

IBM Cyber Vault for AIX

Richárd Magyar
Consulting IT specialist
IBM Expert Labs

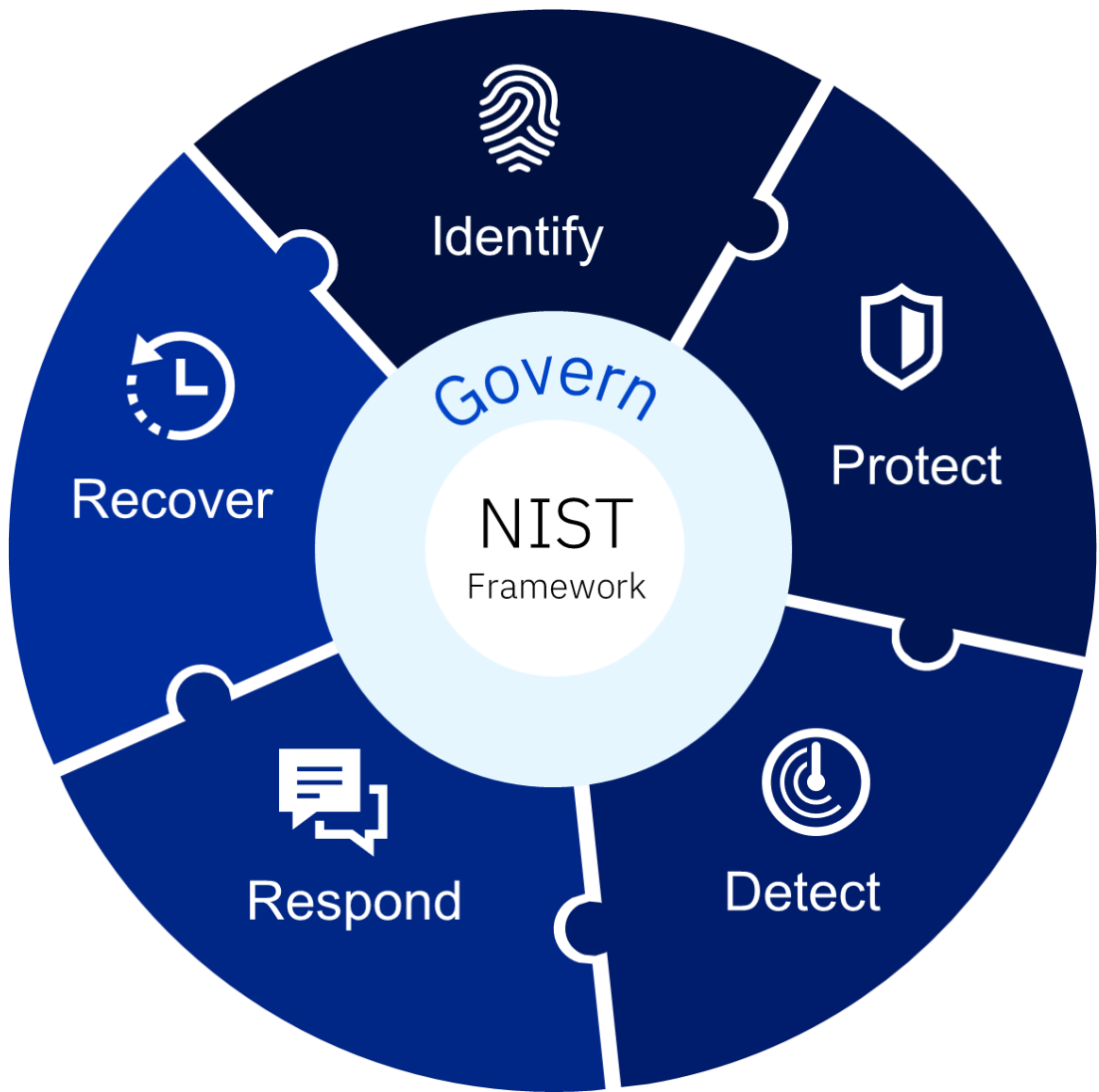


If a cyber incident compromised your system today, how quickly could you restore business operations?

