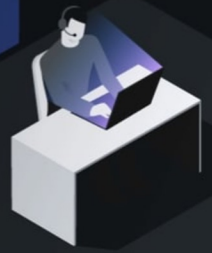
IBM Data Resilience Portfolio



Client Presentation Series

IBM Spectrum Protect

IBM Spectrum Protect Plus

IBM Spectrum Copy Data Management

IBM Safeguarded Copy with IBM FlashSystem Cyber Vault

Roger Didio
Advisory Sales Enablement Leader and
Skills Content Specialist
IBM Storage Data Resilience
rjdidio@us.ibm.com

June 9, 2022

IBM Data Resilience Portfolio

The 4 C's

Cyber

Cloud

Containers

Convergence

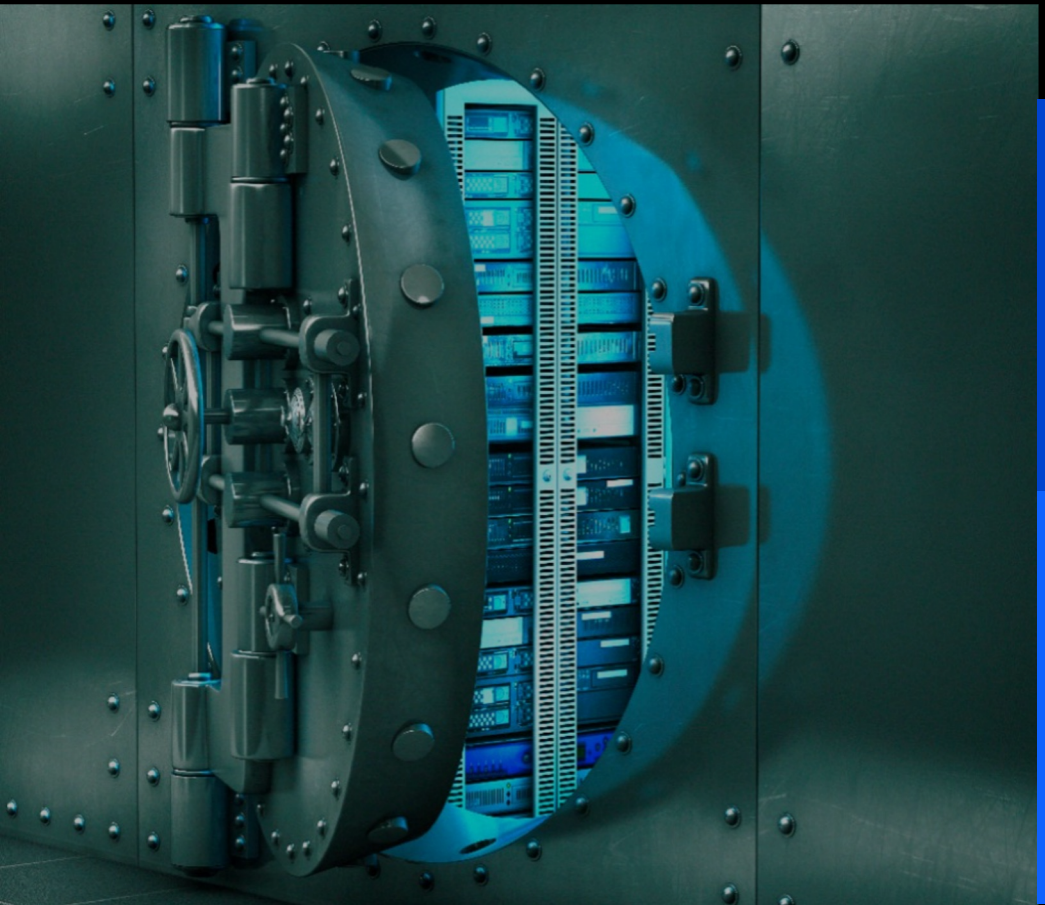
IBM Spectrum Protect

IBM Spectrum Protect Plus

IBM Spectrum Copy Data Management

Portfolio Convergence

Safeguarded Copy with FlashSystem Cyber Vault



When bad things happen to your data

IBM Safeguarded Copy

- Isolated, immutable snapshots of data
- Snapshots on same FlashSystem storage as operational data
- Recovery faster than restoring from copies stored separately

IBM FlashSystem Cyber Vault

- Automatically scans to look for corruption
- Identifies ransomware attacks when they have started
- Identifies which copies have *not* been affected

Solution overview

IBM Storage

- Data volumes and active copies generated and maintained
- Spectrum Virtualize Safeguarded Copy
- Immutable copies
- IBM Tape with encryption and/or write once-read many (WORM) technology
- Secure air-gapped data vault

IBM Spectrum Virtualize

- 100% data availability guarantee
- Audit log integration with QRadar monitors unauthorized activity
- Storage Insights warns for changes in data reduction rates or performance anomalies
- IBM Security solutions

IBM Services

- Services, clustering technologies, and server and storage replication and automation
- Copy Services Manager to manage the entire recovery environment
- IBM Lab Services risk assessment and deployment services

Safeguarded Copy speeds recovery from cyber attacks

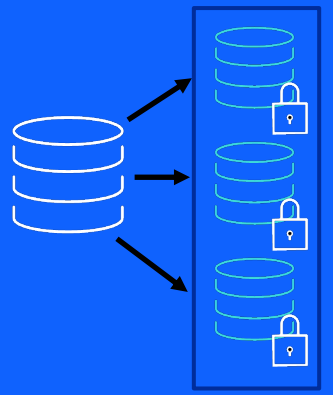
Automatic
creation of regular backup copies

