AI-Enabled SSDs for Fortified Cyber & Physical Security

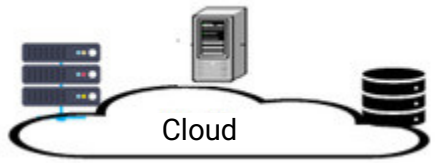
Erik A. Nilsen, PhD
Chief Technology Strategist
Flexxon

©2023 Flash Memory Summit. All Rights Reserved

Current State of Cybercrime

Flash Memory Summit

Vulnerabilities



Application Layer

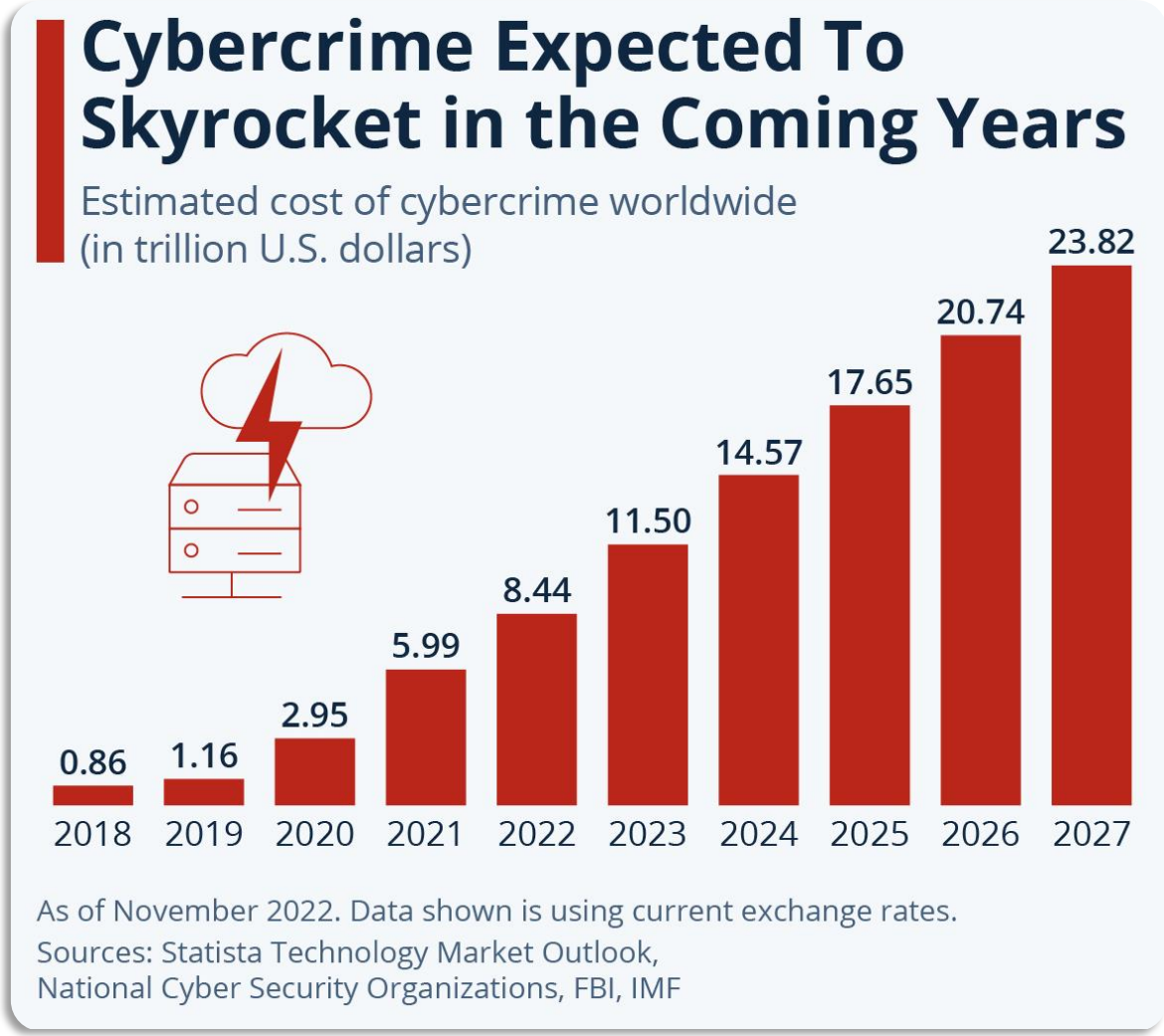
Weak passwords
Weak authentication & authorization
Insecure ecosystem configurations
Insecure network services
Insecure software
Insecure/outdated components

Network Layer

Lack of proper encryption
Weak or hardcoded passwords
Weak authentication & authorization
Insecure network services
Insecure ecosystem interfaces
Insecure security configuration
Insecure firmware

Physical Layer

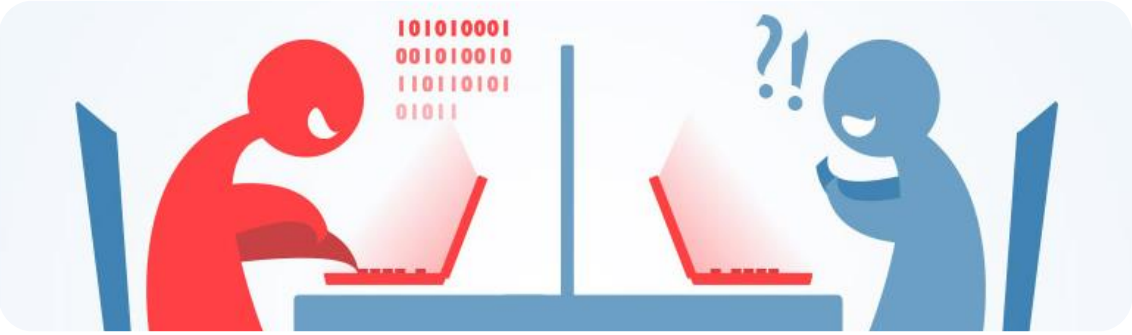
Poor physical security
Lack of proper encryption
Weak or hardcoded passwords
Weak authentication & authorization
Insecure ecosystem interfaces
Unnecessarily open ports
Lack of secure boot processes
Insecure firmware
Insecure/outdated components



©2023 Flash Memory Summit. All Rights Reserved

Causes of Cybersecurity Lapses

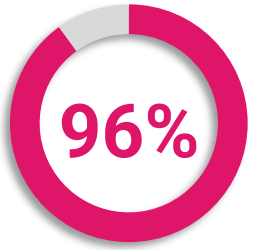
Types of Insider Threats



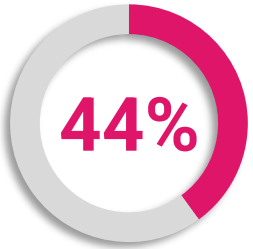
Malicious Insiders
Intentionally use their access to sensitive data to harm the company

Inadvertent Insiders
Cause damage to the company unintentionally

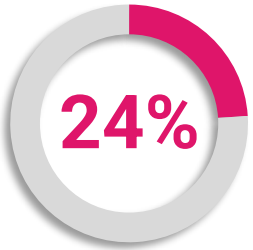
Security Breaches Led by Human Error



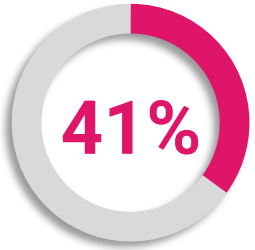
of all security breaches take place due to human error



