X-PHY®

AI Embedded Cyber Secure SSD

Table of Contents

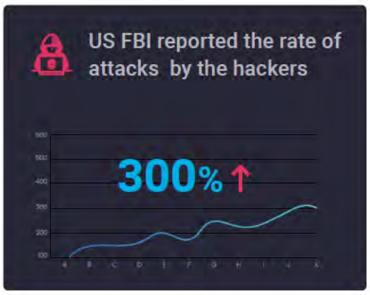
X-PHY®
HARDWARE-BASED CYBERSECURITY SOLUTION

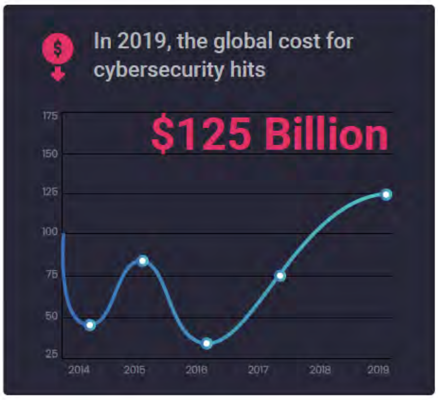
1.0 Executive Summary

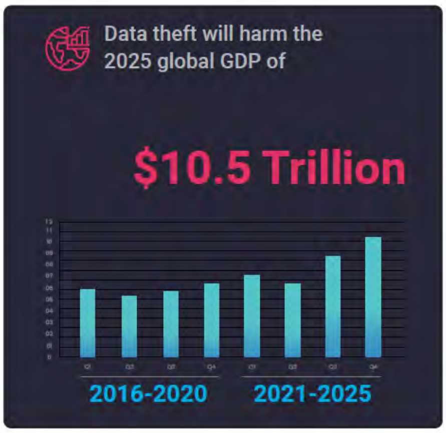
The threat of cybercrime has always been a challenge over the years and especially in today's technologically dependent world where data security plays an extremely important role for all organizations. Projected by Cybersecurity Ventures, the cost of cybercrimes will greatly increase from $3 trillion in 2015 to over $10.5 trillion by 2025. Also, 63% of the companies have reported that there was a potential compromise due to hardware or silicon-level security breach over the past 12 months.

Cyber-attacks can occur anytime from anywhere. The non-volatile SSD memory devices have high market demand due to its reliability and endurance. On the other hand, these are vulnerable to malware, ransomware, and viruses. Flexxon understands that protection needs to available right at the NAND flash level.

Cyber-threats unfold the chances of your valuable data can be at risk of being theft or manipulated. The cyber-attacks are occurring quite frequently and the rate is alarming.







In a comprehensive cybersecurity system, the security of all hardware and software components used in PCs are crucial. Computers hold a significant amount of information and data. In geographically-restricted local networks, this data comprises billions of pages of graphics, texts, and other sources of information through the internet.

The purpose of cybersecurity includes protecting data and property from corruption, theft, or attacks while allowing the data and property to stay accessible and productive to its intended customers.

Today’s challenges:

2.0 Current market cybersecurity solutions are reaching its peak

In our rapidly expanding digital world, spanning over hardware and software that powers everything from our personal devices to the global infrastructure; Cybersecurity is a key foundation. Over the years, while significant progress has been made in many security domains, especially in maturing secure software development processes, hardware security has received limited attention.

Many companies have implemented leading cybersecurity software systems to protect company and customers’ data from the different types of security threats, rendering protection of business data a core business initiative. That alone, however, is not enough.

2.1 Over reliance on software-based defenses

Security and risk management leaders cannot predict future threats but can use the past as an indication of what to prepare for. Current cybersecurity standards are over-reliant on software protection despite modern cyber-attack methods and techniques being capable of penetrating even beyond cloud-based networks.

Software-based cybersecurity solutions could be compromised, spreading damage down to machine-level targeting OS and autonomous end-points which could cost millions and billions of dollars to recover. Thus, a revolutionary solution to rethink how we defend our digital assets is necessary.

2.2 Lack of cybersecurity awareness

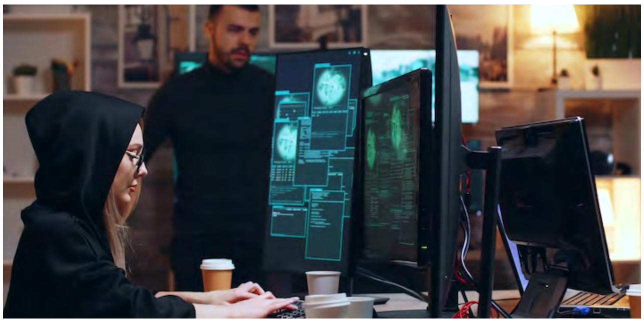
There is no shortcut to implement for cybersecurity such as “Do this and you are safe.” It is rather an ongoing process of constant learning, adjusting safety standards and processes for organizations, and shifting trade-offs between business risks and objectives. Cybersecurity requirements are relatively new to many organizations requiring resources and focus to tackle them.

As security becomes another business requirement, there is a natural concern about whether it slows down the development process, delays the time to market, and therefore impacts the business. For security programs to be successful, it is imperative that it minimally weighs on development velocity, to avoid creating conflicting choices between product security and timely product delivery.

