이메일 보안의 새로운 기준

Receive GUARD

From the Beginning to the End of Mail Service
One stop Mail Platform with AI

KIWONTECH

CONTENTS

이메일 보안의 새로운 기준
ReceiveGUARD

From the Beginning to the End of Mail Service
One stop Mail Platform with AI

ReceiveGUARD

ReceiveGUARD
이메일 보안의 새로운 기준

Chapter

메일 보안 중요성

| 01 | 메일 공격 현황

인터넷 인프라 증가에 따른 해커의 **이메일 공격 270% 급증**

87%
이메일

해킹 유입경로

악성메일 공격
유입 경로 이메일 87%

출처 : 팔로알토 네트웍스 보고서

약 1만건
피해

기업 대상 이메일 공격 피해

2017 상반기 : 3,175건
2017 하반기 : 6,533건

출처 : 트렌드 마이크로 연간 보고서

62%
지능형 공격

이메일 공격 방식

악성메일 중 62%
사람의 취약점 공격

출처 : 밸리메일 보고서

| 02 | 메일 공격 유형 및 사례

Ⅰ. 이메일 주소 사칭 공격

사용자의 계정을 탈취, 동일한 메일 주소를 사용하여
상대방에게 악성 메일 발송

평소 메일을 주고 받던 계정에서 온 메일이기 때문에
아무런 의심 없이 메일을 확인하여 피해 발생

Case 1

H공기업, 직원 계정 이용 악성 메일 PC 감염

ⅰ. 퇴직자 계정 도용, 전 직원 상대 메일 공격
ⅱ. 기업 내 다수 PC 해킹
ⅲ. 발전소 도면 등 주요 기밀 자료 유출

Ⅱ. 유사 도메인 주소 공격

사용자가 눈으로 확인하기 불가능 하도록
정상 계정과 유사하게 계정을 생성하여 악성 메일 발송

평소 메일을 주고 받던 계정에서 온 메일이기 때문에
아무런 의심 없이 메일을 확인하여 피해 발생

Case 2

L사, 해킹 메일 사기로 240억 날려

ⅰ. 거래처 위장 해킹 메일 발신
ⅱ. 바이러스 없는 정상 메일로 공격
ⅲ. 거래 대금 240억 헤커에게 송금

| 02 | 메일 공격 유형 및 사례

Ⅲ. 헤더 위/변조 공격

유명 K기업 관리자를 사칭하여 긴급 통보라는 제목으로
메일 계정과 비밀번호를 요청하는 메일 발송

답장하기를 클릭 했을 때 실제 수신하였던 메일 주소의 아이디
부분 철자가 “o”가 아니라 “a”로 변경된 사실 발견

Case 3

K사 사칭, 개인 정보 탈취 피싱 메일

ⅰ. K사 메일 관리자를 사칭하여 계정 정보를 요청하는 메일 발송
ⅱ. 답장 받는 주소를 실제 주소와 유사하게 위변조하여 발송
ⅲ. 비밀번호 등 기업 정보 탈취를 목적으로 한 사이트 연결

Ⅳ. 본문 악성 URL 공격

세금보고 소프트웨어 회사로 위장하여 세금보고 대행자에게
악성 코드가 심어진 웹사이트 링크 첨부하여 메일 발송

세금보고용 소프트웨어 회사라고 생각하여 본문에 담겨진
링크를 클릭하여 PC에 악성코드가 심어진 개인정보 유출

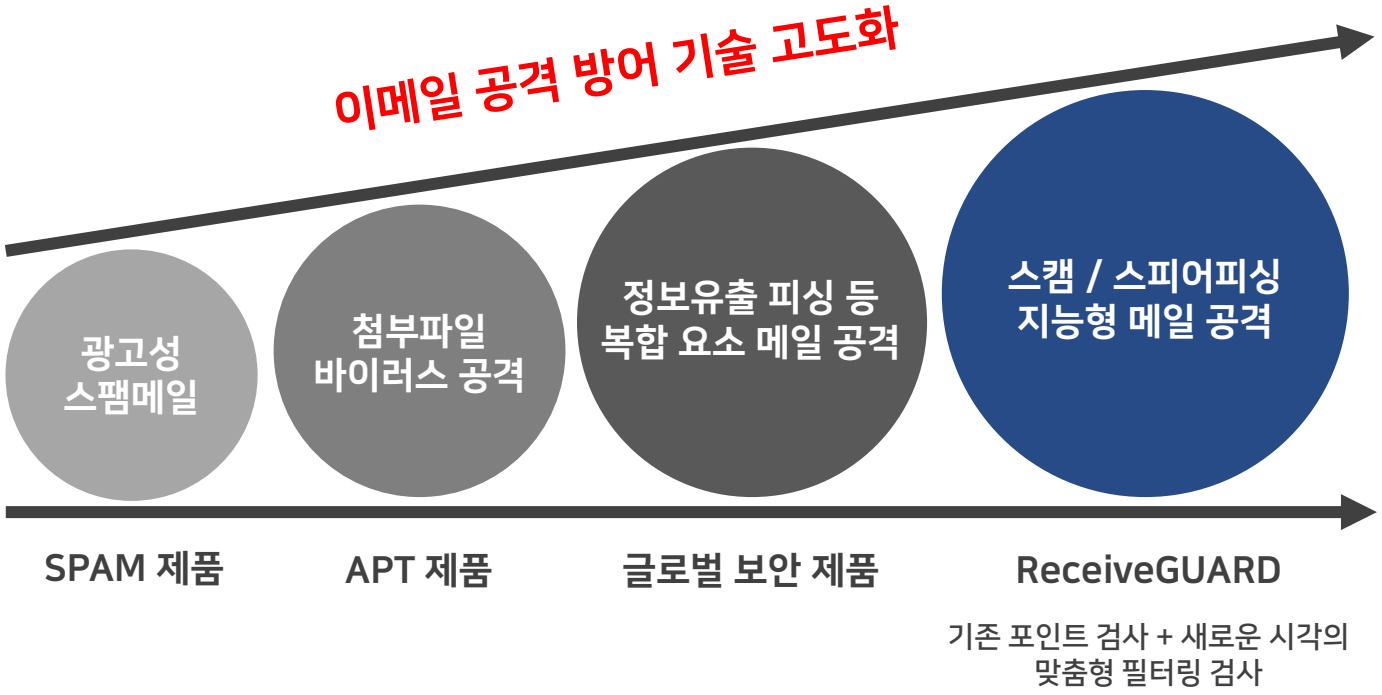
Case 4

회계사, 세무사 타깃 신종 이메일 피싱 사기

ⅰ. 세금보고 대행자 타깃 신종 이메일 피싱 사기 등장
ⅱ. 세금보고용 회사를 가장해 웹사이트 링크 걸린 이메일로
소프트웨어 업데이트 설치하게 유인
ⅲ. 개인정보, 금융정보를 의심 없이 유출하는 사고

| 03 | ReceiveGUARD

SPAM, APT에서 진화된 **맞춤형 필터링**으로 기존 글로벌 제품 **한계 극복!**



ReceiveGUARD는
기존 제품들이 검사하지 못하는 포인트까지 검사
차별화된 차세대 메일 보안 제품

기존 제품의 검사로는 진화된
사회 공학적 / 지능형 메일 공격에 **속수무책!**

| 03 | ReceiveGUARD

ReceiveGUARD는 과거 패턴 업데이트 방식의 사후 정적 분석 대응이 아닌,

발신자의 진위여부를 판단해 사회 공학적 해킹 공격에 유일하게 선제 대응 할 수 있는

Gartner에서 기술력을 인정한 e-mail 보안 **the only Solution**입니다

사기 메일 유일 대응 솔루션	AI와 메일 보안의 결합	랜섬웨어(신종 악성코드) 차단
		
APT공격 및 금융사기 등 BEC(Business e-mail Compromise) 공격에 세계 유일 선제 대응 가능한 기술 보유 국내 유일의 자체 개발 e-mail 엔진 및 서비스 노하우로 행위 기반 동적 필터링 시스템 보유	2017 가트너 IT 10대 트렌드인 AI와 보안기술의 융합! Receive GUARD가 선도! 머신 러닝을 통한 데이터 축적부터 신뢰도 프로그램을 적용, 위험 여부 스스로 판단	행위 기반 동적 분석을 통해 첨부파일의 위험성 판단, 신종 랜섬웨어 위험 사전 차단 기존 안티바이러스 제품의 단점인 패턴업데이트의 정적 분석 한계 극복

