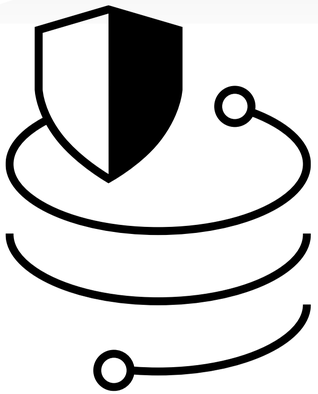
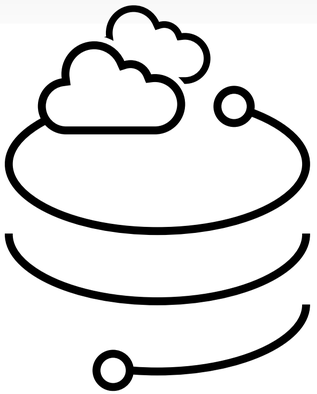
IBM Storage Portfolio Update
Storage for Data Resiliency & Data Efficiency
May 21, 2024

Fabian Michel
Senior IBM Power & Storage Technical Specialist Belux
fabian_michel@be.ibm.com

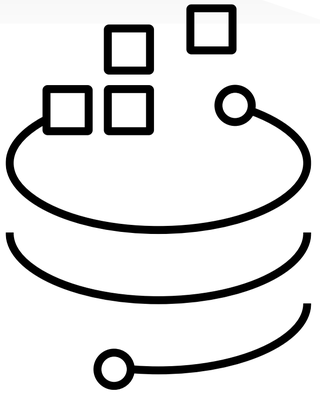
IBM Storage



Storage for
Data Resilience



Storage for
Hybrid Cloud



Storage for
Data and AI

Storage for Data Resilience

FlashSystem 9500

FlashSystem 7300

FlashSystem 5200

FlashSystem 5045

FlashSystem 5015

FlashSystem 9500R

Storage Insights

Storage Control

SAN Volume Controller

DS8900F

TS7700

Storage for Hybrid Cloud

Storage Fusion

Fusion HCI

Storage for Data and AI

Storage Scale

Cloud Object Storage

Storage Scale System

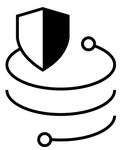
Cloud Object Storage

Storage Virtualize

SAN Switches

IBM Tape / Libraries

Storage Discover



IBM Storage Defender

Storage Archive

Introducing IBM Storage FlashSystem

Common software platform for hybrid-cloud integrations and automation

IBM Storage Insights

IBM Storage Virtualize

Fleet-wide monitoring, analytics and AI assistance

AI-enabled computational storage for efficient data processing and **ransomware threat detection**

Scalable systems for every capacity and performance point

Efficiency

Drive down data storage costs in the Datacenter

Data Resilience

Prevent, discover and recover from Cyber attacks

Cloud Ops

Simple management and consumption

IBM FlashSystem and SVC Family 2024

IBM FlashSystems FAQ

New May 2024

FlashSystem 5300

FlashSystem 5015 and 5045

FlashSystem 7300

FlashSystem 9500 and 9500R

SVC SV3

Hybrid Cloud

Spectrum Virtualize for Public Cloud

Microsoft Azure

aws

IBM Cloud

IBM **Spectrum Virtualize** *Storage function, scalability, interoperability, cloud integration and automation*

IBM **Storage Insights** Anomaly detection, fabric monitoring, full stack visibility, predictive support

IBM NVMe Enterprise Storage

One Family Simplicity

With consistent data services

FlashSystem 9500

4U 48 drives, 4.5PBe*

1.6M** IOPS, 100GB/s

Expert Care Advanced or Premium

x2

FlashSystem 7300

2U 24 drives, 2.2PBe

580k** IOPS, 45GB/s

Expert Care Basic, Advanced or Premium

x2

FlashSystem 5300

1U 12 drives, 1PBe

360k** IOPS, 28GB/s

Basic, Advanced

Choose your capacity

Choose your performance

Choose your support

** IOPS shows are for 16k 70/30/50 workloads and are shown for comparison purposes


IBM
FlashSystem
5300

FlashSystem 5300 concentrates high-capacity and data resilience in a physically small package

~1.45x IOPS

1.3x Gb/s

Front

Rear

1 rack unit

- Holds up to **1.3PB of raw effective capacity**.
- Supports up to **16-32Gb/s or 8-64Gb/s** Fibre Channel ports.
- Comes with **built-in 10/25Gb/s** Ethernet ports
- Includes SW-based **ransomware threat detection** (RTD) and typically also has HW-based RTD

Memory Options

Name	Per Node	Per Enclosure	DIMMs Per Node
Base 1	32G	64G	1x32G
Base 2	**128G**	**256G**	**2x64G**
Option 1	256G	512G	4x64G

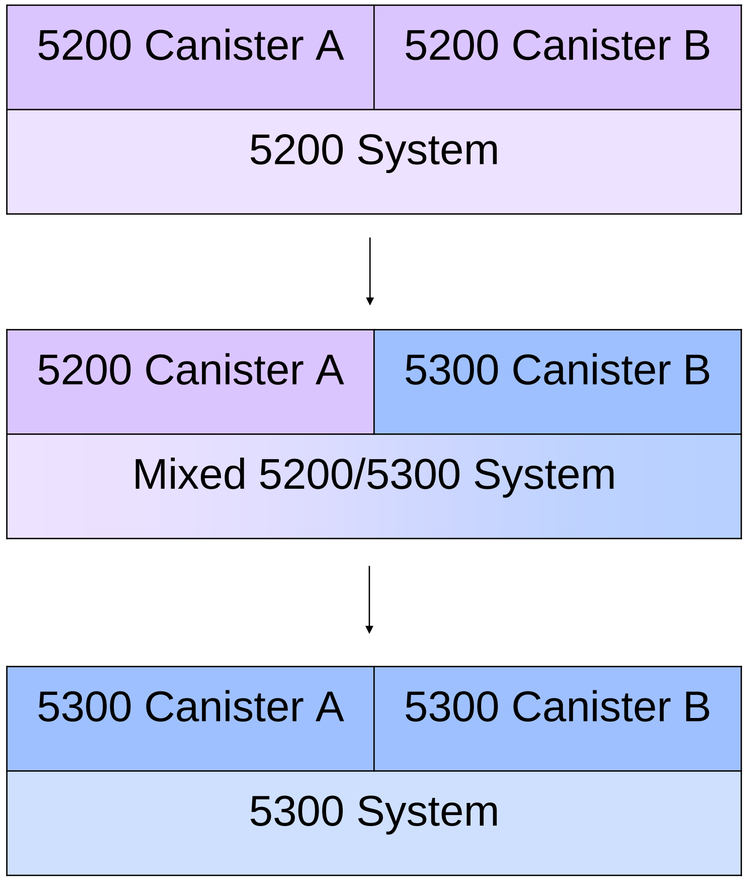
Support for these features requires at least 128G (Base 2) of memory per node:

- Policy-based replication and PB-HA
- Data de-duplication
- Embedded VASA provider and VVols replication
- Storage Insights integration

Development recommend 128G (Base 2) for deployments that require advanced IO Features

Non-disruptive Hardware Upgrade

- 5200 clusters can be upgraded to use 5300 node canisters with no disruption to host IO
- No performance impact to using 5200 midplane at PCIe gen4
- All drives supported on 5200 remain supported on 5300
- Only the 10Gb Ethernet HBA card is supported on the 5300. On board ports run 10/25Gb



Software Highlights

Key Features
– Ransomware Threat Detection with FCM 4.1 and Safeguarded Copy – Embedded VASA provider – Secure Boot/Measured Boot and Secure Firmware – Policy Based Replication and HA

Improved Features
– Snapshot increased to 10PiB of target capacity (compared to 4PiB on the 5200) – More Ethernet I/O Ports – Management Simplification – Performance

Feature Guide: Secure Boot

- 5300 is our most secure product to date
- All secure boot features from the 9500 are included
- Additional security is provided by enabling secure boot capabilities of the PCIe switch

BIOS
Password protected to prevent tampering or force booting from untrusted devices
Checks bootloader signature and only boots if signed with our private key

Boot Drive
All filesystems with execute permissions are encrypted to prevent tampering

TPM
Measures boot process and allows decryption of the boot device only if BIOS, bootloader and kernel signatures are trusted

PCIe Switch (New)
Verifies firmware signatures and only boots if they match key provided at manufacture time

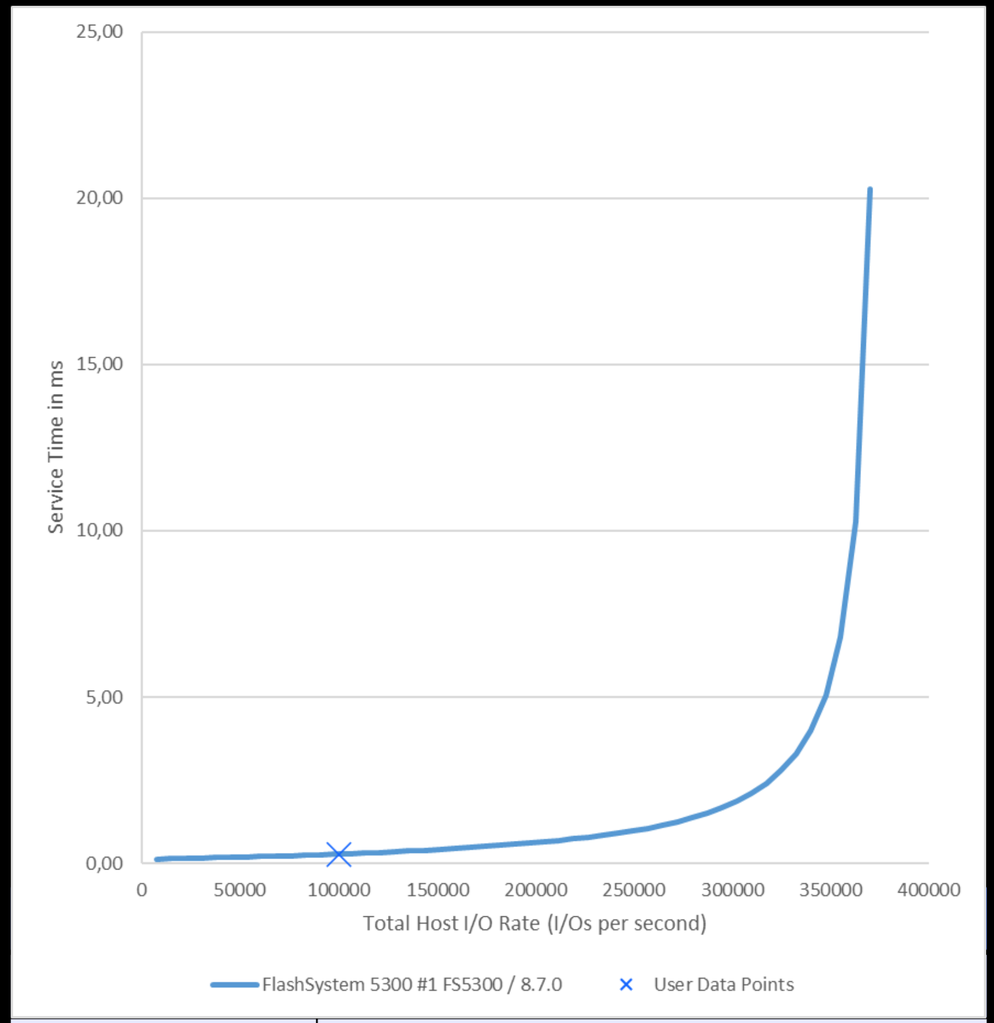
1x **FlashSystem 5300**
Equipped with **12x 38.4 TB FCM4**
In distributed DRAID6 (9+P+Q)

0,340 kW
1 EIA unit

1 PBe with **3:1** comp.
or
682 TBe with **2:1**
or
341 TB w/o compr.

More I/Os & TB
per kWh or € spent !

