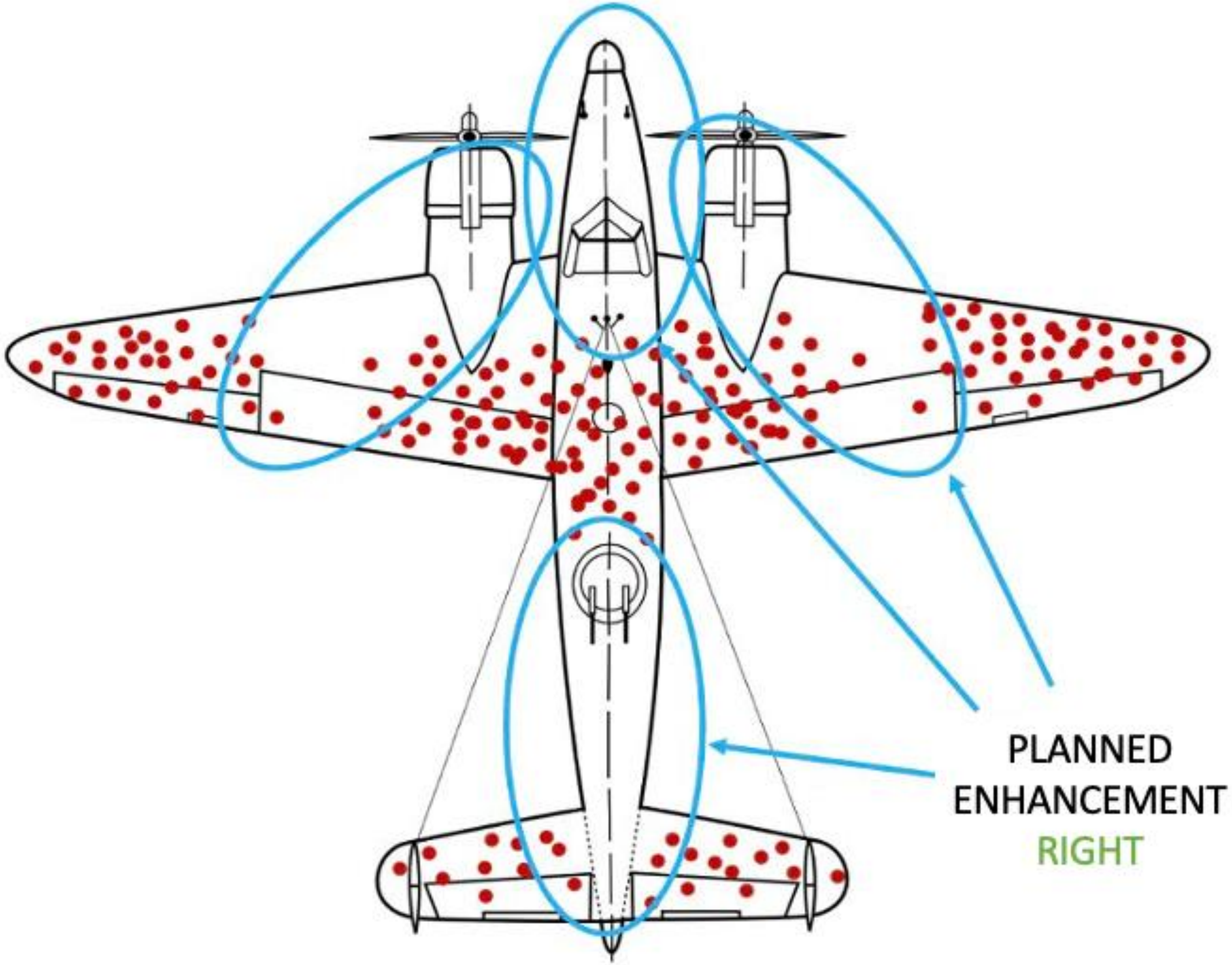
FUELING NIS2 TRANSFORMATION

Bartosz Pizon
Presales Engineer in IBM



Sensitivity: Internal

https://en.wikipedia.org/wiki/Survivorship_bias

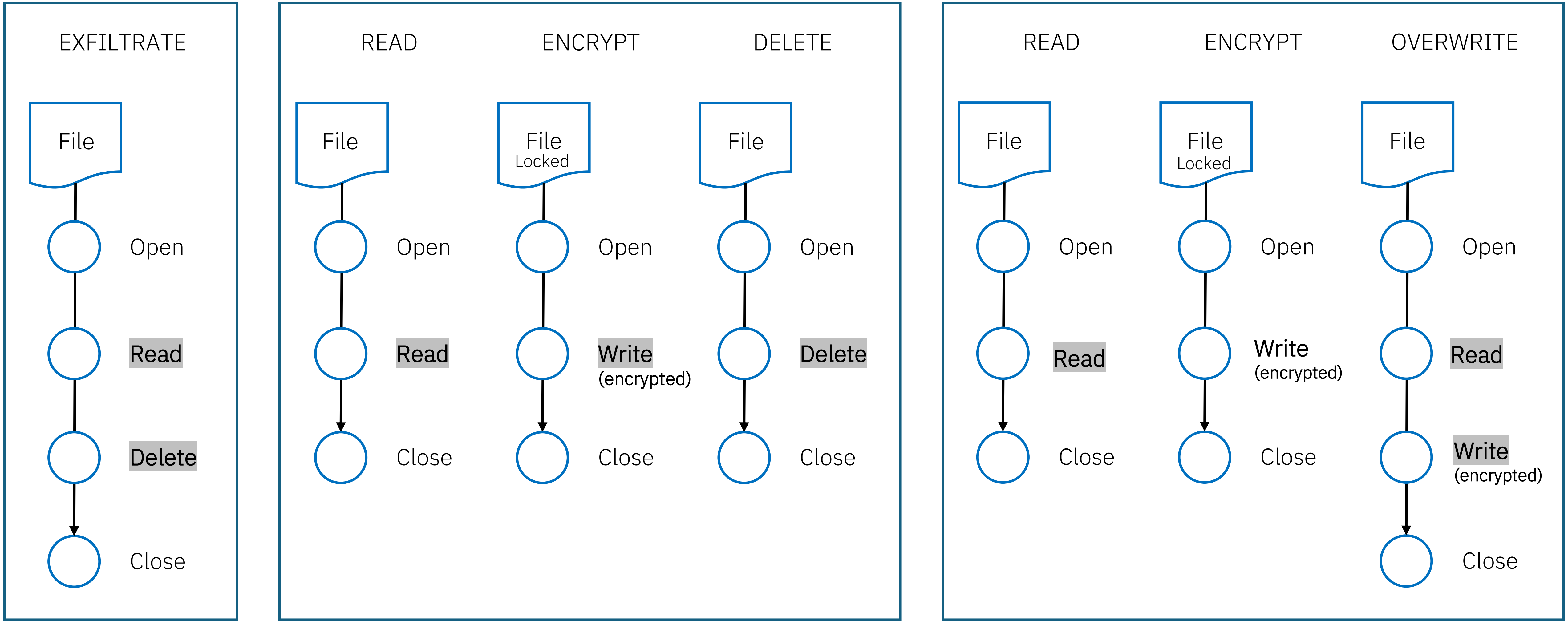
What story about airplanes and NIS-2 have in common?

