TEM: Quantum Safe Data Storage-

Threat to Data-

To protect against quantum decryption, Storage Engine, with our partner IBM, have introduced high performance flash Quantum-Safe Encryption for secure data storage needs. This technology is important to governments and commercial enterprises who should transition to quantum-resistant cryptographic algorithms before large-scale quantum computers become a reality. This quantum-resistant protection will remain compliant with NIST-selected and final standards.

Action to be taken-

EoP Memorandum M-23-02 directs, along with National Security Memorandum 10 (NSM-10) to migrate to a quantum safe cryptographic environment for all High Value Assets.

Storage Engine
Empowering The Critical Enterprise

IBM Making the IBM FCMv4 "Quantum-Resilient"

Glen Jaquette – IBM Security Lead, Office of Storage CTO

- What does it mean to be quantum-safe?
- What does Quantum Safe Cryptography (QSC) deliver?
- What are the consequences of the failure to adopt QSC?
- What's the safest way for IBM Storage to support QSC?
- How IBM’s FCMv4 SED SSD has been transitioned to use QSC?

The Problem

Conventional Public key algorithms:
*Will be **completely broken** when a Cryptographically Relevant Quantum Computer (CRQC) can apply Shor's algorithm directly*

Required Mitigation:
New algorithms and schemes needed

Symmetric key and hashing algorithms:

Impacted by quantum computing – algorithm strengths are reduced by quantum computers using Grover's algorithm

Example Mitigations:
Discontinue use of algorithms such as AES-128
Increase the key or digest sizes to 256-bit min.
(e.g. to AES-256, SHA2-256, SHA-3, etc.)

Post Quantum (PQC) = Quantum Safe (QSC) = Quantum-Resistant

The Impact

- Shor's algorithm for factoring and discrete logarithms can completely break the RSA and Diffie-Hellman cryptosystems, and their elliptic-curve-based variants
  - To address an attack using **Shor’s algorithm**, we need **new Math/Algorithms for classical computers**
- Grover’s algorithm could be used to speed up an exhaustive search for symmetric keys or reverse engineer a cryptographic hash
  - To address an attack using **Grover’s algorithm**, we need to **grow the key and message digest sizes**

Algorithm*	**Purpose**	**Impact from quantum computer**
DES, TDES, AES-128	Encryption	No longer secure
AES-256	Encryption	Secure
SHA-256, SHA-3	Hash Functions	Secure
RSA, DH	Signatures, Key Establishment	No longer secure
ECC, ECDSA, ECDH (Elliptic Curve Cryptography)	Signatures, Key Exchange	No longer secure
DSA (Finite Field Cryptography)	Signatures, Key Exchange	No longer secure
LMS & XMSS	Stateful Hash-based signatures	Secure

Quantum-safe – So what? Why is the time to act now?

- *There are new attack vectors that did not exist before*
- *"Secure" Data is being recorded today with the intent of exposing it tomorrow*
  - Data communications over TLS that are being eavesdropped (a.k.a. harvested)
  - Snapshots of encrypted cloud data taken
  - Encrypted data can be exfiltrated during a data breach
  - Systems storing bulk encryption keys wrapped with public key encryption keys
  - Storage media that is not encrypted with quantum-safe encryption methods and is then lost, stolen, or improperly disposed of

- Crypto algorithms can be broken instead of just being bypassed.
- New protections are needed in areas were crypto is used
  - Data that must be protected for a long time must be encrypted properly to protect from "Harvest now, decrypt later" attacks
  - Potential attacks have already started.
  - Public key use cases like authentication must be revisited and updated to use new cryptographic algorithms and schemes

- Markets wanting to become QS in near future:
  - Government agencies
  - Financial institutions
  - Healthcare services

Progress: Quantum-safe cryptography NIST Selections

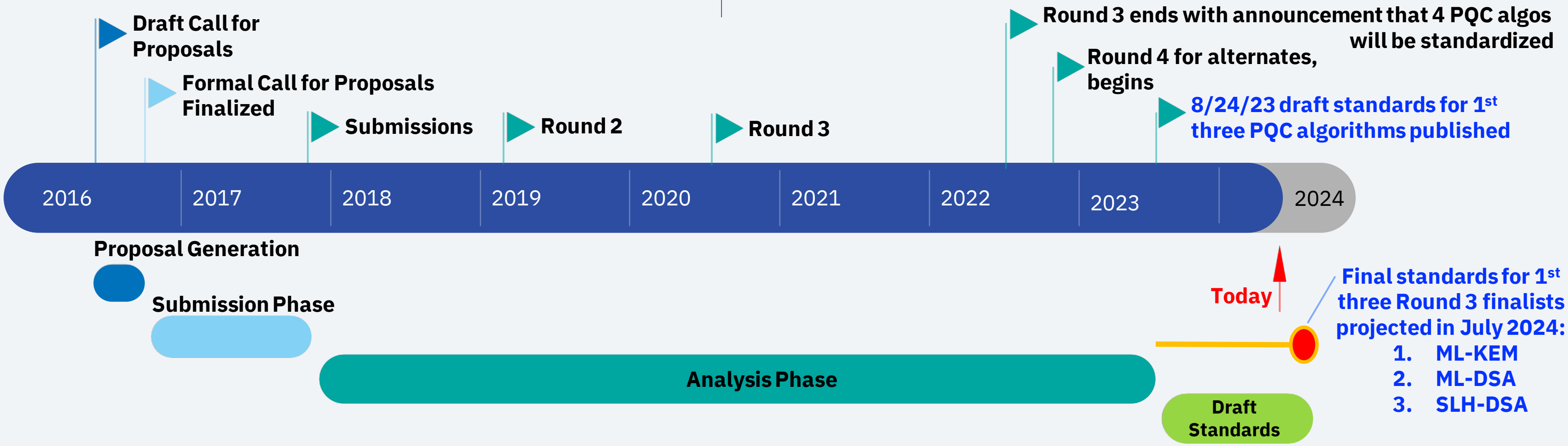
Algorithms NIST has selected for standardization

Key Encapsulation Mechanism, or KEM (enabling symmetric key establishment)

- CRYSTALS–Kyber^* => NIST's "ML-KEM"

Digital Signatures Algorithms, or DSA

- CRYSTALS–Dilithium^* => NIST's "ML-DSA"
- SPHINCS+ => NIST's "SLH-DSA"
- FALCON* => NIST's "FN-DSA"


Draft Call for Proposals
Formal Call for Proposals Finalized
Submissions
Round 2
Round 3
Round 3 ends with announcement that 4 PQC algos will be standardized
Round 4 for alternates, begins
8/24/23 draft standards for 1st three PQC algorithms published
2016
2017
2018
2019
2020
2021
2022
2023
2024
Proposal Generation
Submission Phase
Analysis Phase
Today
Draft Standards
Final standards for 1st three Round 3 finalists projected in July 2024:
1. ML-KEM
2. ML-DSA
3. SLH-DSA

^ NIST has designated ML-KEM and ML-DSA as their primary PQC standards for KEM and DSA respectively

** IBM Research helped to develop these three lattice-based PQC algorithms selected by NIST for standardization.*

Quantum Safe Migration – increasing focus, timeline, and hybrid

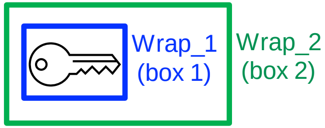
Milestones

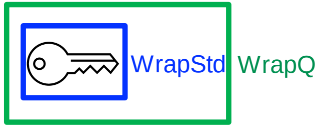
Increasing focus on QSC migration:

- **January 2022 White House memo requires US federal agencies to begin preparing for migration to QSC**
- **NIST's SP 800-56C Rev. 2 allows for "hybrid" (i.e. conventional + QSC) key-establishment usage by FIPS modules**
- **Hybrid use of conventional and QSC algorithms is only as weak as the stronger of the two underlying algorithms**
- **Hybrid implementations are FIPS validate-able now, without having to wait for final NIST Standardization**
- **BSI (Germany) and ANSSI (France) recommend the use of hybrid cryptography in high security applications**
- **Where we can, IBM Storage will use hybrid implementations of QSC to achieve the highest level of security**

IBM Quantum's Condor demo'd 1121 qubits (qb), announced 12/4/23
IBM's Quantum Roadmap: https://www.ibm.com/quantum/technology

