The New Benchmark for Email Security

Receive GUARD

New paradigm of
e-mail security

Intelligent Learning

Prevent APT
Attacks

Block New
Ransomware

Detect Fraud Mail

Analyze Hacker
Information

Establish Customized
Security System

VNETWORK
safe and saved

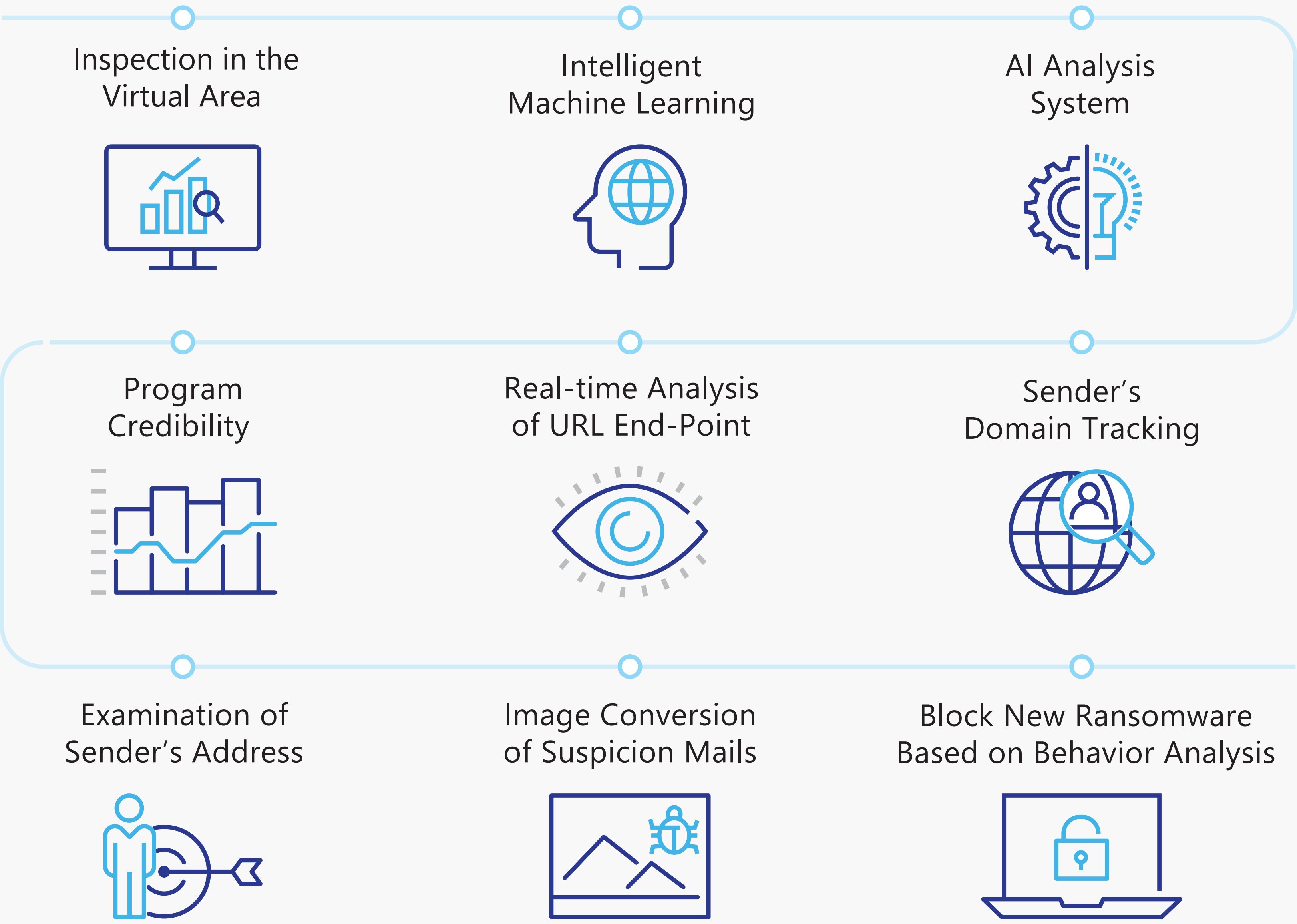
Certified global email security solution - Receive GUARD

Receive GUARD is the must-have innovative e-mail security product that makes up the loopholes of other conventional products by using AI and Machine Learning