Immutable
point-in-time copies of production data

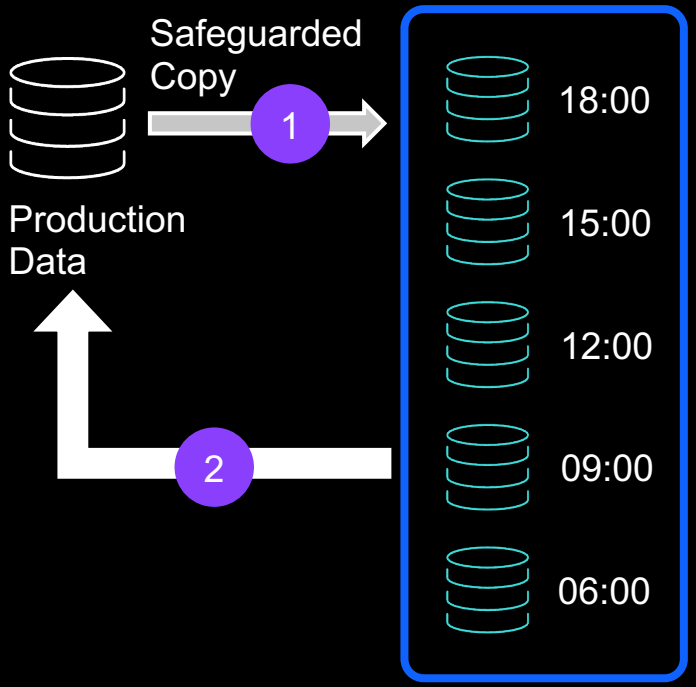
Isolated
logical air-gap offline by design

Fast
restore from copies on primary storage

Prevents modification or deletion of copies due to user error, malicious destruction, or ransomware attack



Safeguarded Copy: how it works

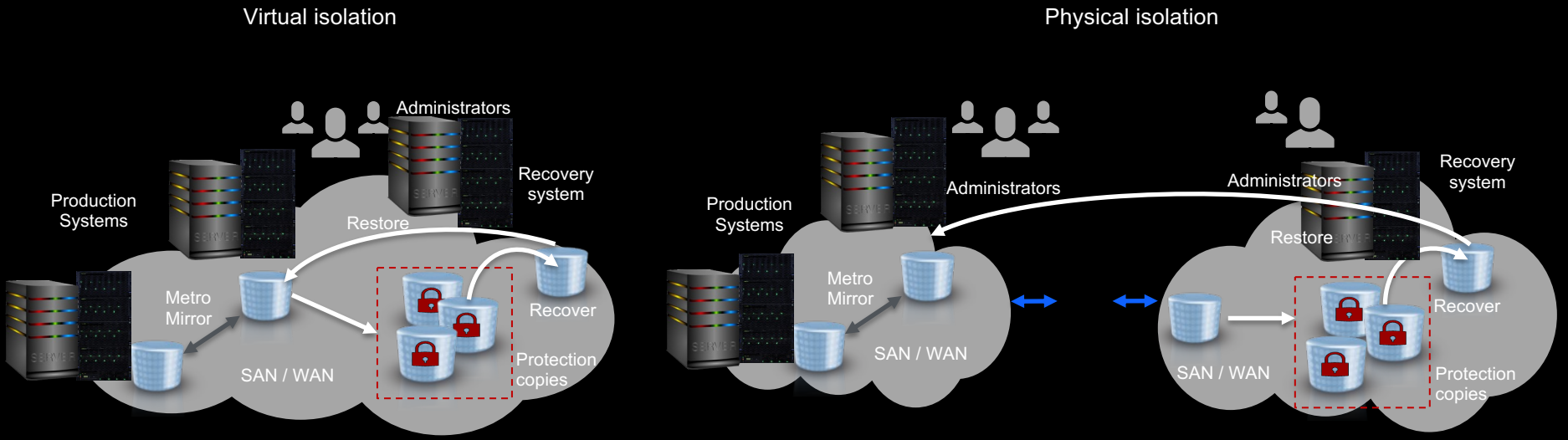


1. Safeguarded immutable copies created throughout the day
2. Ability to perform rapid restore of immutable copy when required

What's next?

Operationalizing Safeguarded Copy with Cyber Vault

Air Gap: logical and physical isolation of protection copies



- Additional storage systems are used for the protection copies.
- The storage systems are typically not on the same SAN or IP network as the production environment.
- The storage systems have restricted access and even different administrators to provide separation of duties.

As simple as 1 – 2 – 3

1

Make immutable copies of data

- Safeguarded Copy
- Copy Services Manager (CSM) to automate creation and restore of copies

2

Test copies of data

- Isolated infrastructure to test copies
- Ensure copies not corrupted using application tools
- Test infrastructure logically or physically air-gapped
- Blueprint for testing and recovery process

