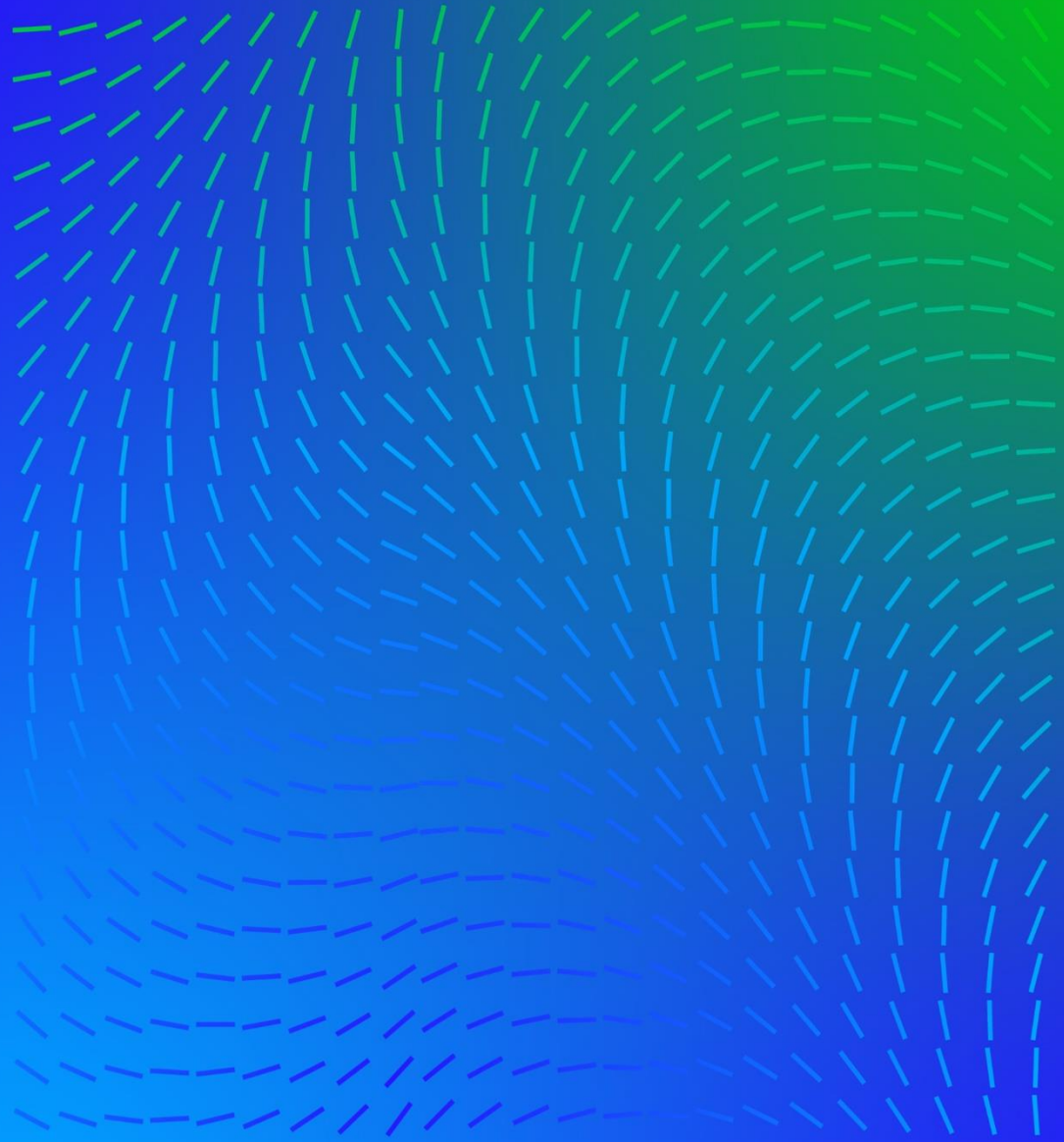
Trellix

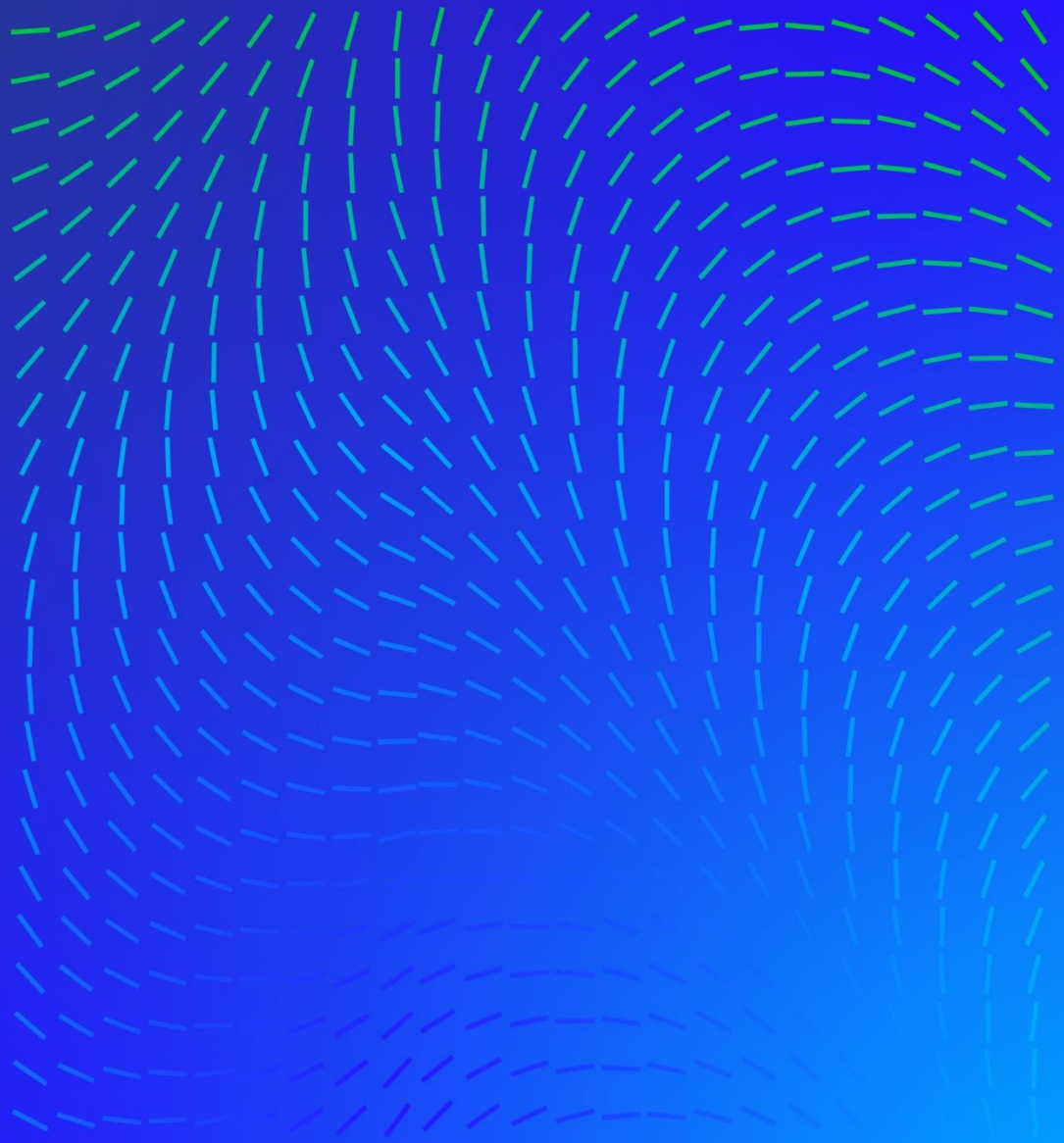
악성메일의 공격 유형과 대응방안

Advanced protection for
the #1 threat vector

위수영 상무

Sep 2023, 삼성동 코엑스





There is no such thing as a safe email

Trellix

이메일은 여전히 최고의 공격 루트

주요 공격 경로

91%

이메일로부터 시작되는
사이버 공격의 비율 *

MS만으로는 충분하지 않음

3M

1058개 고객사에서 1년간
Microsoft가 탐지한 공격 건수 **

클라우드 이메일 도입

70%

클라우드 이메일 솔루션을
사용하는 조직의 비율 및
증가 추세

평균 침해 수명 주기

277 Days

비즈니스 이메일 침해로 인한
결과

* Trellix Advance Research Center
**Gartner Market Guide for email security
***Knowbe4.com Nov 29, 2022
****IBM Cost of a Data Breach Report 2022

공격자는 왜 이메일을 좋아할까?

단순한
보안구조

다수의
개인정보유출

저조한
인증체계
사용률

가장 중요한