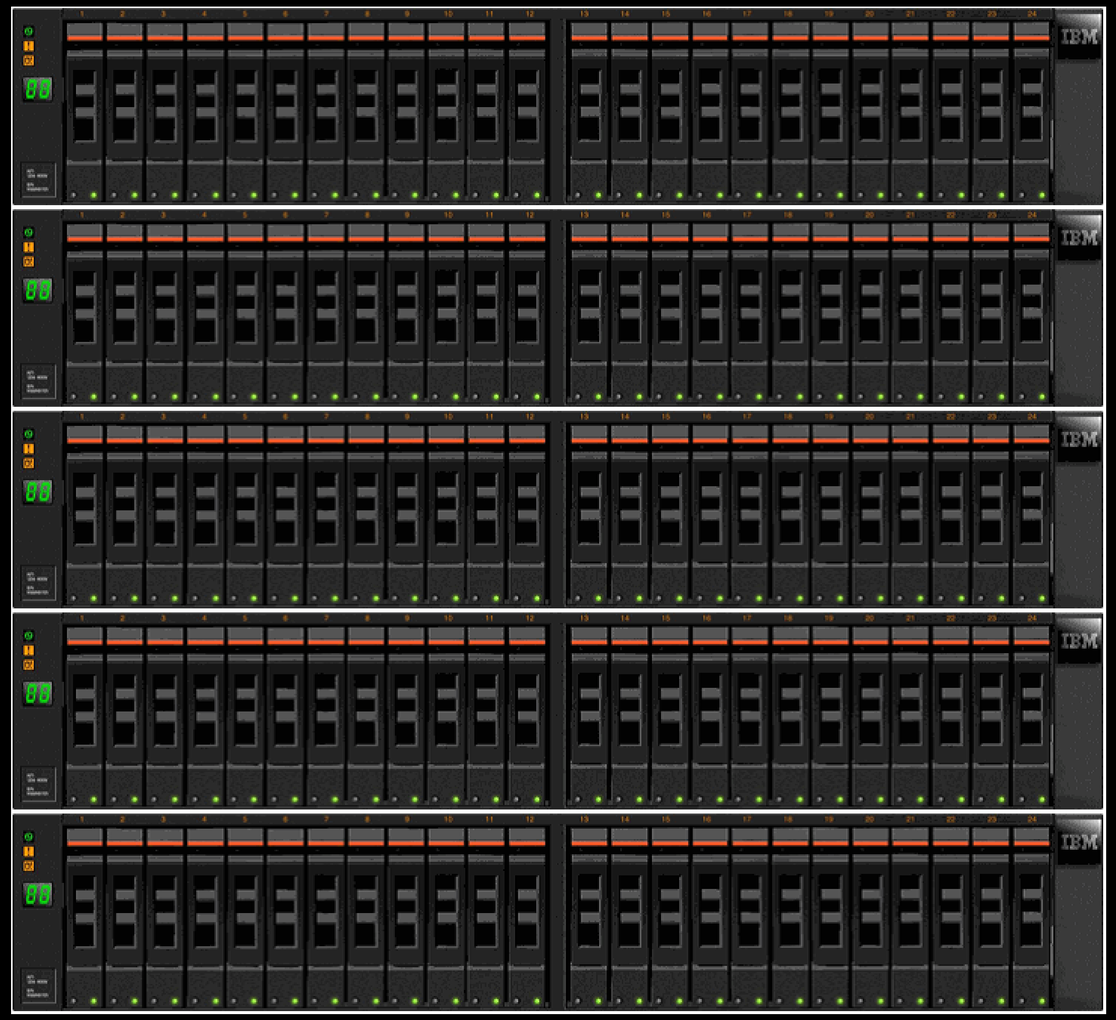
Up to **300 k I/Os**
(250 k < 1 ms latency)
@ 70/30 R/W
50% cache hit
16 KB block



Compression	Inline Native Hardware Compression Algorithm
4.8 TB physical **(S)**	**22 TB Effective (4.5:1)**
9.6 TB physical **(M)**	**29 TB Effective (3:1)**
19.2 TB physical **(L)**	**58 TB Effective (3:1)**
38.4 TB physical **(XL)**	**115 TB Effective (3:1)**

Energy savings estimates (Belgian Client Example with FS5200)

Energy savings : 70%
Physical footprint savings : 90%



Price of kWh in Belgium (€) (1)	***0,30 €***	**Watt**	**BTU/Hr**	**kWh/year**	**Energy savings**
Direct savings (Energy) :		***2010***		17.607,60	5.282,28 €
Indirect savings (Cooling) :			***6.072***	15.588,66	4.676,60 €
Total yearly savings (Energy & Cooling) :					**9.958,88 €**
Total savings for 5 years :					**49.794,39 €**

Sources:

(1) Indicative, please use your cost per kWh

Watts to kilowatt-hour calculation formula

The energy E in kilowatt-hour (kWh) is equal to the power P in watts (W), times the time period t in hours (hr) divided by 1000:

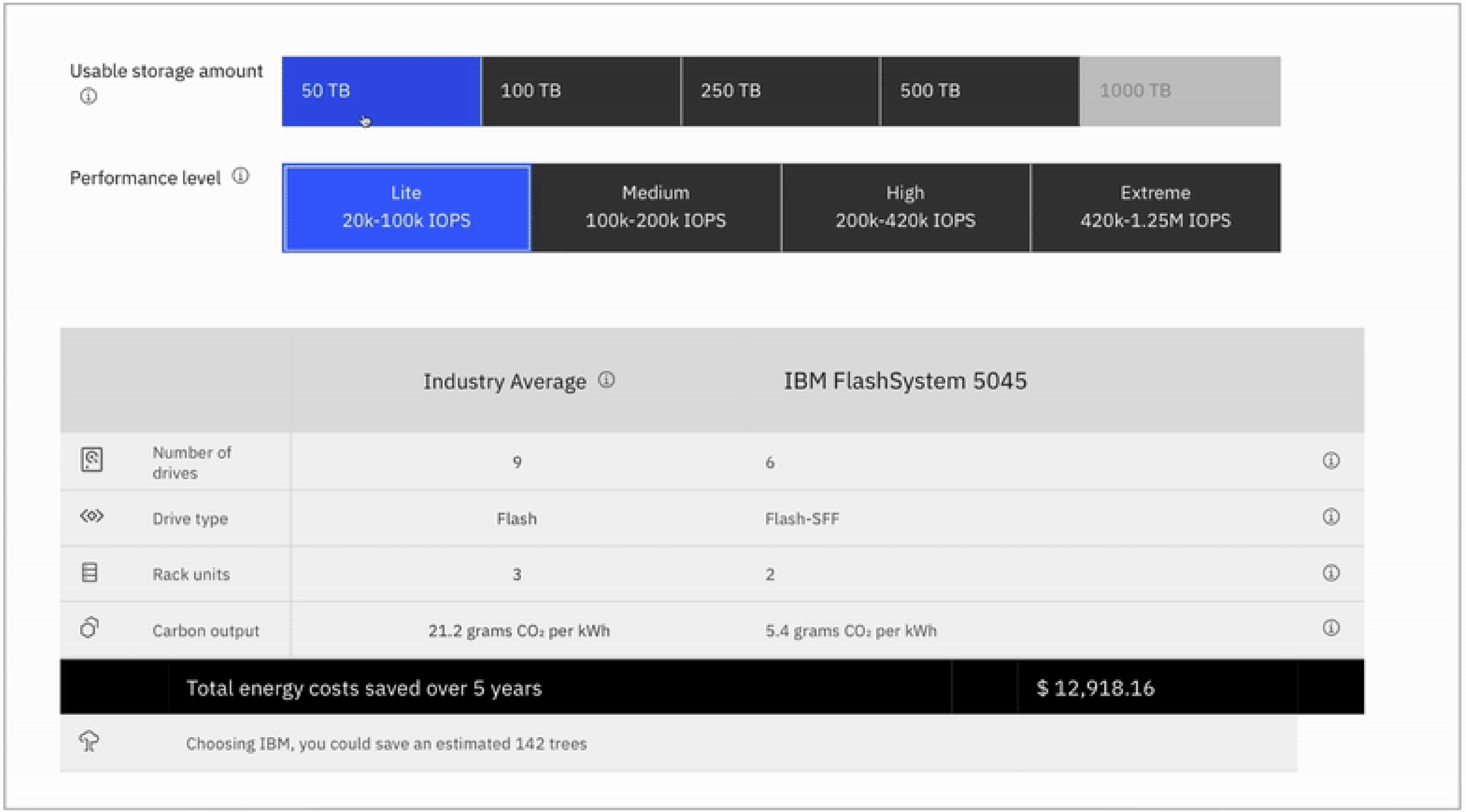
$$E_{(\mathrm{kWh})} = P_{(\mathrm{W})} \times t_{(\mathrm{hr})} / 1000$$

How to convert BTU/hr to watts

$$1\ \mathrm{BTU/hr} = 0.29307107\ \mathrm{W}$$

So the power *P* in watts (W) is equal to the power *P* in BTUs per hour (BTU/hr) times 0.29307107 and is equal to the power *P* in BTUs per hour (BTU/hr) divided by 3.412141633:

€€€



[Data Storage Sustainability - Economic Impact Calculator]