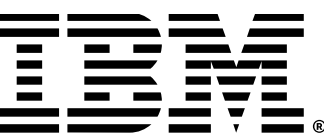
Without a strategic solution, it typically takes longer than the business can afford and with more uncertainty than leadership is comfortable with.



Cyber Crime is a critical threat



* [Sophos The State of Ransomware](#)
** [IBM Cost of a Data Breach](#)
Documents dated 2025



50%
Percentage of attacks that result in data encryption—and attackers target backups first.*

Data encryption is at the lowest level in six years. Down from 70% in 2024.

100 days
4 out of 5 businesses take at least 100 days to recover from an attack.**

- 76% said the recovery took longer than 100 days.
- 26% said recovery took more than 150 days.
- 2% said recovery was possible within as little as 50 days.

\$4.44m
Average cost of a breach**

Dropped from \$4.88m in 2024. Today, most breaches are caused by a range of malicious activities, from phishing to insider threats.

Cyber Security and Cyber Resilience

Cyber Security

Cyber security is about prevention; it's about trying to keep the bad actors out of your environment

Cyber Resilience

Cyber resilience is about an organizations ability to continue operations and rapidly recover despite a cyber-incident

Organizations need to be both cyber secure and cyber resilient

Cyber Resiliency

Preparation & Prevention

- Do you know our critical systems and data?
- Are **patching and vulnerability management** consistently applied?
- Do you have **endpoint detection & response (EDR)** in place?

Protect, Backup & Recovery

- Are backups **regular, automated, and immutable**?
- Have you **tested full system recovery** recently?
- What are our **RTO and RPO targets**, and can you prove you can meet them?

Detection & Response

- How often do you test the backups are **clean and recoverable**?
- How quickly can you **detect an attack**?
- Do you have a **tested incident response plan**?

Resilience & Continuity

- Do you have a **disaster recovery (DR) site or failover plan**?
- Do you run **regular cyber attack simulations**?



IBM Cyber Vault

- Proactive protection with immutable copies
- Rapid ransomware detection
- Automated Response
- Rapid Recovery to meet predictable Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements

Recover Operations in Hours, not Months

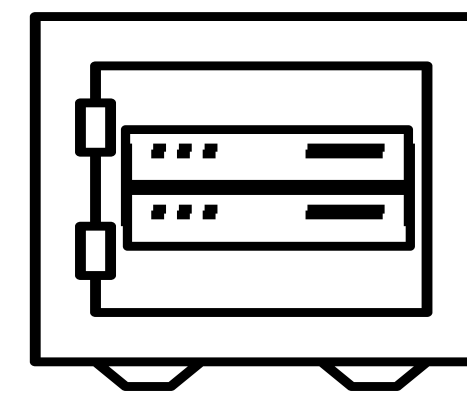


IBM Power Cyber Vault for AIX



IBM Power Cyber Vault is a custom-architected solution from IBM Expert Labs that integrates IBM products and technologies into an automated, comprehensive, end-to-end cyber resiliency solution.

