ADVANCED TECHNOLOGY GROUP (ATG)

Accelerate with ATG Webinar:
IBM FlashSystem's FlashCore Module 4 & integrated Ransomware Threat Detection

Matt Key
Principal Storage Technical Specialist
IBM Advanced Technology Group – FlashSystem
IBM Technology
mkey@us.ibm.com

ADVANCED TECHNOLOGY GROUP (ATG)

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.

2024 Upcoming Webinars – Register Here!

IBM Storage Ceph S3 Object Storage Deep Dive – May 30th, 2024

IBM TS7700 Tape Solution Overview 201 – June 18th, 2024

Why IBM Cloud Object Storage System and, why now? – June 20th, 2024

Unleash the Power of the IBM FlashSystem 5300 – June 25th, 2024

Important Links to bookmark:

ATG Accelerate Site: https://ibm.biz/BdSUFN

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

Offerings

Client Technical Workshops

- IBM DS8900F Advanced Functions
- IBM Fusion & Ceph: A Deep Dive into Next Gen Storage
- **IBM FlashSystem Deep Dive & Advanced Functions:** May 22-23 in Atlanta, GA
- IBM Cyber Resiliency with IBM Storage Defender

TechZone Test Drive / Demo's

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

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

***IMPORTANT* The ATG team serves clients and Business Partners in the Americas, concentrating on North America.**

Registration Open!

Storage @ IBM TechXchange Conference 2024

October 21-24, 2024
Mandalay Bay | Las Vegas
#IBMTechXchange

Key Learnings

- Practical how-to advice
- Patterns and best practices
- Success stories, IBM PoV, proven techniques

Featured Products

IBM Storage Defender
IBM Storage Fusion
IBM Storage Scale + IBM Storage Ceph
IBM Tape + IBM SAN
IBM Storage FlashSystem + IBM Storage DS8000

Collaborate. Learn. Play.

Community

- IBM Champions
- User Groups
- Tech Peers
- Business Partners

Roadmaps

Go deep with people in the know and set the stage for where IBM is going in the future

Sandbox

- Network
- Learn
- Collaborate
- Play

Breakout Sessions

- Trends and Directions
- User Groups
- Product Deep Dives
- Meet the Expert
- Professional Development
- Show the Code
- Birds of a Feather
- Academic/Research

Accelerate your Career

- Labs (Instructor-Led, Self-paced)
- IBM Certification Testing
- Earn up to 25 hours in CPE credits

https://www.ibm.com/community/ibm-techxchange-conference/

Game On! →

Accelerate with ATG Survey

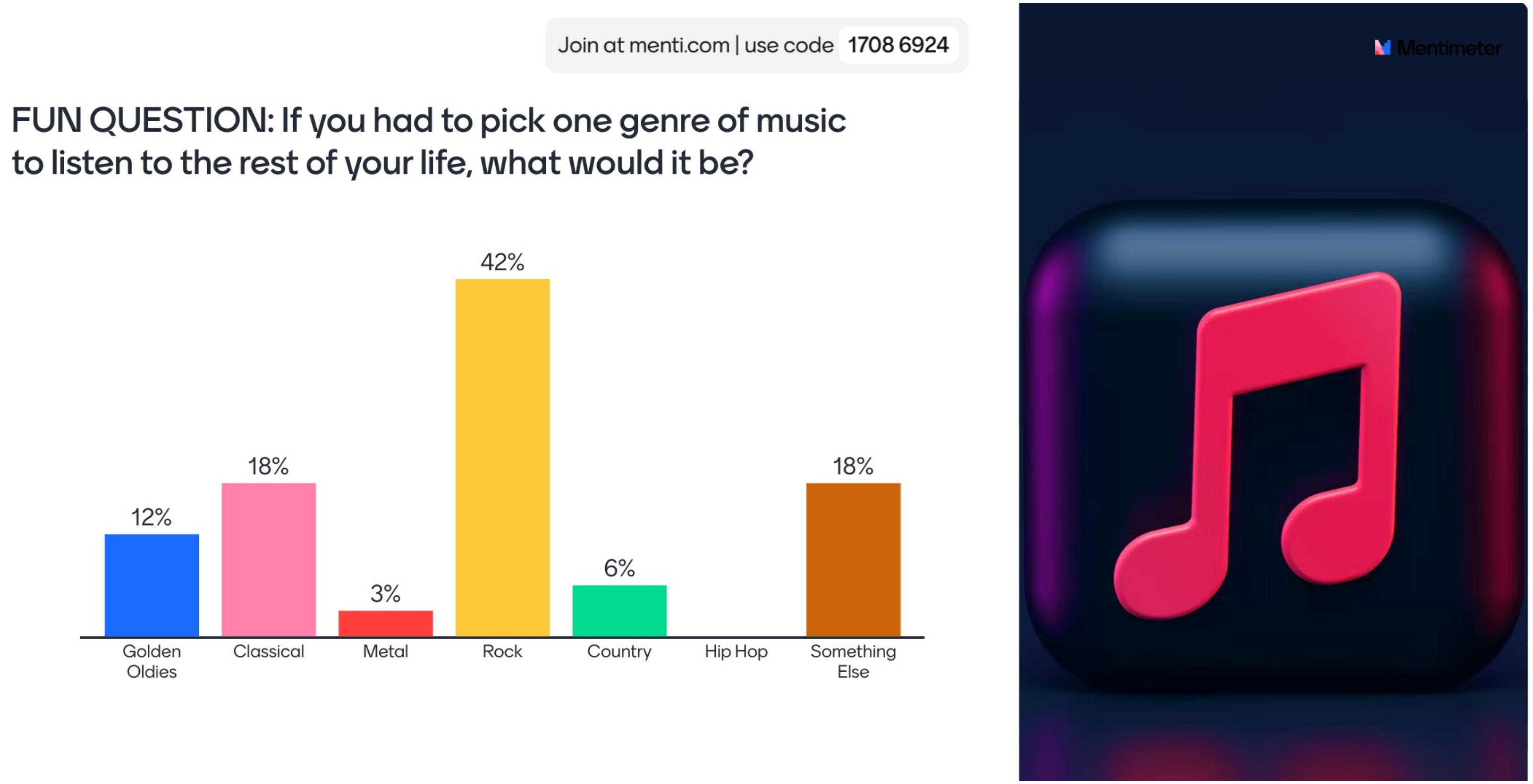
Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 1708 6924 or

Direct link https://www.menti.com/alwhyze7z1gz

Or

QR Code



Join at menti.com | use code 1708 6924

FUN QUESTION: If you had to pick one genre of music to listen to the rest of your life, what would it be?