2.3 Reactive approach is always one step behind

Today cybersecurity is addressed in mostly disconnected silos. Yet, security is a system property that, in order to be comprehensive and responsive, must be considered across domains (hardware, software, firmware, OS, application, network, cloud, etc) and across the system lifecycle (design, development, manufacturing, supply chain, support, and maintenance, etc). For instance, when the Spectre hardware vulnerability was discovered, it was clear that many microprocessors are impacted and cannot be replaced quickly (not to mention the time it takes to re-design and manufacture new parts). As a result, the attention quickly shifted to software, operating system layers and software applications running on it which could be hardened to prevent possible hardware attacks.

What this actually means, is that hardware security is a critical foundation of overall system security and that its integration with “downstream” solutions will enable a more impermeable and higher-responsive approach to cybersecurity.



In today's cyber landscape, modern apps like smart grids, connected industrial systems, autonomous driving, and connected cars broadly summed up under the term IoT have an enormous demand for reliable security.

Under traditional use-cases, for example, authentication of parts, their unique identity, safeguarding and monitoring of system protection is the primary element while system integrity and data security are prerequisites for the successful implementation of new apps and services. The aforementioned, however, requires a significant amount of human intervention and is more of a reactive approach to system security.

Therefore, the need for an integrated system solution, grounded on secured hardware, that secures infrastructure and components from fraud, attacks and sabotage has led to the establishment of modern solutions. In fact, we need hardware that allows software storage, running and upgradation in a secure way that complements the existing framework.

2.4 Encryption Tools could backfire to aid cyberattackers

First, by understanding the principle of encryption and the objective of ransomware hackers, you will be able to know that they do not perpendicularly meet. In other words, their objective is not to read the data that is in there but rather to disallow the user to access the data by adding another lock over it using an encryption tool.

Furthermore, traditional encryption tools actually aid hackers by masking their detection from anti malware tools. By taking advantage of encryption, attackers can bypass most inspection tools to deliver malware inside the system. The encrypted data exfiltration also bypasses security tools without scrutiny.

F5 Labs [1] threat research shows that **71%** of malware uses encryption to hide when it communicates back to command and control locations. Additionally, **57%** of malware sites and 95% of phishing sites were accessed just one time, complicating incident response investigations.

Cybercriminals know that organizations have trouble decrypting and inspecting data traffic—and they use that to their advantage. Using malware such as spyware, ransomware, and rootkits, as well as exploits, attackers can compromise users, networks, and applications to steal personal data. Encryption without filtration will not be able to combat real cyber-threats as the tool will simply be blindly encrypting the files without scrutiny causing even more complications for detection procedures.

[1] https://www.f5.com/resources/library/encrypted-threats/ssl-visibility

3.0 Why X-PHY?

What can X-PHY® prevent:

Ransomware	Cloning Attacks
Malware	Heat & Cold Attacks
Insider Threats	Physical theft of drives

3.1 Security is the system property rooted in Hardware

To ensure optimal cybersecurity, we have developed a hardware-based AI-embedded solution within the firmware-level to close off this gateway of cyber threats at physical layer. By positioning ourselves within this level, we are able to detect anomalies in data access patterns along with the integration of hardware sensors, enabling users with next-level real-time and physical protection capabilities whenever there is a detection of a breach at any of the security layers.

X-PHY® will always be the last line of defense by being at **the closest proximity to the data stream and reacting at a moment's notice by creating a one-ended lockdown environment.** So rather than having users worry about where the various threat vectors are originating. **We focus our solution on positioning ourselves at the choke point of all Ransomware attacks and defeating the malware at that location.**

3.2 Eliminating the weakest link in cybersecurity

Traditionally. We have been relying on Anti-virus software, which requires constant updates, to defend against cyberattacks. Anti-virus software is operating in an open environment where every update on the software poses a new vulnerability to the environment which has to be protected by threats and various attack vectors.

That is why most anti-viruses are unable to flag malicious files whose signatures have not yet been identified. Hackers often take this opportunity to bypass by changing the file's signature and launch the so-called "Zero-day" attacks.

3.3 Zero Trust Security Framework

The goal of cybersecurity is to protect the enterprise at all costs, leaving no potential threat unattended. This goal is achieved by the X-PHY® zero trust model. This model leaves no room for protocol or courtesy for senior employees and treats every insider alike; with suspicion. It requires proper authentication for every single access granted. Every person or system accessing any other system or service first undergoes a multi-factor authentication process and yet their activities are monitored and logged.

