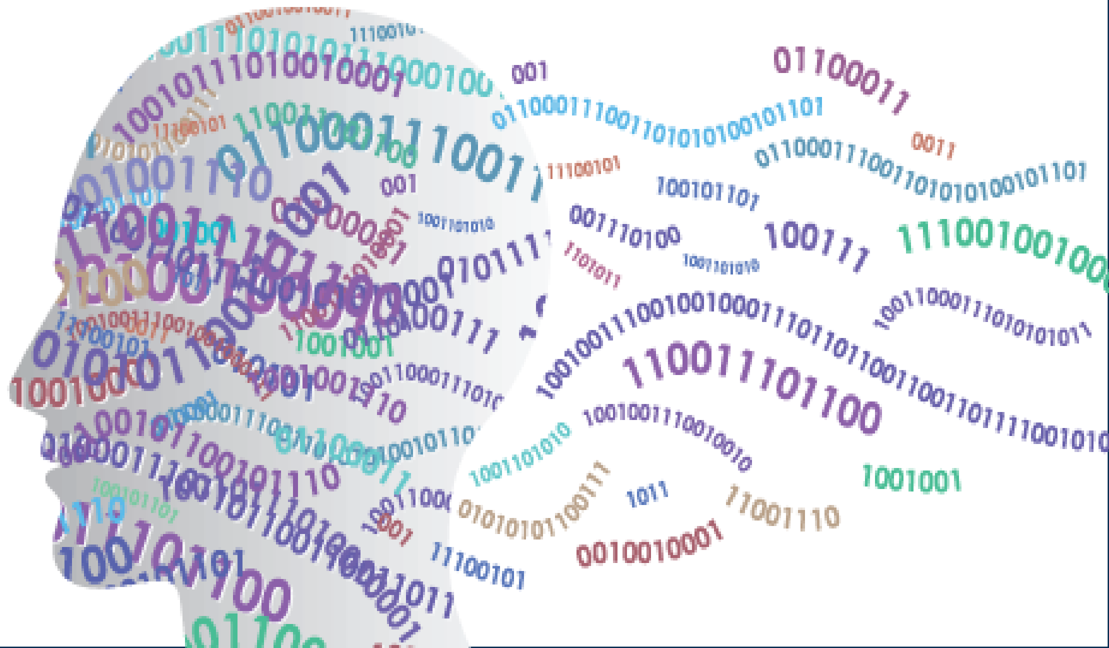
Breakthrough in Cyber Security Detection using Computational Storage

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

Solutions, Architectures, and Community

VIRTUAL EVENT, MAY 21-22, 2024



Presented by

Andy Walls

IBM Fellow, CTO FlashSystem

FCM-4

FLASHCORE MODULE 4

Designed by Ric Halsaver, Copyright IBM Corporation

Cyber Attacks are on the Rise, getting more sophisticated

2X

Cyber Attacks YTY 2022 vs 2021, 2023 YTY 2.5x so far!

51%

of Cyber Attacks are ransomware (24%) or exfiltration (27%)