Paradigm shift: Need for Cyber Recovery

Cyber Recovery is fundamentally different from traditional recovery

Category	Traditional Recovery	Cyber Recovery	
Nature of impact	Random e.g. natural disasters	Targeted engineered for maximum impact	Need Early Detection
Scope of impact	Local / Regional	Global can affect any connected systems	
Backup repository affected	Not typical	Possible	
Recovery point	Known	Unknown need most recent **uninfected** copy	Need Safe And Rapid Recovery
Mitigation objective	RPO/RTO	RPO/RTO + **Safe Recovery**	
Duration of impact	Hours to Days	Days to Weeks	
Relative probability of occurrence	Low	High	

Introducing IBM Safeguarded Copy

Speed recovery from cyber attacks

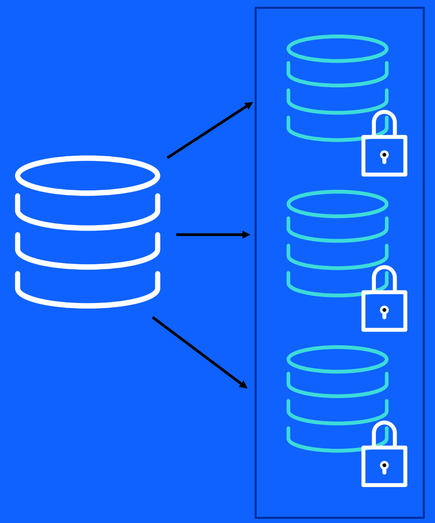
Automatic
creation of regular backup copies

Immutable
point-in-time copies of production data

Isolated
offline by design

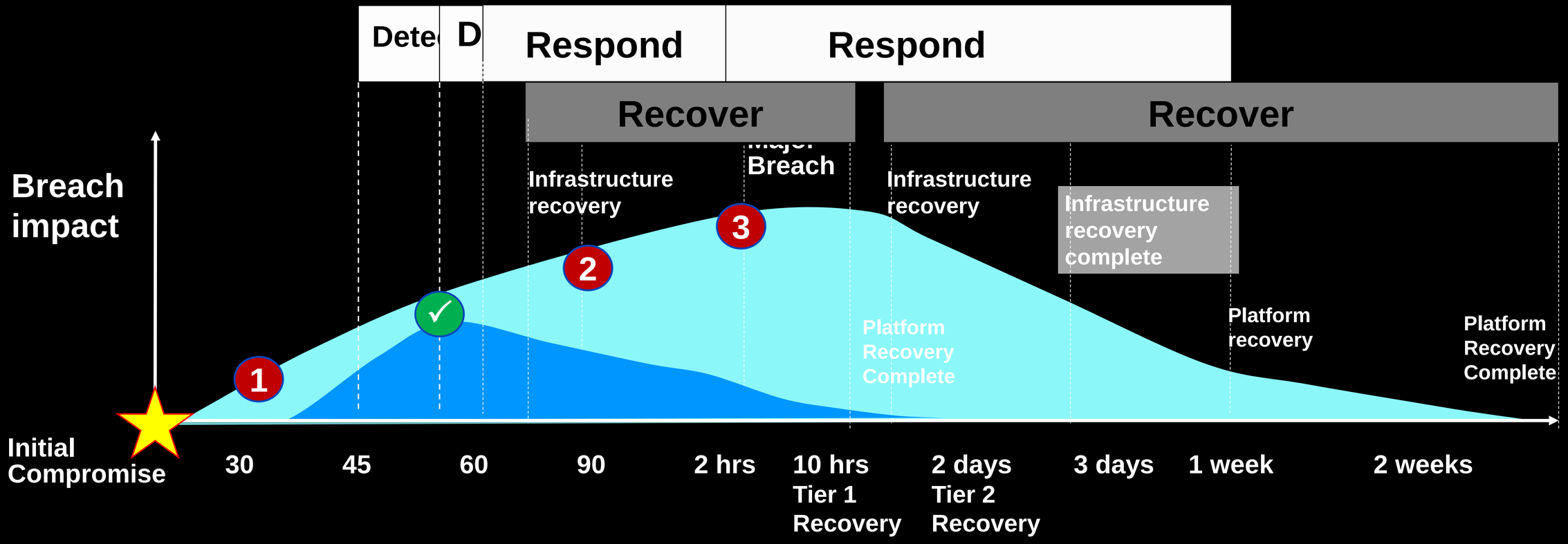
Fast
restore from copies on primary storage

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



Cyber Vault value – Detect, Respond, Recover Faster !

Cyber incident timeline



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

FlashCore Module V4

Side-by-side comparison of IBM FCM4 and Ind. Standard SSD

Unique Capabilities	IBM FCM	Ind. S. SSD
Extensive Built-in Encryption	✓	✗
Extensive Built-in Compression	✓	?
Ransomware Detection	✓	✗
Extensive Health Binning	✓	✗
Extensive Heat Segregation	✓	✗
Variable Voltage	✓	✗
Variable Stripe RAID (Intra Module RAID)	✓	✗
~70µs latency	✓	✗

[IBM FlashCore Module (FCM) product guide]

FCM4 as a Drive

FCM4 is PCIe 4.0 across all drives
(FCM3 was S/M: PCIe 3.0, L/XL: PCIe 4.0)

FCM4 is supported in

- FlashSystem 5200*
- FlashSystem 7300*
- FlashSystem 9500

* PCIe 3.0 auto negotiation

FCM4 is transparently compatible with FCM3 for existing systems

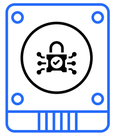
- Able to extend current FCM3-DRAIDs
- Able to run as additional pool
- Already as FCM3 field replacements

