SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Computational Storage: Ransomware Detection Assistance

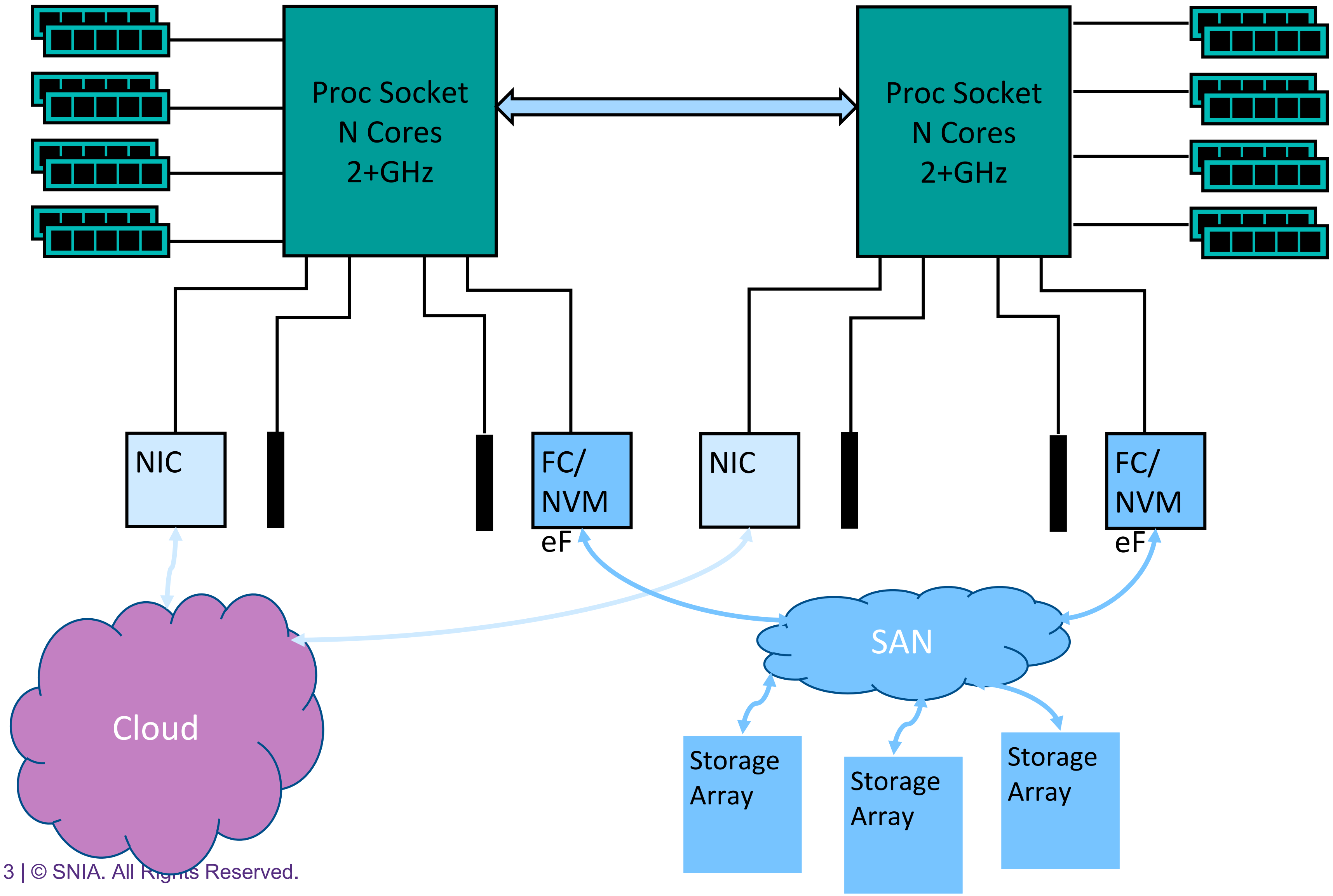
Andy Walls, IBM Fellow and CTO FlashSystem

Moore’s Law is Dead

OK. . . Maybe not dead. But it is not like it used to be!

- Growth rate of transistors and reduction in lithography continues. . . .
- But, no longer does that growth rate result in more powerful processors at the same or lower cost
- Some things like DRAM are not keeping up. . . .

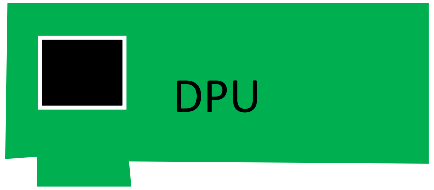
Server Block Diagram



- Sophisticated software and Powerful processors
- All the data brought into the server to be processed
- Memory BW and Network can bottleneck
- Storage mostly --- Stores

Computational Storage

The Array has powerful processor



Smart NIC and DPU are powerful and can offload from server

The SSD has spare NAND bandwidth and can offload without any performance impact.

Bandwidth in a Storage Array

Read throughput can be sustained at up to 100GB/sec

- If Servers and System can process it that fast

FAST – BUT, clogs up switches, CPUs

There is 168+GB/sec of NVMe BW inside Array

There is about 768GB/sec BW off the NAND Flash!

That BW provides tremendous potential for additional analysis

An SSD also has visibility to all the data flowing in the system

- Can Compress and Encrypt with no performance penalty
- Various checks can be made on the data – with no performance penalty
- Has intimate knowledge of access patterns, latency, types of data transfer and IOPs
- Additional Information can be passed to the SSDs about volume, file, OS.
- Trends and predictions can be intelligently made

Which makes one consider:

Although 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

Outline

- Emerging memories are inevitable
- CXL will cause great change
- Chiplets will prevail

Which makes for a very interesting computational storage application!

Realization #2:

To Be Truly Effective in detecting Ransomware
as early as possible requires coordination
between all parts of the System

- Application
- File System
- Security Software
- Block Storage

SSDs can help in early detection of malware that involves the data

- Ransomware
- Wiperware
- Mistaken deletes
- Turning encryption or compression on in application
- Exfiltration – stealing data but not hurting it.

What is Offloaded and How does it Help

- Intelligent SSDs can be given volume and other awareness
- Hints can be passed on types of data accesses
- Various checks for randomness and data transformation can be made ON THE FLY.
- Trends in changes of various data attributes can be identified
- Key access attributes can be recorded and changes can be identified
- Data can be fed into machine learning models to help identify corruption

Benefits and Important Notes

- Early discovery is everything
- Reduces window of corruption
- Thereby speeding up recovery
- Not sufficient in itself
  - Must be combined with all the other security and cyber resilience protection available and being developed!

SNIA

COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Please take a moment to rate this session.

Your feedback is important to us.