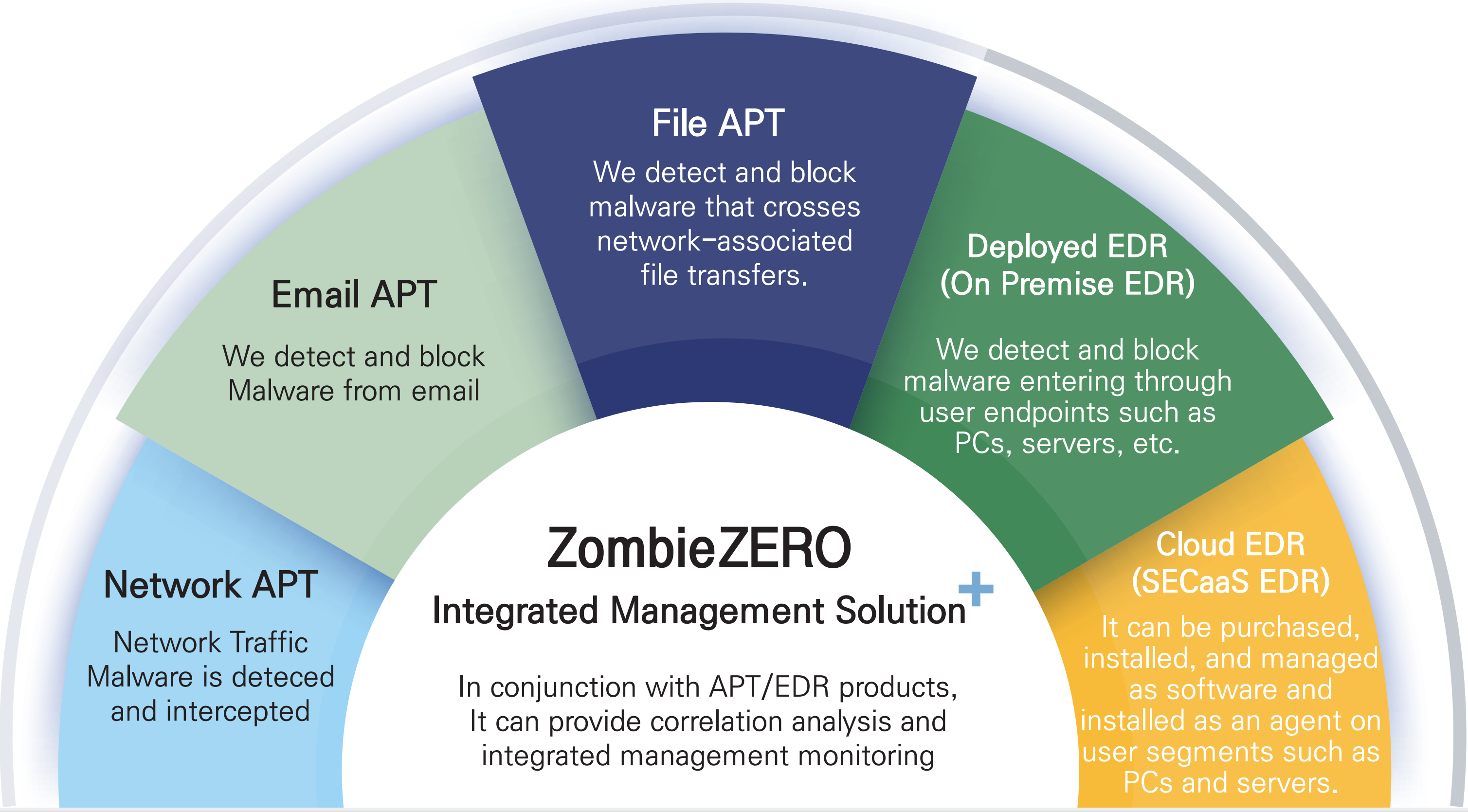
Zombie ZERO

AI-based solutions for new and variant malware and ransomware

We create a secure security environment from cyber threats.

NDCore
New Paradigm Core

AI–based action analysis security solution that detects and blocks new and variant malware such as ransomware and APT



File APT

We detect and block malware that crosses network–associated file transfers.

Email APT

We detect and block Malware from email

Deployed EDR (On Premise EDR)

We detect and block malware entering through user endpoints such as PCs, servers, etc.

