

Là đơn vị tiên phong trong lĩnh vực bảo mật an ninh mạng tại Việt Nam. Mang đến **giải pháp & dịch vụ CNTT** an toàn và tiết kiệm

VNETWORK là Công ty CNTT chuyên cung cấp các giải pháp về hạ tầng, truyền tải và bảo mật an ninh mạng.

Với định hướng phát triển rõ ràng, VNETWORK là đơn vị tiên phong trong việc ứng dụng và chuyển giao công nghệ tiên tiến với các tiêu chuẩn dịch vụ quốc tế tại Việt Nam.

Receive GUARD

Giải pháp bảo mật Mail Gateway thế hệ mới

I



Tầm quan trọng của Email bảo mật

- | 01 Thống kê thiệt hại từ các cuộc tấn công
- | 02 Receive GUARD

1. Thống kê thiệt hại từ các cuộc tấn công

Sự phát triển của tấn công Email **Social Engineering**



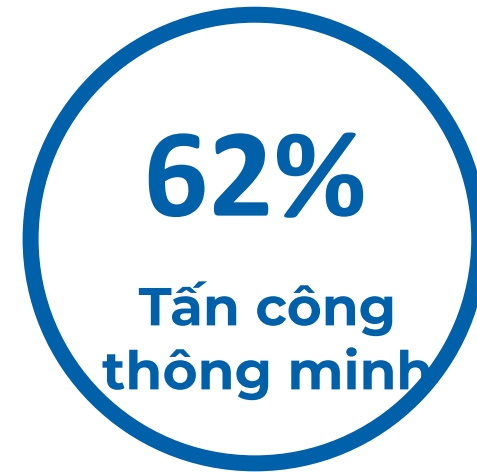
Đường dẫn Hack

Nguồn: Palo Alto Networks



Thiệt hại từ BEC

Nguồn: Trend micro paradigm



Tấn công qua Email

Nguồn: Valimail

1. Thống kê thiệt hại từ các cuộc tấn công

Sự phát triển của tấn công Email **Social Engineering**



Mã độc Ransomware

Nguồn: Trend Micro



Tấn công mạng

Nguồn: VNCERT

2. Receive GUARD



Giải pháp duy nhất có thể chống lại các cuộc tấn công Social Engineering thông qua việc phân tích hành vi

Công nghệ được chứng nhận bởi Gartner®

Chuyên xác định BEC



Cyber Security – Sản phẩm duy nhất trên thế giới đối phó được với các **tấn công APT và BEC** bằng công nghệ tự phát triển, hệ thống lọc dựa trên hành vi, công cụ email và bí quyết dịch vụ.

Chủ động phân tích tổn hại



Phân tích dựa trên hành vi phát hiện các khả năng nguy hiểm trong nội dung, hình ảnh, URL ẩn trong tệp đính kèm.
Chủ động chặn ransomware và các phần mềm độc hại

Loại bỏ tác nhân có nguy cơ gây hại



Khi hành vi bất thường được phát hiện trong email nhận, nó được chuyển đổi thành hình ảnh để loại bỏ rủi ro.
Nếu người dùng trả lời email có địa chỉ giả mạo nguy hiểm, người quản trị sẽ được cảnh báo

2. Receive GUARD



Đánh giá toàn cầu Certification

2017-03

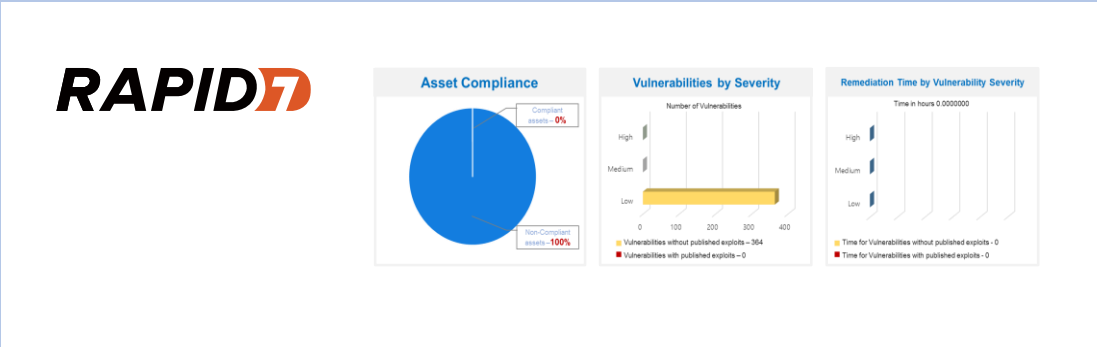


Gartner

Receive GUARD chuyên ngăn chặn các cuộc tấn công có chủ đích

Giải pháp bảo mật email thế hệ mới được ứng dụng trí tuệ nhân tạo và máy học

2017-09



364 bài kiểm tra phân tích lỗ hổng của chính phủ Singapore, kết quả sản phẩm không có lỗi, “điểm yếu bằng 0”