23

days, average recovery after a ransomware attack

26%

clients who paid the ransom still could not recover the data

66%

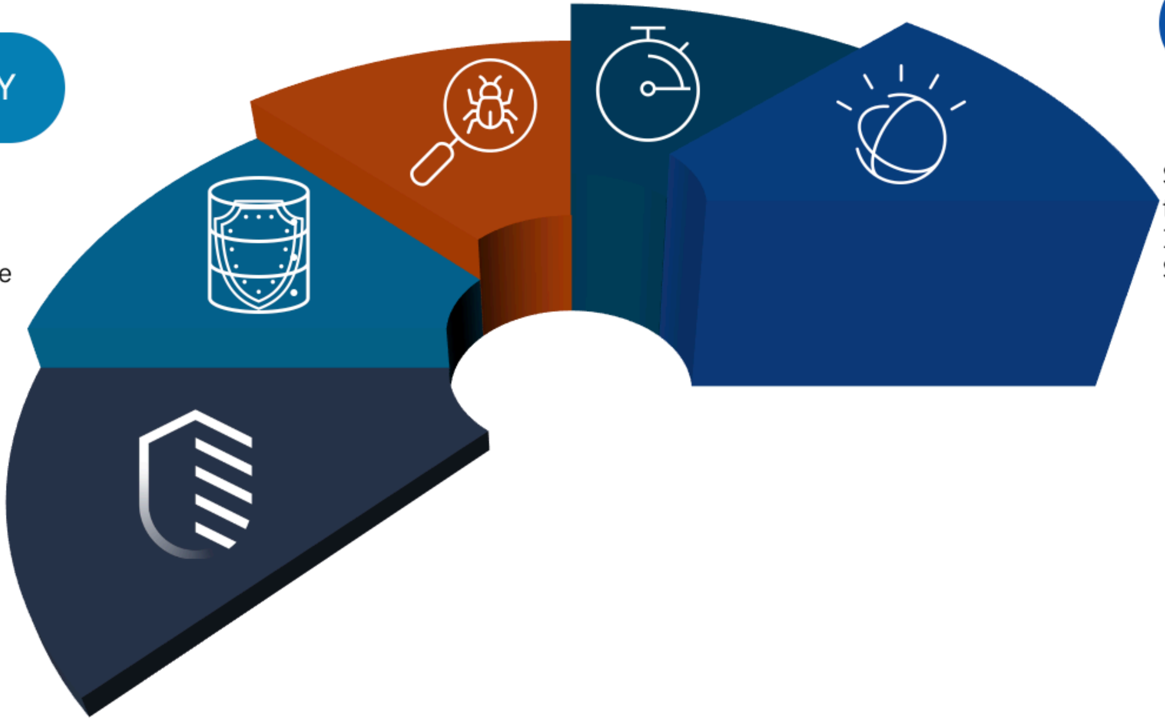
of breaches were not identified by the organization's internal security teams and tools

108

days faster identification and containment of a breach with extensive security AI & automation

Secure & Resilient

Steps to Data Resilience



SECURITY & DATA PROTECTION

01

Predict, prevent, and respond
SOC Integration
Protect from infrastructure failures and Natural disasters

IMMUTABILITY

02

Recoverable data points
Incorruptible, data can not be deleted

DISCOVERY

03

Find active threats
Find & prevent dormant threats

RECOVERY

04

Rapid operational recovery in seconds, minutes, hours
Avoid paying ransoms

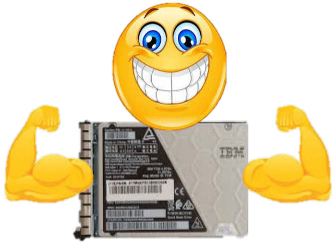
AUTOMATION & TESTING

05

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

IBM Differentiating Flash – FlashCore Module

- Figured out how to get about the same endurance out of QLC as out of TLC
- IBM gets better performance out of the QLC version than our TLC version
- Compression accelerator done in the SSD – offloads an expensive SW task
- Is a computational storage platform using FPGA today.



- **Worlds largest NVMe SSD at 38.4TB Physical.**
- **Only QLC**
- **Can store up to 115TB compressed**
- **U.2 dual port formfactor**
- **4.8, 9.6 and 19.2TB also available**

How FCM transparent compression helps

- Data reduction is transparent to the software.
- SSDs already have to remap and manage metadata and do garbage collection.
- The compression fits in nicely to the FCM architecture.
- Garbage collection and remapping done in ONE place
- Controllers then can be used for storage services and replication, etc.
- **No one else does this!**

Ransomware and other malware is becoming an epidemic! Every part of the stack needs to do its part

A Realization about Block Storage:

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

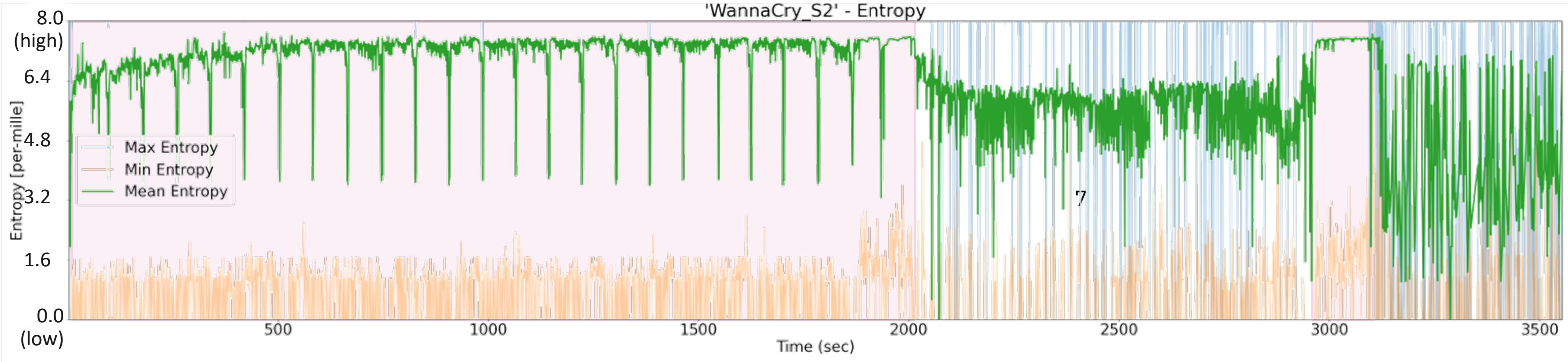
BUT: It can generate data needed for determining Ransomware attacks with less performance impact then any other part of the system

So, we started doing research into how ransomware affected systems containing FCMs

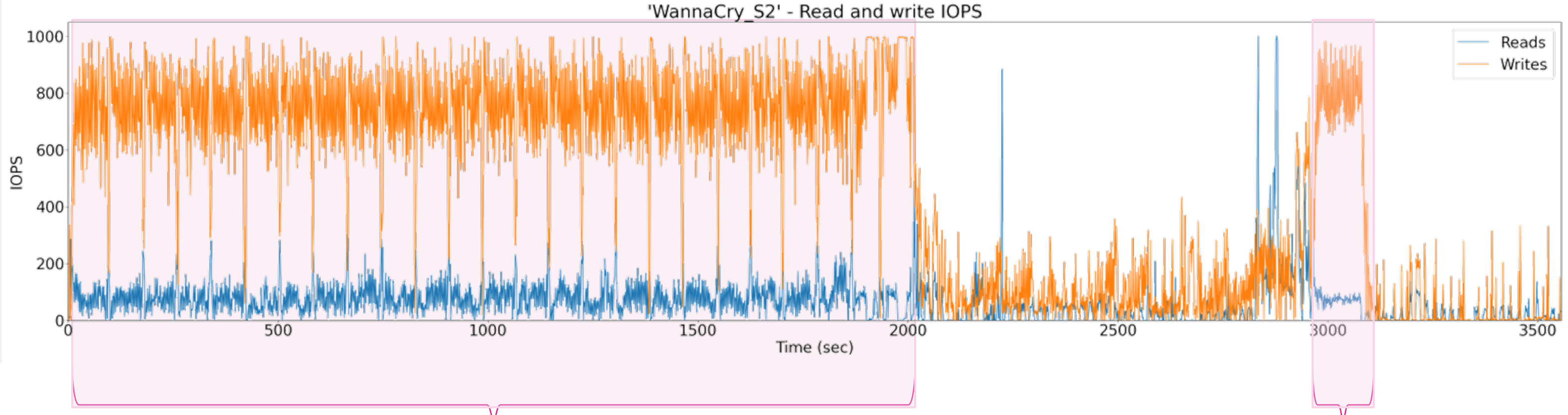
Characteristics Found in IO Traces from Ransomware

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

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

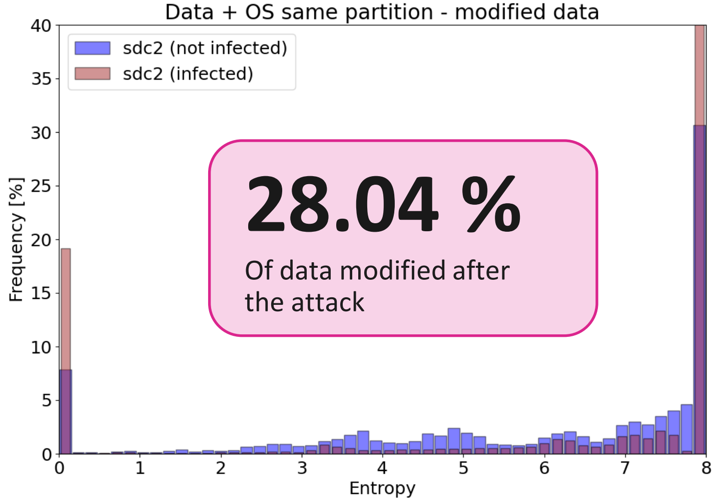


IOPS (– read, – write):