업무 수단

공격단계
단순화

Target
지정가능

위 변조 용이

다양한 형태의
공격유형 전달

Trellix

It only takes ONE email...

KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Phish Leads to Breach at Calif. State Controller

March 23, 2021 35 Comments

A phish
Office (
phisher
time to
targete

AEROSPACE AND DEFENSE MAY 25, 2016 / 2:15 AM / UPDATED 7 YEARS AGO

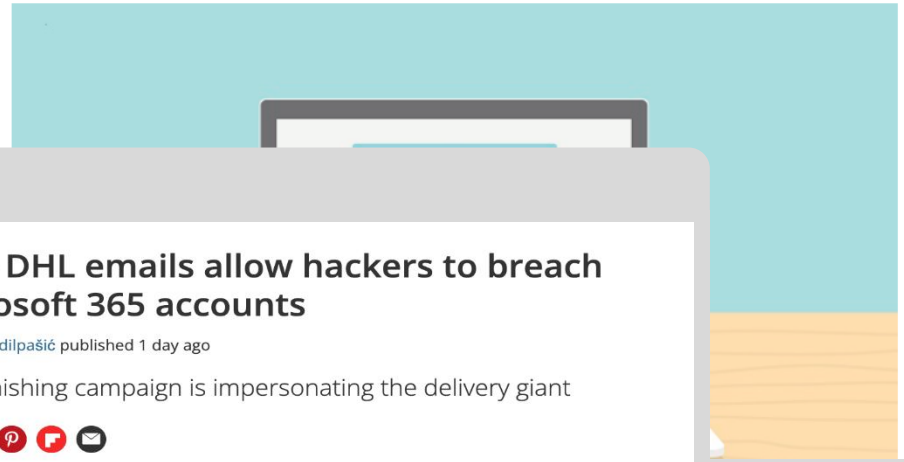
Austria's FACC, hit by cyber fraud, fires CEO

By Reuters Staff 2 MIN READ

VIENNA (Reuters) - The head of Austrian aerospace parts maker FACC has been fired after the company was hit by a cyber fraud that cost it 42 million euros ($47 million).

42,000 Records Breached in Cancer Treatment Center Phishing Hack

A Cancer Treatment Centers of America employee fell victim to a targeted phishing email in May, providing the hacker with their network credentials.



Fake DHL emails allow hackers to breach Microsoft 365 accounts

By Sead Fadilpašić published 1 day ago

New phishing campaign is impersonating the delivery giant

Trellix

Trellix 공격 통계 DATA

12:1

악성 이메일 하나당
12개의 악성 URL이
발견됩니다.

1:7

악성 이메일 7개당
1개의 악성
첨부파일이 있습니다.

>25%

감지된 파일 유형은
MS Office
문서입니다.

10%

이메일 전송 후
악성으로 활성화된
비율 입니다.

Trellix

이메일 공격 대응 기본 이해

- Email을 통한 공격에도 유형 및 종류가 있다.
- Email 공격의 유형 및 종류 별 공격 형태 및 수단은 다양하고, 진화하고 있다.
- 변화하는 공격 유형 / 공격 형태 및 수단에 대응에 얼마나 빠르게 대응할 것인가?

