RSAConference 2023

KOREA PAVILION

San Francisco, Moscone Center

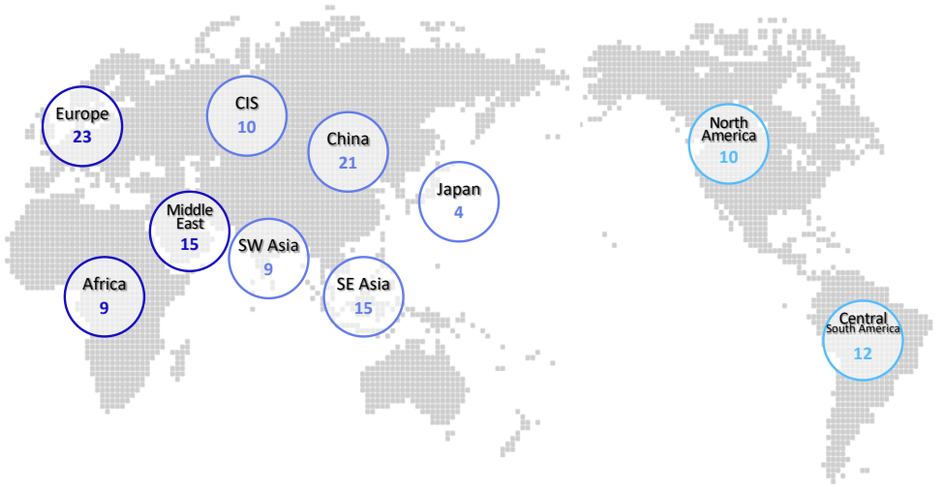
Apr. 24–27, 2023

Korea Trade-Investment Promotion Agency (KOTRA)

Agency established to contribute to the development of the national economy by performing work such as trade promotion, investment between domestic and foreign companies and support of industrial technology cooperation etc.

Main functions and roles

- Expanding medium and small-size enterprises' business in overseas markets
- Supporting small-sized enterprises (SME) to extend their business abroad
- Overseas market information production, spread and consulting
- Attract foreign investment
- SME Global Business Training and attracting foreign professionals
- Improving national brand, supporting international development cooperation, supporting munitions trade
- Performing projects accepted by the government



Located Worldwide

10 local head offices, **128** Korea Business Center (KBCs) in **84** countries

Korea Information Security Industry Association (KISIA)

KISIA is a representative and designated professional association of Republic of Korea for converged security industry covering both cyber and physical security. We represent Korean security companies both locally and internationally.

With over 270 member companies, KISIA is aimed at the growth of the infrastructure of the security industry in Korea. As a specialized and professional body in the private sector, we listen attentively to the voice of the industry and create the optimized ecosystem for the businesses.

Besides, we provide the Korean information security industry with support for global market entry. Organizing overseas business meetings and exhibitions, we encourage domestic companies to gain better chances not only to discover foreign business partners, also develop international trade with many other countries. Furthermore, we make consistent contributions to improvement of national policy by communicating closely with the government and producing the research reports on the information security field in Korea.

KISIA seeks to create a concerted approach among companies, governments and organizations across the world for the comprehensive development of the security communities.

Main Activities

- The settlement of a sound and vital cyber and physical security eco-system
- Survey and Research on market trends and statistics
- Support for the entry into overseas market and global export
- Support for start-up growth
- Support for security workforce training and education
- Interactive program for KISIA members

LOCATION

EXHIBITORS

Company	Main Products
AI Spera	Criminal IP, Criminal IP ASM (Attack Surface Management)
EYL, Inc.	Quantum Entropy Chip, Quantum Random Number Generator, Quantum Shieldz® CipherTM
NETAND	HIWARE Privileged Access Management, HIWARE Identity Management, HIWARE Multi Factor Authentication
PRIBIT TECHNOLOGY	PacketGo
Quad Miners	Network Blackbox
SecuLetter	SecuLetter Advanced Email Security ‘SLE' SecuLetter Advanced Email Security as a Service ‘SLES' SecuLetter Advanced File Security ‘SLF'
SSNC	FPMS (Firewall Policy Management System)
Stealth Solution	Stealth Moving Target Defense (SMTD) v.1.0
WEEDS KOREA	WEEDS BlackBox Suite
Xabyss	NetArgos