Network APT

Network Traffic Malware is deteced and intercepted

ZombieZERO

Integrated Management Solution +

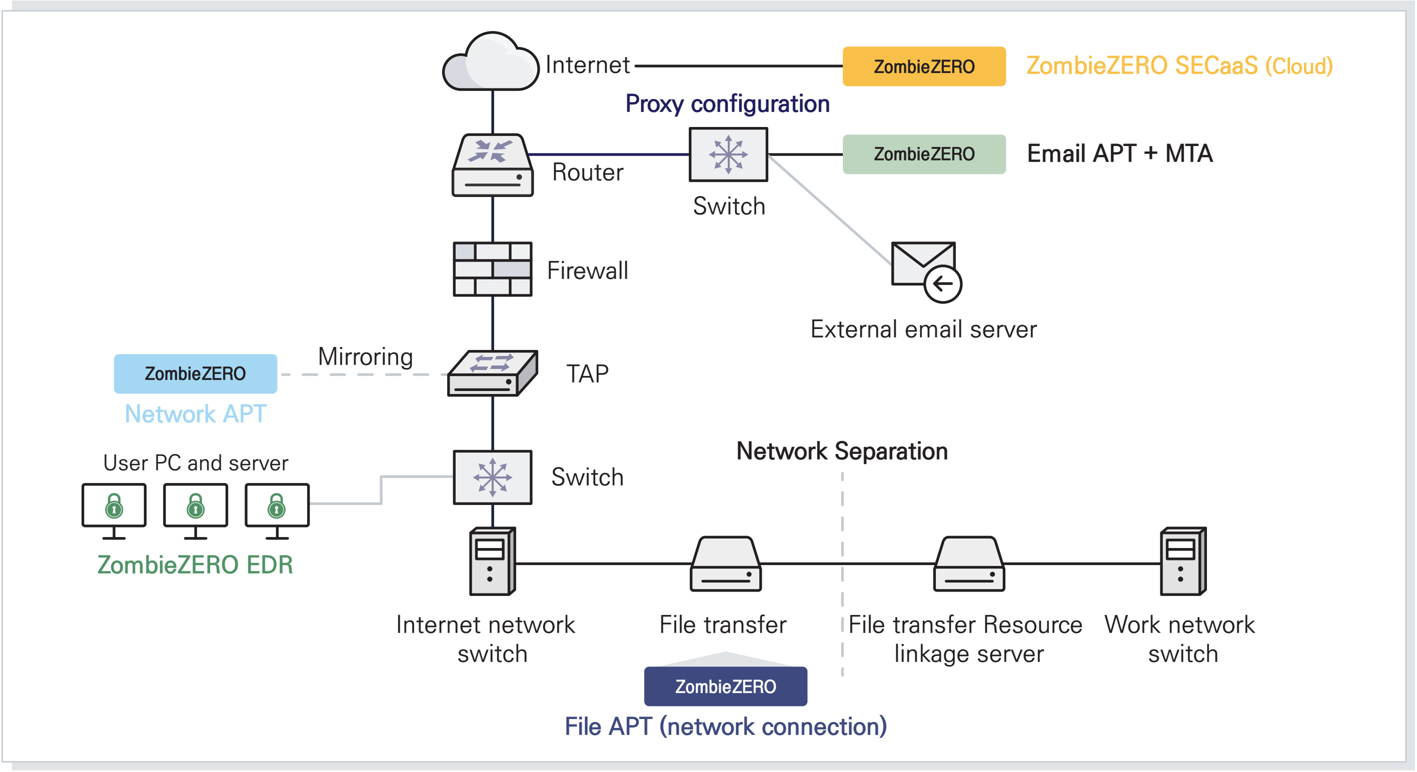
In conjunction with APT/EDR products, It can provide correlation analysis and integrated management monitoring

Cloud EDR (SECaaS EDR)

It can be purchased, installed, and managed as software and installed as an agent on user segments such as PCs and servers.