Enhancement

Tasks according to NIS-2
strengthening the level of cybersecurity of critical infrastructure

- RISK ANALYSIS
- MULTIFACTOR AUTHENTICATION
- PREVENTION DETECTION RESPONSE
- BUSINESS CONTINUITY
- NETOWRKS SECURITY
- CYBERSECURITY TRAINING
- DATA ENCRYPTION
- ACCESS CONTROL POLICY

Cyber Attacks: Similar IO Access Sequences



EXFILTRATE

File

Open

Read

Delete

Close

READ

File

Open

Read

Close

ENCRYPT

File
Locked

Open

Write
(encrypted)

Close

DELETE

File

Open

Delete

Close

READ

File

Open

Read

Close

ENCRYPT

File
Locked

Open

Write
(encrypted)

Close

OVERWRITE

File

Open

Read

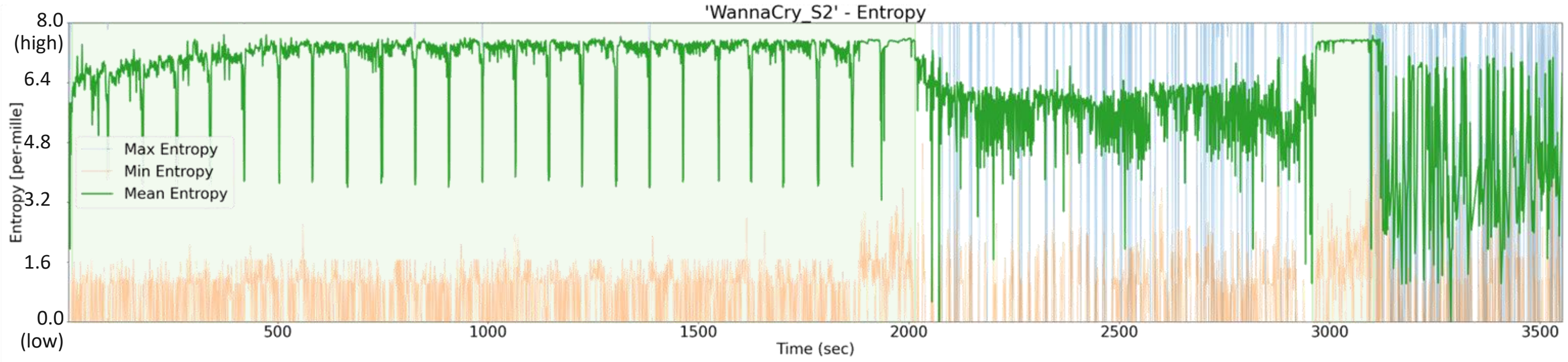
Write
(encrypted)

Close

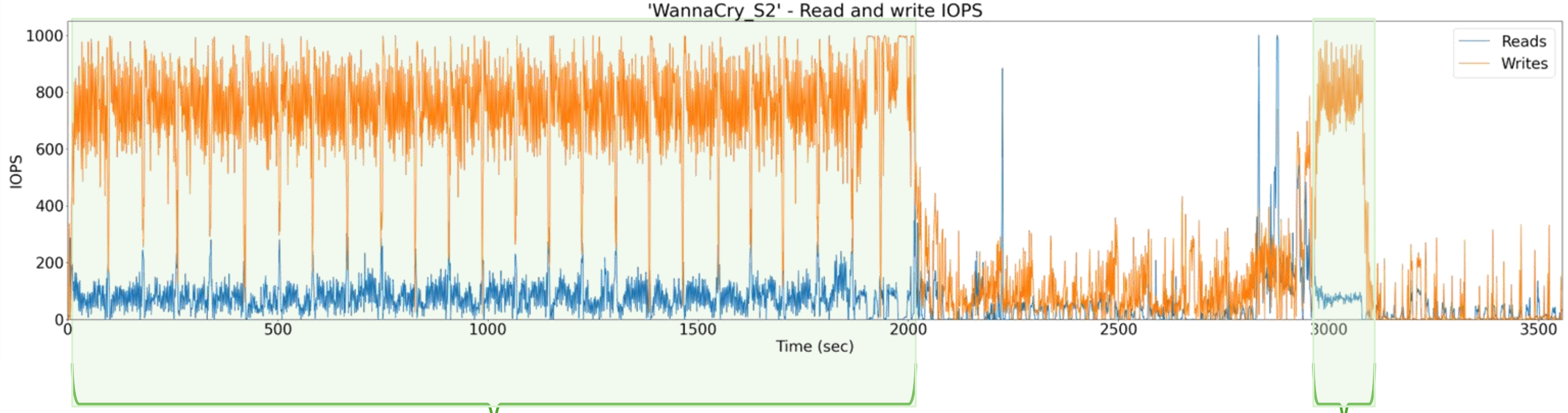
Characteristics found in IO traces from ransomware

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

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

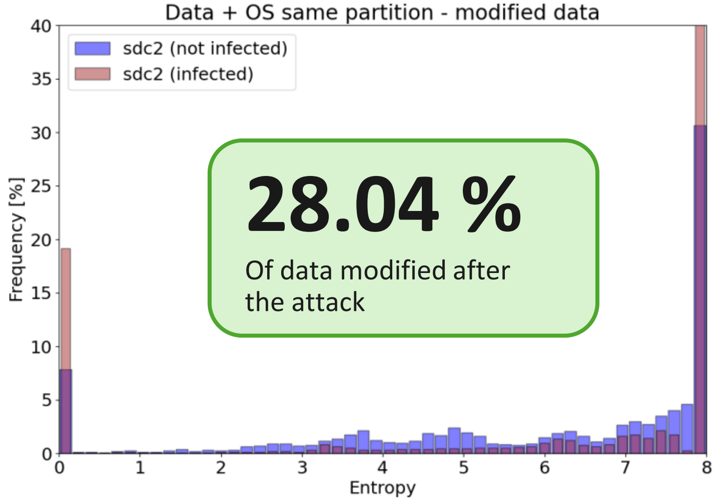


IOPS (– read, – write):



