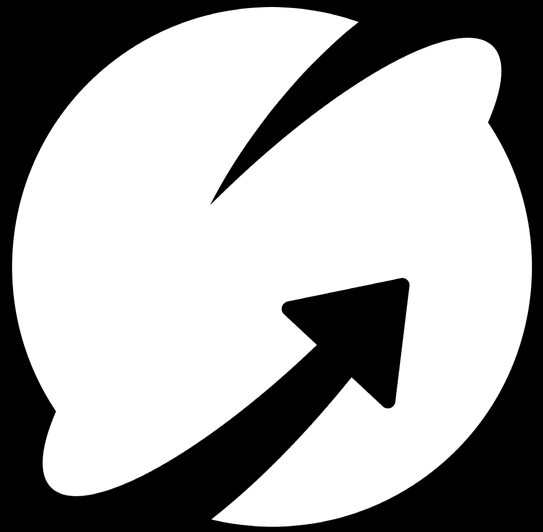
IBM Db2 Recovery Expert

- Analyzes data and conditions to drive the necessary Db2 backup recovery processes to meet Recovery Time Objectives. Recovery plans provide cost and time estimations. with recovery jobs are built and validated PRIOR to execution. Supports point-in-time, dropped object, transaction, redirected, application, system level and disaster types of recovery operations.

IBM Z Cyber Vault software selection – IMS

These are the products that, following IBM Best Practices, provide resiliency capabilities to your IMS database and transaction processing subsystems.

Solution	P	CV	Capability
IBM IMS High Performance Pointer Checker Pointer checking IMS full function databases	✗	✓	Data Validation
IBM IMS Fast Path Solution Pack Pointer checker function for Fast Path databases, aka DEDBs	✗	✓	
IBM IMS Recovery Solution Pack Database Recovery Facility component to validate all assets needed for recovery are available and can get to all of them	✗	✓	
IBM IMS Connect Extensions Collect and write data about IMS transactions coming in through IMS Connect	✓	✗	Forensic Analysis
IBM IMS Problem Investigator Deep dive analysis of IMS logs and IMS Connect Extensions journals	✗	✓	
IBM IMS Performance Analyzer Report on transactions that occurred during a specified period	✗	✓	
IBM IMS Recovery Solution Pack Recover specific IMS systems or databases based on the volume level backups	✓	✓	Surgical Recovery
IBM IMS High Performance Pointer Checker Repair specific segments in IMS full function databases without requiring full recovery	✗	✓	
IBM IMS Fast Path Solution Pack Repair specific segments in IMS Fast Path databases without requiring full recovery	✗	✓	
IBM IMS Queue Control Facility Recover and/or replay specific transactions	✓	✓	



Protect your **non-database-managed** data as **dynamically** as your online data

Modernize your non-database managed data to get **accurate, actionable insights**

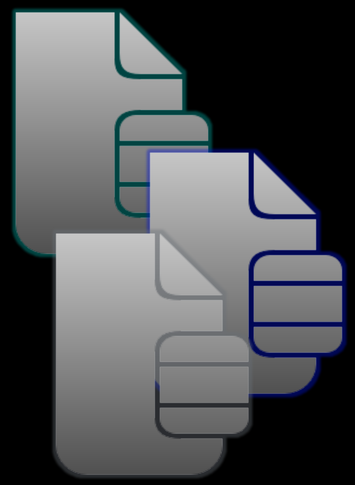
Automate recovery in minutes

Streamline your backup process with minimal human effort

Prove compliance beyond planned events

IBM Z Cyber Vault software – non-database managed files

Database managers keep track of **database activity** (logs) and provide tools to **recover** to a consistency point