ZombieZERO System

· Solutions can be built on various pathways through which malware may enter the system



| ZombieZERO APT

Appliance–based integrated security solution (HW+SW)

Network, Mail, and Files (constructed in the network coordination section)

Network APT

Behavioral analytics complements traditional signature–based analysis **Compensate for zero–day** vulnerabilities that are not detected by the system

- Monitor two–way network traffic for file inflows and outflows
- Collect and analyze key Internet service protocols
- Detect and block access to harmful sites and C&C communications

Email APT

Addressing the limitations of traditional signature–based **spam solutions** that are vulnerable to malware

- Integrate APT with Message Transfer Agents (MTAs)
- Block only malicious information from mail containing spam, spearphishing, and malware
- Analyze email attachments and URLs and send only legitimate mail to the mail serve

File APT

Overcoming the limitations of traditional signature spam solutions that are vulnerable to new and variants

- Analyze and block files in transit in conjunction with network connectivity solutions
- Categorize analyzed files and send only those deemed normal to the business network
- Deliver analysis results using shared folders

Expectations

· When APT and EDR products are deployed concurrently

Response to malware and ransomware

Detection and Response to unknown new and variant malware AV cannot detect

Securing Endpoint Visibility

Visibility on specific situation caused by cyberattack at the endpoint

Preventing possible malware intrusions

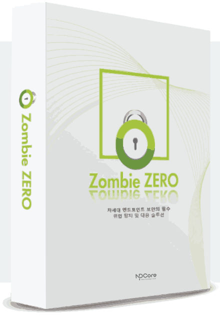
Identifying malware entry paths and connections between systems to improve security by patching holes from within

Cost saving

Built–in ransomware response, backup, and some antivirus features requiring no need to purchase a separate product

ZombieZERO EDR

On-premises / cloud deployment to detect and block malware that flows through user segments such as PCs and servers



Main features

Real-time detection and response for ransomware

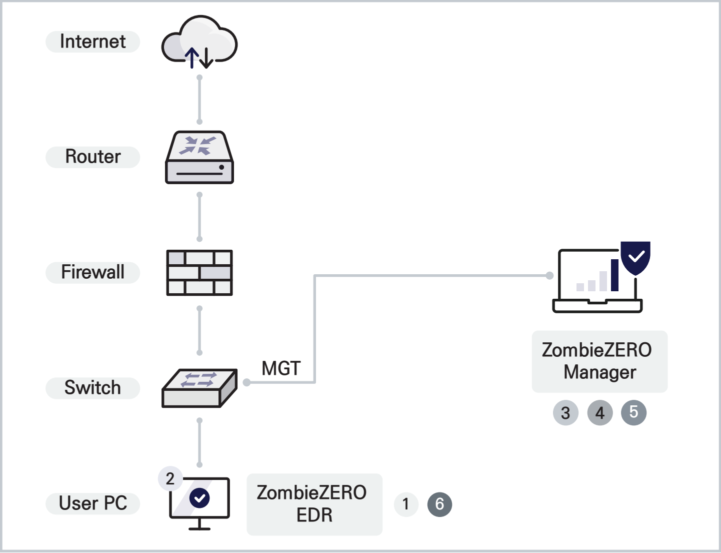
- Counteract file encryption and forgery/tampering by ransomware
- Global antivirus ‘Bitdefender’ adopted

Zero Trust (Execution pending)

- Upload information to the analytics server by suspending execution of files when new files are introduced or threat files are executed

IOC-based real-time threat detection

- Detect indicators of compromise(IOC) for user device behavior (network, file, process, registry, etc.)