IO activity of ransomware

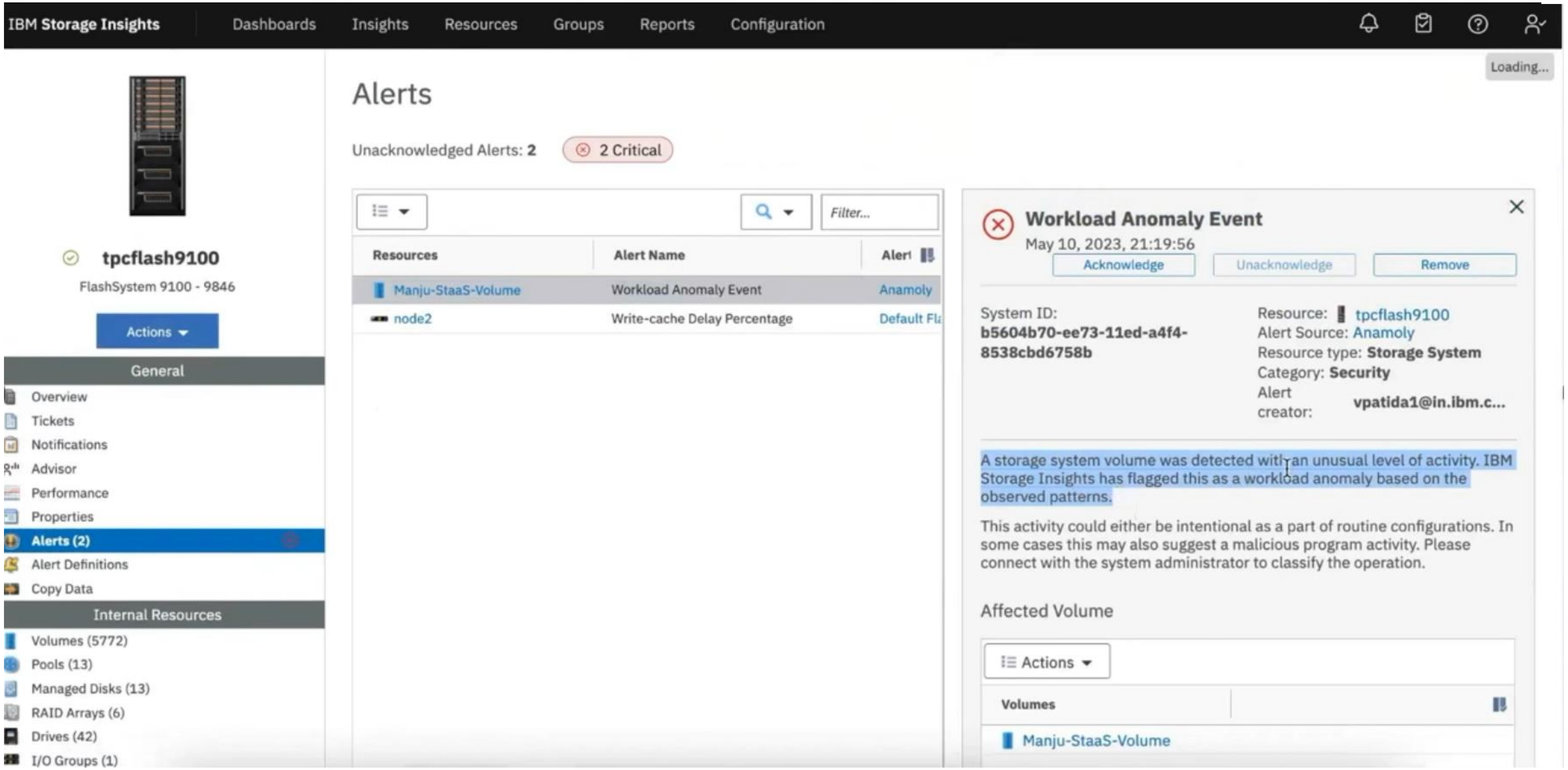
Payload encrypted – before and after attack:



28.04 %

Of data modified after the attack

Data Security with Storage Insights Pro and ransomware detection



tpcflash9100

FlashSystem 9100 - 9846

Alerts

Unacknowledged Alerts: **2** 2 Critical

Resources	Alert Name	Alert
Manju-StaaS-Volume	Workload Anomaly Event	Anamoly
node2	Write-cache Delay Percentage	Default Fl

Workload Anomaly Event

May 10, 2023, 21:19:56

System ID: **b5604b70-ee73-11ed-a4f4-8538cbd6758b**

Resource: tpcflash9100
Alert Source: Anamoly
Resource type: **Storage System**
Category: **Security**
Alert creator: **vpatida1@in.ibm.c...**

A storage system volume was detected with an unusual level of activity. IBM Storage Insights has flagged this as a workload anomaly based on the observed patterns.

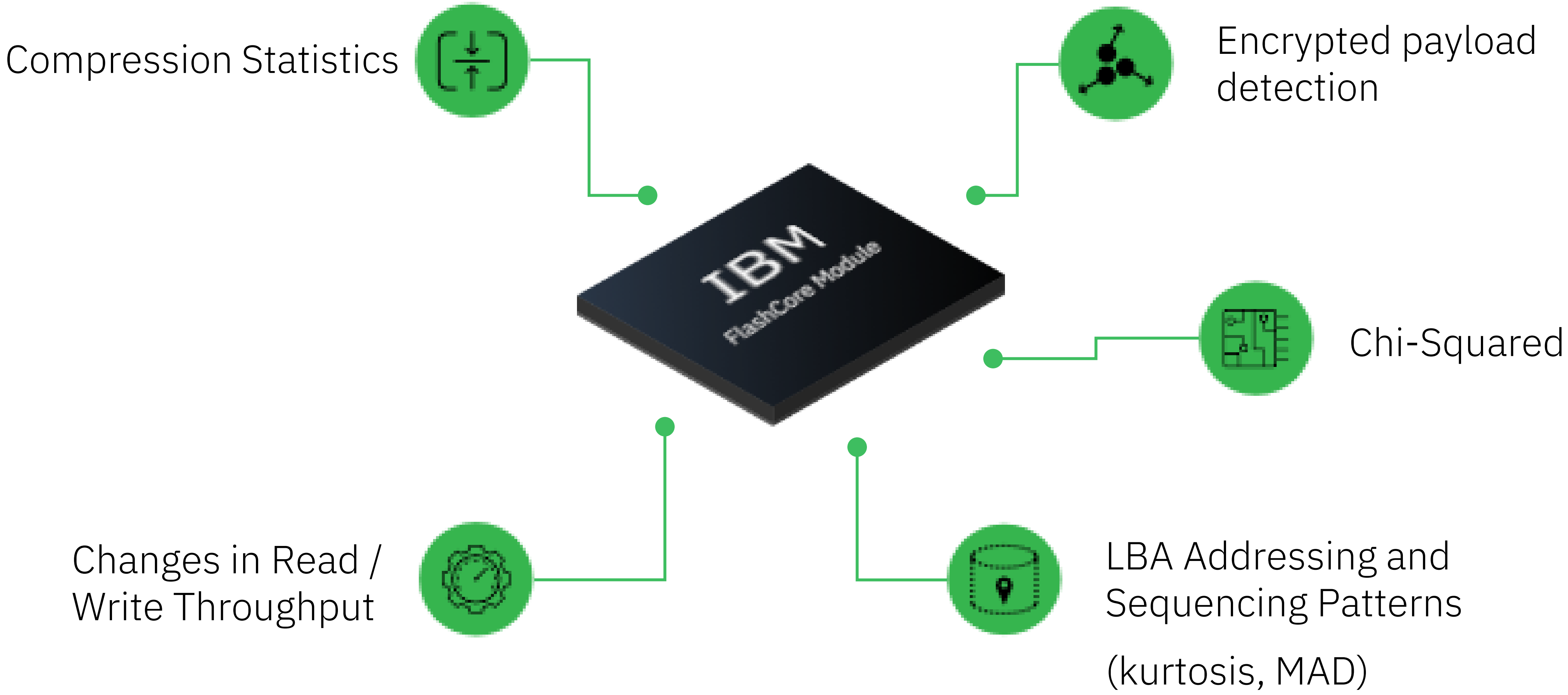
This activity could either be intentional as a part of routine configurations. In some cases this may also suggest a malicious program activity. Please connect with the system administrator to classify the operation.

