



## Accelerate with ATG: What is IBM Storage Defender?

### Speakers:

Christopher Vollmar, Principal WW Storage Technical Specialist

Christian Burns, WW Storage Technical Sales team

Del Hoobler, Principal Storage SWAT Specialist

## Accelerate with ATG Technical Webinar Series

---

*Advanced Technology Group* experts cover a variety of technical topics.

**Audience:** Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to [accelerate-join@hursley.ibm.com](mailto:accelerate-join@hursley.ibm.com).

### 2024 Upcoming Webinars – click on the link to register for the live event:

January 11 – [Introducing the IBM Storage Scale System 6000](#)

January 16 – [IBM c-Type SAN Update](#)

January 23 – [Exploring the IBM Storage Scale GUI](#)



### Important Links to bookmark:



ATG Accelerate Support Site: <https://www.ibm.com/support/pages/node/1125513>

ATG MediaCenter Channel: <https://ibm.biz/BdfEgQ>

## ATG-Storage Offerings

---

### CLIENT WORKSHOPS

- **IBM DS8900F Advanced Functions: December 6-7, 2023 (Virtual)**
- IBM Storage Point of View on Cyber Resiliency
- IBM FlashSystem and Storage Virtualize
- IBM Storage Scale System and Storage Scale
- IBM FlashSystem 9500 Deep Dive & Advanced Functions
- IBM Storage Fusion

Please reach out to your IBM Rep or Business Partner for future dates and to be nominated.

### TEST DRIVE / DEMO'S

- North America ATG Storage - IBM Storage Scale and Storage Scale System GUI
- North America ATG Storage - IBM Storage Virtualize Test Drive
- North America ATG Storage - IBM DS8900F Storage Management Test Drive
- North America ATG Storage - Managing Copy Services on the DS8000 Using IBM Copy Services Manager Test Drive
- North America ATG Storage - IBM DS8900F Safeguarded Copy (SGC) Test Drive
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (Appliance based)
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (VMware based)
- North America ATG Storage - IBM Storage Protect Live Test Drive
- North America ATG Storage - IBM Storage Ceph Test Drive - (VMware based)

Please reach out to your IBM Rep or Business Partner for more information.

## Accelerate with ATG Technical Webinar Series - Survey

---

Please take a moment to share your feedback with our team!

You can access this 6-question survey via [Menti.com](https://www.menti.com) with code 2243 3599 or

Direct link <https://www.menti.com/albneqj15g57>

Or

QR Code





## Accelerate with ATG: What is IBM Storage Defender?

### Speakers:

Christopher Vollmar, Principal WW Storage Technical Specialist

Christian Burns, WW Storage Technical Sales team

Del Hoobler, Principal Storage SWAT Specialist

## Meet the Speakers

---



Christopher Vollmar

Chris is a Principal WW Storage Technical Specialist helping clients design solutions for Cyber and Data Resiliency. He is an IBM Certified IT Specialist (Thought Leader), an IBM Redbooks author, and frequent speaker at events like IBM THINK and IBM TechXchange.



Christian Burns

Christian Burns is a member of the WW Storage Technical Sales team at IBM, specializing in IBM Storage for Data Resilience. He is one of the principal technical experts on Data Resiliency for IBM Storage Fusion and IBM Storage Defender, especially as it pertains to modern container-based hybrid cloud workloads. Christian has had over 20 years extensive experience across the industry in Data Resiliency at IBM and other companies.



Del Hoobler

Del is a Principal Storage SWAT Specialist for IBM Storage Defender. He has spent over 30 years in the data protection industry as a developer, product manager, and technical specialist. He helps clients architect data resilient infrastructures.



SECURITY BREACH

HACKING DETECTED

Our data is under threat

# Cyberattacks



**CYBER  
ATTACKS**



**RANSOM  
WARE**  
"Time to Ransom"  
dropping to a matter of  
hours



**CYBER  
WARFARE**  
Complete data wipe  
No ability to recover



\$10M for noncompliance of Operational Resilience regulations!



# NIST Cybersecurity Framework – end to end data resilience

## Data security

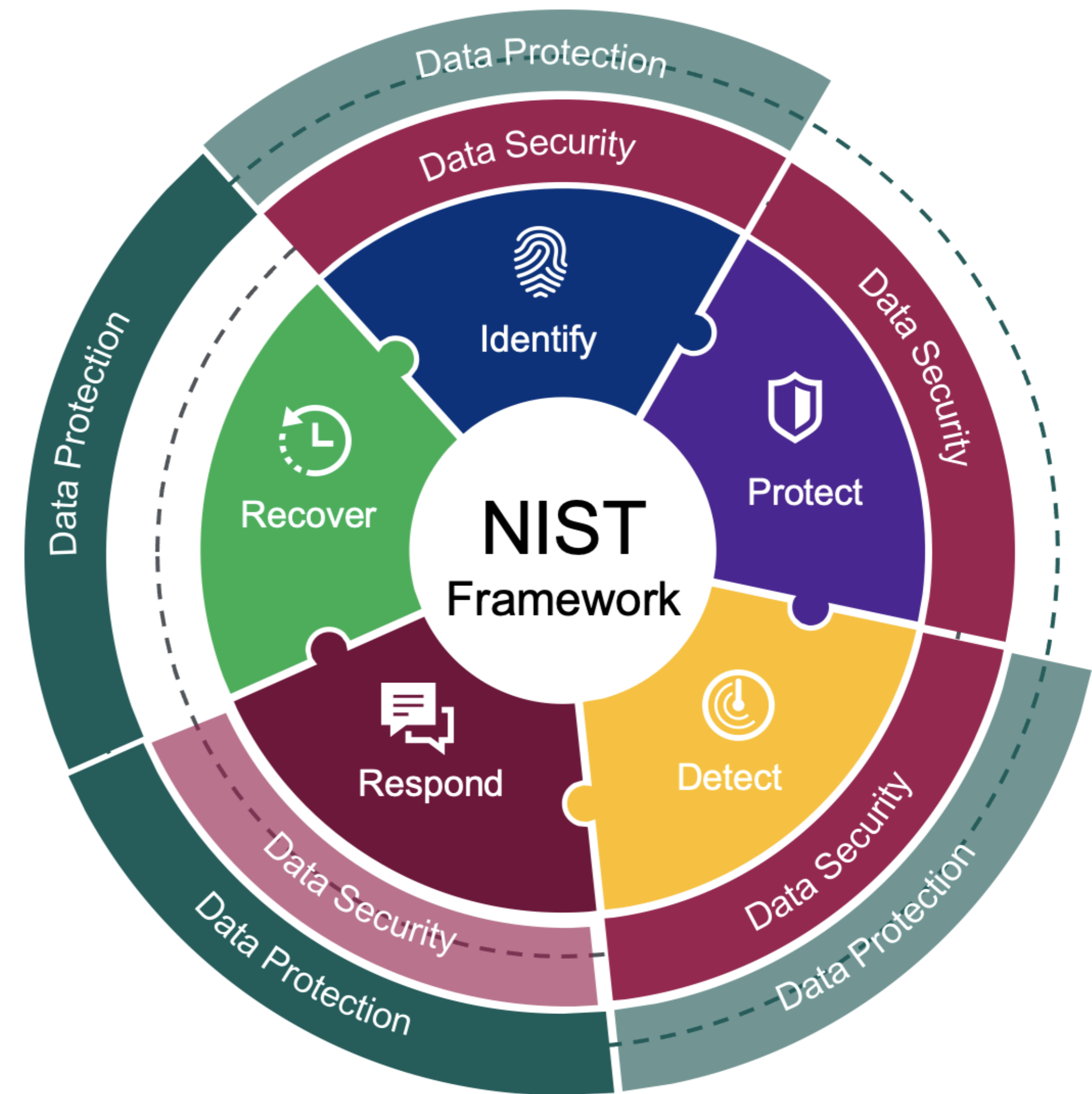
helps detect and prevent attacks, but nothing to recover

## Data protection

is primarily reactionary and does not help avoid attack

**Together**, data security and data protection fulfill the NIST framework

= Data resiliency



# Capability steps to data resilience



## AUTOMATION

Simplified operations plus ability to test and prove recoverability  
Integration between Cyber Security & Cyber Resiliency



## RECOVERY

Rapid business recovery in minutes to hours  
Avoid paying ransomware



## DISCOVERY

Understand when defences have been compromised  
Malware scanner and data pattern insights



