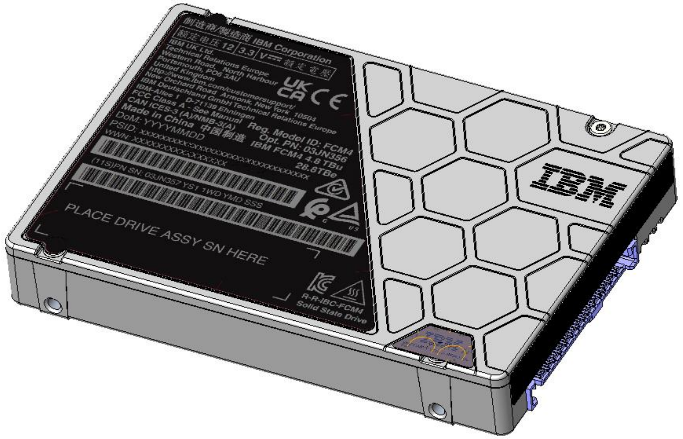


FlashCore Module 4 (FCM)

Meet the Engine Behind IBM's Flash System

Trent Johnson

With help from Andy Walls

FMS the Future of Memory and Storage

FlashCore Module 4

FCM4 Offering

2.5" Dual ported NVMe SSD
U.2 Form Factor

QLC flash

Hardware Compression

Encryption with FIPS 140-3 L2 application filed

Used exclusively In IBM Storage Appliances

Small

4.8TBu → 22TBe
PCIe Gen4
780 MB/s Write BW
2300 MB/s Read BW

Medium

9.6TBu → 28.8TBe
PCIe Gen4
780 MB/s Write BW
2300 MB/s Read BW

Large

19.2TBu → 57.6TBe
PCIe Gen4
1560 MB/s Write BW
3500 MB/s Read BW

XLarge

38.4TBu → 115.2TBe
PCIe Gen4
1560 MB/s Write BW
3500 MB/s Read BW
Market Leading Density

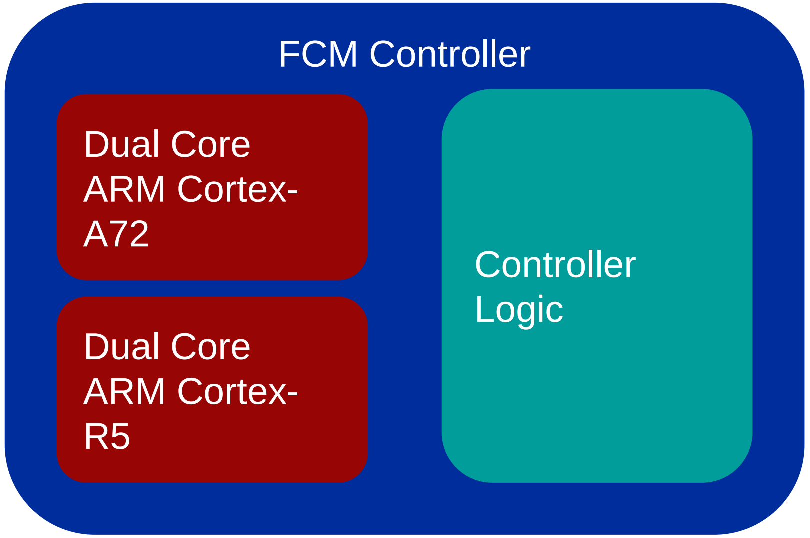
Best Price Point

Best Value

Enterprise Performance and Endurance with *ONLY* QLC
7 Year Endurance Guaranteed

FCM – A Computational Storage Device…

- Cutting Edge Flash Controller with embedded, powerful multi-core ARM processors
- Inline compression provides system processing offload and system memory offload
- Quantum-Safe Encryption
  - TCG Opal
  - Data at rest protected by AES-256
  - Firmware protected by Crystals/Dilithium5
  - Key Encryption Key protected by Crystals/Kyber1024
- Flash Translation Layer processing and metadata contained completely inside FCM
- Application Process Units (APUs) and Programmable Logic collect data for computation
- Real-time Processing Units (RPUs) analyze collected data
- Integrated Ransomware Threat Detection!!! – (added in FCM4)
  - Ransomware
  - Wiperware
  - Exfiltration