CONTENTS

AI Spera

AI Spera

CONTACT INFORMATION

Name	Uijin Jung
Title	Business Development Manager
Department	Overseas Business
Company Address	7, Yeonmujang 5ga-gil, Seongdong-gu, Seoul, Republic of Korea
Phone	+82-10-9503 -5179
E-mail	ejjeong@aispera.com
Website	www.criminalip.io

ABOUT COMPANY

AI Spera provides Cyber Threat Intelligence from a hacker's perspective, and our goal is to offer high-value information on all threat data that is collectible in cyberspace. We process data such as security threats, attackers or attack methods, malicious code, and vulnerabilities to counteract and prevent security breaches and cybercrimes that targets IT assets. Our corporate mission is to free the business from ever-evolving cyber threats and fraud. At the forefront, our innovative up-to-date data-driven security will protect your business from exposure to threats.

MAIN PRODUCTS

· Criminal IP

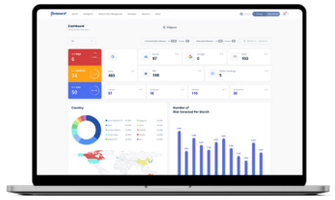
AI-driven search engine that utilizes machine learning and OSINT to detect all kinds of vulnerabilities related to personal or corporate cyber assets in real-time offering true visibility and control.

You can find all types of internet-facing information on malicious IPs, phishing sites, malicious links, certificates, industrial control systems, IoTs, servers, CCTVs, and so forth.

· Criminal IP ASM (Attack Surface Management)

In addition to real-time monitoring, Criminal IP ASM provides significant statistics regarding all possible attack points while showing country status, ASN, services, products, port statistics, and information on detected IT assets.

All you need is a single domain and Criminal IP ASM will find all the related assets, even those scattered and forgotten on the digital surface.



DIFFERENTIATION

· Real-time detection & monitoring

Malicious IPs are always changing, so counting on purchased databases leaves your company vulnerable. However, Criminal IP collects and analyzes all 4.2 billion IP addresses and tens of billions of domain addresses worldwide to provide trusted data.

· Powerful domain scanning

Domain scanners provide information by comparing and verifying against existing blacklists databases, While Criminal IP reaches to the backend of Chrome and reads data in real-time.

· Easy-to-use

A SaaS based product provided with API keys, with a user-friendly interface

REFERENCE CUSTOMERS and KEY PERFORMANCE

· Banking/Fintech Sector

KEB Hana Bank / NHN PAYCO / Hanwha Life Insurance / toss securities / Dunamu

· IT/Service Sector

Yanolja / LIG / NHN TECHORUS / Splunk / MEGAZONE SOFT / Kt ds / SJ E&M / CONNECTALYST. / NC / netmarble / Smilegate / METABORA / NSUS Group Inc. / HYBE / AhnLab / Recorded Future / PIOLINK / SSNC / COONTEC / Wedge IQ / KSIGN / NADDIC GAMES / PEARL ABYSS

· National Defense Sector

Ministry of National Defense / LIG System / LIG Nex1 / Agency for Defnse Development / MOASOFT / Korea Research Institute for defense Technology planning and advancement

· Education Sector

Soon Chung Hyang Univsersity / Sangmyung University / Korea University / Hoseo University / Institue for Basic Science

· Government & Public Sector

Financial Security Institute / Korea Copyright Commission / Ministry of Trade, Industry and Energy / Korea Technology and Information Promotion Agency for SMEs / Ministry of Science and ICT / KISA / NIPA / K data / KERI

EYL, Inc.

CONTACT INFORMATION

Name	Junghyun Francis Baik
Title	Chief Marketing Officer
Department	Marketing Dept
Company Address	(06776) 2F, 7-40, Mabang-ro 6-gil, Seocho-gu, Seoul, Republic of Korea
Phone	+82-10-3168-1418
E-mail	jhbaik@eylpartners.com
Website	www.eylpartners.com

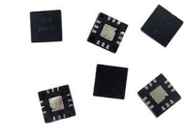
ABOUT COMPANY

Although modern cryptography's random number generation technology plays the most important role in generating and managing encryption keys in the security system, we mainly use a pseudo-random number generator, which makes hacking possible due to the improvement of the attacker's computing power. EYL's Quantum Random Number Generator (QRNG) miniaturization technology is a key technology that guarantees the safety of modern cryptographic system, and is a fundamental technology for quantum cryptography communication and quantum resistant cryptography for the future quantum computing era.
As a company that strengthens the level of convergence security in the IoT-based 4th industry and prepares for and welcomes the future quantum information technology first, EYL, Inc. is a Quantum Shieldz® a variety of quantum security technology based on the original technology that implements QRNG with microchips.