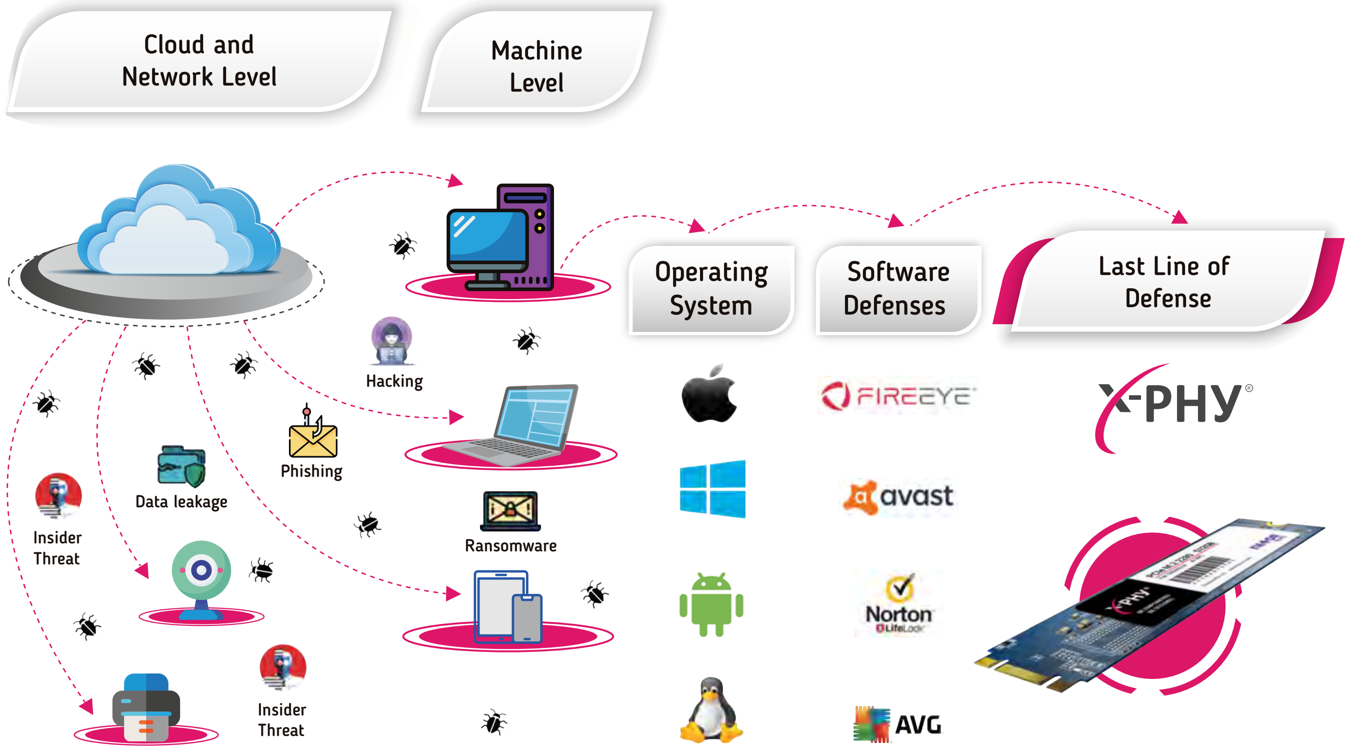
Event logs and access patterns are necessary to detect any anomalous behavior from insiders as well. Many unsuspecting people may believe that they are safe from insider attacks if their employees are happy. It may be true in some cases, but this is putting too much faith in human nature. There will always be someone unhappy, disgruntled or simply negligent. This is where the zero trust model comes into play.

Everyone gets access to the inside through a standard procedure with no inherent trust involved. In fact, according to the **2020 insider threat report by cybersecurity insiders, 68% of the organizations feel moderately to extremely vulnerable to insider attacks.**

In addition to that, the total average cost of insider threats rose from $8.76M in 2017 to $11.45M in 2019, as per the global reports of The Ponemon institute of 2018 and 2020 cost of insider threats. A zero trust model would mean protection from all angles, whether internal or external. Our X-PHY® SSD being the latest innovation in the cyber security world works on this principle of zero trust. It not only protects your systems from external attacks, blocking the execution of all malware, but it also maintains authentication and access controls for insiders. In case of social engineering attacks, it will block the execution of malware and will immediately lock the device until a user unlocks it with proper authentication.

You just have to install it in the system and it'll save you from the hassle of responding to threat alerts, because it is an independent AI-based solution.

3.4 Filling the cybersecurity gaps in data protection



Cybersecurity is dependent upon software protection but modern cyber-attacks go beyond that like cloud-based networks. The threats will flow from the cloud network to the machine-level that target the OS, autonomous, and endpoint devices. This forces the users to rely upon the software defenses. But what if the cyber threats bypass it too? Your data will be at risk and this may cause severe damage and cost millions and billions of dollars to recover. So, top-notch cybersecurity from the firmware level is a must.

Existing cybersecurity solutions are focused on 6 of the 7 layers in OSI architecture, neglecting the physical layer. With the X-PHY, we have addressed a glaring gap in the cybersecurity market, with this patented technological breakthrough. Any change to the physical conditions of your device can leave your data open and vulnerable to attacks provides the consistent environment you need.

By introducing an intelligent and self-learning layer of cybersecurity protection at the firmware level that functions as an added hardware sensor, the X-PHY provides autonomous data protection on the SSD drive at the physical layer.

3.5 Physical Attack Protection

X-PHY® perfectly harmonizes the firmware and hardware, an array of sensors embedded within the hardware utilizing AI for detecting and preventing any form of physical attacks. X-PHY® monitors any request to the SSD in the NVMe protocol whenever the user touches the data. Once ransomware is detected, it will block access and lock down the drive immediately.

Monitoring the power and temperature fluctuations, with physical protection ensures that the data is protected at the source. X-PHY® detects any physical changes or anomalies to the device, preventing any opportunities for the data to be exposed to threats, and assuring users' peace of mind.

3.6 Utilization of Advanced Encryption / Decryption Functions

X-PHY® utilizes a multitude of processes such as inter-chip communication protection, True Random Number Generator (TRNG), Advanced Encryption Standard (AES), and much more to perform SSD encryption and decryption with a specified cryptographic keyc and algorithm to filter malicious codes in ensuring endpoint data security. Inter-chip communication protection is executed by generating cryptographic keys in accordance with a specified cryptographic key generation algorithm, ECDH curve secp192r1 (NIST 192-bit) to **avert any form of data probing.**

At the same time AES, when it comes to the X-PHY®, it performs SSD encryption and decryption in accordance with a specific cryptographic algorithm AES-XTS 256-bit that meets NIST SP800-90B standard whilst also implementing TRNG to achieve a cryptographic key size of 512-bits. Resulting in data protection with the largest bit size that is known and is practically uncrackable by brute force, based on the latest computing standards.