Affected Volume

Volumes
Manju-StaaS-Volume

Sensitivity: Internal

Ransomware Detection With FCMs



Compression Statistics

Encrypted payload detection

Chi-Squared

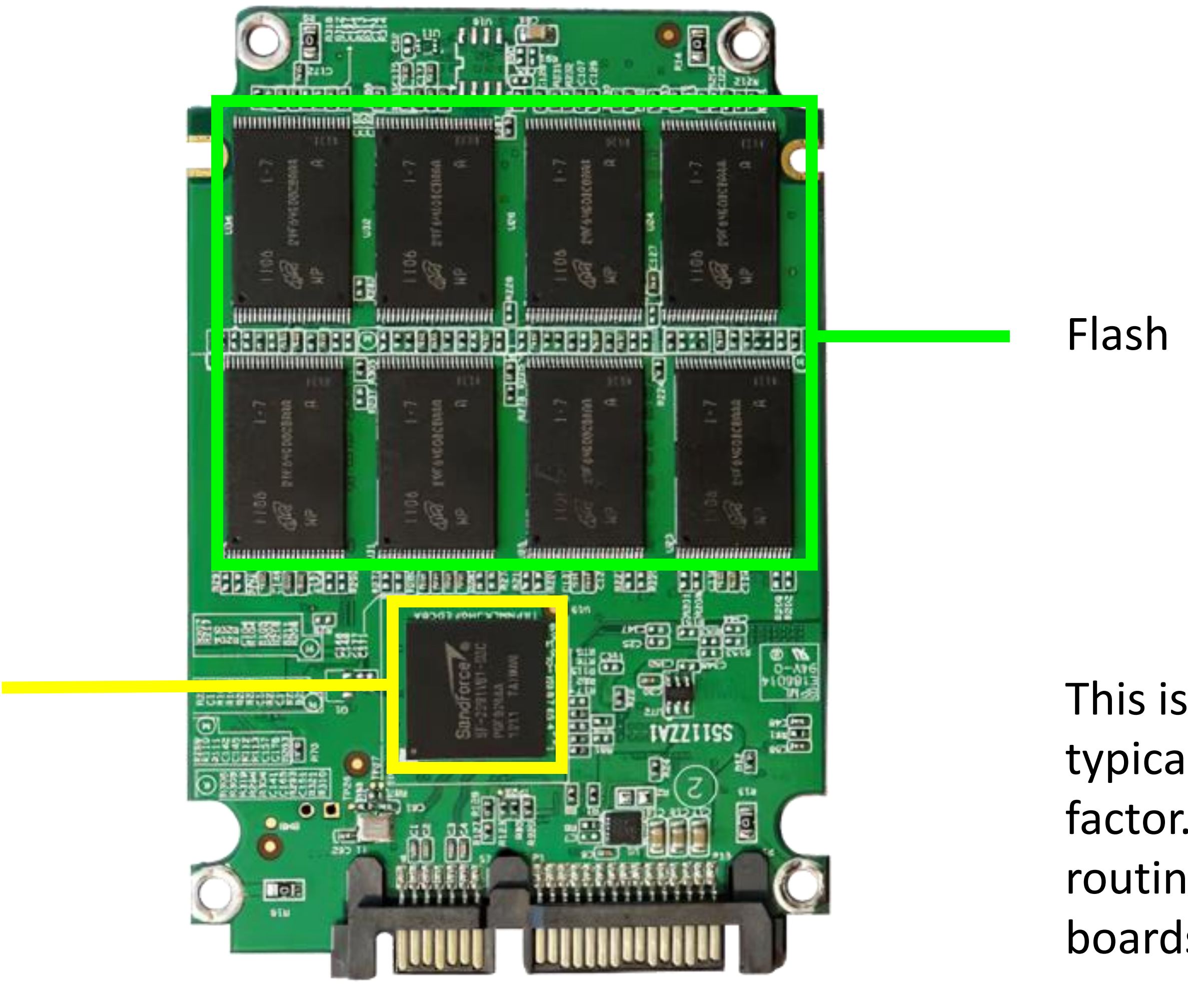
Changes in Read / Write Throughput

LBA Addressing and Sequencing Patterns

(kurtosis, MAD)