MAIN PRODUCTS

· Quantum Entropy Chip

- Enables us to harvest ultimate randomness from nature using radioactive isotope decay.
- because it can dramatically improve the security of all IoT devices, it can provide more secure cryptography powered by quantum entropy chip.



· Quantum Random Number Generator

- USB, modular, PCI-Express type quantum random number generators use quantum entropy chips to provide different speeds and user interfaces to meet customer needs.

· Quantum Shieldz® Cipher™

- A self-sufficient voice encryption device that works with your personal smartphone.
- Securely encrypts the user's voice using an encryption key generated by a quantum random number generator (QRNG) to completely block eavesdropping or unwanted recording through spyware.

DIFFERENTIATION

- It is very small (3 mm) and inexpensive, it can be deployed in all kinds of IoT devices.
- Post-processing provides ultimate randomness and is not required to meet NIST requirements.
- Compared to competing quantum random number generators, EYL's products are three times smaller and less expensive.
- Other companies have commercialized quantum random number generators using optical methods that provide quantum entropy at high speeds, but they are prohibitively expensive and bulky.

REFERENCE CUSTOMERS and KEY PERFORMANCE

· Customer

1. Government security agency (no-name country)
2. Several private enterprises

· Awards

3. “Diamond winner” of Mass Challenge 2016 Boston
4. Selected as a Disrupt 100 company MISP, IoT Security competition “Top Award”

CERTIFICATIONS

· Quantum Shieldz® Cipher™

1. KC (Korea Certification): R-R-EYL-QSC01 (05/18/2022)
2. FCC (Federal Communications Commission): 2A4M4-QSC01 (06/27/2022)
3. CE (Conformity to European): QSC01 (02/21/2023)

NETAND

CONTACT INFORMATION

Name	Junseong(Jason) Yang
Title	Business Development Manager
Department	Global Business Unit
Company Address	(07333) 10F, Hanam bldg., 25, Uisadang-daero 1-gil, Yeongdeungpo-gu, Seoul, Republic of Korea
Phone	+82-10-8643-8145
E-mail	jasonyang@netand.co.kr
Website	www.netand.io

ABOUT COMPANY

NETAND was founded to function as a bridge between networks and humans – for safer and efficient system management amid growingly complex IT infrastructure and increasing security concerns. Our flagship solution product HIWARE is the easiest and most stable way to secure identities and offers an integrated Identity Management (IM) and Privileged Access Management (PAM) solution which helps you balance security and efficiency at work by managing identities and access privileges. HIWARE supports system, database, and active directory. We are the market leader with the biggest market share in South Korea with more than 3,000 customers also some of our customers are big international companies.

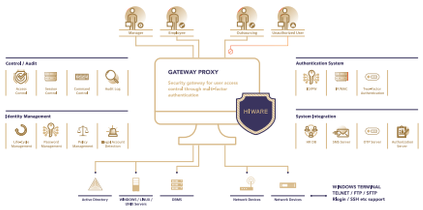
MAIN PRODUCTS

· HIWARE Privileged Access Management

- Privileged Session Management for System
- Privileged Access Management for Database

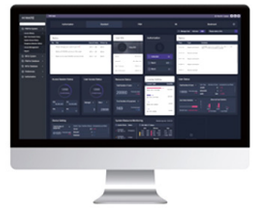
· HIWARE Identity Management

- Identity Management for System
- Identity Management for Database



- Active Directory

· HIWARE Multi Factor Authentication



DIFFERENTIATION

- Provide Competitive Price than global competitors
- Customized UI & solutions (build your own)

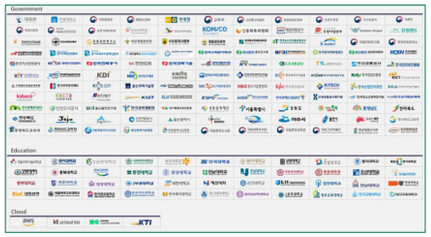
REFERENCE CUSTOMERS and KEY PERFORMANCE

· Key Performance

- HIWARE, our Identity Management and Privileged Access Management solution, will fulfill customer's privacy requirements and protect against privacy violations.
- HIWARE provides both PAM for System and PAM for DB. Our strongest feature of the solution is PAM for DB, which functions with most databases such as Oracle, MariaDB, Sybase, MongoDB etc. In addition, there is no limit to the number of users and devices that can stably access our solution. HIWARE is installed in large infrastructure environments with more than 500,000 different types of devices and more than 40,000 users.