II



Giới thiệu Giải pháp

- | 01 | Các tính năng
- | 02 | Tính năng cốt lõi
- | 03 | Báo cáo thống kê

1. Các tính năng

Phân tích nguyên nhân của Email độc hại và tùy chỉnh lọc



Vùng ảo (VA)

- Kiểm tra theo thời gian thực các email được gửi đến bằng cách phân bổ vùng ảo (VA) cần thiết cho mỗi email.
- Hơn 1000 (VA) có sẵn để phân bổ.
- Đảm bảo tốc độ nhận email và tính chính xác trong quá trình kiểm tra.
- Phân tích URL và các tập tin giả mạo, kiểm tra virus, malwares.



Độ tin cậy của chương trình

- Tạo điểm tin cậy dựa trên kết quả phân tích và học trong VA.
- Xây dựng mức độ tin cậy của mỗi email được gửi đến.
- Xác định việc gửi email đến cho users dựa trên mức độ rủi ro được đánh giá bởi mức độ tin cậy.



Học thông minh

- Phân tích nội dung email trong trường hợp người dùng muốn nhận email bị khoá trước đó
- Tự động tạo các mẫu phù hợp với các trường hợp ngoại lệ khi phân tích thư
- Lưu trữ trong sơ đồ mã hoá để ngăn chặn trường hợp giả mạo thư mẫu



Chặn mã độc Ransomware

- Liên tục quét virus, kiểm tra virus và malware trong các tệp đính kèm email
- Trong VA, hệ thống sẽ mở URL và tải về tệp đính kèm để xác định rủi ro.
- Phát hiện phần mềm độc hại với phần mở rộng tệp.



Phân tích real-time điểm cuối của URL

- Kiểm tra tất cả địa chỉ được liên kết với thư bằng cách mở trước trong VA để kiểm tra các mã độc được ẩn đi.
- Loại bỏ các mối nguy hại tiềm ẩn khác bằng cách kiểm tra tất cả các URL có trong email, nếu nhận thấy có một liên kết khác, hệ thống sẽ tự động mở liên kết đó đến khi đảm bảo không còn URL nào sót lại.



Theo dõi địa chỉ người gửi

- Thông tin lộ trình đầu tiên của email (email routing) cho mỗi tài khoản được lưu trữ.
- Và so sánh với lộ trình mới khi nhận thư từ một địa chỉ đã trao đổi trước đó
- Chèn thông báo cảnh cáo khi phát hiện có sự thay đổi



Kiểm tra địa chỉ người gửi

- Kiểm tra tính hợp lệ của địa chỉ chuyển tiếp email.
- Mặc dù server hợp lệ, hệ thống sẽ vẫn kiểm tra để xác minh địa chỉ người gửi và người nhận nhằm phát hiện các hành vi giả mạo.
- Ngăn chặn các cuộc tấn công Email snoofing.



Chuyển Email đáng ngờ thành hình ảnh

- Cho phép mã hoá email độc hại sang hình ảnh trước khi gửi đến cho người dùng
- Gửi nội dung email cho người dùng sau khi mã hoá thành hình ảnh đối với trường hợp URL đã được kiểm tra trong email đã khoá.
- Gửi nội dung email sau khi xác nhận địa chỉ và mật khẩu qua tài khoản thực được xác nhận.