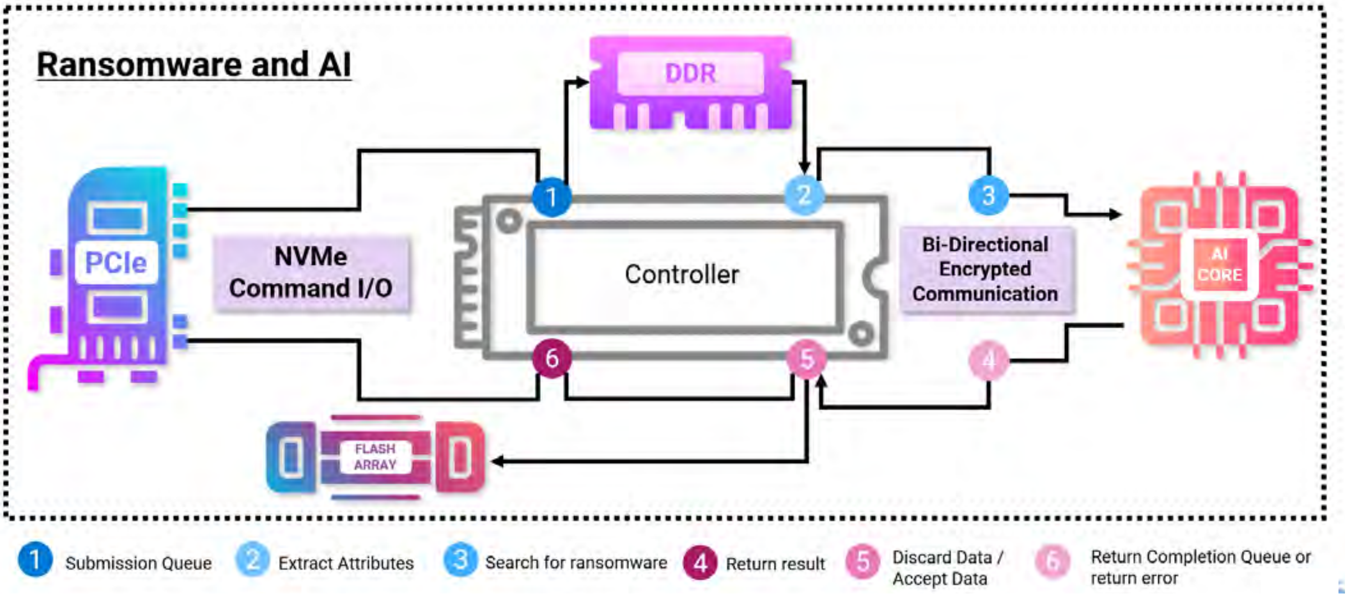
AES is one of many NIST-issued Federal Information Processing Standards (FIPS), which is recognized by the US Secretary of Commerce to ensure legal alignment with the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987 and is renowned to be invulnerable to all attacks and virtually impenetrable even with the use of sheer brute-force methods.

Through this, X-PHY® in itself provides an interconnected, highly secured data encryption system that works as a standalone and therefore does not require any other forms of encryption tools when in operation.

HOW CAN X-PHY® PREVENT AND DEFEND AGAINST CYBERATTACKS?