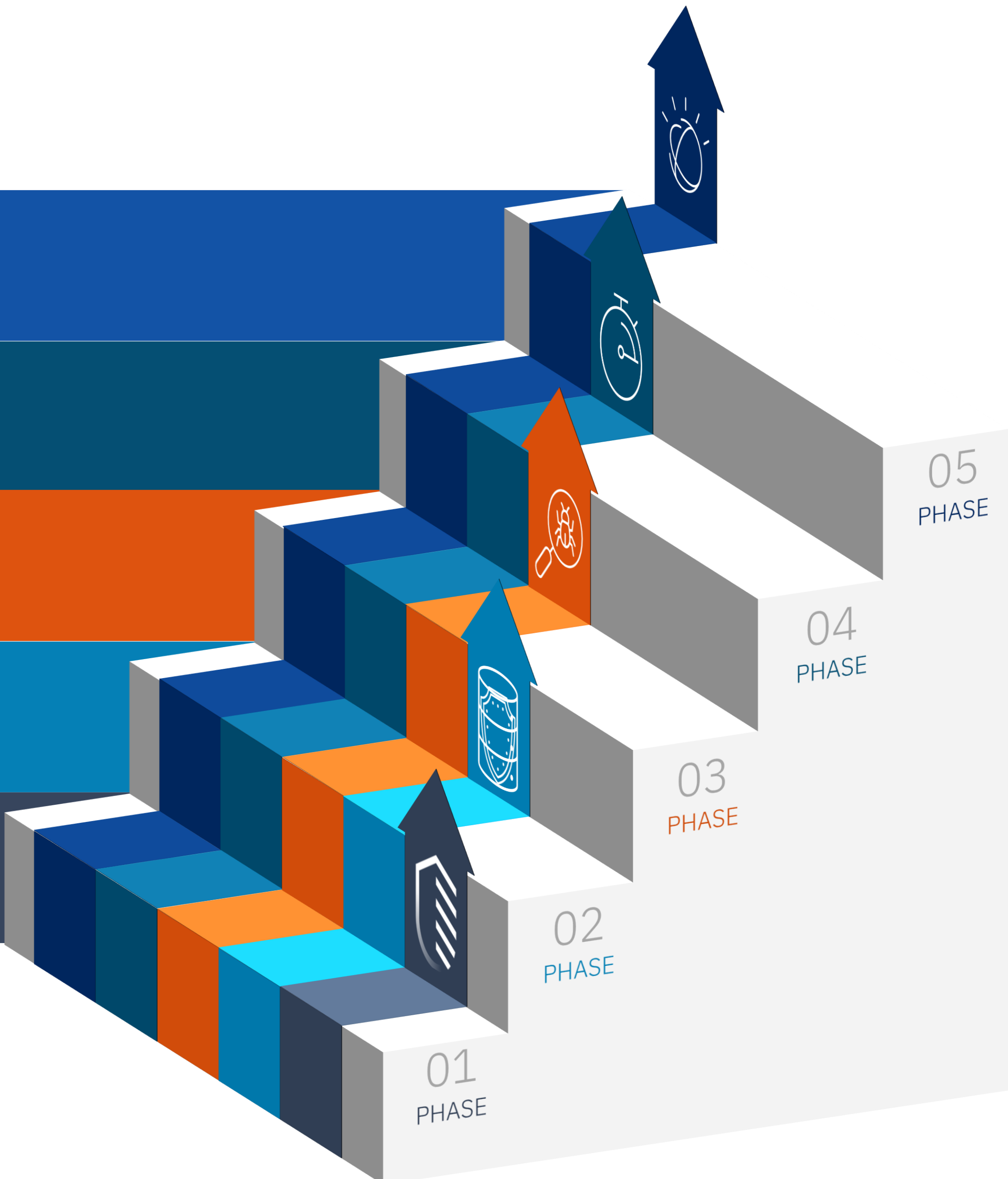
## IMMUTABILITY

Recoverable data points  
Incorruptible, data can not be deleted

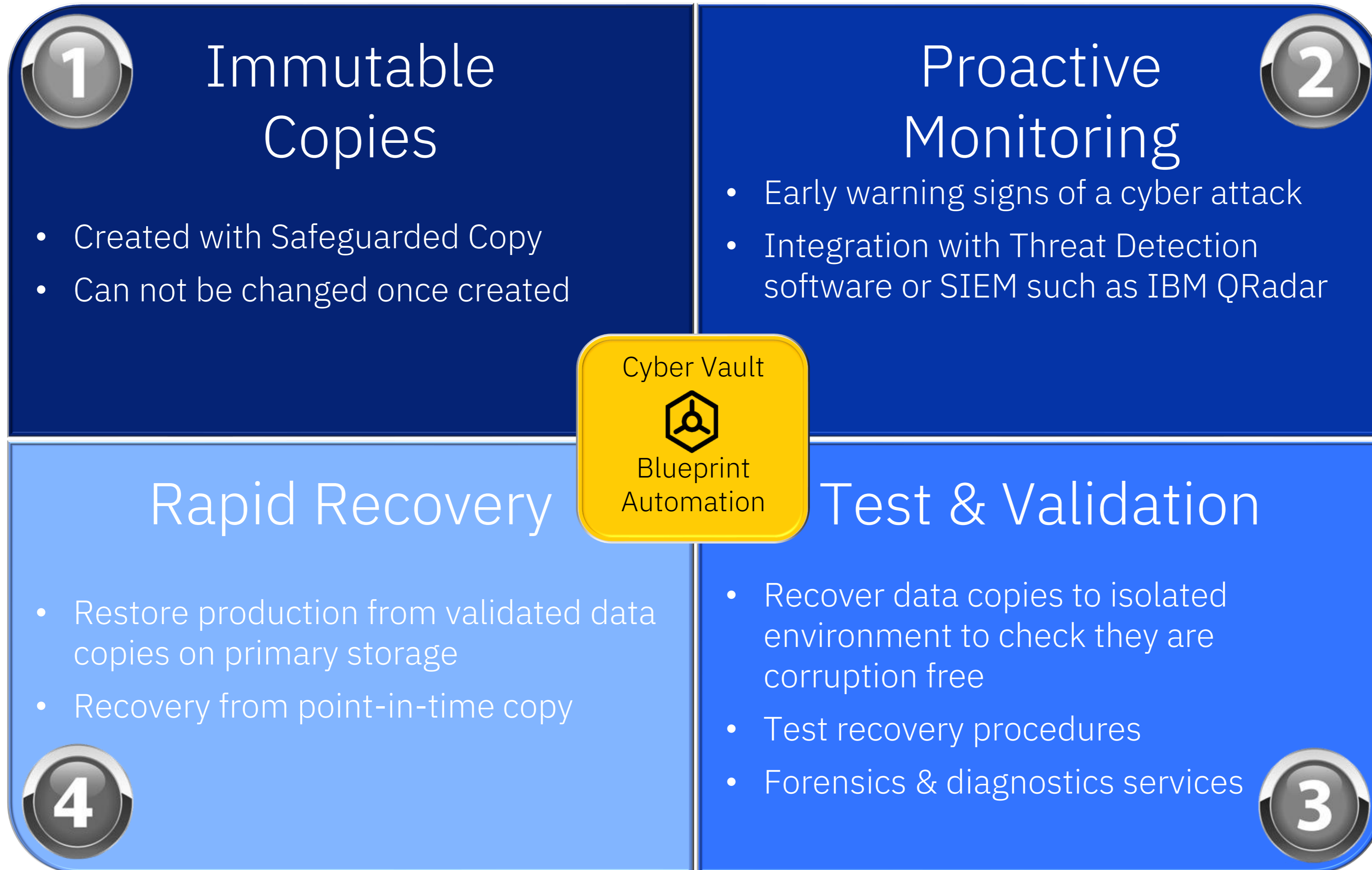


## FOUNDATIONAL SECURITY & DATA PROTECTION

Predict, prevent, and respond SIEM Consultation, QRadar XDR, Guardium  
Protect from infrastructure failures and Natural disasters



# IBM Cyber Vault – Blueprint for Cyber Resilience



March 2, 2023 – IBM announces a large investment in **data resilience**

March 7, 2023 – IBM announces partnership with **Cohesity**

May 26, 2023 – IBM releases **IBM Storage Defender**



IBM Newsroom | Press Releases | Blog | Latest News | Media Contacts | Media Center | Leadership | Global Newsrooms | About | Subscribe

IBM and Cohesity Announce New Data Security and Resiliency Collaboration Advancing Enterprises' Ability to Fight the Impacts of Breaches and Cyberattacks

*New IBM Storage Defender Solution will Manage Data Resiliency for Mission-Critical Enterprise Applications Across the Entire Data Lifecycle*

Mar 2, 2023



Login | 🌐 | 🔍

Clients can strengthen defenses for their data with IBM Storage Defender, now generally available



MAR 7, 2023. 4 min read

**Blue meets green: Why IBM and Cohesity are collaborating now**



# Capability steps to data resilience

## IBM Storage Defender

Holistic visibility, coordinated response, proactive planning  
integration with existing infrastructure, backup and security

### ORCHESTRATION

Simplicity, integration  
with SIEM/SOAR

### MIN VIABLE COMPANY

Fastest recovery, short term  
retention, on-array

### FULL COMPANY

Lower cost, long term  
retention, off-array

### DATA INTEGRITY

Machine learning, malware  
scanning, testing

### ANOMALY DETECTION

Machine learning minimize  
false positives

### DATA ISOLATION

Physical, logical  
air-gapping

### DATA PROTECTION

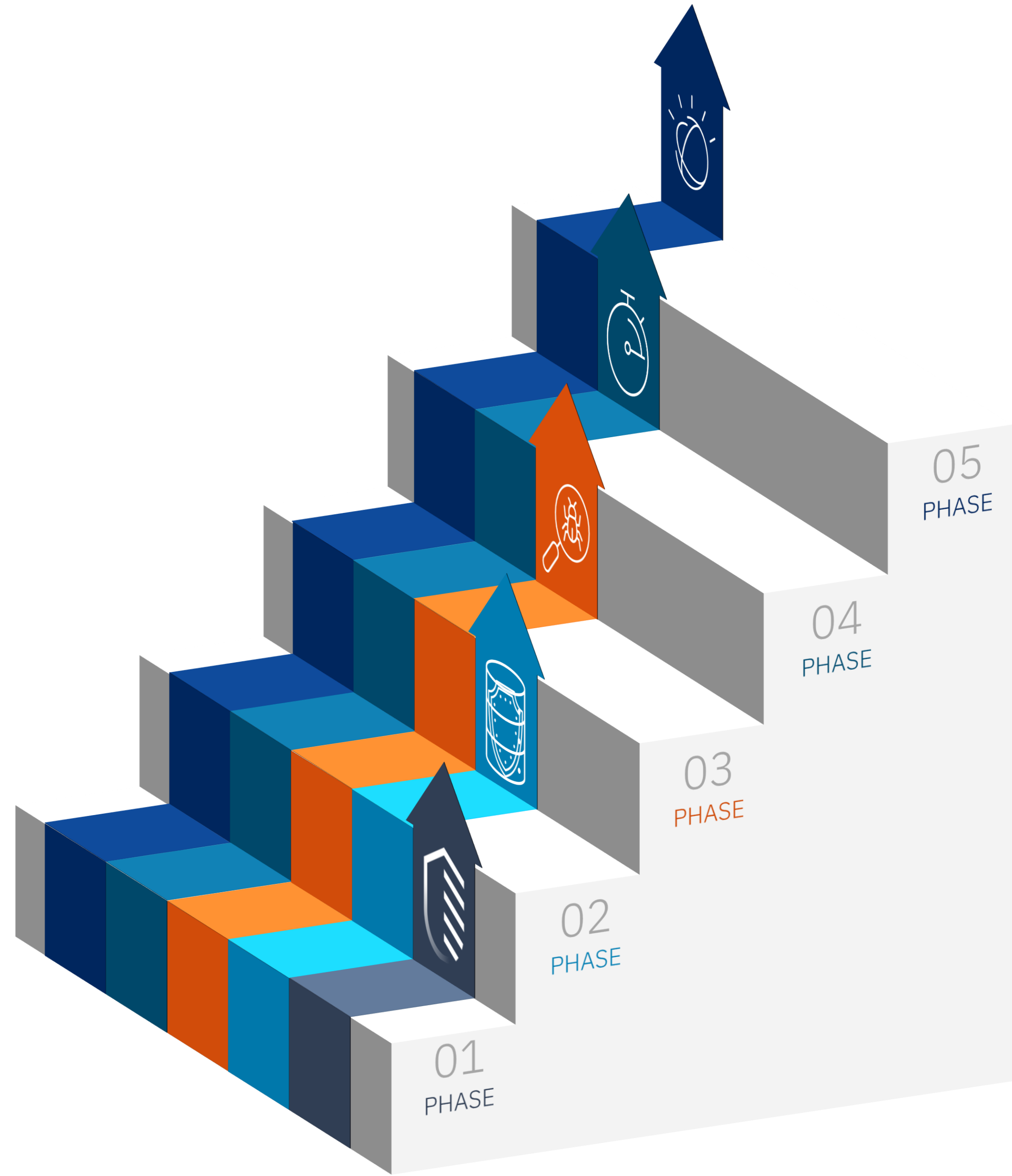
Data copies

### DATA CLASSIFICATION

Compliance, risk,  
Business impact

### CYBER SECURITY

Prevent, detect, respond  
SIEM/SOAR

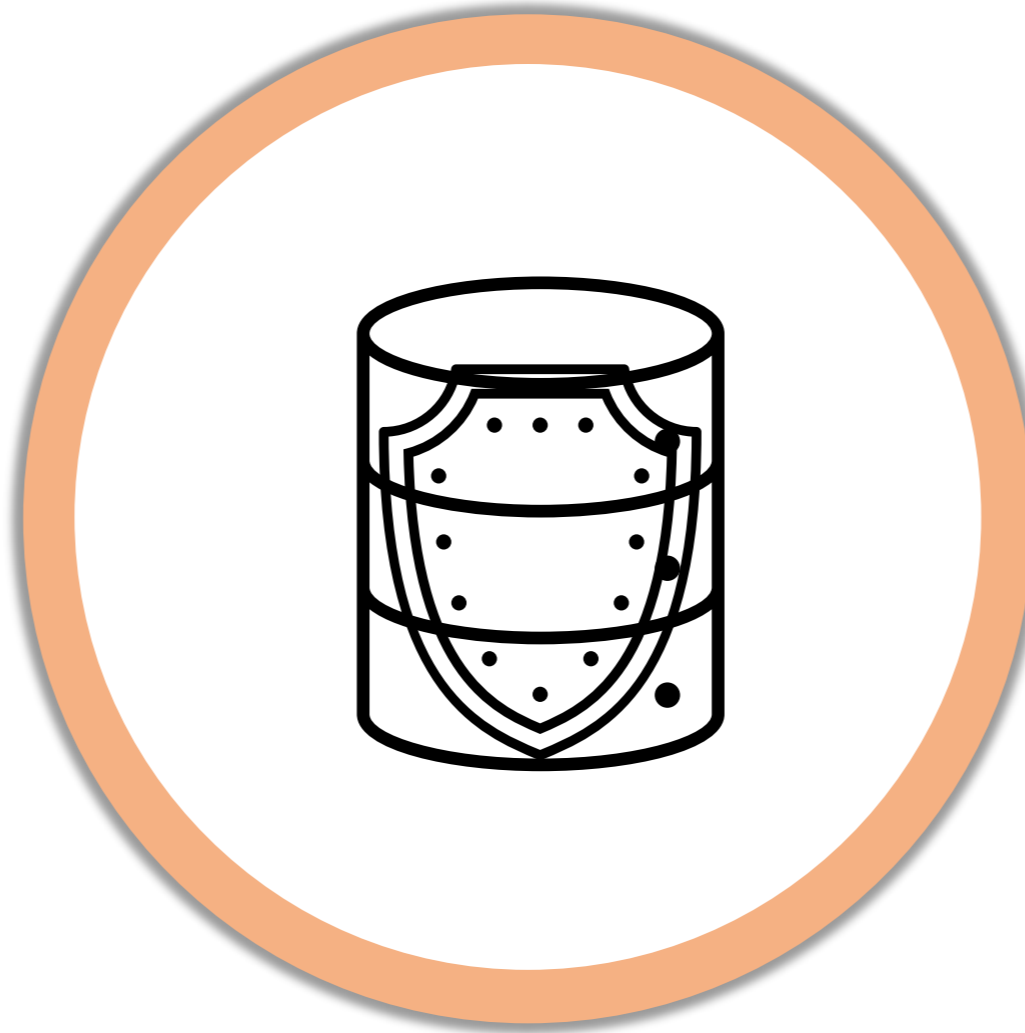
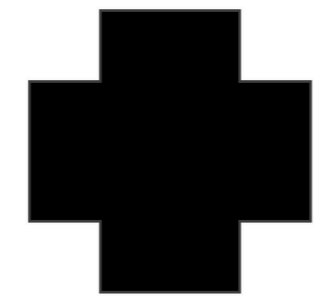