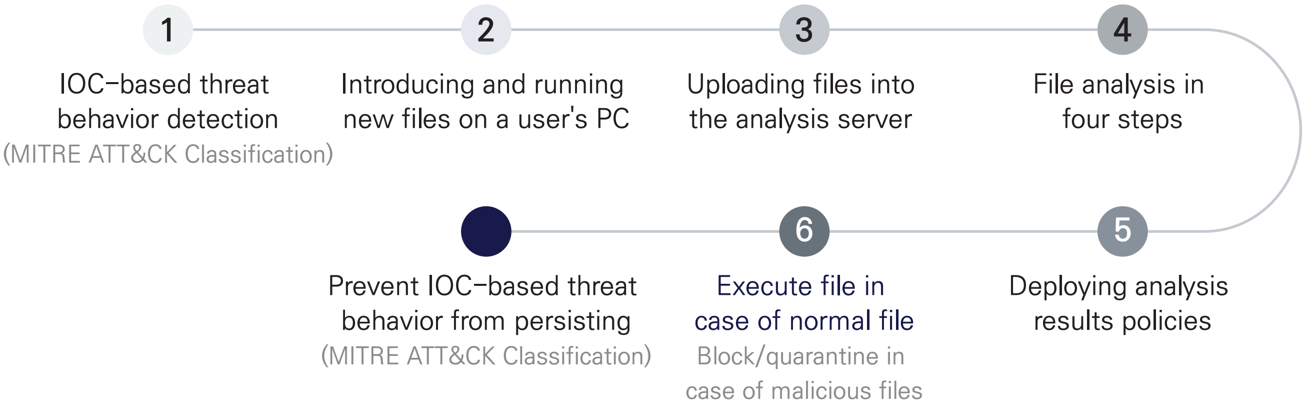


ZombieZERO SECaaS

ZombieZERO EDR Cloud Service

- Install as an agent through a dedicated webpage
- Full functionality including purchase, installation, and centralized management on the web
- High user management and convenience, no H/W introduction cost
- Suitable for SMEs and remote and telecommuting environments

EDR detection and analysis capabilities



1 IOC-based threat behavior detection (MITRE ATT&CK Classification)

2 Introducing and running new files on a user's PC

3 Uploading files into the analysis server

4 File analysis in four steps

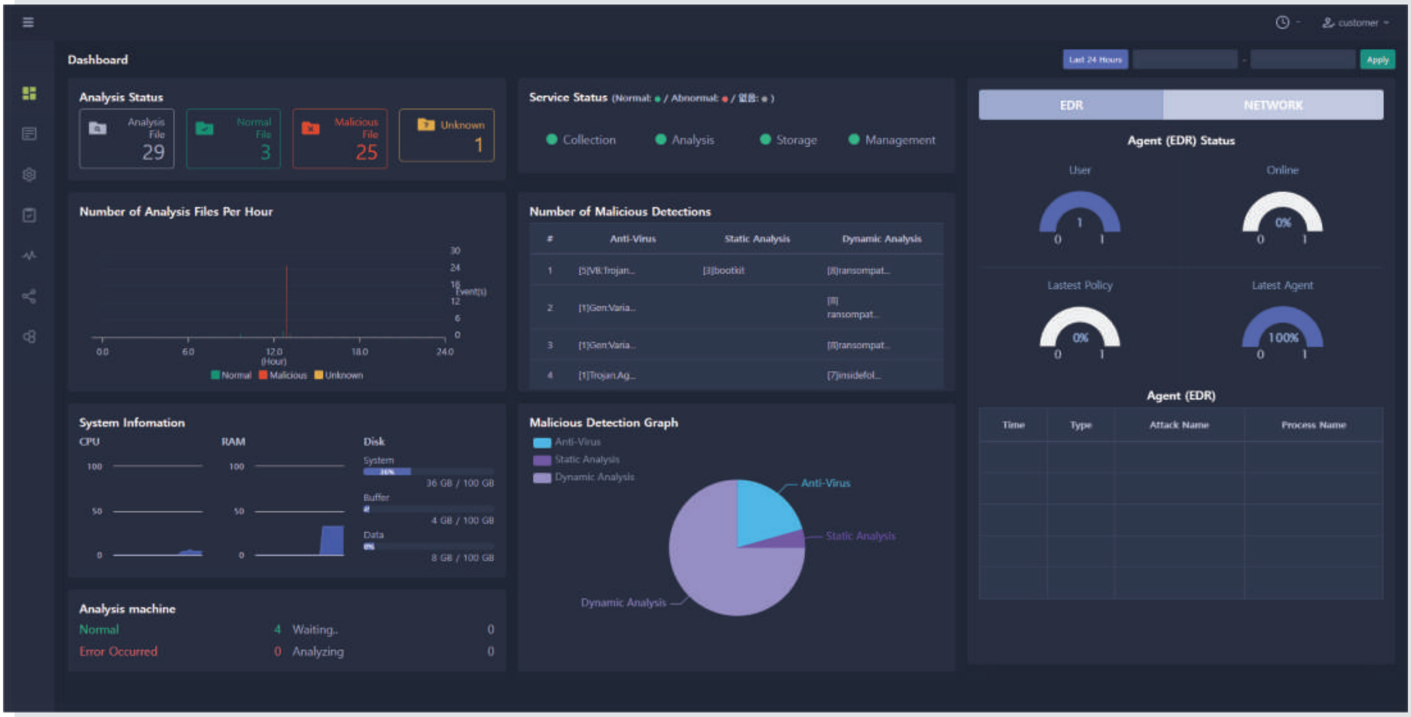
5 Deploying analysis results policies

6 Execute file in case of normal file
Block/quarantine in case of malicious files

● Prevent IOC-based threat behavior from persisting (MITRE ATT&CK Classification)