· References

- NETAND export our product, HIWARE, to 15 countries with more than 3,000 customers and engaging actively marketing activities through overseas partnerships and have references of international company ; Samsung, Hyundai, LG, ING Bank and Shinhan Bank in Vietnam, Nicepay in Indonesia.



CERTIFICATIONS

Certifications	Certification Number	Issue Date
Accreditation Letter for Corporate Research Institute	2010110449	2017-03-23
Designation of the Center for Good Technology Research	201606	2016-10-25
Inno-Biz	R110103-00511	2020-04-11
Confirmation letter for a venture company	20220331030095	2022-03-16
Hi-seoul Brand company designation	2020-507	2020-01-01
2020 DATA-Global Company		2020-06-01
ISO/IEC 27001:2013	No.23-G-0175 Rev.0	2023-01-27

PRIBIT TECHNOLOGY

CONTACT INFORMATION

Name	SEONWOO PARK
Title	Assistant Manager
Department	Technical Support Team
Company Address	(1303) Daerung Post Tower 6, 298, Beotkkot-ro, Geumcheon-gu, Seoul, Republic of Korea
Phone	+82-10-2544-9014
E-mail	seonwoo@pribit.com
Website	www.pribit.com

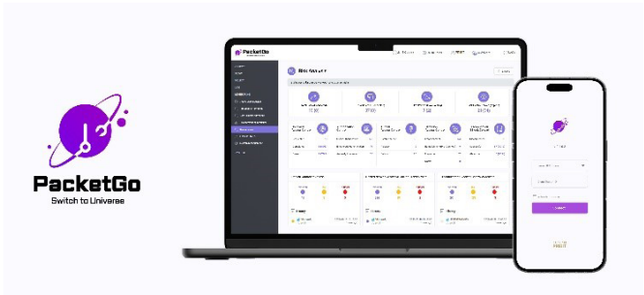
ABOUT COMPANY

Our philosophy is rooted in overcoming the legacy security issues of IP communications technology developed 40 years ago. PRIBIT technology Inc. has been developing Zero Trust based global communication standards.

MAIN PRODUCTS

- **PacketGo**

  Zero trust Internet, PacketGo, solves fundamental problems of internet communication technology even global players have not solved.



DIFFERENTIATION

- PacketGo is an innovative two-way mutual trust communication mechanism for uncontrollable network.
- Its innovative communication technology creates a separate trusted network on the untrusted internet.
- It simplifies the implementation of Zero Trust policies and configurations by providing micro-segmentation to form the foundation of a robust Work From Anywhere.
- It offers advanced 24/7 automated gateway solutions, featuring real-time updates for unparalleled ICT network security tailored to your enterprise requirements.
- PacketGo Passport provides seamless One ID, One Pass authentication, delivering exceptional, robust ICT network security for your enterprise network infrastructure.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- POSCO International has identified 131 applications and 1,383 services and enabled role-based micro segmentation to employees of over 80 domestic and global subsidiaries.
  the introduction of the PacketGo product has resulted in:
  Blocking 71% of risk factors, gaining access within 2 seconds, enhancing performance by 80%, and achieving up to 95% cost reduction.
- Numerous public organizations have been applied(such as Korea Enterprise Data Co., Ltd., Seoul Metro, Korea Technology Finance Corporation, Korea Labor Institute, Korea Youth Work Agency, etc.)