Gartner RAPID7 ITSCC Korea Evaluation and Certification Scheme

Main Functions

Only one specialized BEC Mail Filtering System



Inspection in the Virtual Area

Intelligent Machine Learning

AI Analysis System

Program Credibility

Real-time Analysis of URL End-Point

Sender's Domain Tracking

Examination of Sender's Address

Image Conversion of Suspicion Mails

Block New Ransomware Based on Behavior Analysis

BEC: Business Email Compromise*
VA: Virtual Area*

AI Technology & Marchine Learning

Machine Learning of mail security per every user

AI & Machine Learning

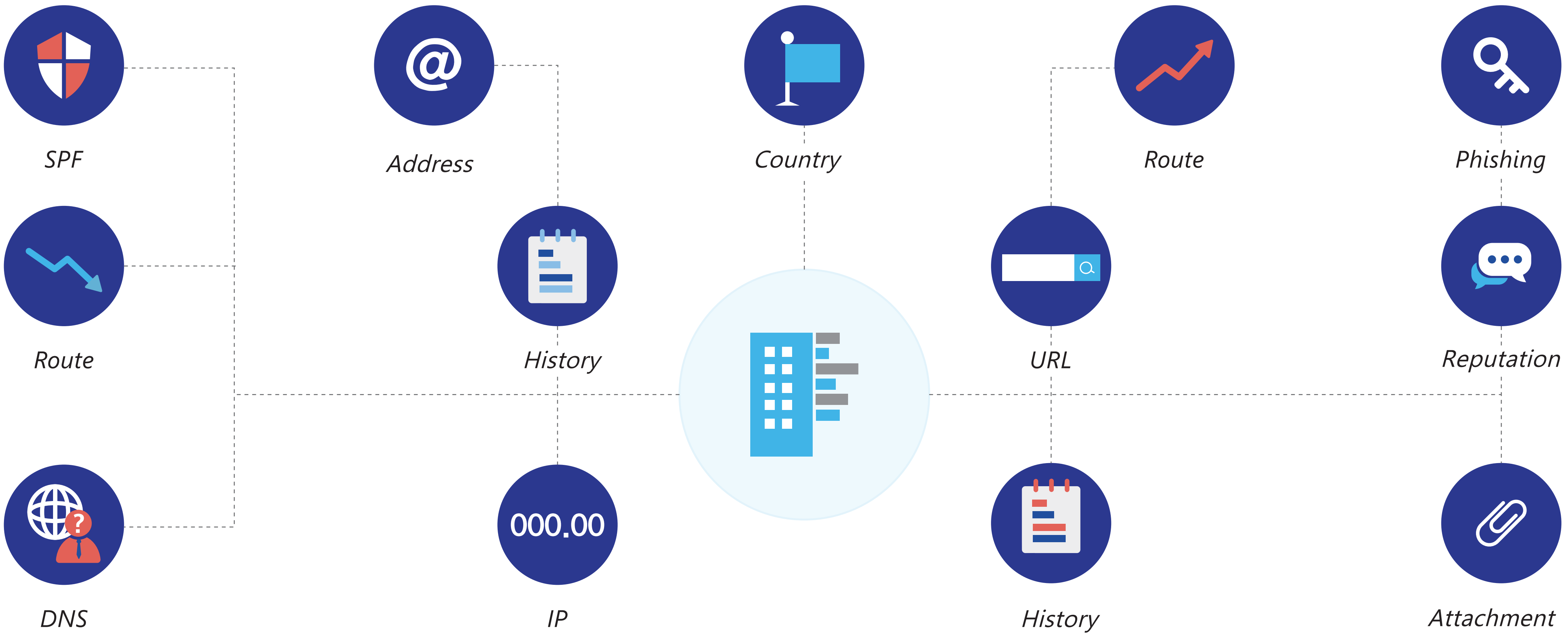
Detection of virus based on behavior analysis

