IBM Z Cyber Vault

It's a dangerous world
Cyber incidents and ransomware attacks are on the rise, as is the extent of the damage to the organization. No business or public sector institution is immune regardless of size. Numerous government institutions and businesses recently had to pay "ransom" to retrieve clean copies of their data that was corrupted by cyber criminals.

The rapid shift to digital in the pandemic has only increased the exposure and likelihood of an attack. According to Ponemon[1], malicious attacks caused 52% of breaches; one in five of these companies experienced an average total cost of breach of $4.77M USD.

Your current cyber resiliency, high availability and disaster recovery (HA/DR) plans may not be sufficient. What if the "trusted" data you count on for recovery is corrupted? Your recovery actions may in fact propagate errors and exacerbate the problem. That's been the case in recent publicized attacks[2]. Fast moving ransomware attacks propagate throughout your infrastructure in minutes or even seconds, causing screens to go blank, data being corrupted and IT staff having no time to respond. Critical systems and their backups failed, because the data had already been compromised. Recovery for one company was based on luck -- one site was offline at the time of the attack. Damages for companies involved were $10B USD.

Your mission critical applications are the lifeblood of your business and the associated data cannot be compromised. That's why **IBM Z® Cyber Vault provides air gapped data corruption protection and tools**. Unlike alternatives, it keeps up to 500 immutable, safeguarded copies of your data in a logical partition that is isolated and separated from your production system. The data is unable to be accessed from your production environment and contains function to identify logical data corruption and recover it with safe and trusted data. The air gapped data vault prevents reloading corrupt or compromised copies of data and can store hundreds of safeguarded copies for more precise restoration with little to no performance impact. You can significantly reduce both the time required to recover from cyber incidents and the impact to your business.

Operate your business with more confidence, even in an unpredictable and sometimes nefarious world.

IBM Z Cyber Vault delivers **cyber resiliency protections:**

- Protection from logical data corruption
- Recovery with corrupted data is eliminated
- Clarify on trusted data source due to frequent, scheduled and automated backup/ restore testing
- IT staff has full confidence to restore the business in a corrupted data scenario
- Cyber resiliency plans are consistent, uniform and dependable across your infrastructure, applications and tooling

Are you prepared for a cyber-attack? Questions to ask yourself:

- Do we have an accidental or malicious data corruption protection plan?
- Are data copies air-gapped to a data vault?
- Does our recovery plan include restoration of a clean, trusted copy of data on which your entire system can depend?
- Is data consistency included in our objectives?
- How long would it take to recover all systems and applications after a cyber-attack?
- Do we have an isolated Point in Time copy of our data?

The IBM Cyber Vault Solution provides

- **Protected isolation** of safeguarded data copies in separate logical partitions from the production environment
- **Data validation** early/often**:** Regular analytics on the copy to provide early detection of a problem or reassurance that it is a good copy prior to further action

1. 2020 Cost of a Data Breach Report-Ponemon
2. Wired :"The Untold Story of NotPetya, the Most Devastating Cyberattack in History"

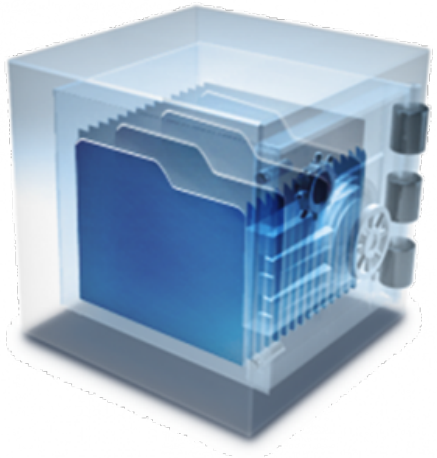
- **Forensic analysis** to identify recovery actions: Start a copy of the production systems from the copy and use this to investigate the problem and determine the recovery action
- **Surgical recovery:** extract data from the copy and logically restore back to the production environment
- **Catastrophic recovery** for worst case scenario: the entire environment is restored back to the point in time of the copy
- **Offline backup** for extra protection: Backup the copy of the environment to offline media to provide a second layer of protection

How it works

- Additional logical partitions (LPARs) are established on an IBM z15™ or IBM z14® system(s) to house, monitor and protect safeguarded copies of your data that is isolated and separated from your production system and all the users.
- Specialized software is enabled to constantly monitor your data, detect corruption, and isolate data that is compromised. Continuous protection of clean, safeguarded copies of your data provide you the ability to quickly recover from logical corruption events with confidence using this air gapped trusted copy of data.
- Isolates recovery systems from impacted systems with EAL5 Common Criteria rated separation of IBM Z partitions (LPARS) (i.e. air gapped servers)
- Minimizes performance impact with the ability to create and maintain up to 500 Safeguarded Copies per volume in one storage system
- Improves forensic analysis using an immutable offline copy of data and test drive forward recovery actions that can later be performed in production
- Performs rapid surgical or worst-case catastrophic recovery of device configurations and data to a clean production infrastructure
- Simplifies management using a single proven management solution
- Integrates comprehensive data corruption identification solutions
- Complements other existing security, HA/DR solutions, and infrastructure
- Leverages IBM Z, a platform designed for seven nines availability[3].

Key offering components:

- IBM DS8000® Storage
- IBM z14 or IBM z15
- IBM GDPS®
- IBM Security Guardium®



"If our cyber defenses fail, and the bank's IT becomes inoperable, how could we recover our 300 most critical services to a consistent point within 24 hours? Without that, the bank could be out of business."
-- global bank

Why IBM:

- More than 50 years of business continuity and disaster recovery experience
- Managed, scalable data protection solutions offering custom or standard services in IBM data centers or on premises
- Experienced in Business Resiliency Services and offerings for over 30 years
- Relied on by the world's largest banks, financial institutions and industries

Act now:

Contact your IBM sales rep to learn more and schedule a complementary Discover and Co Creation Virtual Workshop.

3. Internal data based on measurements and projections used in calculating expected value