IBM Cyber Vault Storage Assessment (CVSA)

Infrastructure expertise to help you prepare for the unexpected

Offering Overview

Kurt Messingschlager
IBM Lab Services – Senior Storage Consultant
kurt.messingschlager@us.ibm.com

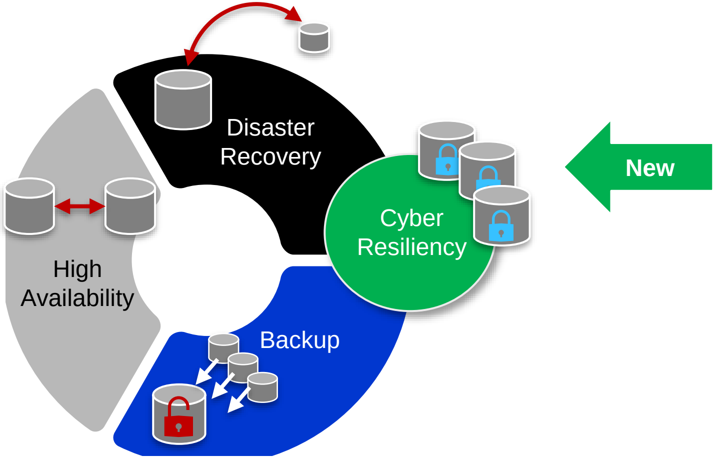
Selwyn Dickey
IBM Lab Services – Managing Power Consultant
sdickey@us.ibm.com

The new 4th data protection practice

Business continuity

"Capability of a business to withstand outages and to operate important services normally and without interruptions in accordance with predefined service-level agreements."

Business continuity consists of four important parts:



New threats call for new methods

The traditional methods (HA, DR, BU) of protection are no longer enough. Organizations need to be Cyber Resilient.

Cyber Resiliency, a new addition to the Business Continuity umbrella, is the ability for an organization to continue to function after a breach has occurred.

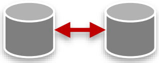
What makes a CR copy different from the other copies?

HA and DR copies are synchronous / asynchronous and will not help against Ransomware

Backup copies are ‘point in time’ (PIT) copies but they are unprotected

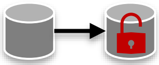
You need protected ‘point in time’ (PIT) copies

✗ High Availability (HA) copies: synchronous copies within a site

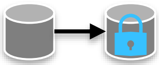


✗ Disaster Recovery (DR) copies: synchronous or asynchronous copies between sites