CERTIFICATIONS

- Holder of 120 Korea and international patents.
- Excellent Innovative Product of the Ministry of Science and ICT in Korea
- Excellent Information Security Company of Korea Internet & Security Agency(KISA)
- Good Software(GS) Certification from Telecommunications Technology Association(TTA) in Korea
- Common Criteria(CC) from IT Security Certification Center in Korea

Quad Miners

Quad Miners

CONTACT INFORMATION

Name	Dilara OZDEMIR
Title	Business Development Manager
Department	Global Team
Company Address	DREAUM Sunghong Tower 6F, #138 Teheran-ro, Gangnam-gu, Seoul, Republic of Korea
Phone	+82-10-9635-1855
E-mail	dilara@quadminers.com
Website	www.quadminers.com

ABOUT COMPANY

Quad Miners will solve security threats such as internal leakage and systematically respond to the network security market. Quad Miners will be known as the next generation security solution that will analyze abnormal behaviors in the network and give real time traffic analysis auditing reports to the network environment.
We believe that we can grow through practical wisdom. Based on our belief, we create a technical oriented ecosystem. Cyber Security market is growing because of the ESM and SIEM market has reached its peak. ESM and SIEM can collect logs and do a part of the analysis but not the way Network Security can store and analyze. Quad Miners has developed a solution where it meets the needs and criteria to store and analyze all network packets in real time.

MAIN PRODUCTS

“Only those who know the truth can respond.”
Network Blackbox a next-generation solution for detecting and responding to threats.
Quad Miners provides a solution called the Network Blackbox. This is a next-generation network detection and response solution that records, stores, and analyses all data flows using the Network Blackbox, from the initial point in time when an event begins, to the time that it is completed and even beyond. The Network Blackbox as it applies to network security is similar to the black box concept used in aircraft.
The most notable feature of the Network Blackbox is that it saves and analyses 100% of packets to detect and respond to all types of cyber security threats. The Network Blackbox consists of 1) threat detection using over 50,000 rules, 2) scenario-based user behavior analysis, 3) extraction and analysis of a variety of content (email, search, translation, etc.), 4) Supervised-learning anomaly detection analysis, 5) internal breach detection through “cyber kill chain” monitoring, 6) detection of malware and determination of whether such code has infected the network internally and 7) forensic analysis, collecting and saving all traffic, while also performing full packet-based information analysis.

DIFFERENTIATION

Quad Miners' NDR product, Network Blackbox,

- Collect and analyze all network traffic (S-N/E-W).
- Detects all threats (Known/Unknown, Internal/External) and visualizes them based on MITER ATT&CK Matrix and TTPs.
- Supports various threat detection methods such as threat detection rules, non-rule, and supervised/unsupervised machine learning-based detection.
- Based on Full Packets, it provides sufficient content (why and how it was detected as a threat) for IT personnel to understand.
- Provides detailed evidence for Network Forensics, such as recovering user web screens, extracting attachments to mail, extracting uploaded/downloaded files, and isolating and downloading PCAPs.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- Network Blackbox has been listed in Gartner’s NDR report for three consecutive years.
- 56+ customers from national defense, tier 1 banks, national infrastructures, global enterprise
- Global Branches in Japan and USA

CERTIFICATIONS

- **International patent application (PCT, United States of America, Japan)**
  - A network forensic system and its method using the system (PCT-KR2019-008860)
- **Patent applications in South Korea**
  - A high-performance packet stream storage system and its method using the system (10–2080477)
  - A pattern-based index processing system and its method using the system (10–2080478)
  - A scenario-centered real-time attack detection system and its method using the system (10–2080479)
  - Included in Forbes 100 APAC 2022 and Gartner Market Guide 2022

SecuLetter

SECULETTER

CONTACT INFORMATION

Name	Julie Sohn
Title	Manager
Department	Global Business Team
Company Address	14F, PangyoInnovationLab, 422-1, Gumto-dong, Sujeong-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
Phone	+82-31-608-8860
E-mail	global@seculetter.com
Website	global.seculetter.com

ABOUT COMPANY

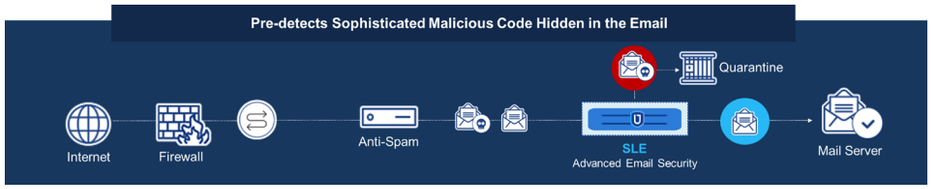
SecuLetter provides proactive protection solution for Email & File security based on own patent technology, 'Automatized Reverse-engineering'. Using our own patent core technology, SecuLetter provides Email & File security solutions. We are different from Anti-Spam, Anti-Virus, or Traditional APT solution that uses sandbox. SecuLetter digs up the deep inside of files to find out malicious code that attackers try to hide. With SecuLetter, you can experience fast & accurate security solution which brings you worry-free work environment.