# IBM Storage Defender – Key Capabilities



## Accelerated Discovery

Malware scanning  
Data pattern insights  
Ecosystem scanner support



## Secure Copies

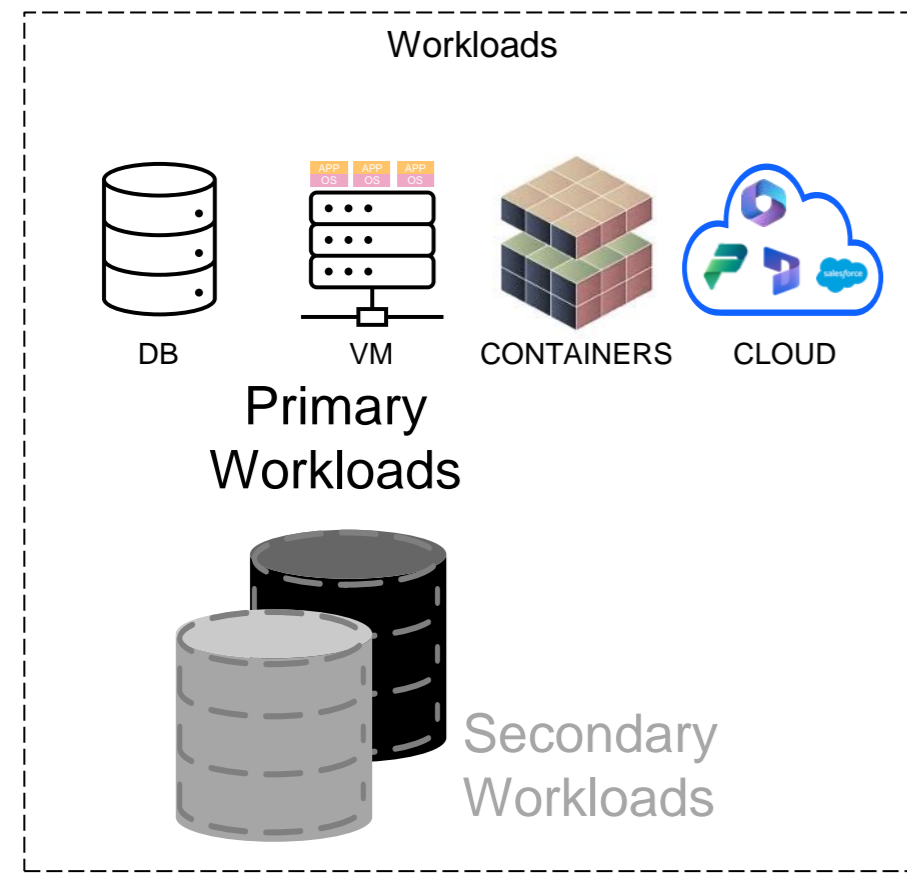
Incorruptible  
Layers of protection  
Clean and reliable data copies