✗ Backup (BU) copies: unprotected PIT copies

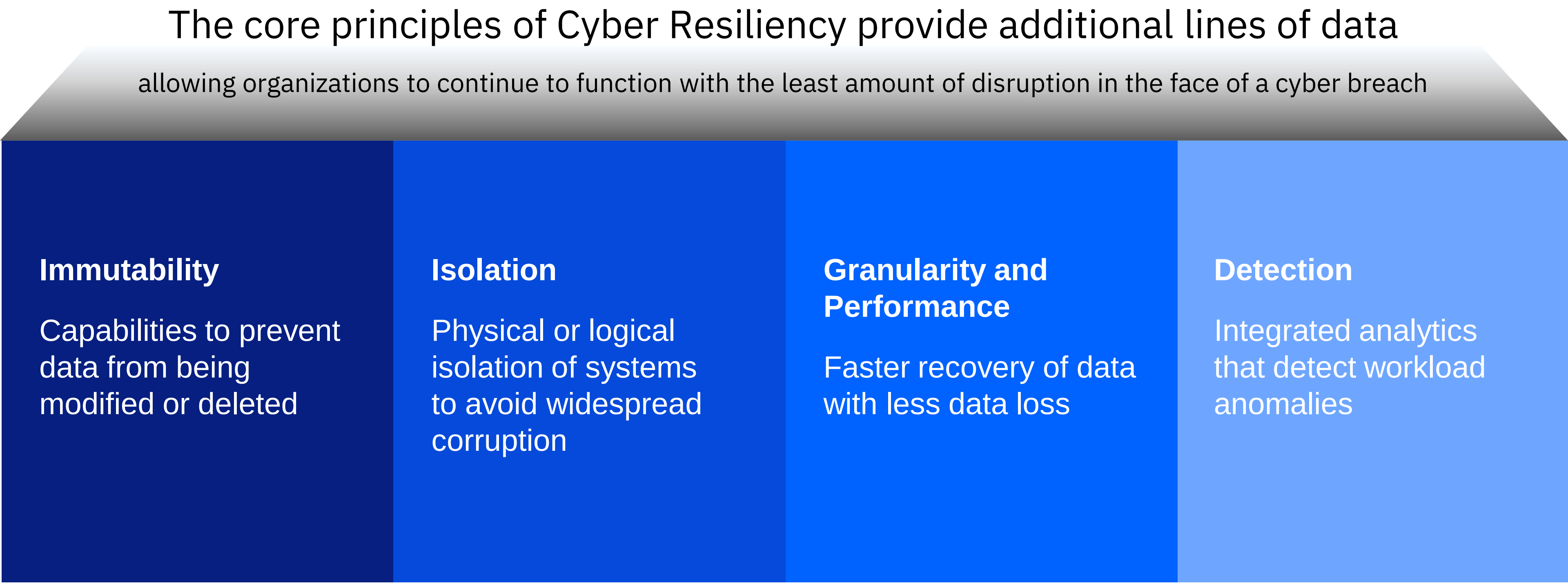


✓ Cyber Resilient (CR) copies: protected PIT copies



Cyber Resilient (CR) copies are PIT copies with added layers of protection: Immutability and/or Isolation

The 4 core principles of Cyber Resiliency



The core principles of Cyber Resiliency provide additional lines of data

allowing organizations to continue to function with the least amount of disruption in the face of a cyber breach