Kiểm tra tên miền tương tự

- So sánh với tên miền đã lưu trữ trước đó
- Nếu nhận thấy sự khác biệt, gửi cảnh cáo cho người dùng

1. Các tính năng

Phân tích nguyên nhân của Email độc hại và tùy chỉnh lọc



Báo cáo

- Quản trị viên được phép thiết lập báo cáo (cho ai và các nội dung báo cáo)
- Chặn email sau khi kiểm tra báo cáo và kết nối các liên kết riêng /Bật cho phép
- Gửi email báo cáo cho người dùng. Ví dụ: lịch sử chặn của họ.
- Các tính năng quản lý email như: lịch sử đến, chặn thủ, cho phép nhận email



Quản lý kinh doanh/ Tin quảng cáo

- Quản lý email thông qua thiết lập các mẫu tiêu đề hoặc nội dung
- Quản lý email dễ dàng thông qua các số liệu thống kê riêng biệt



Cân bằng tải

- Tự kiểm tra trạng thái lưu lượng truy cập, phân phối và chuyển tiếp sử dụng
- Xử lý kịp thời khi nhận được email có dung lượng lớn



Phân tích file giả mạo

- Các mã độc và virus được nguy trang thành các tệp tài liệu dưới định dạng: PDF, HWP, DOC và PPT.
- Kiểm tra trong vùng ảo và ngăn chặn các rủi ro



• Phát hiện rủi ro trong file đính kèm

- Phân tích nội dung của tài liệu đính kèm trong email để phát hiện các liên kết độc hại.
- Phân tích rủi ro của các liên kết dựa trên dữ liệu đã lưu trữ
- Số lượng dữ liệu càng nhiều càng có nhiều cơ sở để phân tích



Chèn cảnh báo vào tiêu đề

- Khi chặn email được cho phép, một cảnh báo [BLOCK], [WARNING] được chèn và gửi đến người dùng
- Kiểm tra tính bảo mật của thư bằng cách kiểm tra nội dung cảnh báo
- Nội dung cảnh báo có thể được thay đổi bởi quản trị viên



Lưu trữ

- Cho phép sao lưu riêng tư thường xuyên theo cài đặt của quản trị viên
- Khôi phục các email đã bị vô tình xóa đi
- Áp dụng lưu trữ giống như hệ thống webmail của người dùng
- Giữ nguyên văn bản gốc như hệ thống Email thực tế bằng cách tách thông tin và File



Xây dựng dữ liệu cá nhân

- Gửi báo cáo định kỳ cho người dùng cá nhân khi chặn Email
- Quản lý dữ liệu của người dùng thông qua một trang web cá nhân chuyên dụng.
- Được áp dụng cho các hệ thống mà không có quản trị viên trung tâm riêng biệt.
- Việc xác minh của nhiều người dùng đảm bảo lọc rõ ràng hơn.

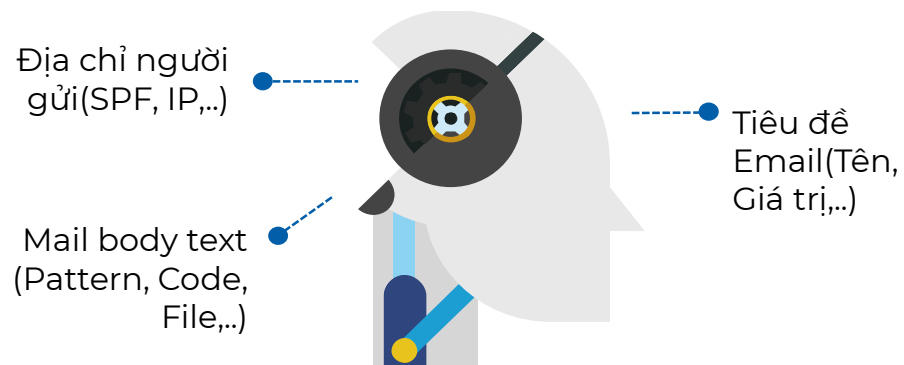


Hỗ trợ đa dạng

- Cung cấp chức năng quản trị viên Website để cho phép kiểm tra với Email Server được kết nối.
- Có yêu cầu RCPT và lịch sử của kết quả chuyển tiếp Email.
- Cung cấp thông tin thời gian thực về toàn bộ hoạt động của hệ thống
- Cung cấp cài đặt cho mạng riêng nội bộ