## Fast and Safe Recovery

Simplicity  
Automation/Orchestration  
Primary and secondary workloads

# IBM Storage Defender - Workflow



1

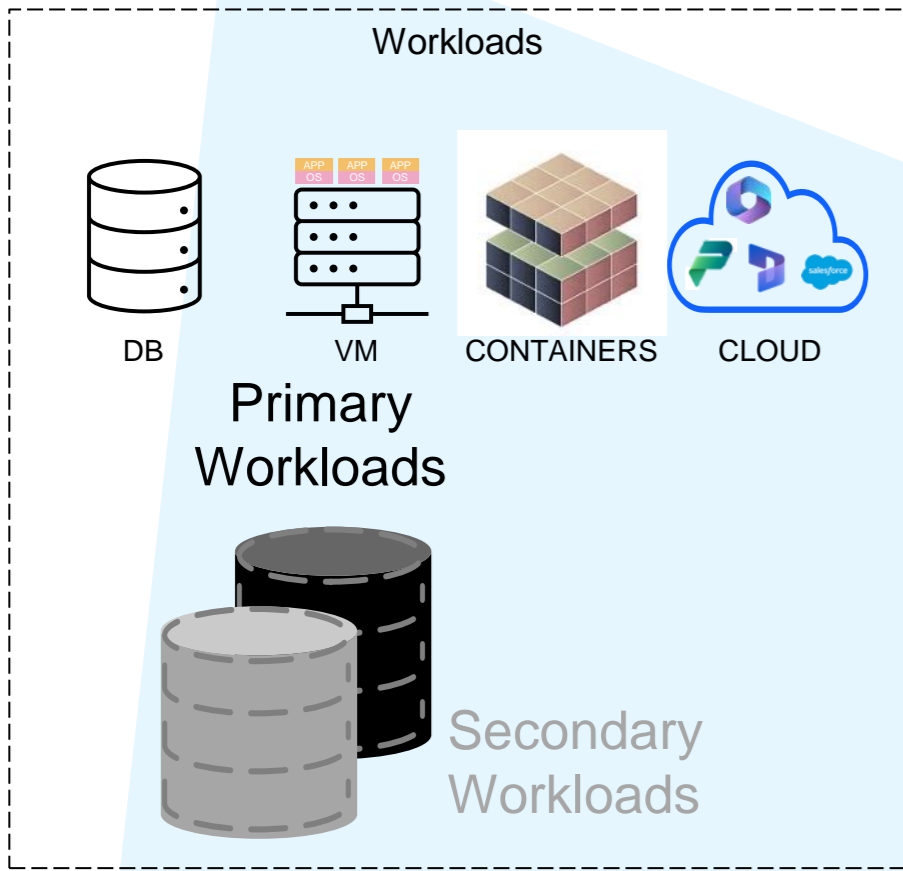
2

3

4

5

# IBM Storage Defender - Workflow



1

Foundational Security & Data Protection

2

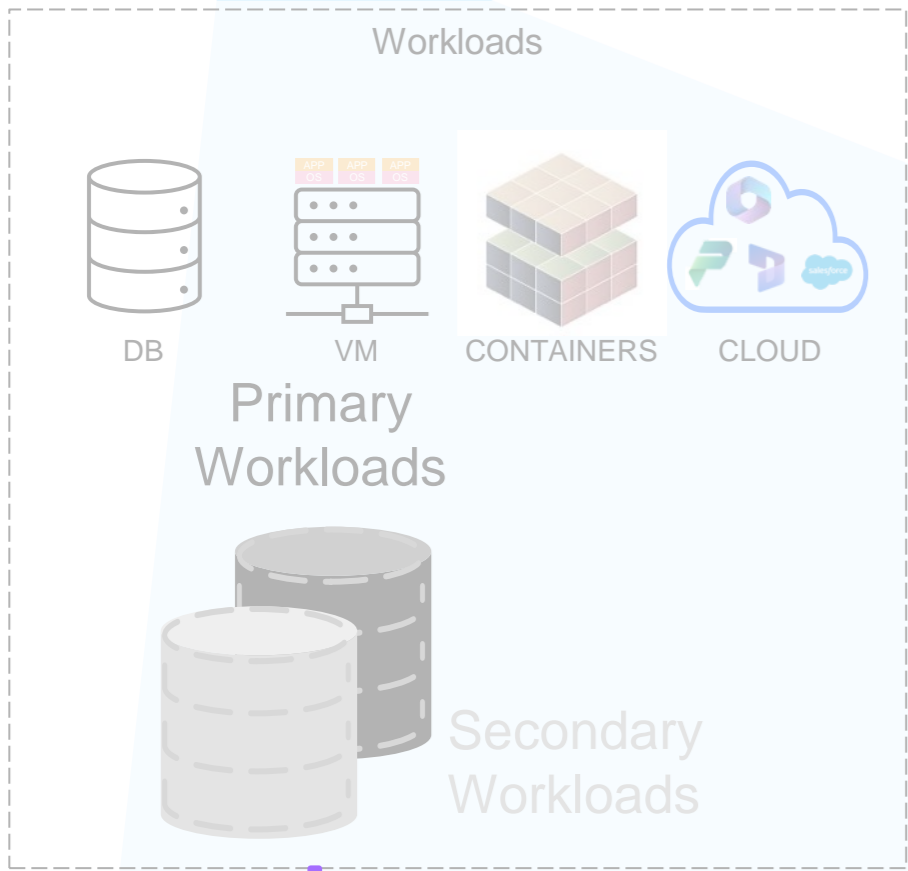
3

4

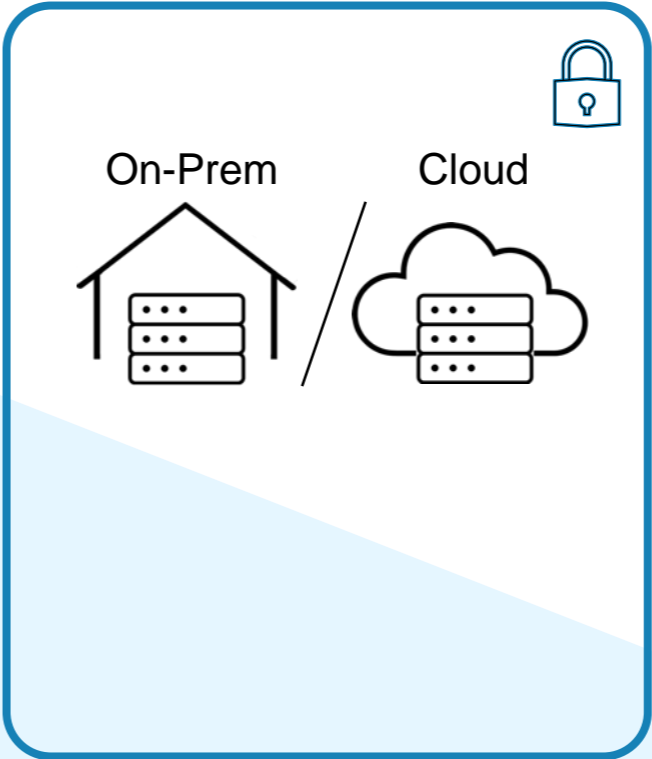
5



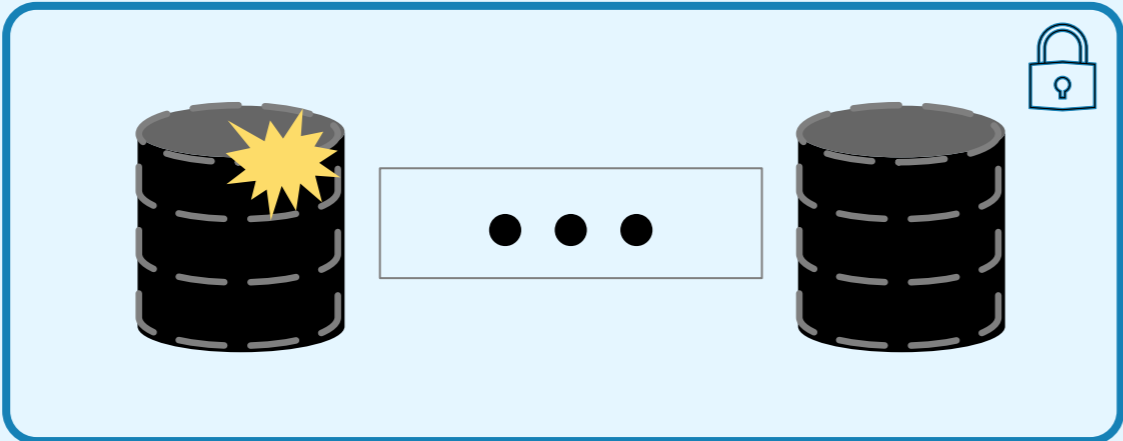
# IBM Storage Defender - Workflow



Isolated Environment

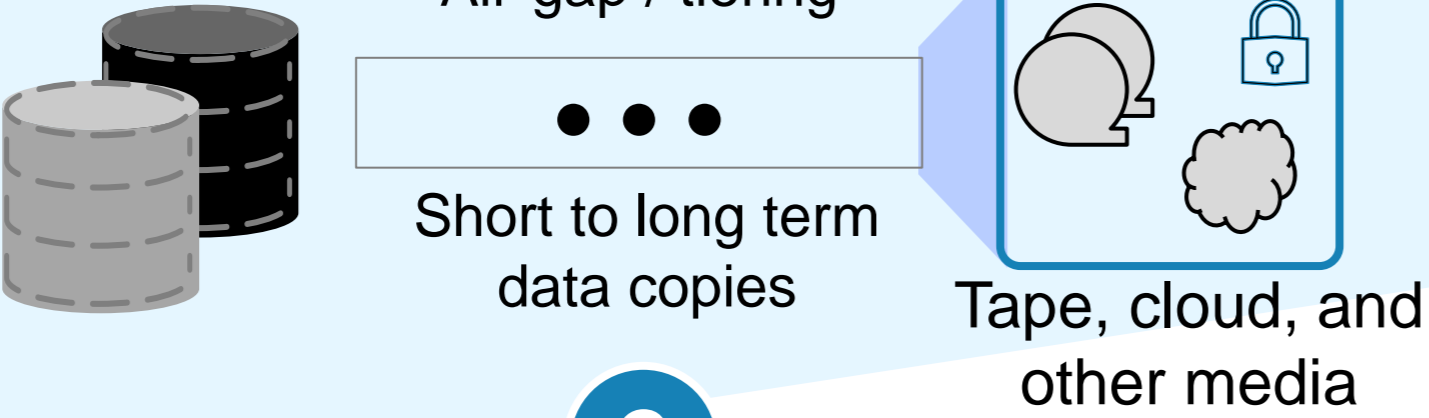


Secure Immutable Copy



Short term data retention for rapid recovery

Air-gap / tiering



1 Immutability

2

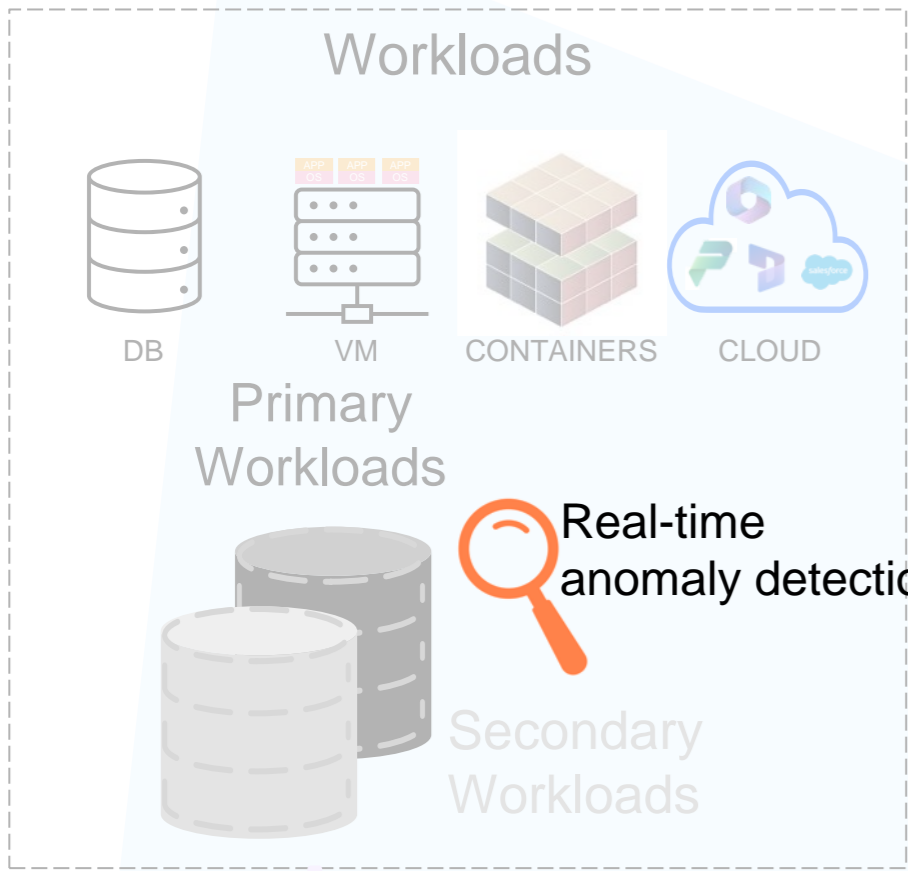
3

4

5

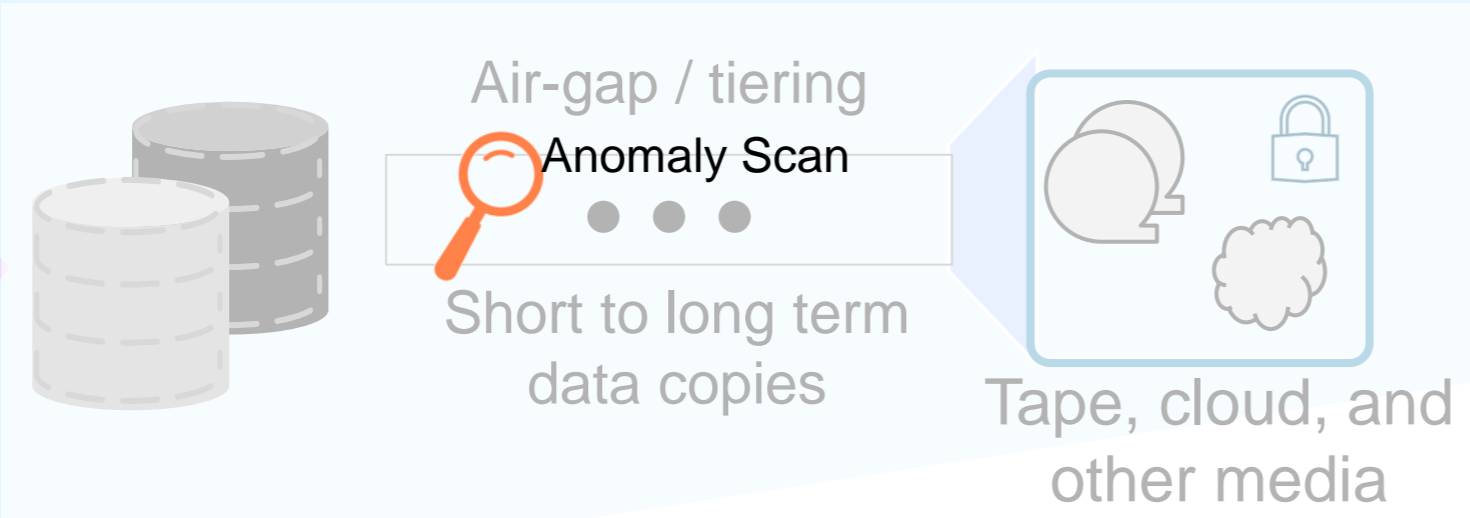
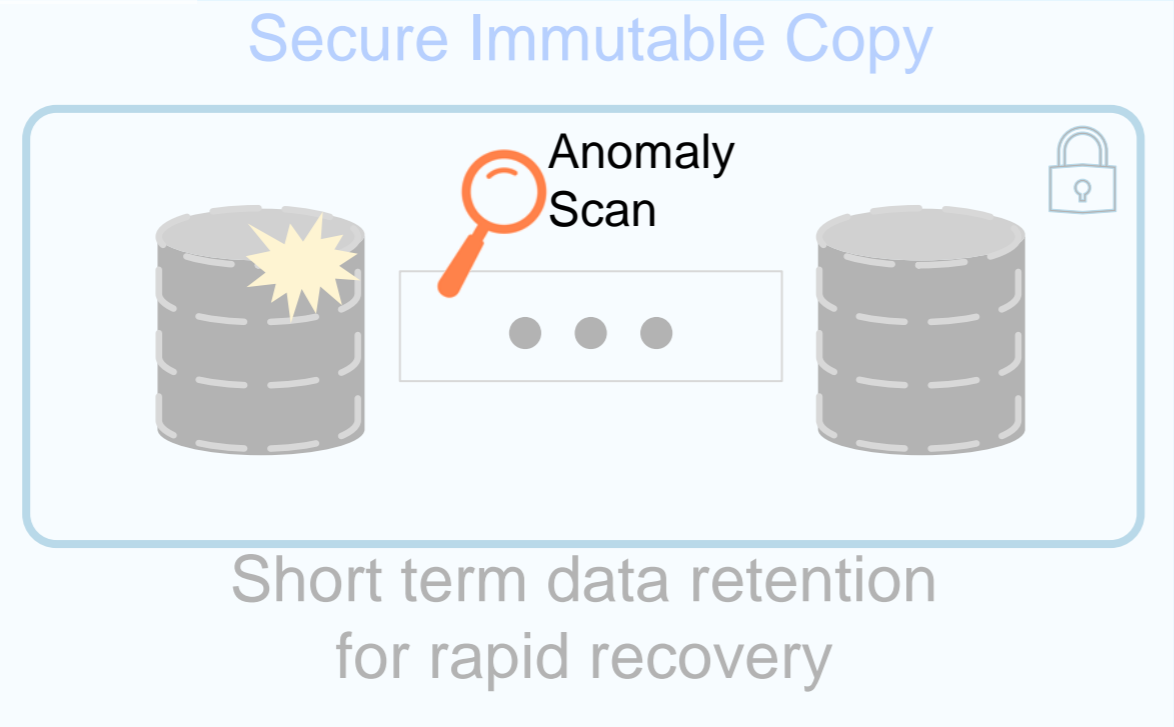
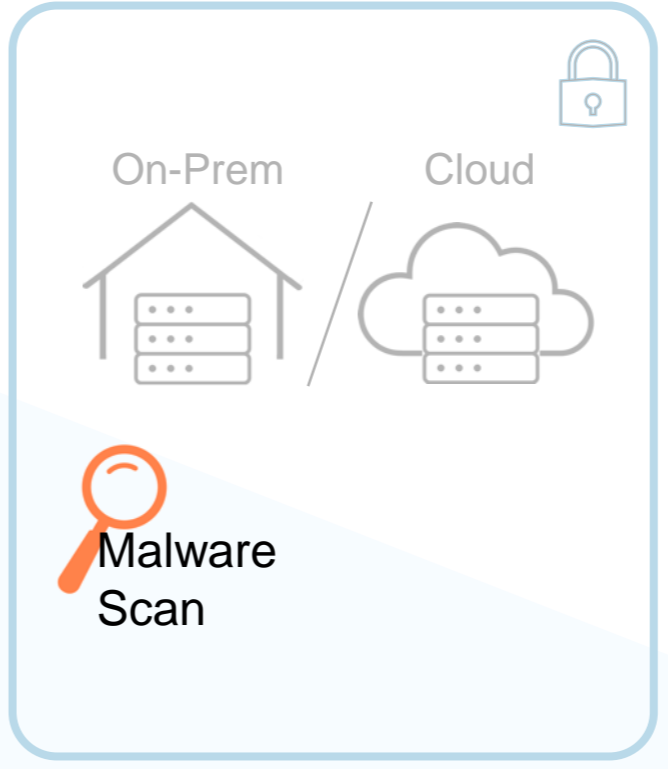