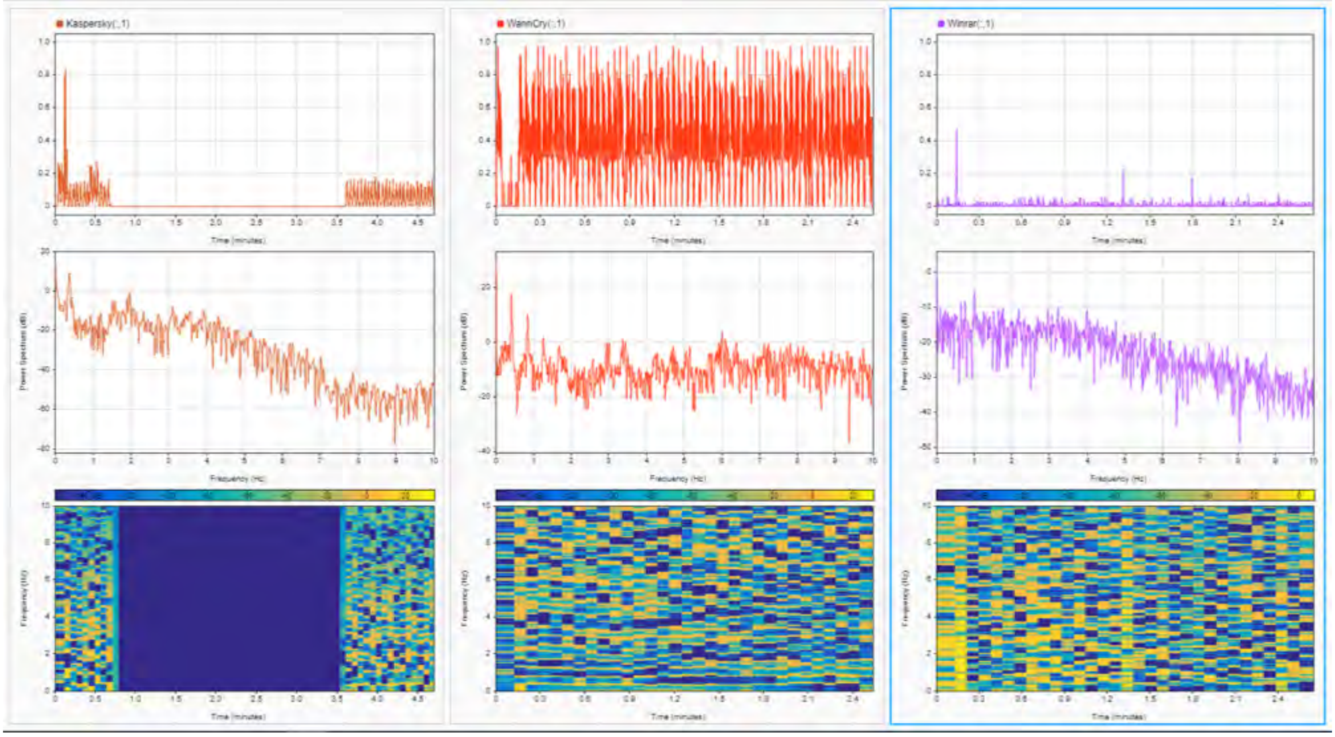
4.1 Ransomware Attacks

X-PHY® solution provides the last line of defense inside the SSD at the NVMe layer. We have developed a lightweight layer inside the SSD firmware at NVMe DoorBell commands processing module and our approach processes only the doorbell IO command not the actual data so there are no changes in the performance of SSD. This is further reinforced by using the AI one core solution to combat against evolving threats. X-PHY® places the threat detection and resolution right at the NAND device-level with an Anomalies AI Data Access Module to have end-to-end data protection within the drive which is beyond software protection.



In the PCIe SSD environment, every NVME's Read/Write command I/O will have to pass through the controller before it goes to DDR SDRAM. DDR SDRAM will process and extract critical attributes to be shared with AI-core so that it can analyze and search for ransomware based on the read/write pattern. The data will then be analyzed and mined. ID3, KNN, RNN etc will then be used to classify the result. If found to be malicious, the action will be declined and the controller will trigger to lock down the access immediately until authenticated.

In our approach the detection and prevention is at SSD level rather than application/OS level, so it doesn't need any additional software and hardware configuration and is independent of the operating system and hardware architecture.



NVMe protocol has 2 primary Commands, read/Write. During the direct access to the SSD from the host, we dynamically construct a virtual table to list all logical block addresses and each LBA has a sub-table to see how many are written and overwritten during a period of time. This information will help to create attributes for the AI-one core. **Above diagram illustrates one of the attributes - read pattern.** Although the behavior might seem similar to a user's, the actual patterns will still allow us to differentiate the variation between one activity to another.

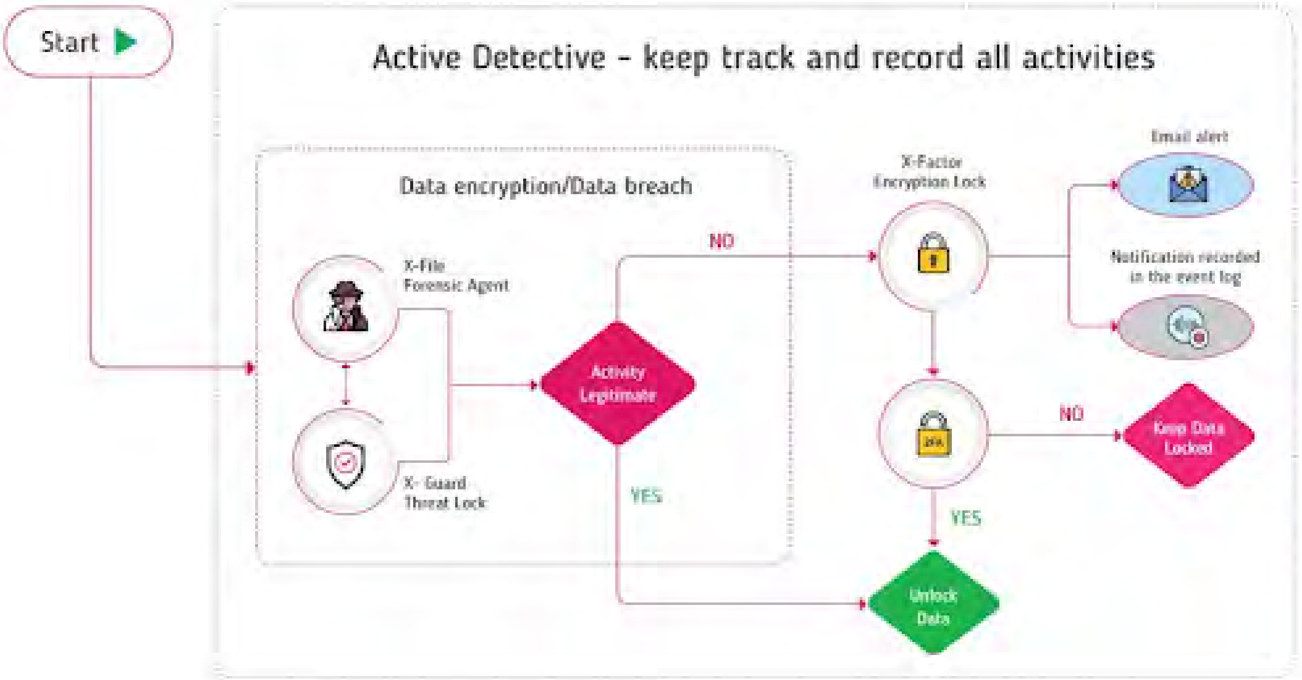
When **Fast Fourier Transformation (FFT)** is applied, X-PHY® converts it from time domain to frequency domain, leading to the generation of power spectrum estimation, which creates a unique pattern of AI for different applications. The AI-pattern of X-PHY® is used for training and in case there is a similarity during the real-time protection and detection, this AI-pattern will be able to identify it from unseen patterns. The AI-pattern of X-PHY® must have a prediction capability along with auto-updates based on continued learning of the extracted attributes. The detection performed by X-PHY® is not based on read/write command, but rather the patterns of the read/write activities. By deploying the multi-tiers detection mechanism, the detection rate of X-PHY® is almost 100% with no limitation.