ZombieZERO UI

- Organize layouts with an intuitive design so admins can easily find the information they're looking for
- Apply visual design to help admins get quick and accurate situational awareness
- Enhance security with authentication and permission controls to ensure only authorized users have access



Analysis Status

Analysis File	Normal File	Malicious File	Unknown
29	3	25	1

Service Status (Normal: ● / Abnormal: ● / 없음: ●)

● Collection ● Analysis ● Storage ● Management

Number of Analysis Files Per Hour

Number of Malicious Detections

#	Anti-Virus	Static Analysis	Dynamic Analysis
1	[5]VB:Trojan...	[3]bootkit	[8]ransompat...
2	[1]Gen:Varia...		[8] ransompat...
3	[1]Gen:Varia...		[8]ransompat...
4	[1]Trojan.Ag...		[7]insidefol...

Agent (EDR) Status

Agent (EDR)

Time	Type	Attack Name	Process Name

System Infomation

Malicious Detection Graph

Analysis machine

Normal	4	Waiting..	0
Error Occurred	0	Analyzing	0

Major Common Features

Multidimensional analysis

AV·Multi-dimensional detection and analysis including static, dynamic, and reputation analysis

Prevent virtual machine bypass

Providing the same dynamic behavioral analytics as real machines

MITRE ATT&CK

Detecting Malware by MITRE ATT&CK Criteria

Malware flowchart

1011100
0101
1110110

Function to detail and monitor attack types based on indicators of compromise

ECSC formula

Integration with Ministry of Education Cyber Safety Center Yara Rule

AI-based malicious code detection

AI-based fast and accurate detection technology for malicious codes

Multidimensional Analysis

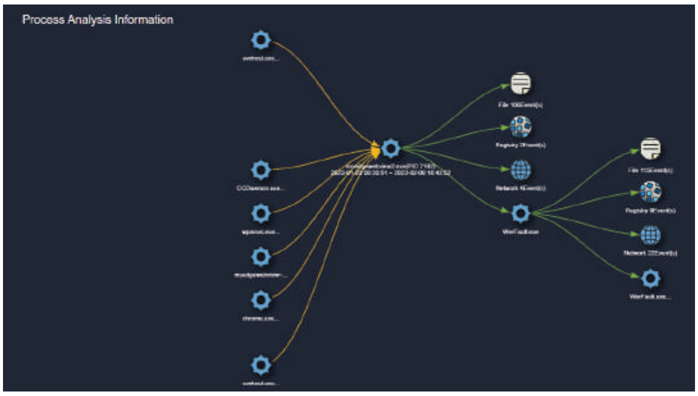
· Detect and block malware with multidimensional analysis of traffic flowing through your network from outside to inside.

HASH ▶ Bitdefender ▶ yara ▶ vmware ▶ VirusTotal

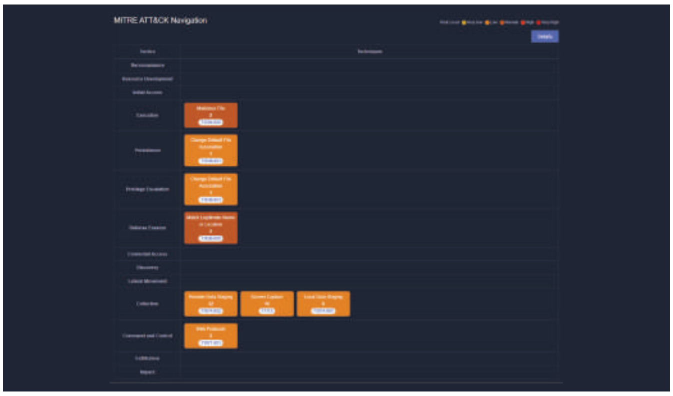
User Black ▶ AV Engine ▶ Yara Rules ▶ VMWare behavior analysis ▶ Reputation analysis