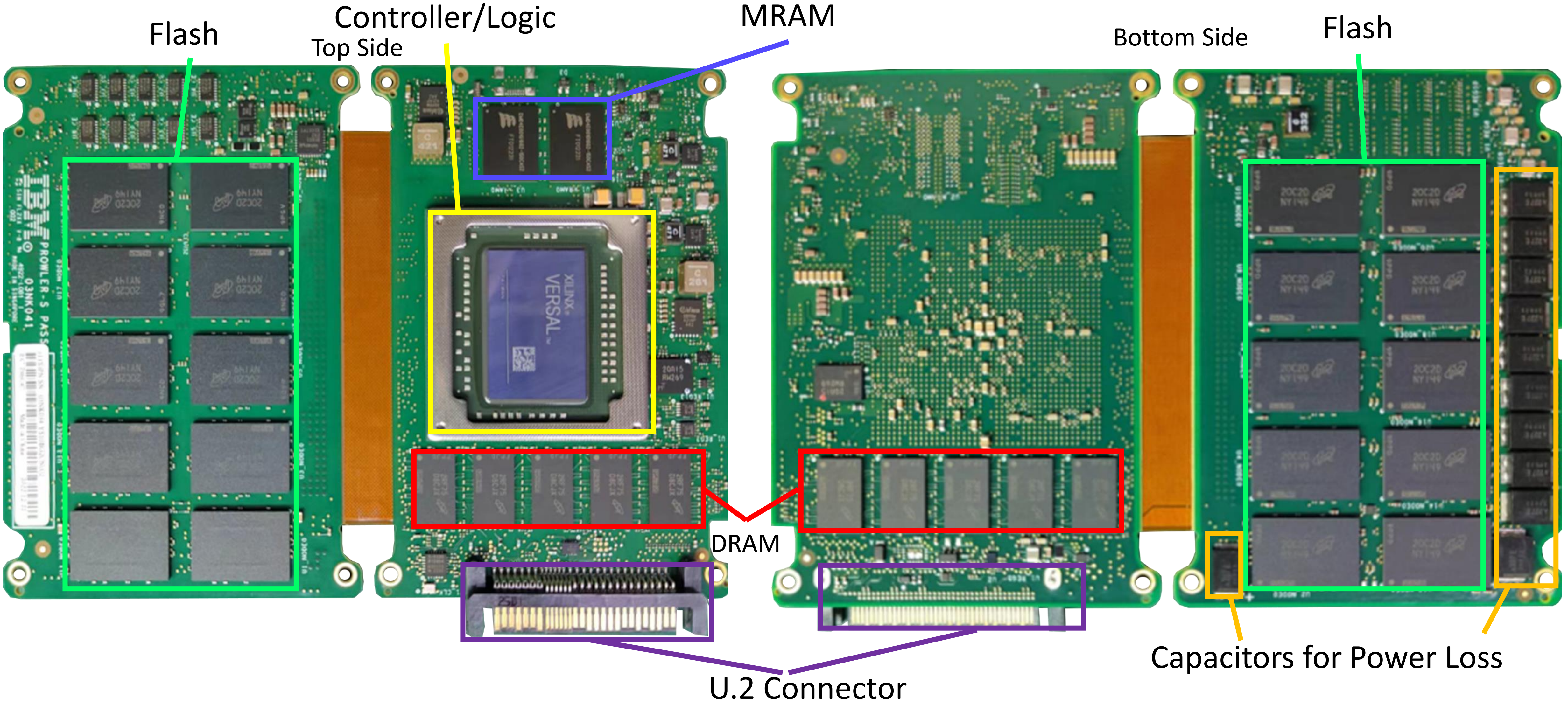
FCM Controller

Dual Core ARM Cortex-A72

Dual Core ARM Cortex-R5

Controller Logic

The Layout of FlashCore Module 4



FMS IBM

the Future of Memory and Storage

FCM-4

FLASHCORE MODULE 4

RANSOMWARE

THREAT DETECTION

A Realization:

Block Storage is missing some context other parts of the system have

BUT: It can generate data needed for determining Ransomware attacks with less performance impact then any other part of the system

Why detect ransomware on the storage array?