The layout of an industry standard **commodity SSD**

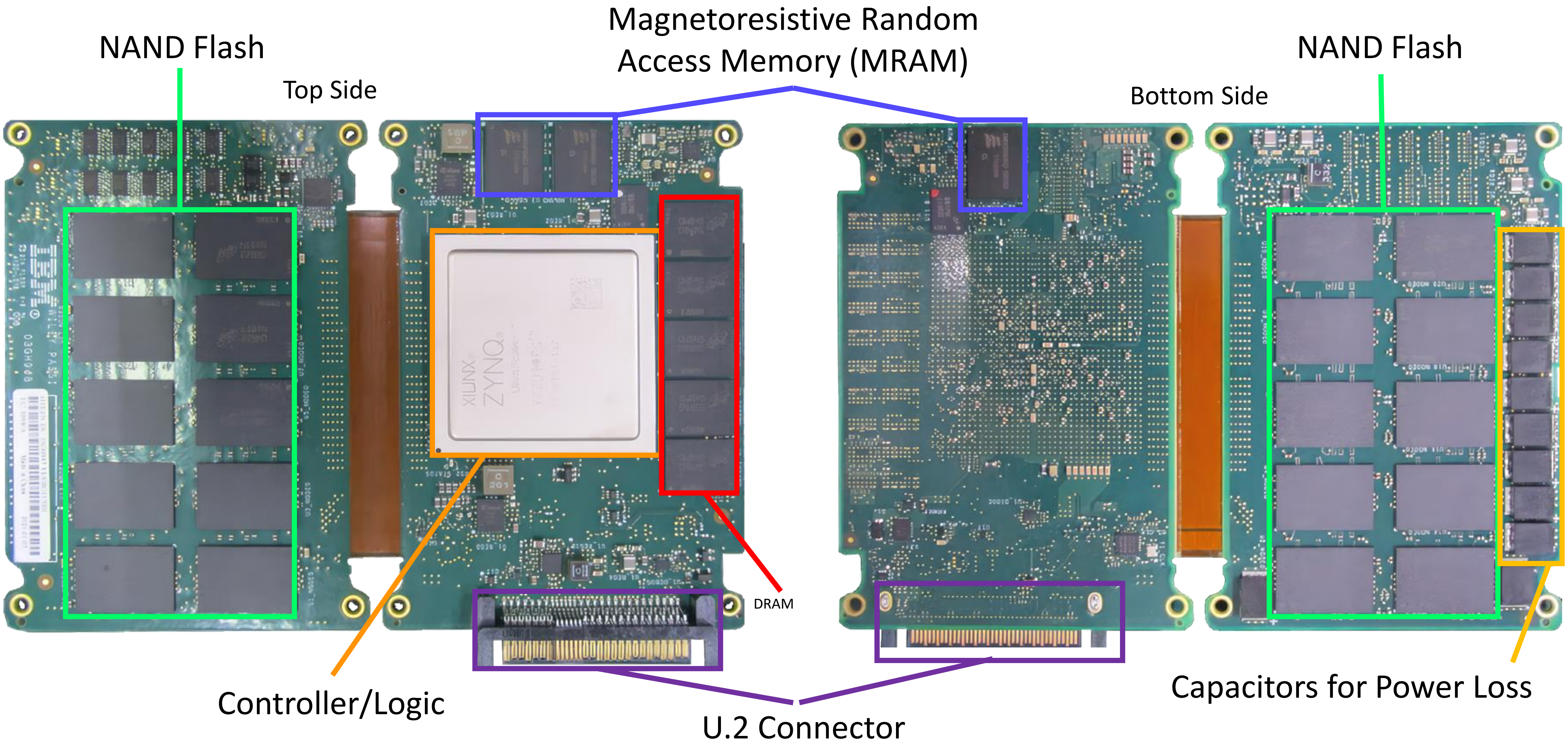
2.5” SFF



This is a single card (IS SSD) that is typically found in a 7mm form factor. For large IS SSDs they will routinely contain two circuit boards.

IBM FlashCore Modules

2.5" SFF



NAND Flash

Top Side

Magnetoresistive Random Access Memory (MRAM)