Immutability

Capabilities to prevent data from being modified or deleted

Isolation

Physical or logical isolation of systems to avoid widespread corruption

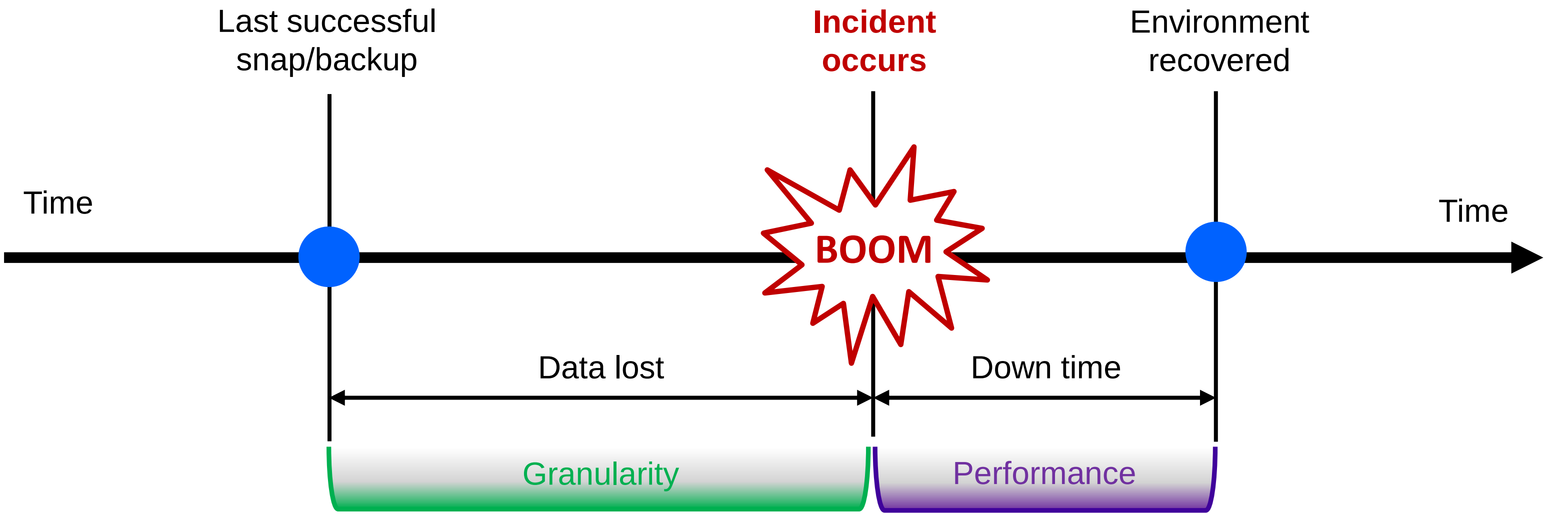
Granularity and Performance

Faster recovery of data with less data loss

Detection

Integrated analytics that detect workload anomalies

When choosing CR solutions, you need to consider the SLOs



Recovery Point Objective (RPO)
How much data loss can be tolerated?
Determined by the frequency of copy creation, i.e. snaps/backups

Recovery Time Objective (RTO)
How fast do we need to recover?
Determined by the amount of time the organization can afford to be offline before losing “too much”, e.g. money, damage to reputation, and/or go out of business

CVSA goal

The Cyber Vault offering

- Is based on IBM's Safeguarded Copy (SGC) solution
- Is a set of three services…
- And is composed of a set of core components

CVSA goal

- To ensure a smooth, tailored and expediated implementation of Cyber Vault, which includes Safeguarded Copy (SGC)

IBM i specific implementation

Install PowerHA tools for IBM i Safeguarded copy

- Configure environment in IBM i to manage the safeguarded Copy
- Configure recovery system for validation/Forensic analysis
- Configure communication to CSM
- Write any custom management CL programs based on customer requirements
- Configure partition to auto set new IP etc on recovery to allow recovery system to come online if required
- Configure job scheduler/management process to automate safeguarded backups
- Configure scheduled checking for SG failures or capacity issues on the storage

- Write processes for recovery/restore after an event

IBM i specific implementation

IBM i Safeguarded copy automation

- STRSGCPY - performs a new Safeguarded Copy backup. Default for expiration interval may be overridden
- STRSGRCY - Performs a safe recovery action by ensuring no current recovery is active. Then it performs the recovery. For Spectrum Virtualize solution it will distribute the LUNS evenly across configured hosts.
- IPLLPAR - activate the IBM i partition
- WRKSTRPRSC/CFGSTRPRSC - Configure the target partitions TPC/IP, tape etc to allow the recovery partition to be used safely after IPL.
- ENDSGRCY - End the active Safeguarded copy recovery
- QZRDIARSGC - CL program to retrieve all current SafeGuarded copy states, information (backupids, expiration interval etc)
- RTVSGCCAP - CL program to retrieve current SG usage and storage remaining capacity

The **Cyber Vault offering** is based on the **IBM Safeguarded Copy solution**

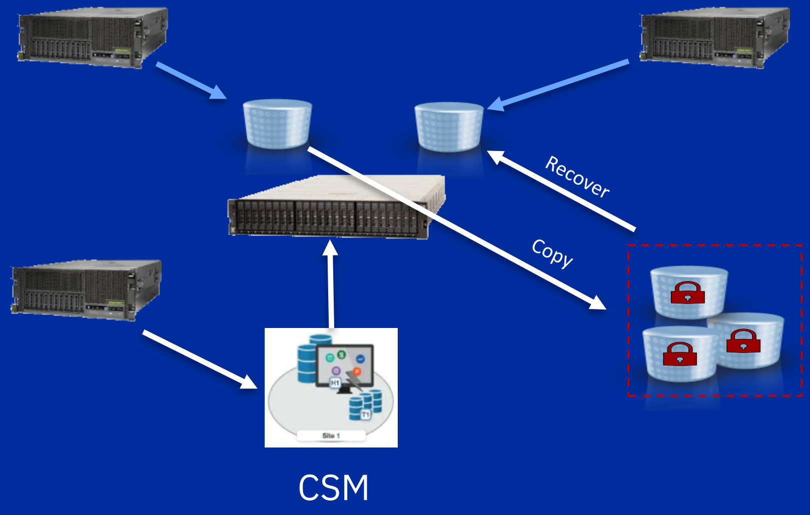
Safeguarded Copy prevents point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks

IBM i Cyber Vault automation

Production partition

Management partition
Orchestration of Safeguarded copy actions

- Start
- End
- Recover
- Restore
- Monitor



Recovery partition
Automatically fixes TCP/IP and other resources per configuration

- Validation
- Forensic analysis
- Surgical recovery

Deployment services for Cyber Vault for Spectrum Virtualize / Flash Systems

Cyber Vault Storage Assessment (CVSA)

- Discuss / confirm client's CR objectives and requirements
- Review Cyber Vault solution components and overall architecture
- Gather inputs to establish scope and sizing for Cyber Vault implementation
- Develop the Cyber Vault future state architecture

Cyber Vault Installation and Configuration

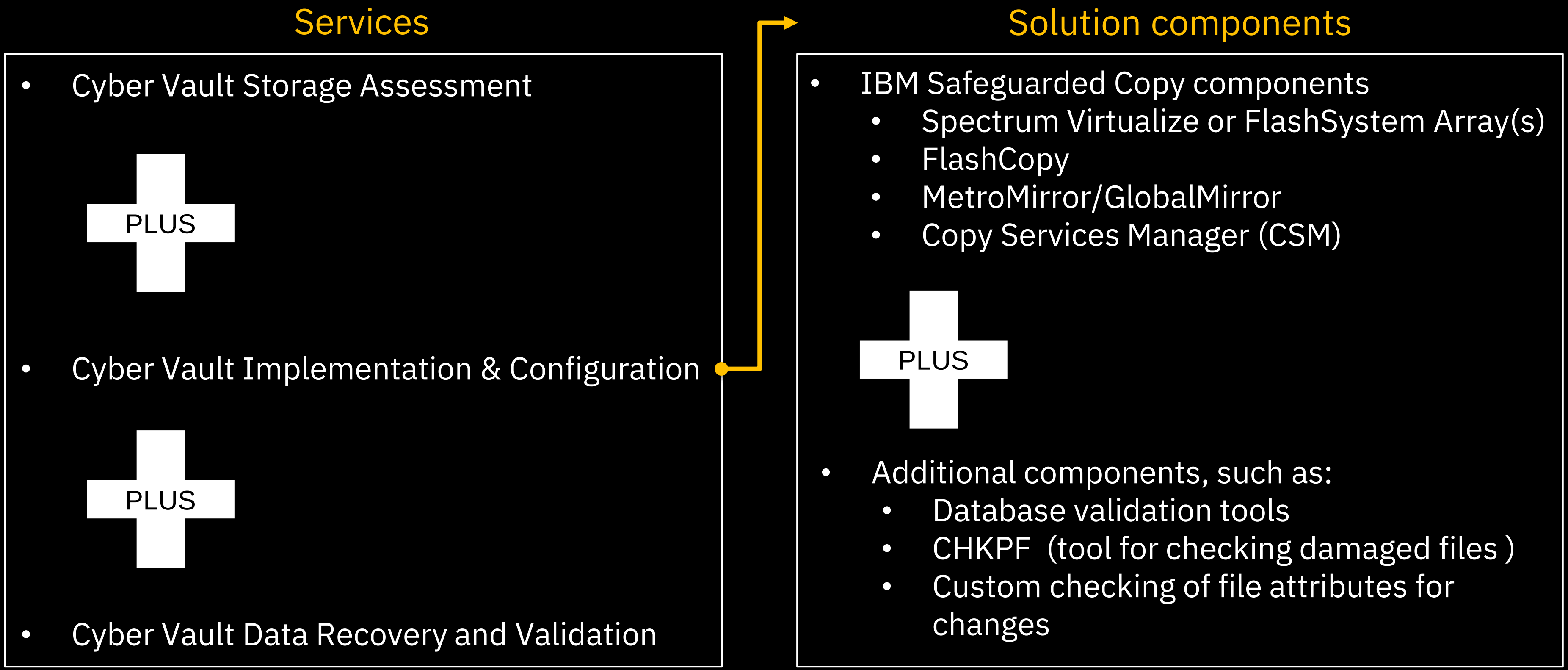
- Install and configure Cyber Vault solution components
- Validate installation completeness
- CV setup and protect knowledge transfer
- CV restore and validate knowledge transfer