of all targeted cyber attacks are laid on employees through emails



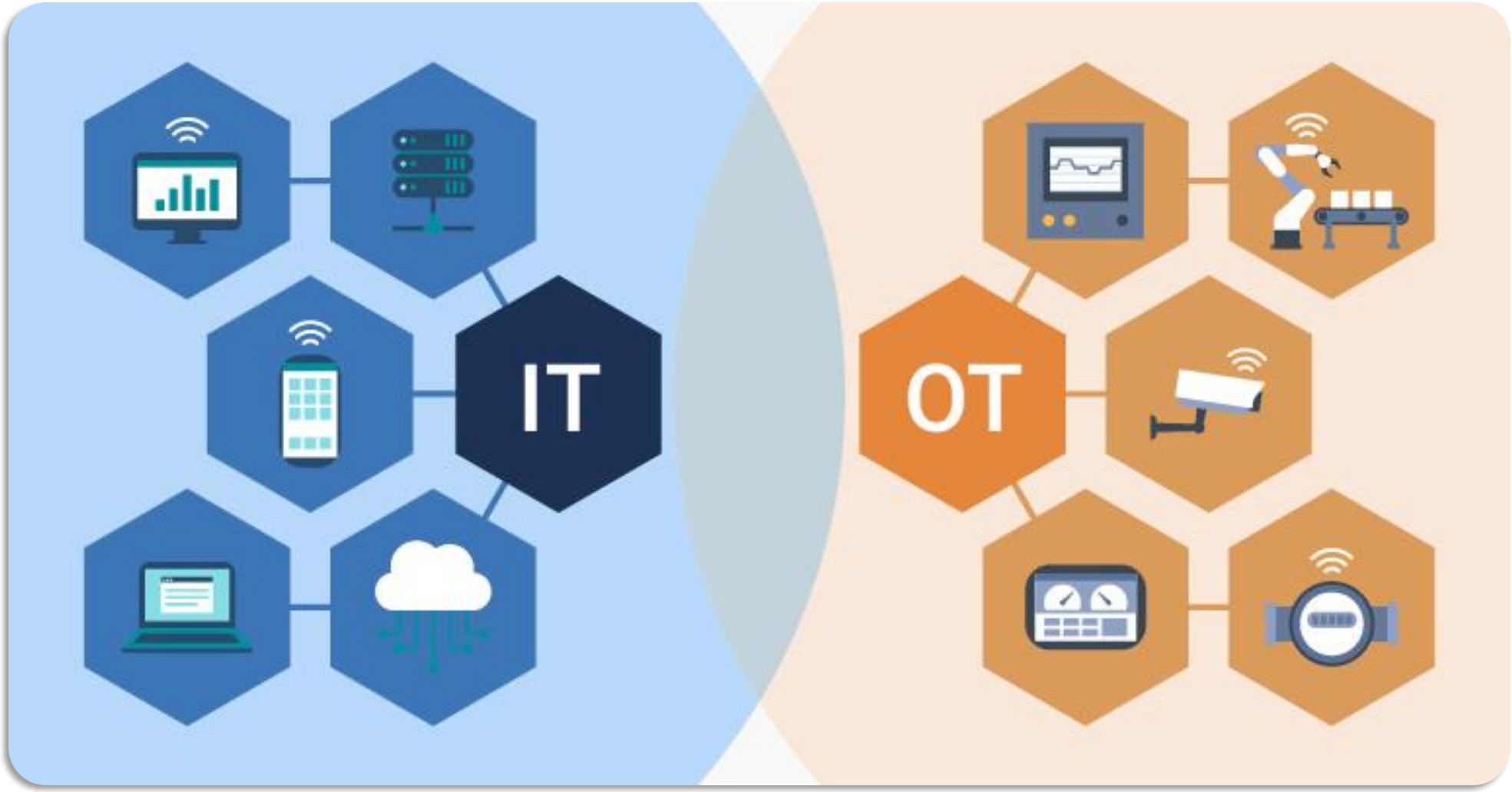
of data breaches occur due to employee negligence or unawareness



of the C-suite executives believe that human error is the primary cause of data breach

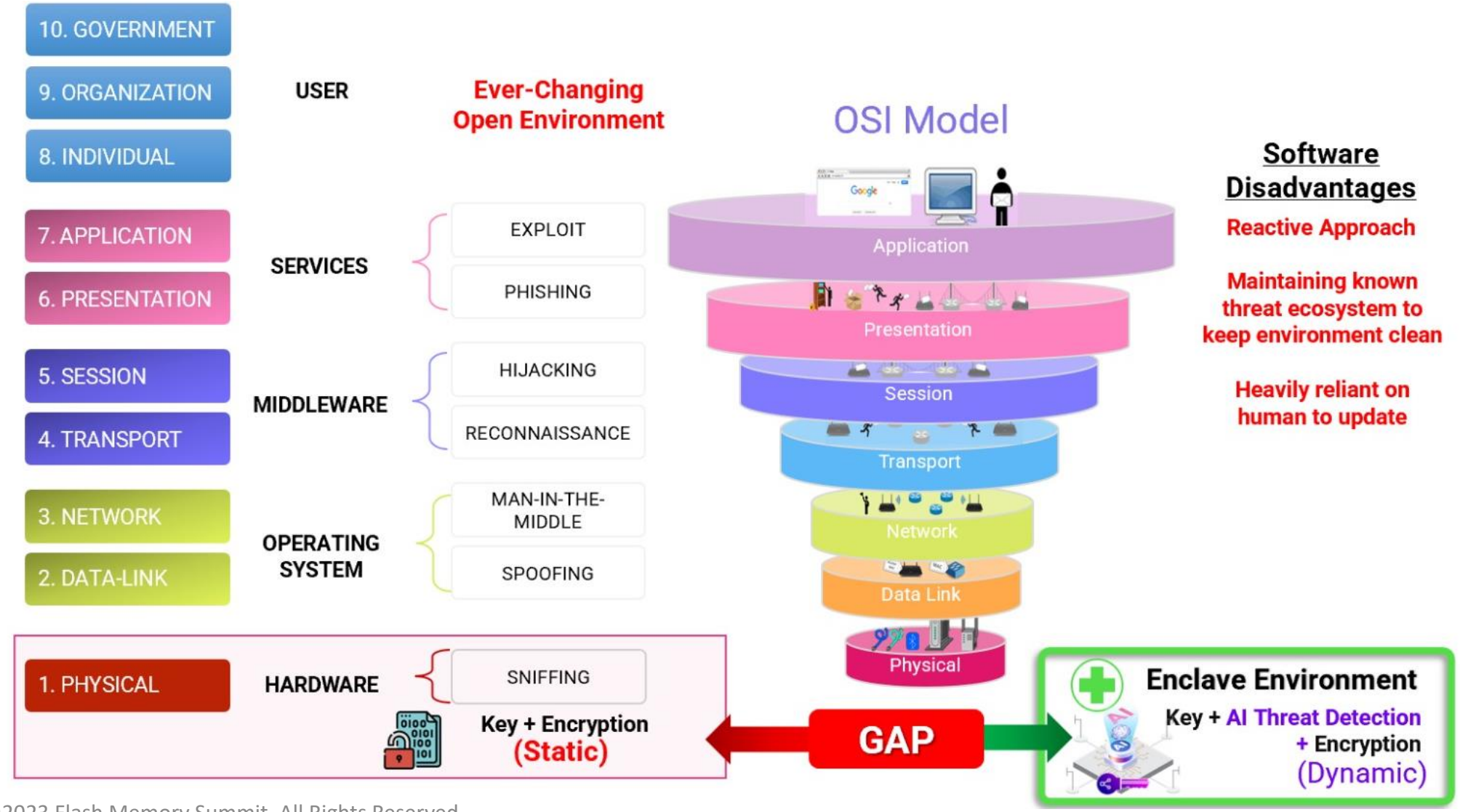
©2023 Flash Memory Summit. All Rights Reserved

IT/OT Convergence



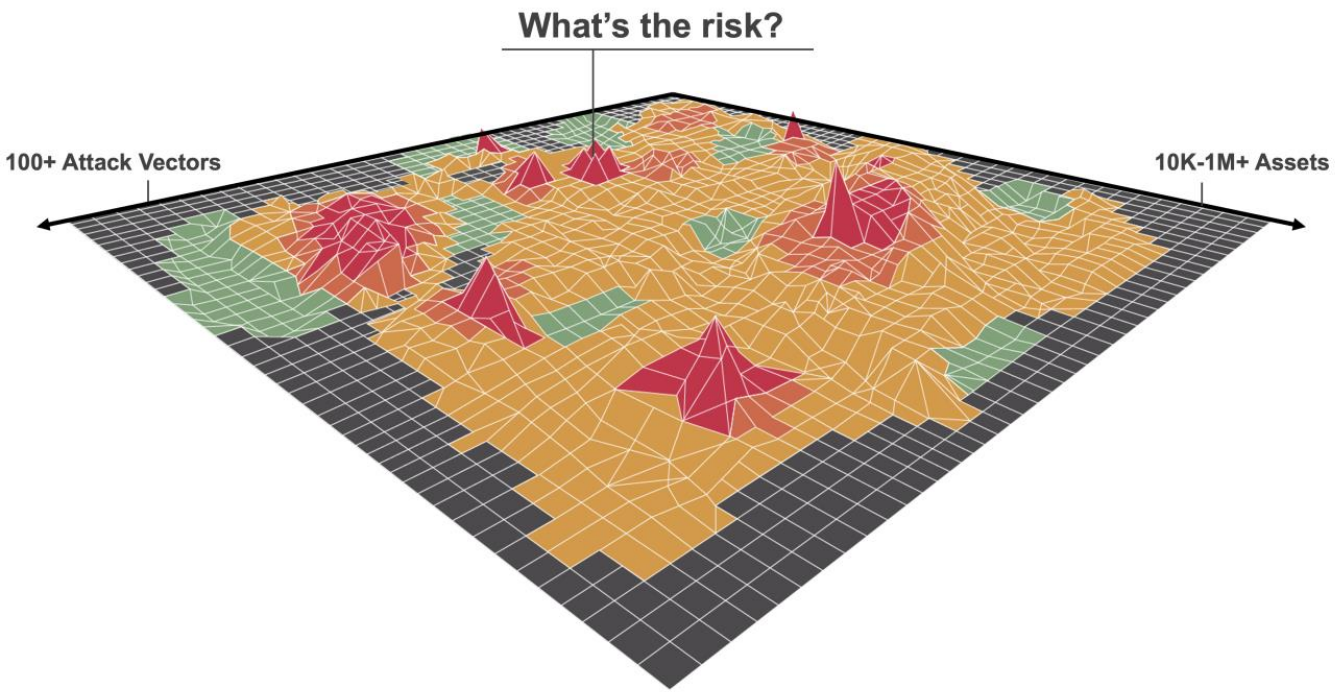
©2023 Flash Memory Summit. All Rights Reserved