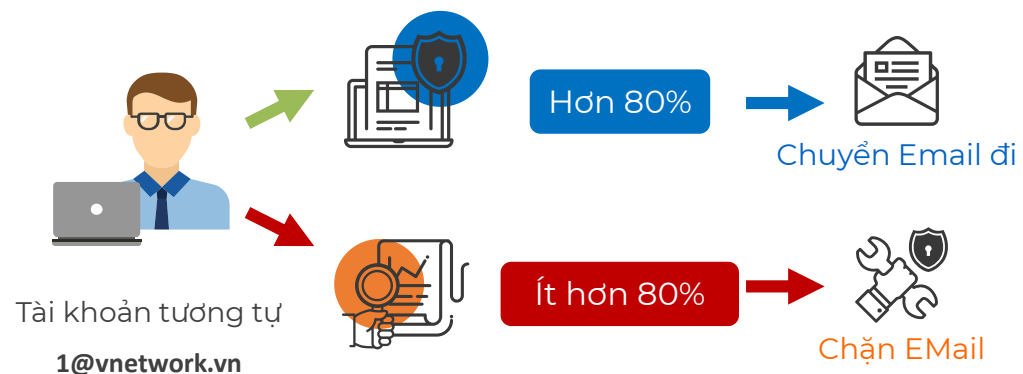
Xây dựng dữ liệu cho mỗi Mail đầu vào

Học, phân tích mỗi tài khoản Email gửi đến



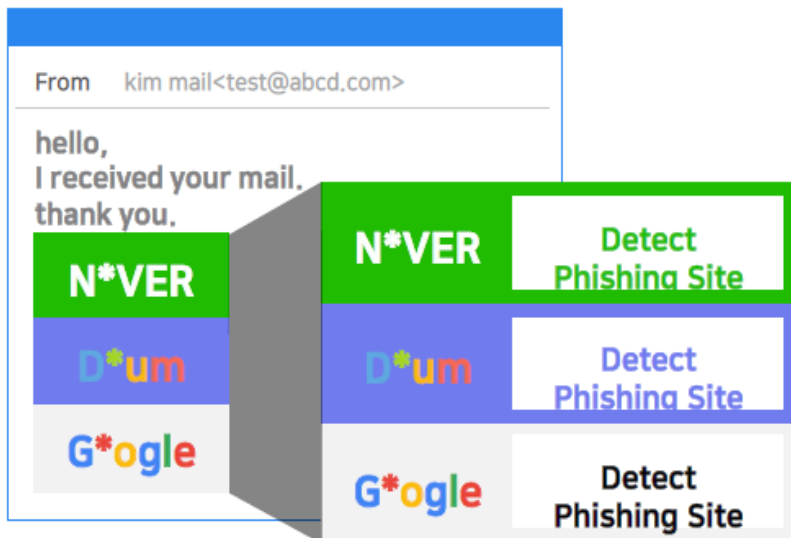
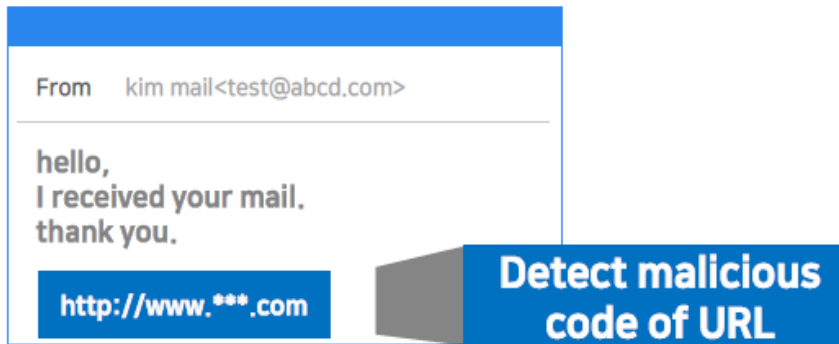
Sử dụng công nghệ “Máy học” để học tất cả Email đầu vào.
Mất khoảng 2~4 tuần để hiểu rõ hành vi của người dùng Email.

Dựa trên việc học, tạo sự tin cậy cho mỗi Email



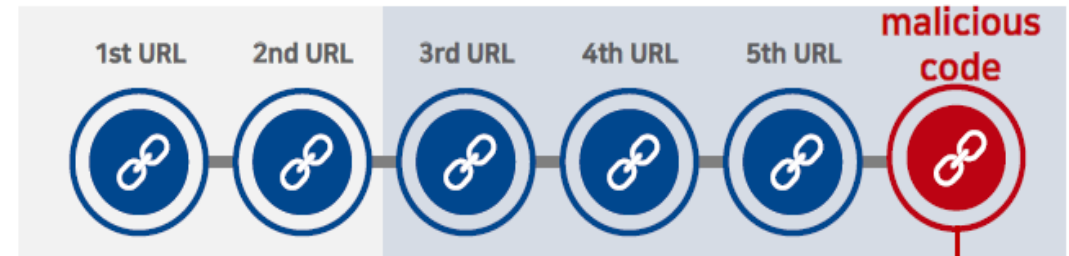
Thông qua kết quả học, so sánh và phân tích thư được gửi từ cùng một tài khoản để xác định xem Email đó có bình thường không.