"*There is a* ***1 in 7 chance that fundamental public-key crypto will be broken by quantum by 2026****, and a 1 in 2 chance of the same by 2031.*" - -Dr. Michele Mosca, University of Waterloo, Canada, in a 1/25/23 Forbes article "Quantum Safe Cryptography – A Quantum Leap Needed Now"





IBM zSystems security innovation driven by a platform strategy

April 7th, 1964 – April 5th, 2022
4 Generations of Technology
12 Families of Innovation

IBM
z14™

Crypto Express6s
CPACF

IBM
z15™

Crypto Express7s
CPACF
Compression

IBM
z16™

IBM Telum Processor

Crypto Express8s

CPACF
Compression

IBM zSystems Security Leadership

Approach: Security integrated into all levels of the stack	Data Protection	Data Privacy Confidential Computing	Cyber Resiliency Continuous Compliance Quantum Safe

Examples of Quantum Safe Migration of IBM Storage devices

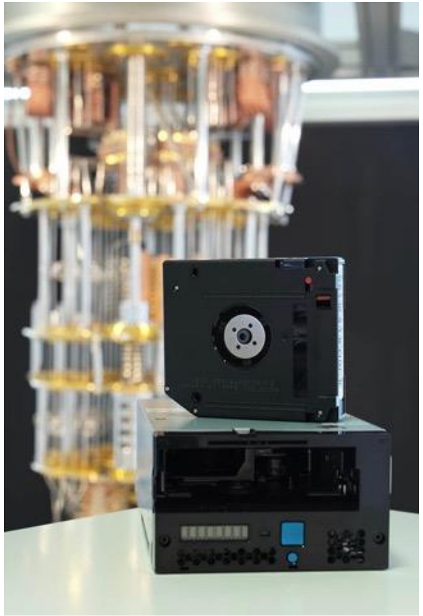
Quantum Safe Migration Example: Tape

In 2019, IBM announced a prototype of the world’s first quantum safe tape drive. Implemented in firmware of TS1160 tape drive.

Uses lattice-based cryptography:

- CRYSTALS-Kyber for secure key transport between tape drive and key manager
- CRYSTALS-Dilithium signatures for authentication and firmware verification

- Data encryption on tape with GCM-AES-256*
- In Dec. '21 we announced support for AES Key Wrap of EEDKs to make Jag cartridge QS, making BPX to now require secret key sharing



* a quantum computer capable of breaking AES-256, at least with any algorithm known today (including Grover's), is likely decades away

Quantum Safe Migration Example: FCM

In 2024, IBM released a new version of our FlashCore Module (FCM) which is "quantum-safe”:

The FCMv4 uses hybrid implementation in both applications of asymmetric cryptography including PQC cryptographic algorithms:

- Hybrid use of CRYSTALS-Kyber for secure key transport of unlock PIN transmitted by FlashSystems storage controller to FCM
- Hybrid use of CRYSTALS-Dilithium signatures for verification of firmware authenticity

- Bulk data encryption on customer data written to flash memory by use of XTS-AES-256*

* a quantum computer capable of breaking AES-256, at least with any algorithm known today (including Grover's), is likely decades away at least

Summary

Classic Asymmetric Cryptographic Algorithms are widely used to protect data and communications in computer systems and networks.

An adversary with access to a sufficiently strong quantum computer can more easily break many classical algorithms we have used for many years.

Risks include theft of digital assets, forged documents, transactions, signatures, code, and the like. Secure communications are also in jeopardy and some are being recorded now.

Researchers and standards bodies are moving to address the threats, by standardizing new quantum-safe cryptographic algorithms that can be used to protect computer workloads and secured data from the attacks that can be launched from quantum computers.

IBM Storage products should:

- **Prepare** to transition to hybrid use of QSC
  - QS education of Prod. Mgmt, Dev, & Test
- **Discover** all usage of vulnerable crypto (e.g. by use of HRL's CBOM/SBOM tool where necessary):
  - Any classic asymmetric, or insufficiently strong (i.e. <256 bit) symmetric, crypto
- **Transformation**
  - Plan transition to use of updated crypto-libraries (e.g. CLiC, GSKit, OpenSSL, etc.) & use of QSC algorithms & QSC signed firmware
- **Observability**
  - Extend existing processes (e.g. piggyback on SPbD & PSIRT) to continuously monitor products for use of vulnerable cryptography

Deployment Model of Quantum Safe Flash Data Storage for High-Performance Secure Data Storage

Trevor Savino – SEI Enterprise Solutions Architect

With
Andy Walls - IBM Fellow and CTO and Chief Architect of Flash Systems

IBM Storage FlashSystem Family of Storage Arrays

Features and Benefits of the FlashSystem platform for DISA and Mission Partners

June 2024

IBM FlashSystem Ransomware Threat Detection Pipeline

1\.

IBM FlashCore modules collect and analyse 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

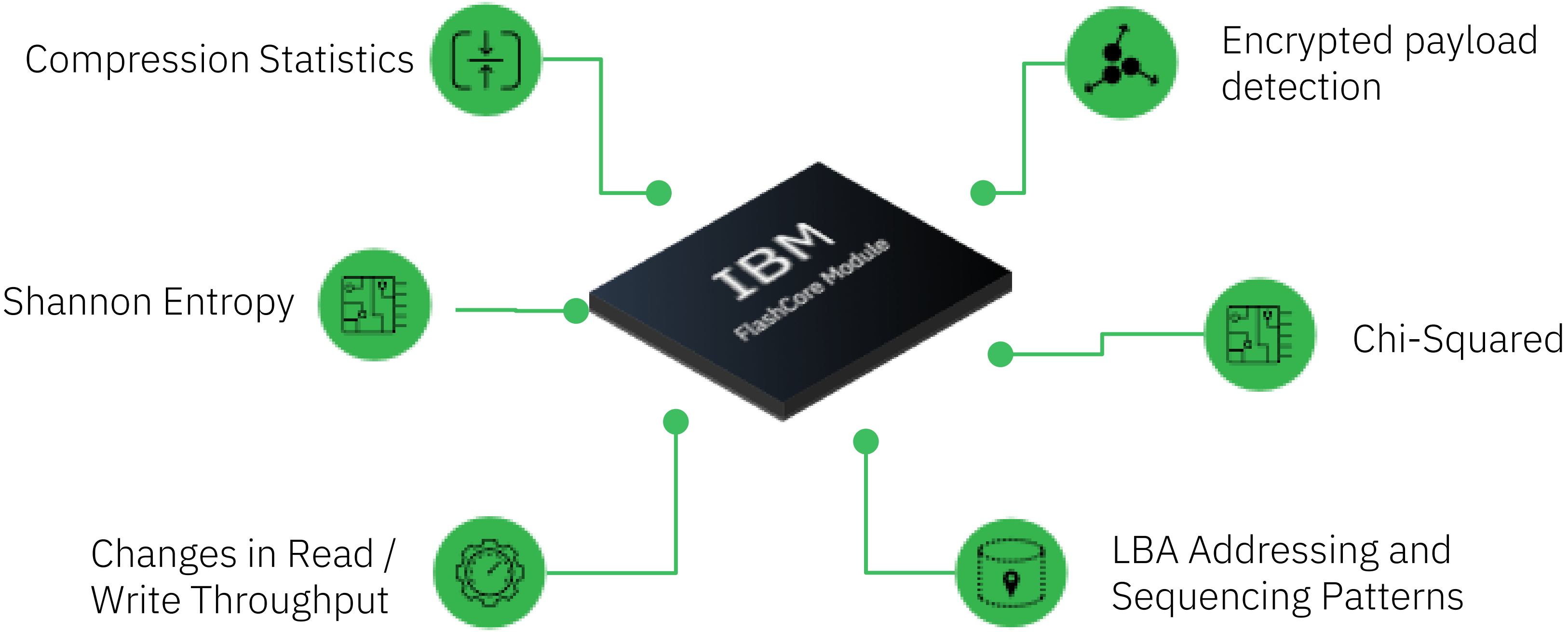
Automated Response

3\.