Detection of fraud mails

Build customized database for each company

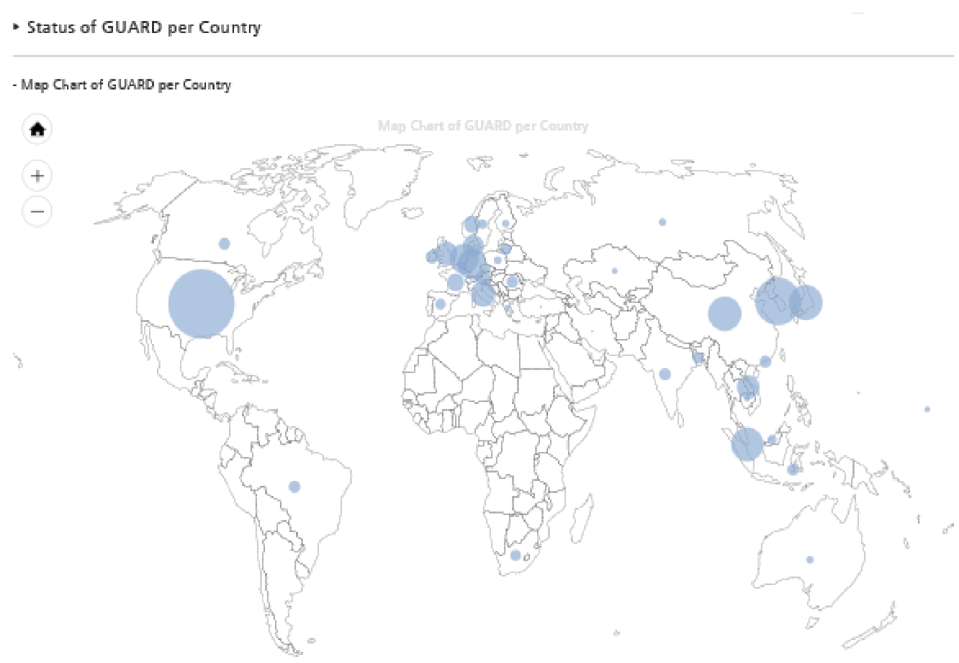
Establish Customized BIG DATA

Build every customer's BIG DATA system



Provide Statistics Report

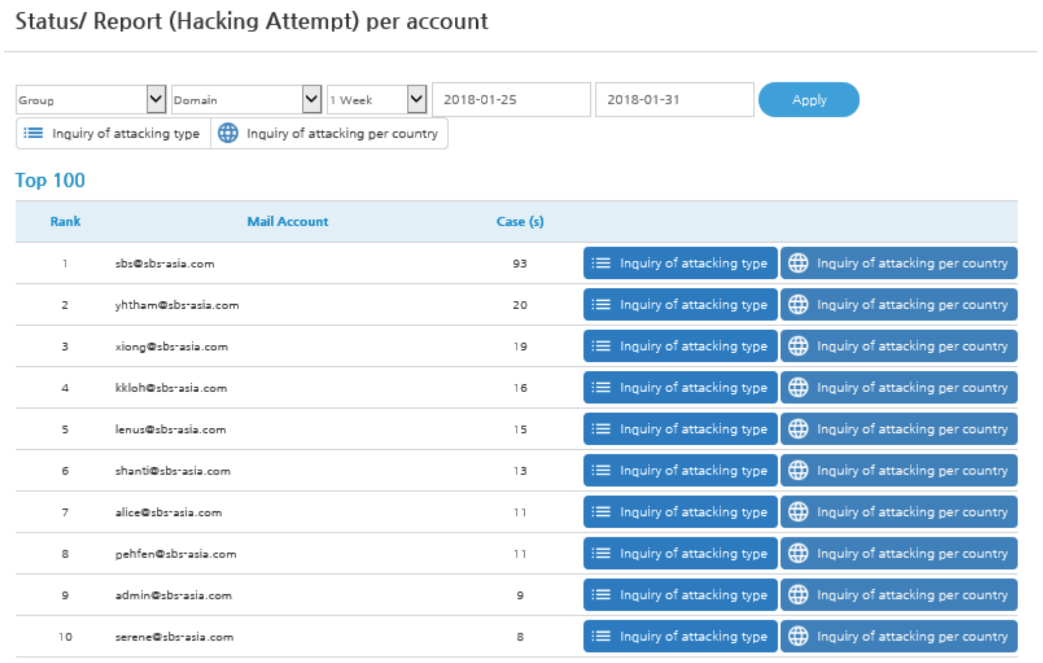
Analyze danger factor in real time



‣ Status of GUARD per Country

- Map Chart of GUARD per Country

Status report of attacks per country



Status/ Report (Hacking Attempt) per account

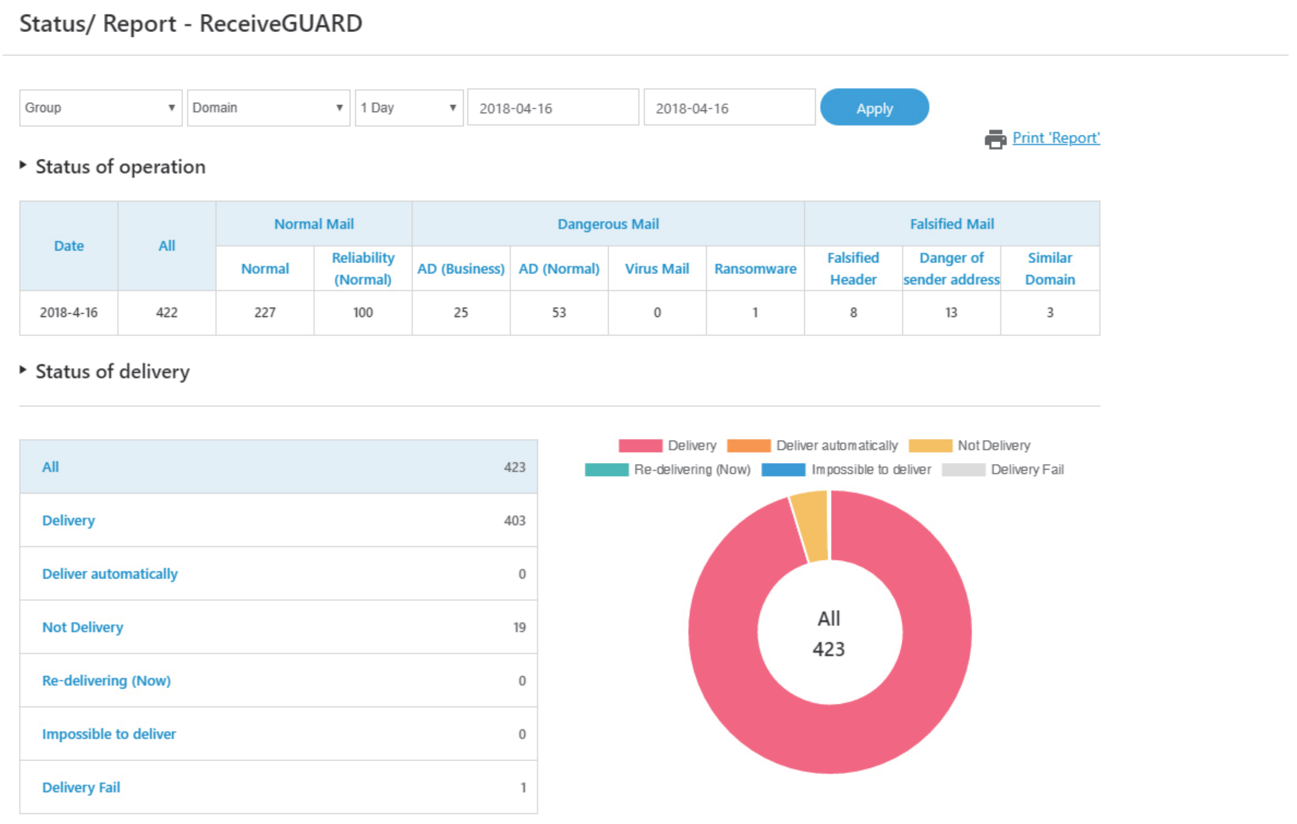
Group | Domain | 1 Week | 2018-01-25 | 2018-01-31 | Apply