3

Automate process

- Automation of making and testing copies
- Automation of test & restore process

Cyber Vault and Safeguarded Copy stand apart

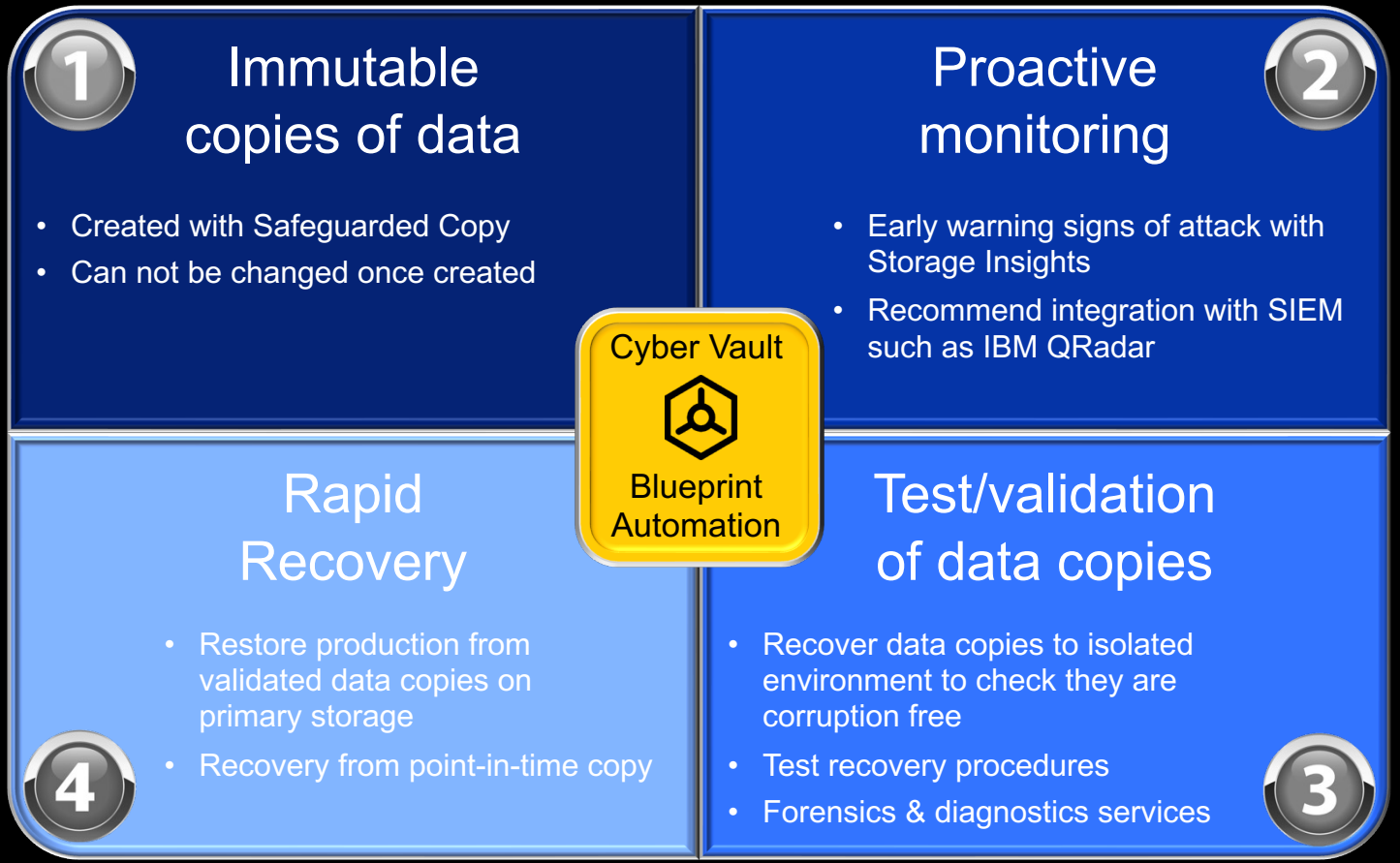
23 days

industry average
recover time

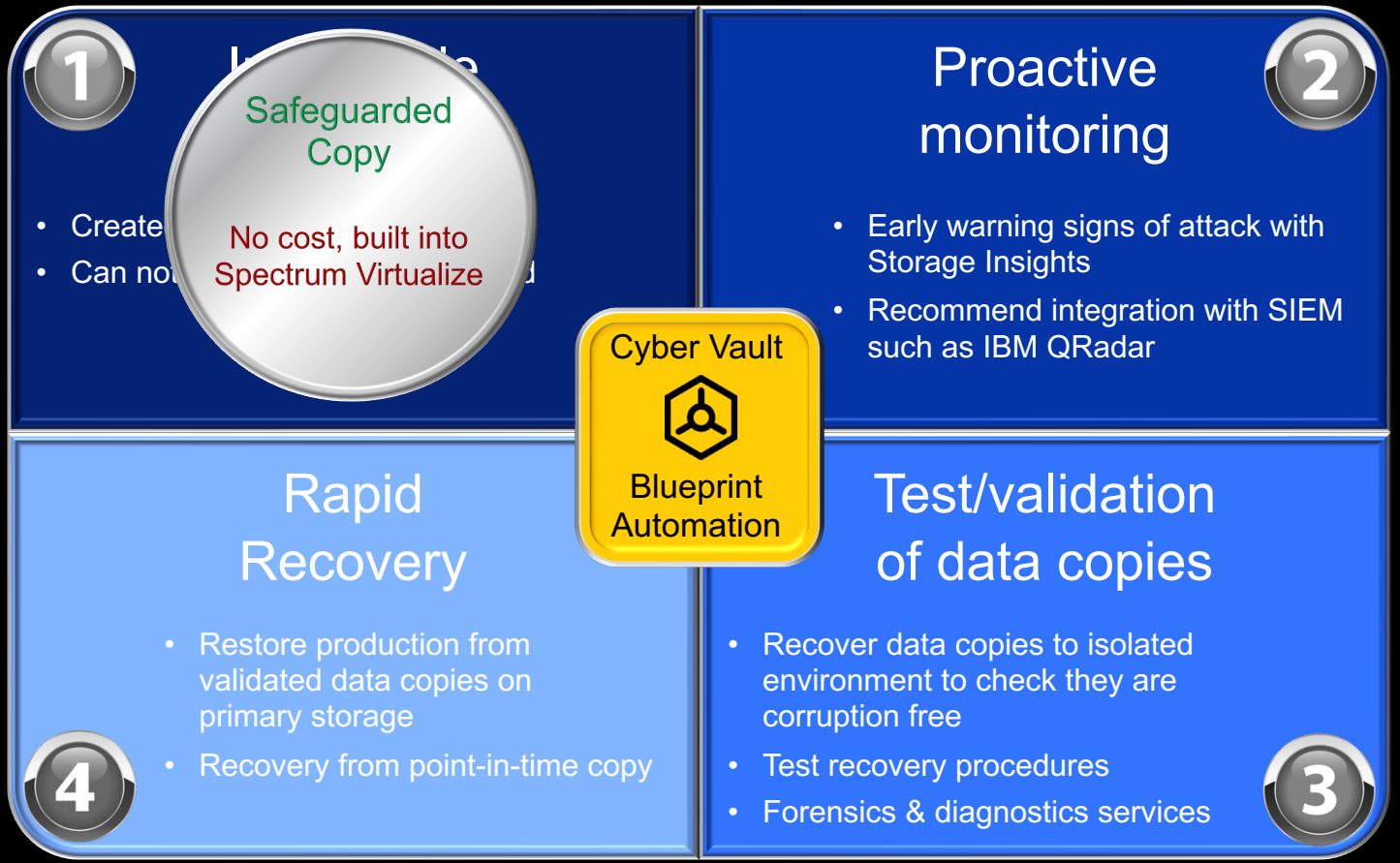
A few hours

Cyber Vault & Safeguarded Copy
average recovery time

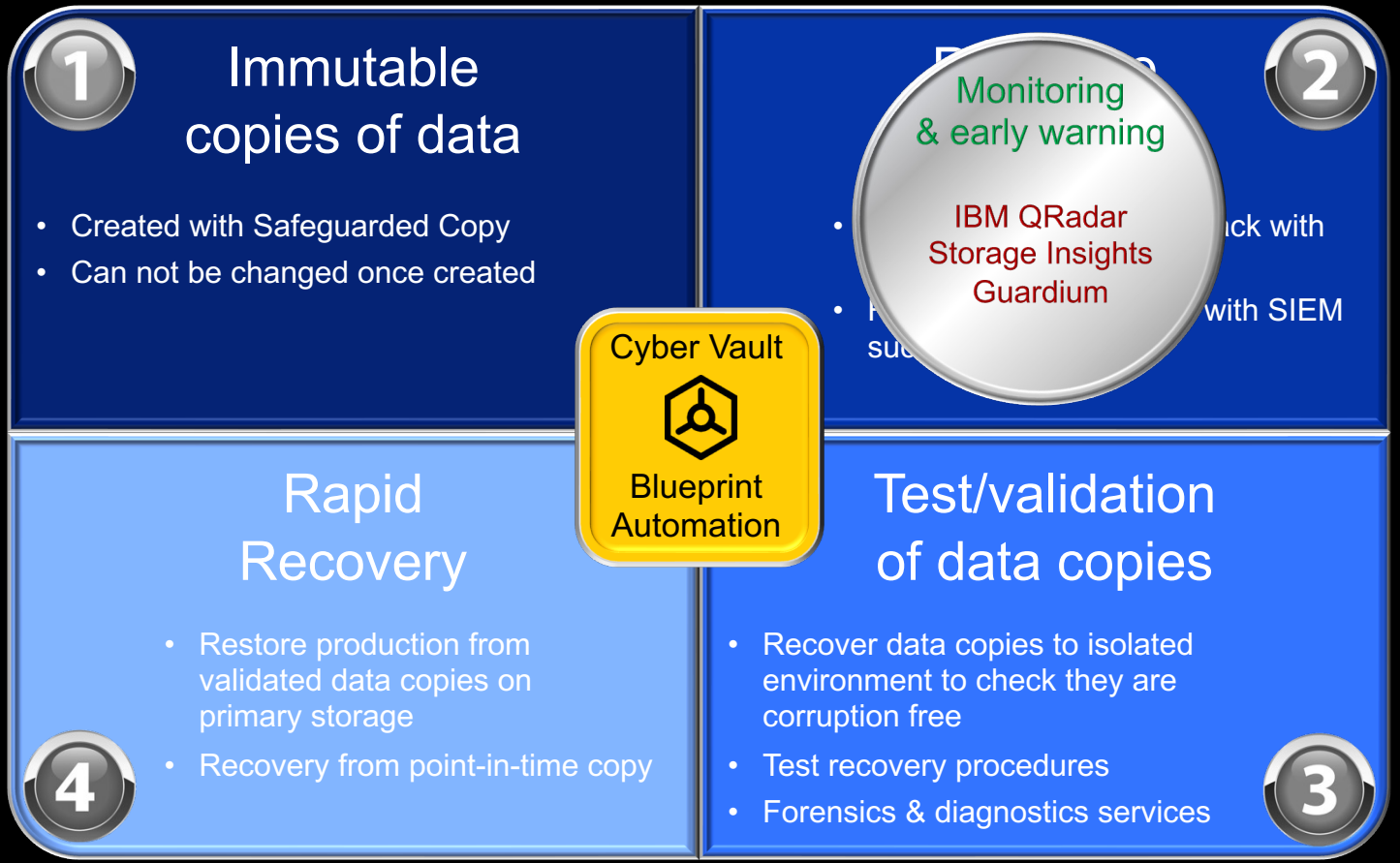
Cyber Vault value and differentiation



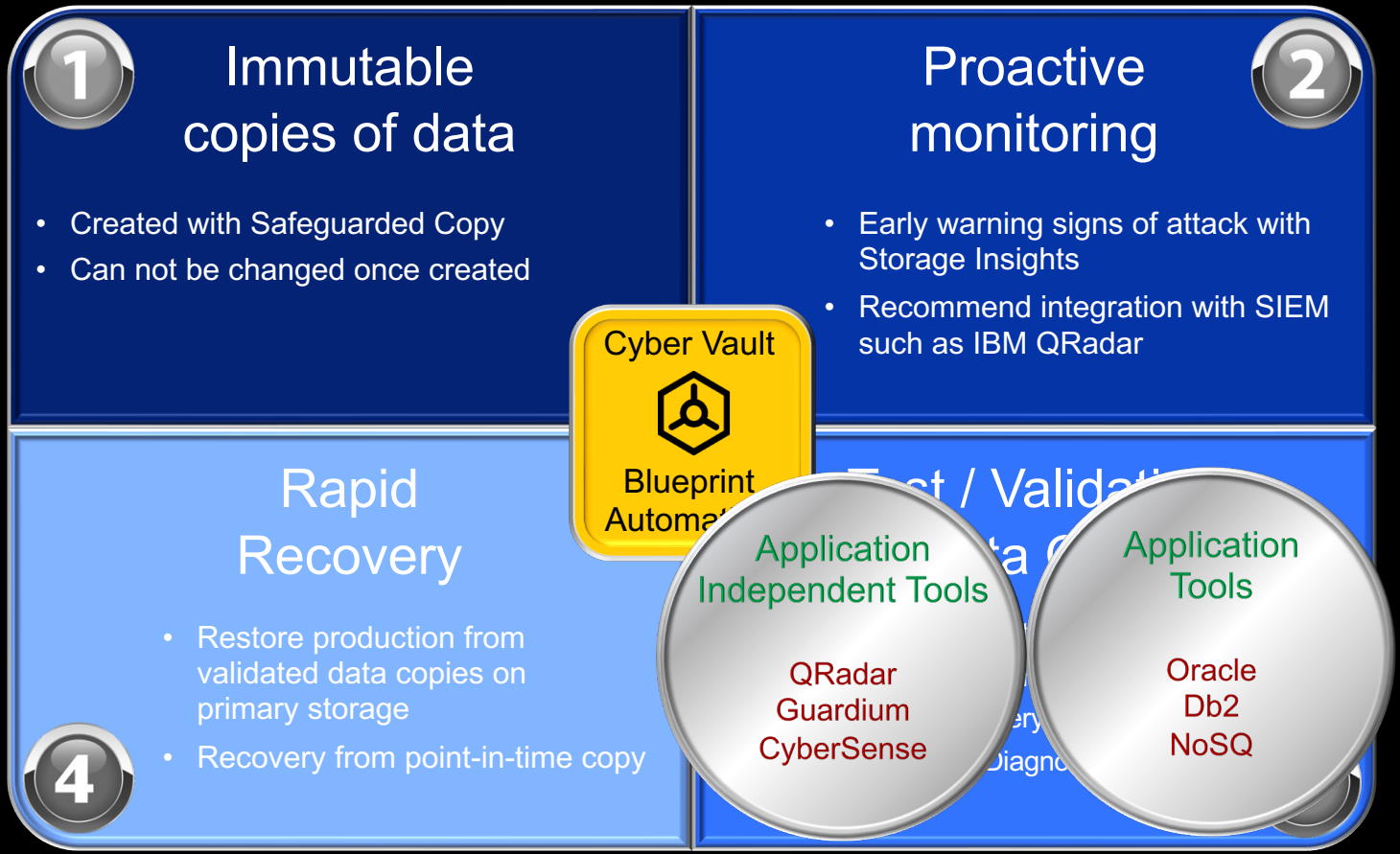
Cyber Vault value and differentiation



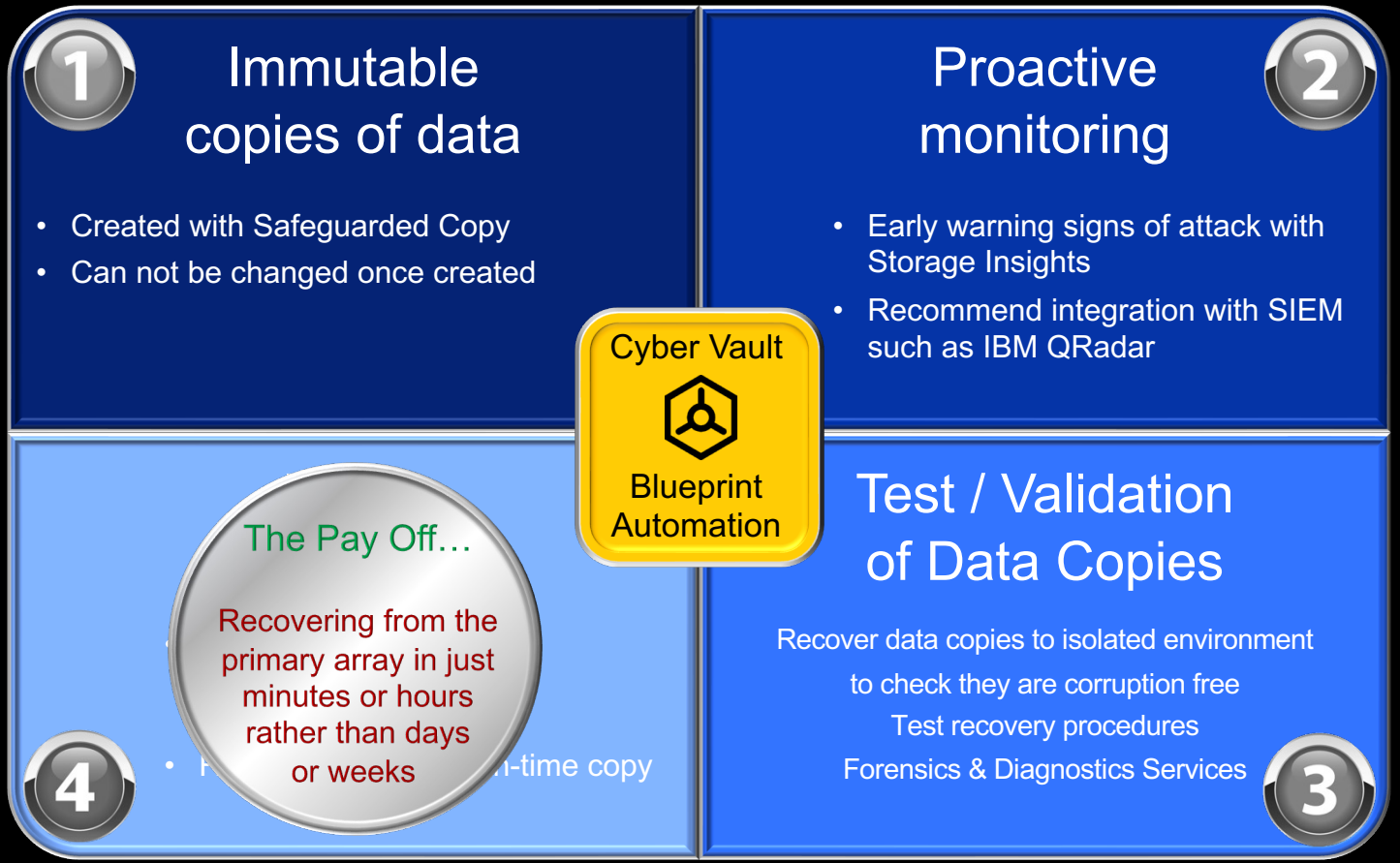
Cyber Vault value and differentiation



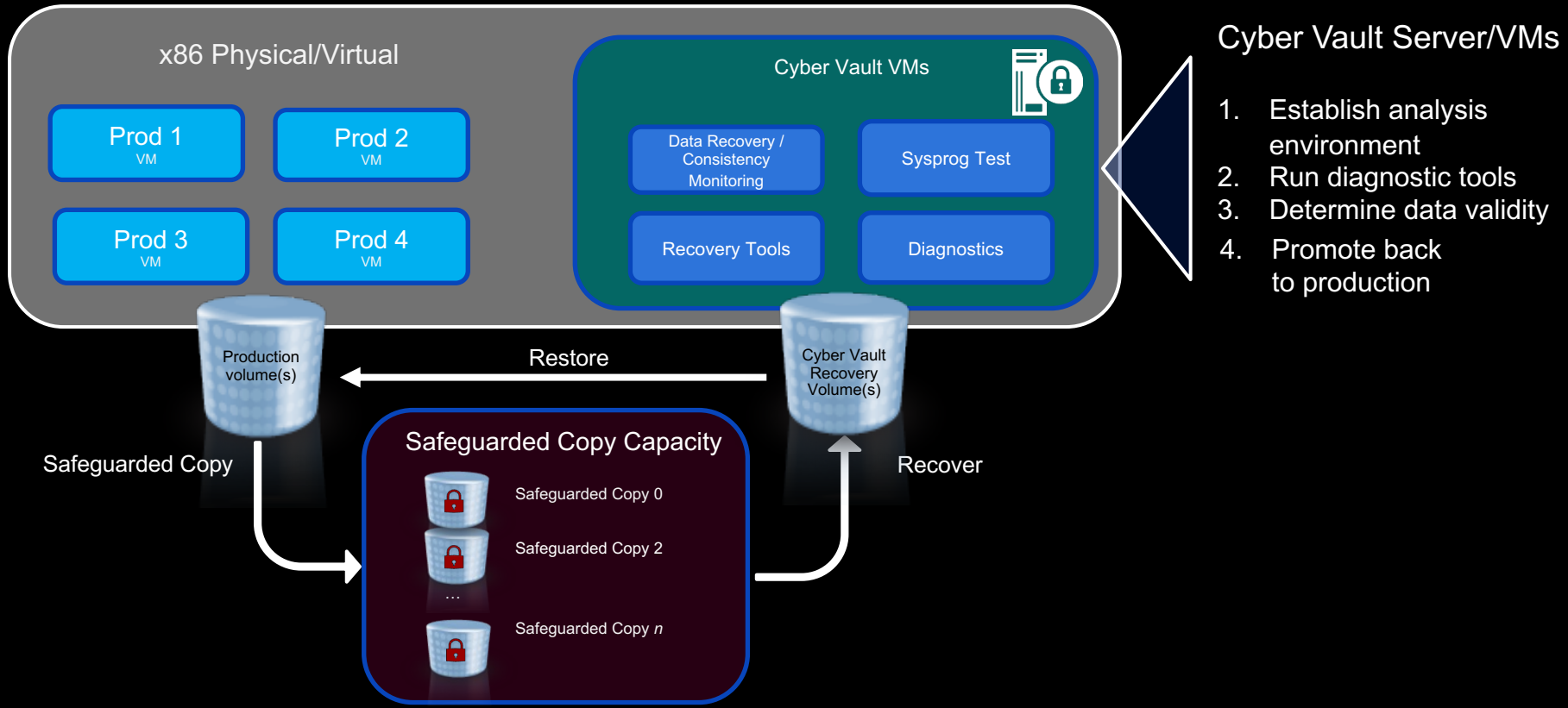