IBM FlashSystem excels in ingesting large amounts of data fast.

If the storage can analyze the data **as it is stored**, we can generate critical insights more efficiently than external backup scanning applications and detect threats **faster**

IBM FlashSystem Ransomware Threat Detection Pipeline

the Future of Memory and Storage

1. IBM FlashCore modules collect and analyze detailed ransomware statistics from **every I/O** with **no performance impact**

IBM Storage Virtualize

2. IBM Storage Virtualize runs an AI engine on every FlashSystem that is fed ML models developed by IBM Research trained on real-world ransomware

   The AI engine learns what’s normal for the system and detects threats using data from FCM

IBM Storage Insights Pro

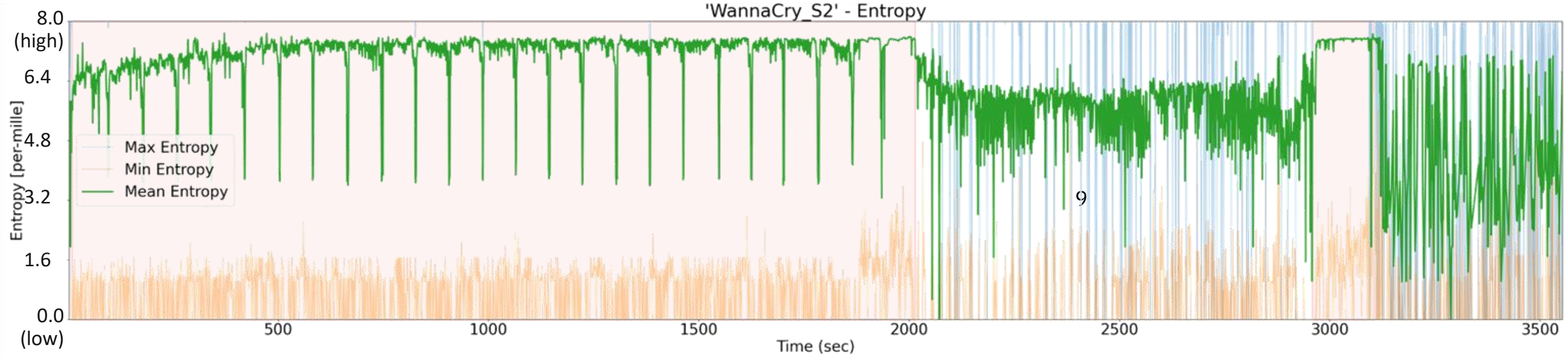
3. IBM Storage Insights collects threat information from connected FlashSystem arrays, alerts users and triggers SIEM/SOAR software to initiate a response