Cybersecurity Landscape

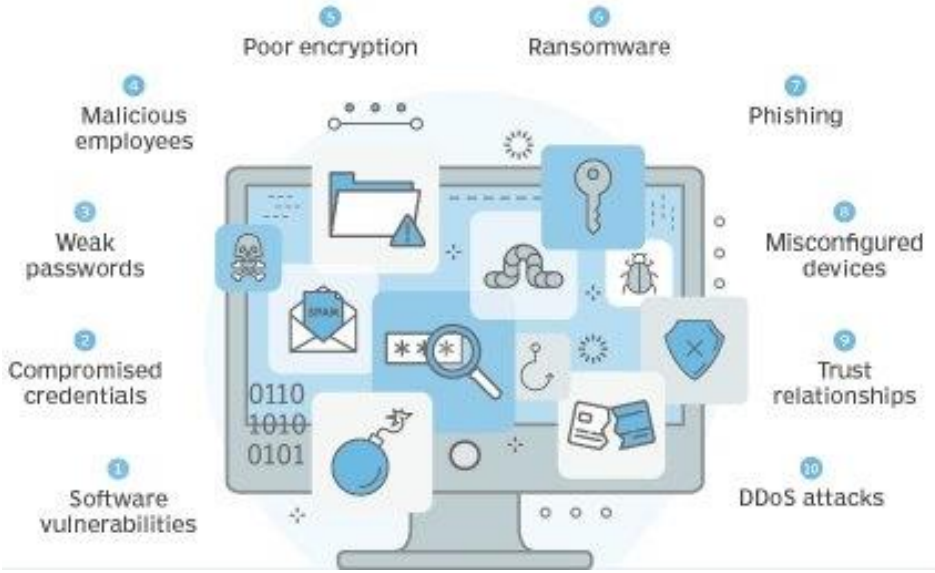


©2023 Flash Memory Summit. All Rights Reserved

Attack Surface & Attack Vectors

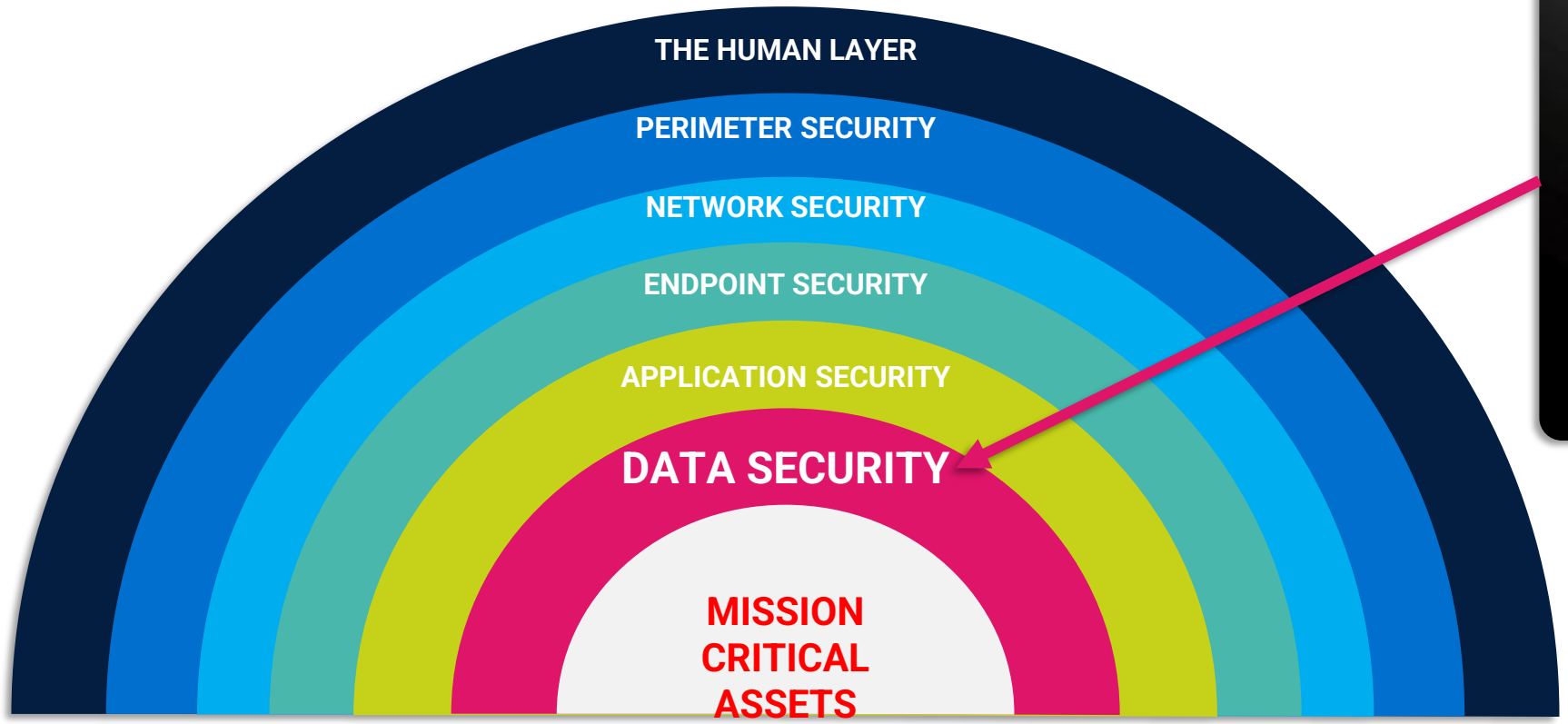


10 Common Attack Vectors



©2023 Flash Memory Summit. All Rights Reserved

Data Safety, Privacy, and Integrity



©2023 Flash Memory Summit. All Rights Reserved

Hardware-Based Security (Hardsec)