Scenario of a Ransomware Attack and how X-PHY® protects your data

1 User clicks on phishing email and unknowingly executes a ransomware file.

2 Once the AI One Core detects ransomware, it will stop all read and write activities and then subsequently lock the SSD and immediately shut down the PC.

3 Should the PC be connected to the internet, an email notification will be sent to the registered email to notify the IT Administrator that there was a ransomware detected in one of the company's endpoints. In addition to the email notification, if the host is offline the event log will be stored in the firmware and can be accessed via the X-PHY® PC User Application Tool.



4 Upon the next boot up, the PC will only be able to boot up to the BIOS screen.

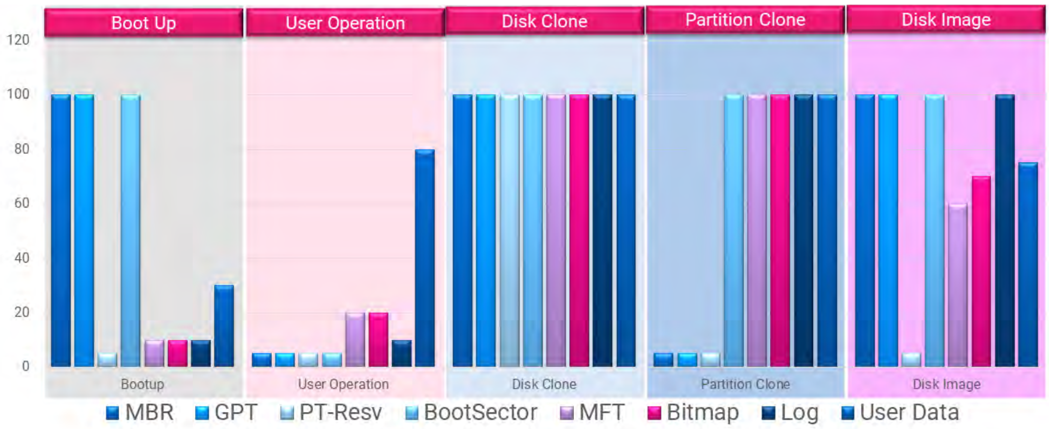
5 End user will have to use either the X-PHY® mobile connect application or plug in the locked SSD as an external drive to a PC with the X-PHY® PC User Application Tool to unlock it. The unlock process is protected by multi-factor authentication whereby a password and OTP from either Google or Microsoft Authenticator is needed to complete the unlocking process.

6 Once the IT administrator has unlocked the SSD, the PC will be able to boot up to the OS and he/she will be able to isolate the endpoint to perform necessary actions for removal of the ransomware.

4.2 Cloning Attacks

Cloning is the process of one-to-one transfer of the entire contents from one storage to another storage. Imaging is the process of creating an archive of the used LBA of a hard drive as a compressed file. The techniques are used for hard drive migration and backup, but unfortunately, it also provides the easiest way for data theft, the data security and integrity are the biggest pain point of most of the service-based MNC due the NDA signed with clients' and customers' information servers and databases (name, email, password, credit card) are most vulnerable for data breach, extracting individual user's data from database and copying it is more difficult and time consuming process, but cloning is simplest method for data hacker and also it can extract signature of the source disk, so an attacker can extract the data at his own pace after cloning.

The cloning or imaging is detected within a few milliseconds and then both read and write access to the SSD will be denied. In our approach the detection and prevention is at SSD level rather than application/OS level, so it doesn't need any additional software and hardware configuration as it is independent of the operating system.



This approach supports four types of cloning:

Disk Cloning
Disk clone is complete SSD cloning from LBA 0 to MAX LBA based on the disk size

Partition Cloning
Clone individual partition instead of reading entire disk

Disk Imaging
The disk imaging work based on partition type, it will not read entire disk/partition, and it reads only the used LBA of the disk/partition using file system bitmap.