Bottom Side

NAND Flash

DRAM

Controller/Logic

U.2 Connector

Capacitors for Power Loss

Sensitivity: Internal

IBM FlashSystem 5300

1.3 PB RAW capacity

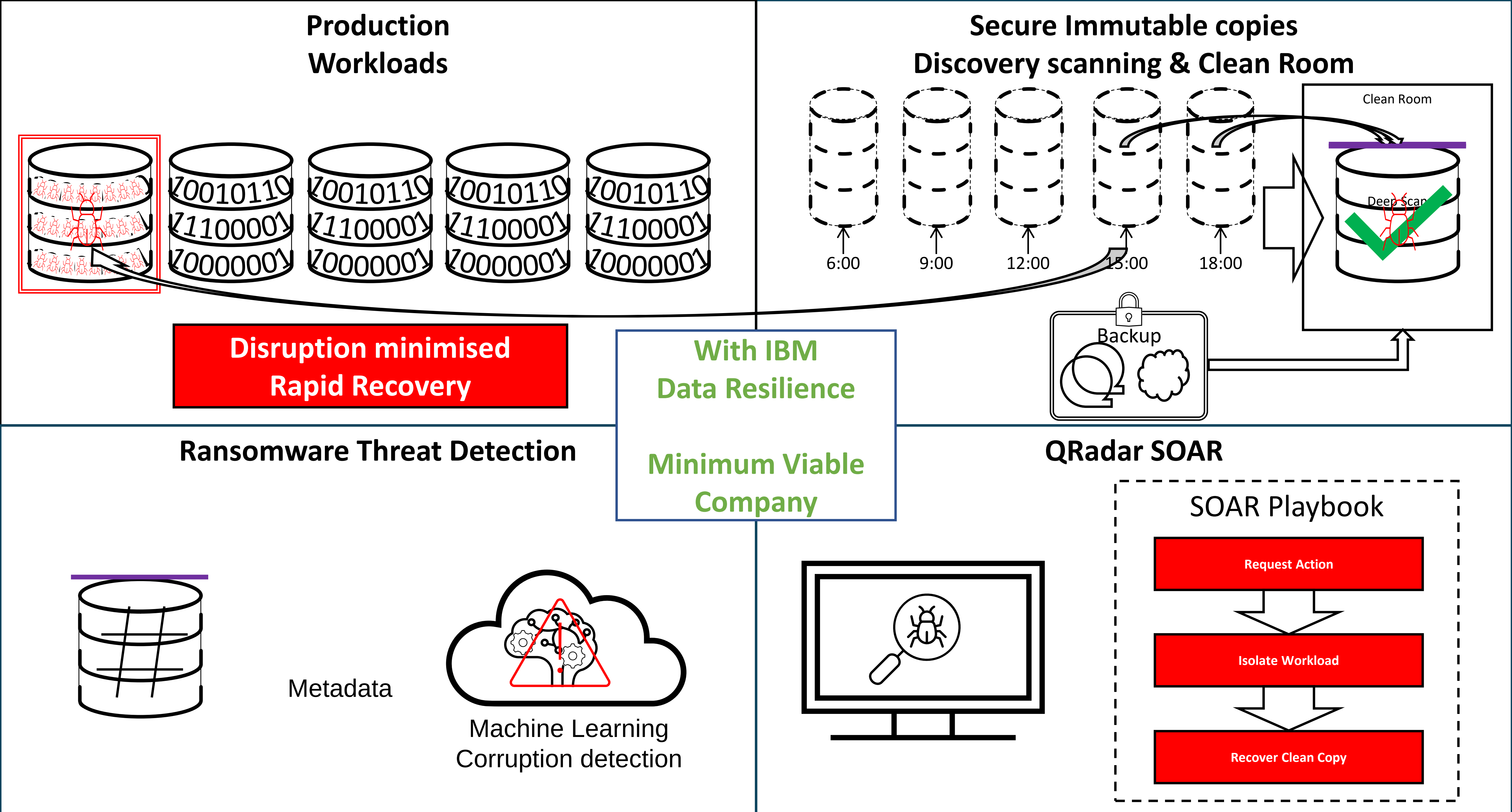
400.000 IOPS
28 GB/s

Front

Rear

1 rack unit

* 16k block size, 70% reads, 30% writes, and a 50% cache hit



Production Workloads

Disruption minimised
Rapid Recovery

Secure Immutable copies Discovery scanning & Clean Room

With IBM Data Resilience

Minimum Viable Company

Ransomware Threat Detection

Metadata

Machine Learning Corruption detection

QRadar SOAR

SOAR Playbook

- Request Action
- Isolate Workload
- Recover Clean Copy

Advanced data resilience

Ransomware Threat Detection

Ransomware Threat Detection in the **Storage Virtualize** software stack

Software-based

Hardware-based

Ransomware Threat Detection with IBM’s unique **FlashCore Module 4.0**

FlashSystem 5300 employs the AI-driven **Storage Insights Pro**

Monitoring and Alerting

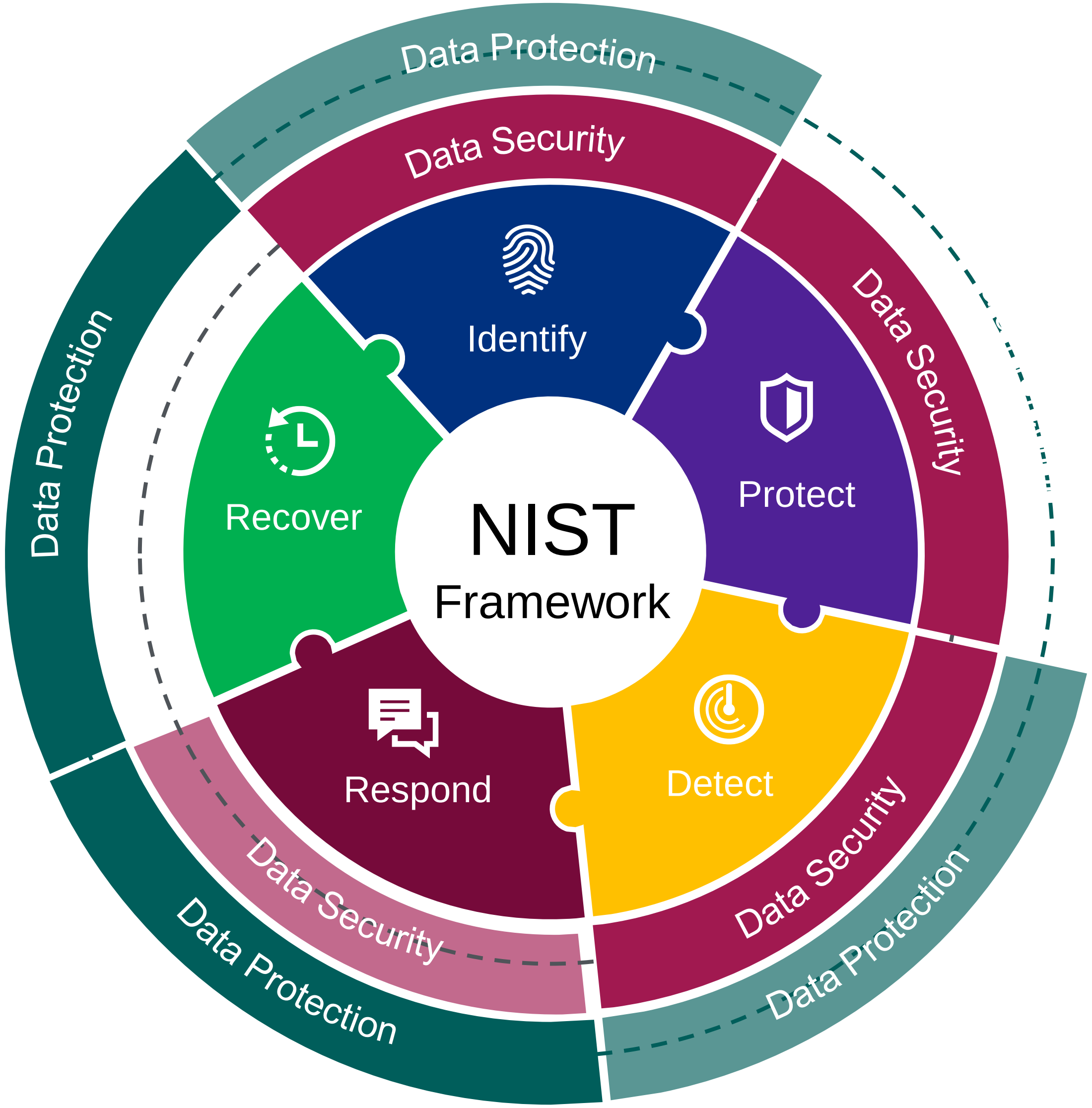
Storage Virtualize enables Safeguarded Copies **Immutable Snapshots**