   Statistics are fed back to IBM to improve ML models

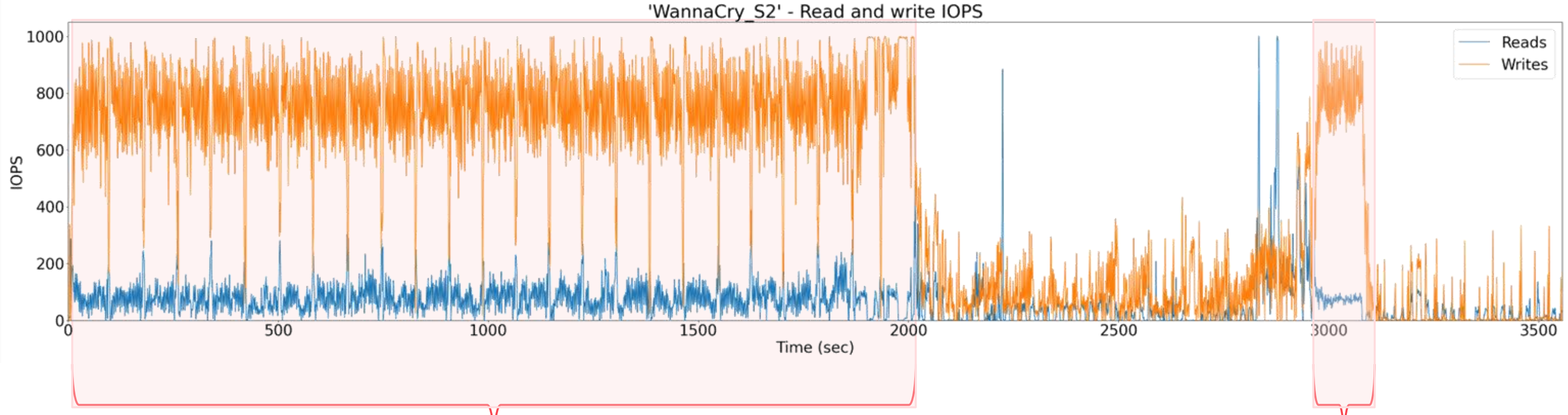
Characteristics found in IO traces from ransomware

- Malware such as ransomware attacks can be detected from storage IO patterns and data analysis
- Example “Wannacry”:

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

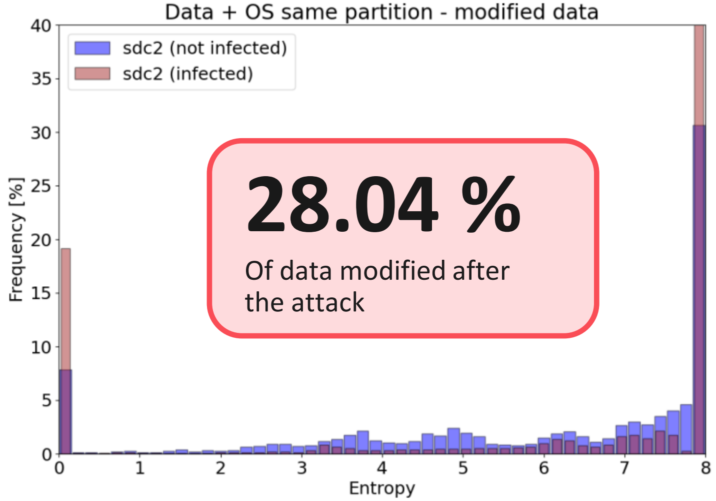


IOPS (– read, – write):