Files Copying
Copying files/data from the disk/partition

Scenario of Cloning Attack

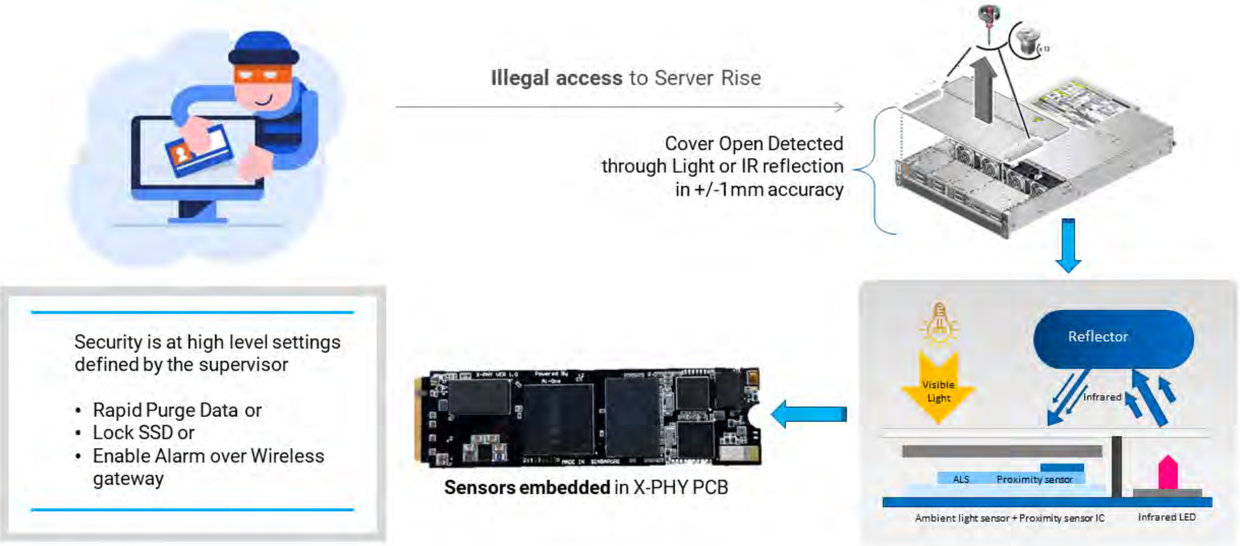
1. User connects to a public WI-FI.
2. Hacker finds a backdoor and manages to track the IP of the user's endpoint.
3. Hacker proceeds to clone the user's partition.
4. X-PHY AI One Core detects the read pattern of the hacker's cloning tool and immediately stops all read/write patterns.
5. The AI Once Core then proceeds to lock the SSD and shutdown the notebook.
6. The X-PHY User Application tool will send an email notification to the IT Administrator to inform he/she that a cloning attack was detected. Furthermore, the event log will also be stored in the firmware which can be accessed using the X-PHY User Application tool.

4.3 Physical Cyberattacks

In order to access confidential data on an SSD, an attacker may infiltrate the OS security over the network or gain physical access to the host. Though these devices usually have some level of security, passwords can be stolen. Once the OS protection is breached, traditional SSDs contain minimal security protections against sophisticated hackers leading to:

1. **Removal of SSD from the CPU**
2. **Probing the hardware data lines**
3. **Temperature attack**

The above are the types of physical attacks performed by the hackers to retrieve the confidential data from the SSD. X-PHY® is able to protect confidential data from intruders or hackers. We have successfully achieved these key features to protect the SSD by developing the firmware-level algorithms and mathematical calculation in a secure manner.



Security is at high level settings defined by the supervisor

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

Illegal access to Server Rise
Cover Open Detected through Light or IR reflection in +/-1mm accuracy
Reflector
Visible Light
Infrared
ALS
Proximity sensor
Ambient light sensor + Proximity sensor IC
Infrared LED
Sensors embedded in X-PHY PCB

Protection against the removal of SSD

X-PHY® has this enhanced security feature to completely lock down the drive upon detection of physical removal of SSD to secure the confidential data and protect against physical attacks. X-PHY® also features an optional function of Wipe Data that performs a rapid purge of confidential data upon detection of physical SSD removal. This optional feature will be useful for industries that are dealing with sensitive data or information whereby the consequence of confidential data leak is significant, thereby ensuring enhanced security.

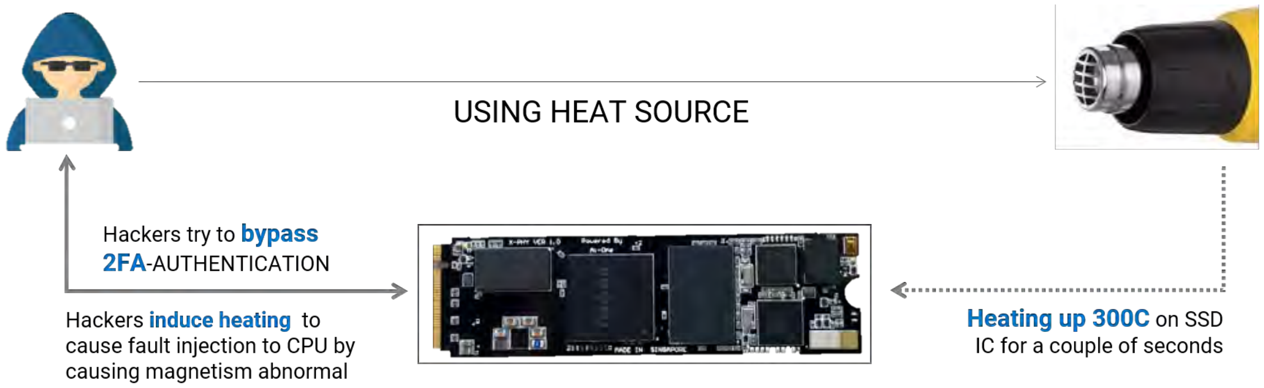
Protection against probing of hardware data lines

Probing data lines within the chipset is the most common snipping method from a hardware perspective, in this scenario, the data from the compromised drive will be retrieved completely without any issues.

Cyber attackers can use the compromised data as ransom to the organization which will be very detrimental to the organization which is keeping the confidential data in the Storage devices with the confidence that the data is protected by Anti-virus software or software level protocols.

Under these application level protection, the confidential information might not be as safe in front of the hardware data line phishing.

Protection against temperature attacks



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

X-PHY® protects against temperature attacks via the secure chip which performs continuous monitoring of the SSD's temperature and compares it against a configured threshold level. Upon detection of a sudden change in temperature, X-PHY® will lock down the drive and data access will be denied. The confidential data in the drive will be protected, rendering the temperature attack failed.