ADVANCED TECHNOLOGY GROUP (ATG)

Accelerate with ATG Webinar: IBM FlashSystem's FlashCore Module 4 & integrated Ransomware Threat Detection

Matt Key
Principal Storage Technical Specialist
IBM Advanced Technology Group – FlashSystem
IBM Technology
mkey@us.ibm.com

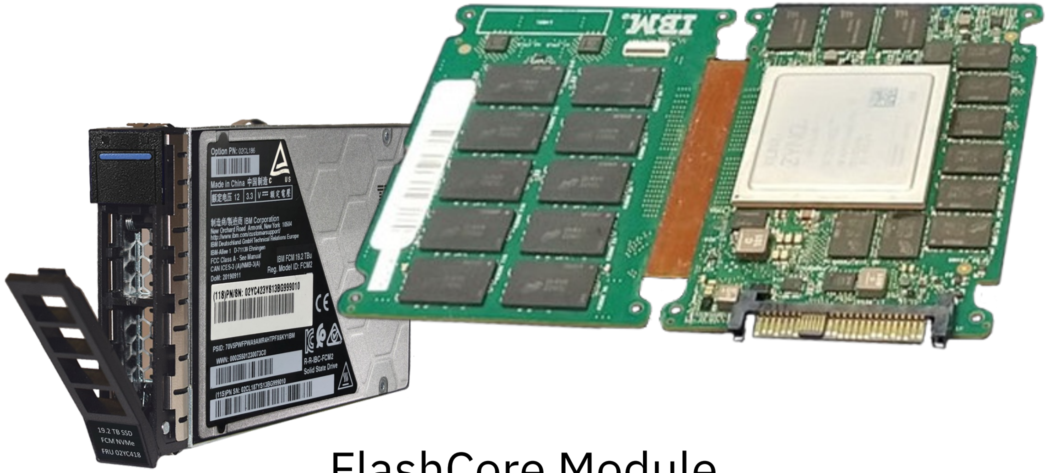
Meet the Speakers – Matt Key

Matt Key is a 18-year veteran of solid state storage and came into IBM through the 2012 acquisition of Texas Memory Systems, the Houston-based engineering group behind the FlashCore Modules in IBM's distributed storage portfolio. Currently, he is the technical lead for Flash in the Advanced Technology Group (ATG), the client-facing group of subject matter experts across the portfolios of storage, servers, and software. Matt graduated Texas A&M (WHOOP!) in 2006 with an engineering degree in telecommunications.

> Any sufficiently advanced technology
> is indistinguishable from magic

- Arthur C. Clarke, 1968

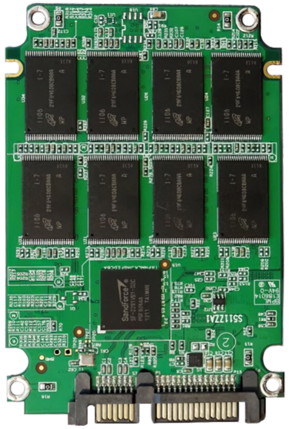
What is a FlashCore Module (FCM)



FlashCore Module

IBM FlashCore Module

- Computational Storage Devices
- Offload heavy lifting from software
- FPGA allows for ‘quick’ and subsequent enhancements
- Value-based development model
  - Performance
  - Security
  - Resiliency

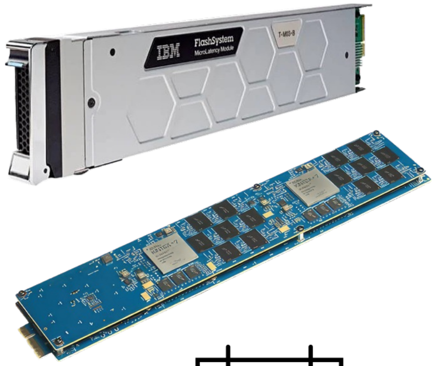


Example 2.5” SSD

Traditional NVMe SSD

- Most value-add provided by storage/x86 software
- Cost-based
- ASIC controller (cost effective, but mostly static IP)
- Usually defined to a specific storage tier (Tier 0/1/2 Flash)

History of FlashCore Technology



2014

MicroLatency Module

Proprietary interface, single-layer cell (SLC) flash, followed up with multi-layer cell (MLC) flash, and in both cases the data path is in hardware

Multiple protection features, including ECC error correction, variable stripe RAID data protection, overprovisioning, and three-dimensional (AE3 flash modules) or two-dimensional (AE2 flash modules) flash RAID

2018

FCM1

NVMe interface, re-implemented into a standard 2.5” form factor, triple-layer cell (TLC) flash with inline 2-to-1 data compression and encryption with no performance penalty

2020

FCM2

NVMe interface, quad-layer cell (QLC) flash with better than TLC performance, inline 2-to-1 data compression and encryption with no performance penalty

2022

FCM3

NVMe interface, quad-layer cell (QLC) flash with SLC abilities, optimized with a “Hinting Architecture” to optimize data placement, with up to 3-to-1 inline data compression, encryption with no performance penalty, L and XL modules based on PCIe G4

2024

FCM4

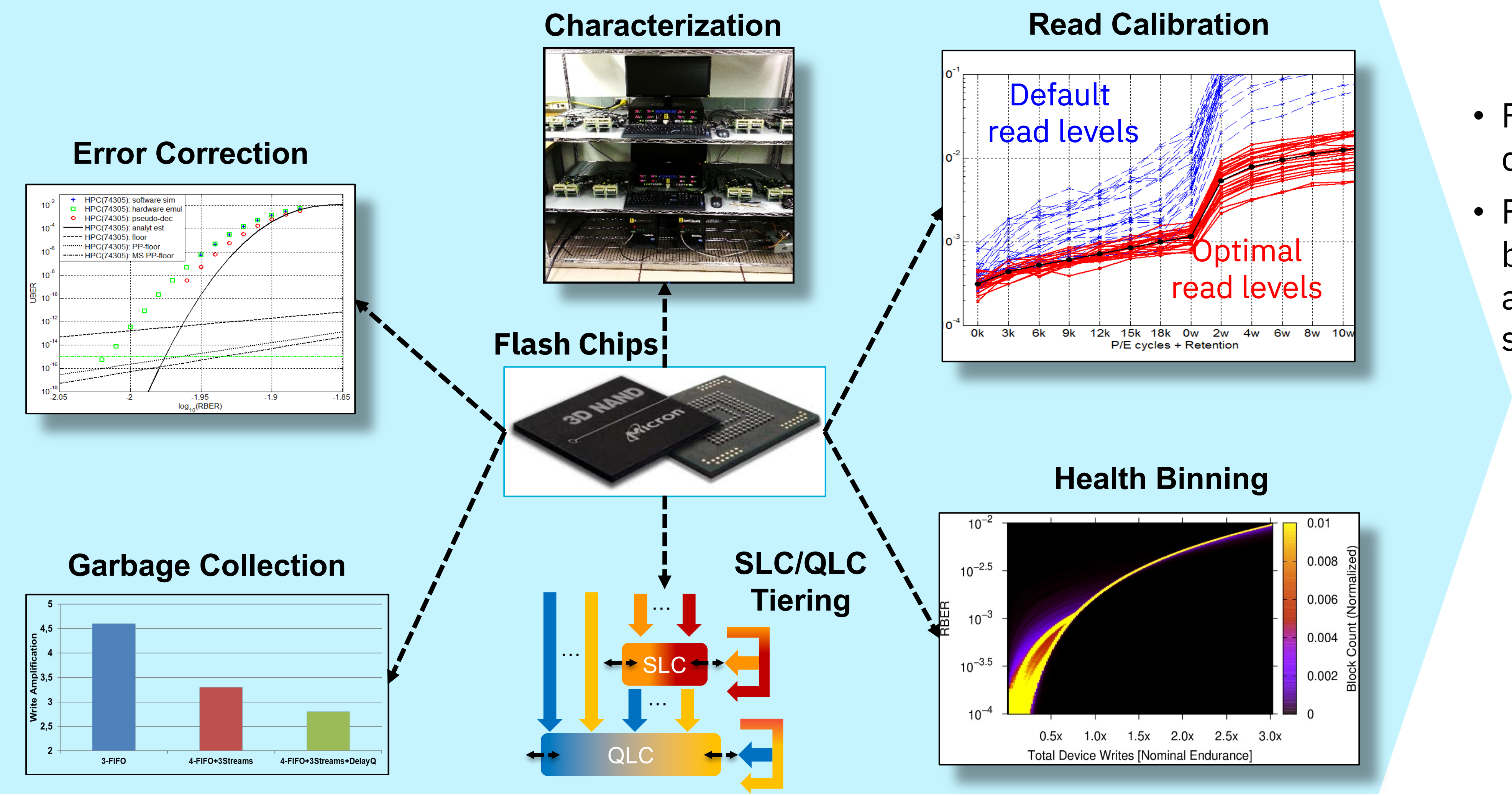
NVMe across PCIe 4.0 interface for all FCM sizes, 176-Layer with SLC and QLC abilities, Quantum-safe encryption, and Ransomware Threat Detection