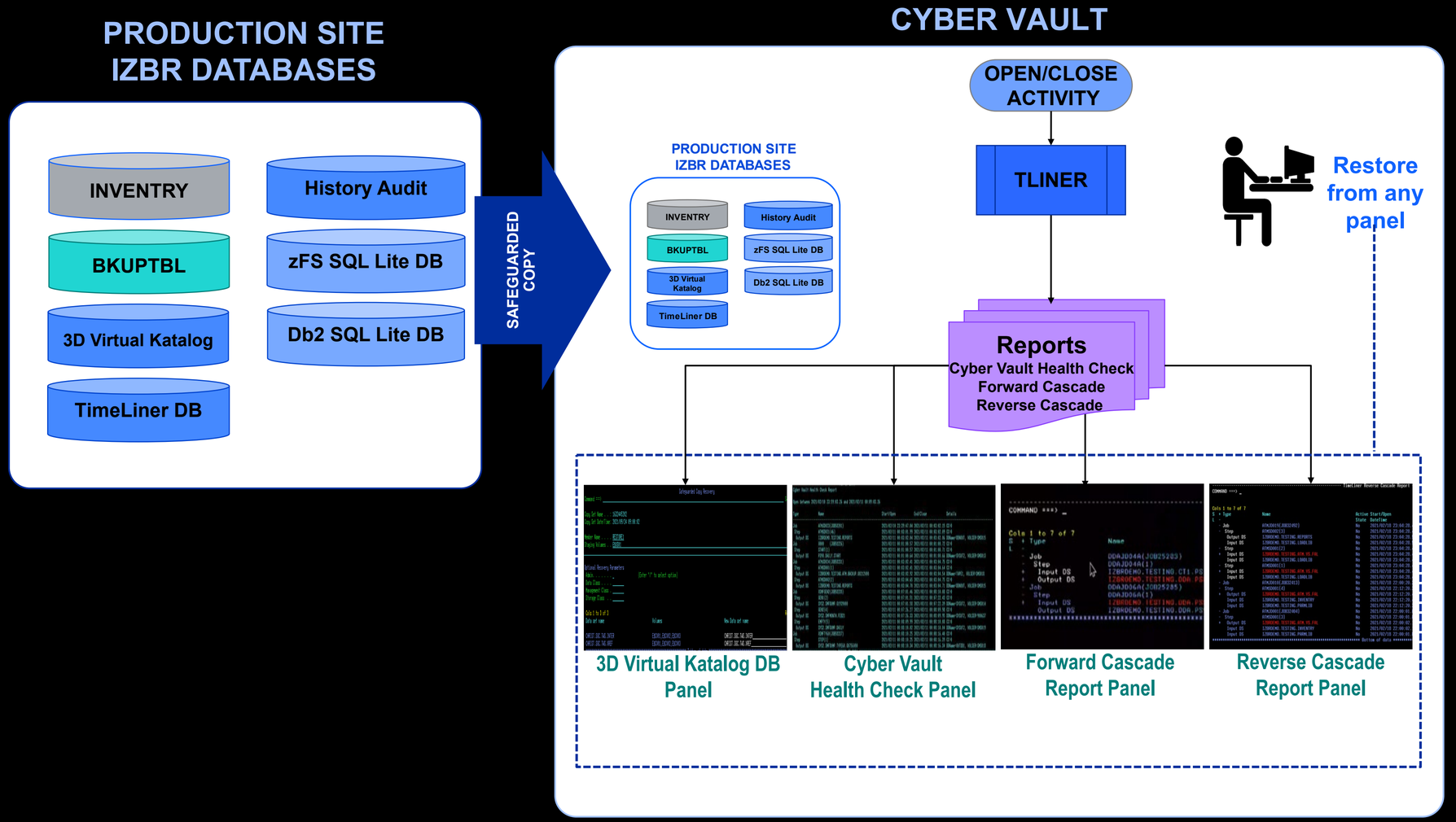
IBM Z Batch Resiliency v1.2 provides **log** and **recover** capabilities for non-database managed data, such as libraries, flat files, and VSAM datasets.