PowerSC



IBM Power Cyber Vault

 **Red Hat**
Ansible Automation Platform



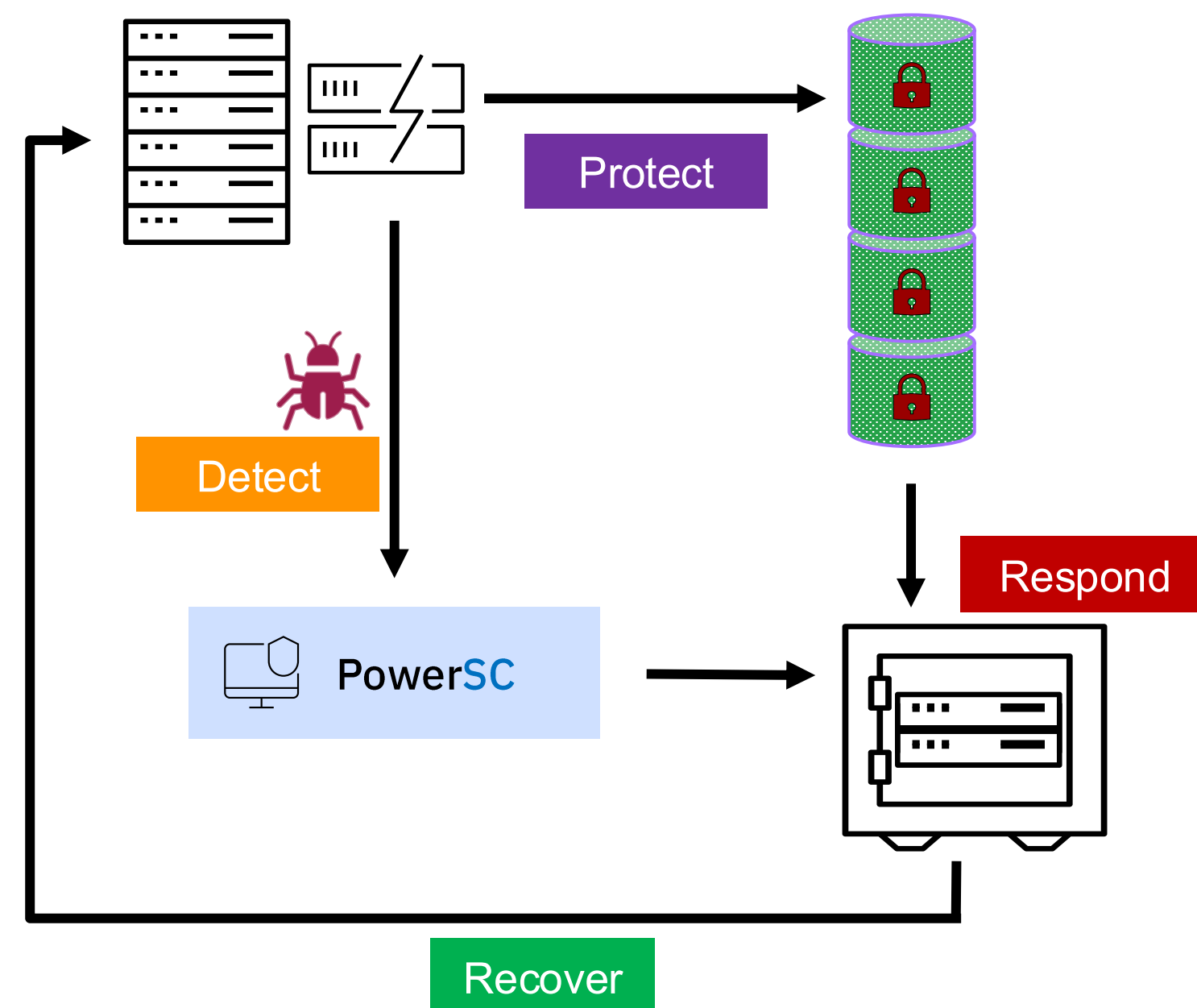
IBM Power Cyber Vault for AIX

Immutable snapshots

Fast threat detection

Automated data validation

Assisted clean room recovery



Frequent
snapshots

Snapshot intervals to support aggressive RPOs and minimize losses

Near real
time detection

Typical ransomware detection time <1 min with automated response to minimize the threat

Data
Validation

Automated, continuous validation ensures safe recovery points for system, data and applications