| 03 | ReceiveGUARD_APT/SPAM/리시브가드 비교

제품 기능 및 콘셉트 비교

APT

검사 방식
- 바이러스 패턴 검사
- 행위 기반 파일 검사

검사 범위
- 이메일 첨부 파일

SPAM

스팸 메일 차단

패턴 바이러스 차단

ReceiveGUARD

검사 방식
- 바이러스 패턴 검사
- 행위 기반 파일 검사
- 지능형 위험 메일 검사

검사 범위
- 이메일 첨부 파일
- 본문/첨부 문서 URL 링크 내 첨부 파일
- BEC 지능형 사기 메일

제품 구성에 따른 보안 범위

▶ SPAM + APT

스팸 공격 → 바이러스 / 랜섬웨어 공격 → 스캠 / 스피어피싱 지능형 메일 공격

▶ SPAM + 리시브가드

| 03 | ReceiveGUARD

세계 1위의 IT 연구 자문사 Gartner

Gartner는 세계 1위의 IT 연구자문사로 해외시장에 널리 알려져 있으며,
주요 비즈니스 언론사가 하루도 빠짐없이 인용할 정도로 그 **공신력**을 인정받고 있습니다.
Fortune 1000 기업의 **71%**, Global 500 기업의 **73%**가 Gartner로부터 자문을 받고 있습니다.

독립성과 객관성을 바탕으로 해외에서 인정받는 IT 연구 자문사

Gartner

26 April 2017

Kevin Kim
KIWONTECH
509 E&C Venture Dream Tower 5 Cha
53 Digital-ro 31
Guro-gu Seoul
08375 KOREA

Dear Mr Kevin Kim,

Please find enclosed a copy of the executed contract between your company and Gartner. The contract has been countersigned by Stuart Brown, an authorised signatory of Gartner. Please keep this contract as proof of the agreement between our two companies.

If you have any questions please feel free to contact your account manager or the undersigned on the details stated below.

Regards,

Contract Director, Corporate Law
Gartner
Level 6, 395 Collins Street
Melbourne, VIC 3000
www.gartner.com

2019-06

㈜ 기원테크

이메일 보안 국내 최초 'Market Guide'

아시아 지역을 대표하는 기업으로 선정!

2017-03

"ReceiveGUARD는 타 e-mail 보안 제품들의 약점이었던
Targeting 공격과 패턴화 되지 않은 해킹 공격들을
AI와 Machine learning을 통해 보완하는
반드시 필요한 혁신적인 차세대 e-mail 보안 제품"

IT보안인증사무국 CC인증 획득!

ReceiveGUARD는 보안 제품에 대한 국제공통평가기준을 만족하여
정부 및 공공기관이 정보보안 제품을 도입할 때 필수적으로 요구되는
CC인증(EAL2)을 획득하였습니다.

ReceiveGUARD V1.0
인증보고서

인증번호 : CISS-0874-2018

2018년 6월

IT보안인증사무국

ReceiveGUARD
이메일 보안의 새로운 기준

Chapter

II

제품 소개

| 01 | 주요 기능

악성 메일 원인 분석, **맞춤형 필터링 대응**

가상공간
- 메일 1건당 필요한 수만큼 VA 투입하여 실시간 메일 검사
- 최소 1,000개 이상의 VA 검사 대기 중
- 메일 속도 향상 및 검사의 정확도 확보
- URL 분석 및 위/변조 파일 분석, 바이러스 탐지, Malware 탐지

신뢰도 프로그램
- VA에서 분석하고 학습한 결과를 토대로 신뢰도 생성
- 수신하는 각 메일 마다 개별 신뢰도 구축
- 신뢰도를 바탕으로 위험성을 부여하여 사용자 전달 여부 결정

지능형 학습
- 차단된 메일을 사용자가 허용했을 경우 해당 메일 원문 전체 분석
- 원문 분석 시 각 예외 사항에 맞도록 자동으로 패턴 생성
- 패턴의 변조를 방지 하기 위해 유동 암호화 방식으로 보관

랜섬웨어 차단
- 기본 첨부파일에 대해 바이러스 및 Malware 검사 진행
- 본문에 링크된 URL을 VA에서 직접 열어본 후, 다운로드 가능한 파일이 있는 경우 VA에서 미리 다운로드 하여 위험성 검사
- Malware 검사 기능을 통해 파일 확장자가 변조된 악성코드 검출

실시간 URL 분석
- 본문에 링크가 연결되어 있는 주소는 VA 에서 미리 열어보고 악성코드 검사
- 본문에 링크 된 URL 확인 결과, 해당 사이트 내부에 추가 링크가 있다면 End-Point까지 추적, 추가 위험성 사전 차단

최초 발송 경로 추적
- 각 계정 별 최초 메일 발송 경로 정보 저장
- 메일 재 수신 시 저장된 경로와 비교
- 발송 경로 변경 시 경고 메시지 삽입

발신주소 위 · 변조 검사
- 메일 발신주소의 유효성을 체크하여 위,변조 검사
- 서버는 유효하나 별도로 발신자 주소의 위,변조 흔적 검출
- 스누핑 공격 예방

위험성 메일 IMAGE 변환
- 필터링 된 메일 전달 시, 위험성 메일 IMAGE 변환 기능
- 차단 메일 중에서 메일 내부에 URL 링크가 있는 경우 메일 내용 자체를 이미지로 변환시켜 전송
- 원문 재전송 요청 시 e-mail, 비밀번호 입력 후 계정 인증서버와 통신을 통해 확인 후 전송

유사 도메인 검사
- 기존 도메인과 유사성 비교 분석
- 위험 계정일 경우 비교 분석 후 경고 표시

| 01 | 주요 기능

악성 메일 원인 분석, **맞춤형 필터링 대응**

리포트 기능
- 관리자에게 리포트 설정 권한을 부여(보고서 제외 대상자 및 기능)
- 리포트 확인 후 별도 링크 접속 후 메일 차단 / 허용 설정
- 사용자에게 차단 내역 등에 대한 보고서 메일 발송
- 메일 관리 기능을 통해 수신 내역 조회, 메일 차단, 메일 허용 기능 제공

업무/광고 메일 구분 관리
- 메일 본문과 메일 헤더 등의 일정 패턴을 통해 메일 구분 관리
- 별도 통계를 통해 손쉬운 메일 관리

로드밸런싱
- 메일 서버 트래픽 상태 자체 확인 후 사용량을 분배해 전달
- 대용량 메일 수신 시 신속한 처리

위·변조 파일 분석
- PDF, HWP, DOC, PPT 등 자주 사용하는 문서 파일로 위장한 악성코드와 바이러스 프로그램 검출
- VA에서 미리 확인하고 위험성 차단

첨부문서 내 위험링크 검출
- 메일 내 첨부된 문서 본문을 분석해 링크 검출
- 링크의 위험성을 이미 누적된 신뢰도 데이터를 바탕으로 분석
- 자체 데이터가 누적될 수록 보다 명확한 검출 가능

메일 제목에 경고 문구 삽입
- 차단 메일 허용 시 [BLOCK] [WARNING] 등의 경고 문구 삽입 되어 사용자에게 전달
- 경고 문구 확인으로 메일의 안전성 확인
- 경고 문구는 관리자에 의해 변경 가능