Inquiry of attacking type | Inquiry of attacking per country

Top 100

Rank	Mail Account	Case (s)		
1	sbs@sbs-asia.com	93	Inquiry of attacking type	Inquiry of attacking per country
2	yhtham@sbs-asia.com	20	Inquiry of attacking type	Inquiry of attacking per country
3	xiong@sbs-asia.com	19	Inquiry of attacking type	Inquiry of attacking per country
4	kkloh@sbs-asia.com	16	Inquiry of attacking type	Inquiry of attacking per country
5	lenus@sbs-asia.com	15	Inquiry of attacking type	Inquiry of attacking per country
6	shanti@sbs-asia.com	13	Inquiry of attacking type	Inquiry of attacking per country
7	alice@sbs-asia.com	11	Inquiry of attacking type	Inquiry of attacking per country
8	pehfen@sbs-asia.com	11	Inquiry of attacking type	Inquiry of attacking per country
9	admin@sbs-asia.com	9	Inquiry of attacking type	Inquiry of attacking per country
10	serene@sbs-asia.com	8	Inquiry of attacking type	Inquiry of attacking per country

Status report(hacking attempts) per each account



Status/ Report - ReceiveGUARD

Group | Domain | 1 Day | 2018-04-16 | 2018-04-16 | Apply

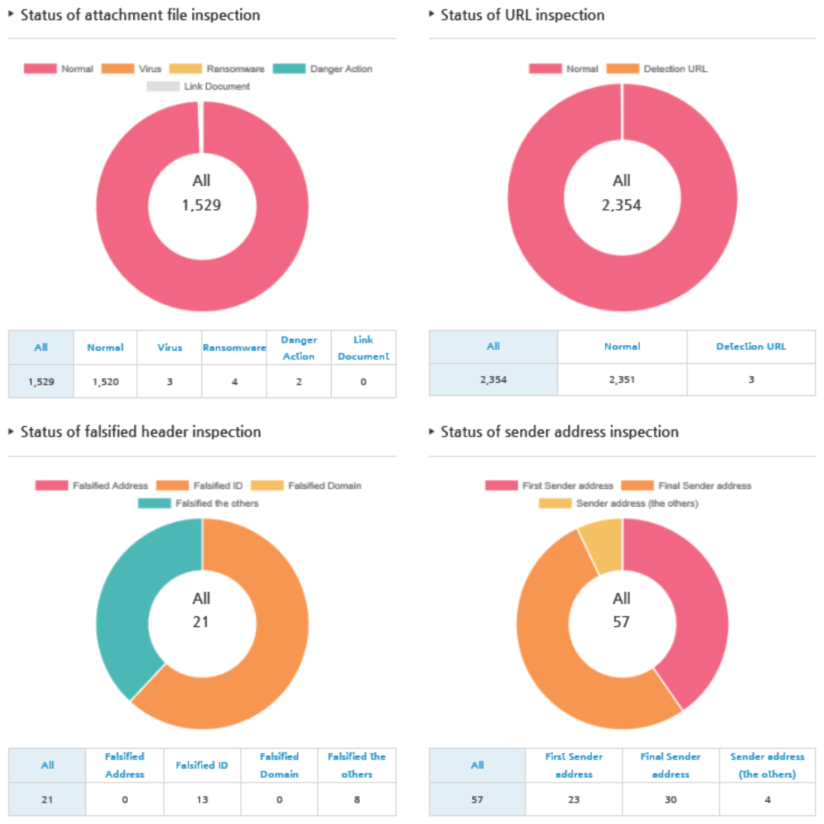
Print 'Report'

‣ Status of operation

Date	All	Normal Mail		Dangerous Mail				Falsified Mail		
		Normal	Reliability (Normal)	AD (Business)	AD (Normal)	Virus Mail	Ransomware	Falsified Header	Danger of sender address	Similar Domain
2018-4-16	422	227	100	25	53	0	1	8	13	3