# IBM Storage Defender - Workflow



## Early Threat Detection

Isolated Environment



1

2

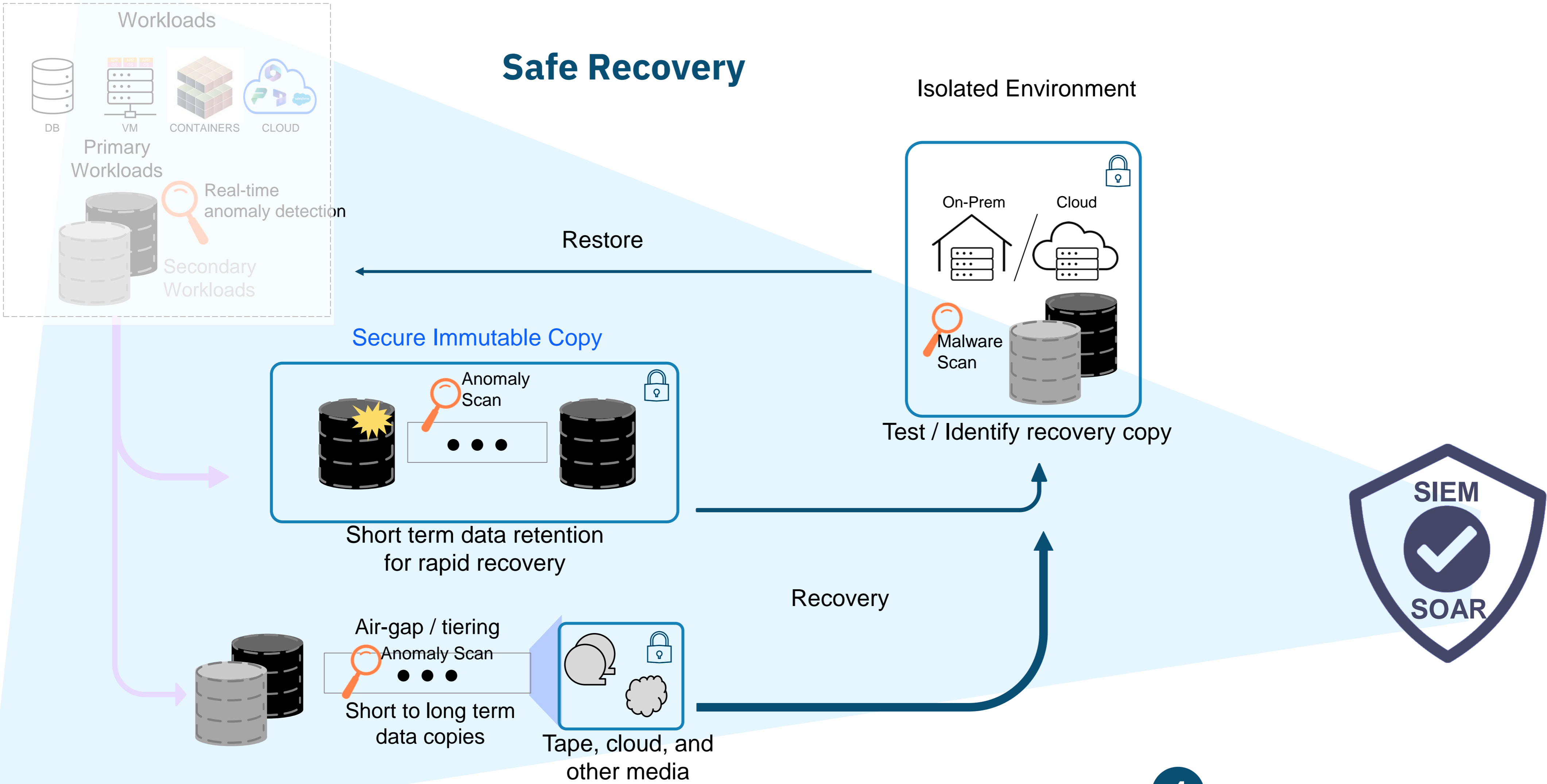
3

Discovery

4

5

# IBM Storage Defender - Workflow



1

2

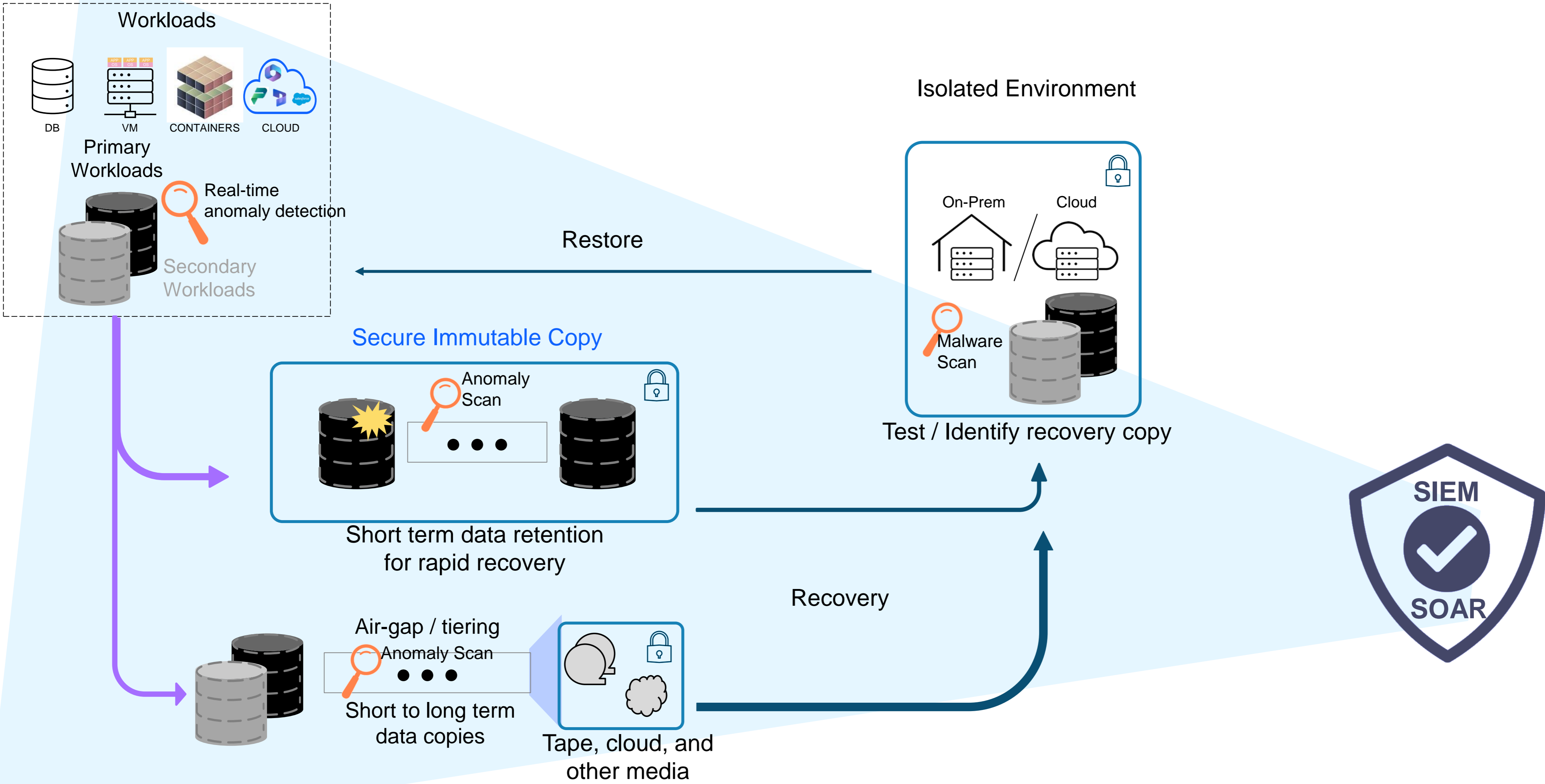
3

4

Recovery

5

# IBM Storage Defender - Workflow



1

2

3

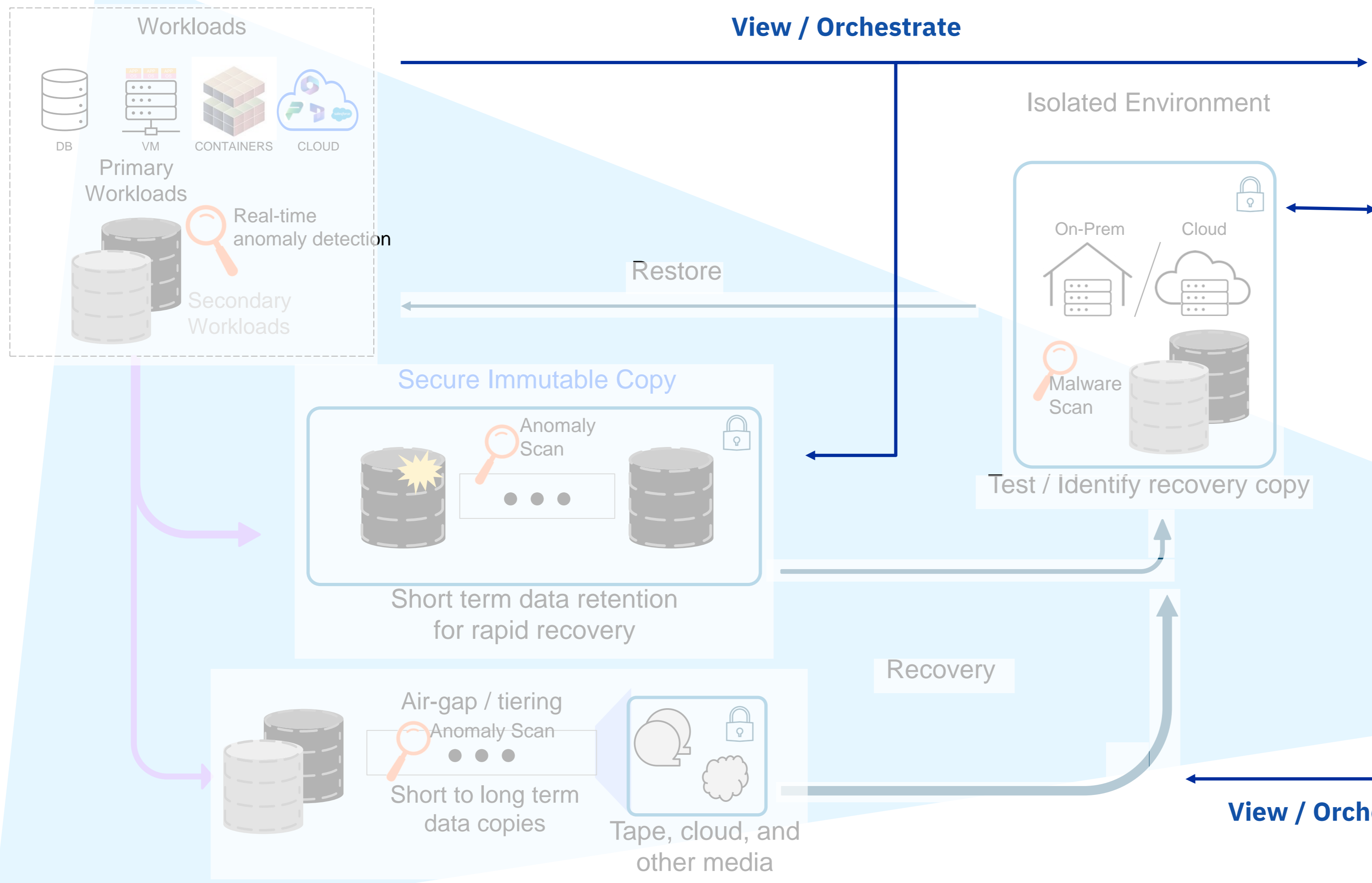
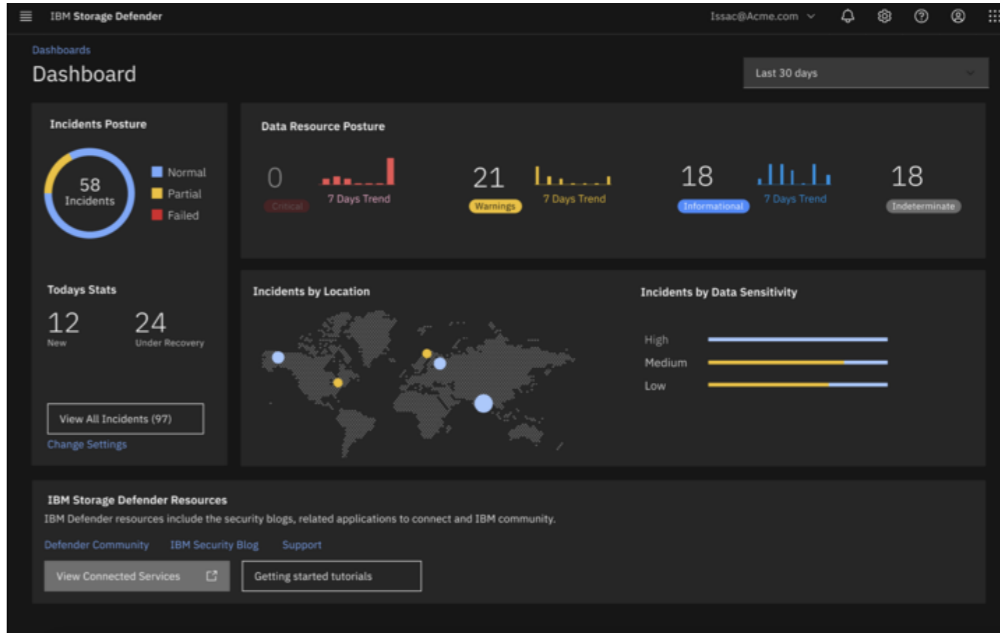
4