- Cyber Vault **health check** report for Safeguarded copies
- **TimeLiner reverse cascade** report for forensic analysis
- **TimeLiner forward cascade** report to create recovery plan
- **Panel driven** surgical recovery

Cyber Vault Support - Complete inventory of every data set in a Safeguarded Copy enables surgical recovery of any data set from Safeguarded Copy with Copy Services Manager (CSM) or GDPS LCP*

Capabilities to benefit recovery in IBM Z Cyber Vault deployments

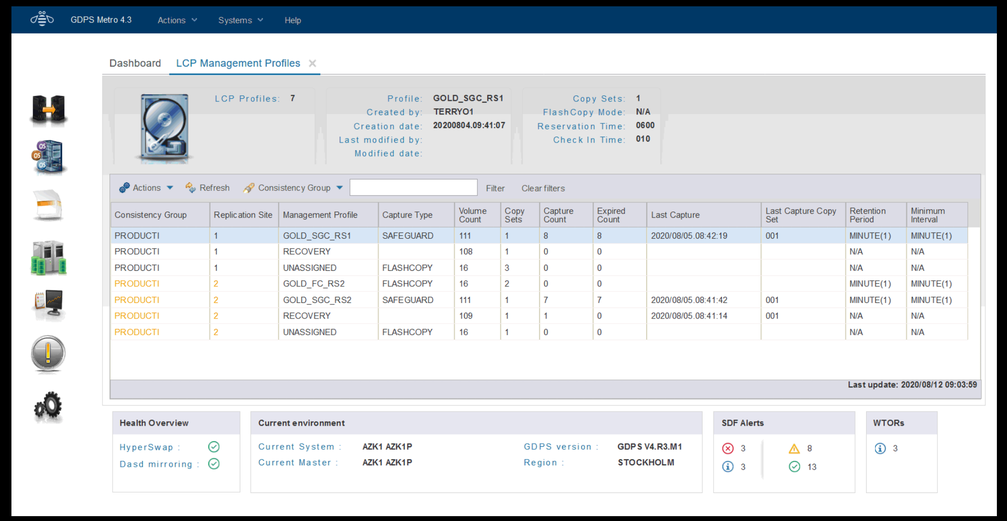
- Surgical recovery of ***any data set*** using 3DVK database, automatically generating accurate restore JCL
- Cyber Vault Health Check report identifies “at risk” non-database managed data in air gapped copy
- Additional forensic capability is created through HISTORY, AUDIT and INVENTRY including identification of critical input tape data
- Reverse Cascade report assists forensic investigation of corruption by identifying jobs and steps that updated the corrupted files, and when
- Forward Cascade Report assists in developing a forward recovery plan for the applications that use the data that is recovered



** Watch this APAR!*
APAR PH47869 – ‘Implement GDPS/LCP recovery support in IZBR’

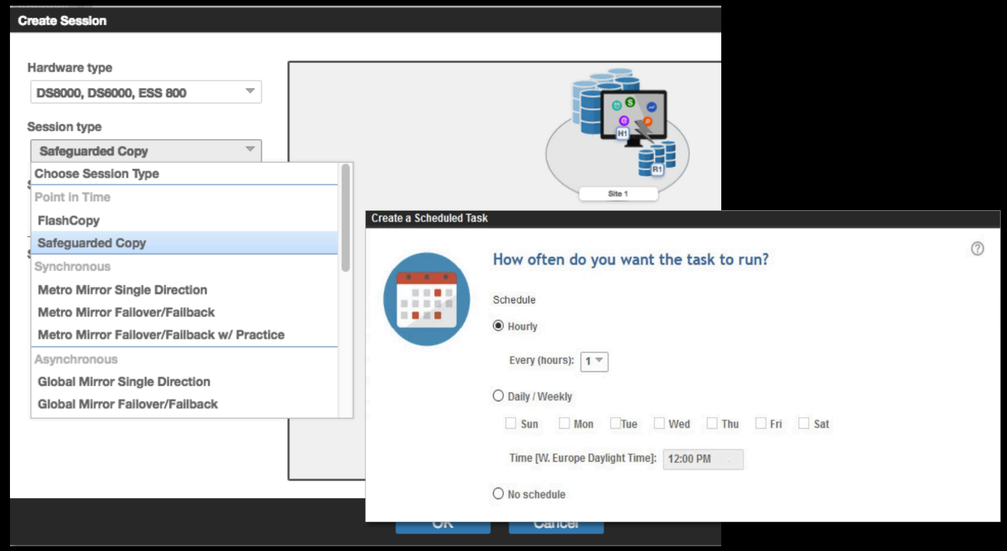
GDPS/LCP or Copy Services Manager (CSM) is needed to manage SafeGuarded Copy