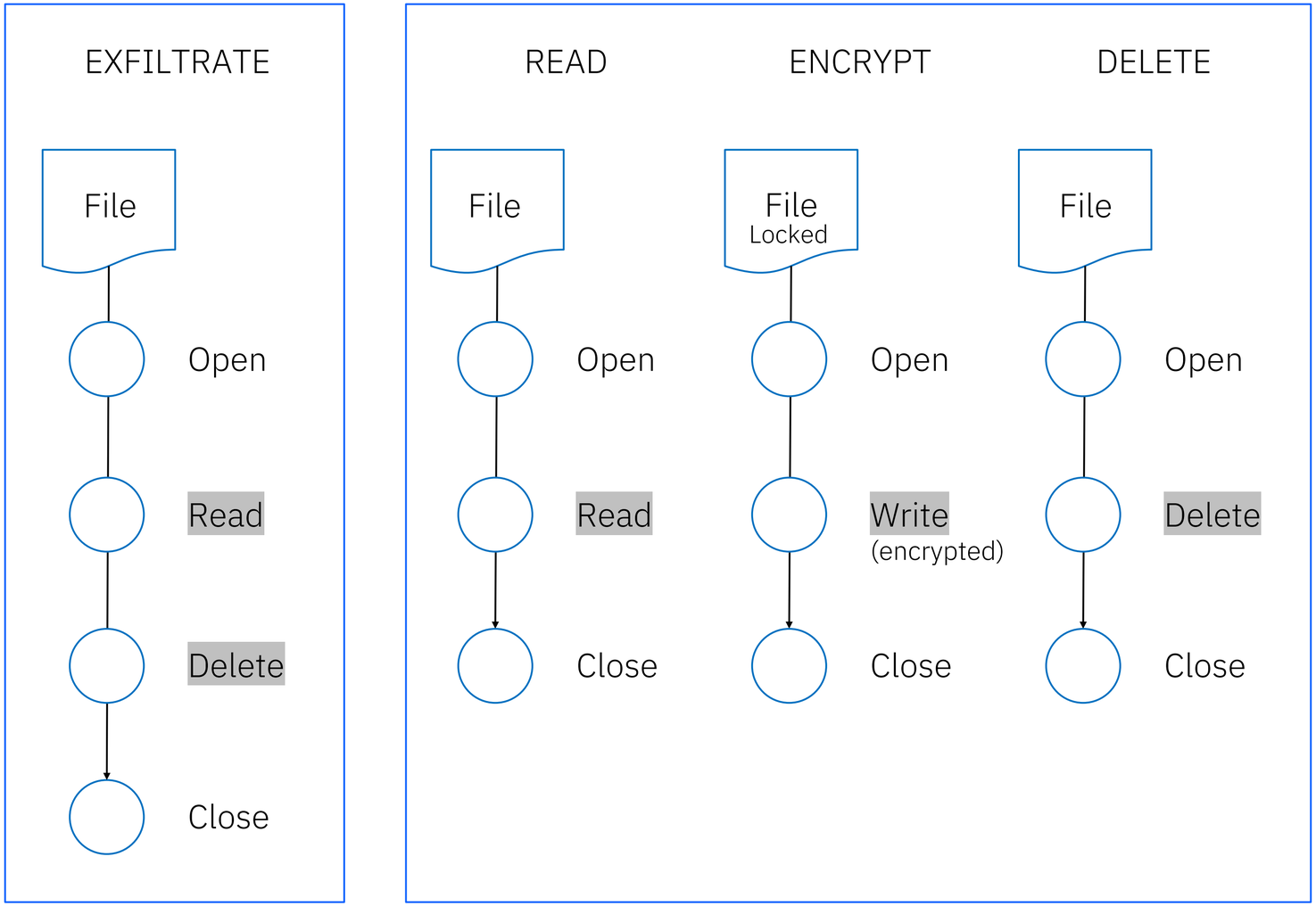
But How Do You Detect Ransomware

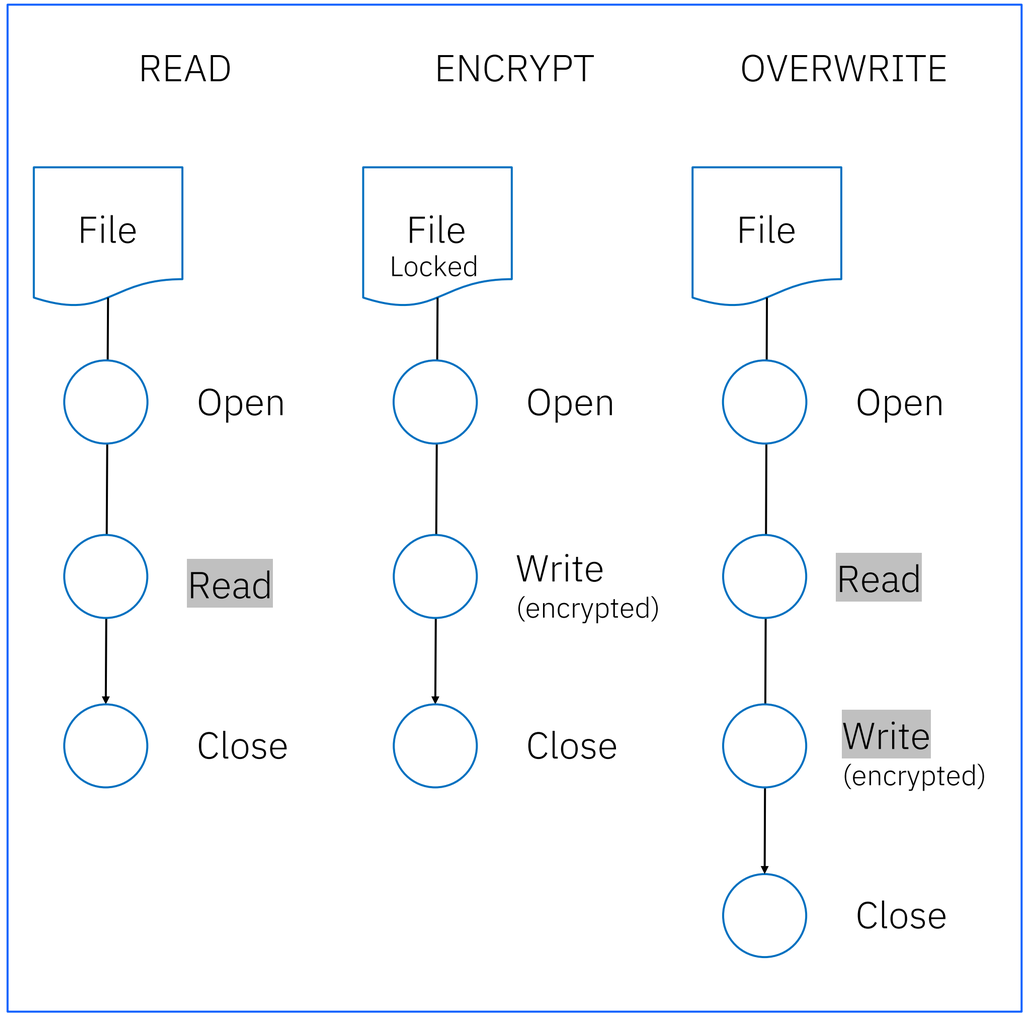
Detection By

Threat Signature	Sample Hash Comparison
Data Behavior Signals	**Block Level Monitoring for Anomalies**
Network Signals	Network-Level Monitoring for Anomalies

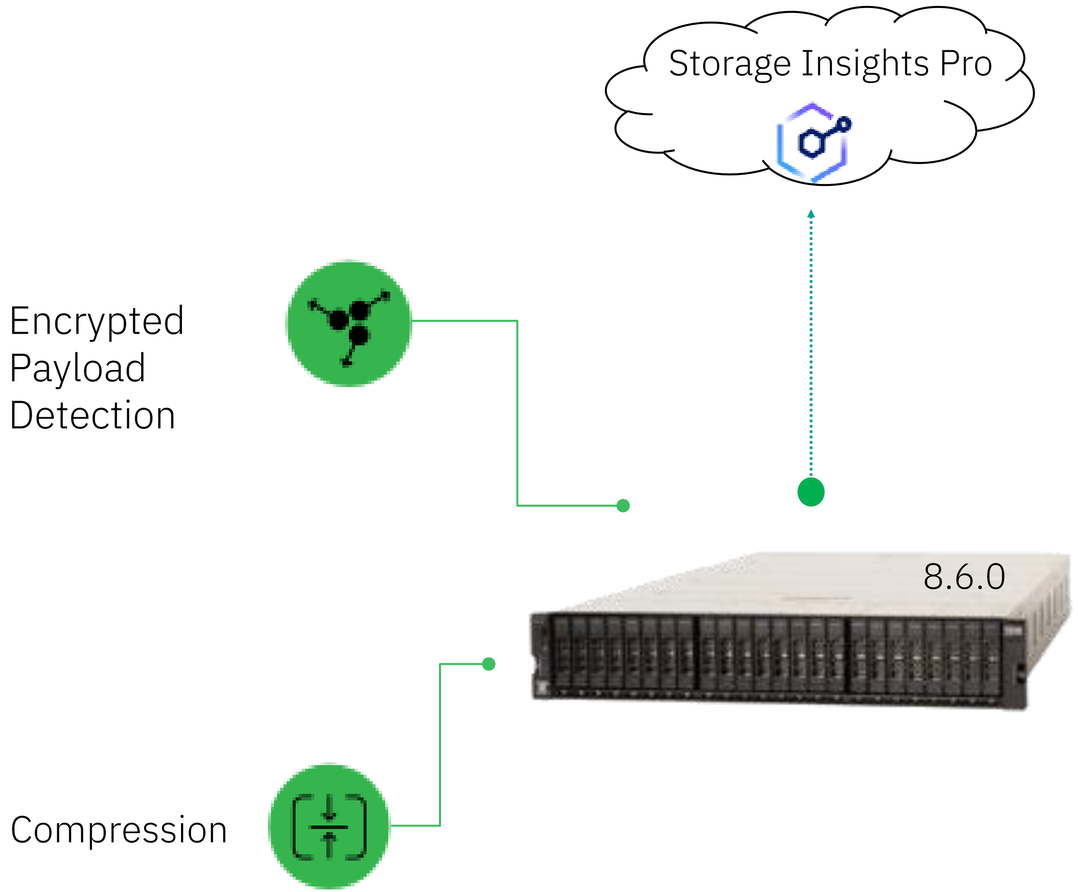
Cyber Attacks: Similar IO Access Sequences







Workload anomaly alerts in 8.6.0 & Storage Insights Pro



Using FlashSystem controller CPU will analyze **incoming write I/Os**

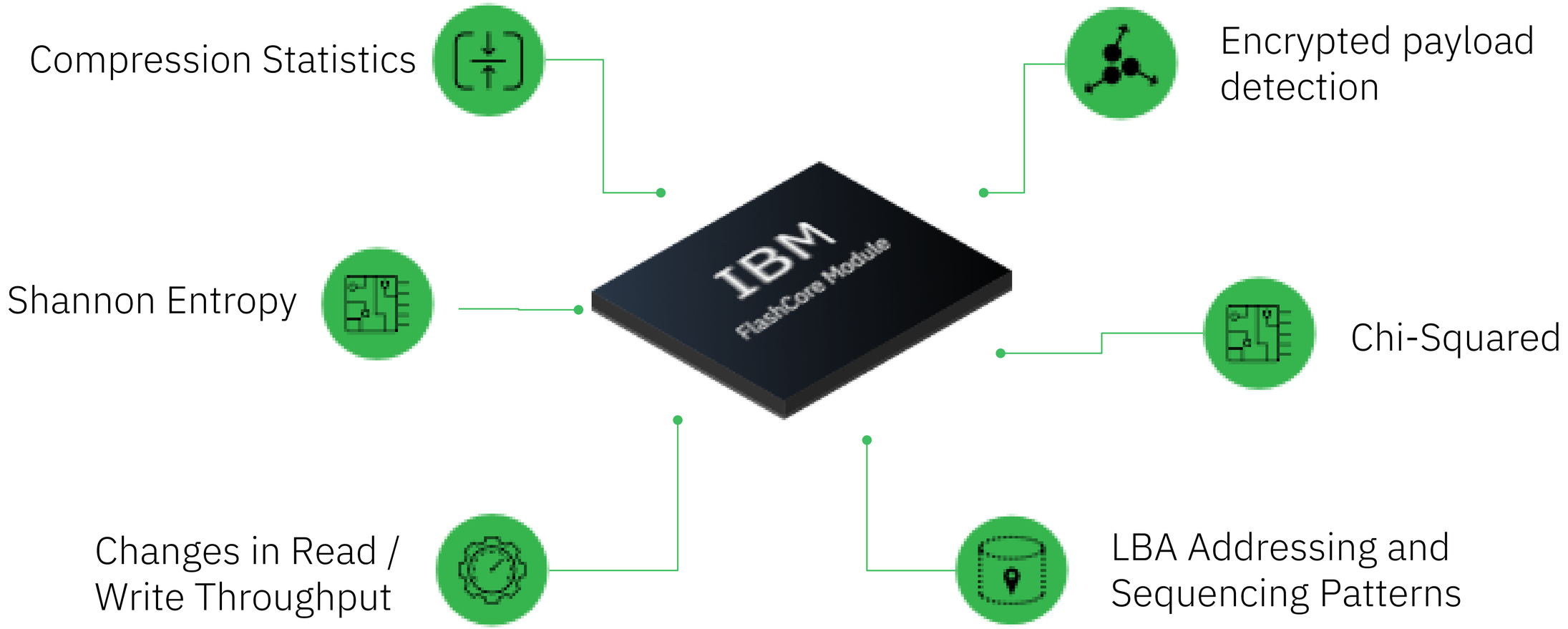
Statistics are used to detect highly random data and IO patterns to detect encrypted data written in by ransomware

Encrypted data detection is computed (byte by byte) in the write cache destage, but it is computationally intensive.

To reduce performance impacts the measurements are collected on samples of 1 in ever 100 IOs

Ransomware Threat Detection With FlashCore Module 4

30+ data statistics analyzed in detection engine



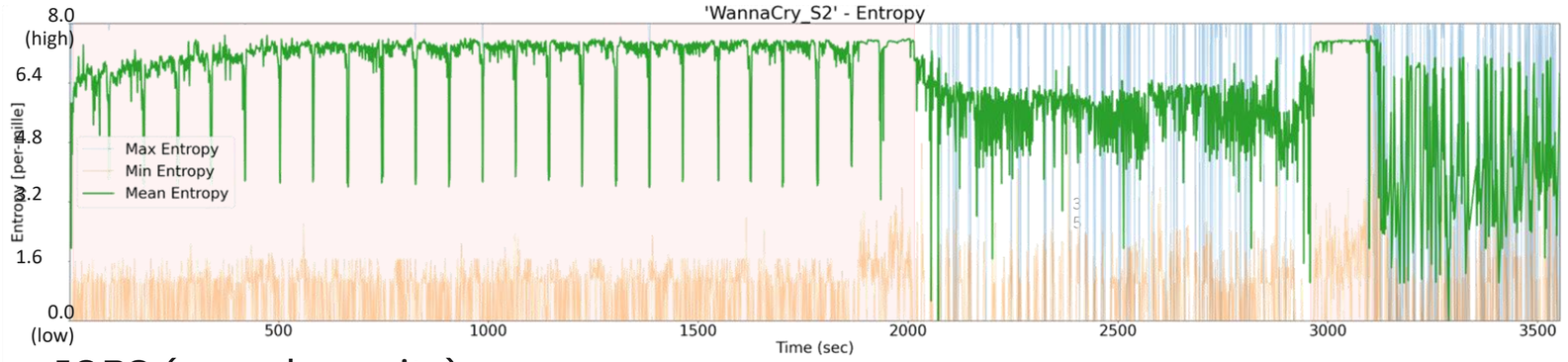
Processed on **EVERY** write with **ZERO performance impact!**