Cyber Vault value and differentiation



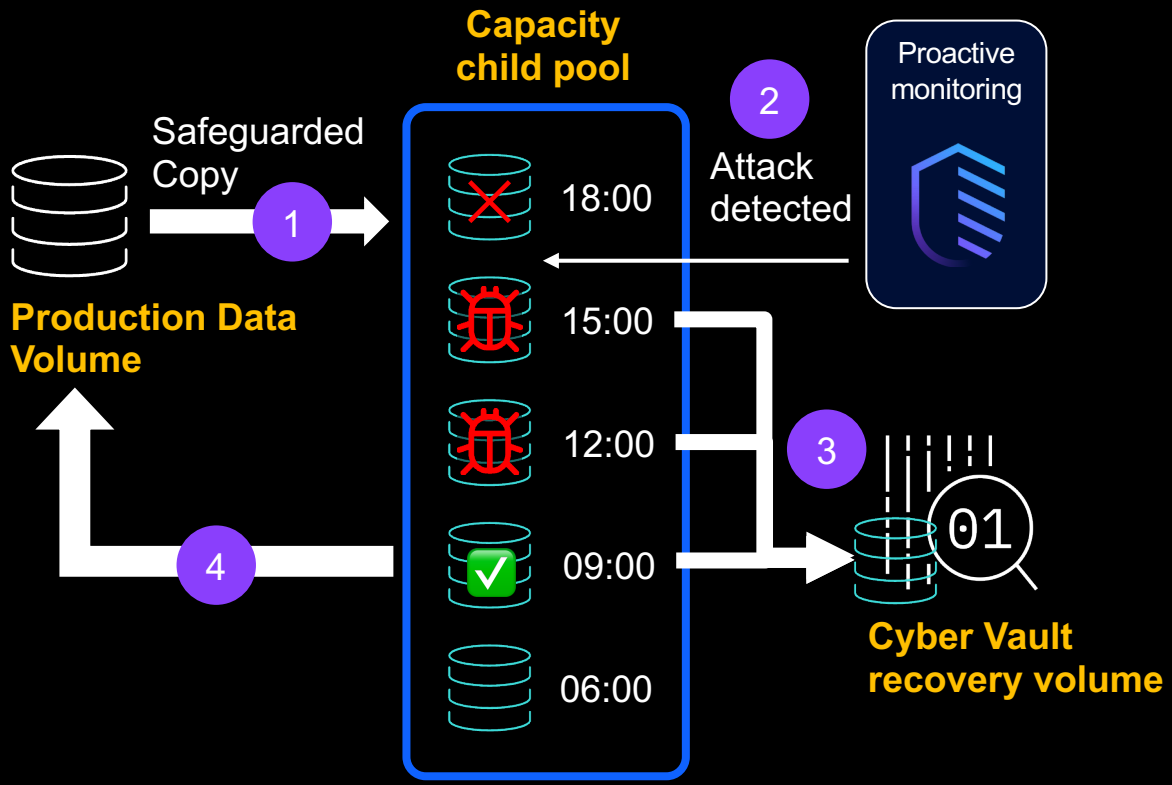
Cyber Vault value and differentiation



Cyber Vault workflow: identify problems, minimize impacts

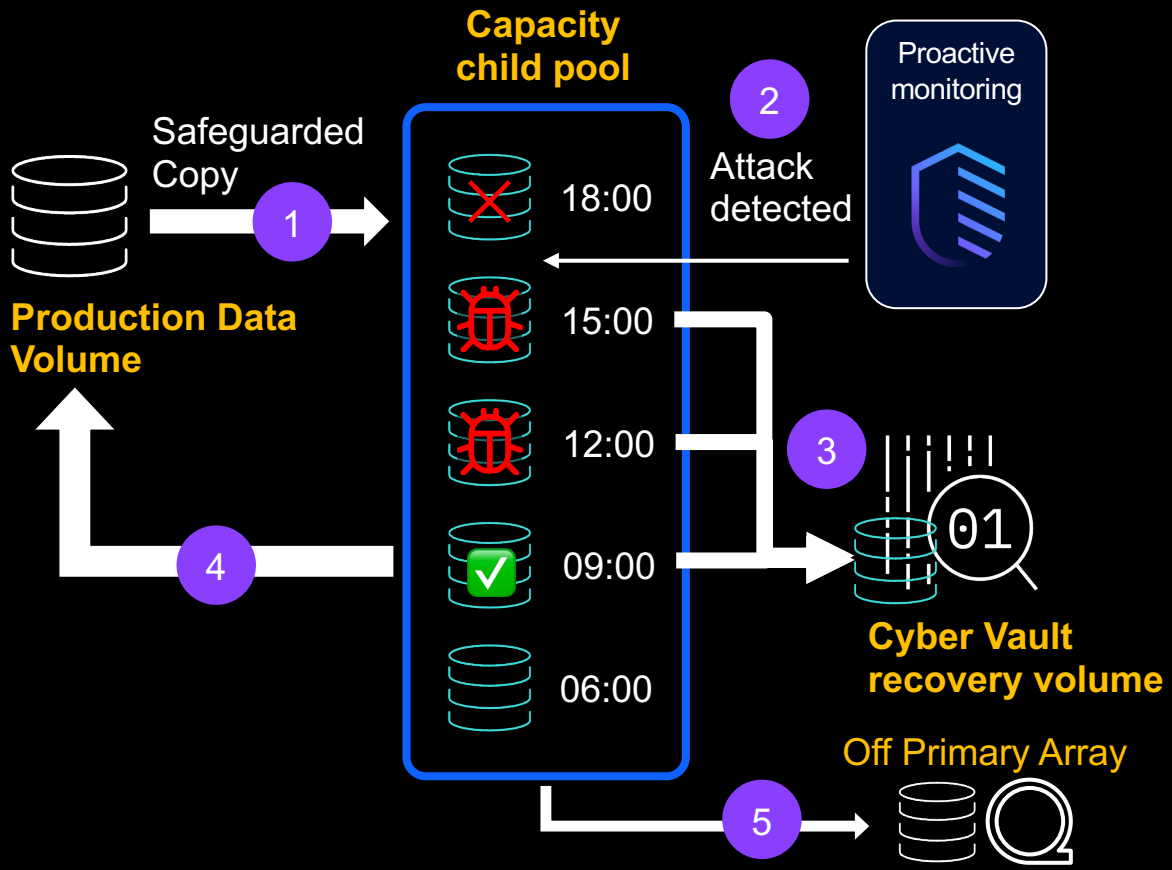


Cyber Vault workflow: test, validate, recover



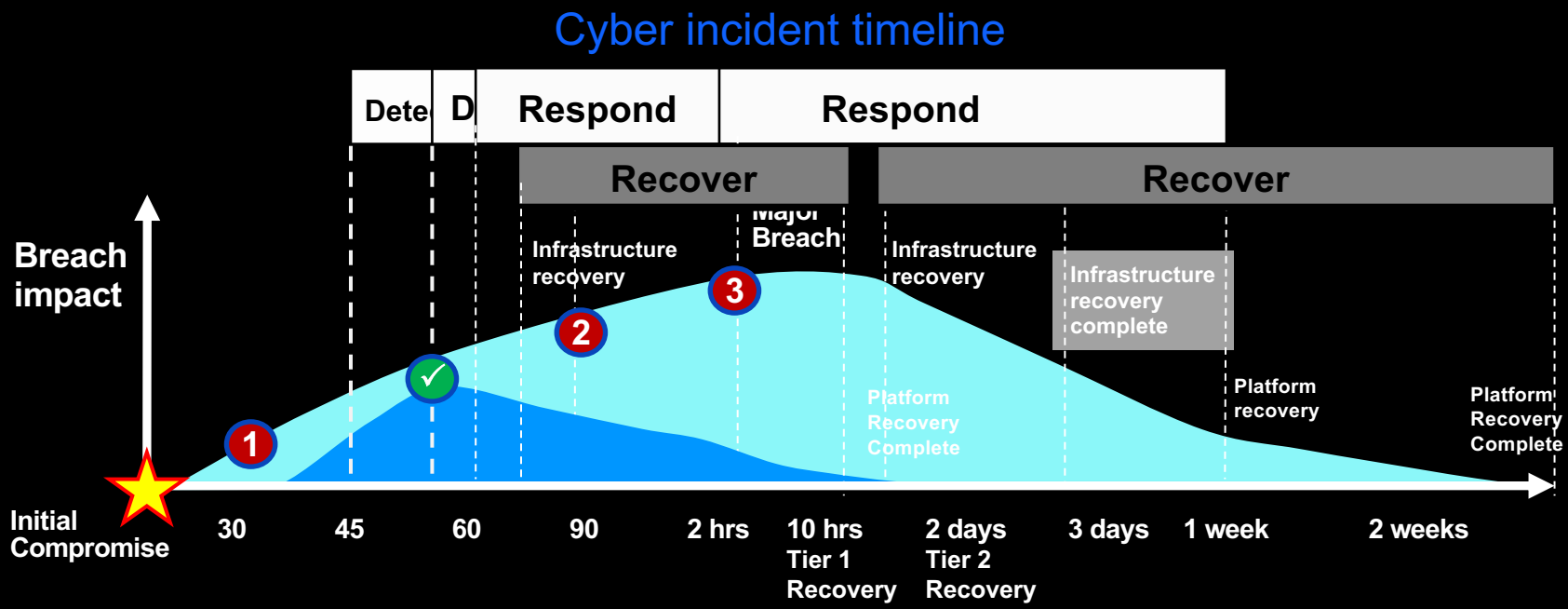
1. Safeguarded immutable copies created throughout the day
2. Attack detected by monitoring software
3. Recovery volumes mounted to Cyber Vault; tools validate if data is clean or corrupted
4. Clean copy quickly identified and restored to production

Cyber Vault workflow: test, validate, recover