MAIN PRODUCTS

· SecuLetter Advanced Email Security 'SLE'

"Cover the blind spots of traditional email security and APT protection solutions by fast and accurate diagnosis result." [On-premise / Cloud Service]

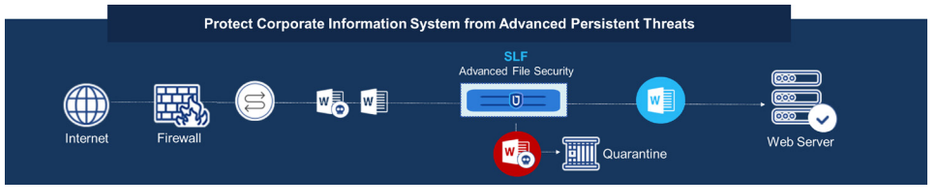
- Pre-detects sophisticated malicious code attack hidden in email & attachments.
- Powerful performance on file-based malware invade via email.
- Block phishing URL included in the email body and attached file.
- Provide dashboard and management console for IT admin.



· SecuLetter Advanced File Security 'SLF'

"Reduced 80% of diagnosis time vs traditional APT protection solution."

- Monitor the file transaction and analyze all files coming after firewall before reaching to the internal file system.
- Integrate with file system via SMB, NFS, SSH (SFTP) protocols.
- Provide CDR(Content Disarm Reconstruction) function effectively eliminates malicious URL & active contents (Macro, JS, etc.) which include execute code in the document file.
- Integrate with WAS (Web Application Server) and Shared Folder.



DIFFERENTIATION

· Fast and Accurate Diagnosis

5 times faster than existing sandbox-based solution and provide accurate diagnosis by analyzing assembly level.

· Powerful Protection against File-based malicious code attack

Effectively detect & block malicious code attack hidden in document files (doc, xls, ppt, pdf, zip etc.)

· Neutralize Evasive Malware

Detect evasive threats which recognize the sandbox environment and does not take any action.

CERTIFICATIONS

· Listed in Gartner Vendor Identification Research for Email Security

· Patent

- "Non-PE File Malicious Inspection Method by Memory Analysis and Device"
- "Malicious File Analysis Device and the Method by Using Virtual Environment."

· ISO 9001 / ISO 14001 / ISO 27001

SSNC

CONTACT INFORMATION

Name	Bona Kim
Title	Manager
Department	Business Planning Team
Company Address	43, Iljik-ro, Gwangmyeong-si, Gyeonggi-do, Republic of Korea
Phone	+82-10-8944-9157
E-mail	bona.kim@ssnc.co.kr
Website	www.ssnc.co.kr

ABOUT COMPANY

SSNC, founded in March 2018, has established itself as a trusted security partner by securing global companies and large financial institutions as clients. It provides endpoint, network, and cloud security solutions, offering solutions and services to protect a company's most valuable assets, Its data and people. With over 70% of their organization composed of engineers and developers, SSNC offers more specialized, technology-focused services.

MAIN PRODUCTS

· FPMS (Firewall Policy Management System)

- The FPMS solution automates all of the processes in firewall management that are being handled manually by administers to eliminate human error & failures and reduce service lead time for users

1. Auto-validate a Rules Upfront

Remove unneeded/redundant rules upfront by validating requests, Allow/deny rules as per pre-defined security criteria to make policies more secure

2. Optimize & Auto-Add-Rules

Optimize rules with optimizer algorithm, Auto-add rules on multi-vendor firewalls through APIs, Make rule application more convenient

3. Post & Consistency Analysis

Rule security analysis & guide

DIFFERENTIATION

- Auto-add rules on multi-vendor firewalls through APIs
- Provide integrated migration when replacing a firewall
- Pre-validate policies before they are applied to eliminate human error, such as misplaced policies
- Integrate with (Internal or 3rd Party) Request & Approval System to efficiently operate request, analysis, and application in one flow
- Differentiated Service Meets Market Needs