아카이빙
- 관리자가 설정한 주기만큼 개인 백업 가능
- 실수로 삭제된 메일도 복원 가능
- Appliance 이지만, 웹 메일 시스템과 동일하게 보관 적용
- 정보와 파일을 분리 함으로 실제 메일 시스템과 동일한 원문 보관

개인 사용자 필터링 구축
- 메일 차단 시 개인 사용자에게 주기 별 보고서 발송
- 개인 사용자 전용 웹 페이지를 통해 데이터 관리
- 별도의 중앙 관리자가 없는 시스템 적용 가능
- 다양한 사용자의 검증으로 보다 명확한 필터링 확보

다양한 지원
- 연결된 메일 서버와 통신 체크가 가능한 웹 관리자 기능 제공
- RCPT 조회, 메일 전달 결과에 대한 로그 기록 조회 가능
- 전체 시스템 운영에 대한 실시간 정보 제공
- 내부 사설 망에 대한 유동 설정 제공

| 01 | 주요 기능

악성 메일 원인 분석, **맞춤형 필터링 대응**

행위 검출

- 첨부파일 직접 실행 시 PC에 위험 행위 감지
- 신종 악성코드(랜섬웨어) 탐지 가능
- 파일 실행 시 악성 행위 확인 가능한 관리자 UI 제공

첨부파일 확장자 차단

- 수신 거부할 첨부파일 확장자를 미리 등록
- 악성코드에 주로 사용되는 파일 확장자를 미리 등록해 차단

발신자 트래킹

- 실제 사용자가 맞는지 사전 1차 검증
- 통신 이력이 없는 메일이 전달될 경우 우선 수신 거부 후 인증 요청

악성 메일 리스트 연동 UI 제공

- 메일 서버 업체의 지원이 있는 경우 악성 메일함 등 임의의 메일함 생성 후 차단 메일 수신 페이지 별도 제공
- API 연동으로 차단 리포트 수신 여부와 상관 없이 언제나 편리하게 차단 메일 확인 가능

메일 열람 시 추가 URL 검사 제공

- 사용자의 PC에서 메일 본문에 URL 링크 클릭 시점마다 악성 URL 검사
- URL 검사 후 사용자에게 링크 연결 여부 알림 발송
- 추후 변질되는 악성 URL 실시간 검출 가능

SMS 알람 기능

- 장비 리소스 임계치 설정 값에 도달 시 알람 메일 관리자에게 문자 메시지 전송
- 기업에서 별도의 SMS 서버나 서비스 소유 시 지원

GDPR 정책 대응

- 관리자에게 GDPR 설정 권한을 부여(국가, 대상자)
- 유럽연합(EU) 정보 보호를 적용할 국가와 대상자의 상세 정보 관리
- 정보 보호 규정상 설정한 주기에 따라 자동으로 관련 데이터 삭제

외부 이미지 CID 변환

- 사용자 망 분리 환경 시, 링크에 연결된 이미지를 직접 다운 받은 후 본문에 이미지로 첨부해서 사용자에게 발송
- 인터넷 미지원 환경에서도 사용자는 이미지가 포함된 메일 확인 가능

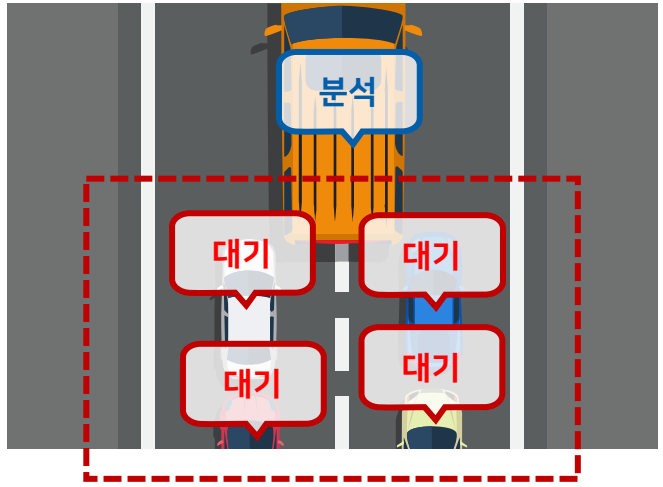
첨부파일 문서 미리보기

- 첨부파일이 문서일 경우 첫 페이지를 이미지로 변환하여 미리 보기 기능 제공
- 매크로 등 파일 자체 위험이 포함된 문서일 경우 관리자가 미리보기로 2차 안전성 여부 확인

| 02 | 상세 기능_가상 공간(VA)

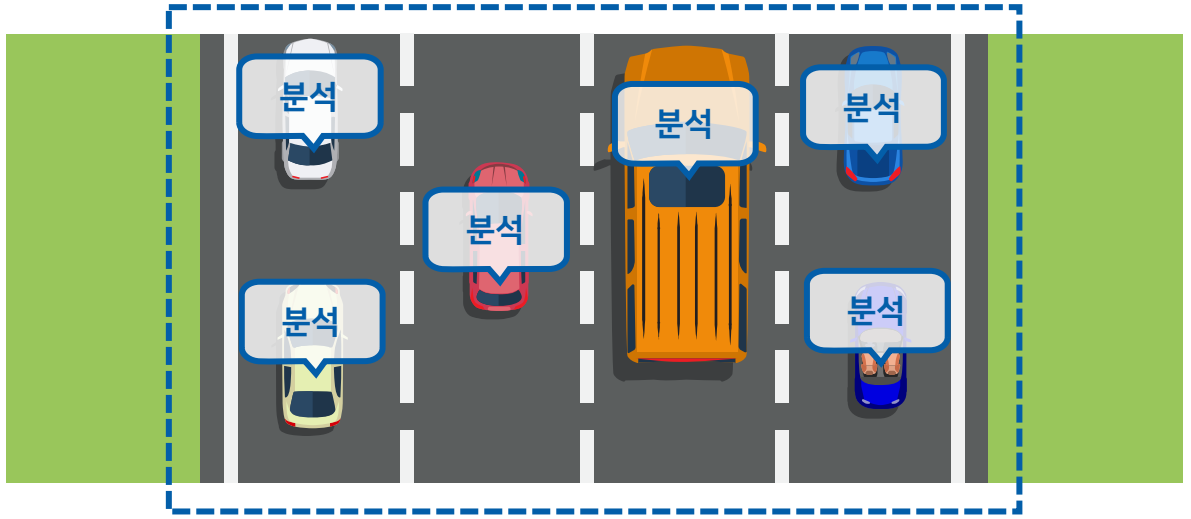
세계 유일의 **AI 메일분석 시스템 VA**

타 제품 분석 방식



고정형 리소스 사용

리시브가드 분석 방식



유동적 리소스 사용

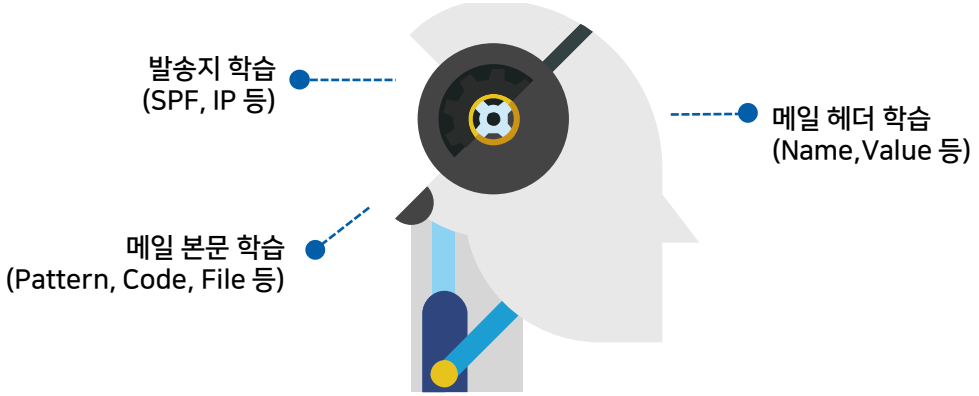
타 제품의 고정형 리소스 사용 메일 분석 방식에서 벗어난
유동적 리소스를 사용하는 분석 방식을 채택하여 빠르고 정확한 이메일 필터링 분석이 가능합니다.