IO activity of ransomware

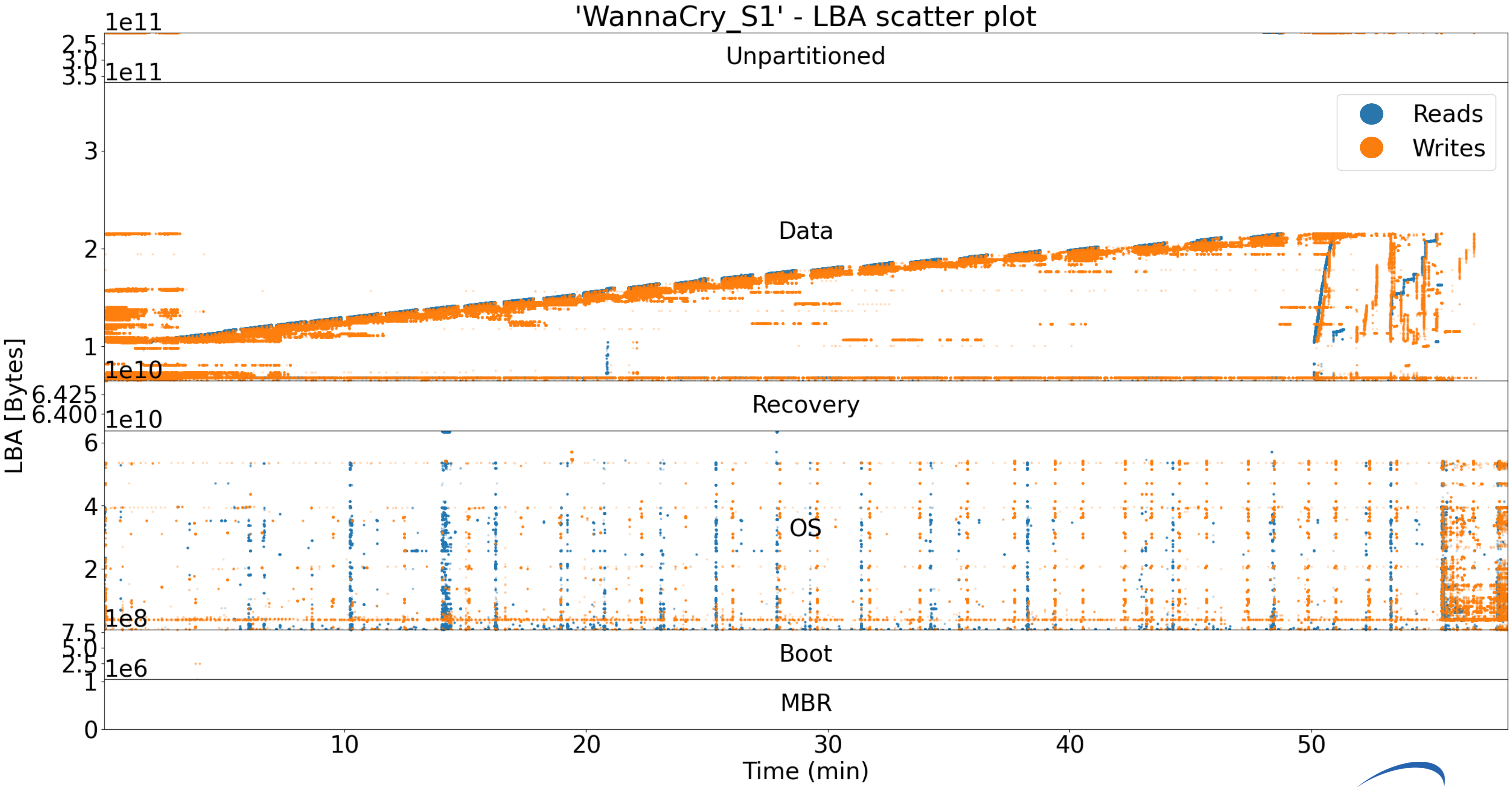
Payload encrypted – before and after attack:



28.04 %

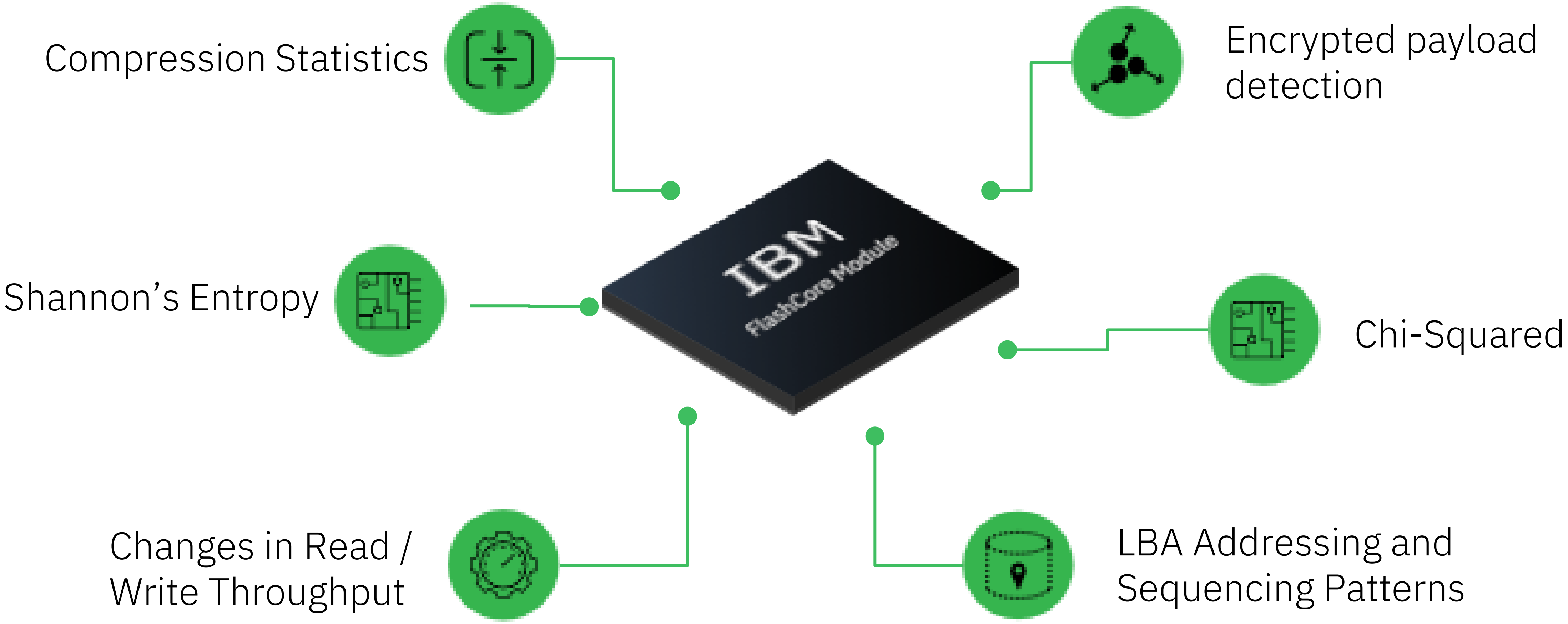
Of data modified after the attack

LBA access analysis – WannaCry - 1 hour



Ransomware Threat Detection With FlashCore Module

40+ data statistics analyzed in detection engine



Compression Statistics

Encrypted payload detection

Shannon’s Entropy

Chi-Squared

Changes in Read / Write Throughput

LBA Addressing and Sequencing Patterns

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

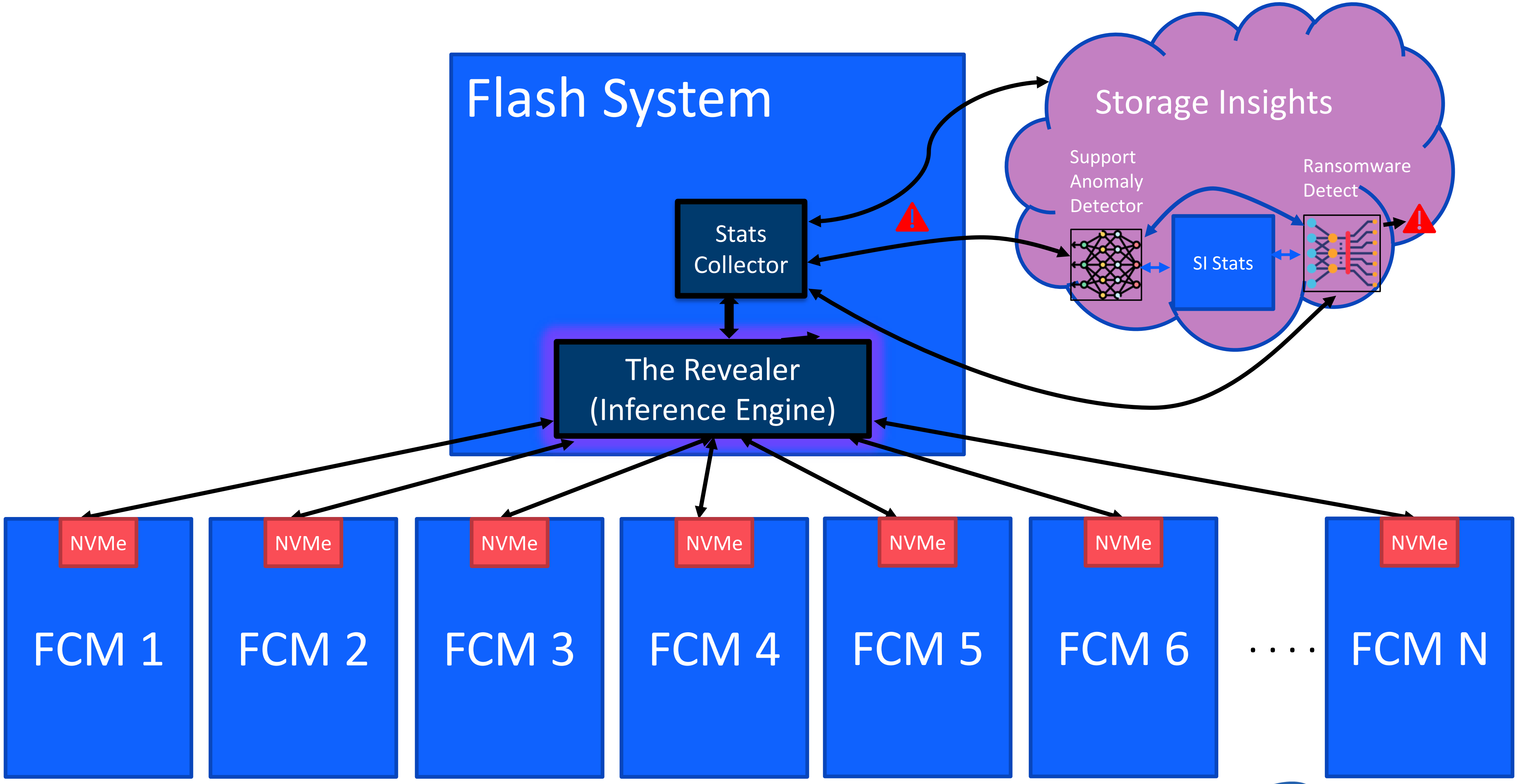
FMS the Future of Memory and Storage

IBM