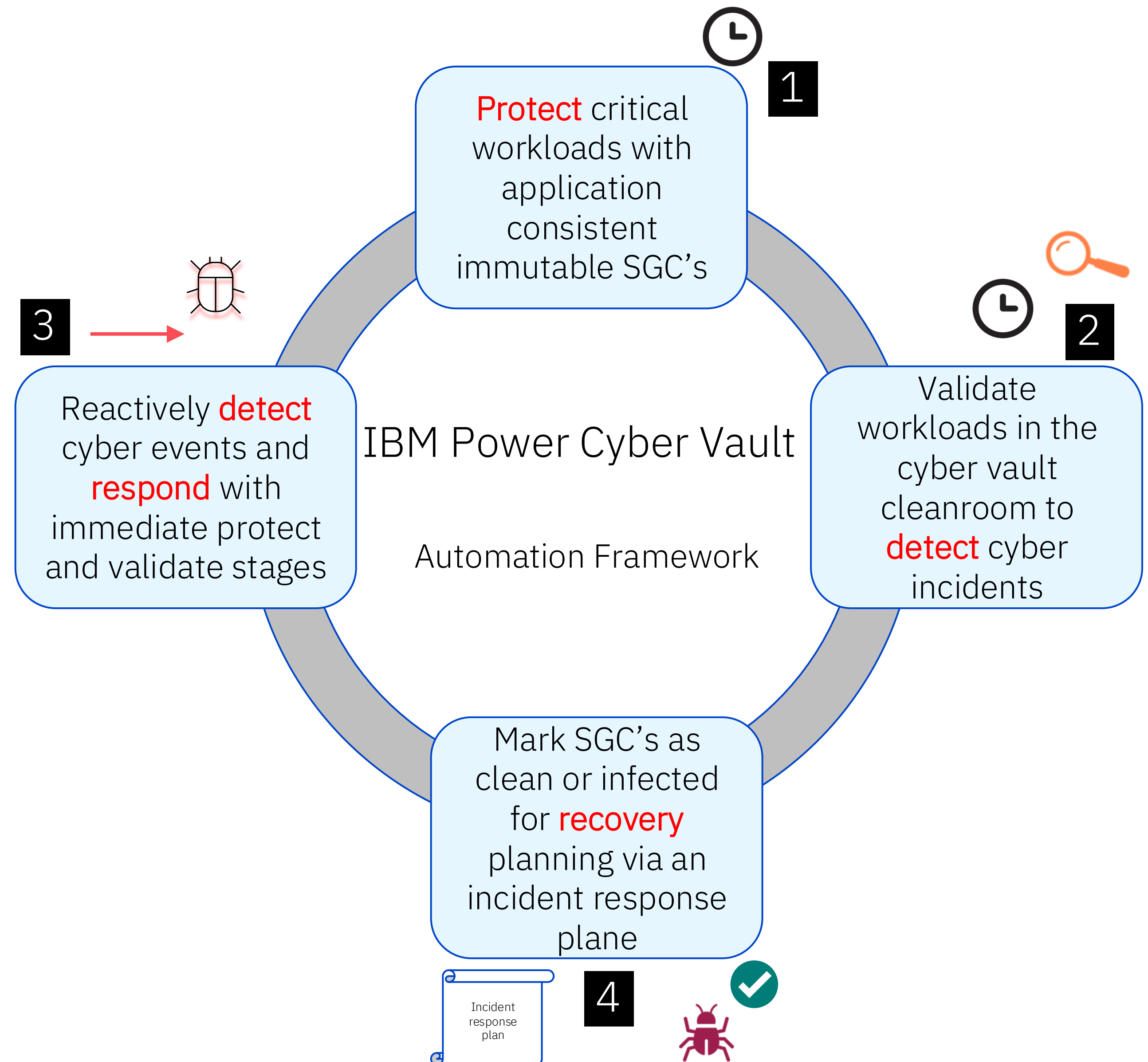
Fast
recovery

Recover business operations on the same day in the event of an attack

IBM Power Cyber Vault for AIX

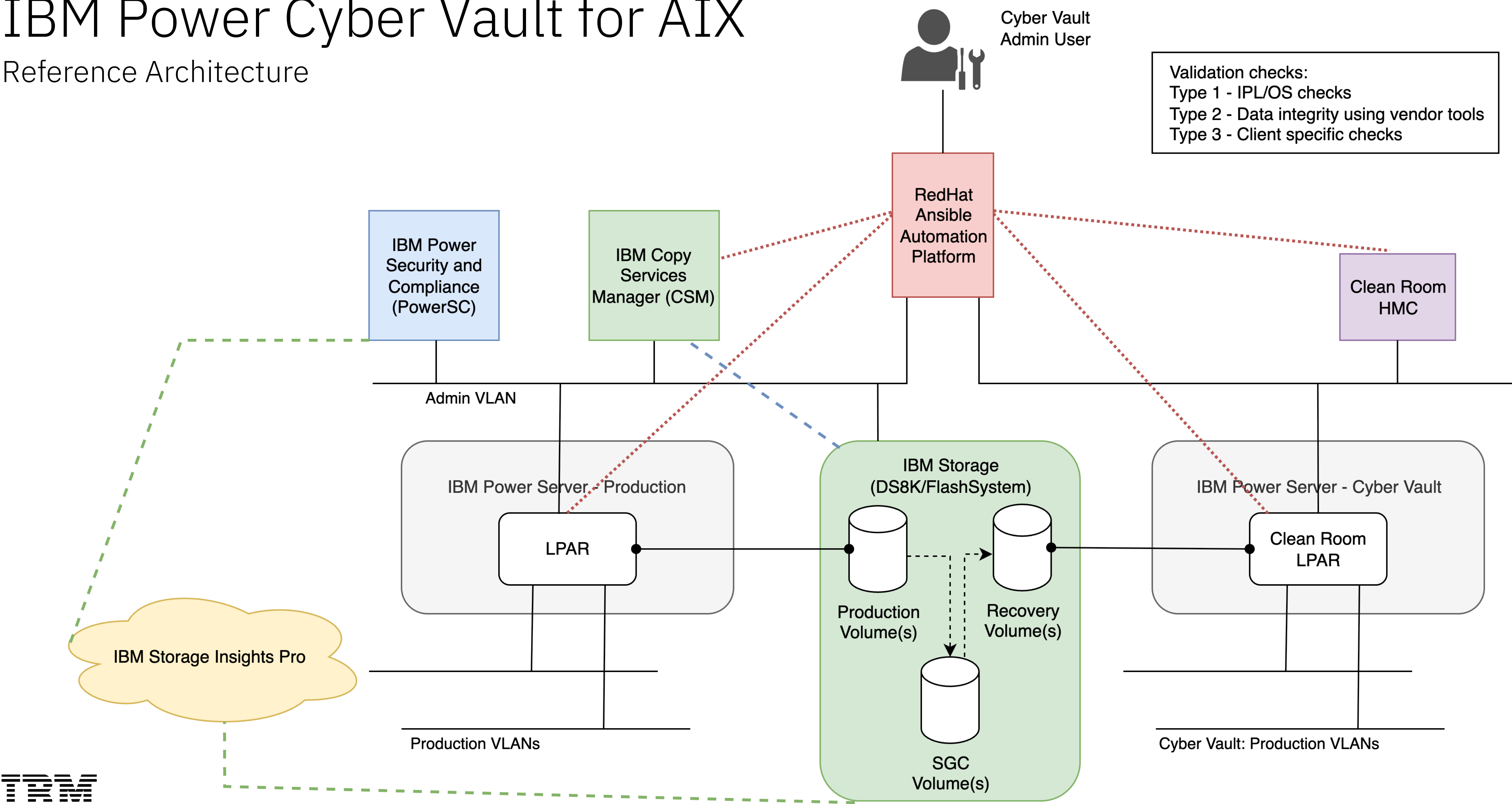
Automation Framework

1. Periodic scheduled copies
2. Periodic testing of immutable copies
3. Reactive validation triggered by security events
4. A list of SGC backups and their validation status