MITRE ATT&CK · Malicious behavior flowchart

· Monitoring the shape of techniques and methods for ongoing attacks, not the results of attacks



Process analysis information
(malicious behavior flowchart)



MITRE ATT&CK Navigation

Real-time backup

· Backup files to a secure folder inaccessible by normal processes at the last minute before file encryption

· Backup and execution at the kernel driver level, eliminating cross-application conflicts and performance degradation

File monitoring ▶ Opening files and changing programs ▶ Instant backup to the drive's folder ▶ Restoring a saved backup file (Original, undamaged files) ▶ Complete double protection

References

No. 1 for APT in Korea with more than 150 clients in Korea and abroad

국세청
경찰청
검찰 PROSECUTION SERVICE
대한민국 국방부 Ministry of National Defense
우정사업본부 KOREA POST
Your Best Credit Partner SGI서울보증

서민금융진흥원
The-K 한국교직원공제회
서울특별시
경상남도 GYEONGNAM
경상북도 GYEONGSANGBUK-DO
서울특별시교육청

경기도교육청
부산광역시교육청
인천광역시교육청
경상북도교육청
전라남도교육청
대구광역시교육청

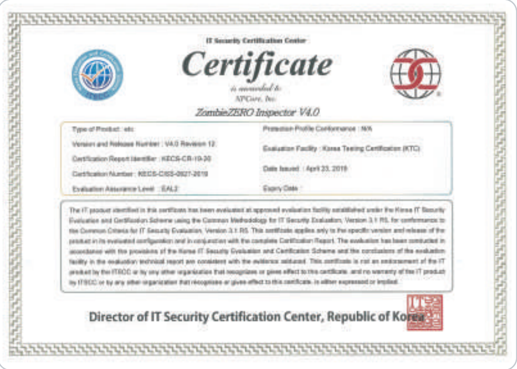
한국장학재단
KGU 경기대학교
동덕여자대학교
OSB저축은행
BNK 경남은행
금융위원회

유한양행
jtbc
LS엠트론
보훈공단 중앙보훈병원
서울특별시 서울의료원
제주대학교병원

indosat ooredoo
Kamisu City Hall, Japan
Royal Malaysia Police
VNPT Vietnam Posts and Telecom Group
Vietnam Cryptography University
Spry

Certificates and Patents

NPCore holds international CC, GS certificate, and Innovative Product certificates, registered 13 patents, including 2 in the U.S. and 1 in Japan.


IT Security Certification Center

Certificate

is awarded to
NPCore, Inc.
ZombieZERO Inspector V4.0

Type of Product : etc	Protection Profile Conformance : N/A
Version and Release Number : V4.0 Revision 12	Evaluation Facility : Korea Testing Certification (KTC)
Certification Report Identifier : KECS-CR-19-20	Date Issued : April 23, 2019
Certification Number : KECS-CISS-0927-2019	Expiry Date :
Evaluation Assurance Level : EAL2	

The IT product identified in this certificate has been evaluated at approved evaluation facility established under the Korea IT Security Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 R5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 R5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Korea IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the ITSCC or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by ITSCC or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Director of IT Security Certification Center, Republic of Korea

International CC Certificate

KTC

소프트웨어 품질인증서
Certificate of Software Quality

1등급

ZombieZERO Inspector V4.0

[illegible]

KTC 한국기계전기전자시험연구원장
President of Korea Testing Certification Institute, Republic of Korea

GS Certificate 1st Grade

The United States of America

The Director of the United States Patent and Trademark Office

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, or importing into the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Patent in US

Certificate No. 2022-401 Ministry of SMEs and Startups

CERTIFICATE OF
THE INNOVATIVE PRODUCT

COMPANY NPCore Inc.
[illegible]

The above product is certified as the Innovative Product in accordance with [illegible] THE GOVERNMENT PROCUREMENT ACT and [illegible] REGULATION ON DESIGNATION OF THE INNOVATIVE PRODUCT AND PROMOTION OF PURCHASE.

December 26, 2022

Ministry of SMEs and Startups

Ministry of SMEs and Startups

Innovative Product Certificate