5

Automation

# IBM Storage Defender - Workflow

## Dashboard

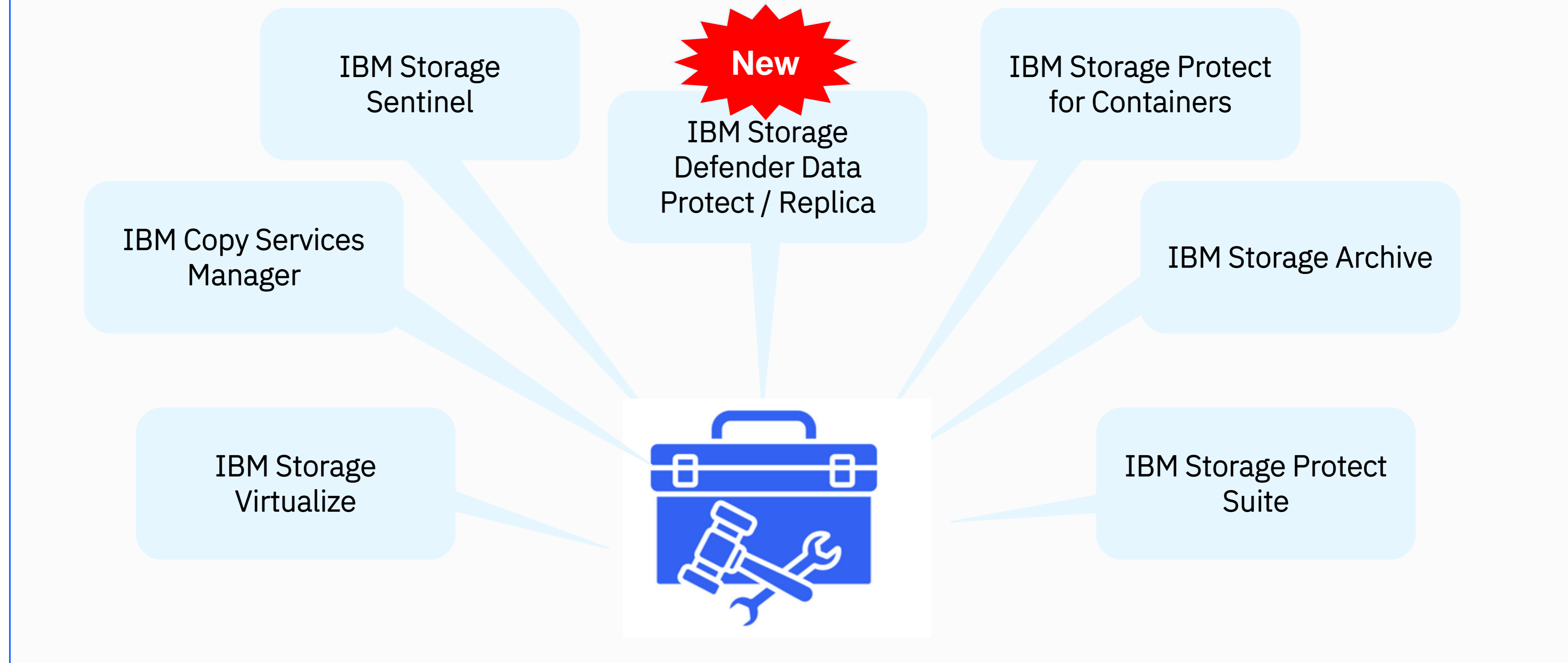


**SOC Integration**



# Available Components

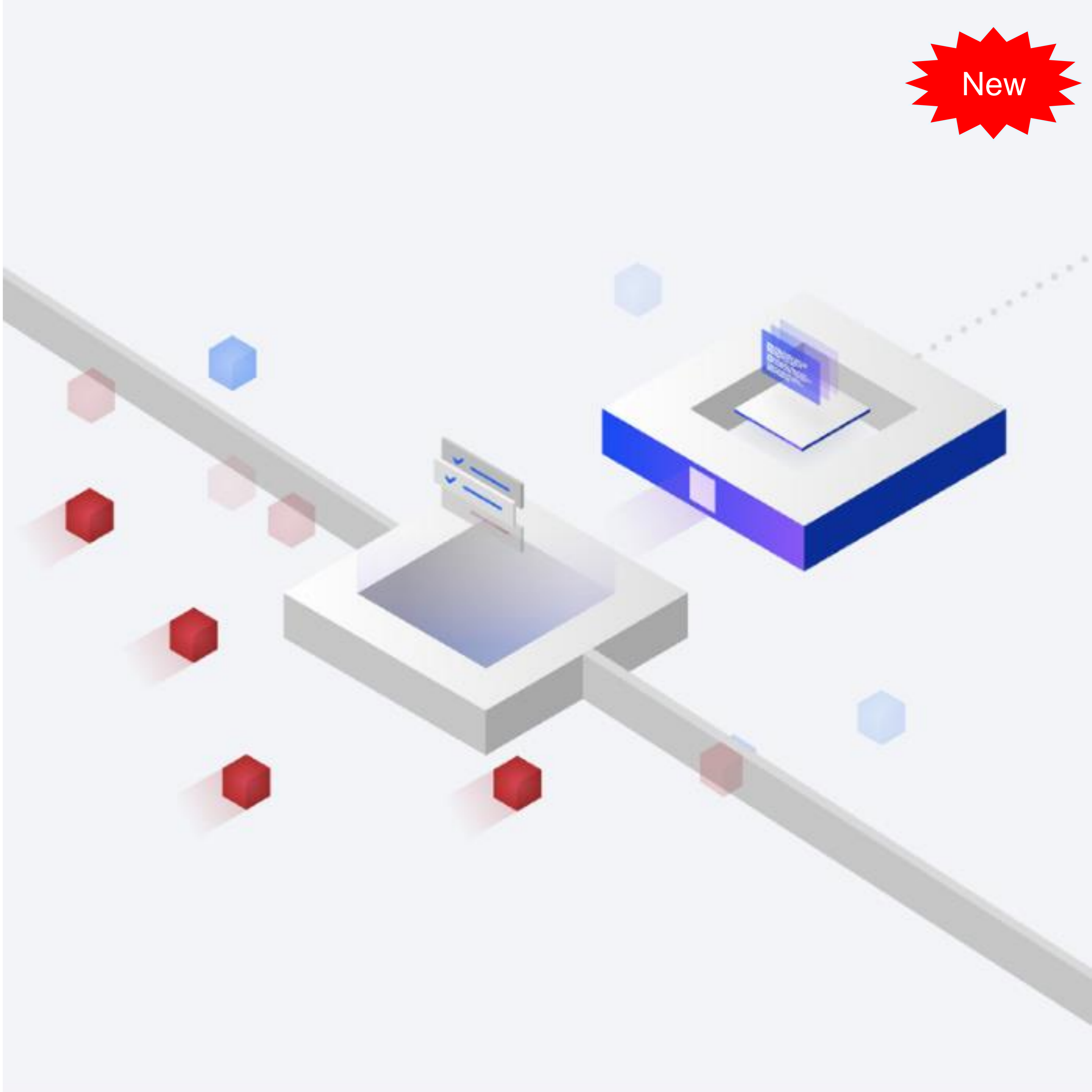
## IBM Storage Defender



- ✓ **Simple licensing** - one license gives you access to everything
- ✓ **Cloud-like consumption** - only pay for what you use

# IBM Storage Defender

## Data Protect



# IBM Storage Defender – Architectural Advantages



## Simple Scale-out Operations

- ✓ Consolidated platform
- ✓ Fast ingest
- ✓ Non-disruptive upgrades



## Global Space Efficiency

- ✓ Variable-length dedupe
- ✓ Compression
- ✓ Erasure coding



## Global Actionable Search

- ✓ Any data, anywhere
- ✓ Across multiple workloads



## Instant Mass Restore

- ✓ At scale
- ✓ Instantly mass restoring any number of virtual machines (VMs)
- ✓ Reduces downtime
- ✓ Reduce costs



## Integrated Cybersecurity

- ✓ Designed on zero-trust principles
- ✓ Ransomware, viruses and vulnerabilities
- ✓ Immutability, WORM, Data encryption
- ✓ Multifactor authentication (MFA)
- ✓ Granular role-based access control (RBAC)
- ✓ Quorum Approval



# IBM Storage for Data Resilience

## Workload Support

### Databases



### Modern Databases



### Cloud-based Databases



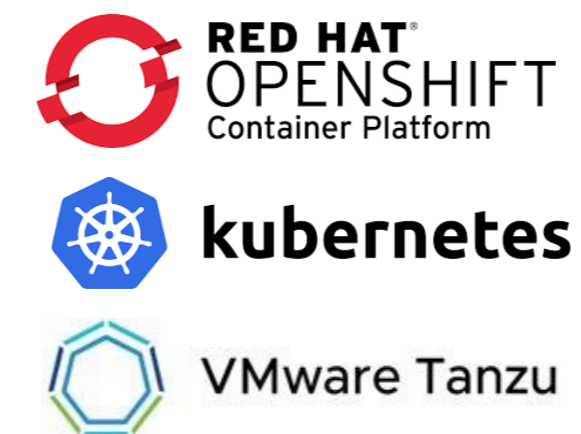
### Primary Storage

Over 500 systems supported

### Hypervisors



### Containers



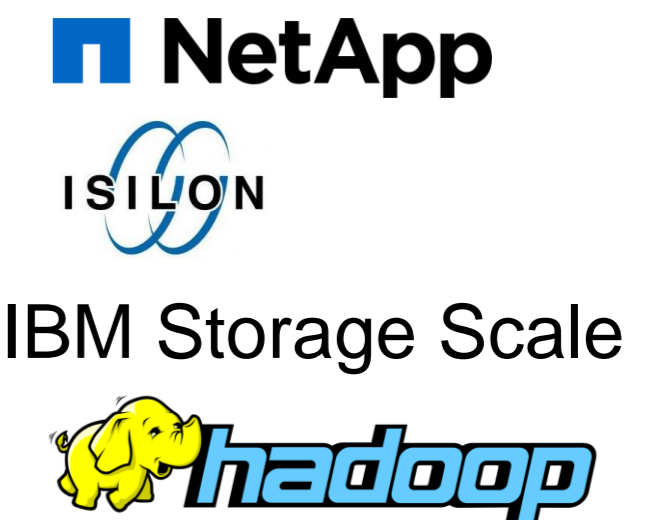
### Physical



### Applications



### File Systems



### Cloud



# Data resilience is a team sport

*IBM and its partners combat threats together.*

Data protection (Snapshot, Backup)	COHESITY	AvePoint	cobalt IRON
Data Integrity (Scanning, Recovery)	INDEX ENGINES	sāf.ai Data, Evolved.	PREDATAR
Data Classification	VARONIS	BigID	IBM Guardium
Data Isolation (Physical, Logical air-gapping)	PREDATAR	COHESITY	cobalt IRON
Threat Detection (Data XDR)	Bitdefender IBM X-Force	AvePoint	COHESITY
Cyber Security (SIEM, SOAR, CASB)	IBM Security QRadar® SIEM QRadar® SOAR	CROWDSTRIKE SentinelOne	CORTEX BY PALO ALTO NETWORKS netskope

# IBM Storage for Data Resilience

*Built for Hybrid Cloud*

- ✓ Back up **to** the cloud
- ✓ Replicate **to** the cloud
- ✓ Back up **in** the cloud



- ✓ Protect **SaaS** applications (ex: Microsoft 365, Salesforce, Azure AD)
- ✓ Protect **cloud-native VMs** (like EC2, Azure VM, Google Compute)
- ✓ Protect **cloud-native applications** (like AWS RDS, CockroachDB)
- ✓ Protect **containerized applications** in the cloud (like OpenShift)

# IBM Storage Defender – Simple Dashboard



✓ Single pane of glass to manage your data protection

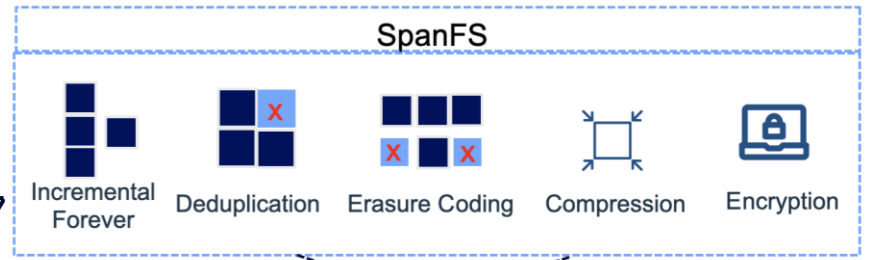
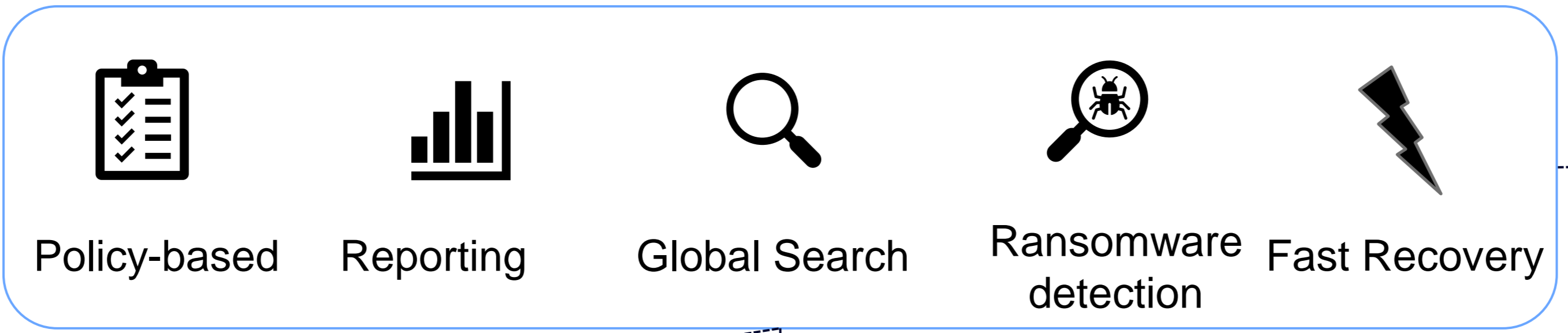
# IBM Storage Defender Data Protect

## Architecture Summary

### Data Management Service (DMS)

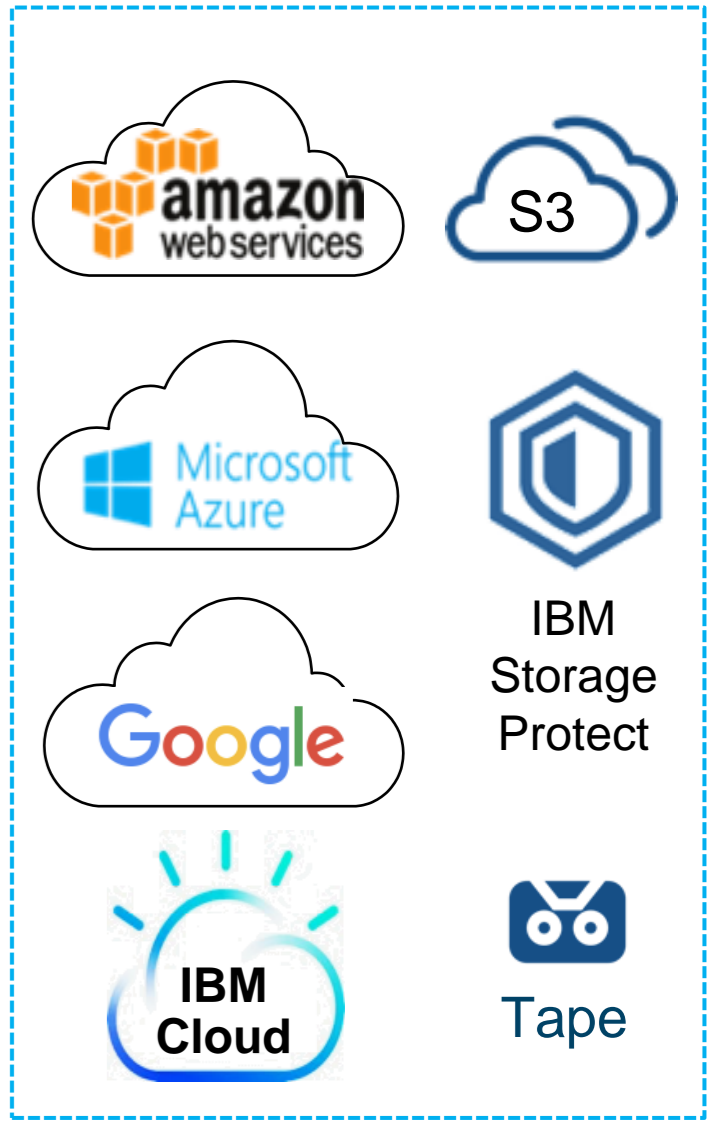
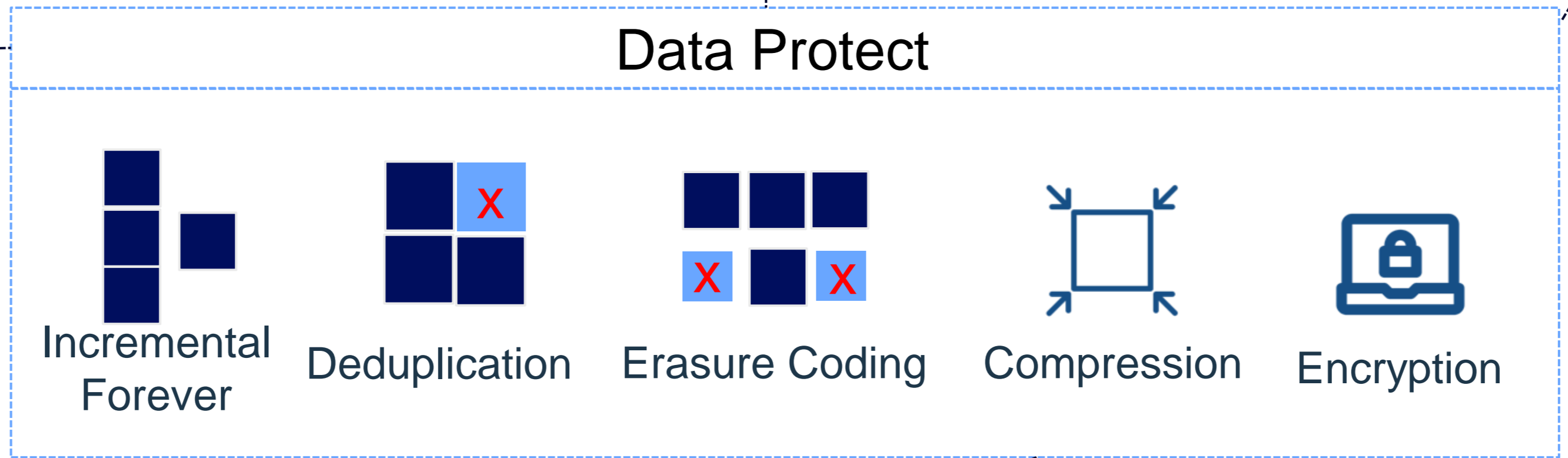