Ransomware Threat Detection – Learning Patterns

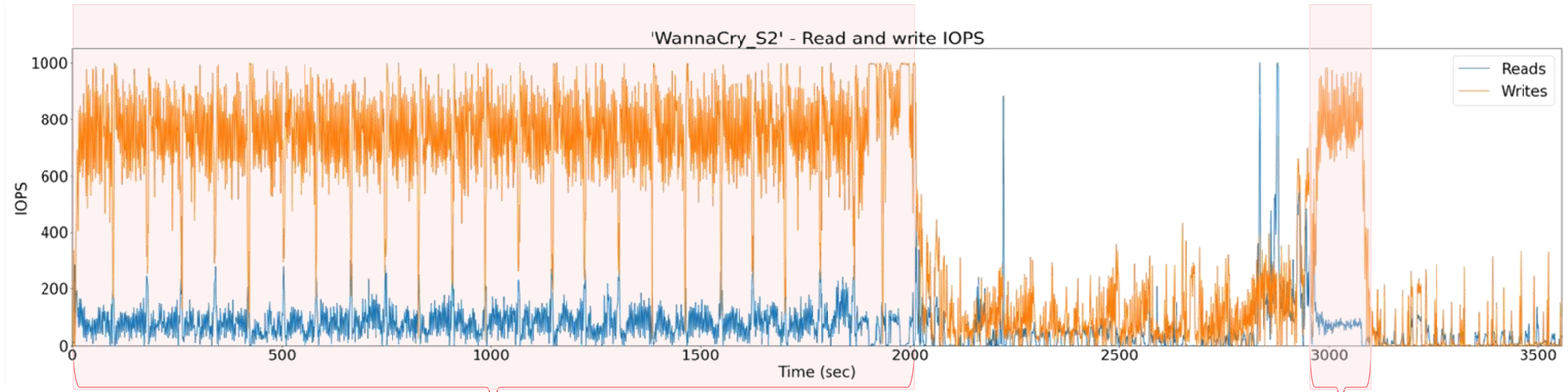
Malware such as ransomware attacks can be detected from storage IO patterns and data analysis

Example “Wannacry”:

Encrypted payload (– avg, – max, – min):

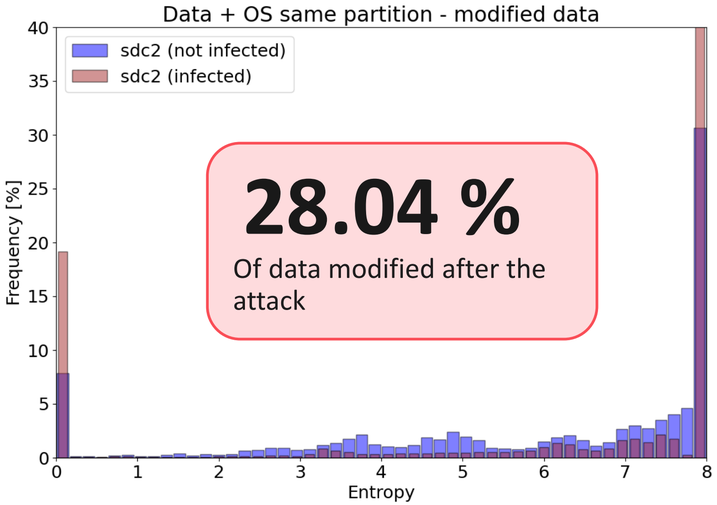


IOPS (– read, – write):



IO activity of ransomware

Payload encrypted – before and after attack:



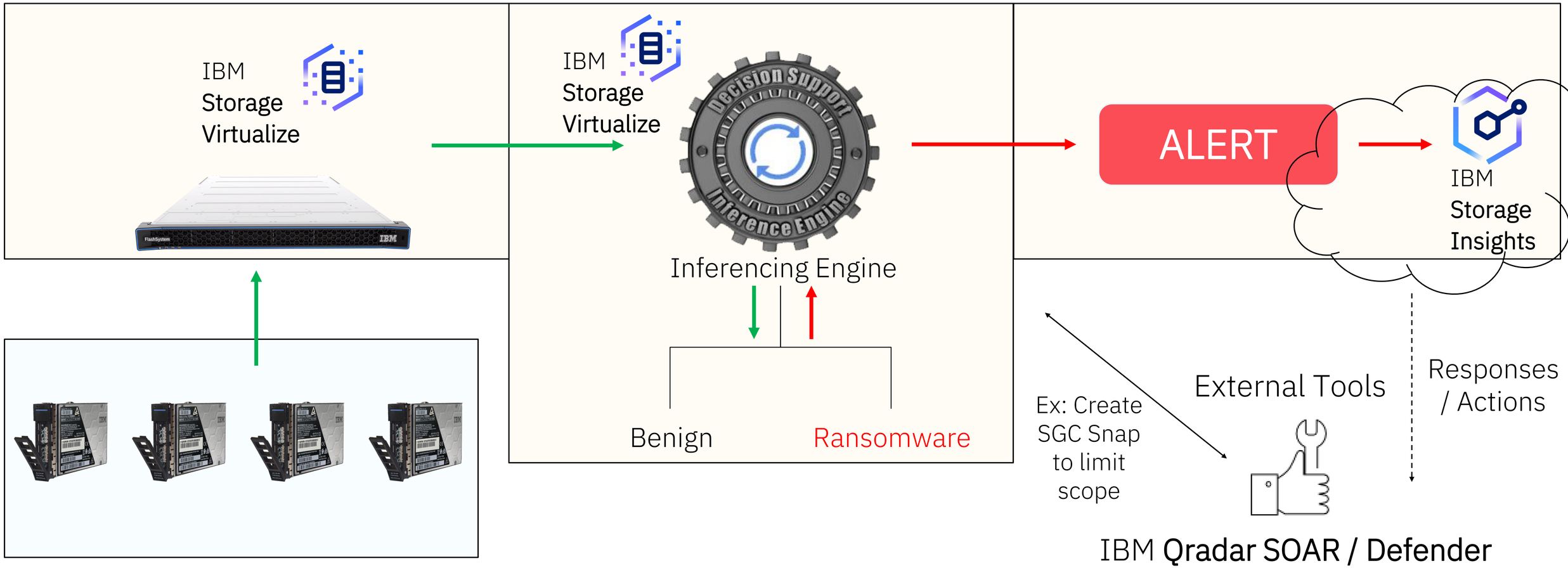
28.04 %

Of data modified after the attack

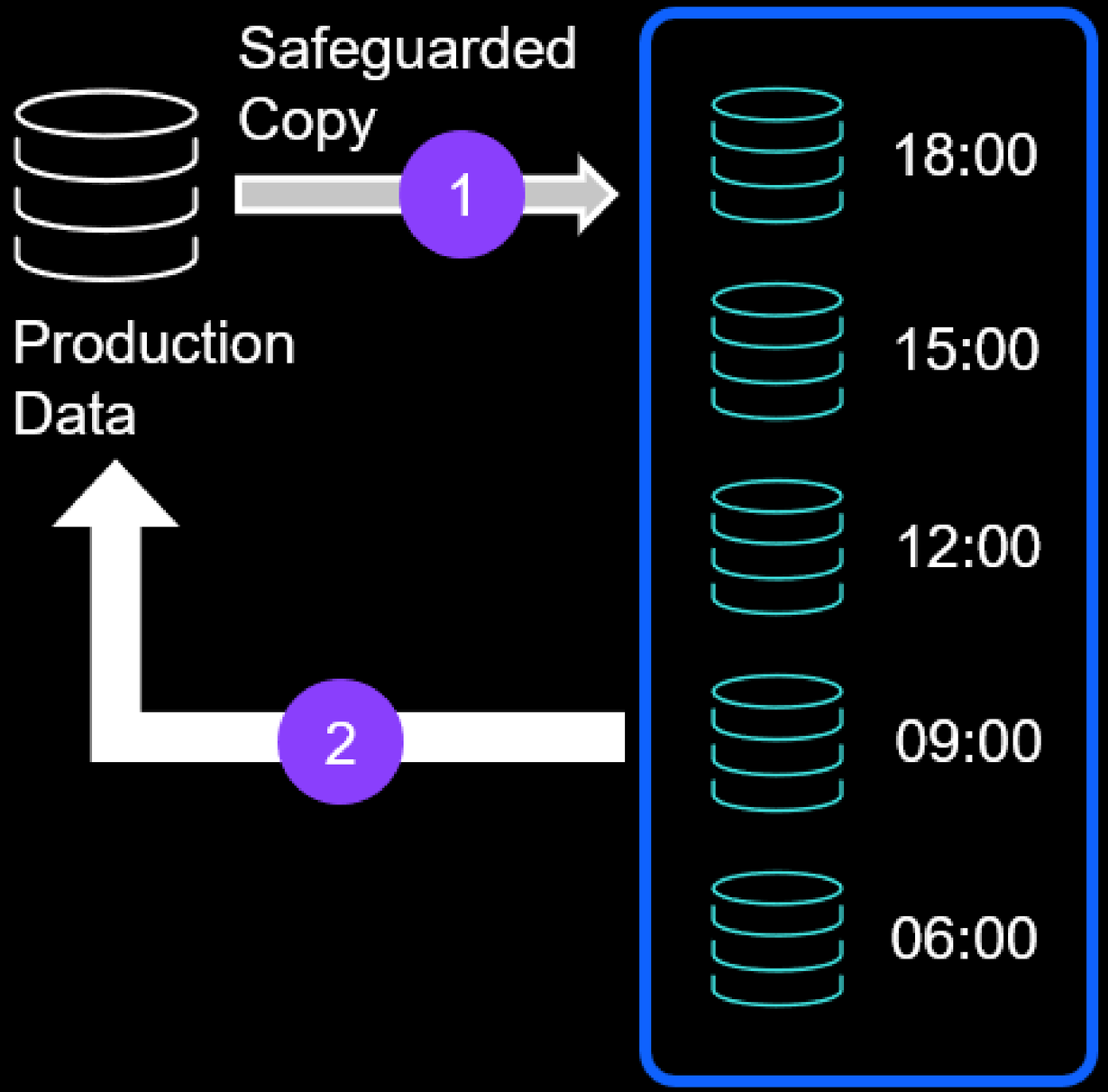
Ransomware Threat Detection with Storage Virtualize