Backwards Compatible with FCM3

IBM FlashCore™

FlashCore Modules (FCM)

At the Heart of Quad Layer Cell (QLC) Enablement

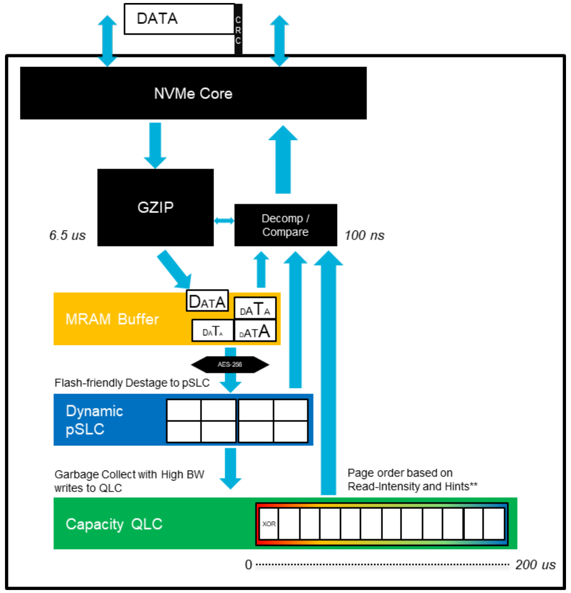


- FlashCore Technology drives FCM
- FCM are the core building blocks for all NVMe FlashSystem storage arrays

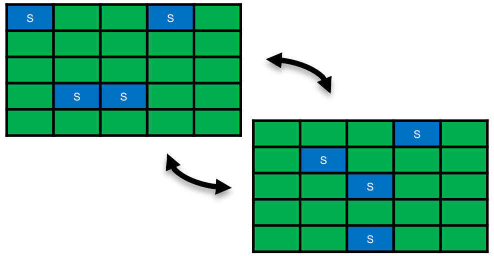
NVMe-based FlashSystem

FlashCore Module 4 Specifications

FCM	Usable Capacity	Endurance (TDW)	PCIe
Small	4.8 TBu	12.2 PBu	PCIe 4.0 x4
Medium	9.6 TBu	24.5 PBu	PCIe 4.0 x4
Large	19.2 TBu	49.0 PBu	PCIe 4.0 x4
XLarge	38.4 TBu	98.1 PBu	PCIe 4.0 x4


DATA
CRC
NVMe Core
GZIP
6.5 us
Decomp / Compare
100 ns
MRAM Buffer
DATA
DATA
DATA
DATA
AES-256
Flash-friendly Destage to pSLC
Dynamic pSLC
Garbage Collect with High BW writes to QLC
Page order based on Read-Intensity and Hints**
Capacity QLC
XOR
0
200 us

FCM Data Path



Dynamic SLC Layer

FlashCore Hints

- XOR and Metadata Acceleration
- Turbo Power
- Proactive LBA Recovery
- Flash block Sweeper
- FCM RAID Sweeper
- Internal End-to-end CRC
- Volume I/O Tagging (New to FCM4)
- Secure Key Passing (New to FCM4)