Flash Memory Summit

c8secure
A Continent 8 Company

CYBERSAFE
YOUR SECURITY, OUR PRIORITY

CYS

ISACA
Singapore Chapter

Standards Development Organisation

FIPS VALIDATED 140-2

Common Criteria

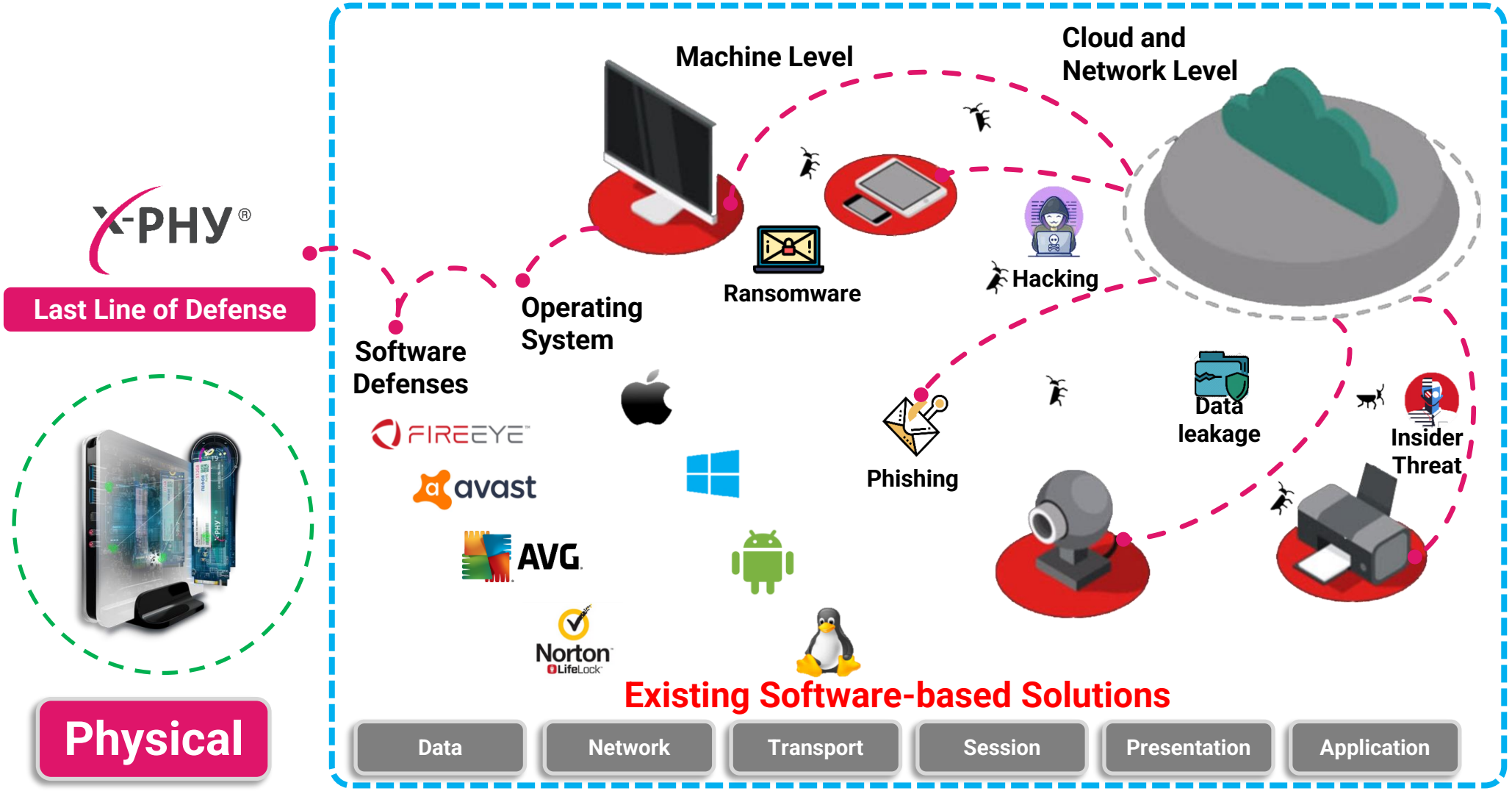
PHASE 01 — Endpoint Security

PHASE 02 — System Security

PHASE 03 — Standards & Ecosystem

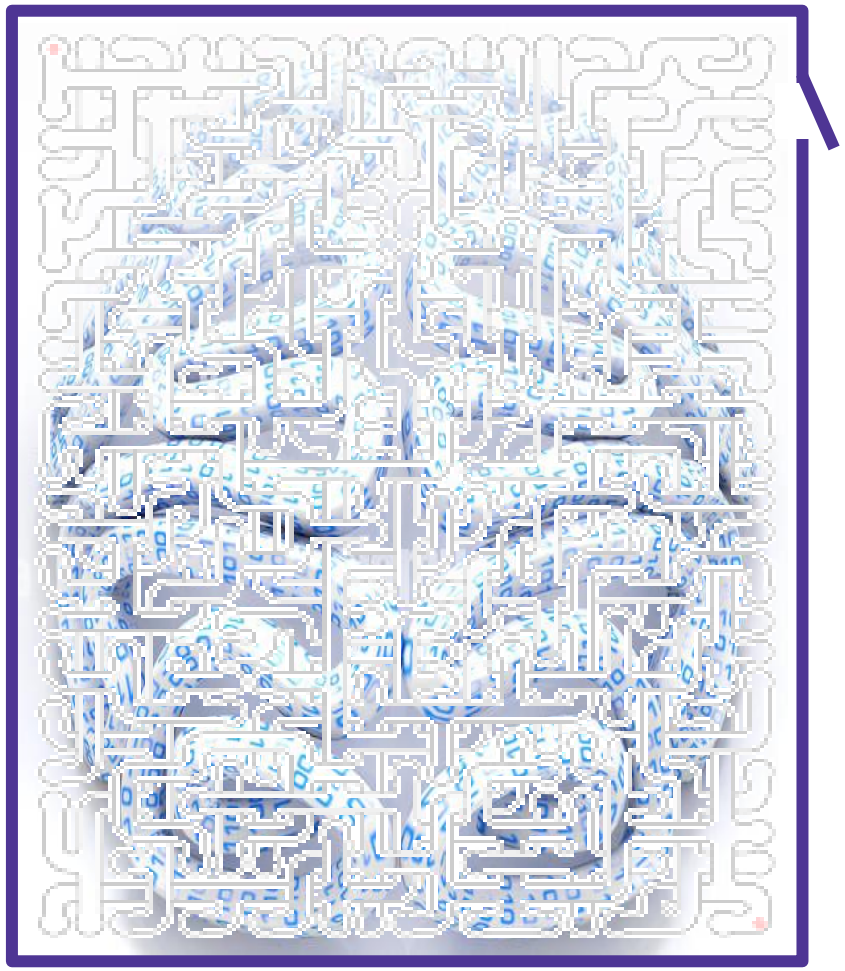
©2023 Flash Memory Summit. All Rights Reserved

Why Data Storage (SSD)?



©2023 Flash Memory Summit. All Rights Reserved

Why Data Storage (SSD)?



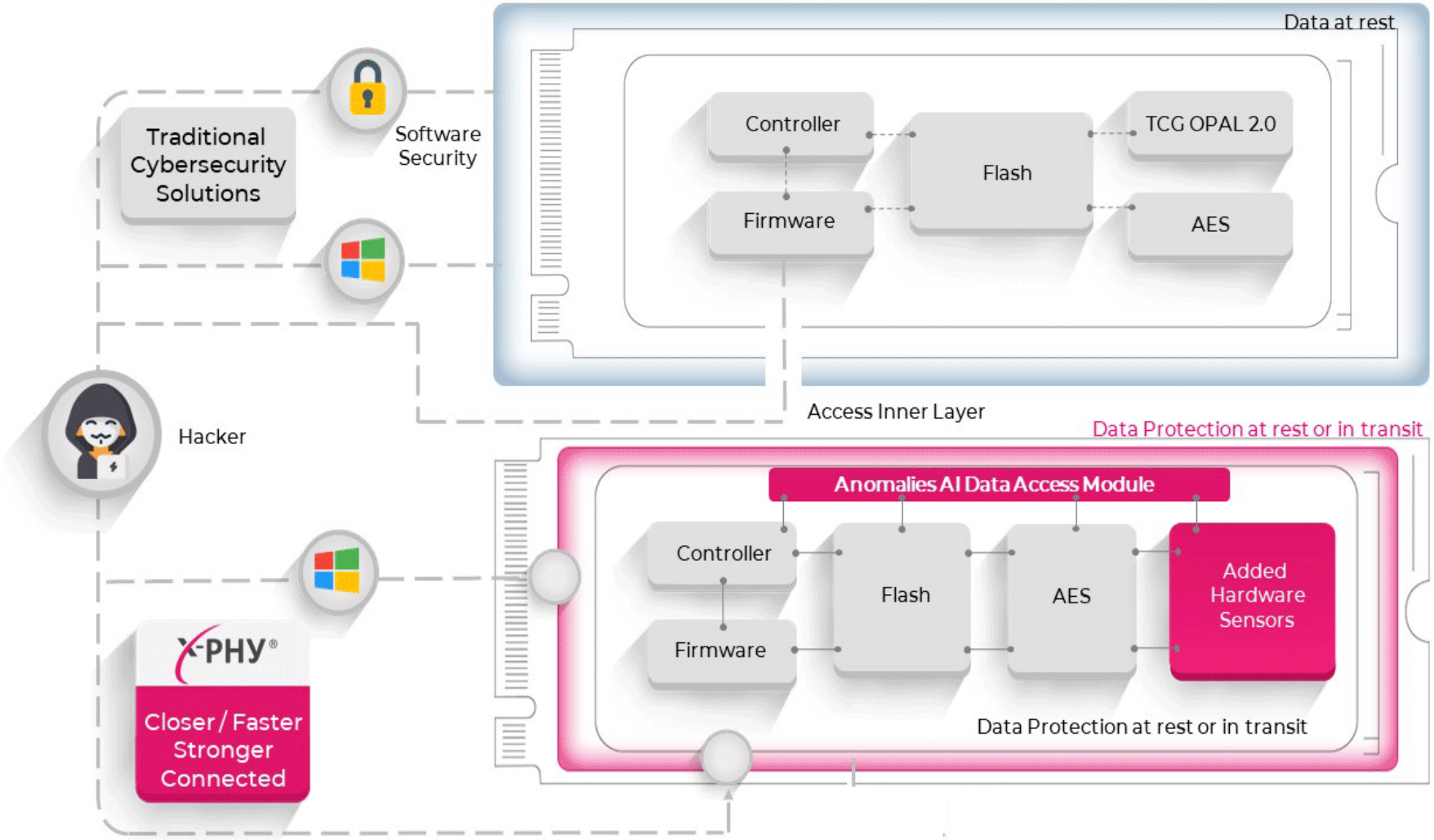
One Door Access PCIe/ NVMe
All data streams must go through a single door access point, reducing the risk of unauthorized access to the data.

Closest proximity to Data
Embedding dynamic cybersecurity features for real-time detection and response.