IBM Power Cyber Vault for AIX

Reference Architecture

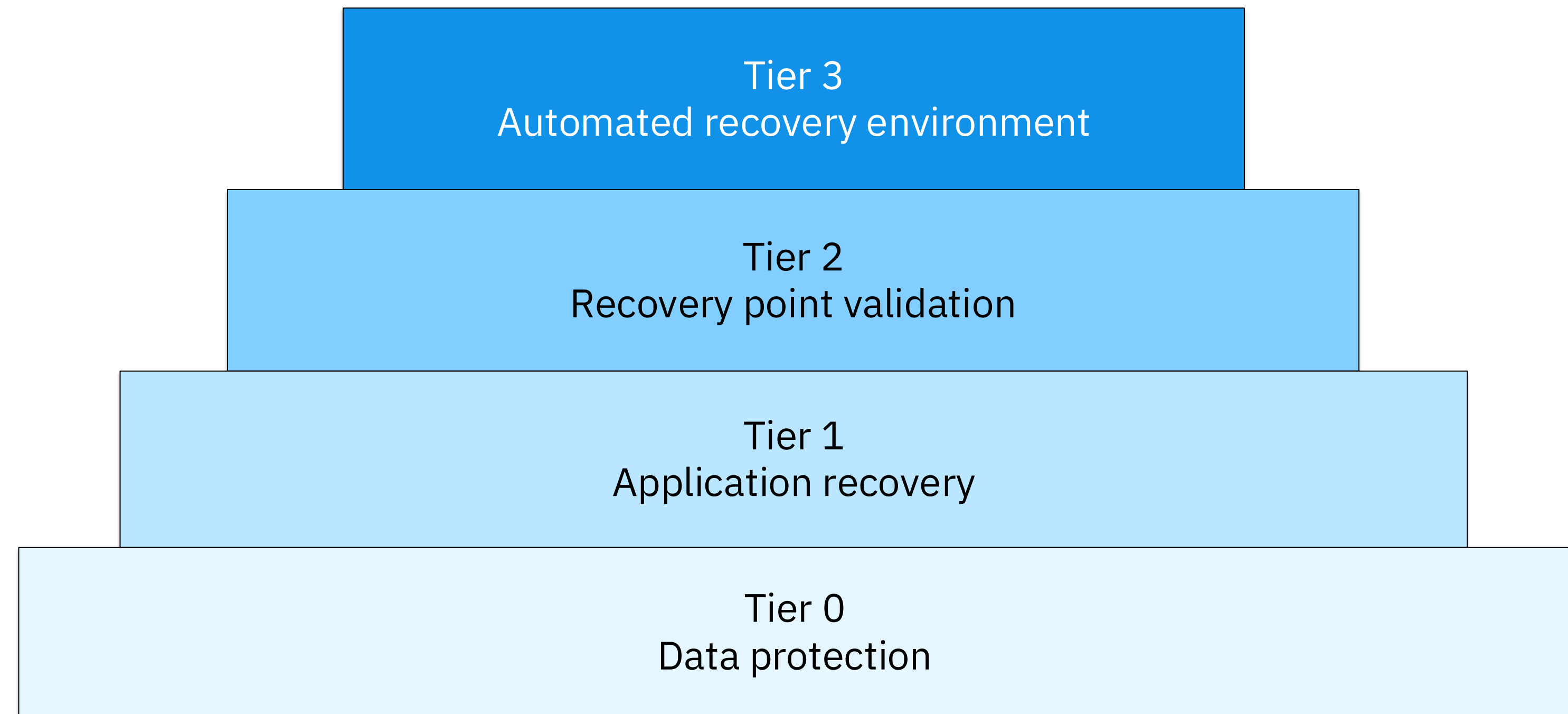


IBM Power Cyber Vault for AIX

Tiers

An IBM Power Cyber Vault is delivered in 4 tiers, each building on the next to deliver increasing levels of protection, recovery speed, and confidence.