New to FCM4

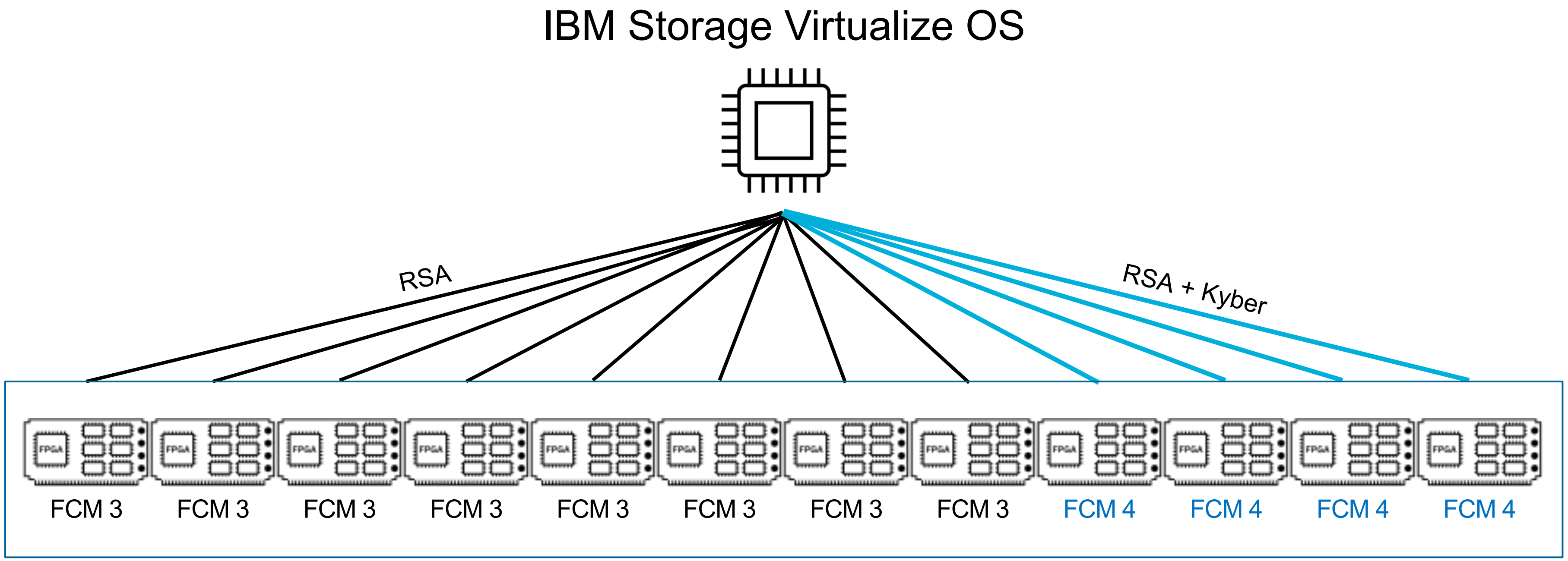
Latest 176-Layer NAND

Post-Quantum Cryptography

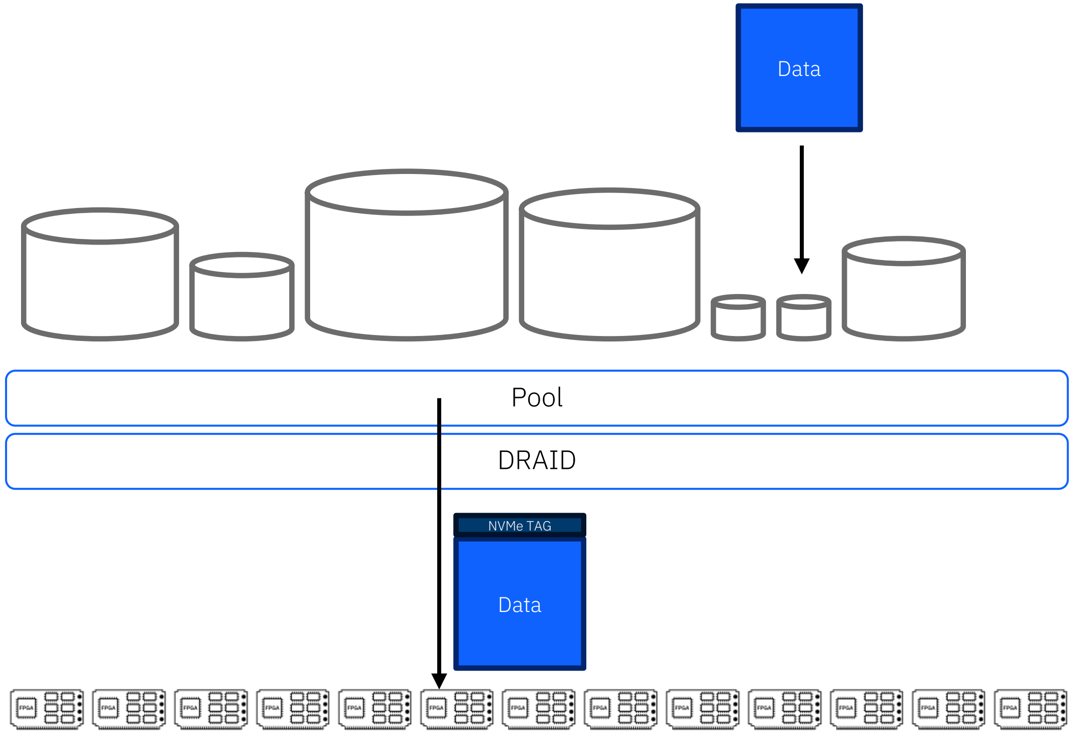
Ransomware Threat Detection

Post-Quantum Cryptography

- Data at Rest is continued as AES-256 Encryption
- IBM Storage Virtualize protects the security PINs of each drive through an IBM-specific protocol of Secure Key Passing (SKP)
- FCM4 Embrace CRYSTALS-Kyber algorithm and RSA for SKP
- Transparent to admin & intermixes with FCM3s cleanly



FlashCore Modules 4 are Volume Aware



FCM-4

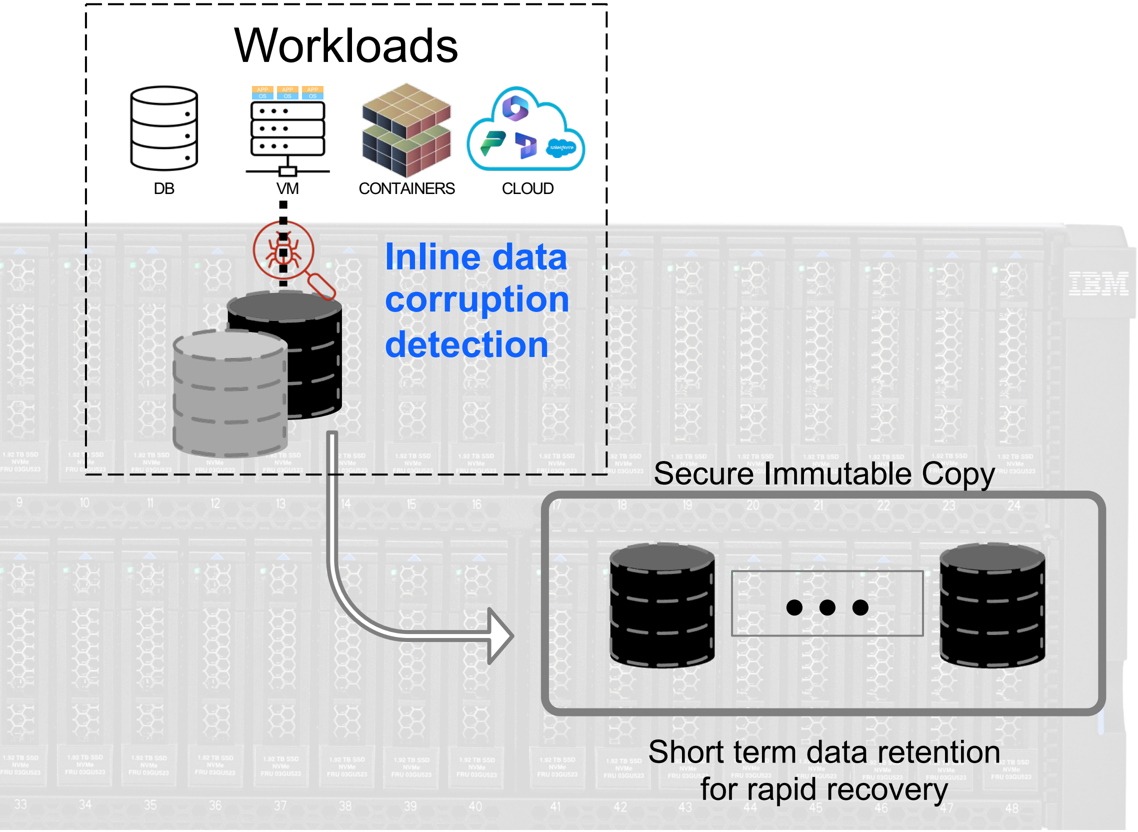
FLASHCORE MODULE 4

RANSOMWARE

THREAT DETECTION

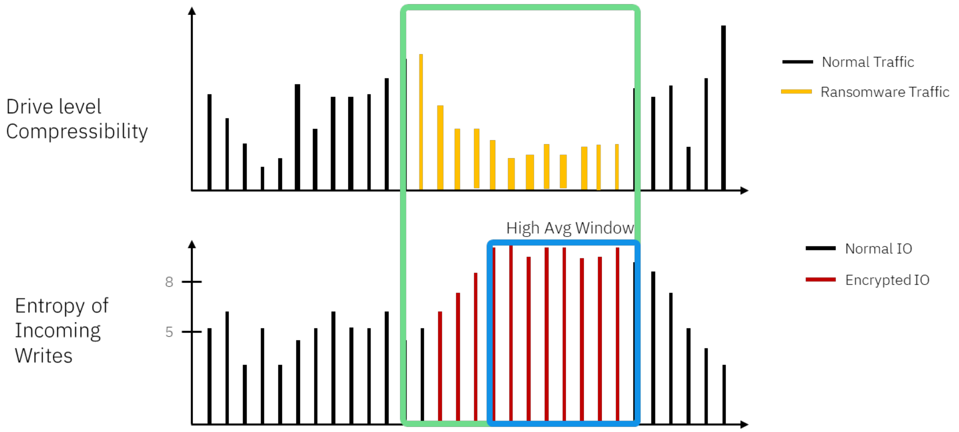
ADVANCED TECHNOLOGY GROUP (ATG)

Inline Data Corruption Detection (Introduced June 2023 w/ Virtualize 8.6.0)