2. Chức năng cốt lõi (Học nội dung Email)



Normally detect this area

Hidden danger area



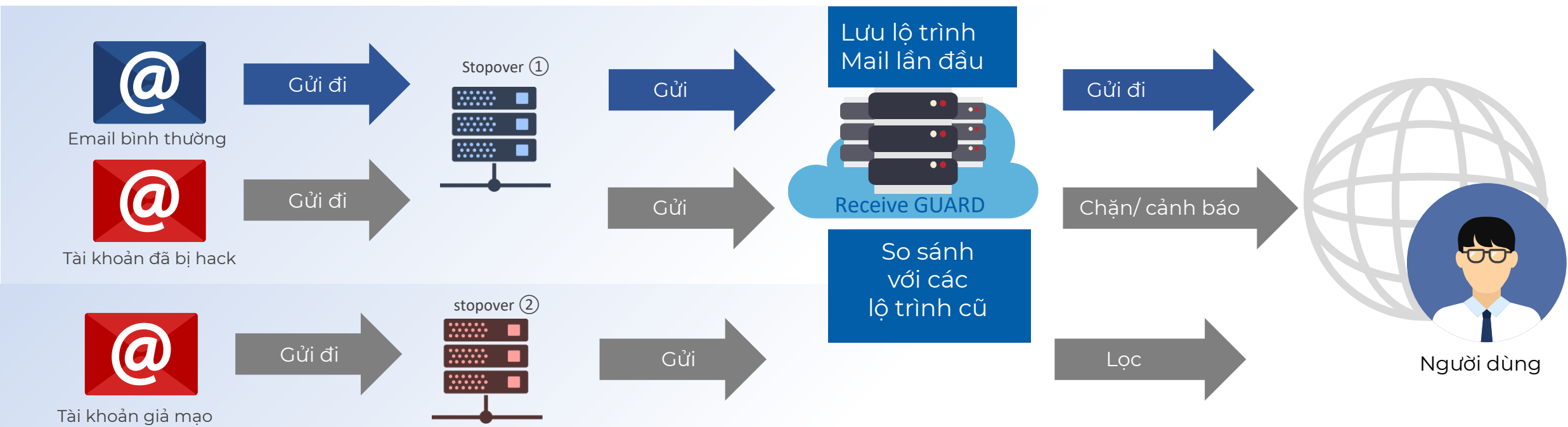
Track to End-points



2. Chức năng cốt lõi (Theo dõi địa chỉ người gửi)



Chặn các lộ trình thay đổi so với thông thường



Receive GUARD lưu địa chỉ người gửi Mail trước đó; nếu nó thay đổi đột ngột, **Receive GUARD** sẽ chặn và cảnh báo người nhận để kiểm tra thêm khi cần.
Người nhận có thể kiểm tra người gửi có thực sự thay đổi địa chỉ hay không