Threat information from connected FlashSystems, alerts users and triggers SIEM/SOAR software to initiate a response

Ransomware Threat Detection With FlashCore Module

30+ data statistics analysed in detection engine



Compression Statistics

Encrypted payload detection

Shannon Entropy

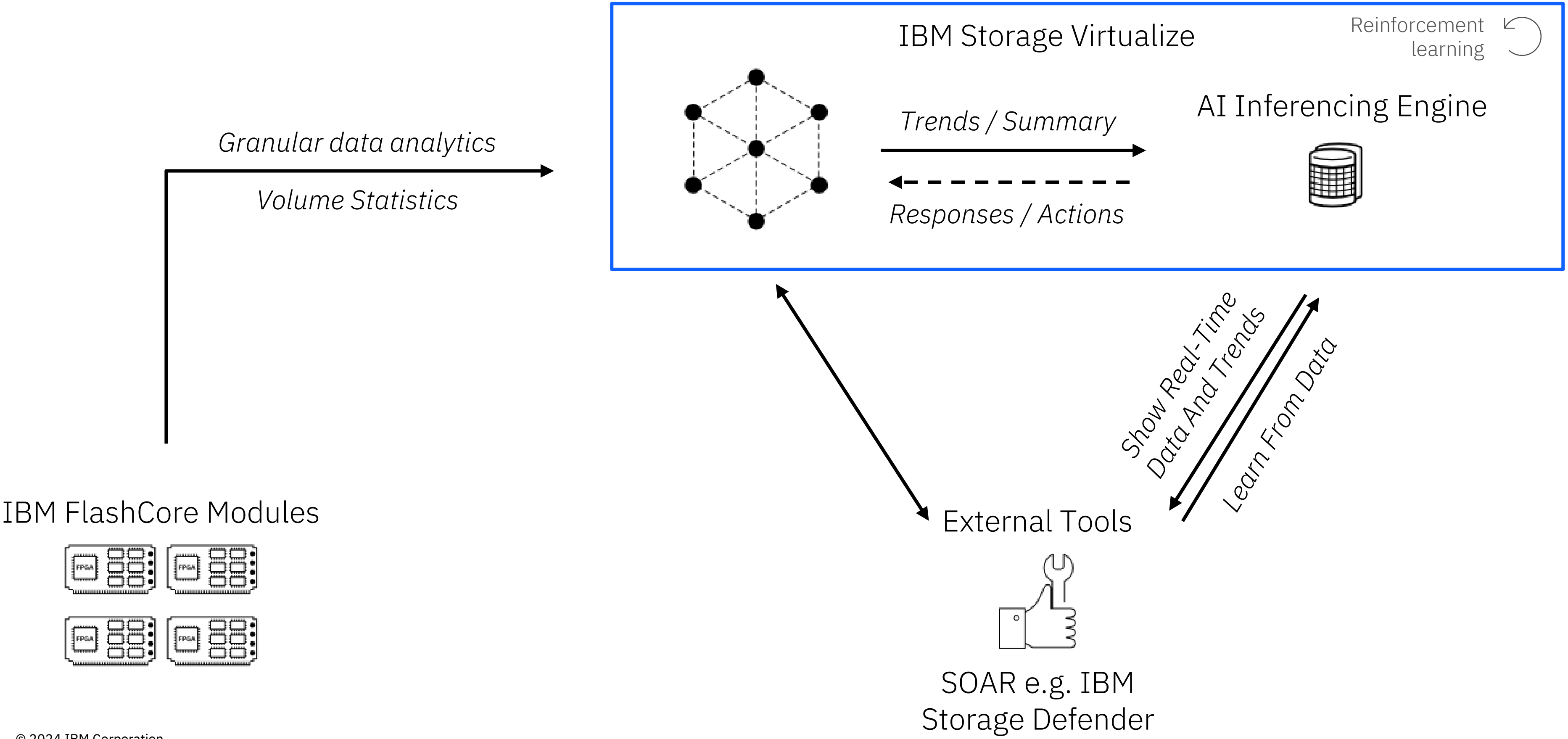
Chi-Squared

Changes in Read / Write Throughput

LBA Addressing and Sequencing Patterns

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

Ransomware Monitoring Architectural Overview



Storage Virtualize Safeguarded Copy provides Cyber Resiliency against a cyber attack

Protect against cyber attack

- ***Immutability***: Safeguarded Copy for immutable point-in-time copies of production data
- ***Isolation***: Air Gap “offline by design”

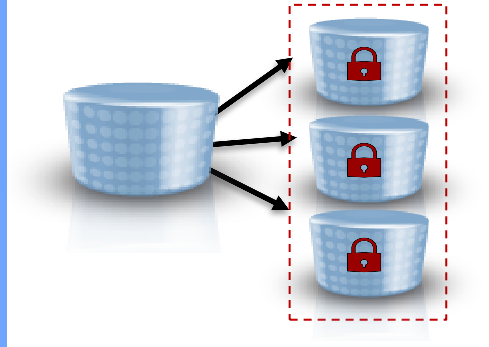
Up to

32,100

Objects to provide immutable point-in-time copies of data

Fast restore from Primary Storage

Prevents modification or deletion of sensitive point-in-time copies due to user error, malicious destruction, or ransomware attack



IBM Storage Sentinel

Automated Cyber Resilience and Recovery

Protect	Isolated & Immutable Snapshots
Verify	Automated Anomaly Scanning Engine
Recover	Safe Recover Point Identification Rapid Data Recovery

June 2022
Epic x86

Sept 2022
SAP HANA x86, PowerLinux

4Q 2022
SAP HANA RH8.4
HyperSwap

1H 2023
Epic ORACLE SGC2
POWER
AIX,

2023+
vmware Microsoft SQL Server

Storage Sentinel Analytics

Full content analytics provide comprehensive insight into data

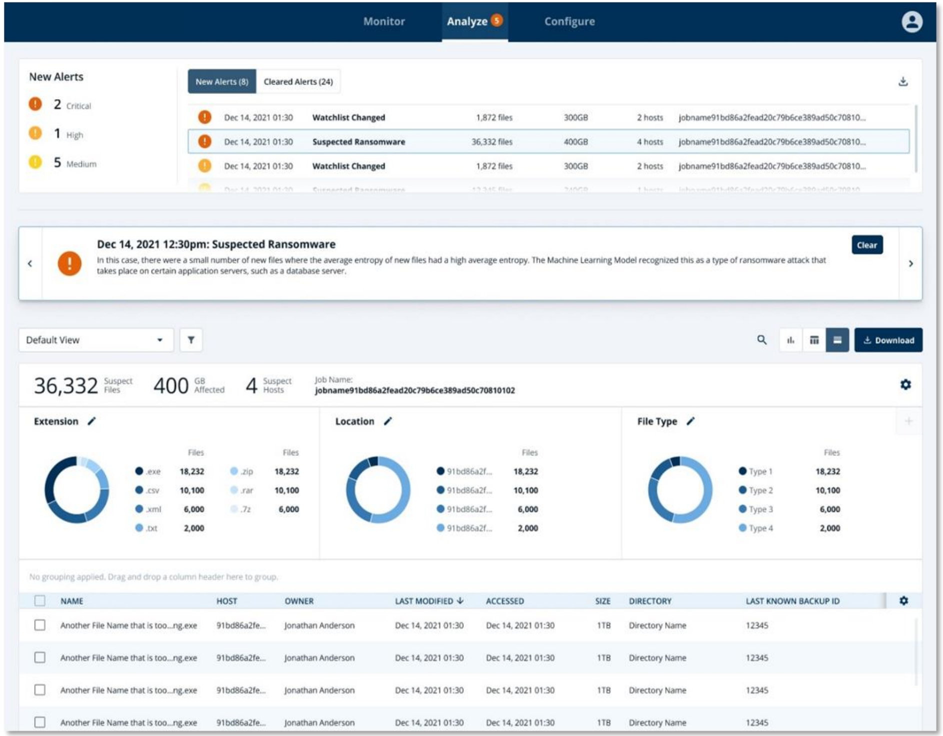
Compares snapshots over time to detect unusual patterns due to a cyber attack

200+ analytics that are indicative of corruption due to a ransomware attack

The only cyber analytics solution that inspects file metadata and content

Machine learning models that have been trained on thousands of variants

99.5% confidence in detecting corruption



New Alerts

2	Critical
1	High
5	Medium

●	Dec 14, 2021 01:30	Watchlist Changed	1,872 files	300GB	2 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...
●	Dec 14, 2021 01:30	Suspected Ransomware	36,332 files	400GB	4 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...
●	Dec 14, 2021 01:30	Watchlist Changed	1,872 files	300GB	2 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...

Dec 14, 2021 12:30pm: Suspected Ransomware

In this case, there were a small number of new files where the average entropy of new files had a high average entropy. The Machine Learning Model recognized this as a type of ransomware attack that takes place on certain application servers, such as a database server.