Trellix

이메일 공격 분류

악성첨부

악성링크

Email APT

피싱메일

BEC
(Business Email Compromise)

Email SPAM

EAC
(Email Account Compromise)

신뢰할 수 있는
서비스
제공업체

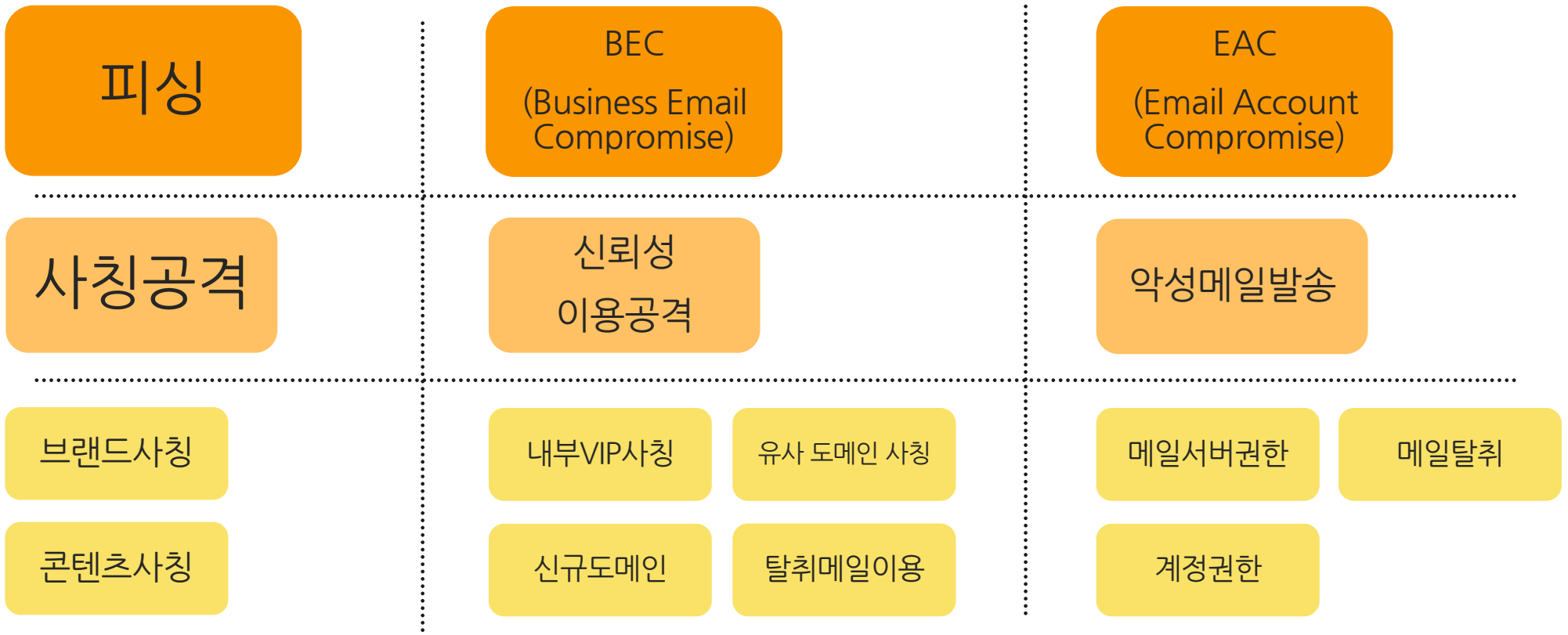
Email
APT/SPAM

Trellix

이메일 공격 분류(악성메일)

Trellix

이메일 공격 분류(피싱 / BEC / EAC)



