The New Benchmark for Email Security

Receive GUARD

New paradigm of email security

Intelligent Learning

Prevent APT Attacks

Block New Ransomware

Detect email Fraud

Analyze Hacker Information

Security system establishing

VNETWORK
safe and saved

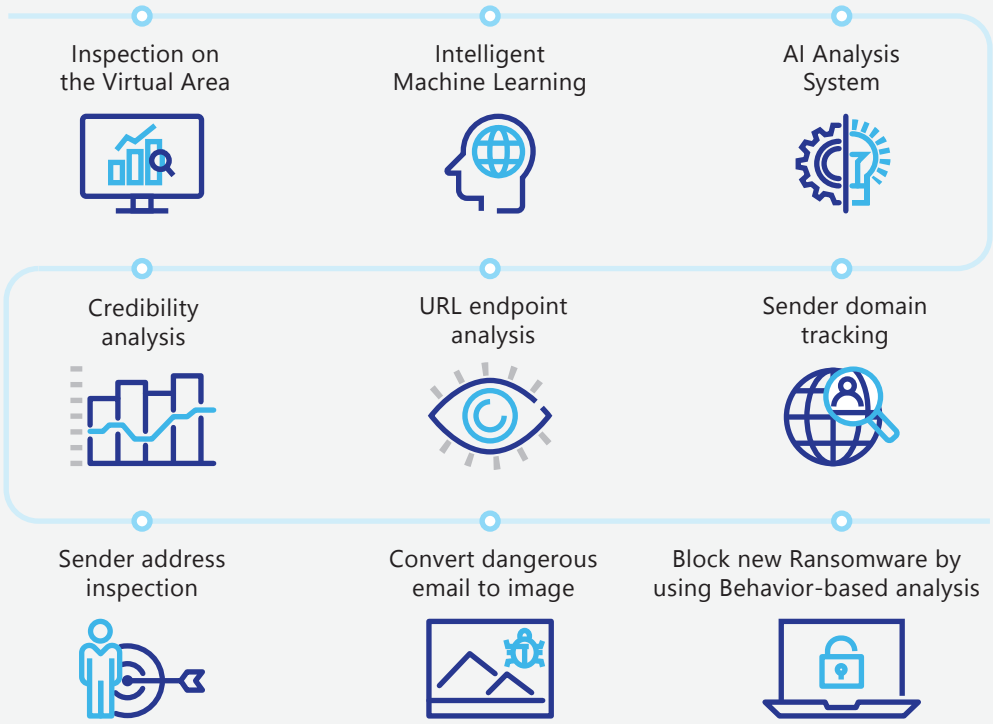
Product Overview

Receive GUARD - The email Security Solution certified by Global Assessments.

Receive GUARD is the must have email security system to make good the shortcomings of other email system by using AI and Machine Learning.

Main Functions

The most dedicated BEC Filtering System



AI Technology

Machine Learning - Securing User Emails

Develop customized database for enterprise

Detect email fraud

Detect virus by using behavior-based analysis

Case 1.
Attack by using same email account

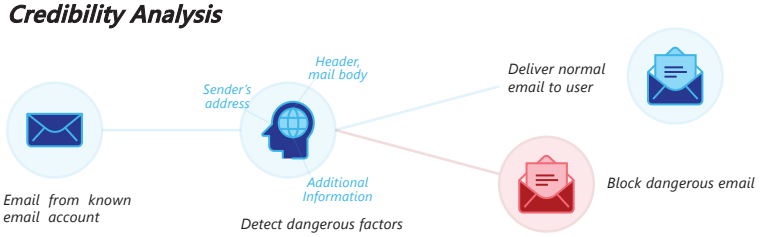
Hackers impersonate as a company employee.

i. Impersonating as a retired employee to send email included dangerous factors
ii. Recipients open email without any suspicion
iii. The company network will be infected with ransomware

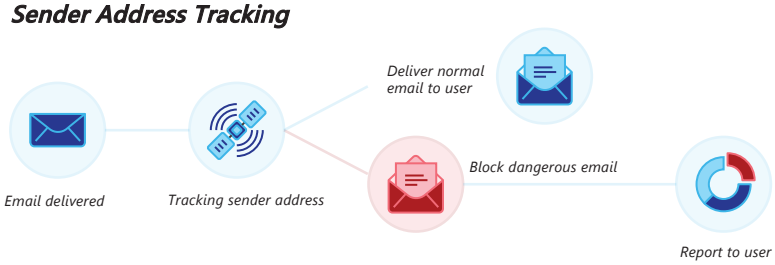
If it is a same domain, how can you tell which e-mail is from hacked?