Cyber Vault Data Recovery & Validation

- Discuss operational processes and application integration / orchestration required for CV recovery
- Prepare for Cyber Event by exercising the process
- Based on exercises, revisit and tune the process where necessary

Iterative

IBM Cyber Vault is a set of services and solution components



Services

- Cyber Vault Storage Assessment

PLUS

- Cyber Vault Implementation & Configuration

PLUS

- Cyber Vault Data Recovery and Validation

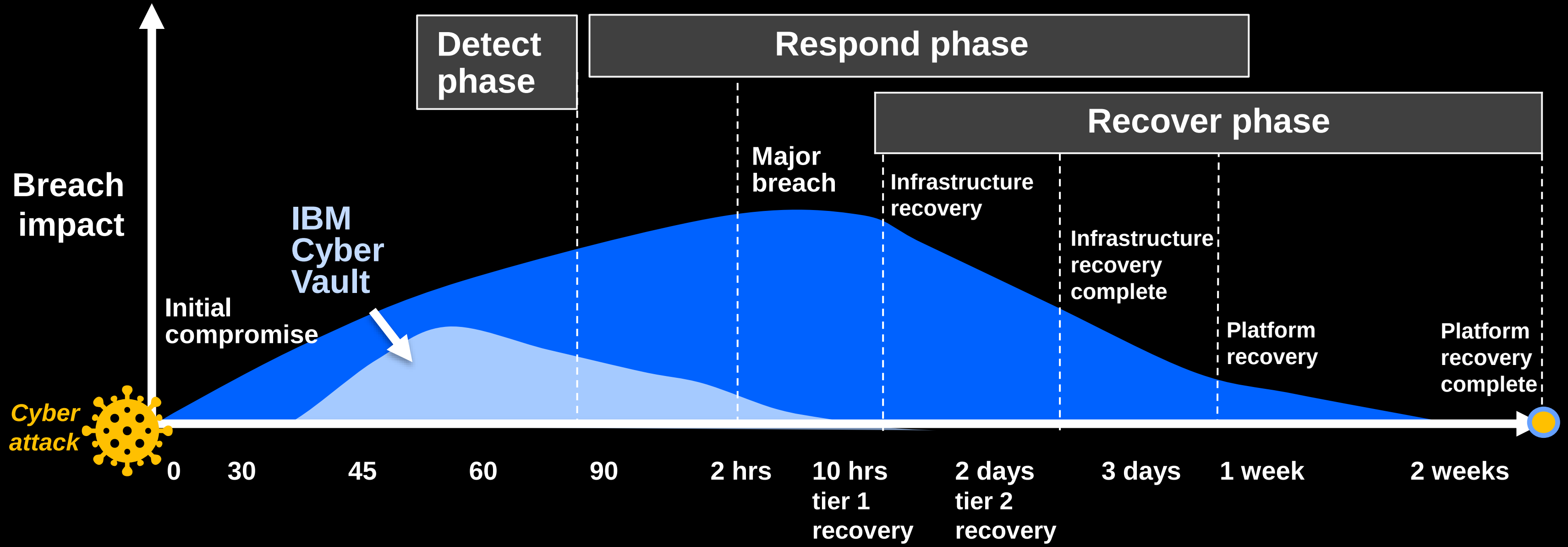
Solution components

- IBM Safeguarded Copy components
  - Spectrum Virtualize or FlashSystem Array(s)
  - FlashCopy
  - MetroMirror/GlobalMirror
  - Copy Services Manager (CSM)

PLUS

- Additional components, such as:
  - Database validation tools
  - CHKPF (tool for checking damaged files)
  - Custom checking of file attributes for changes