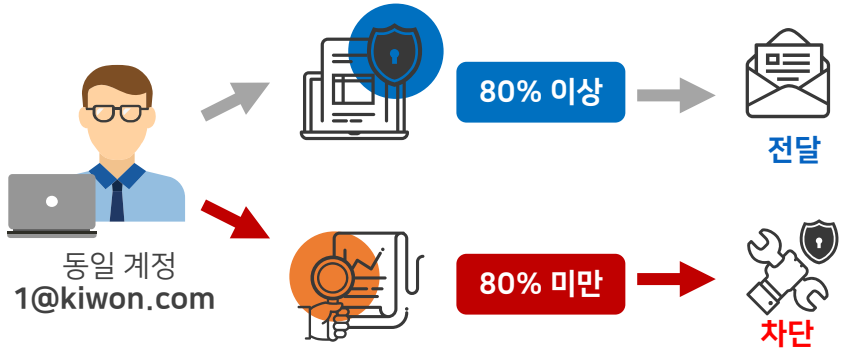
| 02 | 상세 기능_신뢰도(해커 발신 검출)

각 개인 사용자 **맞춤형 개별 학습 데이터 구축**

01 계정별 수신 메일 정보 분석 및 학습

02 학습 정보 이용, 수신 메일 신뢰도 적용





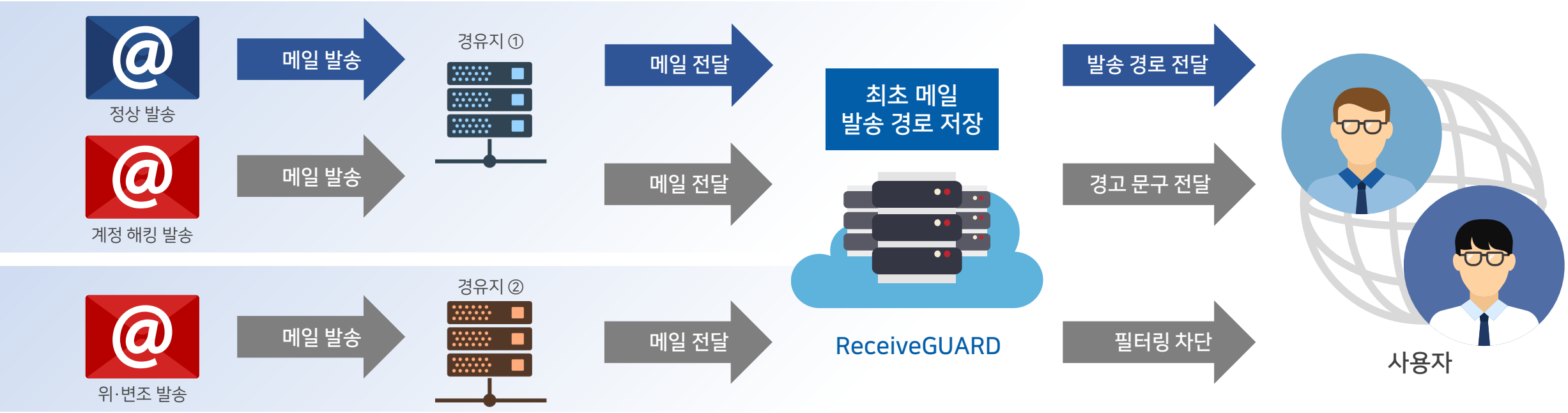
모든 수신 메일을 기원테크만의 노하우로 개발된 머신러닝 기술을 이용하여 학습합니다.

학습 기간 후 동일한 계정에서 발송한 메일에 대해 이미 학습한 데이터와 비교 / 분석하여 정상 여부를 판단합니다.

방대한 데이터는 인메모리 방식을 채택하여 정확하고 빠른 데이터 처리가 가능합니다.

| 02 | 상세 기능_발송 경로 추적

정상적인 경로가 아닌 **변경된 발송 경로 차단**



기존 메일이 발송되던 경로를 저장하였다가 발송 경로가 변경되어 메일이 수신되었을 경우 해당 메일을 차단하며,
사용자가 해당 메일을 수신한 경우 해당 메일의 변경된 발송 경로를 보여주게 되어 사용자에게 해당 메일에 대한 경각심을 심어주며,
수신자는 발신자에게 실제로 변경된 것이 맞는지 확인할 수 있습니다.

| 02 | 상세 기능_유사 도메인 검출

1@KIWONTECH.COM
대문자 i

1@KlWONTECH.COM
소문자 L

유사성 필터링(상·중·하) 사용자 경고 알림

[유사성-위험] 의심스러운 메일 주소와 메일을 주고 받았을 경우 경고 알림

[유사성-상] 1@KIWONTECH.com ->1@KlWONTECH.com (1개 검출)

[유사성-중] 1@KIWONTECH.com -> 1@KIW0NTECH.com (2개 검출)

[유사성-하] 1@KIWONTECH.com -> 1@KIW0MTECH.com (3개 검출)

정확한 판단을 위하여 개인별 DB화 색인 분석

사람의 시선으로 구분하기 힘든 유사한 도메인 검출

사람의 시선으로 구분하기 힘든 유사 도메인 검출

수신 받은 메일 주소 및 도메인(계정)에 대해 기업 및 개별 사용자 별로 데이터를 구축합니다.

추후에 수신 된 계정에 대해 유사성 검사를 실시하여, 사람의 시선으로 구분하기 힘든

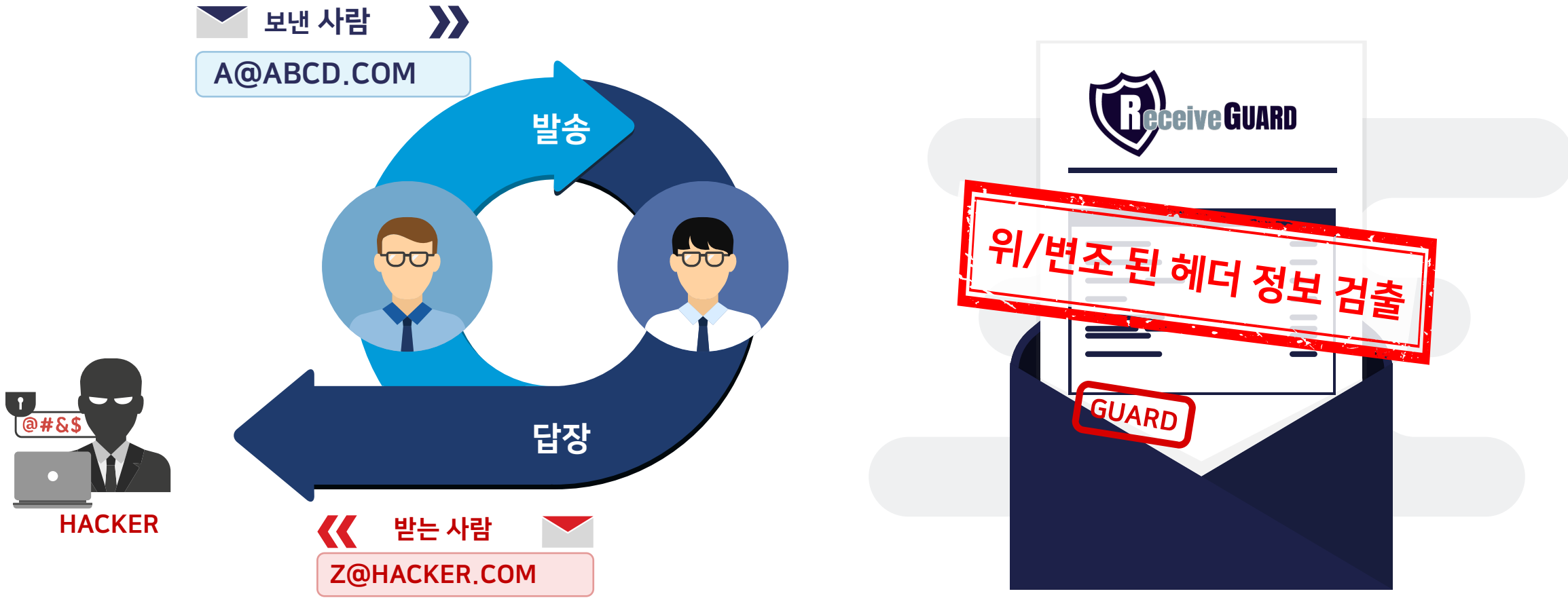
유사 주소가 발견되면, 사용자에게 경고 문구로 유사성이 검출됨을 알립니다.