2. Chức năng cốt lõi (Phát hiện tên miền tương tự)



1@VNETWORK.VN



Capital letter - O

1@VNETWORK.VN



The number - 0

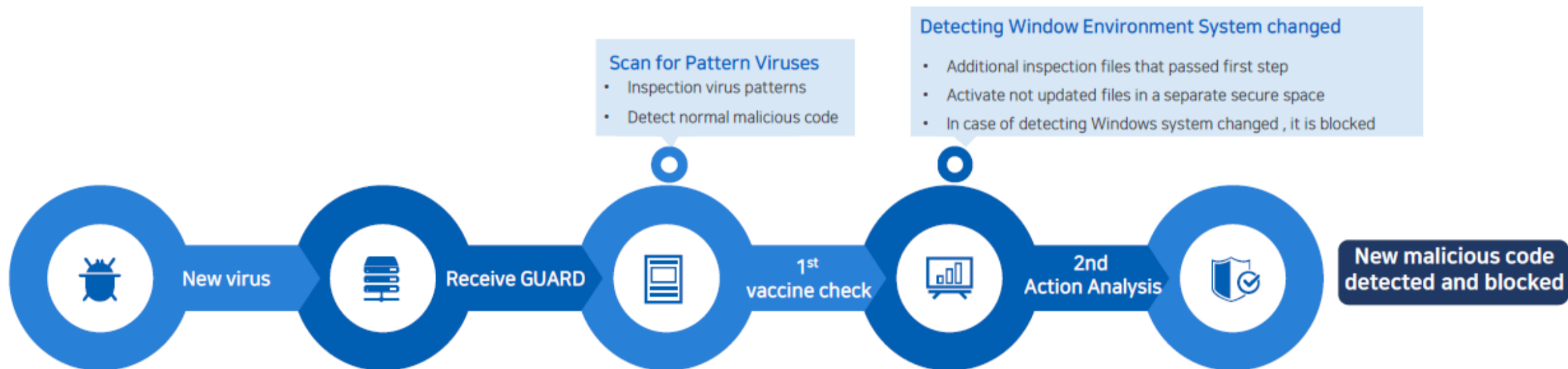
Lọc các điểm tương tự (Cảnh báo, Thận trọng, Cần xem) thông báo cảnh báo người dùng)

“Phát hiện tên miền tương tự mà mắt thường không phân biệt được”

- Xây dựng dữ liệu cho từng doanh nghiệp và người dùng cá nhân cho các địa chỉ Email và tên miền (tài khoản) đến.
- Nếu các địa chỉ tương tự được tìm thấy, người dùng sẽ được cảnh báo bằng cách tiến hành kiểm tra tương tự trên tài khoản nhận được trong tương lai.

2. Chức năng cốt lõi (Phát hiện Virus mới)

Multiple different inspection ways for analyzing all of behavior case



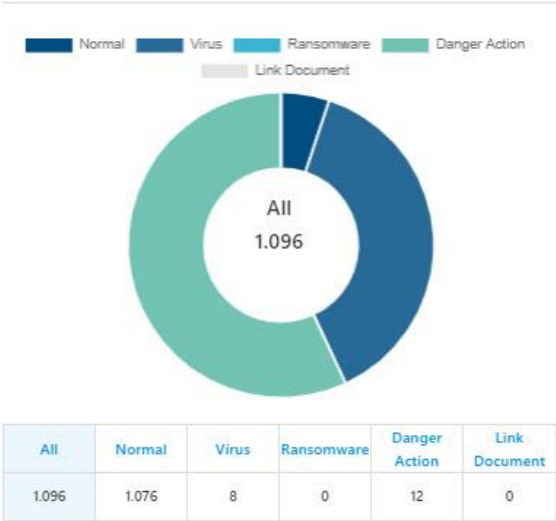
I. Perform an examination of files even though no abnormalities were detected in the 1st vaccine test.

2. 2nd test is to filter attachments based on the purpose of action regardless of MS or vaccine.

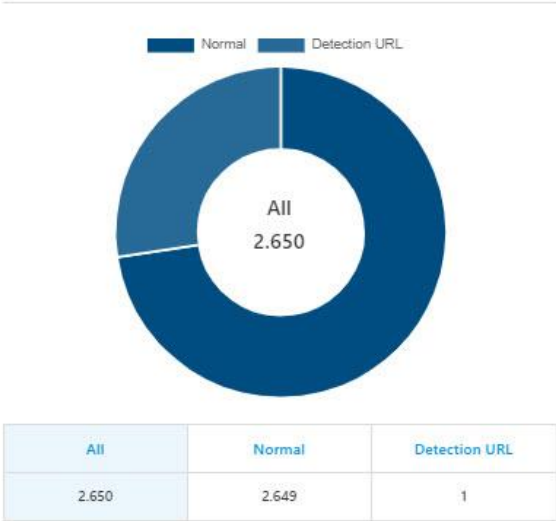
- Files attempting to change parameters of Windows system
- Files trying to act beyond the limits as a downloaded file
- Programs attempting to install unknown software in the system during compression or decompression

3. Báo cáo thống kê

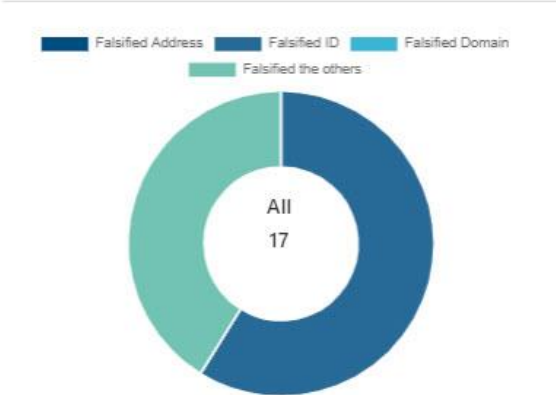
► Status of attachment file inspection



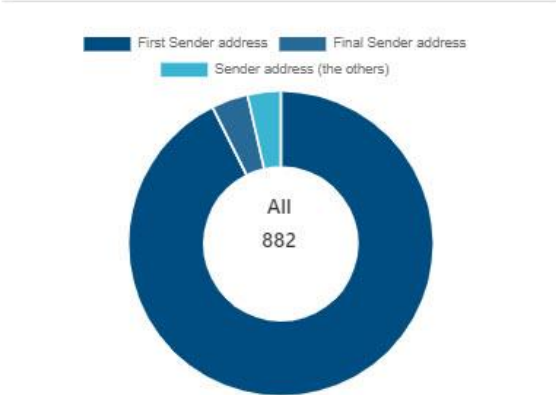
► Status of URL inspection



► Status of falsified header inspection



► Status of sender address inspection

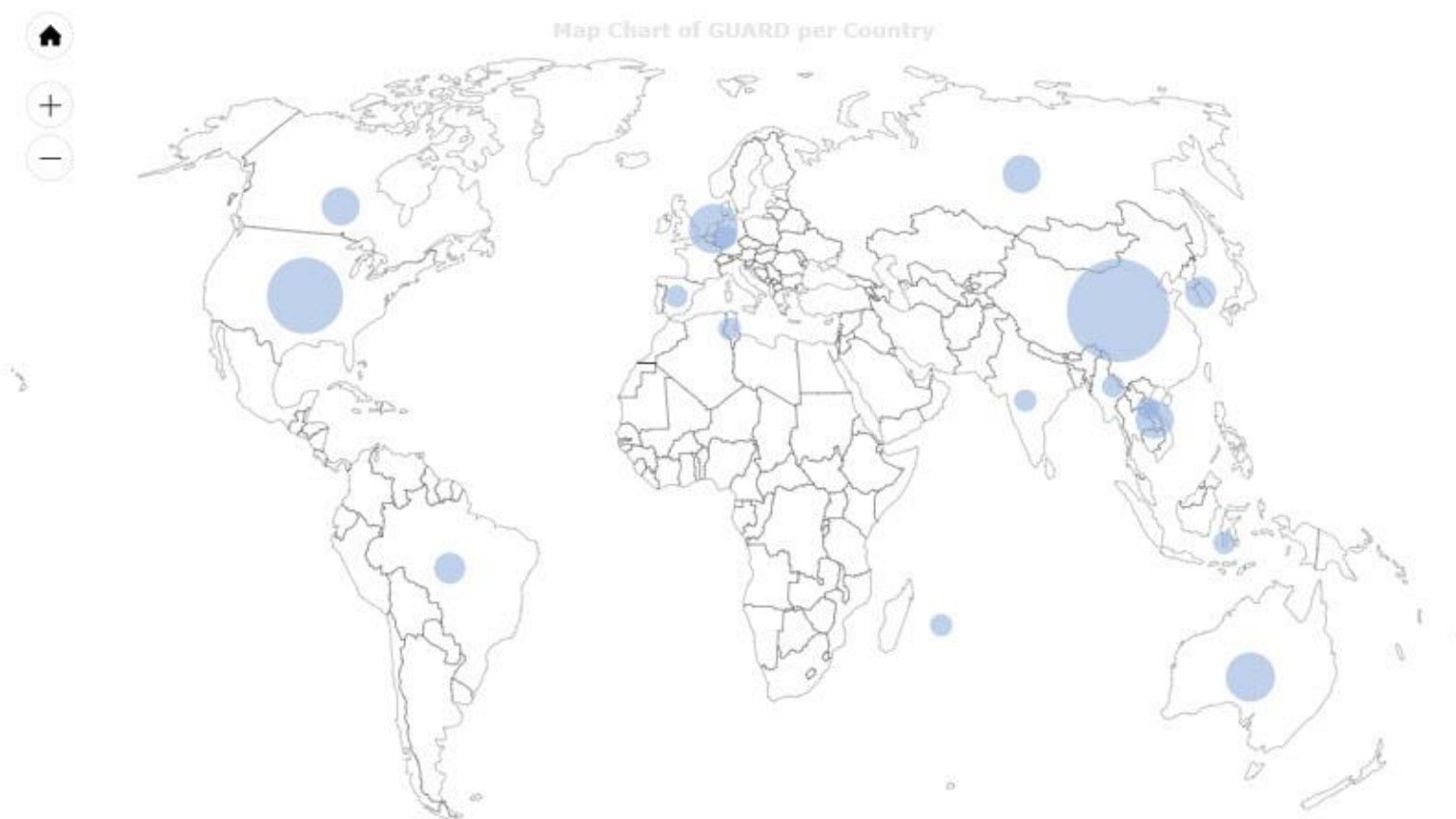


3. Báo cáo thống kê – Lọc



- Status of GUARD per Country

- Map Chart of GUARD per Country



3. Báo cáo thống kê – Lọc

Status/ Report - ReceiveGUARD

Group

▼

Domain

▼

1 Day

▼

2019-03-07

2019-03-07

Apply

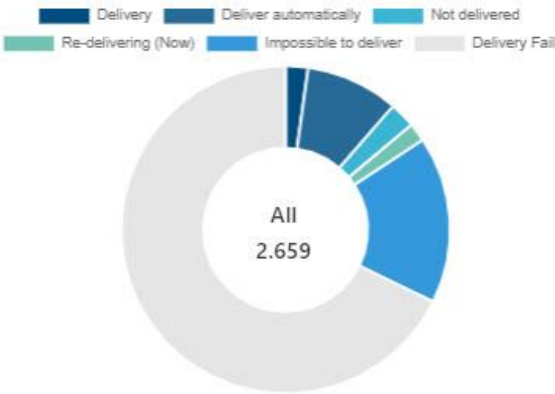
 [Print 'Report'](#)

► Status of operation

Date	All	Normal Mail		Dangerous Mail					Falsified Mail		
		Normal	Reliability (Normal)	AD (Business)	AD (Normal)	Virus Mail	Ransomware	Danger Action	Falsified Header	Danger of sender address	Similar Domain
2019-3-7	2.613	1.071	91	21	141	8	0	12	17	882	2