Artificial Intelligence (AI) feature
Added into the controller to detect any anomalous read/write activities at memory level.

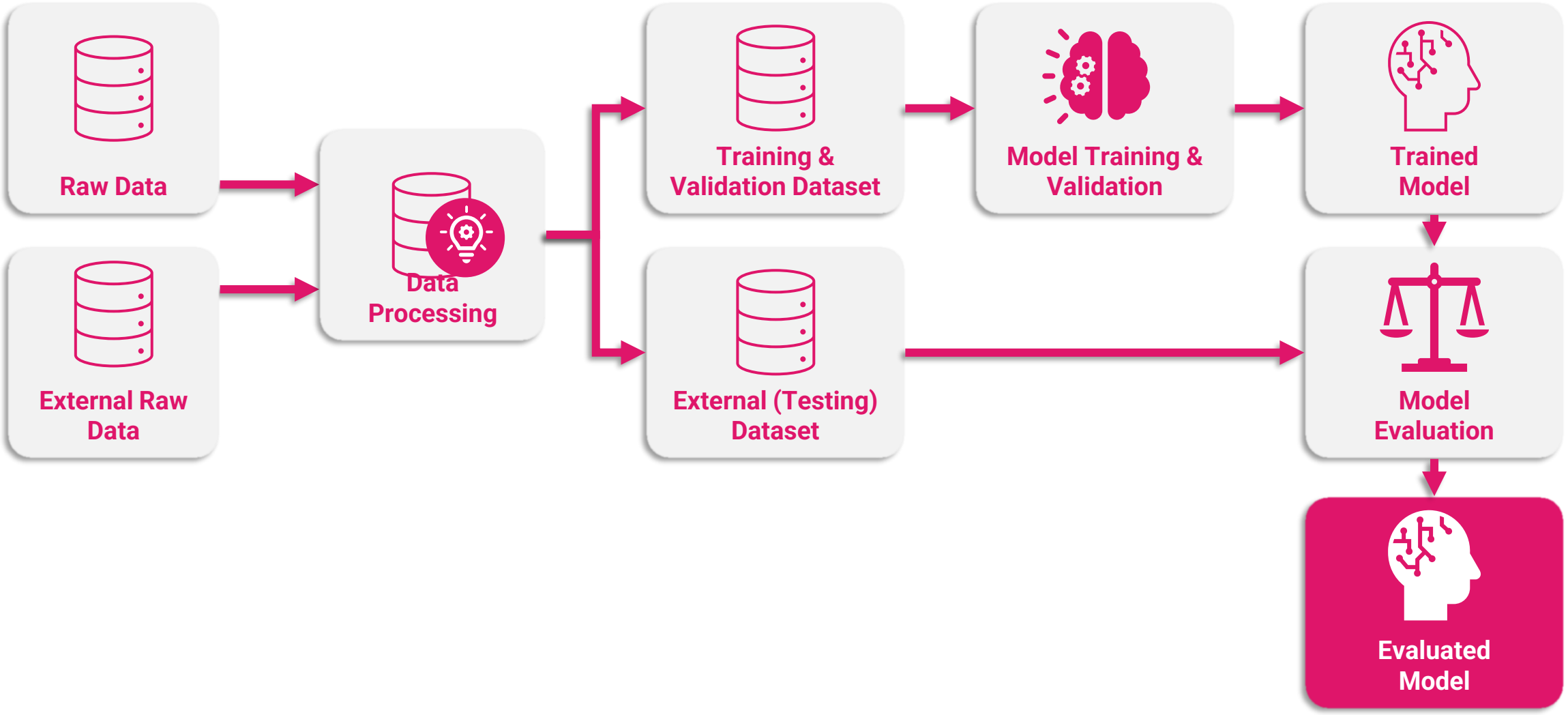
©2023 Flash Memory Summit. All Rights Reserved

AI-Enabled SSD vs. Traditional SSD



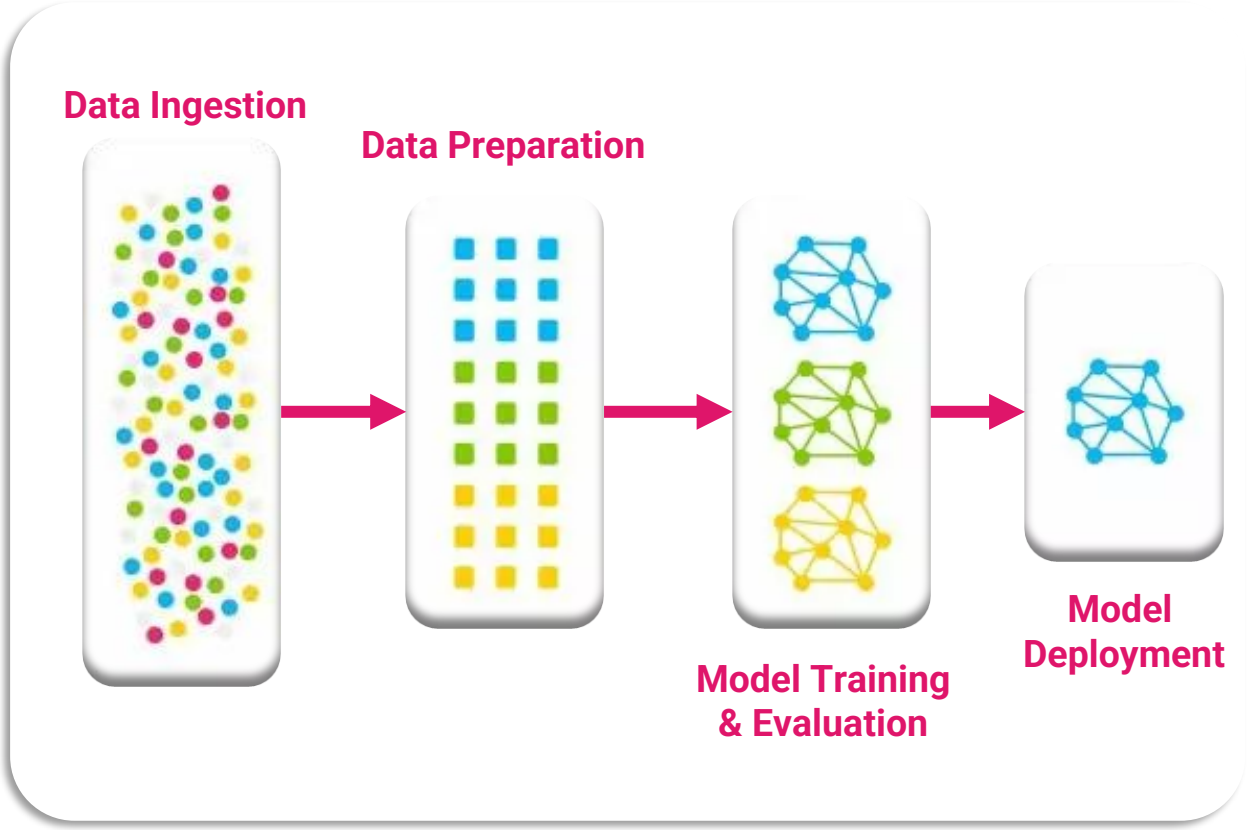
©2023 Flash Memory Summit. All Rights Reserved