IBM Storage Defender

Data Security helps detect and prevent attacks, but nothing to recover

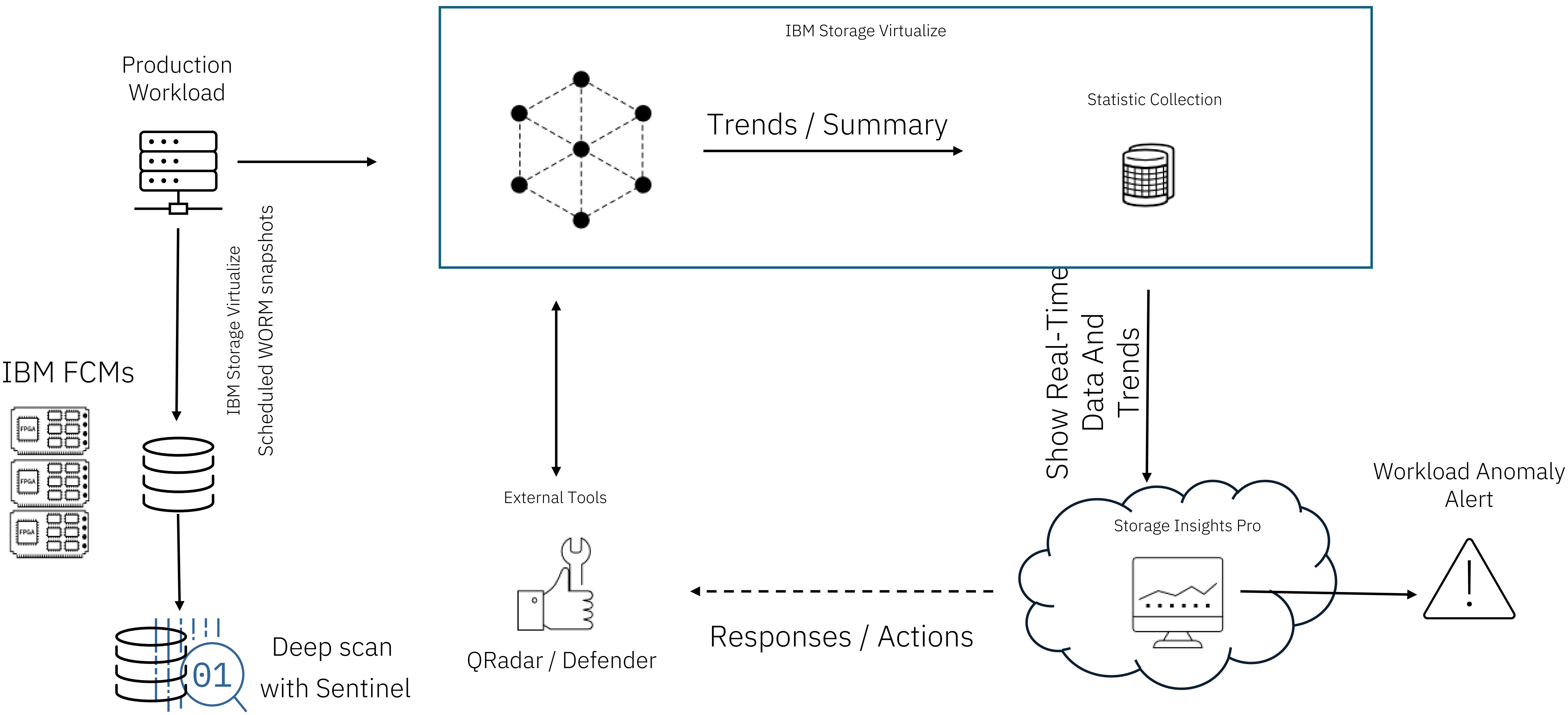
Data Protection is primarily reactionary and does not help avoid attack