Receive GUARD will runs inspection for every incoming email so that AI can make sure about the email safety based on learned - data. Moreover, "Sender address tracking" has ability to prevent attacks by tracking the route of sent mails. Receive GUARD will alert user if having any changes compared to the previous record.

Credibility Analysis



Sender Address Tracking



Case 2.
Attack by using similar domain

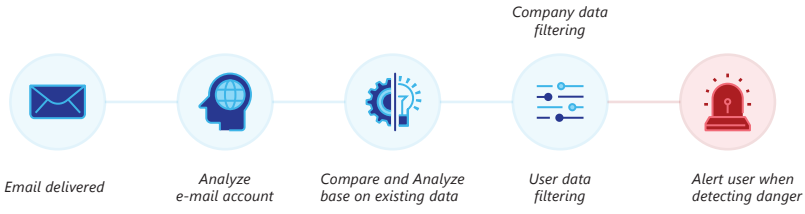
Financial loss due to lacking of vigilance

i. Impersonating as a client to send email to enterprise
ii. Normal email account with no suspicious element or virus
iii. Transactions are processed, causing financial damage

How can you tell the difference between hacker's domain and normal domain?

Receive GUARD learns all received emails data. Based on that, Receive GUARD compares and analyzes email and alert the user.

Analyzing and filtering similar email address



Case 3.
Attack by using Malicious URL

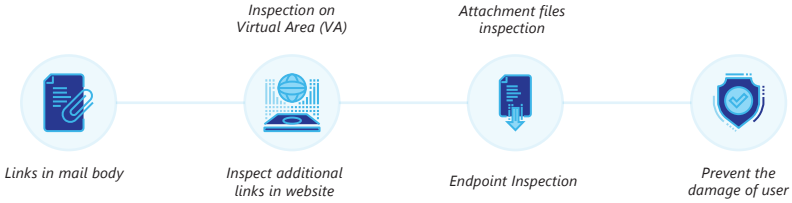
The private information of global company customers

i. Impersonating as a client to send Phishing email
ii. Viruses are hidden in the URLs
iii. When clicking on the URL, causing the leakage of confidential business information

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

Before delivering email to user, Receive GUARD runs a simulation and inspects the email body, links as well as attachment files. Receive GUARD will track till the URL Endpoint to prevent any additional threats or danger.

Inspect body text and block any dangerous possibility



Case 4.
Attack by using New Ransomware (Malicious codes)

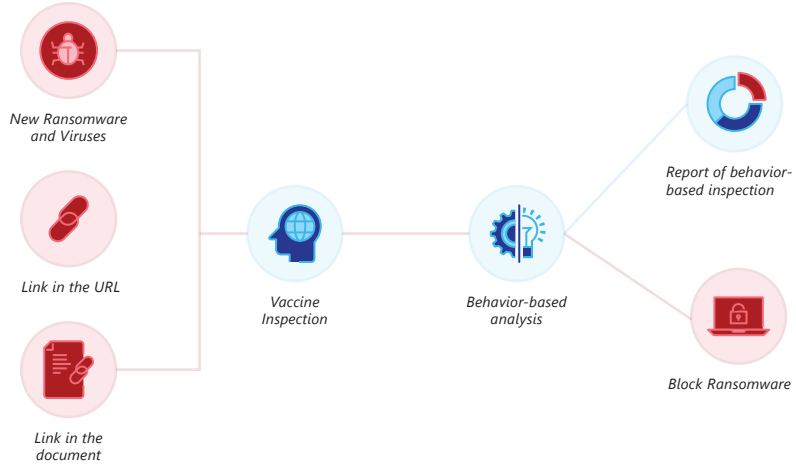
Ransomware attacks users via attachment files

i. Disguising as State organization or Government.
ii. Click on the attachment file without any suspicion
iii. When company network infected with ransomware, hackers will request payment to decrypt data.

How can you identify all dangerous factors in this case?