‣ Status of delivery

All	423
Delivery	403
Deliver automatically	0
Not Delivery	19
Re-delivering (Now)	0
Impossible to deliver	0
Delivery Fail	1



‣ Status of attachment file inspection

All	Normal	Virus	Ransomware	Danger Action	Link Document
1,529	1,520	3	4	2	0

‣ Status of URL inspection

All	Normal	Detection URL
2,354	2,351	3

‣ Status of falsified header inspection

All	Falsified Address	Falsified ID	Falsified Domain	Falsified the others
21	0	13	0	8

‣ Status of sender address inspection

All	First Sender address	Final Sender address	Sender address (the others)
57	23	30	4

Status report of each type of attacks

Receive GUARD's range of security

The New Benchmark for Email Security

Compared to other products, Receive GUARD has differentiated range of security

APT
UnShare VM

Inspection type

- Vius Pattern
- Behavior-based file inspection

Inspection Range

- Attached files

SPAM

- Block SPAM
- Block Patterned Virus

Receive GUARD
Share Virtual Area

Inspection type

- Virus Pattern
- Behavior-based file inspection
- Intelligent mail attack

Inspection Range

- Attached files
- Attached files in the body text, attachment , URL
- BEC

Case 1.

Attack by using same e-mail account

Ransomware attack disguised
as company's employee

i. Impersonating as a retired employee
e-mail attack occurred against all employee

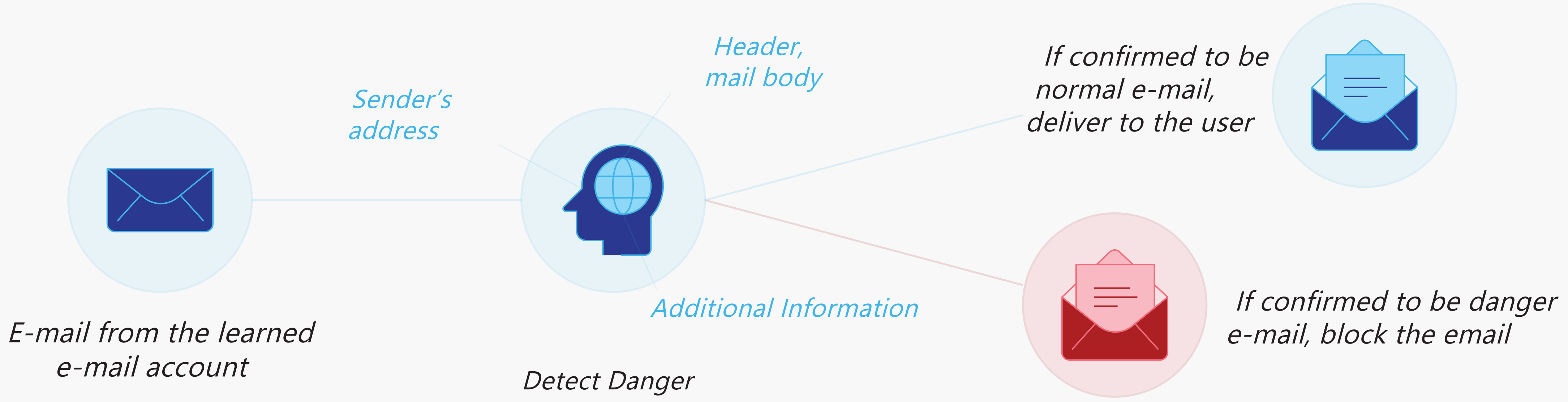
ii. Click the file without any suspicion

iii. Crashed the company's network
by new ransomware

If it is a same domain, how can you tell which e-mail is from the hacked account?

Even the account is approved by the user, Receive GUARD still runs ispection for every e-mail so that the AI can confirm the e-mail's safety depending on it's learned data. Moreover, Sender's address tracking can prevent the attack. By tracking back the route the mail was sent, Receive GUARD warm the user with danger if the route has been changed compared to the previous record. Therefore, the user can double check the safety of the e-mail