Data Security + Data Protection =
Data Resiliency



Sensitivity: Internal

Target Architecture



How to enhance IT infrastructure by IBM

RISK & SECURITY ANALYSIS

RANSOMWARE DETECTION
STORAGE INSIGHTS PRO

MFA & ACCESS CONTROL

STORAGE VIRTAULIZE
FLASHSYSTEM

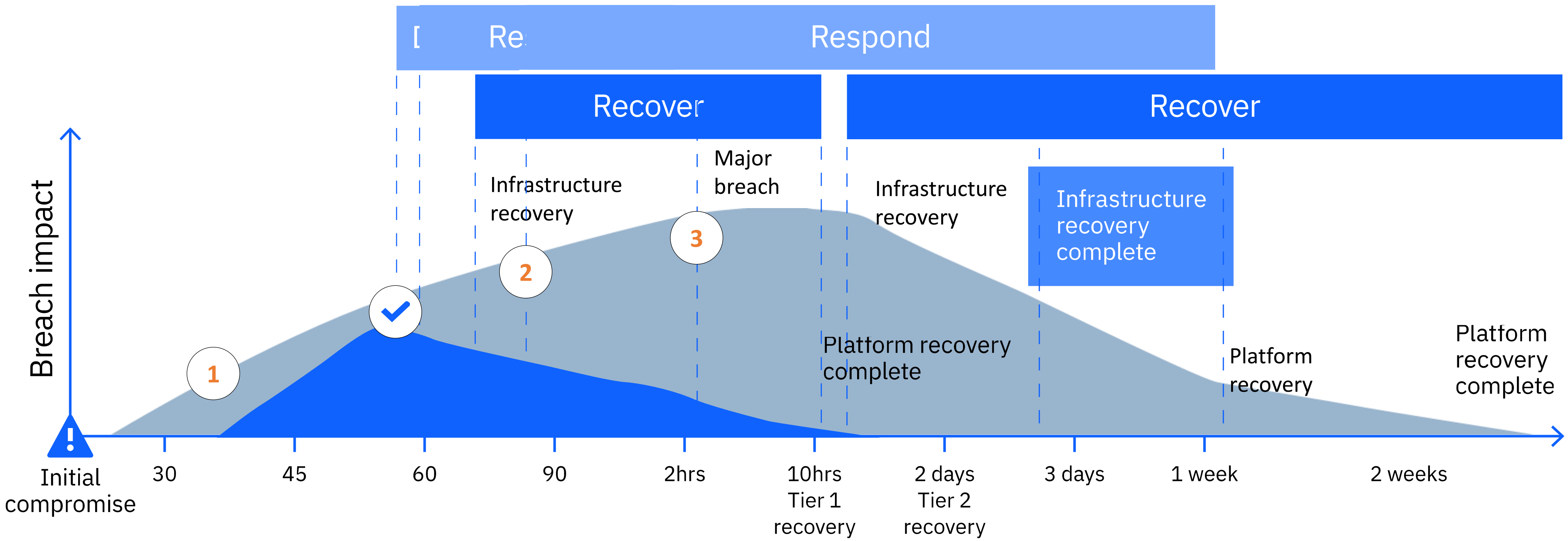
PREVENTION DETECTION RESPONSE

IBM CYBER VAULT + SIEM
STORAGE DEFENDER + QRADAR

HA & DR DATA ENCRYPTION

POLICY BASED REPLICATION
FLASHSYSTEM

Detection and recovery of data after an attack



1 Data corruption is taking place – but not yet detected.

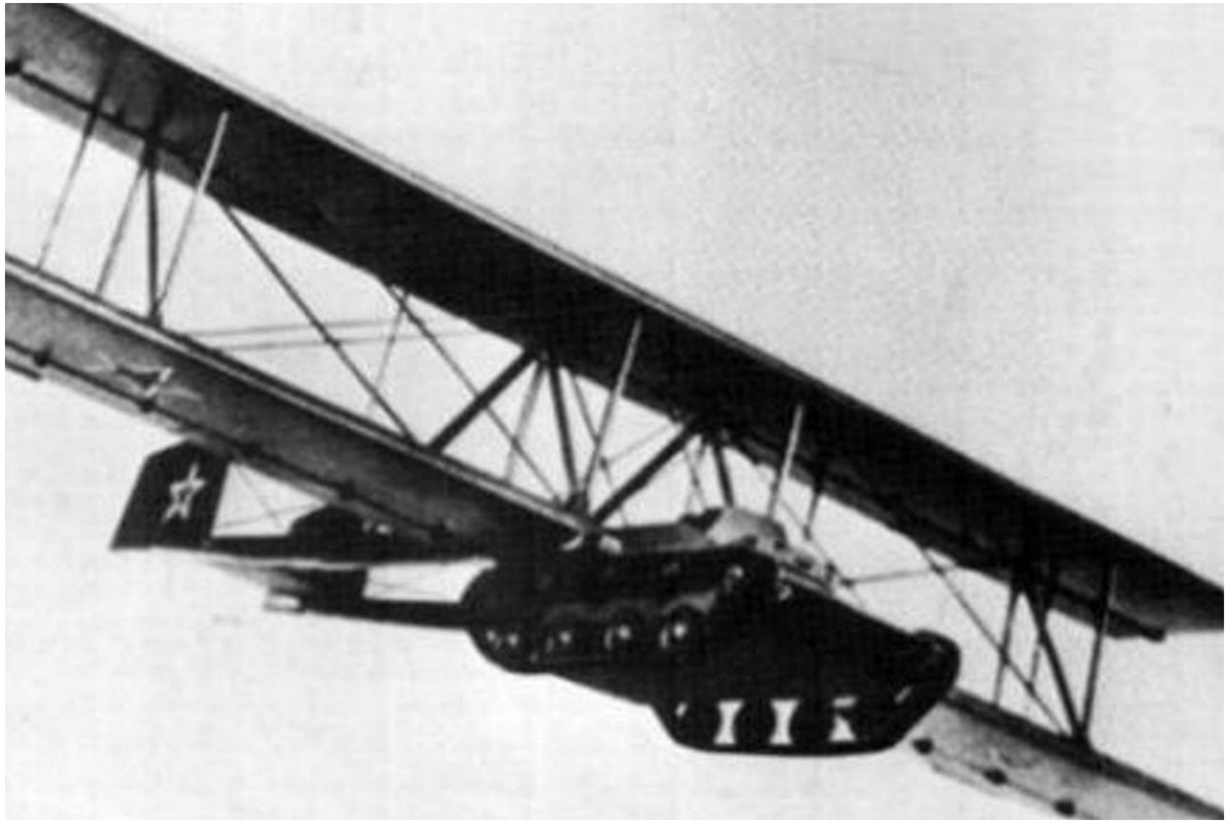
2 Corruption. Without a Cyber Vault environment, corruption is detected much later and has a greater chance of spreading.

3 It takes even longer to identify all affected data when corruption has spread throughout the enterprise.

✓ IBM Cyber Vault

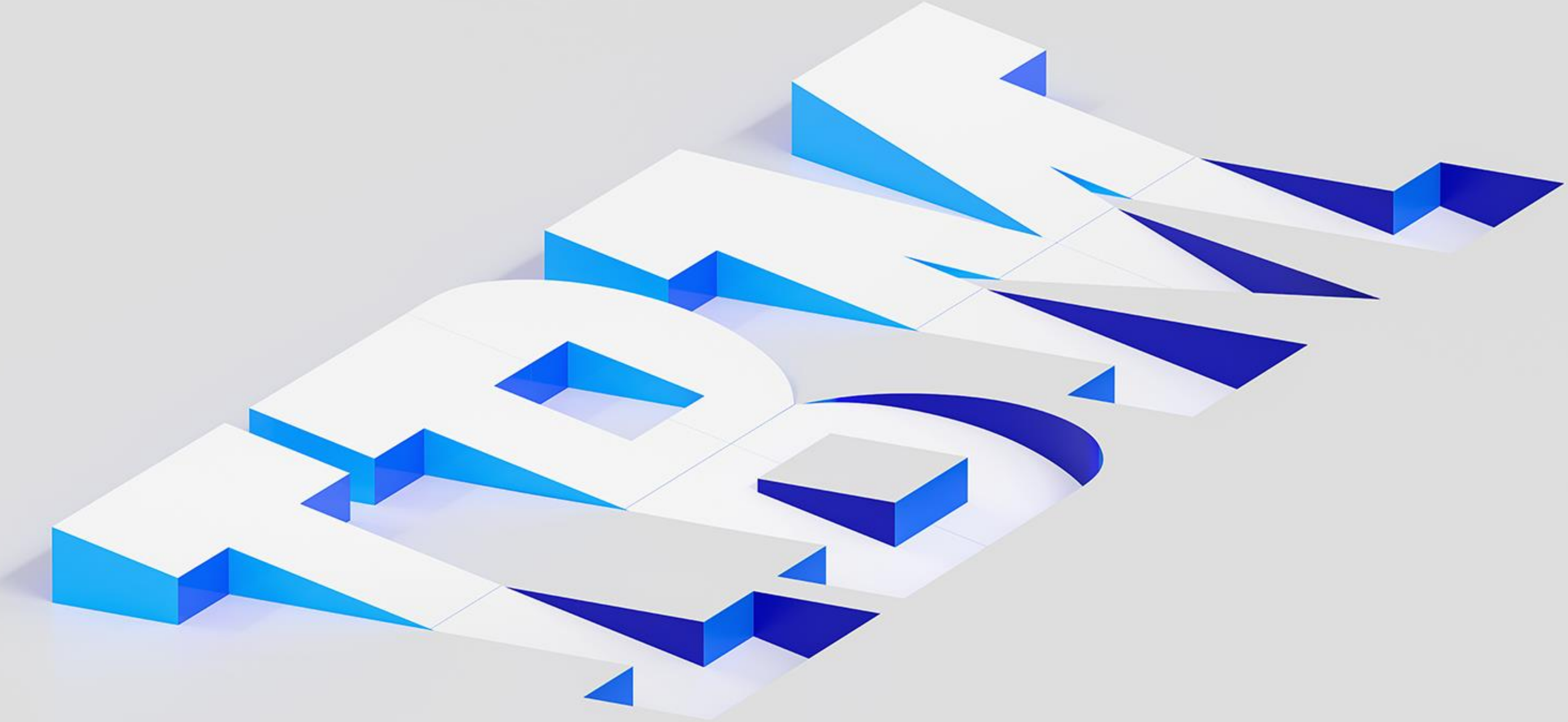
Thanks to the Cyber Vault environment and the use of Safeguarded Copy technology, data is constantly checked, and corruption is detected and undone earlier and faster.

Choose how to protect your data and choose wisely



https://en.wikipedia.org/wiki/Antonov_A-40

https://en.wikipedia.org/wiki/Lockheed_Martin_F-35_Lightning_II


IBM