36,332 Suspect Files 400 GB Affected 4 Suspect Hosts Job Name: jobname91bd86a2fead20c79b6ce389ad50c70810102

Extension

	Files		Files
● .exe	18,232	● .zip	18,232
● .csv	10,100	● .rar	10,100
● .xml	6,000	● .7z	6,000
● .txt	2,000		

Location

	Files
● 91bd86a2f...	18,232
● 91bd86a2f...	10,100
● 91bd86a2f...	6,000
● 91bd86a2f...	2,000

File Type

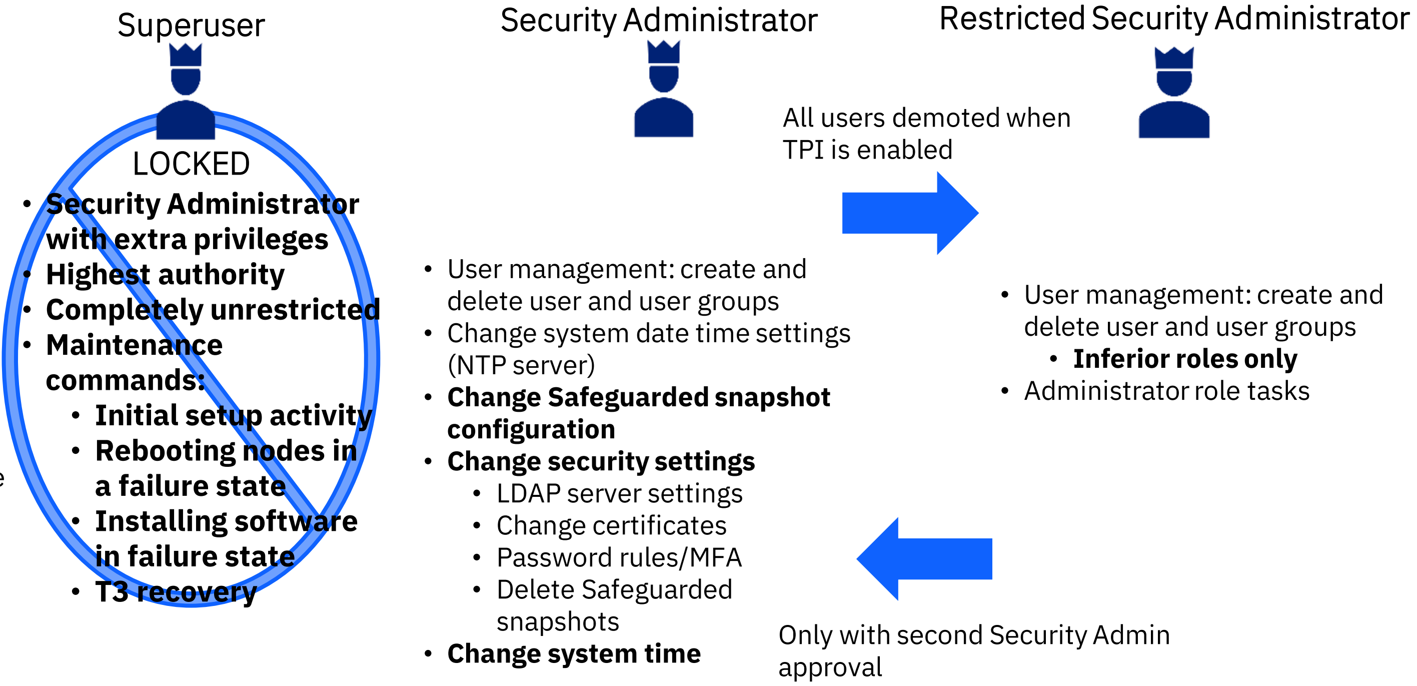
	Files
● Type 1	18,232
● Type 2	10,100
● Type 3	6,000
● Type 4	2,000

No grouping applied. Drag and drop a column header here to group.

□	NAME	HOST	OWNER	LAST MODIFIED ↓	ACCESSED	SIZE	DIRECTORY	LAST KNOWN BACKUP ID
□	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345
□	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345
□	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345
□	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345

Two Person Integrity (TPI): Time Based User Promotion

- System wide setting (on/off)
- Locks the superuser account
- Changes Security Admin users to Restricted Security Admin role which has privileges similar to Administrator
- Only Restricted Security Admin users can be elevated to Security Admin role and it is time limited
- Approvers can only have Restricted Security Admin or Security Admin role
- Approver can specify the time limit for the elevated privileges
- System enforces a maximum time allowed for elevated privileges of 24 hours
- Works with remote or local users
- Maximum of 4 elevated users at a time



Superuser

LOCKED

- **Security Administrator with extra privileges**
- **Highest authority**
- **Completely unrestricted**
- **Maintenance commands:**
  - **Initial setup activity**
  - **Rebooting nodes in a failure state**
  - **Installing software in failure state**
  - **T3 recovery**

Security Administrator

- User management: create and delete user and user groups
- Change system date time settings (NTP server)
- **Change Safeguarded snapshot configuration**
- **Change security settings**
  - LDAP server settings
  - Change certificates
  - Password rules/MFA
  - Delete Safeguarded snapshots
- **Change system time**

Restricted Security Administrator

- User management: create and delete user and user groups
  - **Inferior roles only**
- Administrator role tasks

All users demoted when TPI is enabled

Only with second Security Admin approval

Enhanced Security Capabilities

- IBM Storage devices and software provide **dual authorization and temporary authorization elevation** so no single administrator (or compromised administrative account) can destroy data.
- IBM Storage devices and software **support Multi-Factor Authentication, data complexity/age/reuse rules and integration with security directories, but still allows local accounts in an emergency.**
- IBM Storage devices and software **prevent data deletion even using multiple compromised accounts**.
- IBM Storage Defender components can be configured following **“Least Privilege”** practices and **separate security domains** for different copies of data.

In summary, the storage and data protection environment should be configured to be at least as secure as the data being protected and be able to operate under a variety of attack or disaster scenarios.

Quick Comparison of FlashSystem Family

	FlashSystem 5015	FlashSystem 5045	FlashSystem 5300	FlashSystem 7300	FlashSystem 9500	FlashSystem 9500R
All-Flash and/or Hybrid	AF √ - H √	AF √ - H √	AF √ - H √	AF √ - H √	AF √ - H ✗	AF √ - H ✗
Max cache per control enclosure	64GB	64GB	512GB	1.5TB	3.0TB	3.0TB x 2
Host adapter slots per control enc.	2	2	4	6	12	12 x 2
Storage Class Memory support	No	No	Yes	Yes	Yes	Yes
NVMe SSDs and IBM FCMs	No	No	Yes	Yes	Yes	Yes
NVMe-oF support	No	No	Yes	Yes	Yes	Yes
SAS SSDs and SAS HDDs	√ and √	√ and √	√ and √	√ and √	√ and ✗	√ and ✗
Support for SAS devices	Yes – Control & Exp.	Yes – Control & Exp.	Yes – Expansion	Yes – Expansion	Yes – Expansion	Yes – Expansion
Max physical capacity raw in 1U, 2U or 4U control enclosure	720TB	720TB	460.8TB	921.6TB	1843.2TB	1843.2TB x 2
Max usable effective with DRAID in 1U, 2U or 4U control enclosure	573TB	573TB	1PB* Or up to 2.3PB*	2.3PB* Or up to 4.6PB*	4.5PB* Or up to 9.2PB*	4.5PB* x 2 Or up to 9.2PB* x 2
Maximum capacity with clustering	NA	32PB (2-way)	32PB (2 to 4-way)	32PB (2 to 4-way)	32PB (2 to 4-way[1])	32PB (2-way)
Data Reduction	None	Software DRP	FCM4 (no impact) DRP (Hdw assist)	FCM4 (no impact) DRP (Hdw assist)	FCM4 (no impact) DRP (Hdw assist)	FCM4 (no impact) DRP (Hdw assist)
Installation and support	Customer set-up with Storage Expert Care options	Customer set-up with Storage Expert Care options	Customer set-up with Storage Expert Care options	Customer set-up with Storage Expert Care options	IBM install, w/ storage expert care options	IBM install, w/ storage expert care options
Hardware Encryption (FIPS 140-3 Ready)	NO	NO	Yes	Yes	Yes	Yes

* With 3:1 data reduction via FCM

← All-Flash and Hybrid

All-Flash Only →

[1] Four-way via RPQ

FlashSystem - Enhanced Data Resilience

FCM4 Enhancements

- Observability for every I/O - **no performance impact!**
- Ransomware threat **detection in seconds**
- **On-prem** inference engine
- FIPS 140-3
- Quantum Safe encryption
- Available on FlashSystem 5300, 7300, 9500

Policy-Based High Availability

- High performance mirroring between completely independent systems
- Up to 5X higher performance
- Replication between any level Flash System Array

Data resilience made easy

- Two person Integrity (time-based user promotion)
- Orchestrated application aware data integrity validation

Energy Efficiency, guaranteed.