Trellix

이메일 공격 대응 방안

* SPF : Sender Policy Framework

* DKIM : Domain Keys Identified Mail

Trellix

Trellix Email Security

Email Security -

Cloud

Email Security -

Server

Trellix

Flexible Deployment Options
Cloud Email

Scan/Block

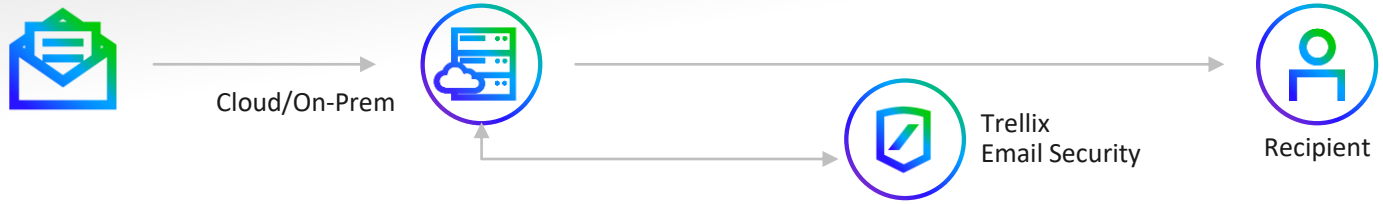
1. **Primary SEG with Full Hygiene.**

Scan/Block

2. **Full Hygiene inline, second hop, behind a 3rd party SEG.**

Scan/Drop

3. **Full Hygiene in BCC mode and sends alerts.**

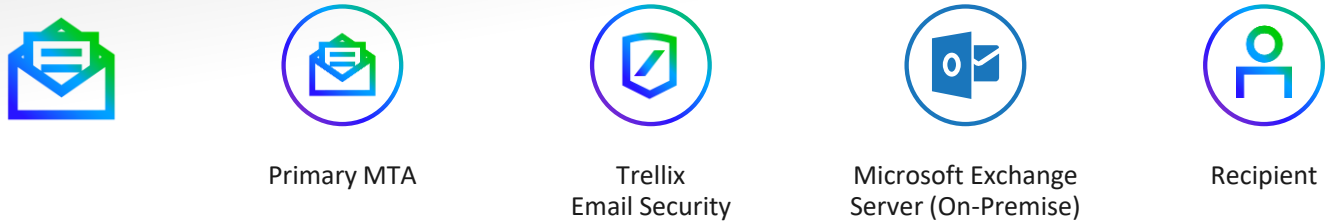


4. **MS365/Google Workspace Native API Integration**

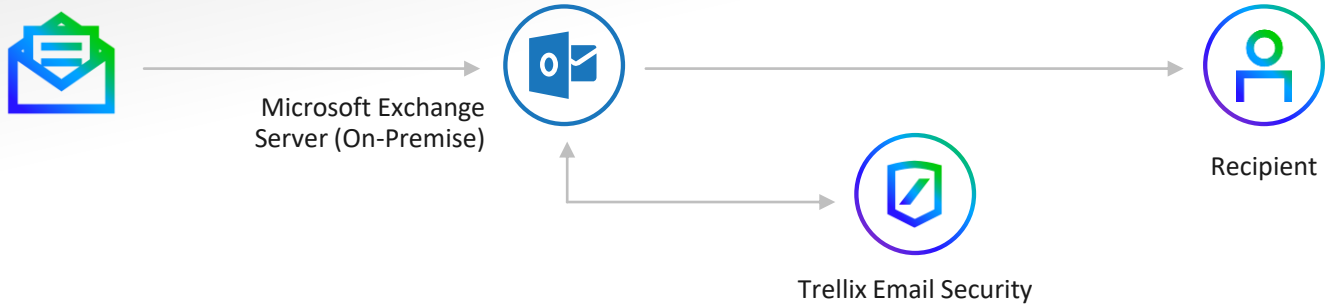
Google Workspace Microsoft 365

Flexible Deployment Options
Server Email

1. **On prem Inline mode**



2. **On prem in BCC/Monitor modes**



3. **Appliance deployments (Form factors)**

Trellix

기존 고객분들 / 신규 솔루션 검토 고객분들 다시 한번 자세한 설명을 들어보세요.

다 같은 이메일 보안 솔루션이 아닙니다.