Credibility Program



Sender's address

Header, mail body

If confirmed to be normal e-mail, deliver to the user

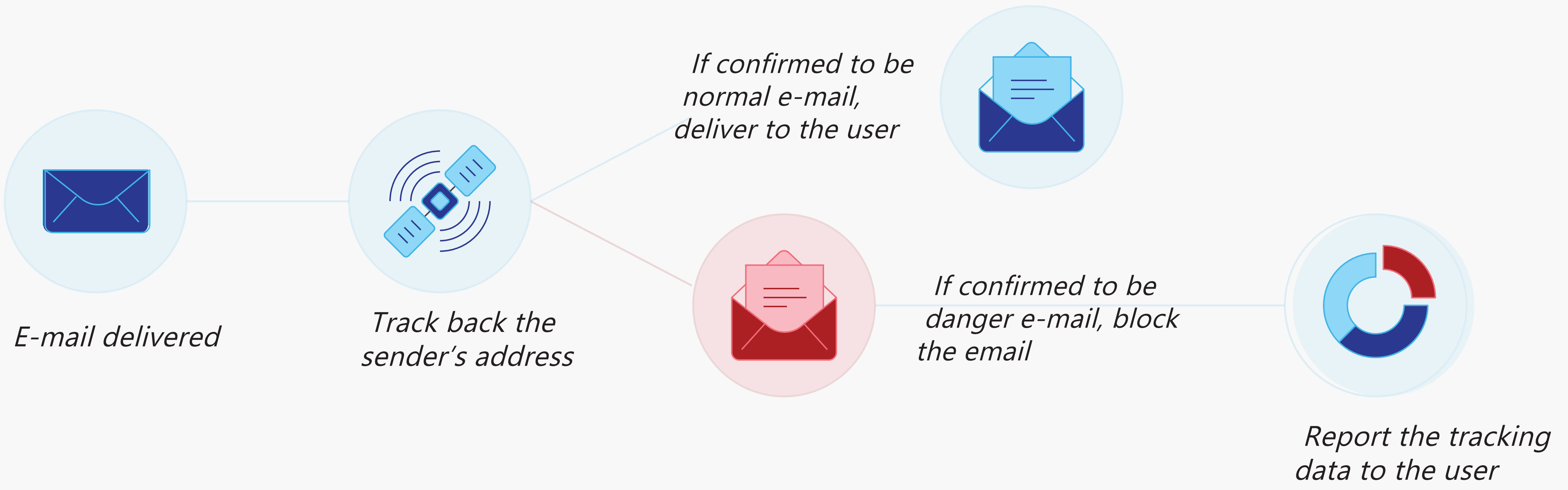
Additional Information

If confirmed to be danger e-mail, block the email

E-mail from the learned e-mail account

Detect Danger

Sender's Address Tracking



If confirmed to be normal e-mail, deliver to the user

E-mail delivered

Track back the sender's address

If confirmed to be danger e-mail, block the email

Report the tracking data to the user

Case 2.

Attack by using similar(look-alike) domain

Financial damage due to look-alike domain

i. Impersonating as a client, sent e-mail for hacking

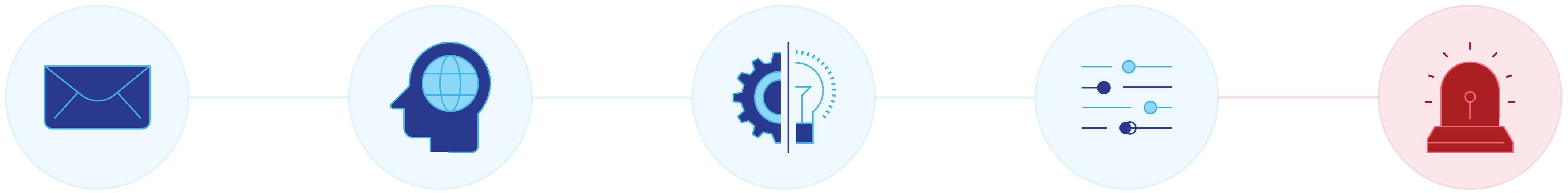
ii. Normal e-mail account without any virus

iii. Since it looked like a client, transacted money that resulted in financial damage

How can you tell the difference when the hacked domain looks identical to the normal domain?

Receive GUARD learns all the data of all the e-mail received by the entire company. Based on the data, Receive GUARD compare and analyze the e-mail's data and alert the user with danger when some factors that are hard for user to notice is detected

Analyze and filtering about similar mail address



Company data filtering

E-mail delivered

Analyze e-mail account

Compare and Analyze based one existing data

User data filtering

Alert when danger detected

Case 3.

Attack by using Malicious URL

How can you tell the URL is malicious when it is just written in the mail body without any suspicious factor?

Before delivering the e-mail to the user, Receive GUARD runs simulation and inspect through the e-mail body, and the link in the body as well as the attachment files and links in the files. If the URL in the e-mail turns out to be including another URLs, Receive GUARD tracks till the End-Point and prevent any additional threats or danger.

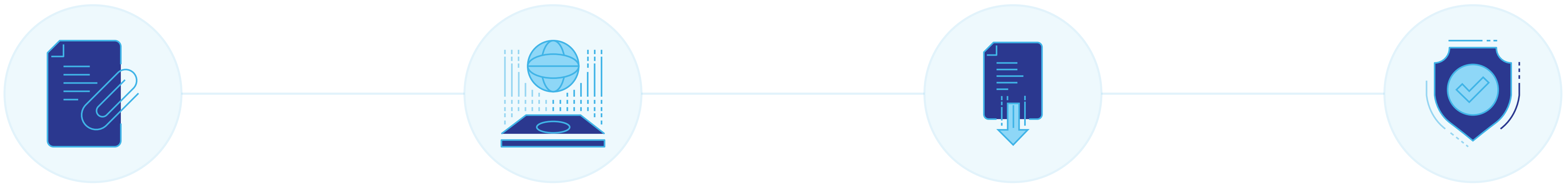
Global company, leak private information of customers due to hacking e-mail

i. E-mail phishing disguising as client

ii. Virus file in the URL in the Phishing mail

iii. By clicking the URL, hackung attempt succeeded that resulted in the leakage or private information of customers

Inspect body text and Pre-emptive block any danger possibility



Inspection in the VA

Inspection for attachment files

Mail body link in the file

Inspection of additional links inside the website

Inspection through End-Point

Prevent the damage of user

Case 4.