Manage the whole Data Corruption Protection lifecycle with the same tool you manage your CA and DR environment with – GDPS/LCP is an enhancement to existing GDPS implementations. CSM can manage all DISK copy services.



Customer has GDPS installed?

GDPS/LCP to manage the data corruption protection solution is preferred



Customer has CSM installed?:

Integrate the data corruption protection solution

IBM **Z** Cyber Vault solution

IBM storage

Data volumes and active copies generated and maintained

DS8000 SafeGuarded Copy

Immutable backups

TS7700 Virtual Tape with Encryption and/or WORM

Secure air-gapped data vault

IBM Z and Software

The only System with a 99.99999% availability

EAL 5+ certified IBM Cyber Vault for Z LPAR for validation, testing and forensics

Data monitoring, consistency and anomaly detection

Management Software

IBM Security solutions

IBM Services

IBM GDPS provides services, clustering technologies, and server and storage replication and automation

Logical Data Corruption (LCP) and Copy Services Manager (CSM) enhancements manage the entire recovery environment

IBM Lab Services risk assessment and deployment services

The IBM Z Cyber Vault journey provides exponential value at each step.

Provides the foundation to respond to corruption events.

Reduces business impact by reducing the time to detect, respond and recover.

Improves compliance with retention requirements.

Implement SGC and GDPS LCP	*Create IBM Z infrastructure*	*Implement infrastructure to restore production*	*Implement and automate validation scripts*	*Implement infrastructure for offline backups*
Meets requirement to maintain PIT copies	Meets requirement to be able to recover a given SGC, IPL, and perform analysis	Meets requirement to be able to restore production from a given SGC	Aids in detection of corruption and reduces time to respond and restore services	Meets requirement for longer term retention at a lower cost

Time to restore production is days to weeks.

Time to restore production can be reduced to hours.

- ✓ Introduction and Overview
- ✓ Key threats
- ✓ Configuration Examples
- ✓ Planning and Considerations
- ✓ Storage sizing
- ✓ Safeguarded Copy & FlashCopy
- ✓ Infrastructure Design (GDPS, CSM, etc)
- ✓ Hardware Requirements
- ✓ Software stack
- ✓ Services
- ✓ Deployment and Implementation
- ✓ Sample code

BITMARCK Faces Data Breach, German Insurer Information at Risk

The threat actor claims to have access to hashed passwords, customer personal information, VIP customer and C-Level employee personal information and more.

by **Editorial** — January 18, 2023 in **Cybersecurity News** 1

German-managed IT service provider BITMARCK has been listed on a dark web data leak forum. A threat actor under the alias LeakBase has shared sensitive data from Jira and the database of the company.