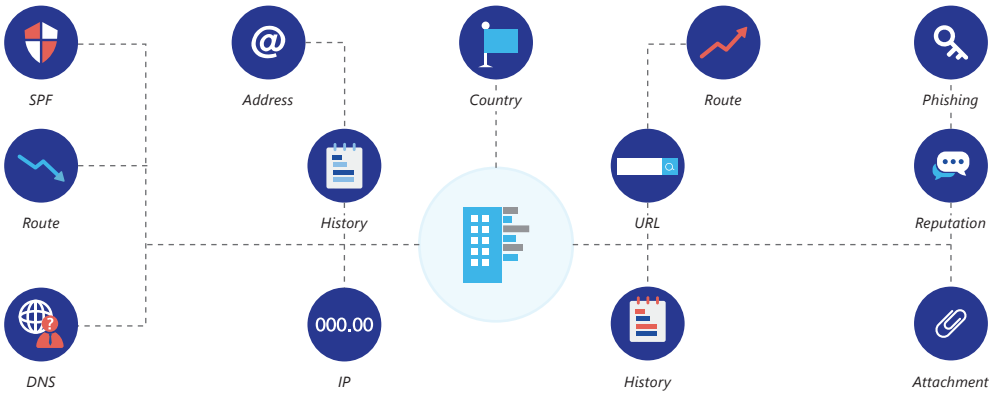
If ransomware included in attachments, links or URL in the email body, it is difficult for Vaccine Inspection to prevent them all. Thus, several layers of inspection are needed. Besides, behavior-based analysis inspects all the files including dangerous factors in the Vaccine Inspection

Inspect vaccine and behavior analyzing



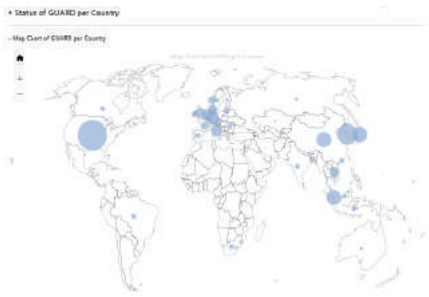
BIG DATA Customization

Build BIG DATA System for each customer

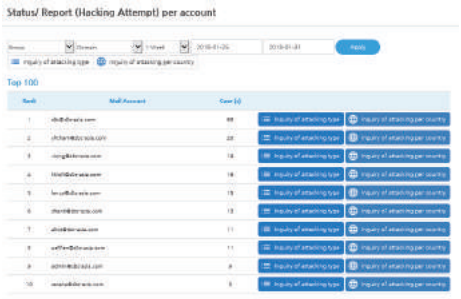


Statistics Report

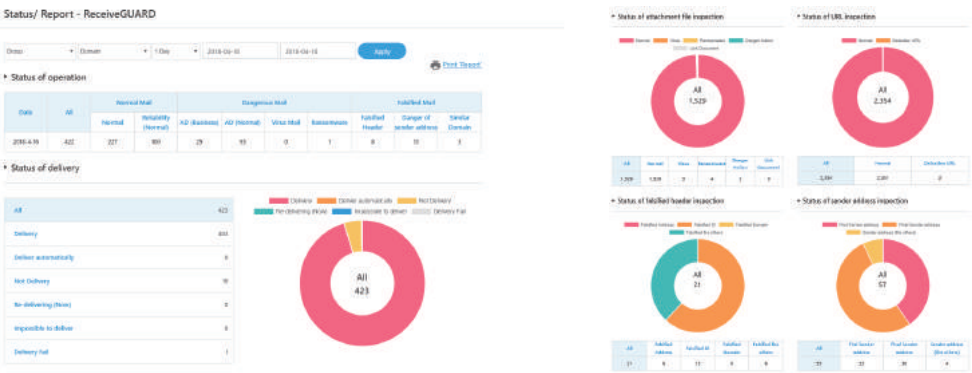
Dangerous factors analysis in real time



Attacks per country Report



Hacking attempts per account Report



Types of attacks Report

SCM GUARD Platform

From start to end of e-mail

Receive GUARD

Next generation firewall for e-mail security

SECUMAIL

Self-developed Email System

Send GUARD

Coming Soon

Email Management Solution to protect Confidential Business Information

Security range of Receive GUARD

New standard of email security

Receive GUARD has a different security range compared to other systems

APT
UnShare VM

Inspection type
- Virus Pattern
- Behavior-based file inspection

Inspection Range
- Attached files

SPAM

- Block SPAM
- Block Virus pattern

Receive GUARD
Inspect on VA
(Virtual Area)

Inspection type
- Virus Pattern
- Behavior-based file inspection
- Social engineering attacks

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

Global Market

Receive GUARD - World's choice of Email Security Solution

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]** sales@vnetwork.vn