Attack by using New Ransomware (Malicious codes)

Ransomware attack by e-mail disguising as a global shipping company

i. E-mail disguising as shipment instruction from the shipping company

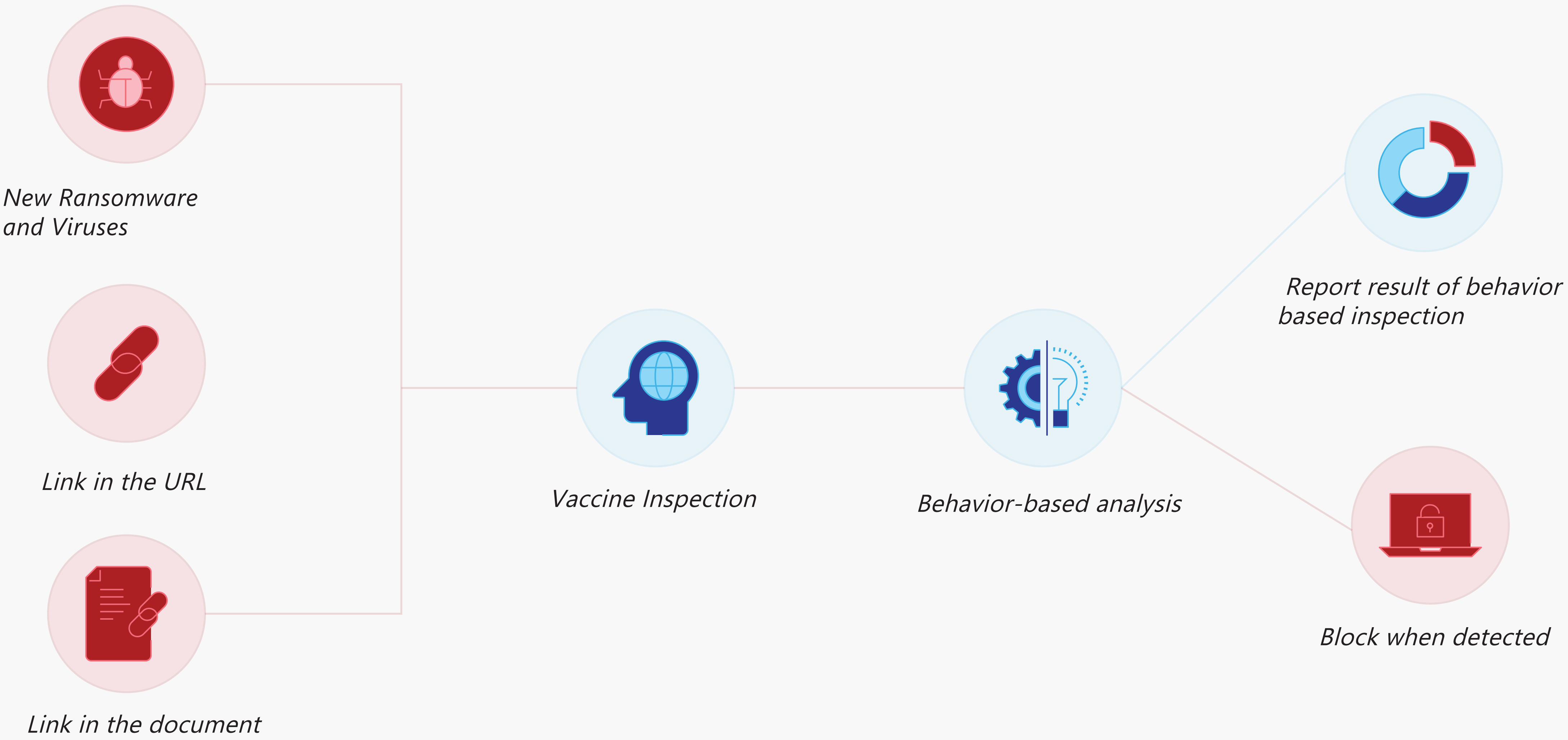
ii. Click the attachment file without any suspicion

iii. Ransomware file disguised as image installed an network infected by ransomware - Hacker demand bitcoin in exchange to decrytion

How can you confirm the file's danger in this case?

If there are ransomware inside the attachment file, link in the document, URL in the mail body, it is hard for conventional vaccine inspection to prevent all those dangers. Therefore, several levels of inspection is needed sush as vaccine inspection-behavior-based analysis to prevent ransomware. Especially, behavior based analysis runs an inspection of all the files including those that are not detected with any danger in the vaccine inspection.