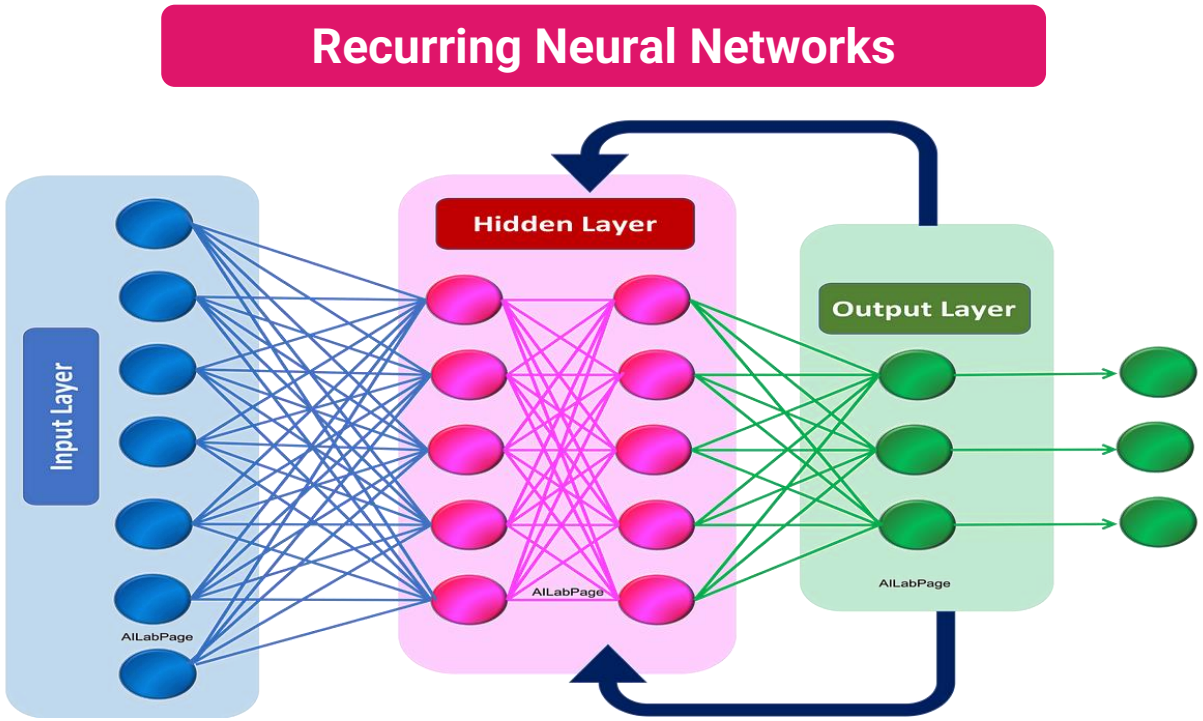
AI-Powered Analysis



©2023 Flash Memory Summit. All Rights Reserved

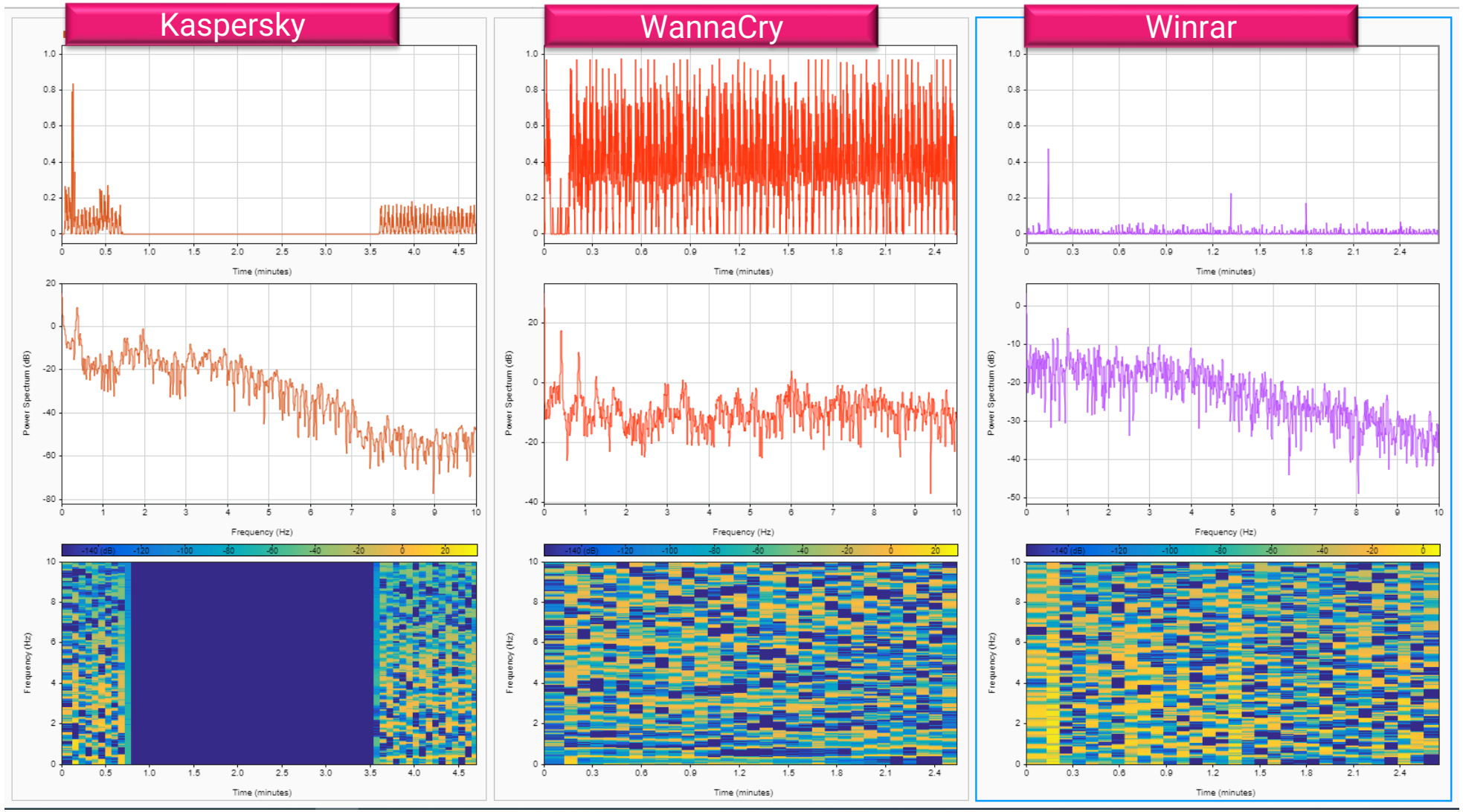
AI-Powered Analysis





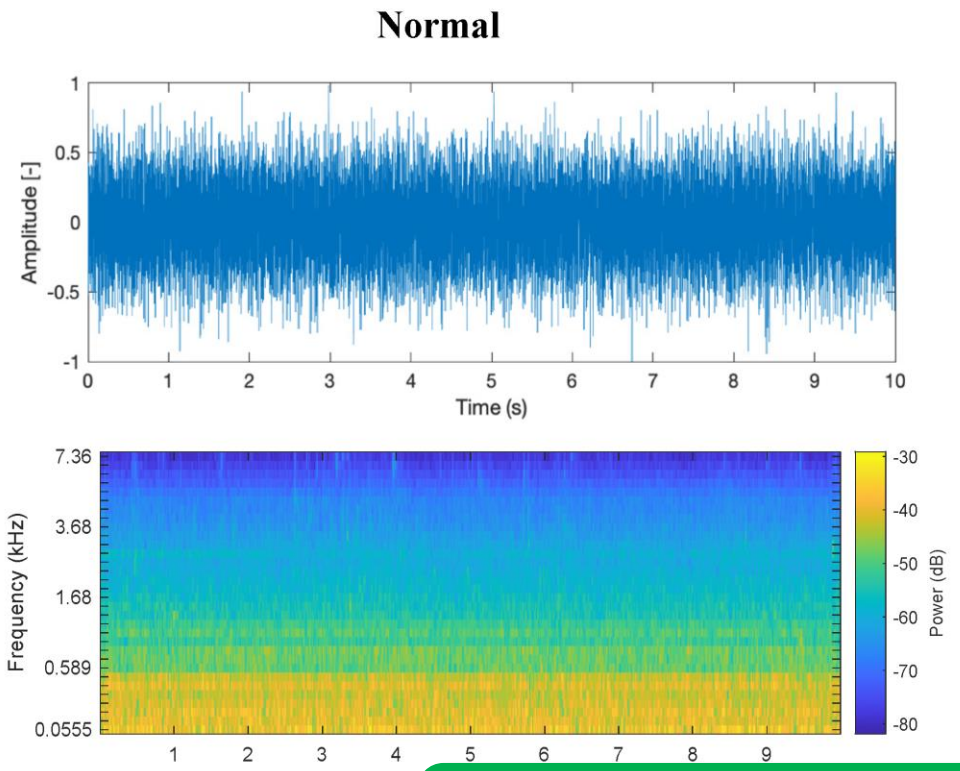
©2023 Flash Memory Summit. All Rights Reserved