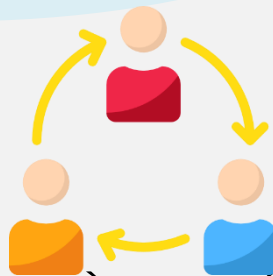
► Status of delivery

All	2.659
Delivery	1.202
Deliver automatically	5
Not delivered	1.405
Re-delivering (Now)	1
Impossible to deliver	9
Delivery Fail	37



4. Tính năng vượt trội

Tính năng vượt trội của **SECUMAIL**

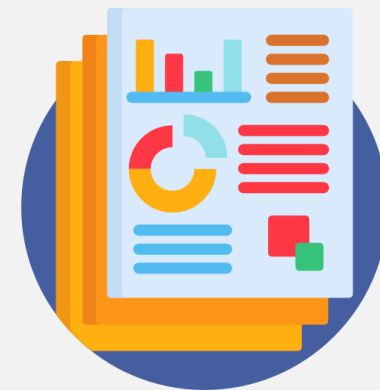


Chia sẻ email

- Chia sẻ email trong cùng một nhóm email.
- Khi người nhận phản hồi bất kì email nào trong nhóm thì tất cả các thành viên đều nhận được.
- Thiết lập hẹn giờ gửi mail.

Tệp đính kèm

- Dung lượng lên đến 10GB
- Cho phép gửi bằng Outlook



4. Tính năng vượt trội



SECUMAIL – “Sự lựa chọn tốt nhất cho giải pháp bảo mật Email”





X-04.59, lầu 4, Sunrise City North Tower,
27 Nguyễn Hữu Thọ, P. Tân Hưng, Q. 7, HCM, Việt
Nam



<https://vnetwork.vn>



contact@vnetwork.vn



(84-28) 73 068 789

THANK YOU