유사성은 상, 중, 하,TLD(상위도메인)으로 나뉘며, 유사성 검출 계정과

사용자가 메일을 주고 받을 경우 보안담당자에게 긴급 경고를 알려 위험을 차단합니다.

| 02 | 상세 기능_헤더 위·변조

헤더를 변경해 **답장 받는 주소가 다른 메일을 검출**



| 02 | 상세 기능_본문 URL 검출/이미지화

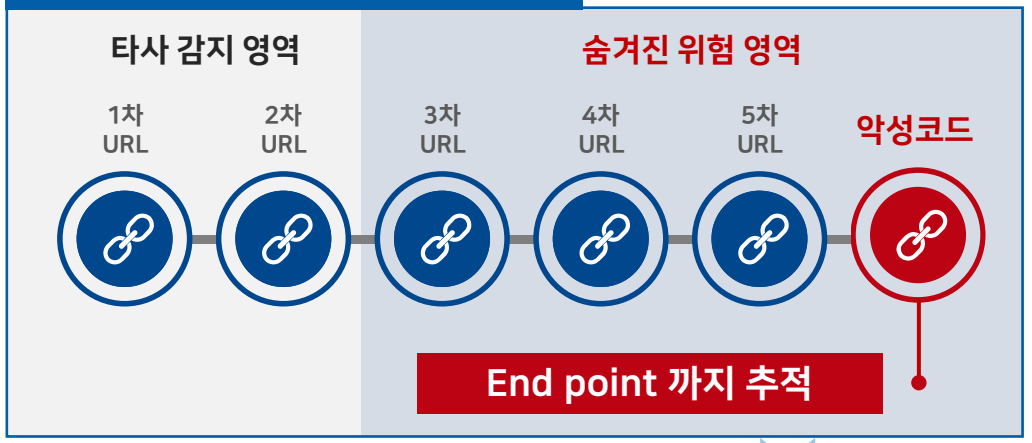
① 본문 악성 URL 첨부 메일 발송

보낸사람 김메일<test@abcd.com>

안녕하세요,
보내주신 메일을 잘 받았습니다.
아래 링크에서 자료 다운로드 받으세요.
감사합니다.

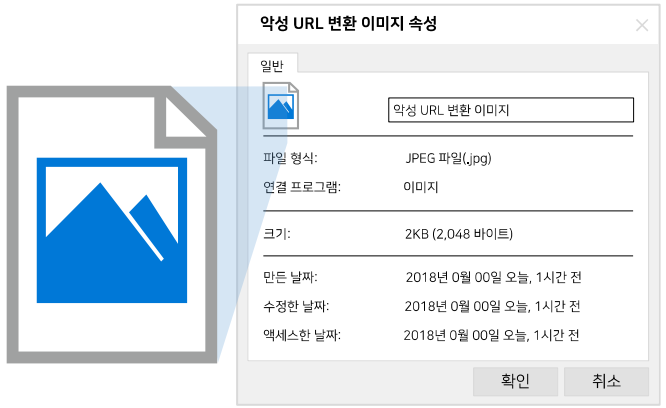
www. G*ogle.com/312334534

② 리시브가드 URL EndPoint 직접 검사



③ 악성코드 / 피싱사이트 검출

④ 사용자에게 안전하게 이미지로 변환해서 전달

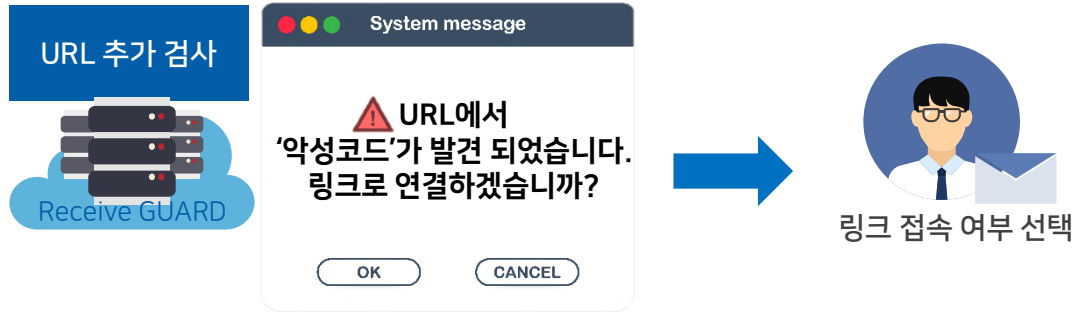


| 02 | 상세 기능_메일 열람 시 추가 URL 검사 제공

실시간 URL 추가 검사를 통한 악성 URL 대응

① 사용자 URL 링크 클릭 시 추가 검사

② URL 검사 결과 제공



1차 검사 결과 정상으로 필터링 된 URL은 내부에 저장 후 사용자의 URL 클릭 시점에 악성 URL로 활성화되는 경우를 대비하여 추가 검사를 실시합니다.

이후 사용자에게 URL 검사 결과창을 제공, 사용자가 URL 링크 접속 여부를 선택합니다.

| 02 | 상세 기능_신종 랜섬웨어 검출

한번의 검사가 아닌 **각각 다른 방식의 검사로 사용자 PC 감염 대응**

첨부파일에 악성코드 파일, 랜섬웨어 등의 파일이 첨부된 메일의 경우 1차적으로 백신에서 검출해 내고,
검출되지 않은 첨부파일에서 신종 악성 파일의 가능성이 있기 때문에 2차도 Windows 환경에서 첨부파일의 행위를 분석합니다.
해당 첨부파일이 PC의 특정 폴더 안에 강제적으로 설치 된다거나, 혹은 시스템을 변경하려는 시도가 감지되면 메일 서버에 도착하기 이전에 차단하여
한 번의 검사가 아닌 각각 다른 방식의 검사가 이루어져 사용자의 PC감염에 안정적으로 대응할 수 있습니다.

| 03 | 통계 리포트_필터링/장비

ReceiveGUARD 현황

그룹 ▾ | 도메인 ▾ | 1일 ▾ | 2018-04-16 | 2018-04-16 | 적용

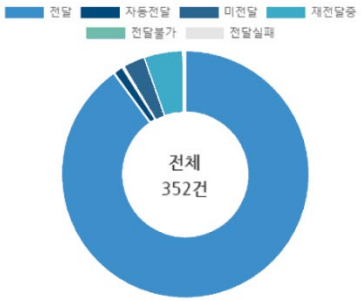
보고서 인쇄하기

▸ 운영 현황

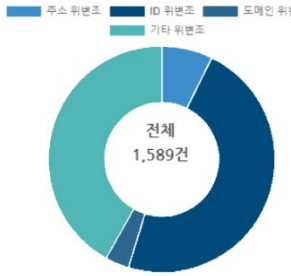
일자	전체	정상메일		위험메일				변조메일		
		정상	신뢰도(정상)	업무성	광고성	악성메일	랜섬웨어	헤더 위변조	발송지 위험	유사 도메인
2018-4-16	351	184	83	20	47	0	1	7	10	1