Inspect vaccine and behavior analyzing



New Ransomware and Viruses

Link in the URL

Link in the document

Vaccine Inspection

Behavior-based analysis

Report result of behavior based inspection

Block when detected

Our Clients

VIETSOVPETRO

NFRI National Fusion Research Institute

Quân đội nhân dân

HYUNDAI HEAVY INDUSTRIES CO.,LTD.

OCI

TÀI NGUYÊN & MÔI TRƯỜNG BÁO ĐIỆN TỬ CỦA BỘ TÀI NGUYÊN MÔI TRƯỜNG

TAISUN Growing Together

MARVELHOUSE Singapore International Preschool

LG Chem

KOLON

NHAT TIN logistics

COSMO

TOYOTA HUẾ

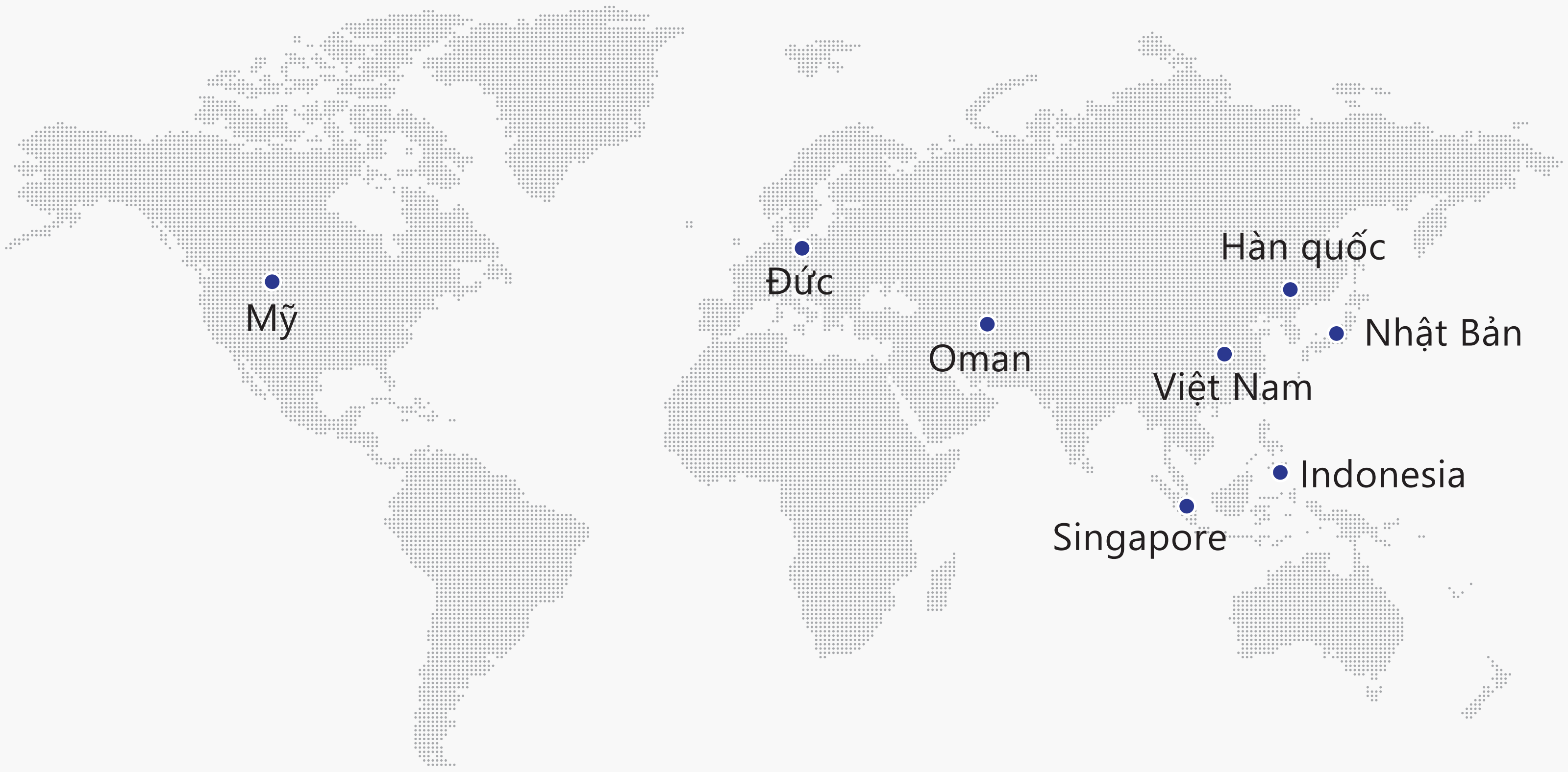
GILIMEX

DINTEC

Fahasa.com

Global Bussiness Area

The world-chosen e-mail security product, Receive GUARD



VNETWORK JOINT STOCK COMPANY

[A] X0-4. 59, Floor 4, Sunrise City North Tower,
27 Nguyen Huu Tho, Tan Hung, Dictrict 7,
Ho Chi Minh City, Viet Nam

[T] (028) 7306 8789 - **[E]** contact@vnetwork.vn

www.vnetwork.vn