Centrally Managed

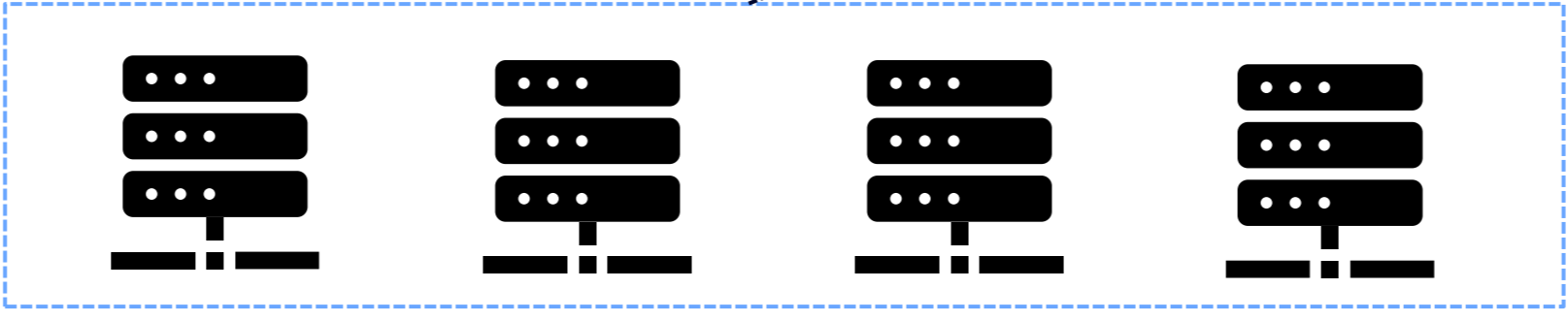


Replicated

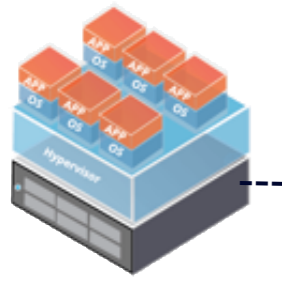
Optimized/Immutable



Copied



Scale-out Cluster



VMs



DBs/Apps



NAS/Filers



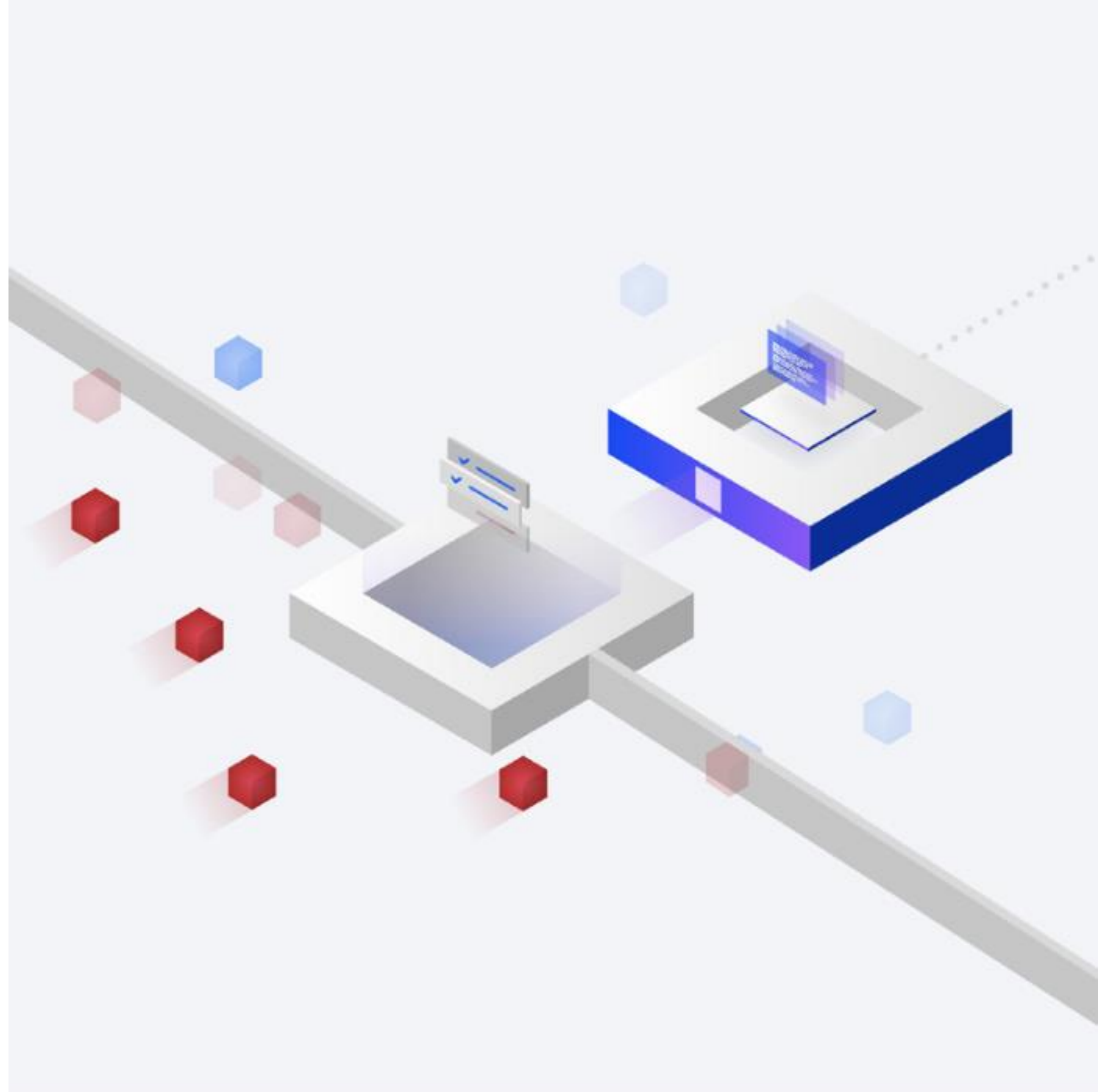
Cloud

Workloads

# IBM Storage Defender

## Data Protect

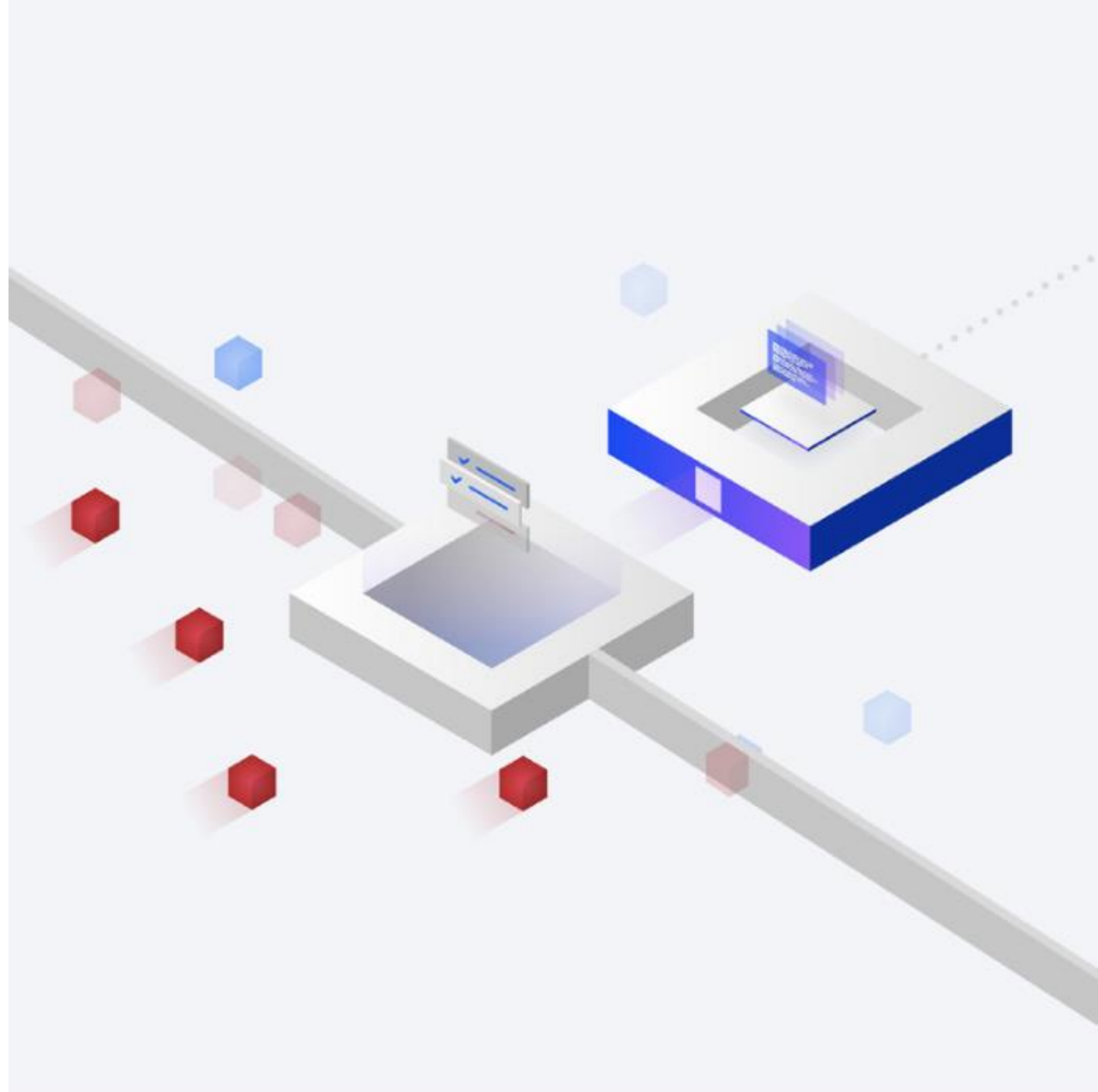
# Demo



# IBM Storage Defender

Why it Matters ...