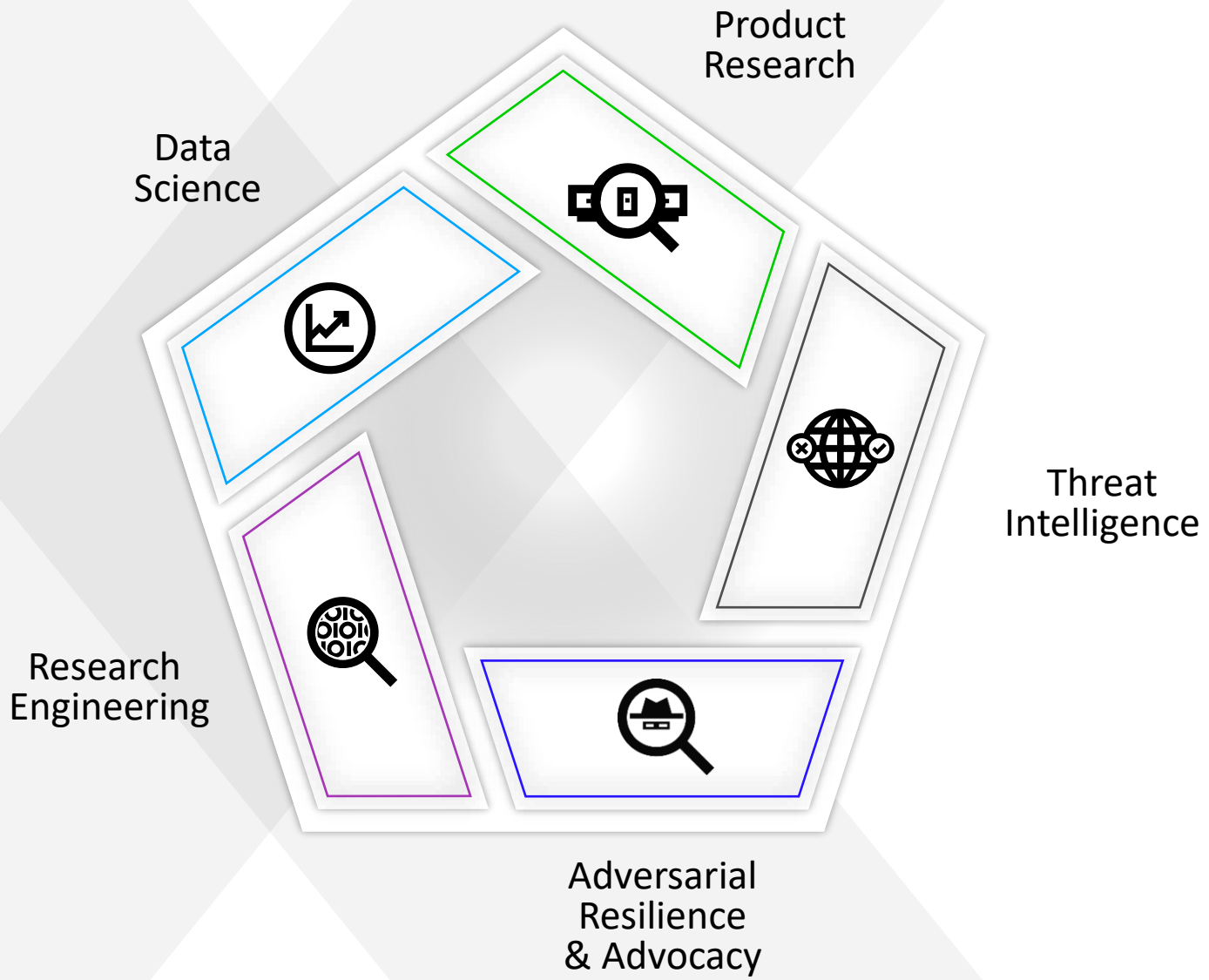
이메일 위협의 유형과 고객사 환경에 맞는 최적의 솔루션을 제안 드리겠습니다.

미팅 요청 : korea@trellix.com

Trellix

Advanced Research Center

Trellix는
고객과 함께
진화합니다.



Trellix

Thank You

Trellix