REFERENCE CUSTOMERS and KEY PERFORMANCE

1. Samsung Group

- Schedule when to add rules (after hours, real-time) in various work environments
- Adding ID-based rules provides user/admin convenience
- The migration feature enables perfectly seamless, speed firewall vendor replacement

2. Financial Institutions

- NH NongHyup: One of Korea's leading financial institutions, is using FPMS to efficiently manage over 600 firewalls.
- By reducing their firewall management staff from 12 to 3, they were able to allocate the remaining staff to other tasks, such as responding to cyber threats.
- Additionally, they were able to save 88% of their firewall policy verification time and reduce their workload by 57%, maximizing the efficiency of their firewall operations.

CERTIFICATIONS

- GS Certification : Good Software
- Excellence award by the 6th Korea SW Product Quality Awards, 2019

Stealth Solution

CONTACT INFORMATION

Name	Eric Li
Title	CTO
Department	Technical Engineering & Lab
Company Address	7F, 17, Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Republic of Korea
Phone	+82-10-3034-1633
E-mail	info@stealths.co.kr
Website	www.stealthsolution.co.kr

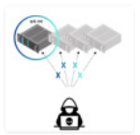
ABOUT COMPANY

Stealth Solution is a paradigm-shifting cyber security platform company which consistently invests on security infrastructure, constructs cyber threat response environment, and eliminates cyber threats. Especially it has been developing Network based Moving Target Defense technology which can end the game against hackers.

MAIN PRODUCTS

· Stealth Moving Target Defense (SMTD) v.1.0

SMTD mutates IP address and PORT number of network host continuously and randomly so that it makes impossible for attackers to identify the network host from the first attack stage.

Moving	Target	Defense
Random & Continuous Mutation of host's Network IP & PORT	Blocking hacker's attack by Mutation	Failure of host-targeting by Automatic Defense
		

DIFFERENTIATION

1. Zero-Trust

SMTD, based on Zero-trust which forces the authentication before the connection instead of the widely used current system, which is the other way around, mutates the address of the server so that only allowed clients are able to connect the server. Therefore, the advanced cyber security architecture is produced.

2. Dividing the Attack Surface, Making it Harder to attack

The host mutates its address continuously and randomly whose complexity perfectly disturbs the attacker since the attack surface they must consider has become too narrow. Moreover, even if the first attack has been succeeded, since the address mutates continuously into others, the attack cannot be continued. Also, SMTD makes it complex to attack from the first stage, blocking the intent to attack and building an active defense system automatically.

3. Insider threat

SMTD platform only reveals mutated IP and port to outside. Since it does not reveal hidden address which is needed for actual connection, the unauthorized user, attacker, and unidentified insider cannot connect the server directly, authorized user having to connect through SMTD. If there is abnormal access, SMTD also can effectively react not only the outsiders' connection but also the abnormal insiders.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- Korea Air Forces
- Korea Army

CERTIFICATIONS

- GS Testing-Certification (acquired)
- NET (New Excellent Technology) Certification (acquired)

WEEDS KOREA

CONTACT INFORMATION

Name	Ji Hyeon (Michelle) Yoon
Title	Overseas Project Manager
Department	Global Business Division
Company Address	321, Gonghang-daero, Gangseo-gu, Seoul, Republic of Korea
Phone	+82-10-3442-7677
E-mail	jihyeon.yoon@weeds.co.kr
Website	www.weeds.co.kr

ABOUT COMPANY

WEEDS Korea has not only been the most trusted UEBA solution pioneer in Korea for the past two decades but also grown as the No.1 sought-after solution supplier in its market, now aiming to contribute to the globe by providing AI-and-Big-Data-based audit & monitoring systems. WEEDS Korea disruptively secure sensitive personal data collected by governments, hospitals, colleges or leading companies against any unanticipated insider threats.

MAIN PRODUCTS

- **WEEDS BlackBox Suite**

  WEEDS BlackBox Suite (WBS) enables you to automate compliance reporting and achieve compliance with your national regulations by saving and managing data access logs in the application server.
  The WBS excels at gathering security information logs streamlining insider threat detections and incident response by identifying abnormal behaviors of a malicious insider through AI analysis.