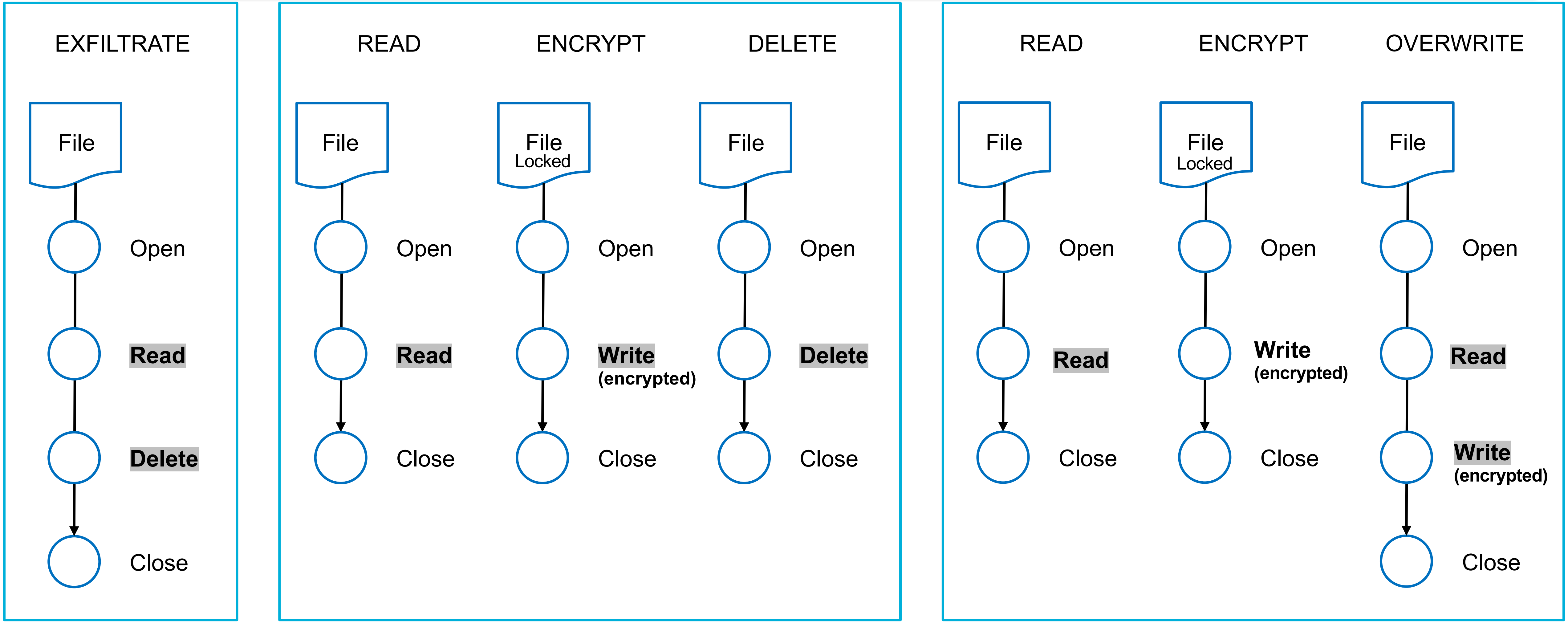

Workloads
DB
VM
CONTAINERS
CLOUD
Inline data corruption detection
IBM
Secure Immutable Copy
Short term data retention for rapid recovery

Early detection is essential to containing corruption

- Actively scanning IO before written to flash can alert of intrusion much earlier, potentially limiting impact to a single application or volume.
- Dramatically reduce the impact of a landed cyber attack, saving time to recovery.

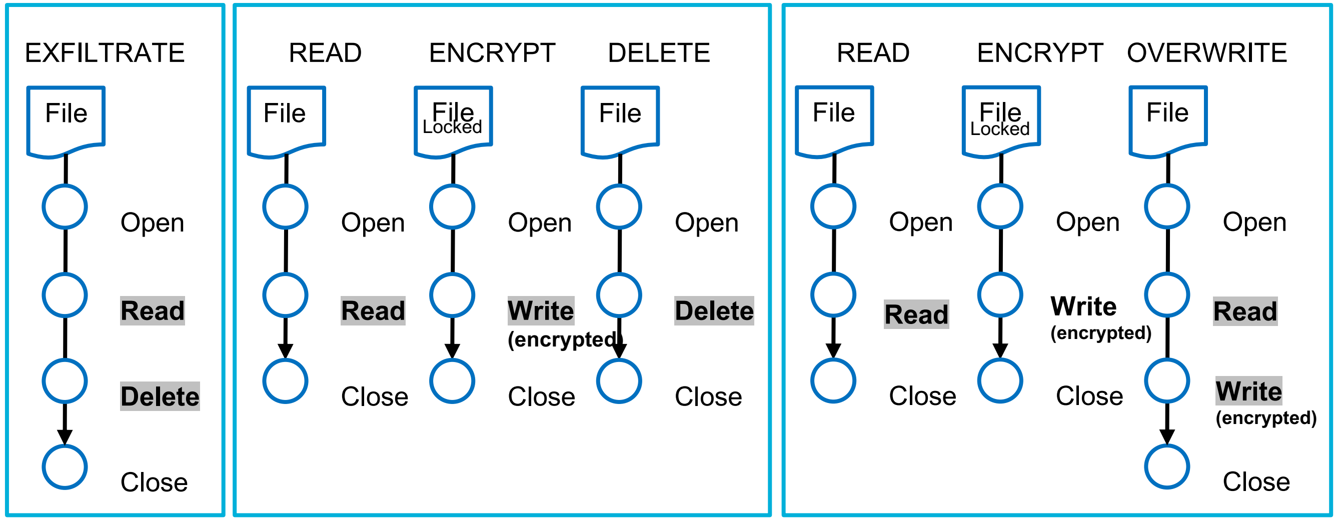


Cyber Attacks: Similar IO Access Sequences

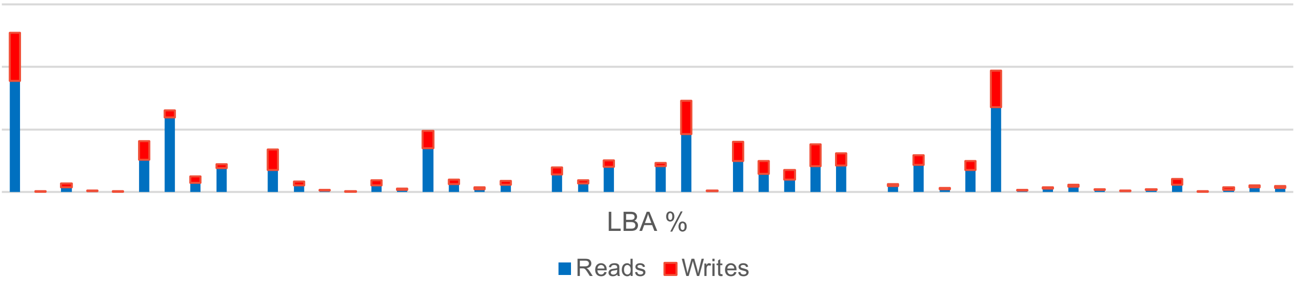


Dimensions of Analysis (What, Where, and How)

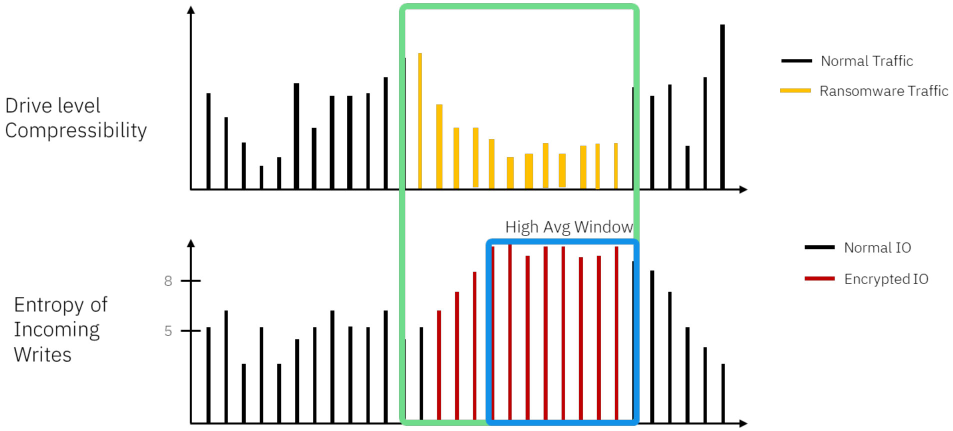
1) Cyber Attacks: Similar IO Access Sequences



