IBM Z Cyber Vault

Cyber resiliency for a zero-trust world

Highlights
IBM Z Cyber Vault is designed to:

Address rising cyber threats with resilient protection

Provide immutable backups to safeguard critical data

Enhance recovery confidence with automated validation

Accelerate restoration with flexible recovery options

It's a dangerous world

Cyberattacks and data corruption threats are escalating in scale and sophistication. Ransomware, malware, and insider threats can cripple critical systems in seconds, leaving organizations unable to deliver services and facing severe financial and reputational damage. According to the *Cost of a Data Breach Report*, breaches caused by malicious insiders average $4.99M,[1] and the *IBM X-Force Threat Intelligence Index Report* finds that attacks using stolen credentials have surged by 71% year-over-year.[2]

Traditional high availability and disaster recovery (HA/DR) strategies are not enough. If data has been corrupted, recovery processes may introduce additional complications. Fast-moving ransomware can compromise traditional backups almost instantly. Businesses need a solution that ensures clean, validated recovery points—even in the face of logical corruption.

$4.99M

Average cost of a data breach

71%

Year-over-year increase in attacks using stolen credentials

A new standard for cyber resiliency

IBM Z® Cyber Vault provides an air-gapped, immutable data vault and automated processes designed to proactively detect protect against logical data corruption and enable rapid recovery. Unlike conventional approaches, IBM Z Cyber Vault:

- Creates up to 1,024 immutable, crash-consistent Safeguarded Copies per volume using IBM DS8000® storage.
- Stores backups in an isolated environment, —physically or virtually separated from production.
- Automates capture, validation, and recovery using GDPS® Logical Corruption Protection (LCP) Manager.
- Enables proactive validation of snapshots to ensure integrity before recovery.
- Supports forensic analysis, surgical recovery of specific datasets, and catastrophic recovery of entire environments.
- Integrates with advanced tools like IBM Z Backup Resiliency (IZBR) and IBM Threat Detection for z/OS (TDz) for enhanced protection.

Key capabilities

- *Immutable backups*: Point-in-time copies that cannot be altered or deleted.
- *Automated validation*:
  - Infrastructure validation (IPL and subsystem restart).
  - Data structure validation (Db2, IMS, VSAM, RACF, catalogs).
  - Application data validation.
- *Forensic analysis:* Investigate corruption scope and root cause using logs, SMF data, and IZBR analytics.
- *Recovery options*:
  - *Surgical recovery*: Restore specific datasets or subsystems.
  - *Catastrophic recovery*: Incremental restore of entire environment from validated Safeguarded Copy.
- *Offline backups*: Tape-based air gap for long-term retention and compliance.
- *Offensive security*: Isolated environment for penetration testing and red teaming without production risk.

How it works

- Storage domain: IBM DS8000 with Safeguarded Copy for immutable backups.
- Automation domain: GDPS LCP Manager orchestrates capture, validation, and recovery; supports scripts for CAPTURE, RECOVER, RESTORE.
- Environment domain: Isolated IBM Z LPARs for validation and recovery; network segmentation via VLAN, NAT, and firewalls. Software tools to support validation, analysis and recovery.
- Security: Zero trust principles, role-based access, dual control, multi-factor authentication (MFA), and Security Information and Event Management (SIEM) integration.

- **Benefits**
- Rapid, reliable recovery from logical corruption or ransomware.
- Minimized RPO/RTO and reduced downtime.
- Compliance with NIST, DORA, ISO 27005 frameworks.
- Enhanced security posture with air-gapped architecture and layered defenses.
- Scalable design for evolving business needs.

"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

Questions to ask yourself

- Do we have a plan for accidental or malicious data corruption?
- Are our backups immutable and air-gapped?
- Can we validate recovery copies proactively?
- How quickly can we restore critical services after a cyberattack?
- Do we have an isolated environment for forensic analysis and recovery?
- What is the risk to our brand and reputation?
- Are we compliant with our regulatory environment?

Why IBM

- Over 50 years of leadership in business continuity and disaster recovery.
- Proven expertise in cyber resiliency and mainframe security.
- Trusted by the world's largest banks, insurers, and enterprises.
- Comprehensive services: design, deployment, and ongoing support.

For more information

To learn more about IBM Z Cyber Vault, contact your IBM representative or IBM Business Partner to schedule a Cyber Vault Discovery and Architecture Workshop and start building a cyber resiliency strategy that protects your most critical assets. Learn more in the IBM Z Cyber Vault Redbook.

Key components: IBM DS8000 Storage | IBM Z | IBM GDPS | IBM Z Backup Resiliency | IBM Security Guardium® | IBM TS7700 Virtual Tape

1. IBM Corporation, "Cost of a Data Breach Report 2025," 2025.
2. IBM Corporation, "IBM X-Force 2025 Threat Intelligence Index," 2025.

Produced in the
United States of America
January 2026