▸ 전달 현황

전체	352 건
전달	333 건
자동전달	0 건
미전달	18 건
재전달중	0 건
전달불가	0 건
전달실패	1 건

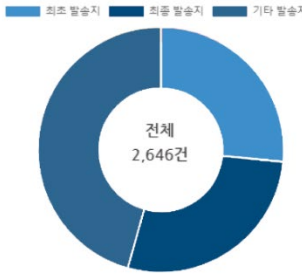


▸ 헤더 위변조 현황



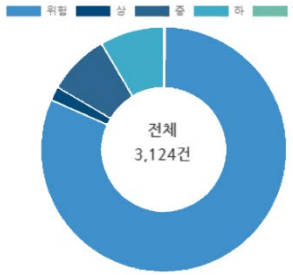
전체	주소 위변조	ID 위변조	도메인 위변조	기타 위변조
1,589 건	116 건	754 건	54 건	665 건

▸ 발송지 위험 현황



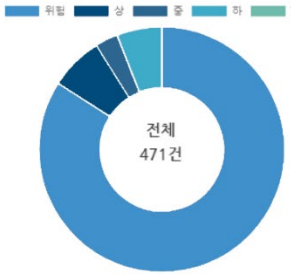
전체	최초 발송지	최종 발송지	기타 발송지
2,646 건	703 건	735 건	1,208 건

▸ 유사 도메인 (전체대상) 현황



전체	위험	상	중	하	TLD
3,124 건	6 건	2,544 건	58 건	252 건	264 건

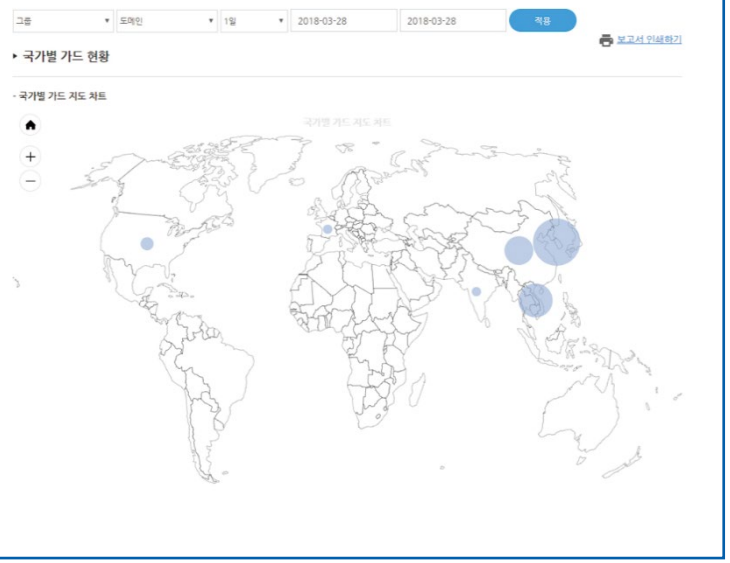
▸ 유사 도메인 (개인대상) 현황



전체	위험	상	중	하	TLD
471 건	0 건	396 건	33 건	14 건	28 건

| 03 | 통계 리포트_국가/계정별

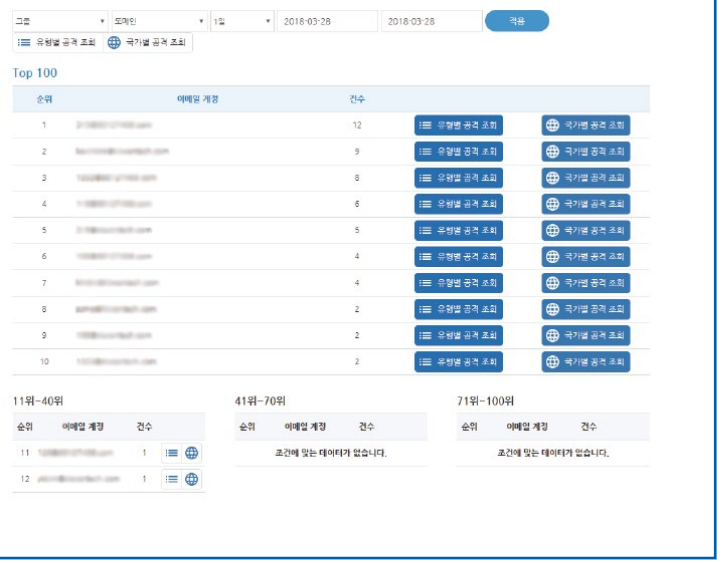
국가별 가드 현황



국가별 가드 현황표

국가명	위험메일				변조메일				총계
	업무성	광고성	악성메일	랜섬웨어	헤더 위변조	발송지 위험	유사도메인 (전체)	유사도메인 (개인)	
아랍에미리트	1	1	0	0	0	0	0	0	2
안티가바부다	0	3	0	0	0	0	0	0	3
아르메니아	1	0	1	0	0	1	0	0	3
아르헨티나	0	9	0	0	0	1	0	0	10
오스트리아	0	4	0	0	0	1	0	0	5
호주	1	1	0	0	0	0	0	0	2
아제르바이잔	0	0	0	1	0	1	1	0	2
방글라데시	4	6	0	11	5	0	0	0	15
벨기에	1	1	0	0	0	1	0	0	3
불가리아	1	2	0	0	3	1	1	0	8
브라질	3	46	0	1	2	5	0	0	56