FCM4 and Ransomware Threat Detection

- FCM4 calculates entropy (estimate of randomness) and change in compression on every IO
- FCM4 keeps statistics on each IO like block size, LBA , etc.
- FCM 4’s ARM cores process all this information
- All this information is statistically summarized into a relatively small amount of information per volume
- These summaries are passed every 2 seconds to an inference engine on the Flash System

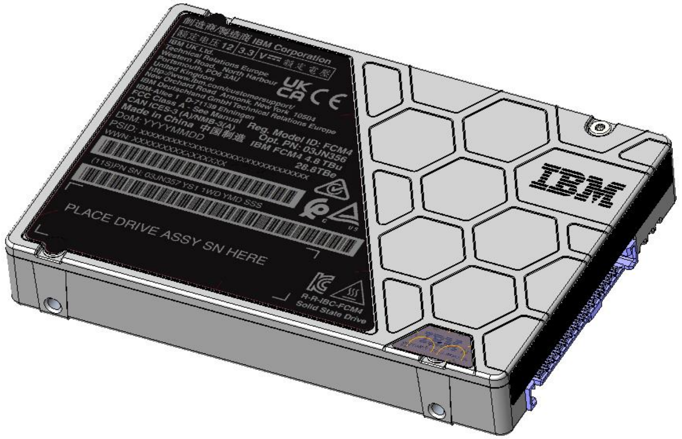
FlashSystem Ransomware Detection Conceptual Model