Proven Machine Learning (ML) model trained on real-world ransomware

Non-disruptive patchable updates to keep up with new attack patterns

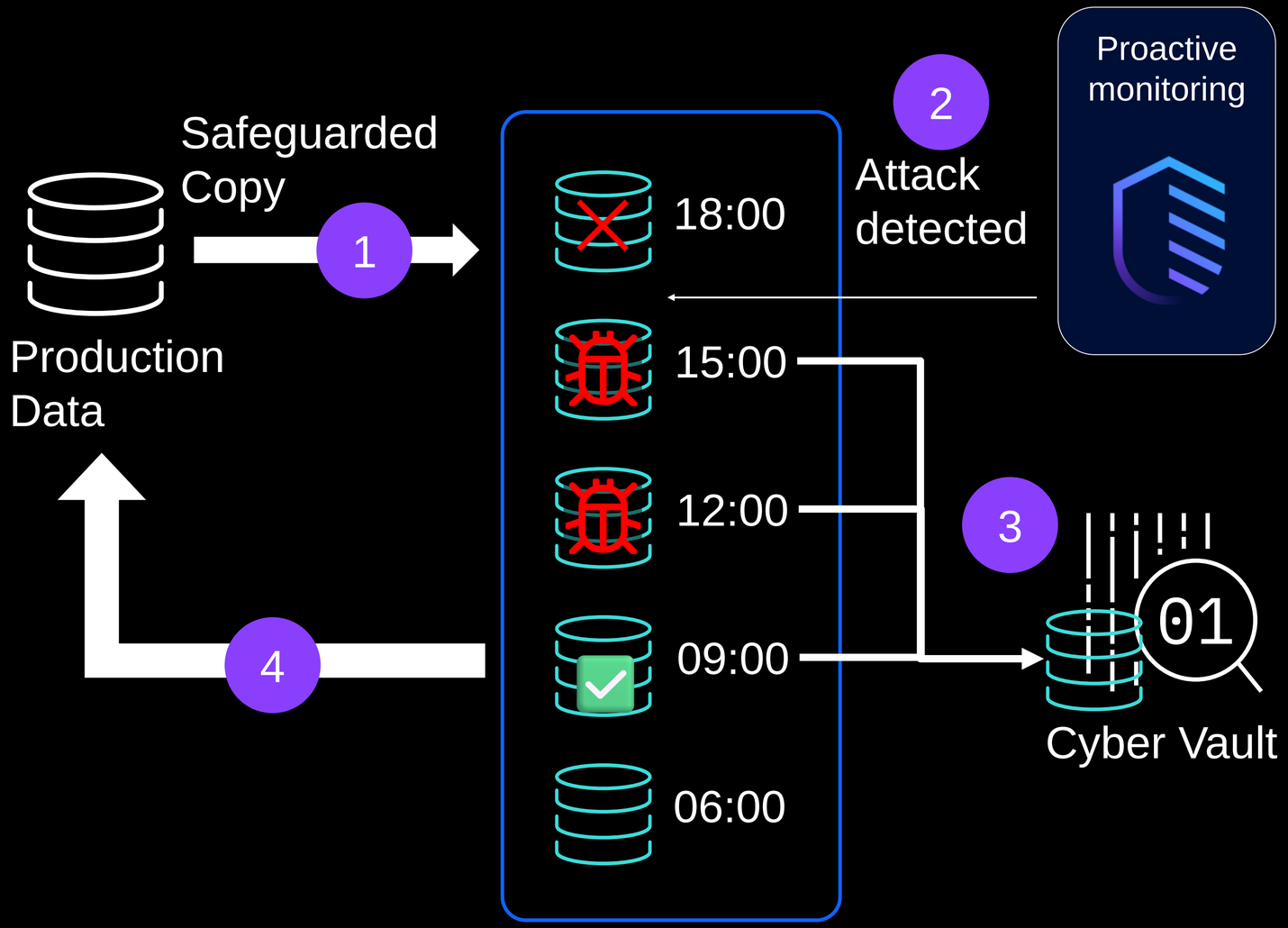


Q3 2021: IBM FlashSystem SafeGuarded Copy



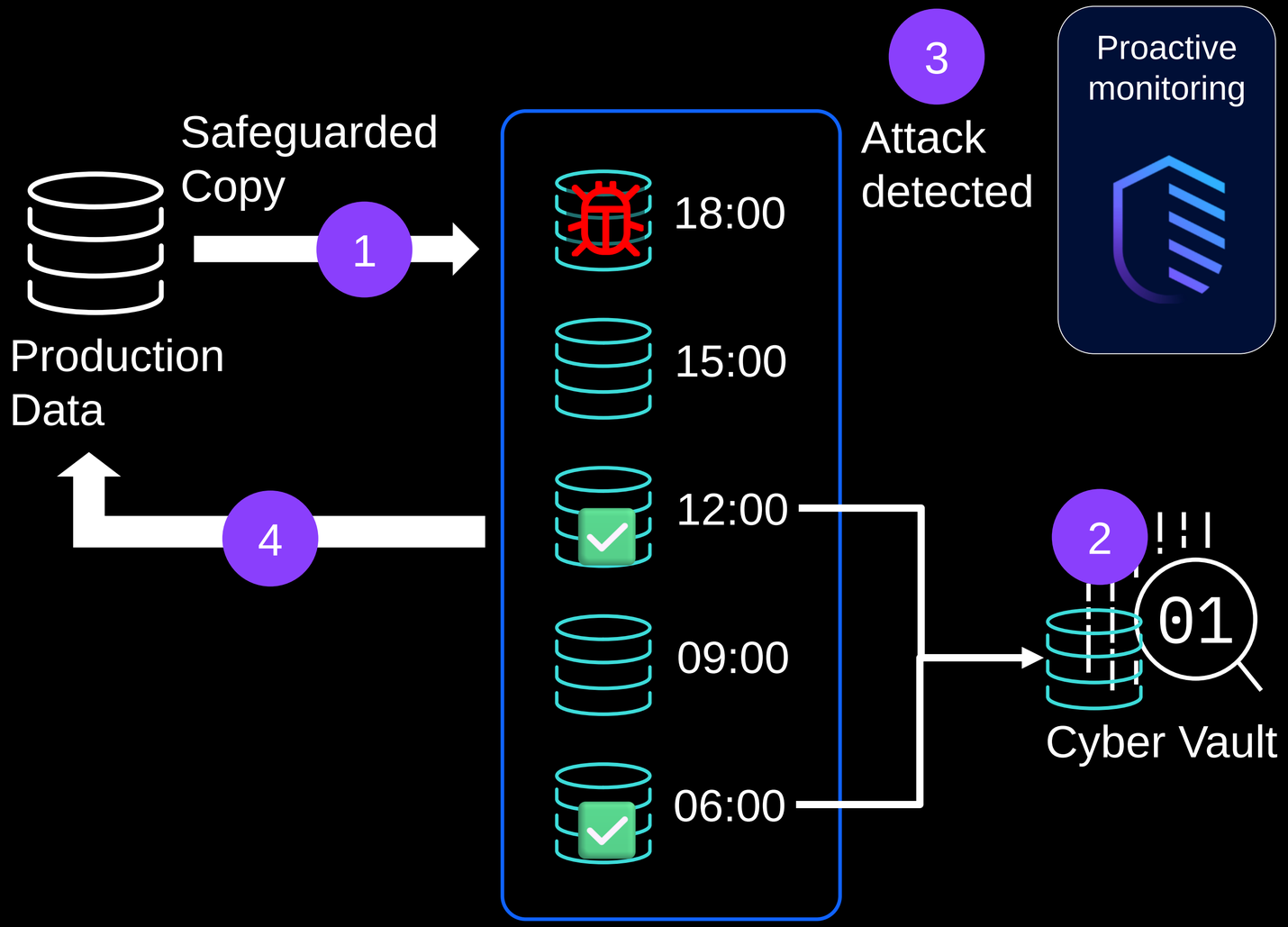
1. Safeguarded immutable copies created throughout the day
2. Ability to perform rapid restore of immutable copy when required

Cyber Vault Workflow
Test & Validate data before recovery



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

Cyber Vault Workflow
Test & Validate data copies proactively



How Cyber Vault Works

Identify problems and solutions faster, minimize recovery impacts

Production VMs

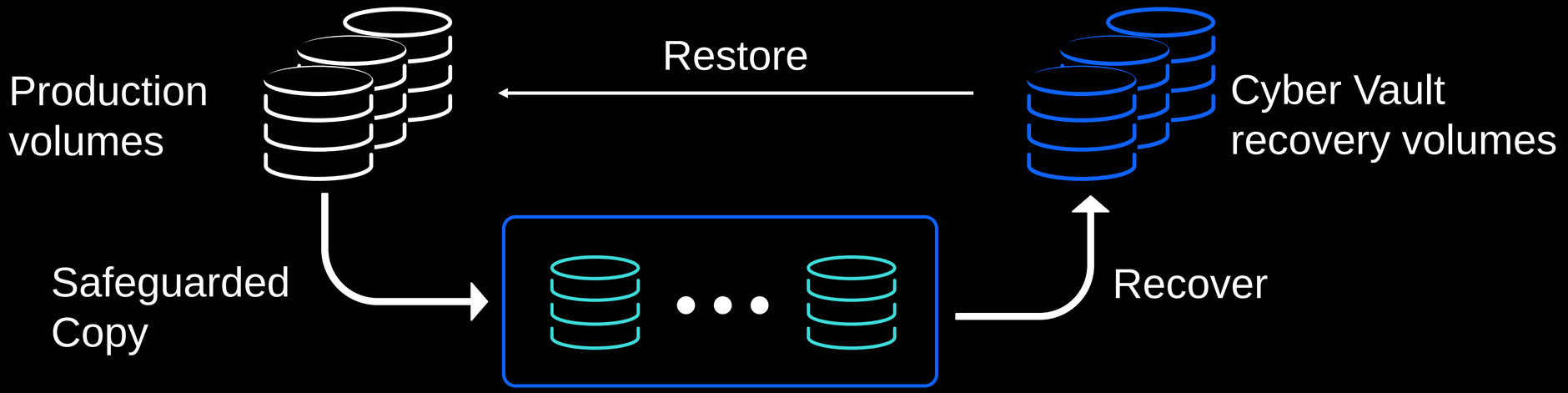
App 1 | App 2 | App 3 | App 4

Cyber Vault VMs

Data recovery and consistency monitoring | Test | Recovery Tools | Diagnostics

Cyber Vault

1. Establish analysis environment
2. Run diagnostic tools
3. Determine data validity



Cyber Resilience Assessment

The Cyber Resiliency Assessment provides a way to evaluate the current data resilience of the organization, identifies strengths and weaknesses and provides recommendations to **build an effective cyber resilience plan**

[IBM Cyber Resiliency Assessment]


Storage Cyber Resiliency & Disaster Recovery Assessment Report

IBM Security & Resilience

January 5, 2021

Overview

IBM is pleased to present [a report based on our findings from the IBM® Storage Cyber Resilience & Disaster Recovery Assessment workshop that took place with the [Customer] team on December 5th, 2019. It is understood that an effective cybersecurity resiliency program must be grounded in effective systems and processes that provide valuable insight into information and events that occur within an environment and provide the confidence for an orchestrated storage resiliency process in order to not disrupt [Customer]'s business continuity objectives. By evaluating the current cybersecurity and resiliency environment, the organization now has specific recommendations designed to help increase the value of the solution and services in its environment and meet RTO and RPO requirements.