계정별 공격 현황

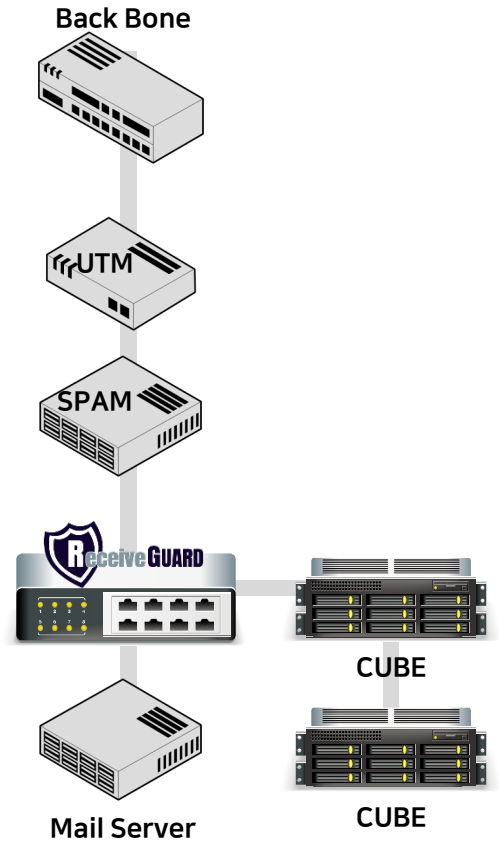


필터링 통계자료 제공

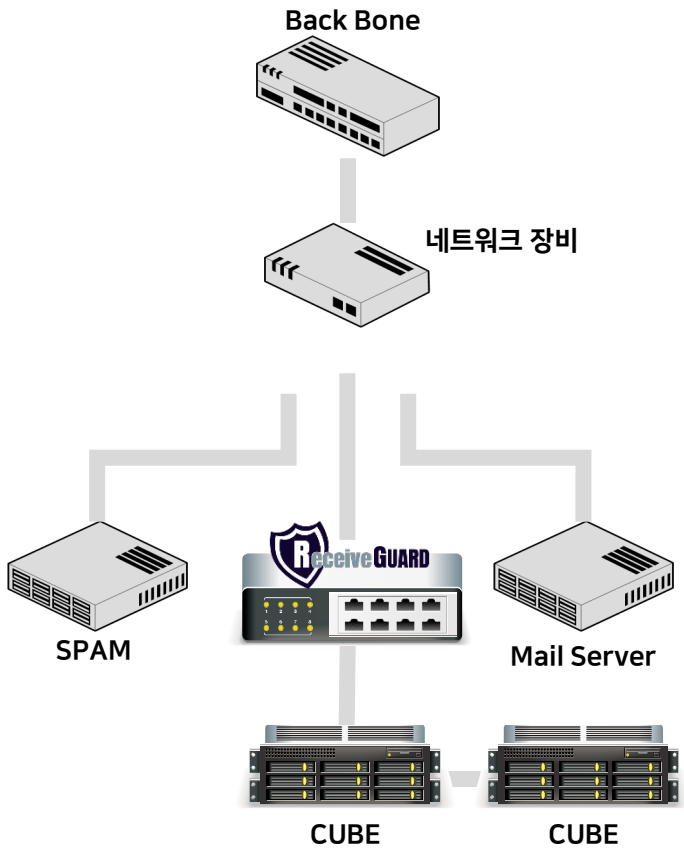
- 기간 설정하여 통계 데이터 검색 가능
- 각 필터링 별 통계 결과 조회
- 장비 상태 히스토리 검색 및 원 클릭 인쇄 기능 제공

| 04 | 네트워크 구성_ReceiveGUARD

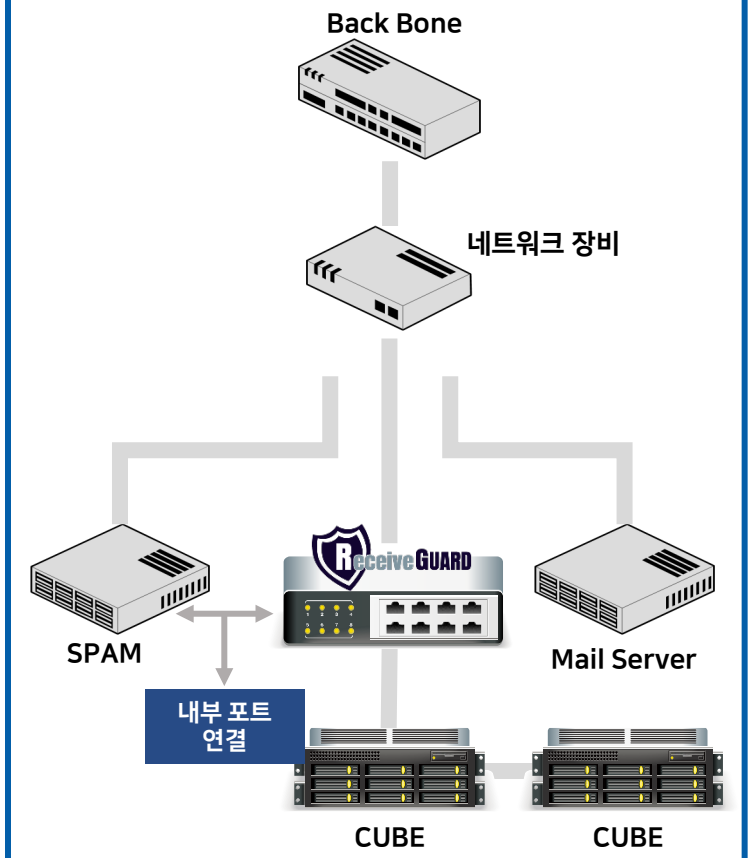
기본 구성



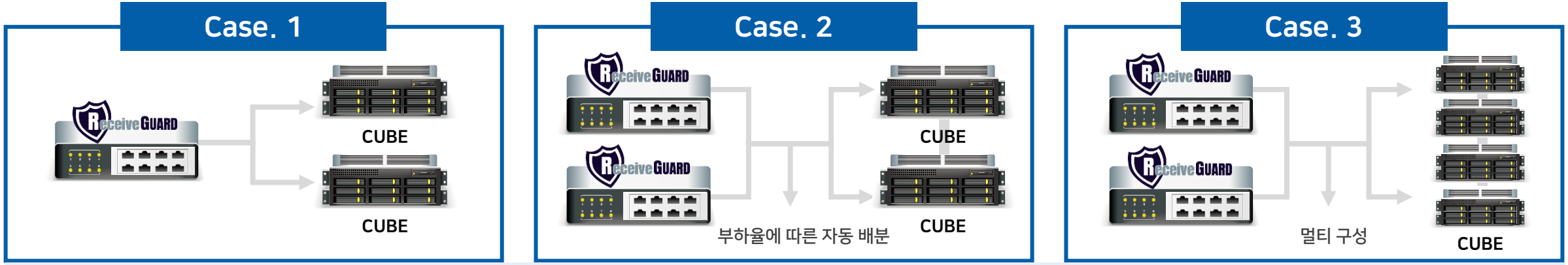
프록시 방식



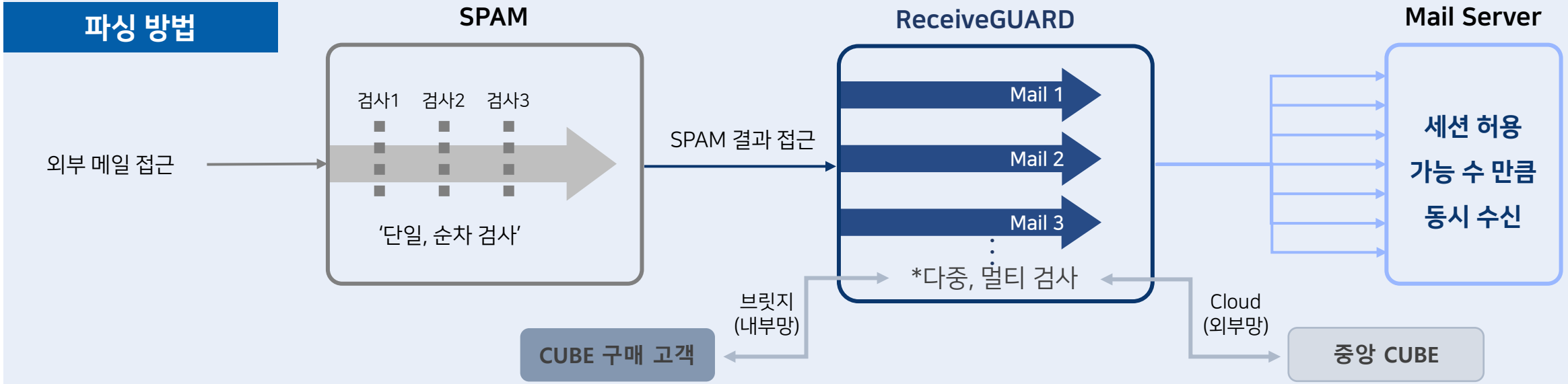
브릿지 방식



| 04 | 네트워크 구성_CUBE



파싱 방법



ReceiveGUARD
이메일 보안의 새로운 기준

Chapter

III

사업 진행 현황

| 01 | 해외 사업 현황

세계가 선택한 이메일 보안 제품,
ReceiveGUARD!

싱가포르, 베트남, 일본 등
IDC 및 콜센터 운영!

글로벌 보안 데이터 구축!

| 02 | 국내·외 고객 현황

고객과 함께 이메일 보안의 새로운 기준을 만들어갑니다.

대기업

LG화학 | HYUNDAI HEAVY INDUSTRIES CO.,LTD. | Hyundai Oilbank | 현대E&T | 현대오일터미널 | HYUNDAI and SHELL Base Oil | 현대케미칼 | 현대오씨아이

제조업

NEXEN 주식회사 넥센 | HWASEUNG 화승R&A | SAMGONG | (주)동원테크 DONGWON TECHNOLOGY CO.,LTD | 한국알콜산업 | SHKI (주)신기인터모빌 | DINTEC | for a better future KEP

신성델타테크(주) SHINSUNG DELTATECH CO., LTD. | SL Corporation | COSMO OIL | CIDO | PHARMA RESEARCH PRODUCTS | 주식회사세동 | S-TECH | 서울기계공업주식회사 SEOUL MACHINERY CO., LTD.