A Real Customer Example










**It's not about backup ...**

**it's all about restore!**



# Real Customer Challenge:








*Recovery was far too slow*

Scenario	Scope of VMs	Time to Recover Today
 Deleted or Corrupted File	1	Variable based on file-count
 Single VM Corruption	1	2 hours
 Storage Volume Corruption	30-50	3 hours
 Storage Array Corruption	300-1,200	8 hours
 Application Upgrade Rollback	1-50	30 minutes
 OS Patching Goes Wrong	300-1,000	5 Days
 Large-Scale Malware Attack	1,000-16,000	4 Weeks

\*Note: Customer-provided

# Customer's Goal:

*Find solution to speed time of recovery*

Scenario	Scope of VMs	Time to Recover Today	Time to Recover Goal
 Deleted or Corrupted File	1	Variable based on file-count	Variable based on file-count
 Single VM Corruption	1	2 hours	<10 minutes
 Storage Volume Corruption	30-50	3 hours	<10 minutes
 Storage Array Corruption	300-1,200	8 hours	8 hours
 Application Upgrade Rollback	1-50	30 minutes	<10 minutes
 OS Patching Goes Wrong	300-1,000	5 Days	< 1 hour
 Large-Scale Malware Attack	1,000-16,000	4 Weeks	< 24 hours








\*Note: Customer-provided

Customer's Goal



# Actual Results:

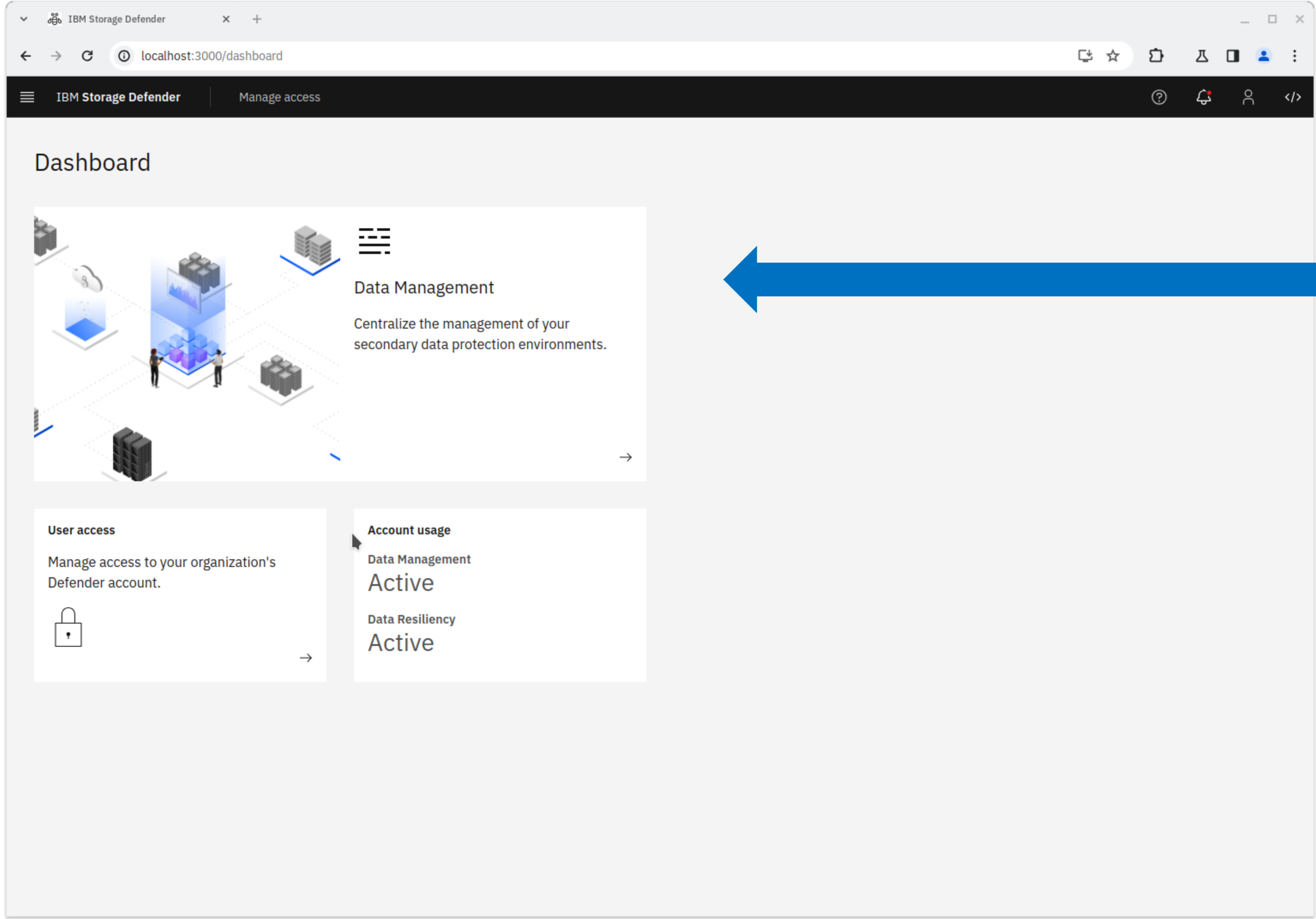
*Recovery times drastically improved*

Scenario	Scope of VMs	Time to Recover Today	Time to Recover Goal	POC Results
 Deleted or Corrupted File	1	<b>Variable</b> based on file-count	<b>Variable</b> based on file-count	<b>&lt; 1 minute</b>
 Single VM Corruption	1	<b>2 hours</b>	<b>&lt;10 minutes</b>	<b>&lt; 1 minute</b>
 Storage Volume Corruption	30-50	<b>3 hours</b>	<b>&lt;10 minutes</b>	<b>&lt; 3 minutes</b>
 Storage Array Corruption	300-1,200	<b>8 hours</b>	<b>8 hours</b>	<b>39 minutes</b>
 Application Upgrade Rollback	1-50	<b>30 minutes</b>	<b>&lt;10 minutes</b>	<b>&lt; 3 minutes</b>
 OS Patching Goes Wrong	300-1,000	<b>5 Days</b>	<b>&lt; 1 hour</b>	<b>&lt;7 minutes</b>
 Large-Scale Malware Attack	1,000-16,000	<b>4 Weeks</b>	<b>&lt; 24 hours</b>	<b>47 Minutes</b> Back on primary storage = 4 hours

Far exceeded customer's requirements!



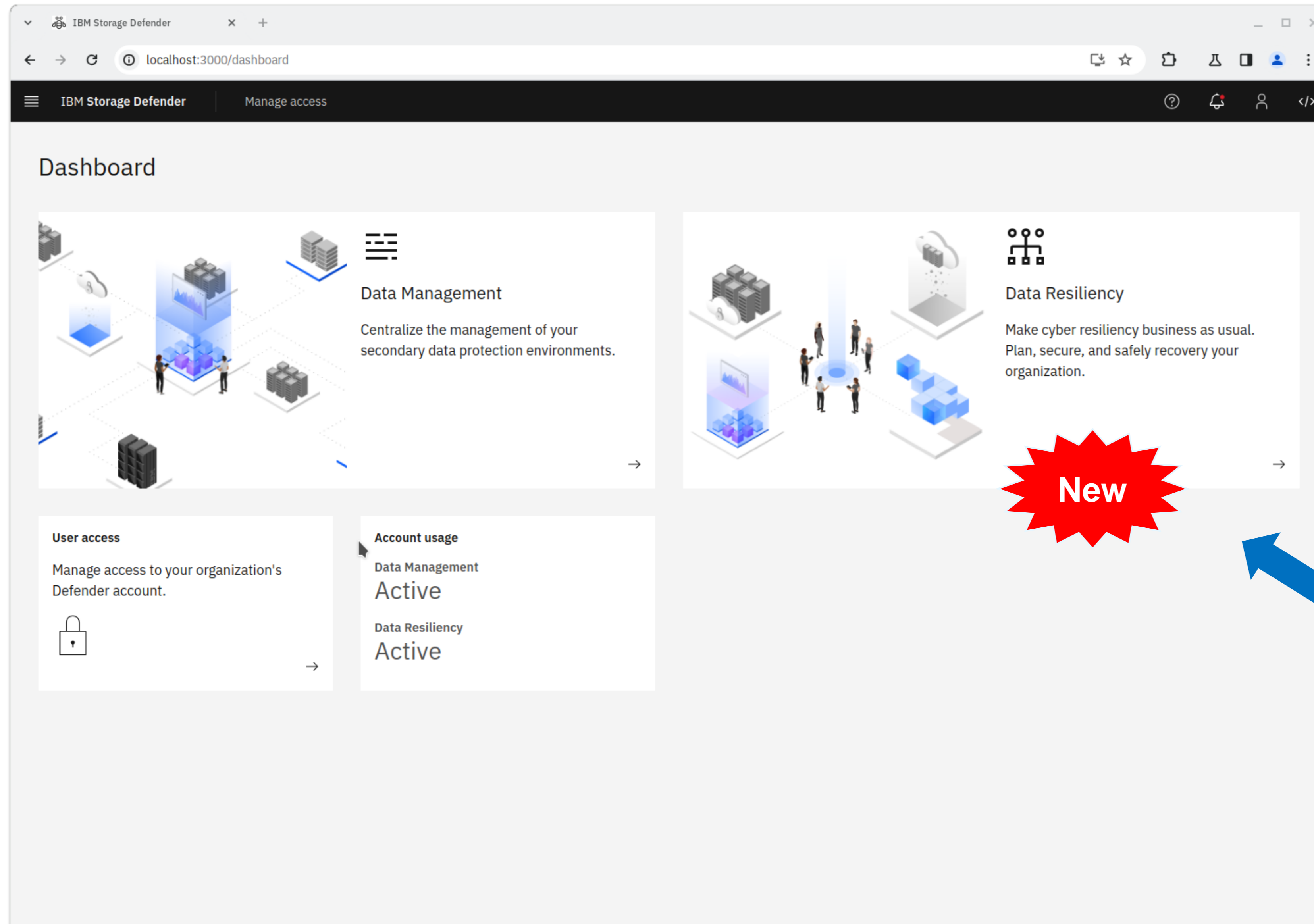
# IBM Storage Defender – Web Portal



Data Management Service (DMS)



# IBM Storage Defender – Web Portal



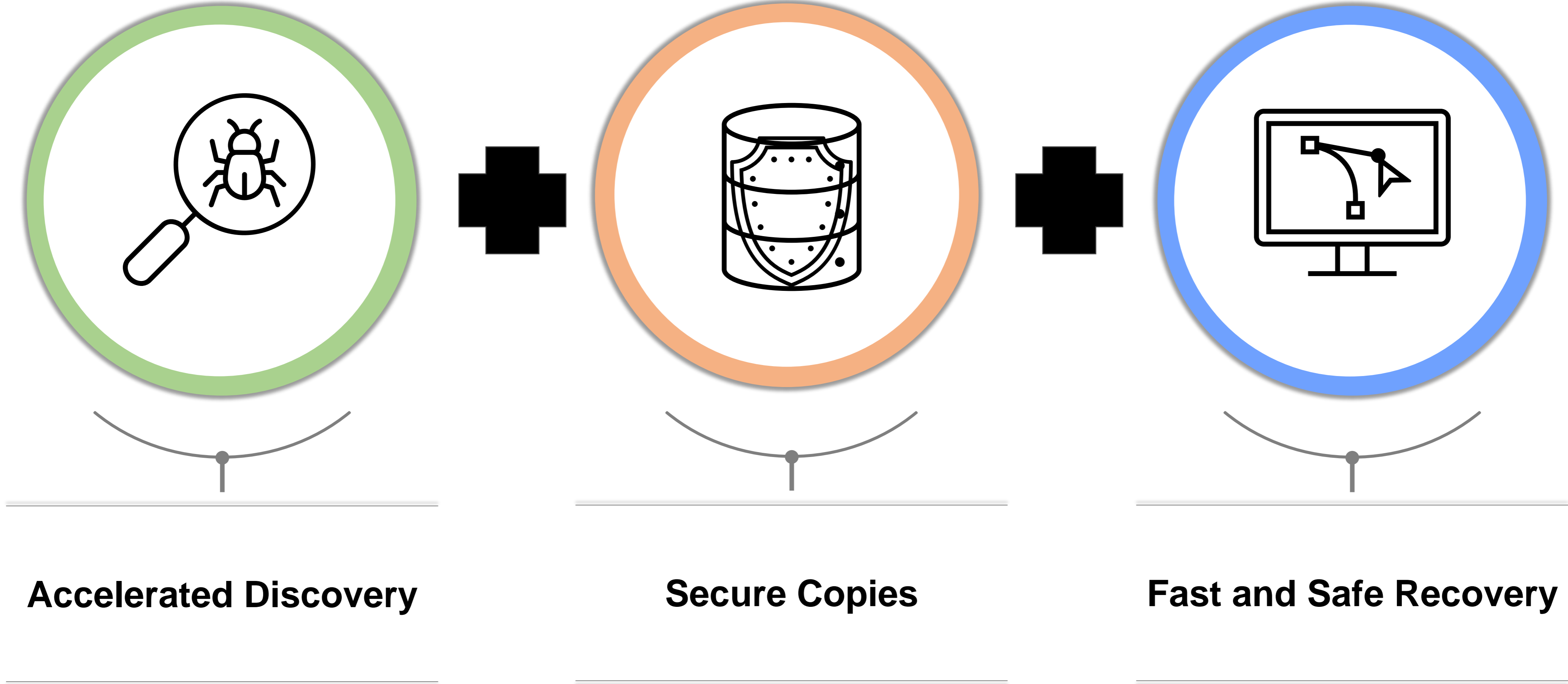
Data  
Management  
Service  
(DMS)

Data  
Resilience  
Service  
(DRS)

Coming next week!



# IBM Storage Defender – Summary



Bringing you an end-to-end data resilience solution

# Am I prepared?

- What do you have in place to **prevent** attacks?
  - Are you **encrypting** your data?
  - Are your snapshots and backups **immutable**?
  - Do you have an **air gapped** copy of your data?
- How do you **detect** attacks against your data?
  - Are you **scanning** your snapshots and backups?
  - Do you conduct regular **recovery testing**?
- Have you conducted a **cyber recovery test** of your key business applications?
- How long would it take you to recover 100 VMs? How about 1000 VMs?
- How long would it take to recover a large database?

## Accelerate with ATG Technical Webinar Series - Survey

---

Please take a moment to share your feedback with our team!

You can access this 6-question survey via [Menti.com](https://www.menti.com) with code 2243 3599 or

Direct link <https://www.menti.com/albneqj15g57>

Or

QR Code





## Accelerate with ATG: What is IBM Storage Defender?

---

**Thank you!**