Additionally, [Customer] will be able to help deliver faster return on investment and higher operational productivity by leveraging time-tested practices and updates to product features and resiliency functions. It will be able to help decrease errors and inconsistency through the implementation of the incremental recommendations we have provided in this document.

Executive summary

Based on the information gathered during our initial reviews within IBM during 4Q 2019 as well as the assessment workshop in Benton Harbor on December 5th, [Customer] has realized great value from its investment in cyber resilience and is generally on-par with other customers that IBM has worked with. However, there are several areas where [Customer] has exposure to risk resulting in unrecoverable data loss or corruption and where more value can be realized.

[Customer] has many IT service providers of which IBM is a significant partner. Of the many environments considered and reviewed for this assessment, we have taken an enterprise-view.

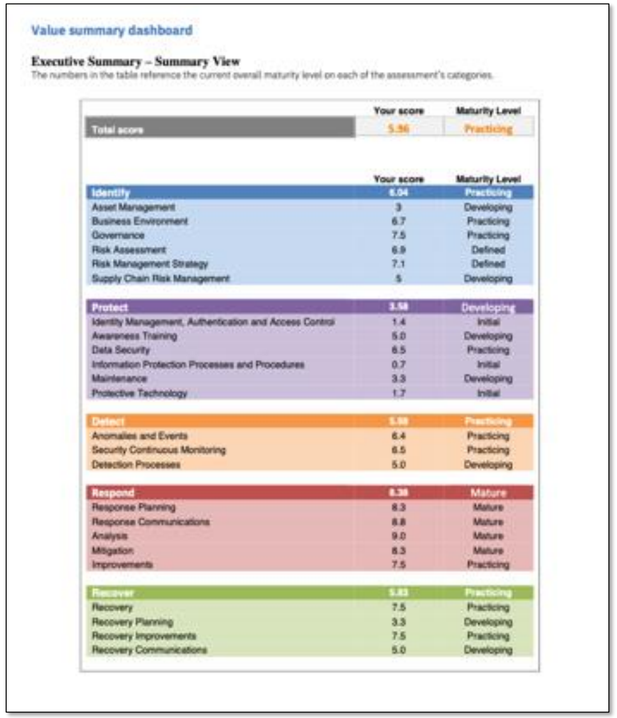
Performance in the environment is satisfactory, though [Customer] recognizes that the organization is one cyber breach away from severely impacting business continuity. [Customer] senior management must understand that risk is the new normal. Being a digital enterprise in 2020 incurs significant risk and Cyber Resiliency (protection, data vaulting and recovery) is now an absolute part of the cost of doing business.

Additionally, IBM feels that [Customer] would benefit from the use of Spectrum Insights to measure different performance and capacity areas in order to drive them toward strong outcomes.

Cyber resiliency should be viewed as a dynamic and ever-evolving practice that requires continuous improvement and focus. With the continued expansion of the threat landscape and pace of technology change, it is imperative that organizations constantly take inventory of how they are doing and where they need to be evolving.

Please review the Recommendation Section for our roadmap, which, if followed, will improve functionality and increase the value realized from implementing resiliency and disaster recovery best practices and solutions. Establishing a mature cyber security and resiliency plan will enable a more proactive approach in detecting, identifying, and protecting their environments, as well as their ability to respond and recover quickly.

IBM

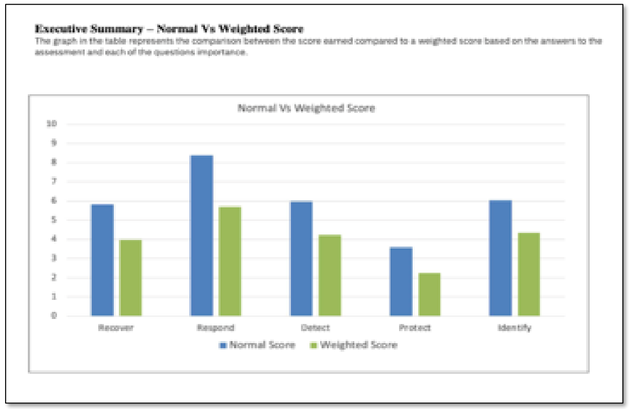

Value summary dashboard

Executive Summary – Summary View

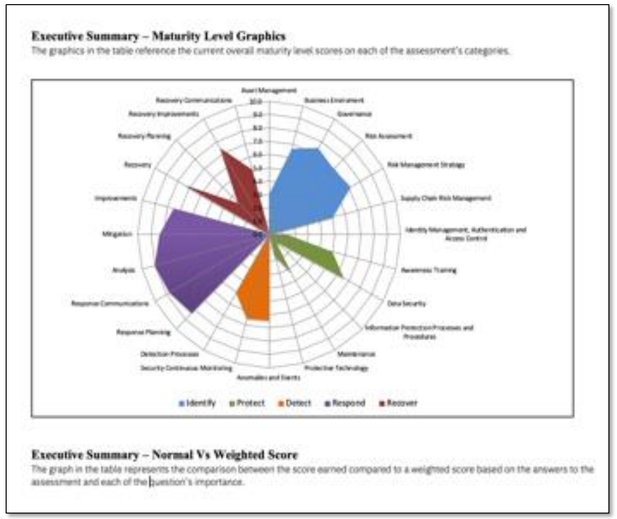
The numbers in the table reference the current overall maturity level on each of the assessment's categories.

	Your score	Maturity Level
Total score	5.86	Practicing

	Your score	Maturity Level
Identify	6.04	Practicing
Asset Management	3	Developing
Business Environment	6.7	Practicing
Governance	7.5	Practicing
Risk Assessment	6.9	Defined
Risk Management Strategy	7.1	Defined
Supply Chain Risk Management	5	Developing
Protect	3.58	Developing
Identity Management, Authentication and Access Control	1.4	Initial
Awareness Training	5.0	Developing
Data Security	6.5	Practicing
Information Protection Processes and Procedures	0.7	Initial
Maintenance	3.3	Developing
Protective Technology	1.7	Initial
Detect	5.93	Practicing
Anomalies and Events	6.4	Practicing
Security Continuous Monitoring	6.5	Practicing
Detection Processes	5.0	Developing
Respond	8.38	Mature
Response Planning	8.3	Mature
Response Communications	8.8	Mature
Analysis	9.0	Mature
Mitigation	8.3	Mature
Improvements	7.5	Practicing
Recover	5.83	Practicing
Recovery	7.5	Practicing
Recovery Planning	3.3	Developing
Recovery Improvements	7.5	Practicing
Recovery Communications	5.0	Developing


Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the questions importance.


Executive Summary – Maturity Level Graphics

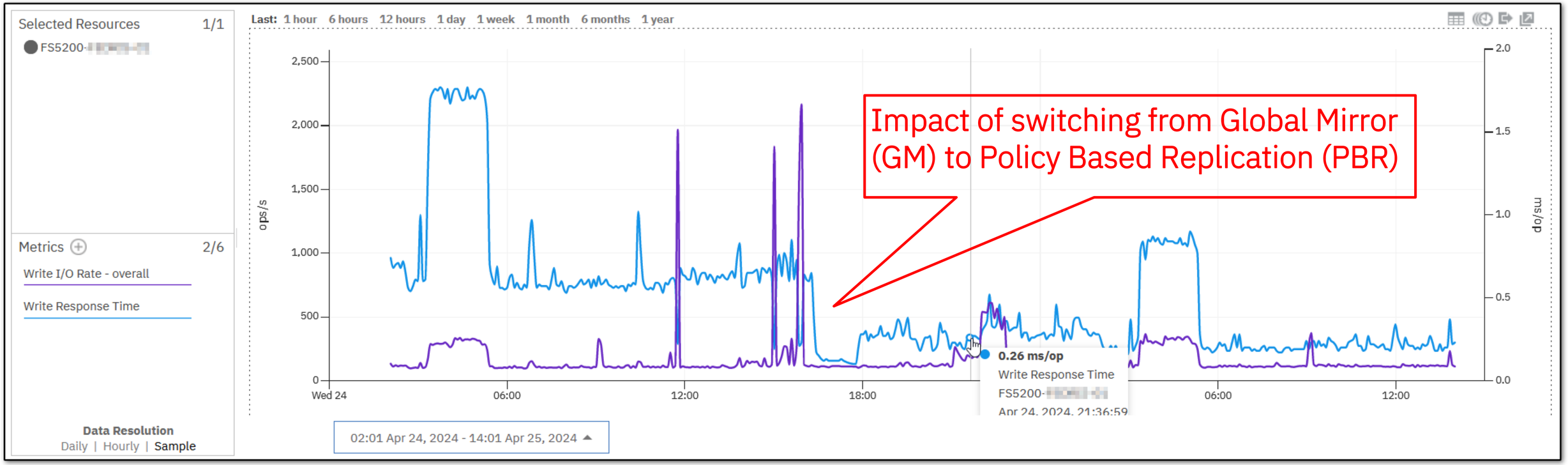
The graphics in the table reference the current overall maturity level scores on each of the assessment's categories.

Executive Summary – Normal Vs Weighted Score

The graph in the table represents the comparison between the score earned compared to a weighted score based on the answers to the assessment and each of the question's importance.