IO activity of ransomware

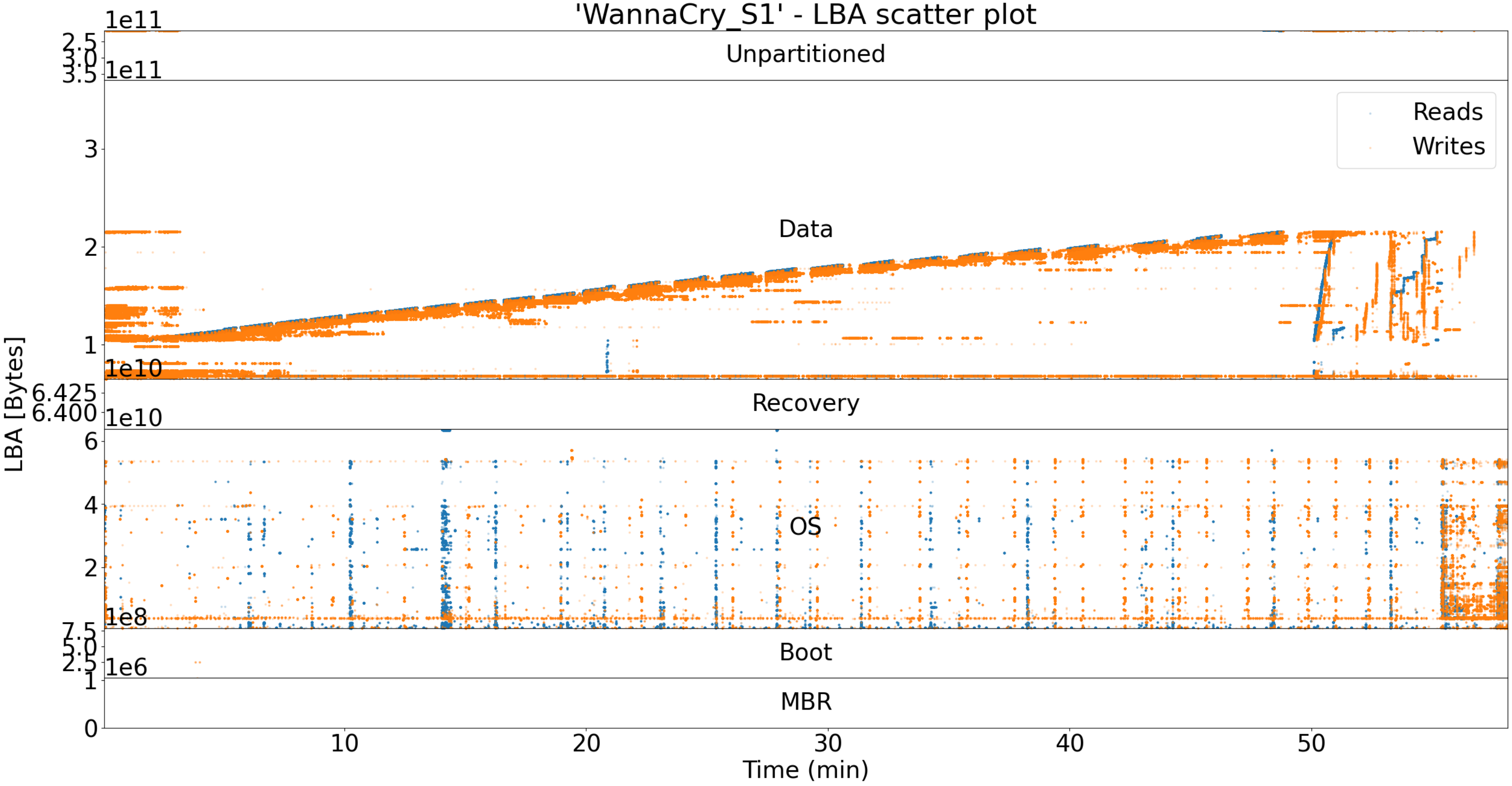
Payload encrypted – before and after attack:



28.04 %

Of data modified after the attack

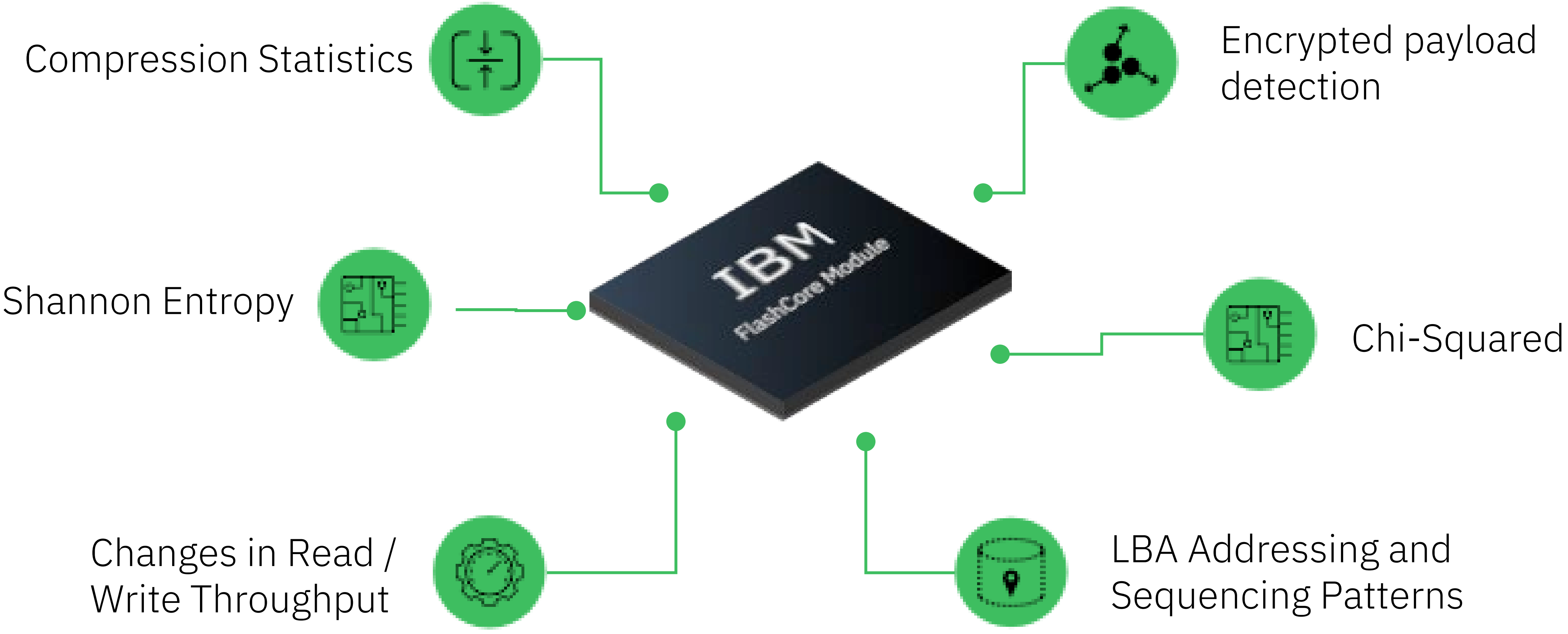
LBA Access Analysis – WannaCry - 1 Hour



Ransomware Threat Detection With FlashCore Module

40+ data statistics analyzed in detection engine

Thanks to Computational Storage Offload in the FCM



Compression Statistics

Shannon Entropy

Changes in Read / Write Throughput

Encrypted payload detection

Chi-Squared

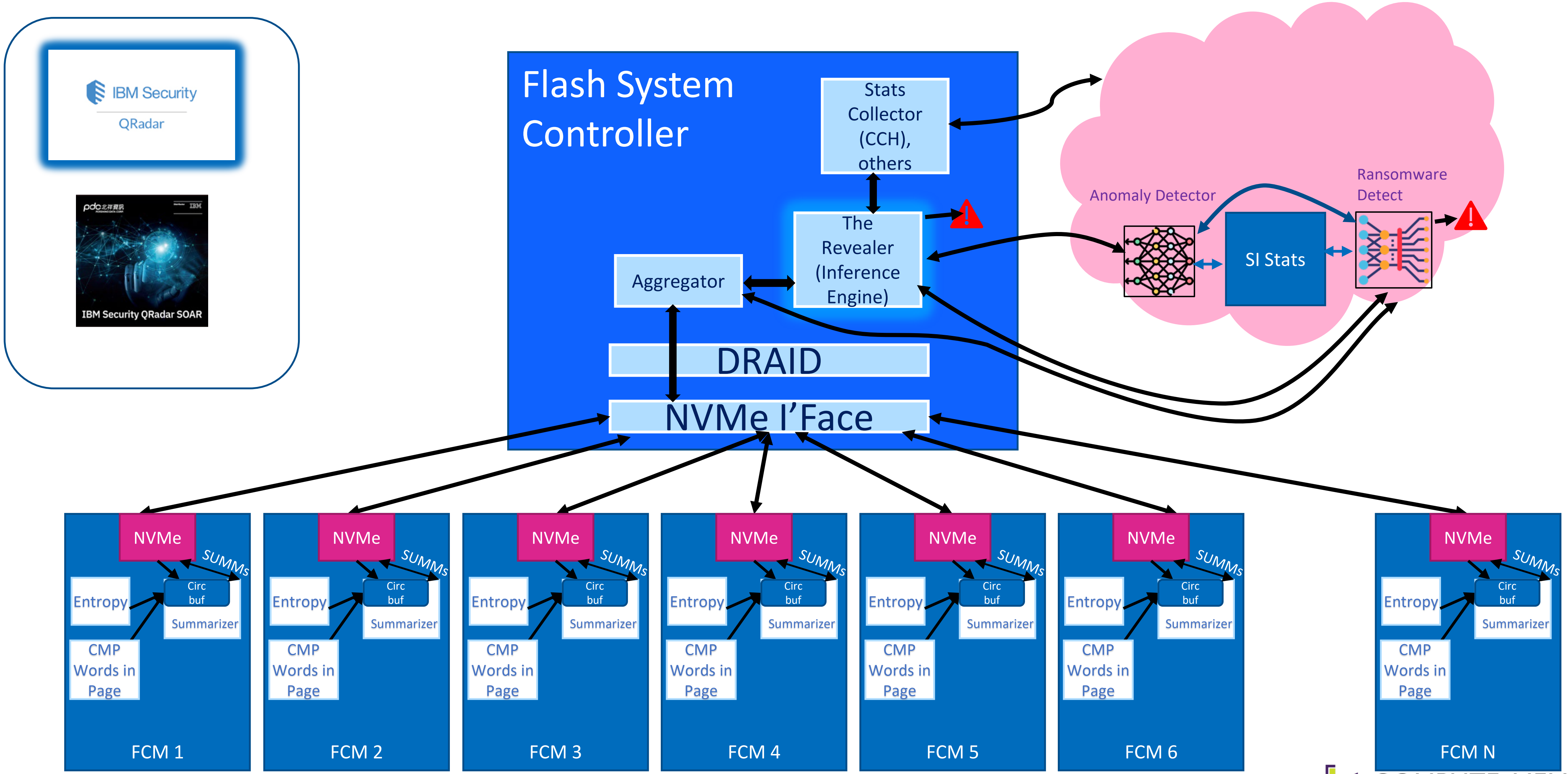
LBA Addressing and Sequencing Patterns

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

FCM4 and Ransomware Detection

- FCM4 calculates entropy (estimate of randomness) and change in compression on every IOP
- FCM4 keeps statistics on each IOP like block size, LBA , Rd
- FCM 4 has 2 small RISC 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 in Storage Virtualize.

FlashSystem Ransomware Detection Conceptual Model



Please take a moment to rate this session.

Your feedback is important to us.

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

Solutions, Architectures, and Community
VIRTUAL EVENT, MAY 21-22, 2024