2) Logical Block Addressing (Spatial Locality)

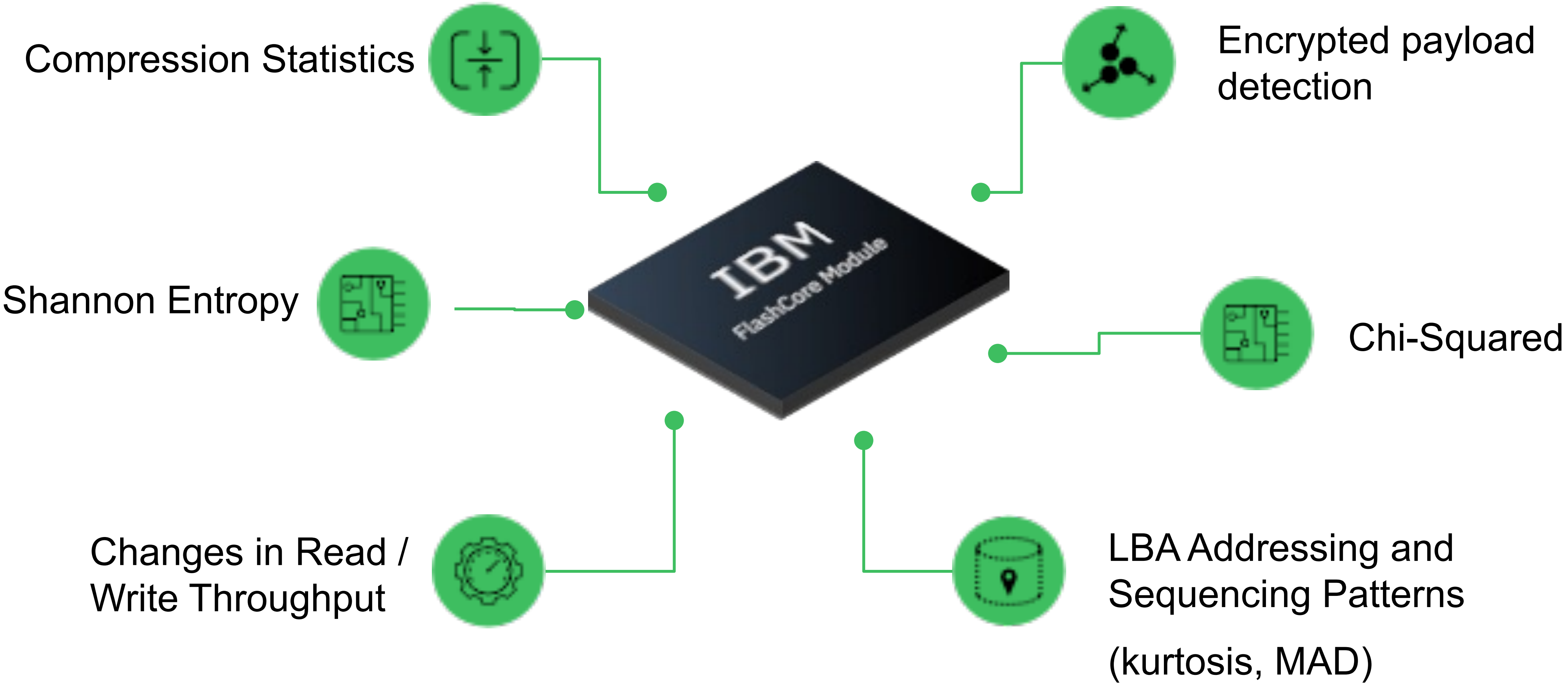


3) Data Characteristics



Ransomware Detection With FCMs

40+ data statistics analyzed in detection engine



Compression Statistics

Encrypted payload detection

Shannon Entropy

Chi-Squared

Changes in Read / Write Throughput

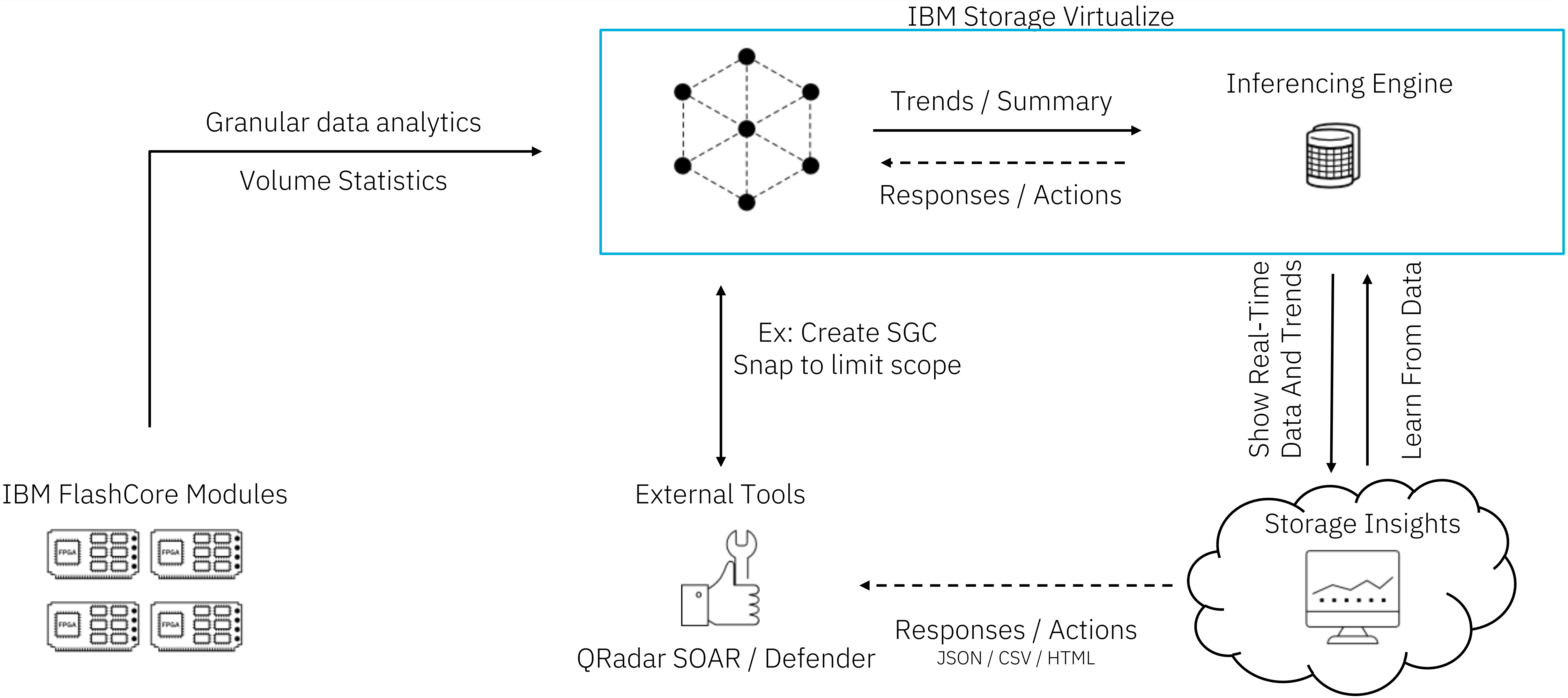
LBA Addressing and Sequencing Patterns

(kurtosis, MAD)