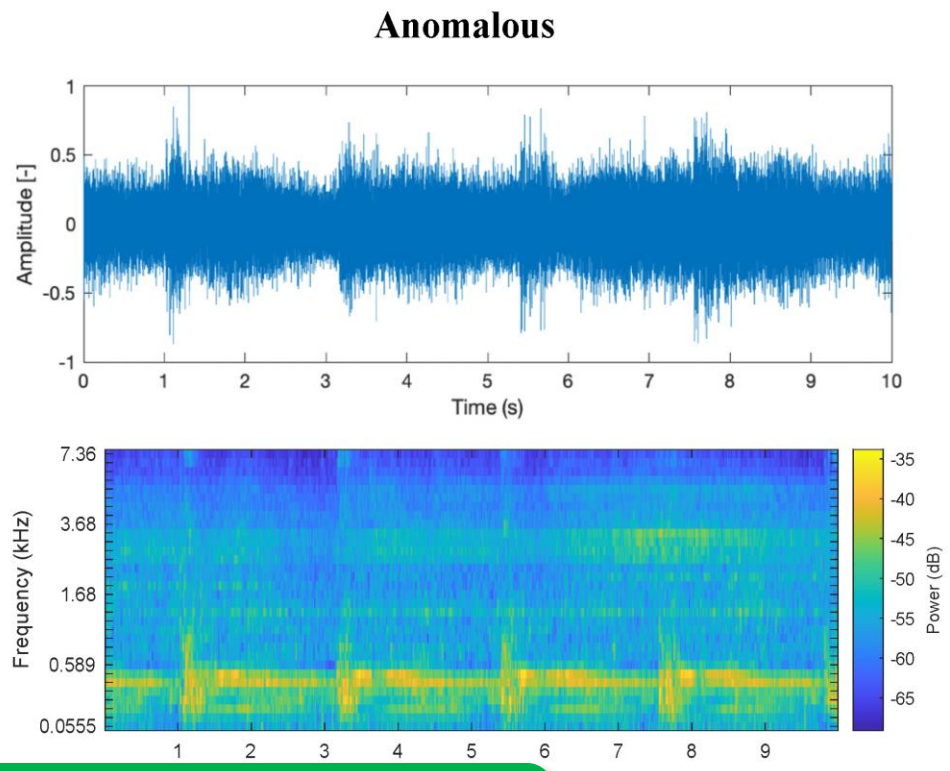
Distinguishable SSD Reads



©2023 Flash Memory Summit. All Rights Reserved

Anomaly Detection in SSD Writes

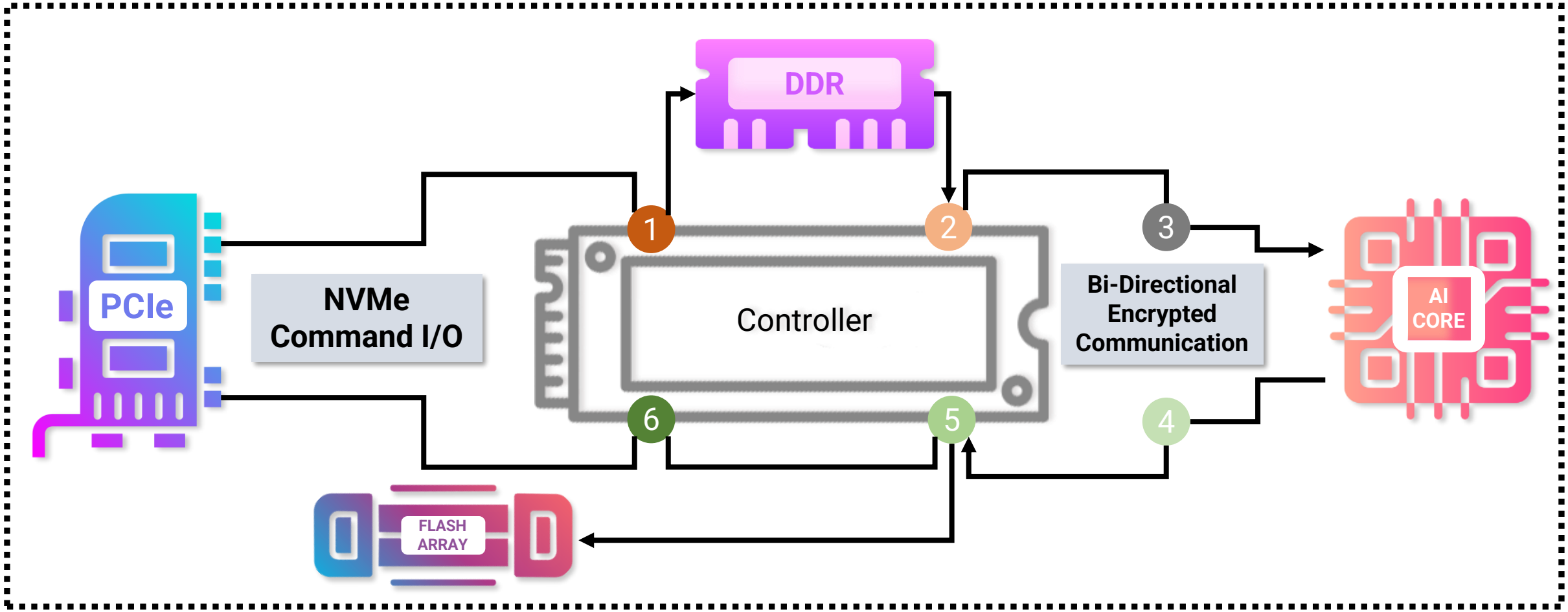




AI Validation Database

©2023 Flash Memory Summit. All Rights Reserved

Ransomware Detection



1 Submission queue

2 Extract attributes

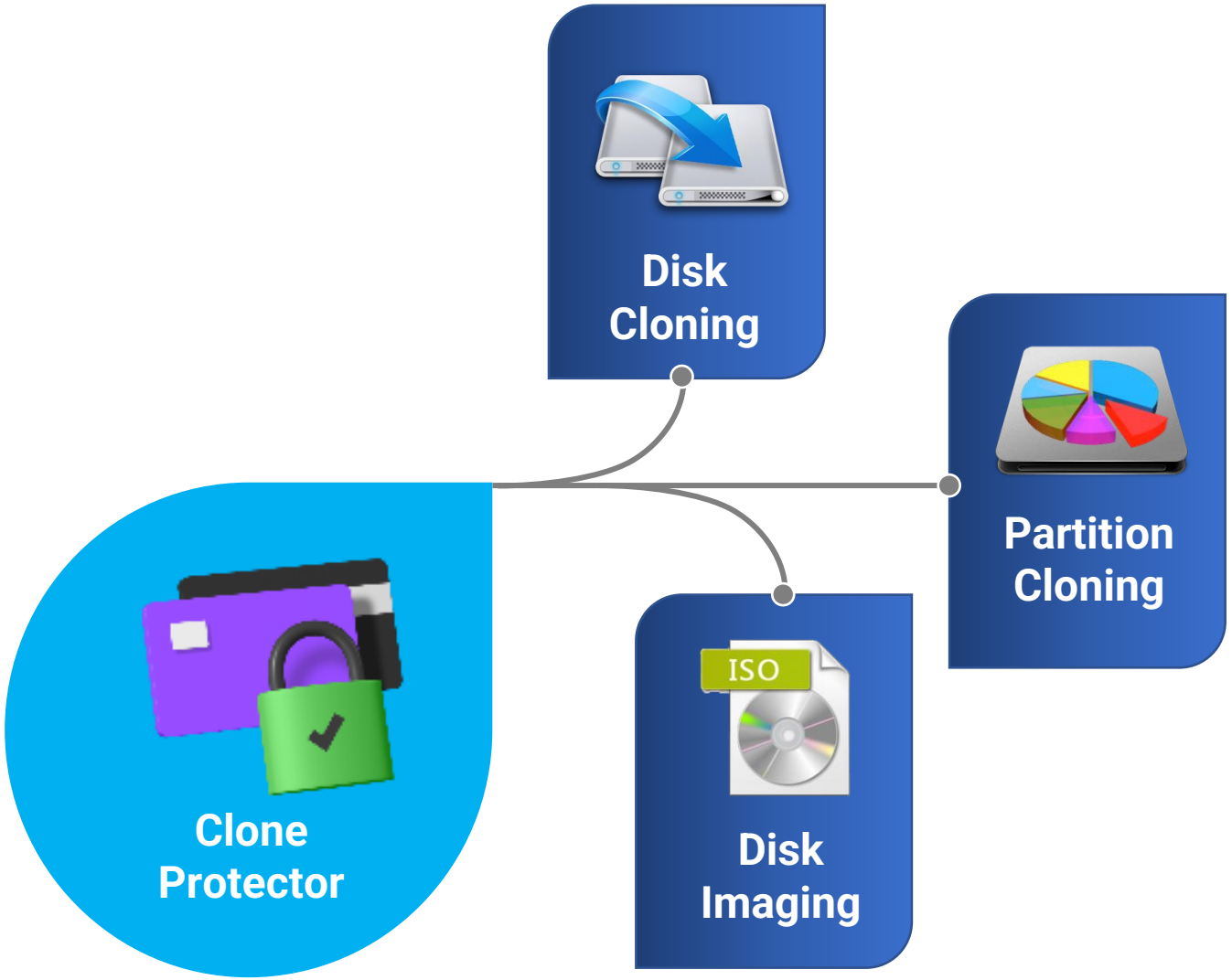
3 Search for ransomware

4 Return result

5 Data keep? (yes/no)

6 Return completion or error

Cloning Protection

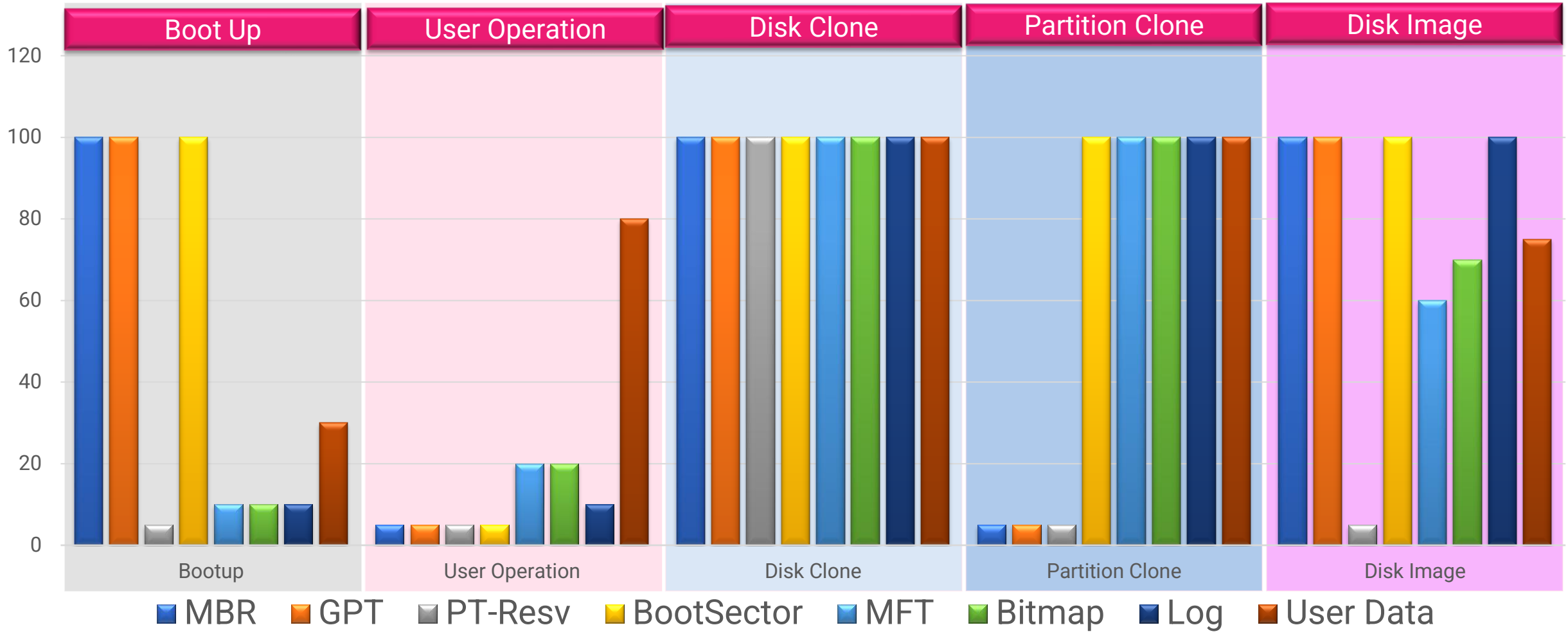


Functions Isolated from Host's

- Operating System (OS)
- Software
- Hardware

©2023 Flash Memory Summit. All Rights Reserved

Cloning Protection



AI Validation Database

©2023 Flash Memory Summit. All Rights Reserved

Multiple Simultaneous Cyberattacks

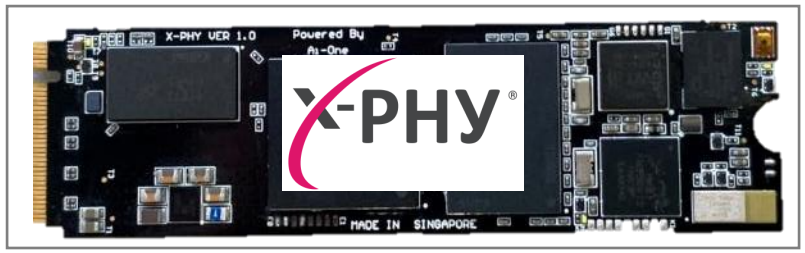
©2023 Flash Memory Summit. All Rights Reserved

Temperature Attack

USING HEAT SOURCE

Hackers try to **bypass 2FA**-AUTHENTICATION

Hackers **induce heating** to cause fault injection to CPU by causing magnetism abnormal



Heating up 300C on SSD IC for a couple of seconds

All log stored in SSD lock itself and enable **high level of security**

KALMANFILTER analyze the status to make sure it is not **drifting or wrong alert**

CPU check **internal + external sensors**

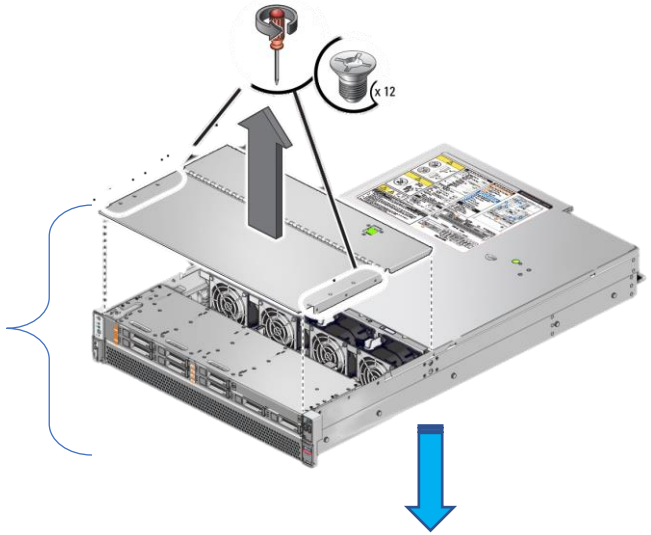
Temperature sudden rise within couple of seconds

©2023 Flash Memory Summit. All Rights Reserved

Tampering and Theft

Illegal Access

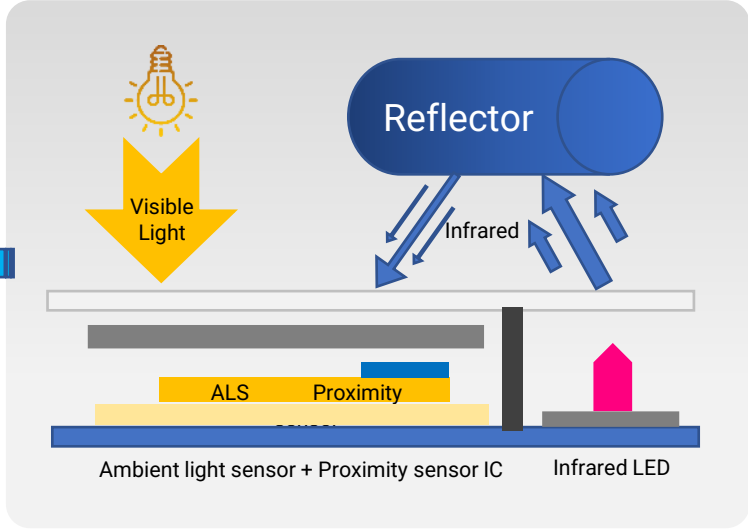
Cover open detected through Light or IR reflection in +/- 1mm accuracy