1. Safeguarded immutable copies created throughout the day
2. Attack detected by monitoring software
3. Recovery volumes mounted to Cyber Vault; tools validate if data is clean or corrupted
4. Clean copy quickly identified and restored to production
5. Clean data copy used for long term retention off the primary array

Cyber Vault value – detect, respond, recover



1. Corruption of data occurs - but not yet detected
2. Without the IBM Cyber Vault environment corruption is detected much later and has a greater chance to spread
3. It takes even longer to identify all impacted data once the corruption has spread within the enterprise

IBM Cyber Vault Effect

Due to the Cyber Vault environment and the use of Safeguarded Copy technology, data is continuously checked and corruption is found and corrected EARLIER and FASTER

Enterprise-grade cyber security and resiliency

Data validation
Detect data corruption early or certify that the copy is clear

Forensic analysis
Investigate the problem, 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

Oracle tools such as DBVerify, backup tools to validate checksum or run with db_checksum

Db2 tools such as Db2 inspect and db2dart

SQL Server tools such as checkdb or checktable

MongoDB tools – backups and oplog forward recovery

Warehouse databases – Typical to have a set of validation SQL that is run against the tables after each load job and use the output of that SQL against the live dbase to validate that the data in the tables was still good

QRadar / Guardium

Index Engines CyberSense

Next Steps
Take an assessment

Storage Cyber Resiliency Assessment Tool

No-charge assessment

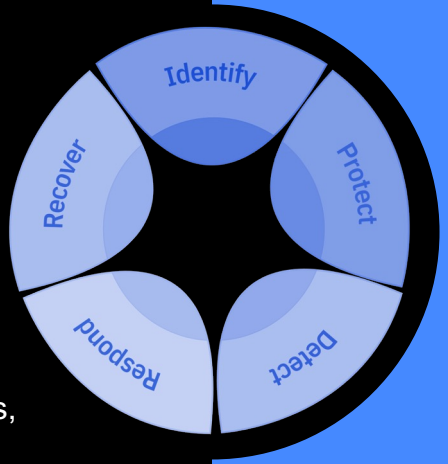
Helps assess your current state

Identifies gaps, strengths, and weaknesses against best practices

Outcomes

- Identify blind spots and recommended areas for improvement
- Discover use of existing solutions, integrations, and overlaps that can be fine-tuned
- Create customized cyber resilience strategy

To request an assessment, contact your IBM Sales Rep or Business Partner, or send an email to the following address: Request an assessment.



Cyber Incident Response Storage Assessment

Identifies strategic cyber resiliency goals

Overview of storage and current cyber resiliency capabilities

Identifies gaps and exposures

Provides recommendations and highlights best practices

Outcomes

- Develops a cyber resiliency plan that aligns storage infrastructure capabilities and business requirements
- Provides a prioritized recommendations roadmap


IBM