Prerequisites for Ransomware Threat Detection

- Pool must be ONLY FCM4s, updated to FW v4.1
- Pool must be created with v8.6.2+
- Only a single FCM DRAID in the pool (pre-existing req)
- DRAID6
- Storage Insights Pro alerting
- 128GB+ RAM per node
- Standard Pools only (and Fully Allocated in DRP is OK)

Ransomware Monitoring Architectural Overview



IBM Storage Virtualize

Granular data analytics

Volume Statistics

Trends / Summary

Responses / Actions

Inferencing Engine

Ex: Create SGC
Snap to limit scope

Show Real-Time
Data And Trends

Learn From Data

IBM FlashCore Modules

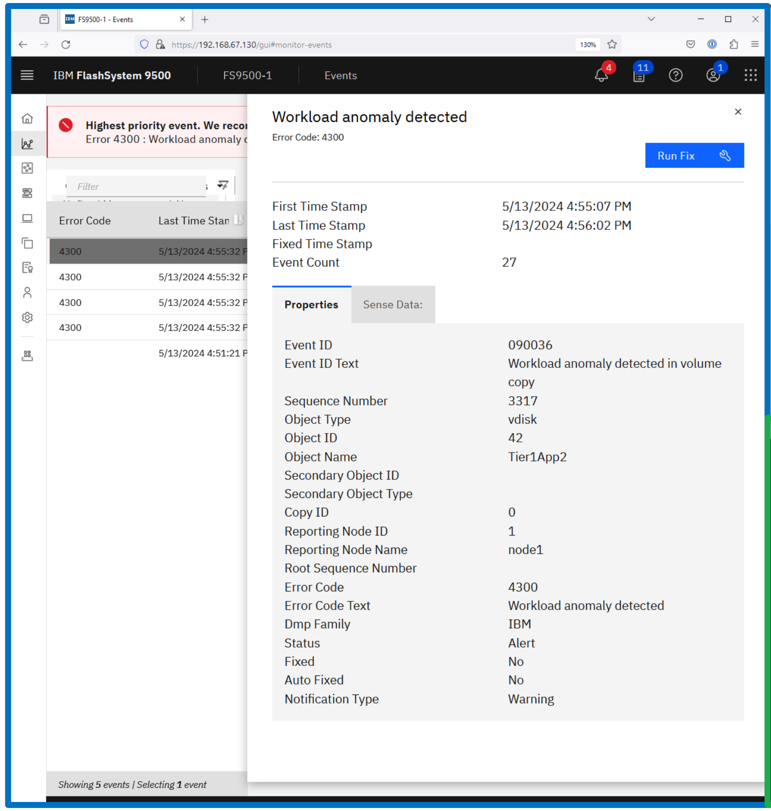
External Tools

QRadar SOAR / Defender

Responses / Actions
JSON / CSV / HTML

Storage Insights

Ransomware Threat Detection in Action



Highest priority event. We recor
Error 4300 : Workload anomaly d

Error Code	Last Time Stan
4300	5/13/2024 4:55:32 P
4300	5/13/2024 4:55:32 P
4300	5/13/2024 4:55:32 P
4300	5/13/2024 4:55:32 P
	5/13/2024 4:51:21 P

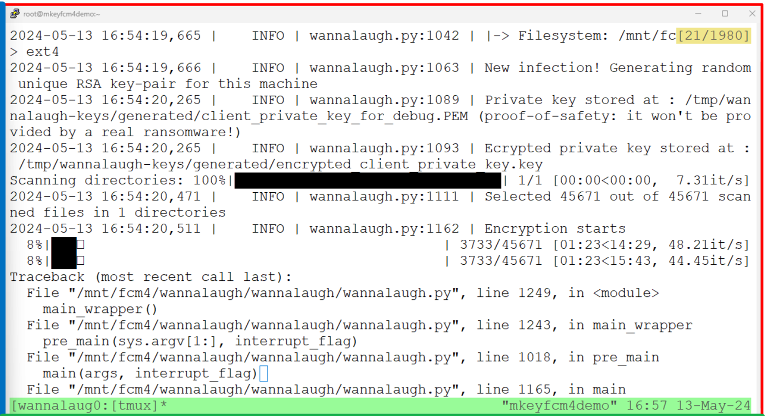
Showing 5 events | Selecting ***1*** *event*

Workload anomaly detected

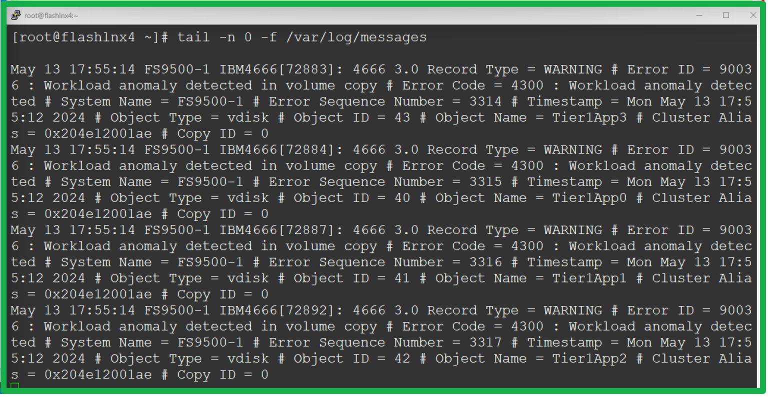
Error Code: 4300

First Time Stamp	5/13/2024 4:55:07 PM
Last Time Stamp	5/13/2024 4:56:02 PM
Fixed Time Stamp	
Event Count	27