Highly Available

100% data available guarantee

Rapid Recovery

guaranteed recovery of immutable snapshot

Storage Engine
Empowering The Critical Enterprise

IBM®

Takeaway:

1. **High-Performance Quantum Safe Data Storage is available now.**
2. **Time is of the essence in the high-stakes game of cybercrime.**

All follow-up can be directed to:

John Gallaway, III
SEI – Federal Sales for Quantum
Phone: 301-834-1560
Email: John.gallaway@storageengine.com

Additional Information

IBM Storage FlashSystem

Ransomware Threat Detection Overview

Story All organizations are facing increased threats to their data from cyber attacks. Many geographies are introducing cyber-security related regulations to ensure businesses have robust protections in place.

The need to be prepared is crucial, or the financial and legal implications could be very significant.

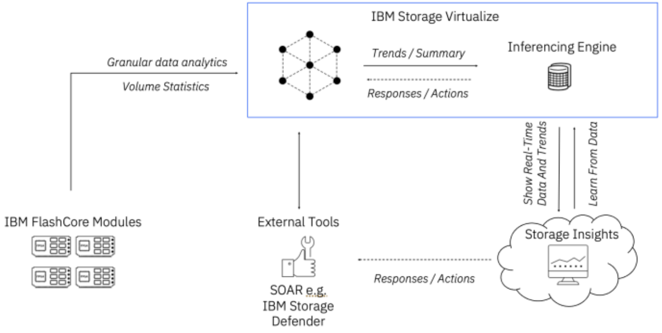
Being able to detect cyber threats as early as possible enables fast response to attacks, reducing the amount of data that needs to be recovered and minimizing business impact.

IBM's Solution

IBM Storage FlashSystem provides resilient data storage to protect, discover and recover in the event of a cyber-attack.

With AI inline inferencing and machine learning models, IBM FlashSystem with FlashCore Module 4 (FCM4) offers leading edge computational storage capable of identifying ransomware threats in real-time without compromising performance by learning and analyzing workload anomalies that include, but are not limited to, changes in compression ratio, encryption level, data entropy, and various data access patterns.

IBM Storage Insights Pro collects threat information from connected FlashSystem devices, alerting users to initiate a response, and feeding back statistics to improve AI models.



Key Differentiators

- IBM's unique computational storage technology with FCM4 means FlashSystem can collect and analyze data patterns and statistics associated with ransomware attacks on every I/O with no performance impact. 30+ statistics analyzed every 2 seconds
- The FlashSystem threat detection AI model has been tested and trained against ransomware from prevalent groups such as LockBit, BlackBasta and Conti, and is capable of detection in less than a minute
- IBM Storage FlashSystem uses AI reinforcement learning to improve cyber-threat detection over time
- FlashSystem helps you discover and respond to threats quicker, with alerts across systems through Storage Insights Pro cloud-based AIOps platform
- In the event of an attack, recover a Safeguarded Copy of data in 60 seconds or less, we guarantee it
- FlashSystem provides AI-powered Cyber Resiliency For All across our portfolio of NVMe storage systems, to suit all business sizes: 5300, 7300 & 9500

Availability

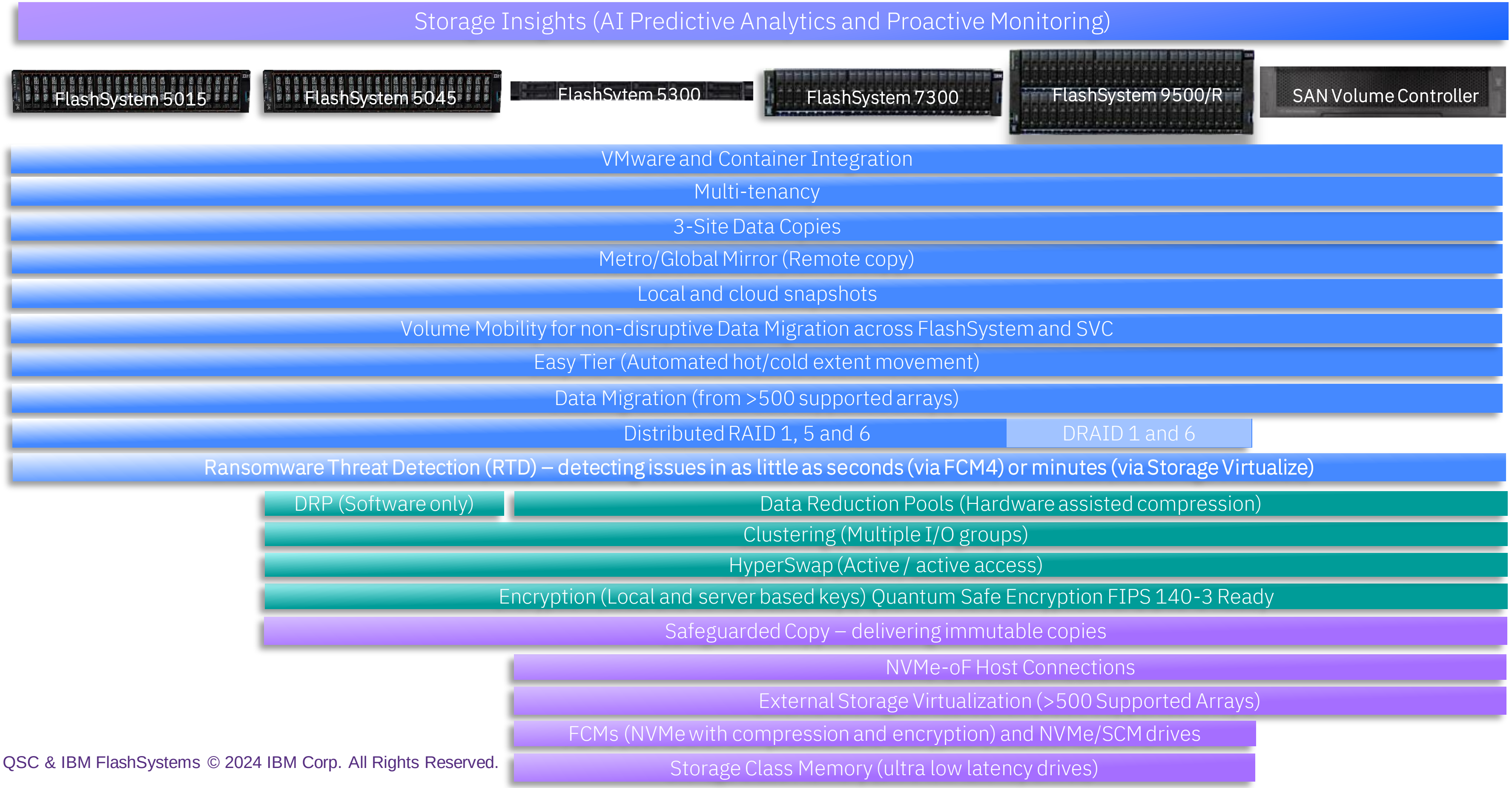
Supported platforms:
IBM FlashSystem 5300, 7300, 9500

The ransomware threat detection feature requires:

- An all-FCM4 array with firmware 4.1
- Storage Virtualize 8.6.3
- Storage Insights Pro

Storage Virtualize Across The Family

IBM Storage Virtualize



Storage Insights (AI Predictive Analytics and Proactive Monitoring)

FlashSystem 5015

FlashSystem 5045

FlashSytem 5300

FlashSystem 7300

FlashSystem 9500/R

SAN Volume Controller

VMware and Container Integration

Multi-tenancy

3-Site Data Copies

Metro/Global Mirror (Remote copy)

Local and cloud snapshots

Volume Mobility for non-disruptive Data Migration across FlashSystem and SVC

Easy Tier (Automated hot/cold extent movement)