연구기관(공공)

NFRI 국가핵융합연구소 National Fusion Research Institute | 한국여성정책연구원 Korean Women's Development Institute | KRICT 한국화학연구원 | KERI 한국전기연구원

협회·금융·제약

울산테크노파크 Ulsan Technopark | BR 보령제약 | 아주저축은행 | KMA 대한의사협회 Korean Medical Association | JEIL 제일약품

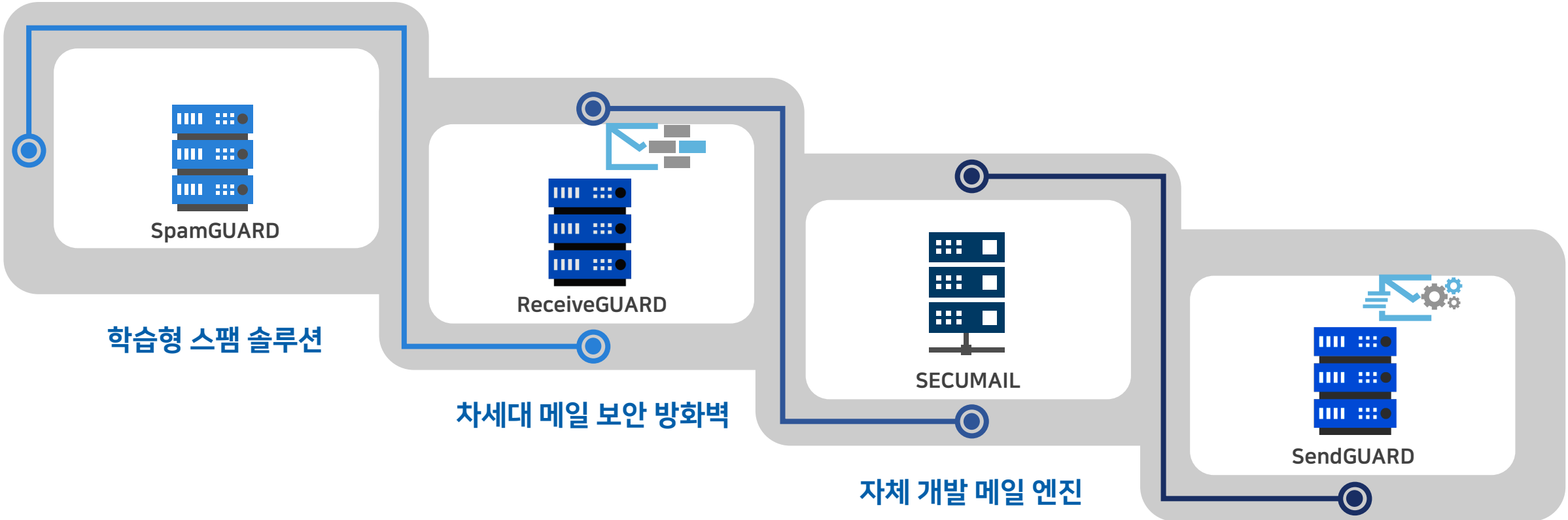
해외 기업 (베트남·싱가폴 · 오만 · 일본)

Quân đội nhân dân | TÀI NGUYÊN & MÔI TRƯỜNG | グッドット株式会社 Goodot Inc. | ASUKADESIGN | 株式会社タナカカメ TANAKA KAME CO.,LTD. | MARVELHOUSE Singapore International Preschool | TOYOTA HUẾ | FProfessionals

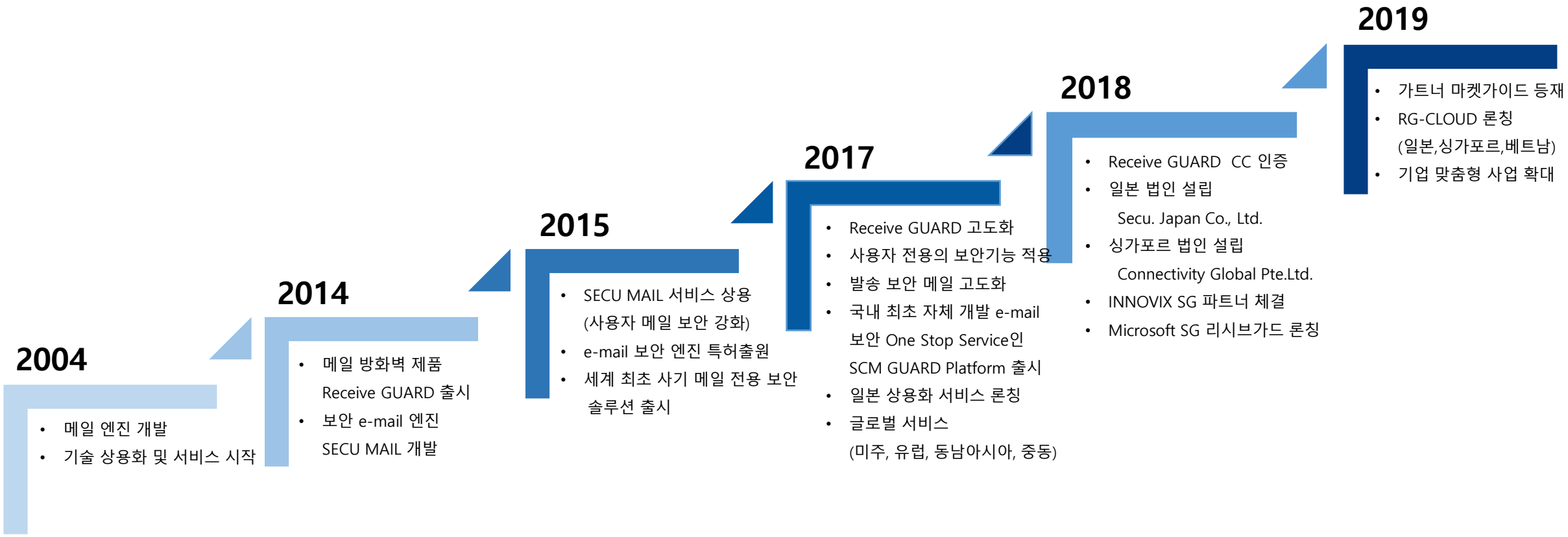
Directize Directize Consulting Group | Fannel.COM | ASCA Design | 株式会社LSIメディエンス | ネットパーク21 | Fahasa.com | GILIMEX

| 03 | EG-Platform

이메일의 처음부터 끝까지! 국내 유일의 자체 개발 **e-mail, One Stop Service**



자체 **이메일 엔진 보유** 기업이 만든 이메일 전용 보안 솔루션!!



| 04 | 기업 소개

KIWONTECH

기 업 명	주식회사 기원테크
주 소	서울시 구로구 디지털로31길 53 E&C 5차 509호
대표이사	김동철
설 립 일	1994년 최초 설립
홈페이지	www.kiwontech.com
대표전화	T)02-6012-7406 / F)02-6085-4330
운영 IDC	서울시 양천구 목동로 233-5 KT ICC

ReceiveGUARD

감 사 합 니 다

From the Beginning to the End of Mail Service
One stop Mail Platform with AI

(주)삼에스소프트

㈜삼에스소프트는 KIWONTECH 의 베스트 파트너입니다.

경기도 수원시 영통구 창룡대로 256번길 91, 에이스광교타워 2차 909호
대표전화 : 031 - 212 - 3390 I 팩스 : 031 - 212 - 3345
㈜삼에스소프트 기술영업팀 (010 – 3576 – 9186 / sales@3es.co.kr)
http://www.3es.co.kr