IBM Power Cyber Vault for AIX is a modular, extensible offering designed to evolve into a comprehensive and integrated enterprise-class resilience solution



IBM Power Cyber Vault for AIX

Tiers

	Tier 0	Tier 1	Tier 2	Tier 3
Stage	Data Protection	Workload Protection	Recovery Point Validation	Automated Response
What	Protect volumes with frequent crash-consistent Safeguarded Copies and fast ransomware threat detection	Recover application from application-consistent Safeguarded Copies and easy recovery tools	Clean copies are validated with automatically scheduled tests in a dedicated clean room	Reactive clean room staging and validation triggered by ransomware alerts
How	- Built-in Storage snapshot software - Real-time detection in FlashCore Modules	- Copy Services Manager - Red Hat Ansible playbooks	- Dedicated Power capacity - Red Hat Ansible playbooks	- Dedicated Power capacity - Red Hat Ansible playbooks
Outcomes	- Recover data in the event of an attack - Reduced RPO & RTO - Minimized data loss	- Avoid manual database repair - Further reduce RPO & RTO - Quickly recover with automated tools	Reduce RPO & RTO further with proactive identification of clean copies	- Minimized RTO - Confidence in recovery strategy and peace of mind



IBM Power Cyber Vault for AIX

Solution Tiers and components

Components		Tier 0 Protect Volumes	Tier 1 Protect Workloads	Tier 2 Proactive validation	Tier 3 Reactive validation
1	IBM Power server(s)				
2	IBM Storage with required SGC capacity and current-generation FlashCore Modules*				
3	Red Hat Ansible Automation Platform (AAP)				
4	IBM Copy Services Manager				
5	Clean room IBM Power server(s) with capacity to host validation LPARs				
6	IBM Power and Security Compliance (PowerSC)**				
7	IBM Zero Trust Execution for AIX (Optional)				

*Dashboard alerts and regular detection model updates require Storage Insights.

** Included with AIX Enterprise Edition or sold separately



IBM Power Cyber Vault for AIX

Validation Types

Type 1 – System Data Validation

Validate that the OS images can successfully perform an Initial Program Load (IPL) from the recovery volumes.

- Ensure all volumes are included
- AIX Trusted Execution checks on key files
- PowerSC validation checks (optional)
- Zero Trust Execution for AIX validation (optional)

Type 2 – Data Structure Validation

Validate the structural integrity of critical system and database components.

- Customized to focus on critical data and time to validate
- Database able to start, mount and open successfully
 - Oracle DBVerify/RMAN logical validation
 - Db2 inspect/Db2dart

Type 3 – Data Content Validation

Validate the business data for critical applications.

- Application level specific validation scripts and commands, to identify potential corruption.

IBM Power Cyber Vault for AIX

References

IBM Zero Trust Execution for AIX (ZTEA): <https://www.ibm.com/support/pages/getting-started-ztea>

IBM Power Cyber Vault for AIX: <https://www.ibm.com/support/pages/node/7248605>

IBM PowerSC: <https://www.ibm.com/products/powersc>

IBM Expert Labs: <https://www.ibm.com/products/expertlabs>



Legal disclaimer



© Copyright IBM Corporation 2026.

IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/legal/copytrade.

This document is current as of the initial date of publication and may be changed by IBM at any time.

IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Examples presented as illustrative only. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

Not all offerings are available in every country in which IBM operates.

It is the user’s responsibility to verify the operation of any non-IBM products or programs with IBM products and programs. IBM is not responsible for non-IBM products and programs.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.