Data Migration (from >500 supported arrays)

Distributed RAID 1, 5 and 6

DRAID 1 and 6

Ransomware Threat Detection (RTD) – detecting issues in as little as seconds (via FCM4) or minutes (via Storage Virtualize)

DRP (Software only)

Data Reduction Pools (Hardware assisted compression)

Clustering (Multiple I/O groups)

HyperSwap (Active / active access)

Encryption (Local and server based keys) Quantum Safe Encryption FIPS 140-3 Ready

Safeguarded Copy – delivering immutable copies

NVMe-oF Host Connections

External Storage Virtualization (>500 Supported Arrays)

FCMs (NVMe with compression and encryption) and NVMe/SCM drives

Storage Class Memory (ultra low latency drives)

IBM FlashSystem 9500

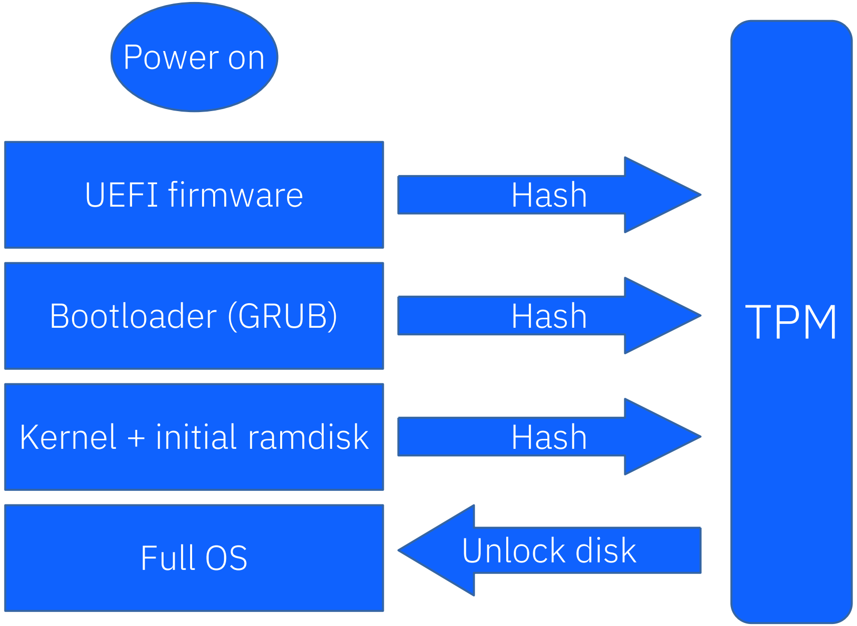
Dual Active-Active Array Controllers with 48 dual-ported NVMe Flash bays

- Two 24-core Ice Lake CPUs per controller
- 96-cores per system
- Up to 3TB of cache per system
- “Hero Numbers” are up to 8M IOPS and 100GB/s per system
- Ability to cluster up to 4 systems

- Up to 12 Storage Class Memory (SCM) drives to accelerate workloads
- Up to 48 NVMe FCM4 with hardware Compression
- Up to 48 NVMe industry standard SSDs
- Ability to intermix all three drive types within the control enclosure
- FlashSystem 9500 / 9500R deliver 99.9999% uptime
- FlashSystem 9500 delivers **Ransomware Threat Detection and Quantum Safe Encryption**

Secure and Trusted Boot

Trusted boot



“Physical access is king” – not anymore!

On traditional servers someone with physical access can change any code on the system

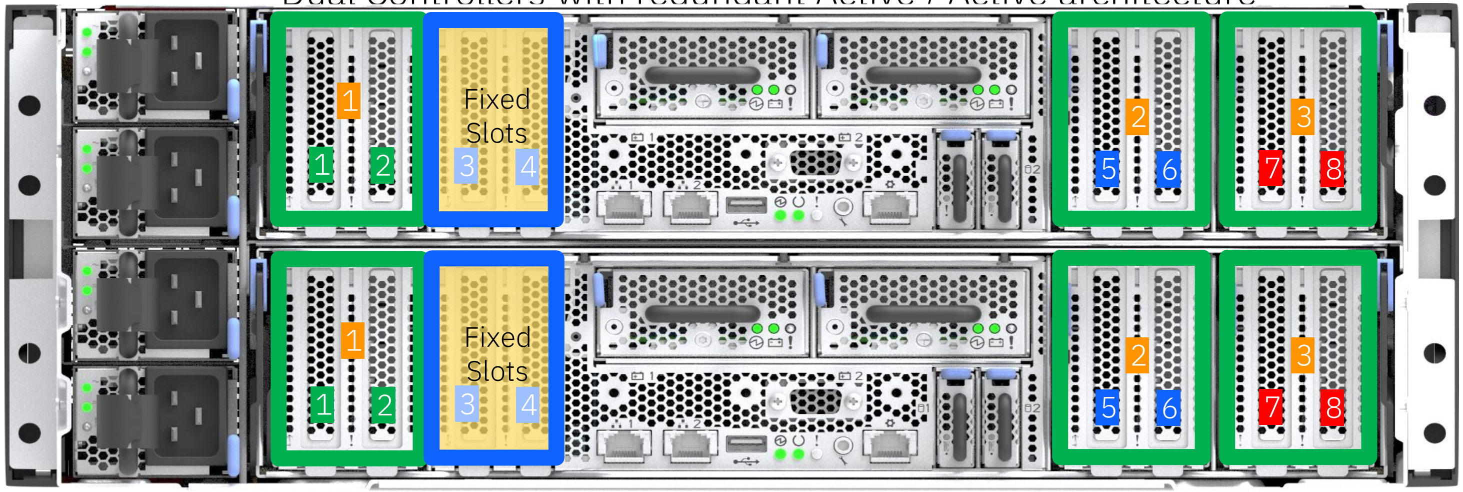
Encrypting the partitions of the boot drive with code on prevents the code from being modified

Passphrase is stored within Trusted Platform Module (TPM)