Speed recovery to significantly reduce the impact of breaches

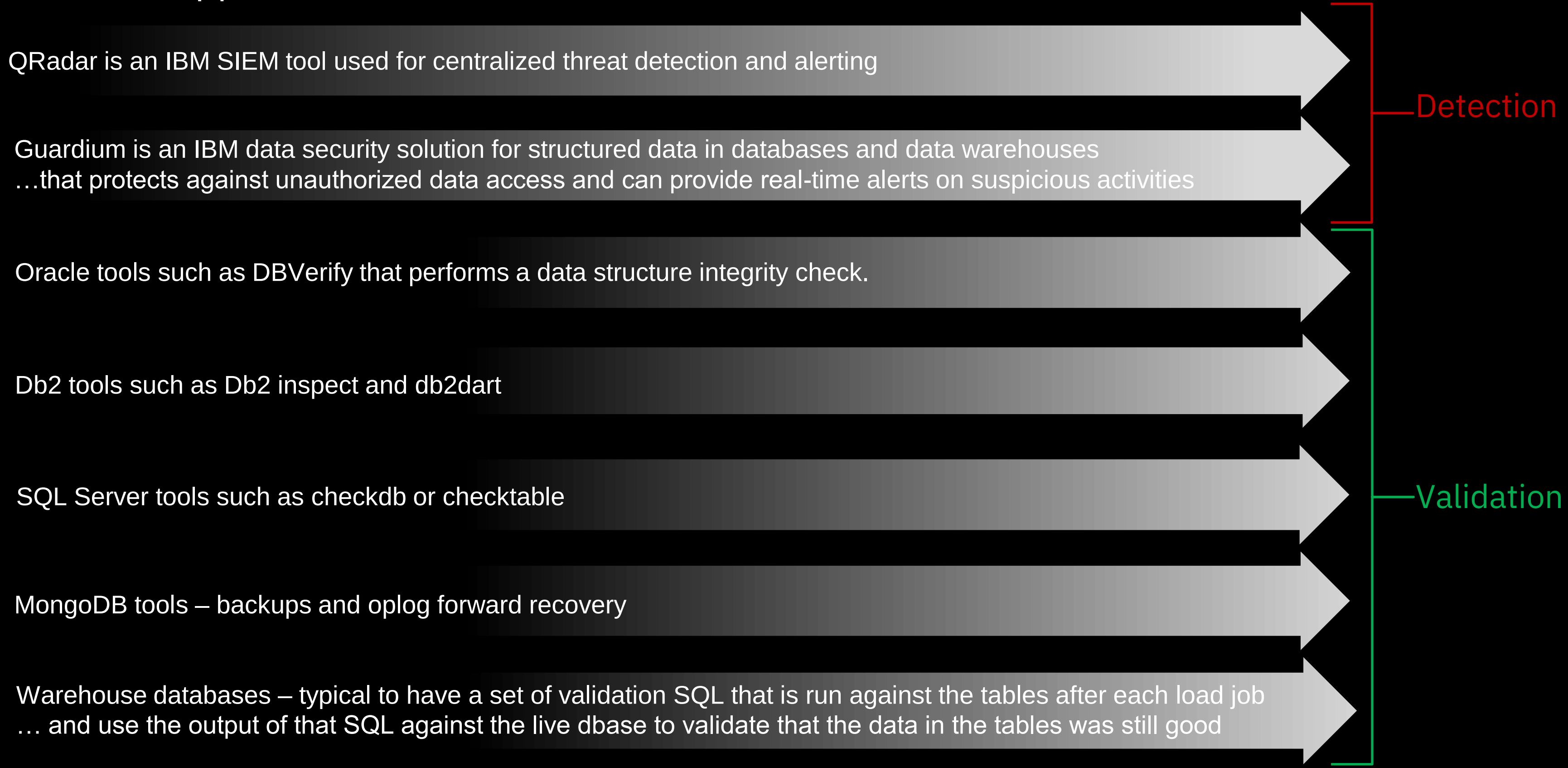


Cyber Vault’s high-speed disk or flash based environment combined with SafeGuarded Copy technology, along with detection and validation tools results in a shortened impact time

(Note: timeline is an example, however based on real client experience)

IBM Cyber Vault additional components

Detection and Application Validation



QRadar is an IBM SIEM tool used for centralized threat detection and alerting

Guardium is an IBM data security solution for structured data in databases and data warehouses
…that protects against unauthorized data access and can provide real-time alerts on suspicious activities

Oracle tools such as DBVerify that performs a data structure integrity check.