Event ID	090036
Event ID Text	Workload anomaly detected in volume copy
Sequence Number	3317
Object Type	vdisk
Object ID	42
Object Name	Tier1App2
Secondary Object ID	
Secondary Object Type	
Copy ID	0
Reporting Node ID	1
Reporting Node Name	node1
Root Sequence Number	
Error Code	4300
Error Code Text	Workload anomaly detected
Dmp Family	IBM
Status	Alert
Fixed	No
Auto Fixed	No
Notification Type	Warning



```
2024-05-13 16:54:19,665 |    INFO | wannalaugh.py:1042 | |-> Filesystem: /mnt/fc[21/1980]
> ext4
2024-05-13 16:54:19,666 |    INFO | wannalaugh.py:1063 | New infection! Generating random
 unique RSA key-pair for this machine
2024-05-13 16:54:20,265 |    INFO | wannalaugh.py:1089 | Private key stored at : /tmp/wan
nalaugh-keys/generated/client_private_key_for_debug.PEM (proof-of-safety: it won't be pro
vided by a real ransomware!)
2024-05-13 16:54:20,265 |    INFO | wannalaugh.py:1093 | Ecrypted private key stored at :
 /tmp/wannalaugh-keys/generated/encrypted_client_private_key.key
Scanning directories: 100%|████████████████████████████████| 1/1 [00:00<00:00,  7.31it/s]
2024-05-13 16:54:20,471 |    INFO | wannalaugh.py:1111 | Selected 45671 out of 45671 scan
ned files in 1 directories
2024-05-13 16:54:20,511 |    INFO | wannalaugh.py:1162 | Encryption starts
  8%|███                                       | 3733/45671 [01:23<14:29, 48.21it/s]
  8%|███                                       | 3733/45671 [01:23<15:43, 44.45it/s]
Traceback (most recent call last):
  File "/mnt/fcm4/wannalaugh/wannalaugh/wannalaugh.py", line 1249, in <module>
    main_wrapper()
  File "/mnt/fcm4/wannalaugh/wannalaugh/wannalaugh.py", line 1243, in main_wrapper
    pre_main(sys.argv[1:], interrupt_flag)
  File "/mnt/fcm4/wannalaugh/wannalaugh/wannalaugh.py", line 1018, in pre_main
    main(args, interrupt_flag)
  File "/mnt/fcm4/wannalaugh/wannalaugh/wannalaugh.py", line 1165, in main
[wannalaug0:[tmux]*                                       "mkeyfcm4demo" 16:57 13-May-24
```



```
[root@flashlnx4 ~]# tail -n 0 -f /var/log/messages

May 13 17:55:14 FS9500-1 IBM4666[72883]: 4666 3.0 Record Type = WARNING # Error ID = 9003
6 : Workload anomaly detected in volume copy # Error Code = 4300 : Workload anomaly detec
ted # System Name = FS9500-1 # Error Sequence Number = 3314 # Timestamp = Mon May 13 17:5
5:12 2024 # Object Type = vdisk # Object ID = 43 # Object Name = Tier1App3 # Cluster Alia
s = 0x204e12001ae # Copy ID = 0
May 13 17:55:14 FS9500-1 IBM4666[72884]: 4666 3.0 Record Type = WARNING # Error ID = 9003
6 : Workload anomaly detected in volume copy # Error Code = 4300 : Workload anomaly detec
ted # System Name = FS9500-1 # Error Sequence Number = 3315 # Timestamp = Mon May 13 17:5
5:12 2024 # Object Type = vdisk # Object ID = 40 # Object Name = Tier1App0 # Cluster Alia
s = 0x204e12001ae # Copy ID = 0
May 13 17:55:14 FS9500-1 IBM4666[72887]: 4666 3.0 Record Type = WARNING # Error ID = 9003
6 : Workload anomaly detected in volume copy # Error Code = 4300 : Workload anomaly detec
ted # System Name = FS9500-1 # Error Sequence Number = 3316 # Timestamp = Mon May 13 17:5
5:12 2024 # Object Type = vdisk # Object ID = 41 # Object Name = Tier1App1 # Cluster Alia
s = 0x204e12001ae # Copy ID = 0
May 13 17:55:14 FS9500-1 IBM4666[72892]: 4666 3.0 Record Type = WARNING # Error ID = 9003
6 : Workload anomaly detected in volume copy # Error Code = 4300 : Workload anomaly detec
ted # System Name = FS9500-1 # Error Sequence Number = 3317 # Timestamp = Mon May 13 17:5
5:12 2024 # Object Type = vdisk # Object ID = 42 # Object Name = Tier1App2 # Cluster Alia
s = 0x204e12001ae # Copy ID = 0
```

16:54:20 EST – Attack Starts

16:55:14 EST – Alert Received

54 seconds!

Ransomware Threat Detection

Brought to you by

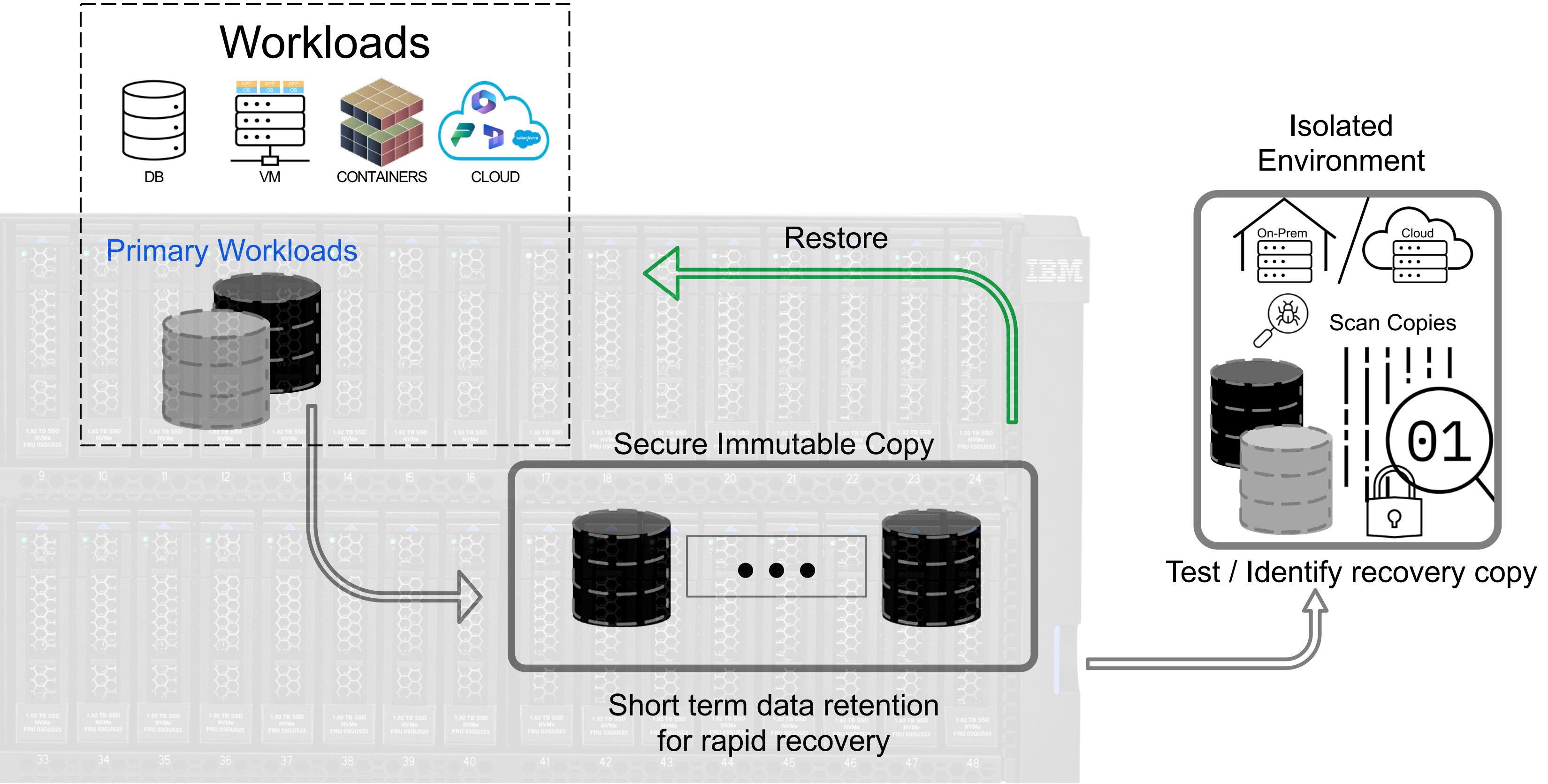
IBM Research

IBM Storage Virtualize

IBM FlashCore

IBM Storage Insights Pro

Data Validation – Extending Ransomware Threat Detection with Cyber Vault



- Application Aware-ness and App Consistency
- Deep scan data with anomaly detection software
- Automate and catalog with Copy Data Manager
- Identify known-good copy
- Testing builds confidence and ensures compliance

Thank you!

Accelerate with ATG Survey

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

You can access this 6-question survey via Menti.com with code 1708 6924 or

Direct link https://www.menti.com/alwhyze7z1gz

Or

QR Code