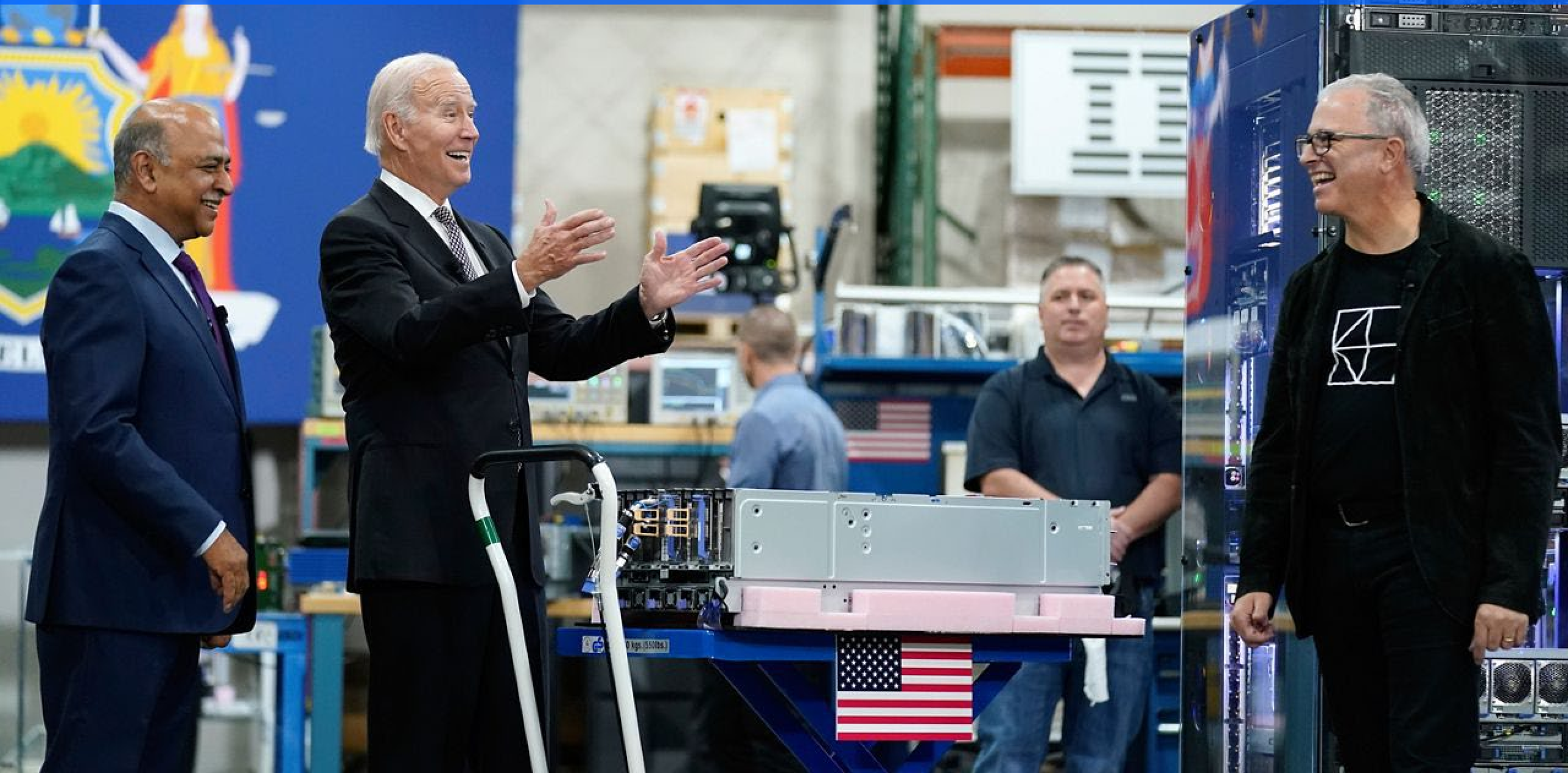
BITMARCK is a leading provider of IT solutions for the German public health insurance market, offering services to a variety of health insurers, including company and craft guild insurers, DAK-Gesundheit, and alternative insurers.

> The threat actor claims to have access to hashed passwords, customer personal information, VIP customer and C-Level employee personal information, user and employee personal information.

BITMARCK provides technical infrastructure, solutions, and consulting in the field of public health insurance. The company, which began operation in 1994, serves customers throughout the country.

IBM and CEO Arvind Krishna Welcome President Biden to Poughkeepsie Site, Company Plans to Invest $20 billion in the Hudson Valley Region Over 10 Years.

Oct 6, 2022




z16
CPC, I/O drawers
+ service elements
max 522 lbs


z16
Lansmont
ON
START


DANGER
PINCH POINT
z16