Db2 tools such as Db2 inspect and db2dart

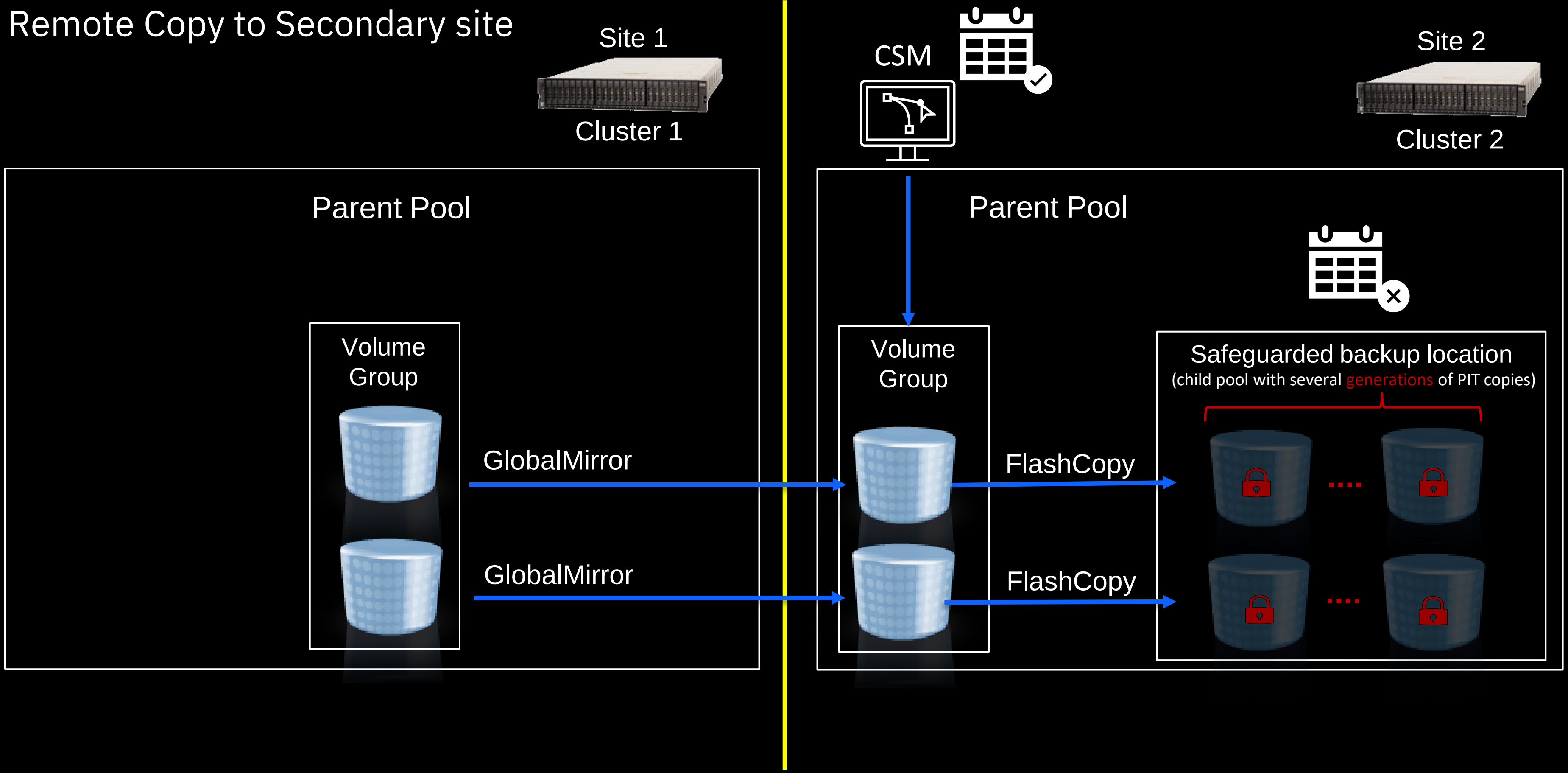
SQL Server tools such as checkdb or checktable

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

Cyber Vault components and topology

Remote Copy to Secondary site



Thank you!