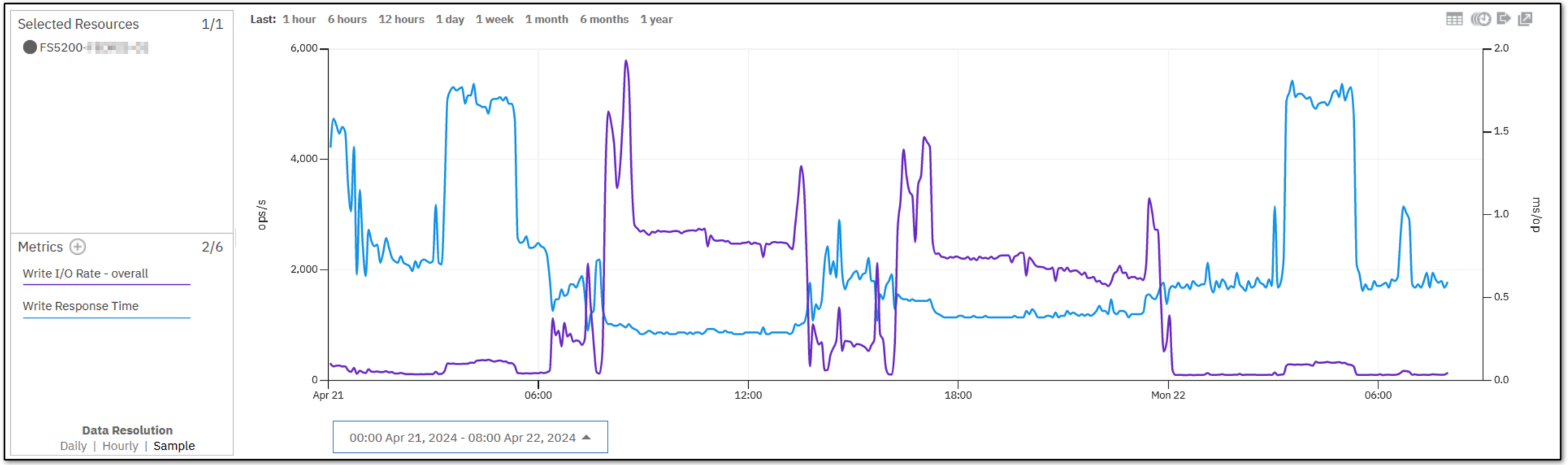
Policy Based Replication (PBR) vs Global Mirror (GM)

GM vs PBR

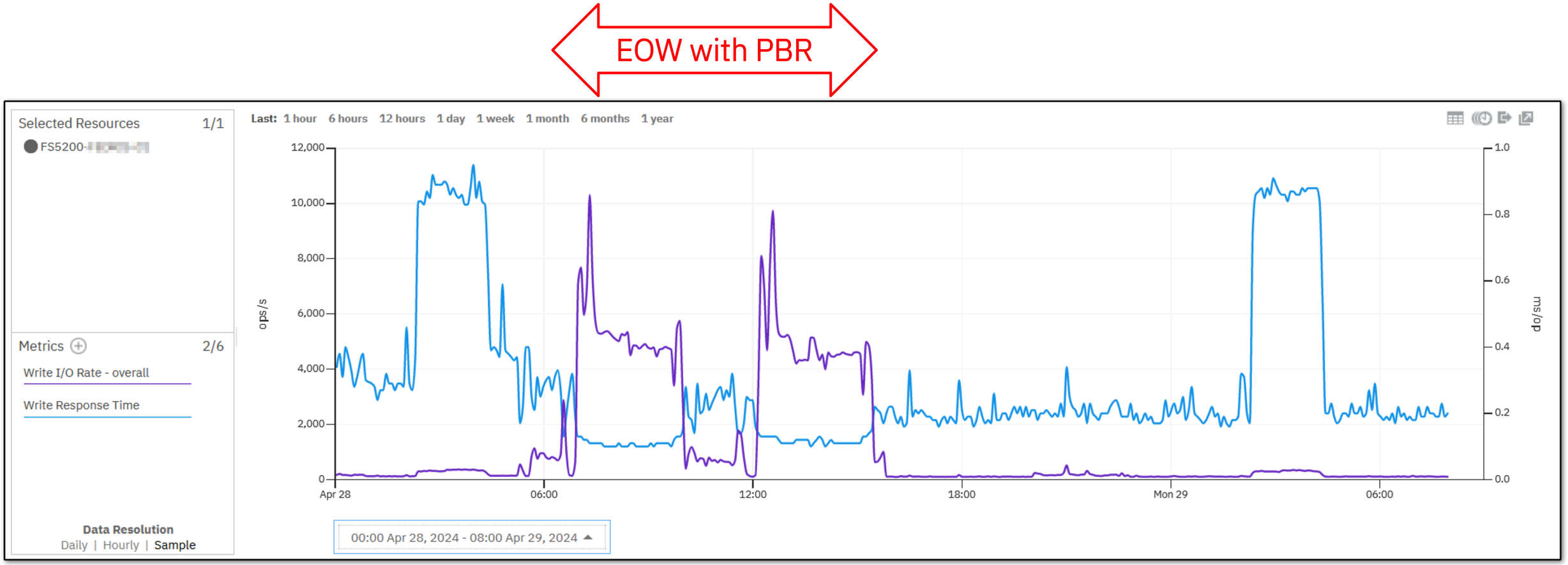

Selected Resources 1/1
FS5200-
Metrics 2/6
Write I/O Rate - overall
Write Response Time
Data Resolution
Daily | Hourly | Sample
Last: 1 hour 6 hours 12 hours 1 day 1 week 1 month 6 months 1 year
ops/s
ms/op
2,500
2,000
1,500
1,000
500
0
2.0
1.5
1.0
0.5
0.0
Wed 24
06:00
12:00
18:00
06:00
12:00
Impact of switching from Global Mirror (GM) to Policy Based Replication (PBR)
0.26 ms/op
Write Response Time
FS5200-
Apr 24, 2024, 21:36:59
02:01 Apr 24, 2024 - 14:01 Apr 25, 2024

EOW with GM

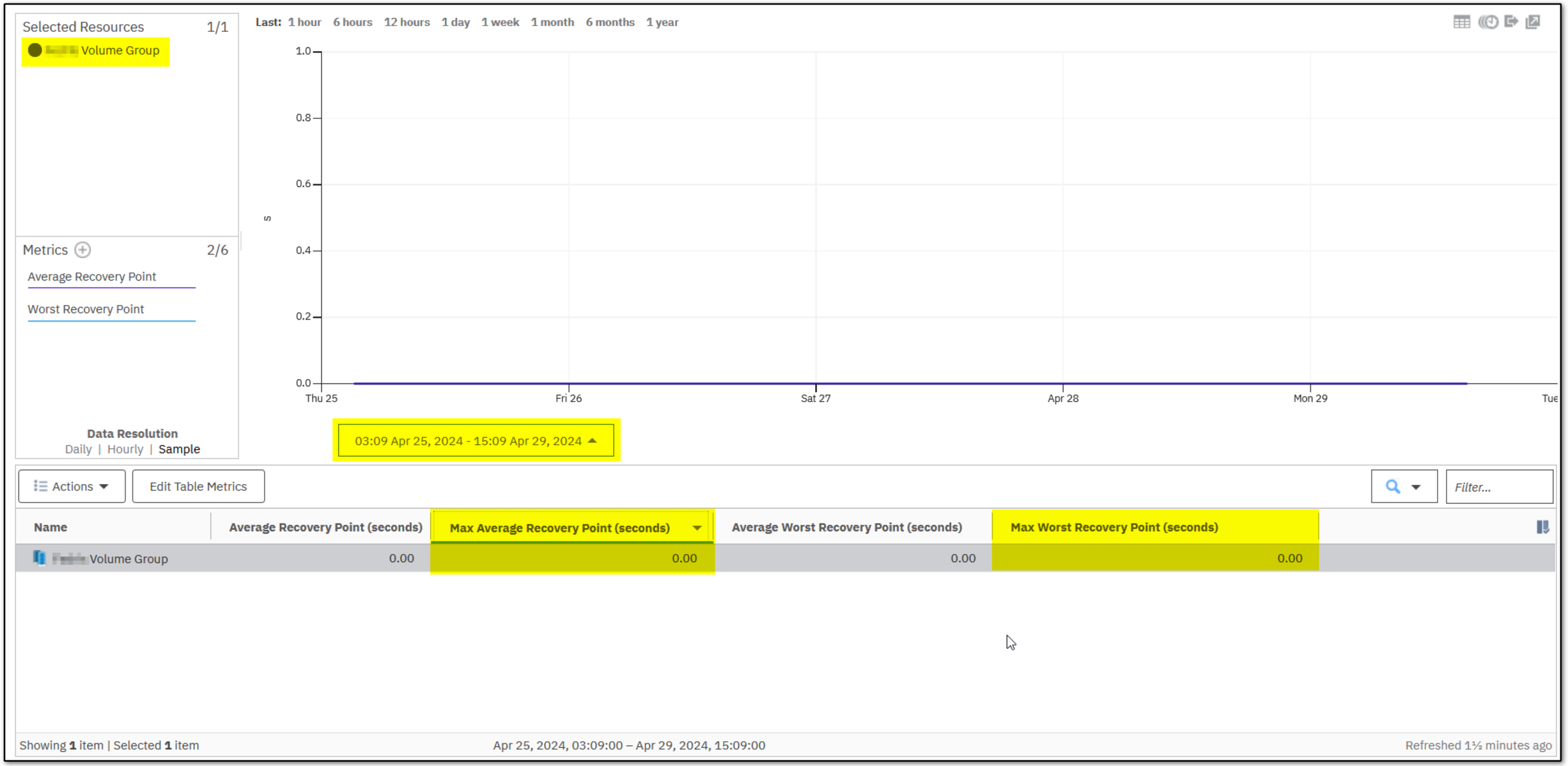
End of week duration with GM



EOW with PBR


EOW with PBR
Selected Resources 1/1
FS5200-
Metrics 2/6
Write I/O Rate - overall
Write Response Time
Data Resolution
Daily | Hourly | Sample
Last: 1 hour 6 hours 12 hours 1 day 1 week 1 month 6 months 1 year
ops/s
ms/op
12,000
10,000
8,000
6,000
4,000
2,000
0
1.0
0.8
0.6
0.4
0.2
0.0
Apr 28
06:00
12:00
18:00
Mon 29
06:00
00:00 Apr 28, 2024 - 08:00 Apr 29, 2024

RPO


Selected Resources 1/1
Volume Group
Metrics 2/6
Average Recovery Point
Worst Recovery Point
Data Resolution
Daily | Hourly | Sample
Last: 1 hour 6 hours 12 hours 1 day 1 week 1 month 6 months 1 year
1.0
0.8
0.6
0.4
0.2
0.0
s
Thu 25
Fri 26
Sat 27
Apr 28
Mon 29
Tue
03:09 Apr 25, 2024 - 15:09 Apr 29, 2024
Actions
Edit Table Metrics
Filter...
Name
Average Recovery Point (seconds)
Max Average Recovery Point (seconds)
Average Worst Recovery Point (seconds)
Max Worst Recovery Point (seconds)
Volume Group
0.00
0.00
0.00
0.00
Showing 1 item | Selected 1 item
Apr 25, 2024, 03:09:00 – Apr 29, 2024, 15:09:00
Refreshed 1½ minutes ago