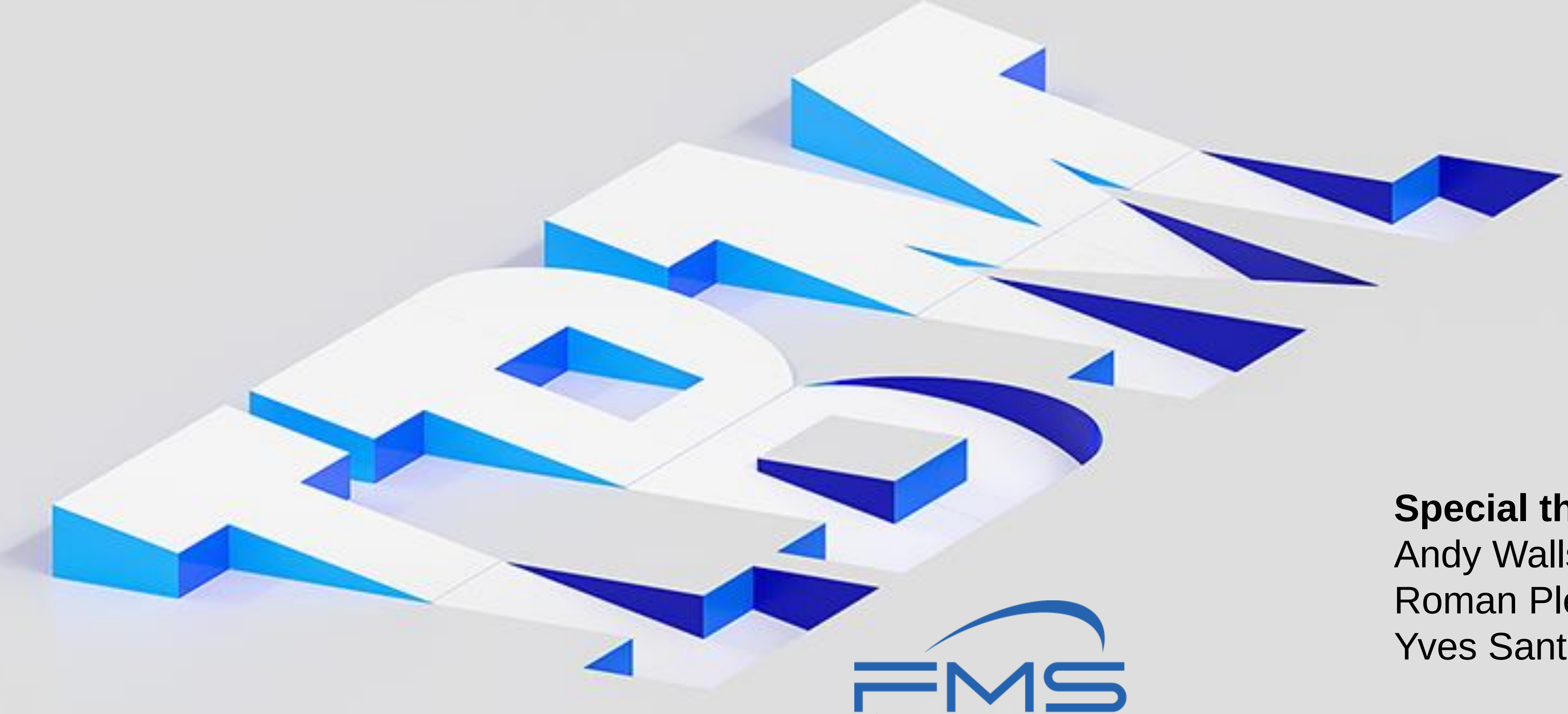
the Future of Memory and Storage

Summarizing the benefits of the FCM 4

- Compression without performance impact
  - Superior cost per effective TB
  - Superior power per effective TB
- Fully encrypted by default
- XOR assists improve RAID performance
- Enterprise storage at low cost enabled with QLC flash
- Fast Ransomware Threat Detection without performance hit
- More compute resources available for future capabilities
- FCM hardware development continues to evolve. Stay Tuned!



Thank You!



Special thanks to:
Andy Walls
Roman Pletka
Yves Santos

FMS
the Future of Memory and Storage

IBM