DIFFERENTIATION

- The pioneer in developing Personal Information Access Log System in Korea
- Trace processing and technology management differentiation
  - Provide perfect visibility for managing personal information
  - Accurately identify Personal Identifiable Information
  - Able to systemize and automate Operating System
- Offer technologies relevant to different Personal Information Processing System
- 20 years of experience in various projects
- Continuously enhancing Customer Support Service System

REFERENCE CUSTOMERS and KEY PERFORMANCE

- Central Government Agency(Republic of Korea) : Supreme Prosecutors' Office, National Police Agency, Ministry of Foreign Affairs, Ministry of Patriots and Veterans Affairs , etc
- Public Institution(Republic of Korea) : Korea Trade-Investment Promotion Agency, Korea Asset Management Corporation, Korea Gas Safety Corporation, Korea Airports Corporation, etc
- Private Enterprise(Republic of Korea) : Samsung Card Co., Ltd, Sony Korea Corporation, Lotte Card CO., LTD, Lotte Shopping e-commerce, Lotte rental, BC Card Co., Ltd, Bank of Korea, etc

  WEEDS BlackBox Suite is the World's First Personal Information Access Log and Management Solution, has been applied and operated safely to more than 19,000 Information Processing System of 700 customers.

CERTIFICATIONS

- CC (Common Criteria) Certification
- GS (Good Software) Certification
- ISO9001

Xabyss

CONTACT INFORMATION

Name	Steven Hong / Kyungho,Park
Title	The head of U.S. branch / CTO
Department	Marketing / Development
Company Address	305 3F, 237, Yeongtong-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea
Phone	+82-70-7510-8200
E-mail	steven.hong@xabyss.com / pgh5247@xabyss.com
Website	www.xabyss.com

ABOUT COMPANY

Founded in 2014, Xabyss Inc. has developed and provided NetArgos**, a value-added Software-defined Network Device [SDND*] to our customers. NetArgos provides an enhanced network security environment to apply security checkup solution to detect and respond to zero-day attacks.

*SDND is a Proprietary software technology based on general-purpose hardware.
**NetArgos: Xabyss registered product name

MAIN PRODUCTS

· NetArgos

- Goal: to detect and minimize damage from cyber attacks
- Features: Zero-day intrusion Detection and Response (ZDR) solution.

1. Captures and stores the network traffic very efficiently and effectively.

- current packets - real time saving only packets including payload needed for the security-check
- historical packets - past packets for at least 3 months with 32TB HDD.

2. Run security checks periodically.

- whenever new Threat Intelligence [TI] is published or user rules are added.

3. Make Smart Report

- analyze the security check results and extract potential threat candidates.
- recommend security policy for real-time security system applications.

4. Optimize the security policy

- the analyzed results are reflected in policies of the network security solutions like IPS, Firewall with REST-API.

5. Extract additional information

- traffic logs, raw packets and files (office, img, html, etc…) to help analyze cyber-threats in detail.

DIFFERENTIATION

· First-N Technology: patented

- saving only packets needed for the security-check in real time.
- Reduce storage and security-check overhead dramatically[1/50] than full packet capture system.

· Security Check: patented

- Vulnerability Security Check
  - re-inspect all packets stored yesterday with entire rules (about 65,000) every day.
- Zero-day Security Check
  - re-inspect packets that have been stored for at least 1 month whenever new TI is distributed.

REFERENCE CUSTOMERS and KEY PERFORMANCE

· References

- National Defense: http://www.mnd.go.kr
- Finance
  - Shinhan Bank (https://www.shinhan.com/index.jsp)
  - BNK system: https://www.bnksys.co.kr/web/main.do
- Research lab
  - KT: https://www.kt.com
  - ETRI: https://www.etri.re.kr
- Local government: Daegu Metropolitan City (https://www.daegu.go.kr/index.do)
- Educational Institution: Korea National University of Transportation (http://www.ut.ac.kr)

· Key Performance

- Store the network packets for at least the previous 3 months with First-N technology.
- Reinspect the stored packets during at least 30 days within about 5 hours.
- Add custom inspection TI and reinspect the stored packets with various user options.

CERTIFICATIONS

- GS(Good Software) Certification
- PCT Patent : “Method for network inspection saving packet and system performing the same”

Stronger Together

kotra
Korea Trade-Investment Promotion Agency

kisia
Korea Information Security Industry Association