5.0 Conclusion

X-PHY® is the world's first AI-embedded firmware-based cybersecurity solution and the critical last line of defense against cyberattacks in today's highly interconnected landscape. With a multitude of access points through a range of IoT devices, endpoint security is essential in securing your devices and data. The integration of the X-PHY® at the core of each device grants enhanced security across the entire spectrum of IoT devices from mobile and personal computing devices, to servers, and core enterprise data storage.

This breakthrough technology detects anomalies in behavioral data access patterns and effectively shuts down potential known and unknown incursions in real-time, without the need for human intervention. This means that the X-PHY® effectively fends off Zero-Day exploitation, and provides protection against a range of cyberthreats including hardware attacks, malware, ransomware, and power glitches.

By introducing an intelligent and self-learning layer of cybersecurity protection at the firmware-level that functions as an added hardware sensor, the X-PHY® provides autonomous data protection on the SSD drive at the physical layer.

Awards and Certifications

CSA SINGAPORE

COMMON CRITERIA CERTIFIED EAL2+

Black Unicorn Award

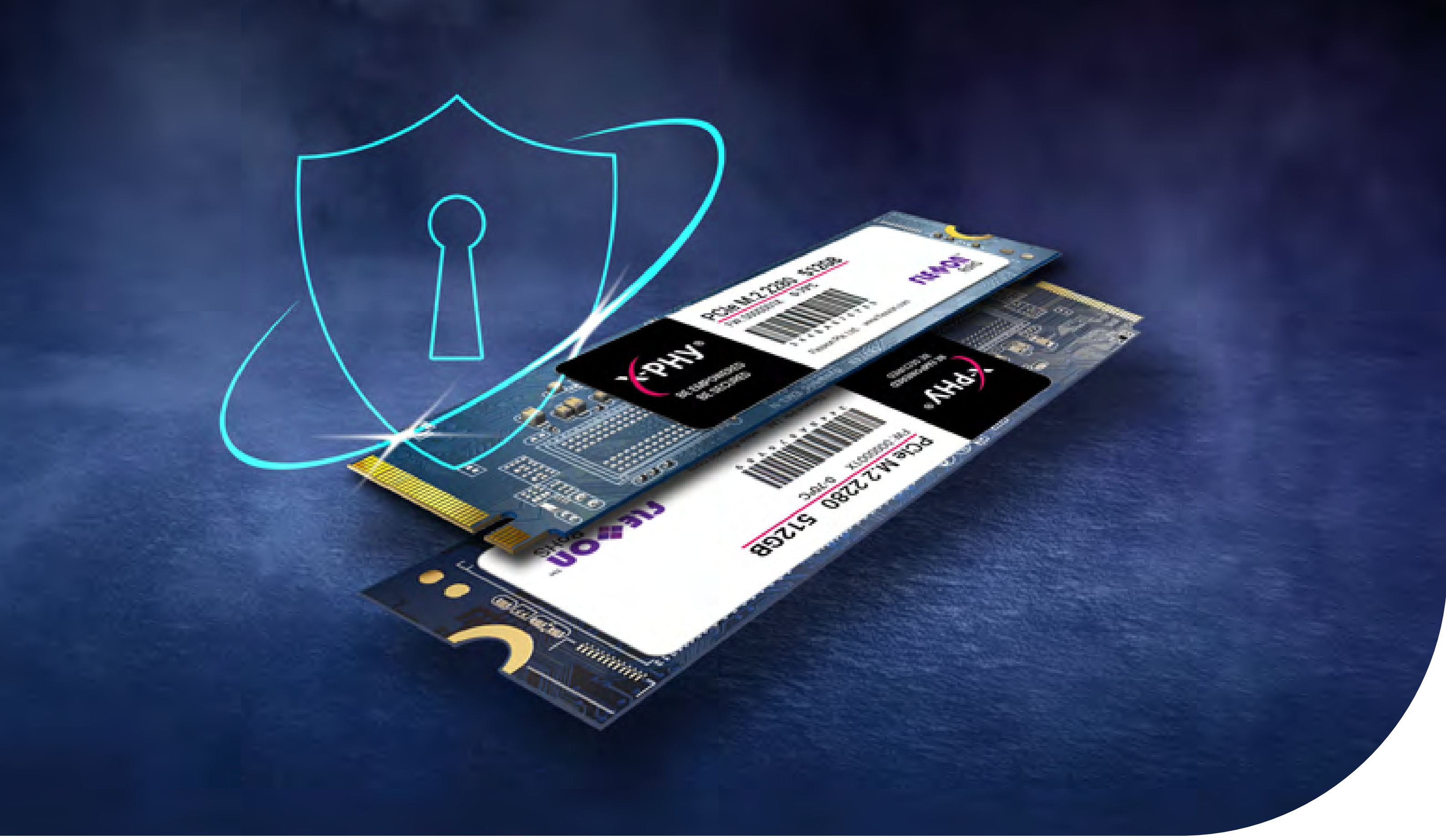
Top 10 Women in Cybersecurity Award

Govware X Ice71 Startup Pitch Pit Awards

Editor's Choice in Cybersecurity Artificial Intelligence

Cutting Edge in Data Security

Editor's Choice in Endpoint Security



CONTACT US

Singapore

28 Genting Lane,
#09-03/04/05
Platinum 28,
Singapore 349585

☎ +65-6493 5035

📠 +65-6493 5037

✉ info@x-phy.com

Hong Kong

Workshop 3 on 2/F,
Wah Lai Industrial Centre,
NOS 10-14, Kwei Tei Street,
Shatin, Hong Kong

☎ +852-2711 5886

📠 +852-3011 3058

✉ info@x-phy.com