Security is at high level settings defined by the supervisor

- Rapid Purge Data or
- Lock SSD or
- Enable Alarm over Wireless gateway

Sensors embedded in X-PHY PCB



©2023 Flash Memory Summit. All Rights Reserved

AI-Enabled SSD (X-PHY®) Prevents…

Flash Memory Summit

- Ransomware
- Cloning Attacks
- Malware
- Heat & Cold Attacks
- Insider Threats
- Physical Theft of Drives

©2023 Flash Memory Summit. All Rights Reserved

X-PHY® vs. Software-Based Protection

		X-PHY®	Software – Signature Based	Software – Behavioral Based
Detection approach	Method	**Data Access Pattern (Read / Write)**	Signature Library	Behavioral Patterns
	Perimeter	**Internal Protocol**	External Environment	
Human Intervention		**None**	High	Medium
Zero-day Protection Coverage		**Tested with 100% accuracy**	Low (Known threats only)	Medium (Defined variable and threshold)
False Positive		**Low**	High	Medium
Physical Protection		**Yes**	No	No

©2023 Flash Memory Summit. All Rights Reserved

Questions?

Flash Memory Summit

THANK YOU

Erik A. Nilsen, PhD

Chief Technology Strategist

eriknilsen@flexxon.com

FLEXON

©2023 Flash Memory Summit. All Rights Reserved

CONTACT US

SINGAPORE
28 Genting Lane, #09-03/04/05 Platinum 28,
Singapore 349585
Tel : +65-6493 5035
Fax : +65-6493 5037
Email: flexxon@flexxon.com

HONG KONG
Workshop 3 on 2/F,
Wah Lai Industrial Centre,
NOS 10-14, Kwei Tei Street,
Shatin, Hong Kong.
Tel: +852-2711 5886
Fax: +852-3011 3058

X-PHY® Last Line of Defense
www.x-phy.com

©2023 Flash Memory Summit. All Rights Reserved