TPM only gives out the passphrase in a *trusted* environment

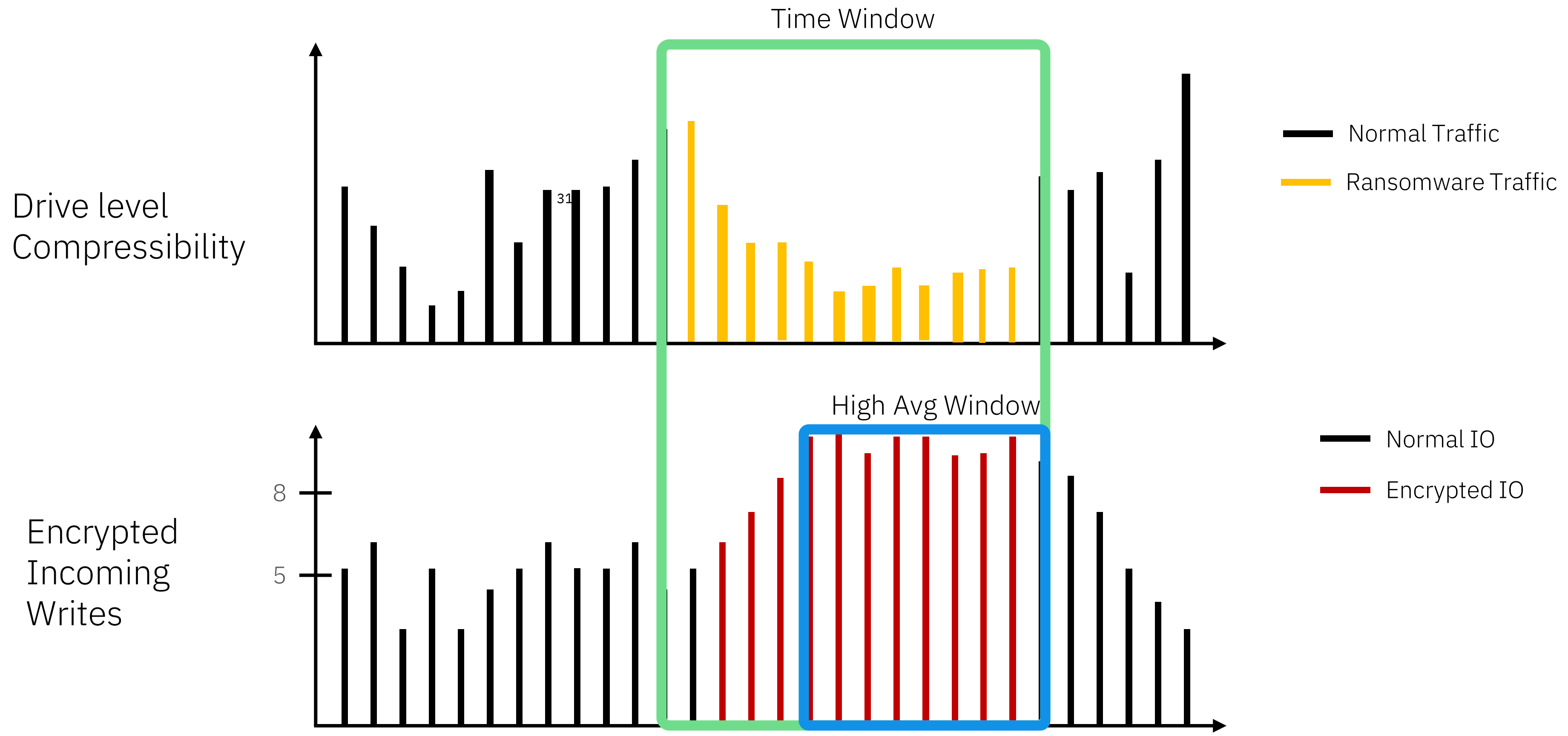
IBM FlashSystem 9500: I/O architecture

Dual Controllers with redundant Active / Active architecture



12 x I/O Adapter Slots Supporting:	Ports per adapter card	Max adapter cards per system	Max number of ports per system
10/25 GbE (RoCE / iWARP – iSCSI / NVMe)	2	12	24
32 Gb Fibre Channel	4	12	48
64 Gb Fibre Channel	4	6	24
100 GbE (NVMe / RDMA over RoCEv2)	2	12	24
12Gb SAS (Expansion Only)	2	2	4

How to detect ransomware data signals at the block level

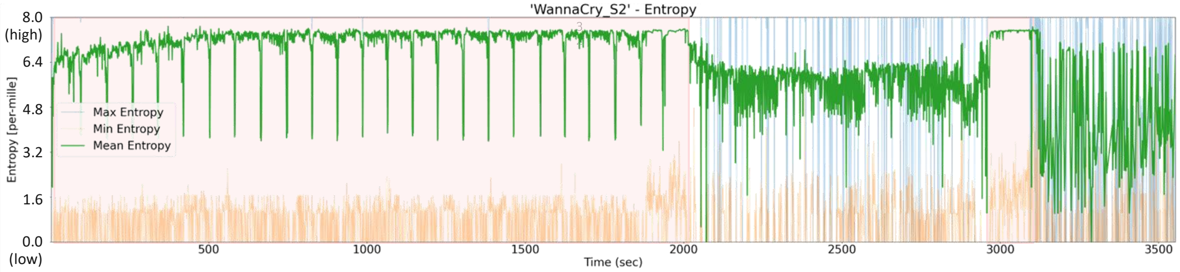


Ransomware Threat Detection – Learning Patterns

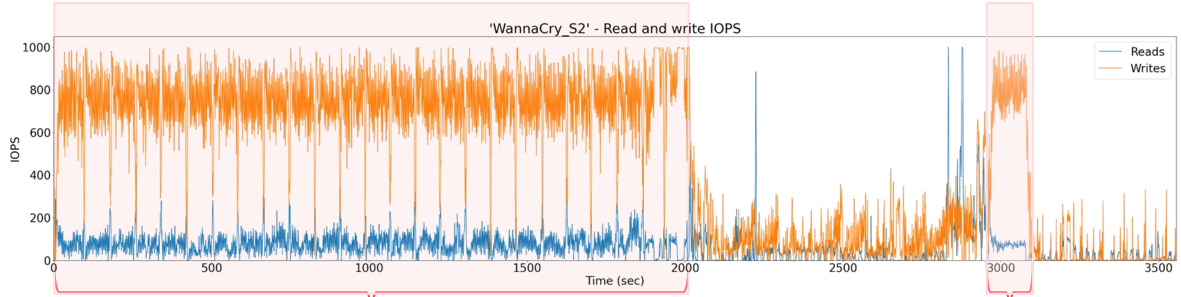
Malware such as ransomware attacks can be detected from storage IO patterns and data analysis

Example “Wannacry”:

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

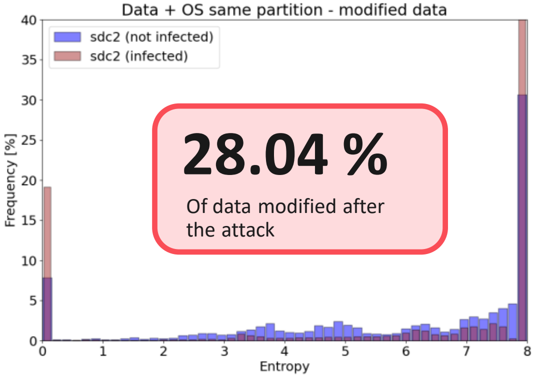


IOPS (– read, – write):



IO activity of ransomware

Payload encrypted – before and after attack:



28.04 %

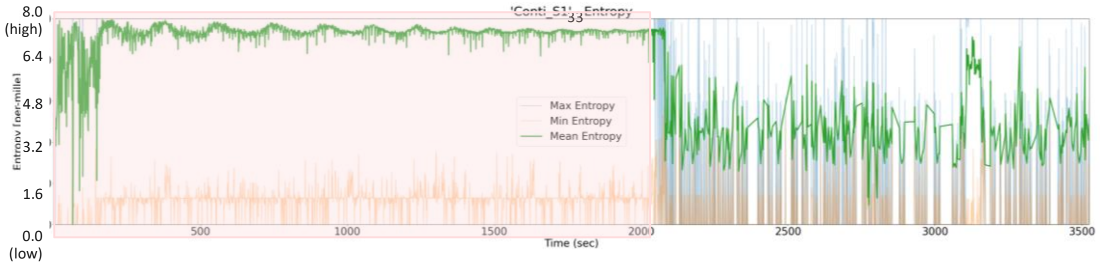
Of data modified after the attack

Ransomware Threat Detection – Learning Patterns

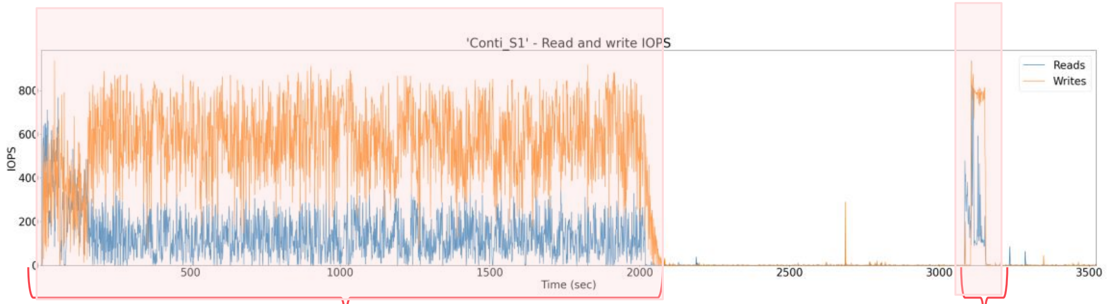
Malware such as ransomware attacks can be detected from storage IO patterns and data analysis

Example “Conti”:

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

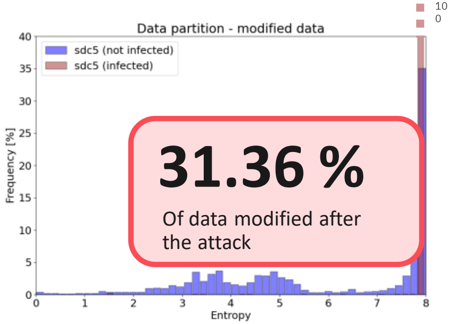


IOPS (– read, – write):



IO activity of ransomware

Payload encrypted – before and after attack:



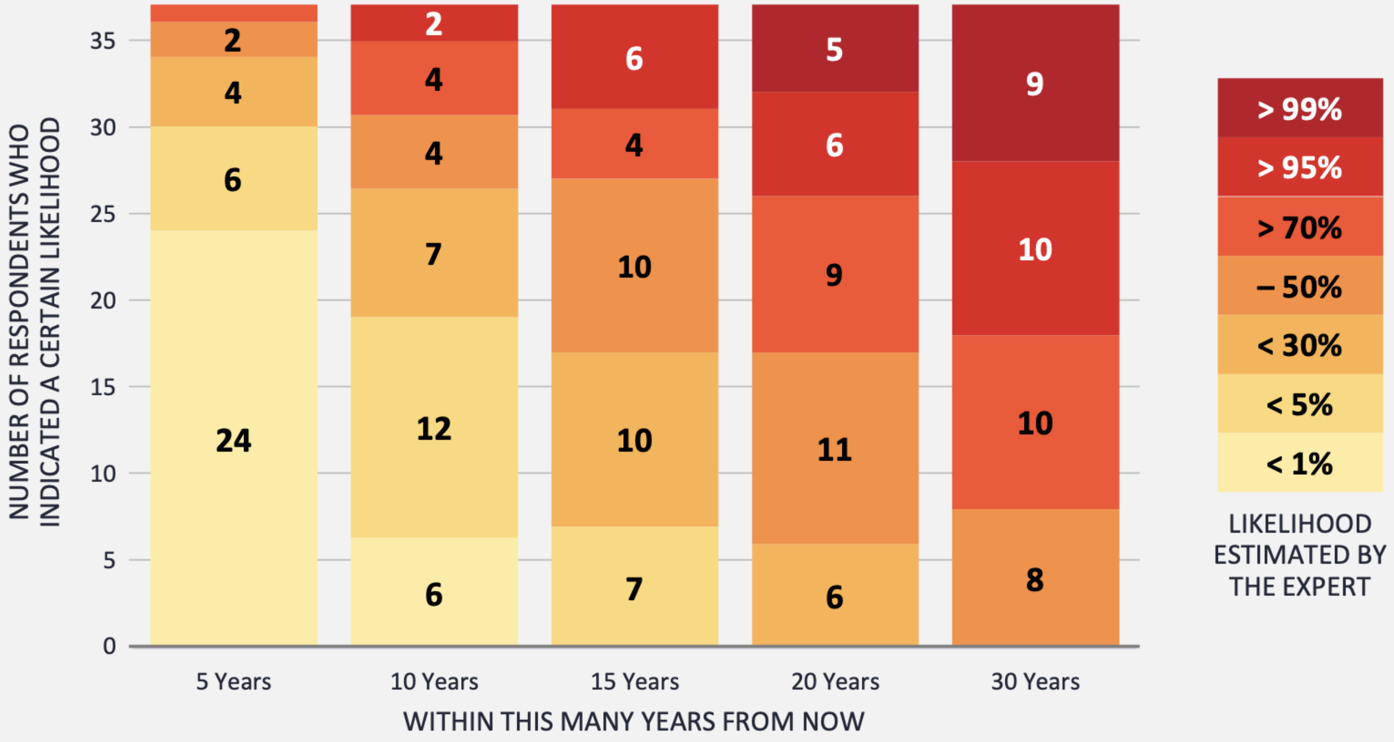
31.36 %

Of data modified after the attack

Quantum Threat to RSA-2048

2023 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

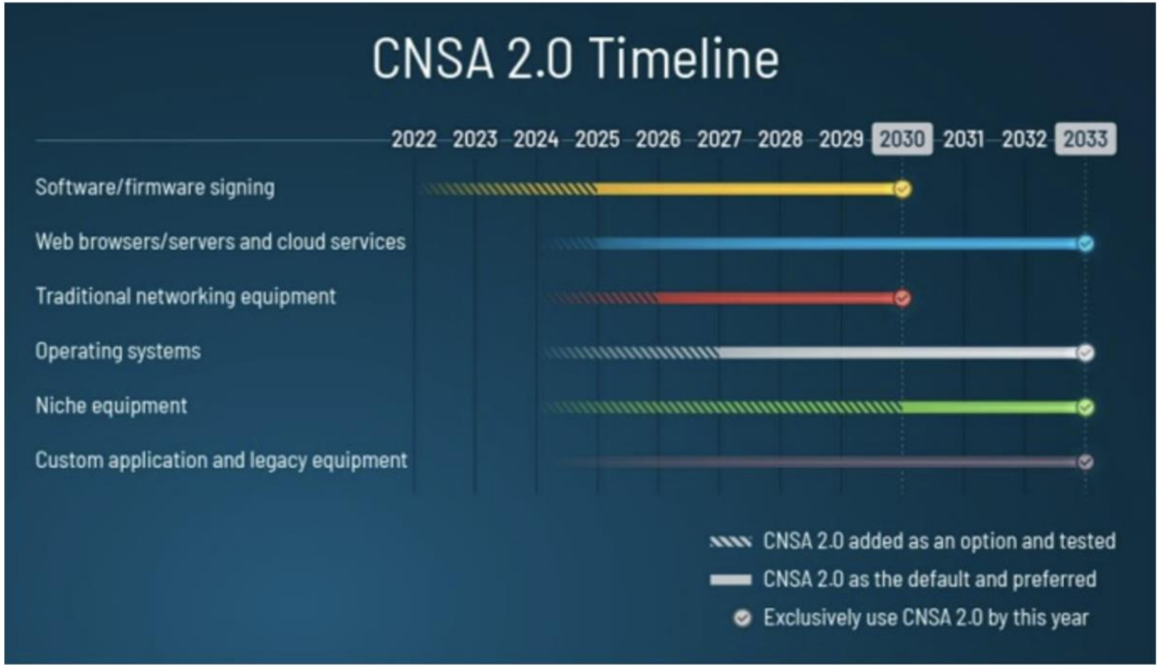
The experts indicated their estimate for the likelihood of **a** quantum computer that is cryptographically relevant-in the specific sense of being able to break RSA-2048 quickly-for various time frames, from a short term of 5 years all the way to 30 years.



Source: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

US Government mandates quantum safe for federal agencies

CNSA 2.0: Quantum-safe standards are preferred for national security systems by the mid-2020s and required by the early 2030s to defend against threats.



Source: National Security Agency, CNSA 2.0 Cybersecurity Advisory, September 2022.

NSA - Commercial National Security Algorithm Suite 2.0

In Sept.'23, NSA released the following timetable for implementing other CNSA 2.0 requirements for NSS:

- Software and firmware signing: begin transitioning immediately, support and prefer CNSA 2.0 by **2025**, and exclusively use CNSA 2.0 by **2030**.
- Web browsers/servers and cloud services: support and prefer CNSA 2.0 by **2025**, and exclusively use CNSA 2.0 by **2033**.
- Traditional networking equipment (e.g. NICs, HBAs, VPNs, networks, routers): support and prefer CNSA 2.0 by **2026**, and exclusively use CNSA 2.0 by **2030**.
- Operating systems: support and prefer CNSA 2.0 by **2027**, and exclusively use CNSA 2.0 by **2033**.
- Niche equipment (e.g. constrained devices, large public-key infrastructure systems): support and prefer CNSA 2.0 by **2030**, and exclusively use CNSA 2.0 by **2033**.
- Custom applications and legacy equipment: update or replace by **2033**

NSA sets 2035 deadline for adoption of post-quantum cryptography across national security systems

Public-key
CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates
Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

The Commercial National Security Algorithm (CNSA) 1.0 and 2.0 Suites

Algorithm Type	CNSA 1.0	CNSA 2.0	Comment
Block Cipher for symmetric encryption	AES-256	AES-256 (per FIPS 197)	AES-256 is quantum-safe
Cryptographic Hash	SHA-384	SHA-384 or SHA-512 (per FIPS 180-4)	SHA-384 & SHA-512 are quantum-safe
Key Establishment over a public channel	RSA-3096* or EC-DH* (P-384)	ML-KEM-1024 Level 5 (per FIPS 203)	ML-KEM will be a NIST approved PQC algorithm
Software/Firmware Code Signature	RSA-3096* or EC-DSA* (P-384)	(LMS or XMSS per SP 800-208) or ML-DSA-87^ Level 5	(Stateful hash-based) or stateless PQC algorithm
Digital Signature (for all other use cases)	RSA-3096* or EC-DSA* (P-384)	ML-DSA-87 Level 5 (per FIPS 204)	ML-DSA will be a NIST approved PQC algorithm

* RSA and EC based algorithms are not quantum-safe, a CRQC that can break them easily will eventually be developed

^ per FIPS 204, see also https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF