

# proofpoint.

# 이메일보안 소개

Jun 30, 2023 - V1.0 : Jun 30, 2023



S.Pin Technology | 솔루션 사업실 [Cloud.solution@spintech.co.kr](mailto:Cloud.solution@spintech.co.kr)



# proofpoint.

# Agenda

- 01 - 배경 및 목적
- 02 - 주요위협 및 문제점
- 03 - proofpoint를 통한 해결방안
- 04 - 제품의 특징점
- 05 - 성공사례
- 06 - 기대효과 / TCO
- 07 - 구축방안 및 지원사항

# proofpoint.

# 01

## 배경 및 목적



# 01

## Enterprise DX환경에서 가장 걱정되는 부분은

보안



비용

가버넌스

리소스

컴플라이언스

```
function(e, t, n) {
  var r, i = 0,
      a = e.length,
      o = n(e);
  if (o) {
    for (; o > 1; i++)
      if (r = t.apply(e[i], n), r === !1) break;
  } else if (o) {
    for (i in e)
      if (r = t.apply(e[i], n), r === !1) break;
  } else if (o) {
    for (; o > i; i++)
      if (r = t.call(e[i], i, e[i]), r === !1) break;
  } else {
    for (i in e)
      if (r = t.call(e[i], i, e[i]), r === !1) break;
  }
  return e;
}

function(e, t) {
  var n = t || {};
  return null != e ? "" : b.call(e);
}

function(e) {
  return null != e ? "" : (e + "").replace(C, "");
}

function(e, t) {
  var n = t || {};
  return null != e && (Object(e)) ? x.merge(n, "string" == typeof e ? [e] : b.call(n, e)), n : n;
}

function(e, t, n) {
  var r, i = 0,
      a = e.length,
      o = n(e);
  if (o) {
    for (; o > 1; i++)
      if (r = t.apply(e[i], n), r === !1) break;
  } else if (o) {
    for (i in e)
      if (r = t.apply(e[i], n), r === !1) break;
  } else if (o) {
    for (; o > i; i++)
      if (r = t.call(e[i], i, e[i]), r === !1) break;
  } else {
    for (i in e)
      if (r = t.call(e[i], i, e[i]), r === !1) break;
  }
  return e;
}
```



\* Flexera, '2020 스테이트 오브 클라우드 리포트

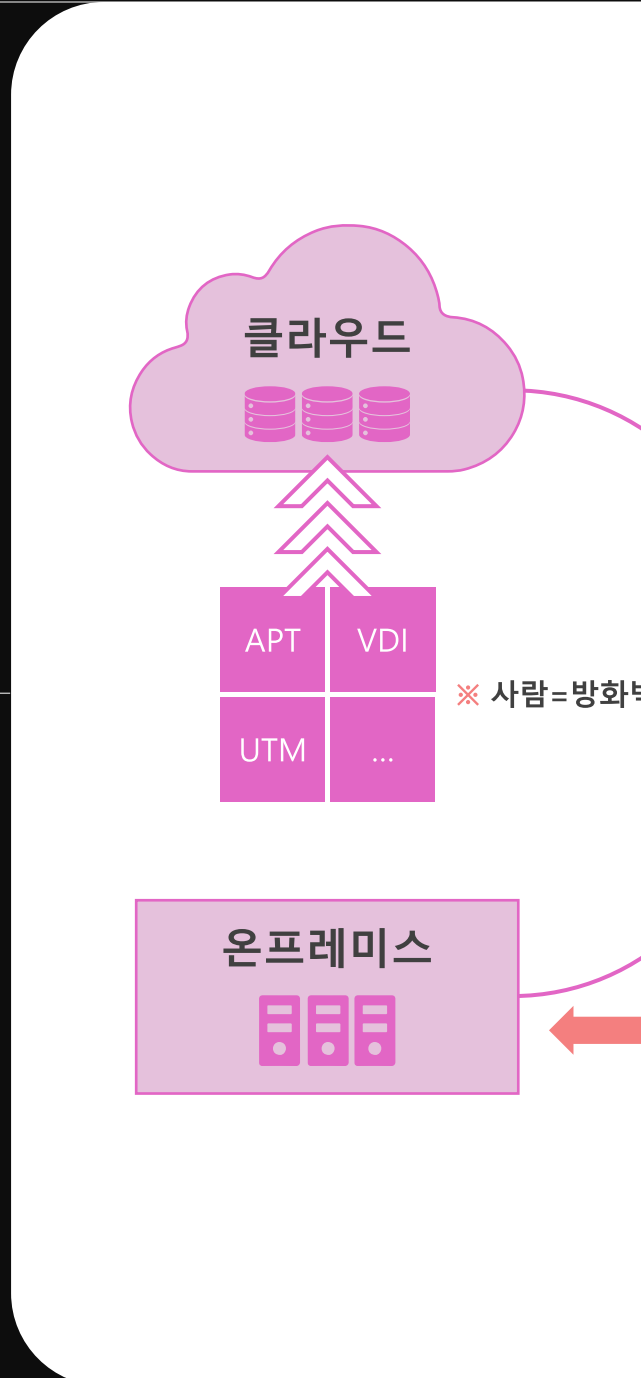




# 01

## 네트워크, 인프라 보안은 많은 투자 그러나,

인프라 네트워크 보안에만 집중 투자 해왔음.



해커들의 공격대상은

# 이미 사람을 타겟

이메일/랜섬웨어/ 잠복형/피싱/...



\* Flexera, '2020 스테이트 오브 클라우드 리포트



# 01

## 해결 되어야 할 사람을 통한 사이버 위협

### ※ 대표 위협

- 44%	가장 큰 손실	BEC
- 90%	이메일을 통한	랜섬웨어
- 85%	인적요소와 관련	데이터침해

## 우리 조직의 사이버 보안 위협 점검 필요성

피해사례

- 기프트 카드 사기
- 급여 전환
- 공급업체 송장 사기
- 거래처 계좌 변경 메일 사기
- 퇴사자 메일 도용 정보 유출
- 고객센터 안내 위장 메일
- 지인 사칭 악성코드 첨부 메일

?

점검 포인트

- BEC 변형의 조직 경험 있는지?
- 위험한 공급자가 누구인지?
- 솔루션은 다단계 랜섬웨어 차단?
- 클라우드 계정 및 앱(Office365) 보안이 안전?
- 현재 이메일 보안공급자가 교차공격 방어?
- 피싱 사용자를 어떻게 식별 & 치료?
- 발견된 위협과 손실을 대처하는 프로세스가 있는가?

\* Flexera, '2020 스테이트 오브 클라우드 리포트

# proofpoint.

02

## 주요위협 및 문제점



# 02

## 직면한 사이버 위협 즉시대응 필요

이메일

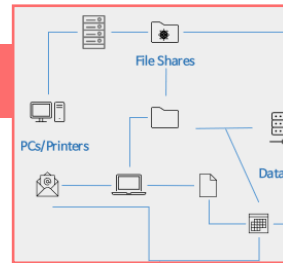
BEC

랜섬웨어

User Activity (ITM)



## 고급위협대응 이메일Gateway



기업IT시스템

고도로 표적화&사람에 집중

대부분의 사이버보안위협은 이메일에서 시작





## 02

# 직면한 사이버 위협 즉시대응 필요

이메일

BEC

랜섬웨어

User Activity (ITM)

## BEC 공격메일

전자 메일을 사용하여 상대방이 금전을 보내거나 기밀 회사 정보를 누설하도록 유도하는 사이버 범죄

### ★ [긴급요청] 결제 계좌 변경 및 대금 지급 요청

보낸사람 : 김프로 대리 <kpro@proofpoint.com>

받는낸사람 : 최프로 <cpro@proofpoint.com>

잘 지내시는지요?

다름이 아니라 저희 회계부서로부터 **긴급하게 요청** 받아서 메일 드립니다.

저희 쪽 세금 신고 문제로 인해서

금번 대금 지급을 아래 **계좌로 변경**하여 진행 부탁드립니다.

그리고 저희가 긴급히 세금 신고 마감 처리를 해야해서,

가급적 대금지급을 오늘 중으로 처리 부탁드립니다.

ABC Bank : 123-456-789999



# 02

## 직면한 사이버 위협 즉시대응 필요

- 이메일
- BEC**
- 랜섬웨어
- User Activity (ITM)





# 02

## 직면한 사이버 위협 즉시대응 필요

이메일

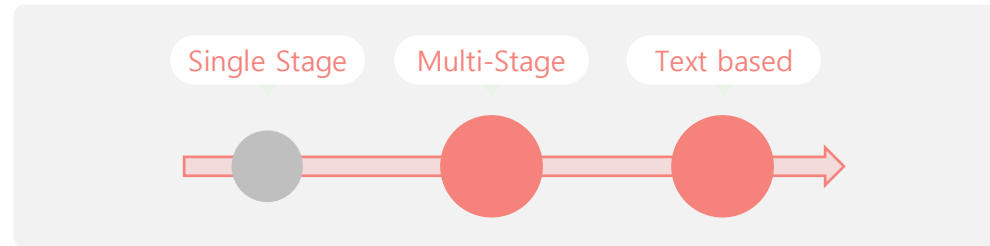
BEC

랜섬웨어

User Activity (ITM)

# 랜섬웨어

파일 암호화 및 시스템 접근 제한 후 금전 보상 요구하는 악성 소프트웨어 (멀웨어)의 일종



# 90%

이상이 이메일을 통해 감염



# 02

## 직면한 사이버 위협 즉시대응 필요

이메일

BEC

랜섬웨어

User Activity (ITM)

### Very Attacked People

확인해본 실제 기업의 상황

#### Very Attacked People

You have 289 VAPs that are over 2.7x more attacked than the average person in your organization.

SHOW CHART

Rows per page: 20 1-20 of 289

Person	Attack Index	Breakdown by Threat Family		
		0k	2k	4k
1 Alexander Harris Director of Marketing Commu...	4,333	[Bar chart showing breakdown of threats]		
2 William Lewis Senior Product Manager	4,325	[Bar chart showing breakdown of threats]		
3 Daniel Walker QA Engineer	4,198	[Bar chart showing breakdown of threats]		
4 Aria Moore Director of Engineering	3,745	[Bar chart showing breakdown of threats]		
5 Jacob Scott Director of Finance	3,453	[Bar chart showing breakdown of threats]		
6 Harper Martinez Senior Corporate Counsel	3,355	[Bar chart showing breakdown of threats]		
7 Noah Brown Junior Sales Engineer	3,334	[Bar chart showing breakdown of threats]		
8 Michael Brown Senior QA Engineer	3,330	[Bar chart showing breakdown of threats]		

- MalSpam
- Consumer Credential Phishing
- Credential Phishing
- Malware
- Corporate Credential Phishing
- Impostor
- Backdoor



## 02

# 직면한 사이버 위협 즉시대응 필요

이메일

BEC

랜섬웨어

User Activity (ITM)

## BEC와 랜섬웨어



동시에  
방어할 수 있는  
솔루션은?

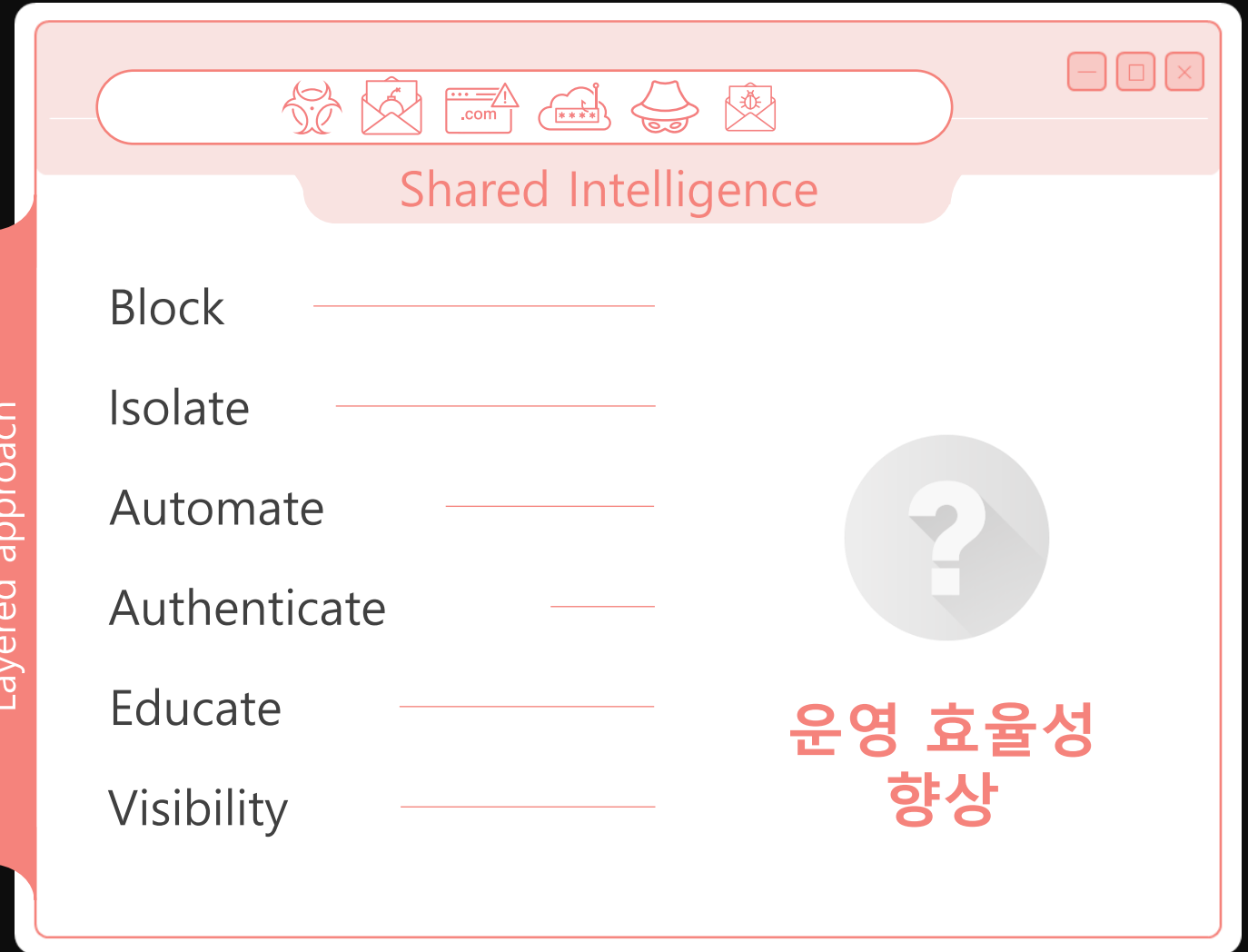


# 02

## 직면한 사이버 위협 즉시대응 필요

점점 많아지고 위중해지는 CISO & 보안 운영 관리자의 미션

Layered approach





# proofpoint.

03

# Email Protection - Powerful Email Gateway

---



# 03 Proofpoint 이메일 보안 제품 Line-up

BEC까지 방어할 수 있는 유일 솔루션

## 이메일 GW(PPS/POD)

## 샌드박스(TAP)

## 이메일 위협 사후 대응(TRAP)

### 이메일 보안 기능

- SPAM
- Anti-Virus
- Email Firewall

### 이메일 사기(BEC) 탐지 - Supernova

- 심층 헤더 분석
- 송/수신자 관계 분석
- 송신자 평판 분석
- 메일 메시지 구문 분석

### 이메일 인증

- SPF, DKIM, DMARC

### 이메일 Tagging

- 메일에 다양한 경고를 태깅하여 수신자에게 알림

### Cloud 샌드박스

- URL Defense : 메일 내의 URL 주소를 재설정 하여 추후 해당 URL이 악성으로 변경되어도 실시간으로 검사 및 탐지
- Attachment Defense : 메일 첨부파일에 대한 행위 분석 수행

### VAP(Very Attacked People) 리스트

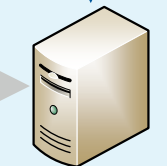
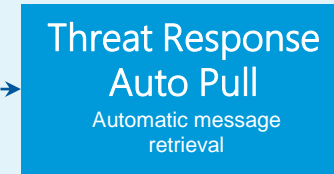
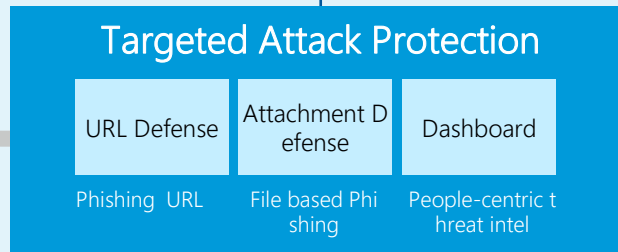
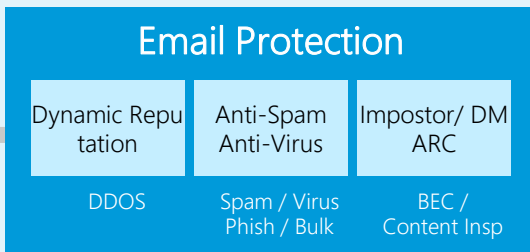
- 위험에 노출된 사용자에게 대한 가시성 제공

### mSoar

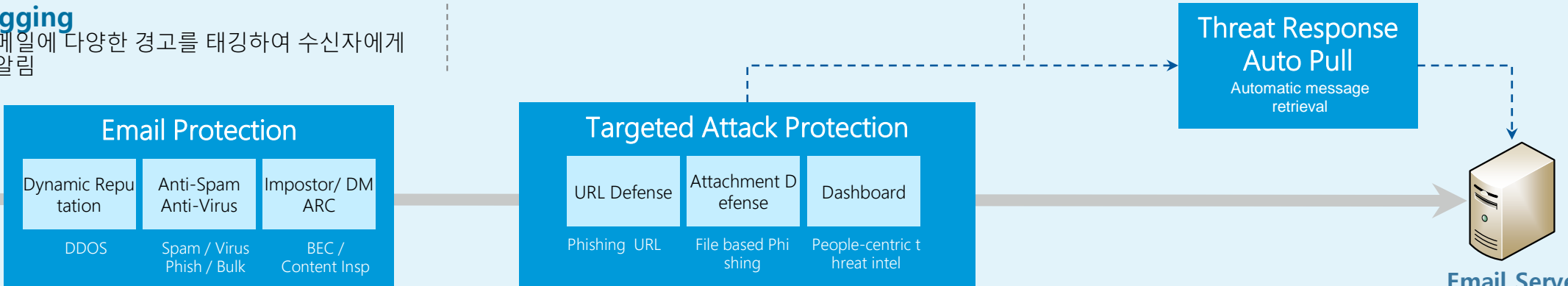
- 이메일 전달 후 악성으로 확인된 메일을 Mailbox에서 자동 격리

### CLEAR

- 악성 의심 메일에 대한 최종 사용자 보고 기능 제공 및 보안 대응을 간소화



Email Server



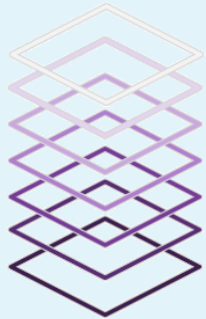


# 03 Proofpoint 이메일 보안 제품 Line-up

BEC까지 방어할 수 있는 유일 솔루션

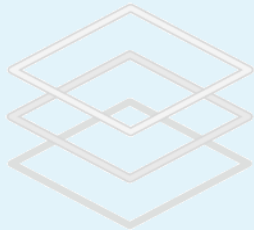
## 악성 URL 탐지

### Proofpoint URL Defense



- Reputation Analysis
- Predictive Sandbox Engine
- Static Analysis
- Dynamic Analysis (URLs & files)
- ML Feedback Loop
- Automated Expert Systems
- Browser Isolation

### Microsoft Safe Links



- Reputation Analysis
- Static File Analysis
- Dynamic File Analysis

## 악성 첨부파일 탐지

### Proofpoint Attachment Defense



- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection
- Evasion Detection
- URL Extraction
- Network & Protocol Analytics
- Ecosystem Partnerships
- ML Feedback Loop
- Automated Expert Systems

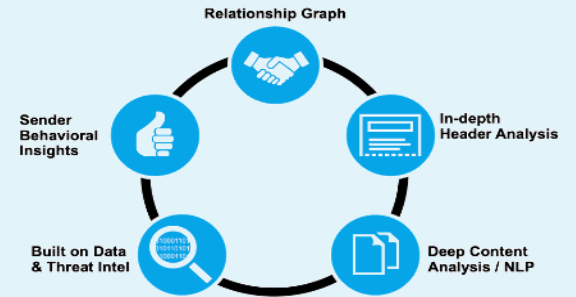
### Microsoft Safe Attachments



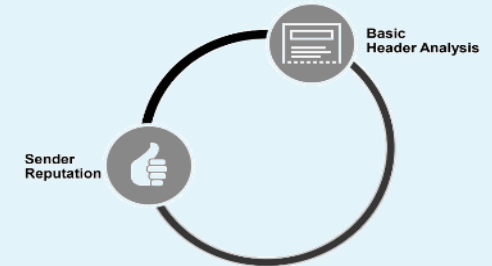
- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection

## 이메일 사기 탐지

### Proofpoint Supernova

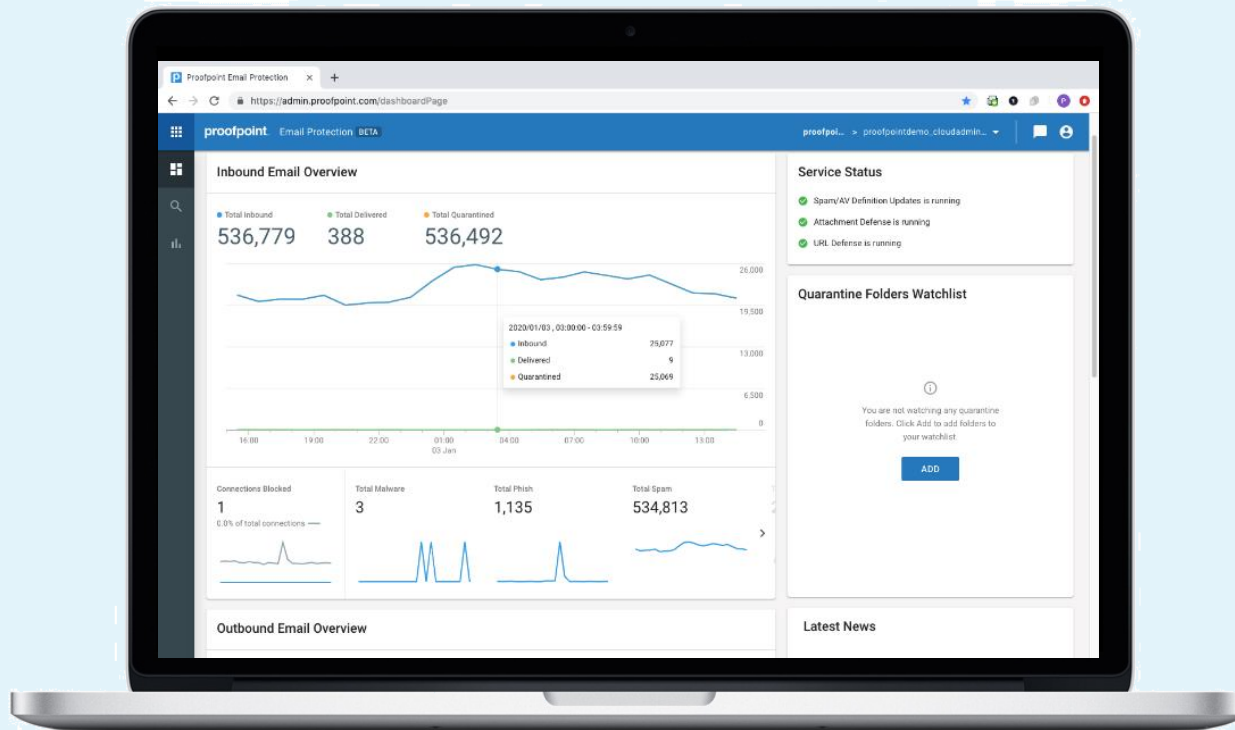


### Microsoft Spoof Intelligence





## 03 Proofpoint Email Protection



- 뛰어난 이메일 보안 효과 제공
  - Email 방화벽 정책
  - Anti-Spam
  - Anti-Virus
- 탐지하기 어려운 BEC 위협 탐지
  - Supernova 인텔리전스 (40억/1day, 1.5조/1year 메일 분석 빅데이터 및 머신러닝)
  - SPF, DKIM, DMARC 인증
- 빠른 이메일 추적과 위협 예방으로 생산성 향상
- 일반 사용자의 보안 인식 향상
  - 이메일 Tagging

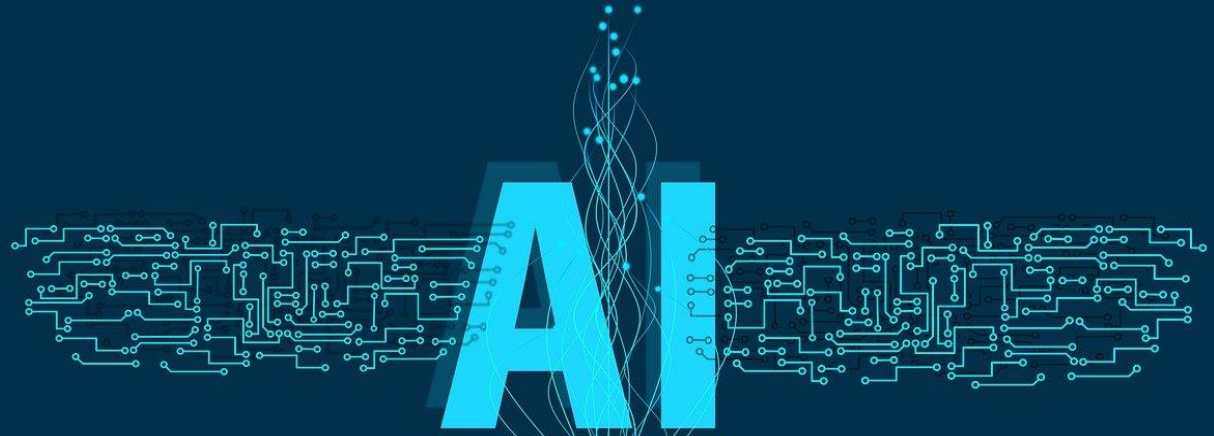


## 03 AI 엔진, Supernova

*"20년 이상의 머신러닝 기술을 활용한 이메일 인텔리전스"*

실시간 고급위협 인텔리전스 제공

- ✔ 심층헤더분석
- ✔ 송신자/수신자 관계분석
- ✔ 송신자분석
- ✔ 메시지 구문 분석
- ✔ BEC 라벨링



전세계 모든 신종 위협에 대한 인지





## 03 Proofpoint Email Protection

### Supernova - BEC 위협방어

From: Accounts Receivable accounts@manufacturer.ext

Reply-to: manufacturer@dr.com

x-originating-IP: 193.567.xxx.xxx

To: Accounts Payable

Subject: Urgent payment

The following invoices are due or will be due in April and we haven't received payment from your side. Could you please help arrange the payment? See the updated bank account info below.

Thank you

BANK NAME: STANDARD CHARTERED BANK

SWIFT: SCBLXHXXX

BENEFICIARY NAME: SHENN TRADE LIMITED

ACCOUNT NO.:57431130576

Total amount due: USD 2,511,789.92

Inv	Amount (USD)	Due date
INV11234	180,000.23	Mar 10, 2020
INV11235	13,528.07	Mar 19, 2020



#### 송신자 평판

송신자의 평판을 확인 한 결과, 그 결과는 정상으로 확인 되었습니다.



#### 심층헤더분석#1

송신자의 주소와 Reply-to 주소의 일치성 여부를 판단 한 결과 일치 하지 않았으며 따라서 BEC의 신호로 판단 하였습니다.



#### 심층헤더분석#2

이메일을 보낼때 송신자의 IP는 x-originating-IP 헤더에 포함이 됩니다. 해당 IP는 기존에 송신자가 보낸 국가가 아니기에 BEC의 신호라고 판단 하였습니다.



#### 메세지 구문 분석

본문에 긴급함을 요구, 금적인 것을 요구하는 것이 포함이 되었으며, 계좌 정보가 가 포함이 되어 있어 BEC의 신호라고 판단 하였습니다.





## 03 Proofpoint Email Protection

### 이메일 경고 태그

Rule ID	Language	Title	Body
dmarcfail	Korean (한국어)	이 메시지에주의하십시오	발신자의 신원을 확인할 수 없으며 누군가가 발신자를 가장하고있을 수 있습니다.
domainage	Korean (한국어)	이 메시지에주의하십시오	발신자의 이메일 도메인이 짧은 기간 동안 활성화되어 안전하지 않을 수 있습니다.
homoglyph	Korean (한국어)	이 메시지에주의하십시오	이 메시지는 가짜 웹 사이트에 대한 링크가 포함되어있을 수 있습니다.
impostor	Korean (한국어)	이 메시지에주의하십시오	보낸 사람이 사기꾼 일 수 있습니다.
inbound	Korean (한국어)	이 메시지는 외부 발신자가 보낸 것입니다	이 메시지는 조직 외부에서 전송되었습니다.
unknownsender	Korean (한국어)	이 메시지는 신뢰할 수 없는 보낸 사람이 보낸 것입니다	이전에이 발신자와 연락 한 적이 없습니다.
unsafe	Korean (한국어)	이 메시지는 안전하지 않을 수 있습니다	오프라인에서 보낸 사람과 확인하고 민감한 정보로 등장하거나 링크를 클릭하거나 첨부 파일을 다운로드하지 마십시오.

#### Settings

Rule ID

Title

Body

[Reset to Defaults](#)

[Show Details](#)

← You replied to this message on 15/07/2019, 09:32. [Show Reply](#)

**Be Careful With This Message**

This message contains links that may be impersonating another domain.

[REPORT SUSPICIOUS](#)

**amazon** Refund Notification

Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: [\[redacted\]](#)

- 최종 사용자가 좀 더 정보에 입각한 결정을 내릴 수 있도록 하여 잠재적인 침해 위험 완화
- 사용자가 경고 태그에서 바로 조치를 취할 수 있도록 함
- BEC 및 EAC 공격 전략에 맞서 보호
  - 이메일 스푸핑
  - 유사 도메인
  - 자격 증명 피싱
- 위험 요소에 관한 간략한 설명 제공



## 03 Proofpoint Email Protection

### 이메일 경고 태그

Rule ID	Language	Title	Body
dmarcfail	Korean (한국어)	이 메시지에주의하십시오	발신자의 신원을 확인할 수 없으며 누군가가 발신자를 가장하고있을 수 있습니다.
domainage	Korean (한국어)	이 메시지에주의하십시오	발신자의 이메일 도메인이 짧은 기간 동안 활성화되어 안전하지 않을 수 있습니다.
homoglyph	Korean (한국어)	이 메시지에주의하십시오	이 메시지에는 가짜 웹 사이트에 대한 링크가 포함되어있을 수 있습니다.
impostor	Korean (한국어)	이 메시지에주의하십시오	보낸 사람이 사기꾼 일 수 있습니다.
inbound	Korean (한국어)	이 메시지는 외부 발신자가 보낸 것입니다	이 메시지는 조직 외부에서 전송되었습니다.
unknownsender	Korean (한국어)	이 메시지는 신뢰할 수 없는 보낸 사람이 보낸 것입니다	이전에이 발신자와 연락 한 적이 없습니다.
unsafe	Korean (한국어)	이 메시지는 안전하지 않을 수 있습니다	오프라인에서 보낸 사람과 확인하고 민감한 정보로 등장하거나 링크를 클릭하거나 첨부 파일을 다운로드하지 마십시오.

#### Settings

Rule ID

Title

Body

[Reset to Defaults](#)

[Show Details](#)

← You replied to this message on 15/07/2019, 09:32. [Show Reply](#)

**Be Careful With This Message**

This message contains links that may be impersonating another domain.

[REPORT SUSPICIOUS](#)

**amazon** Refund Notification

Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: [\[redacted\]](#)

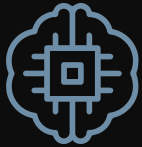
- 최종 사용자가 좀 더 정보에 입각한 결정을 내릴 수 있도록 하여 잠재적인 침해 위험 완화
- 사용자가 경고 태그에서 바로 조치를 취할 수 있도록 함
- BEC 및 EAC 공격 전략에 맞서 보호
  - 이메일 스푸핑
  - 유사 도메인
  - 자격 증명 피싱
- 위험 요소에 관한 간략한 설명 제공

# proofpoint.

04

# Targeted Attack Protection

Advanced Threat Protection and Visibility

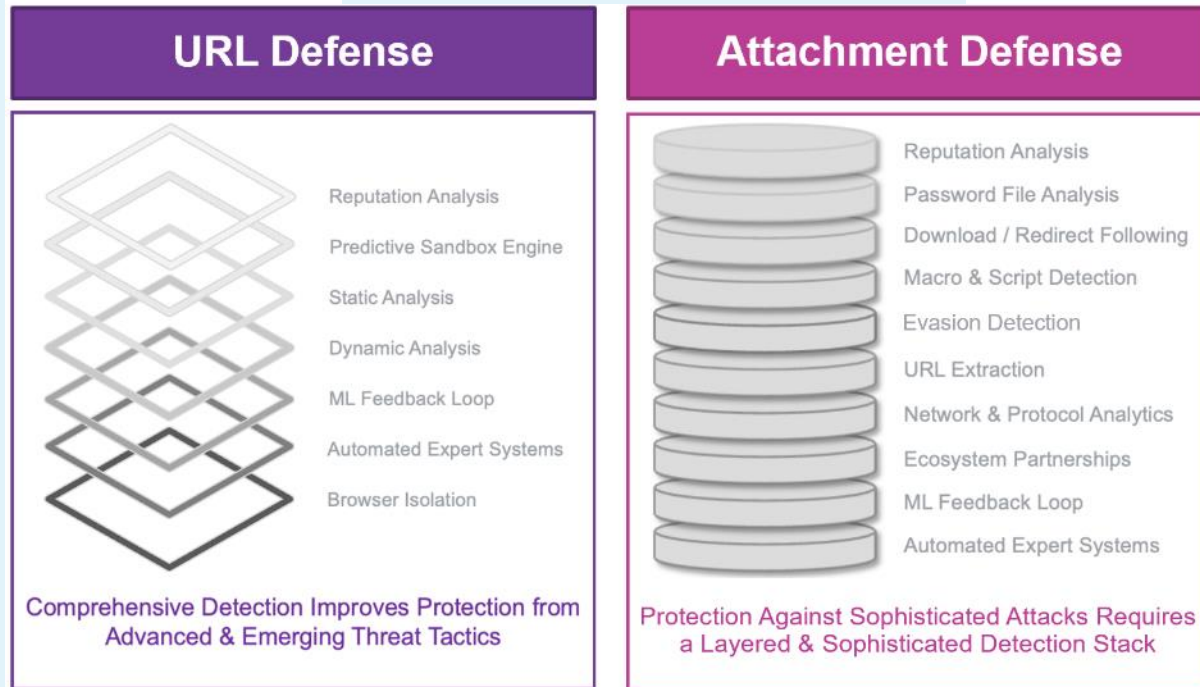


# 04 Proofpoint TAP

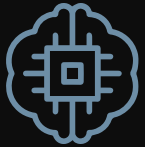
## Proofpoint TAP Module



URL 또는 첨부파일  
이용한 피싱 위협

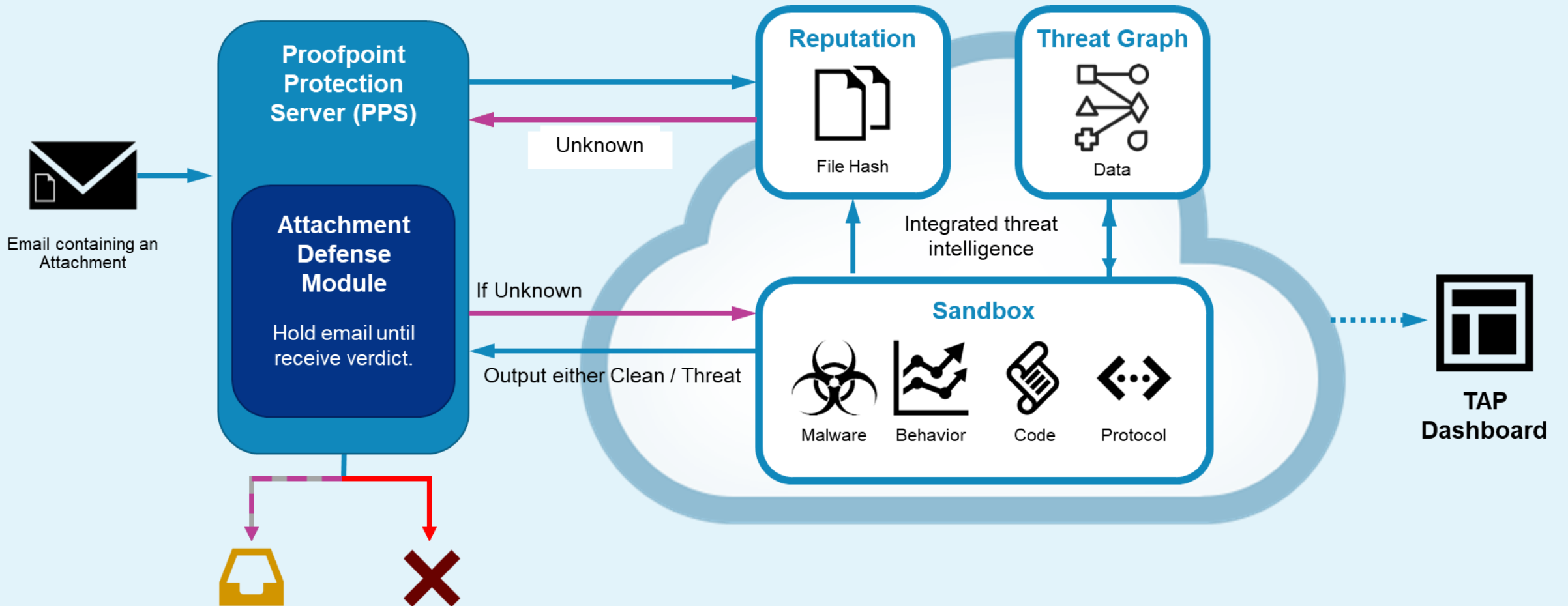


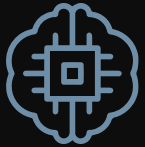
이메일 시스템



# 04 Proofpoint TAP

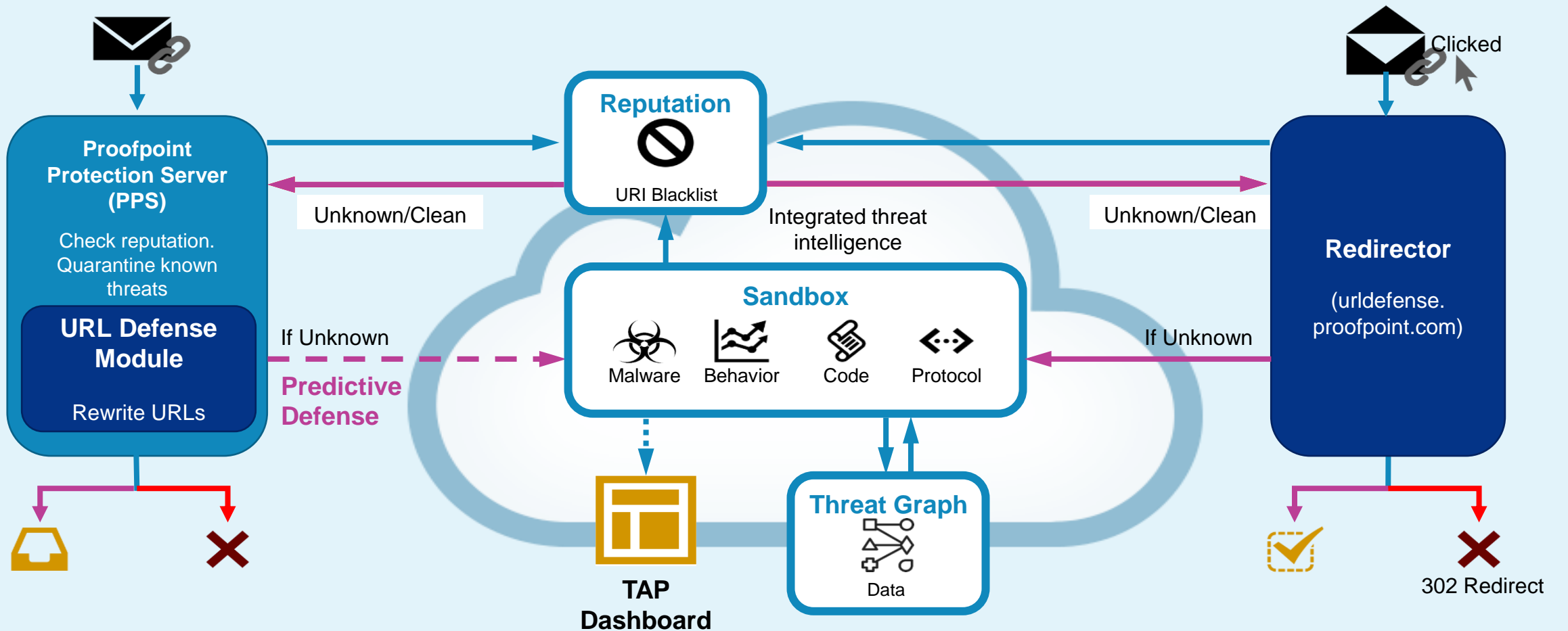
## 첨부파일 검사



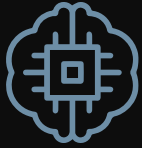


# 04 Proofpoint TAP

## URL 검사





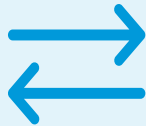


# 04 Proofpoint TAP

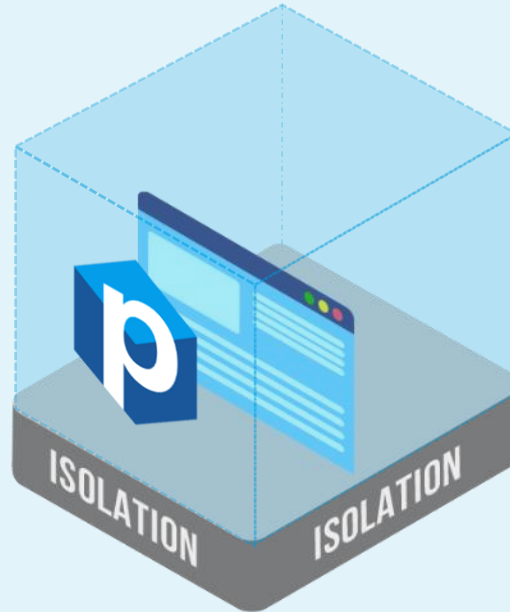
피싱 및 악성코드 피해방지를 위한 웹 격리



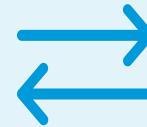
ONLY SAFE CONTENTS  
(HTML-CSS)



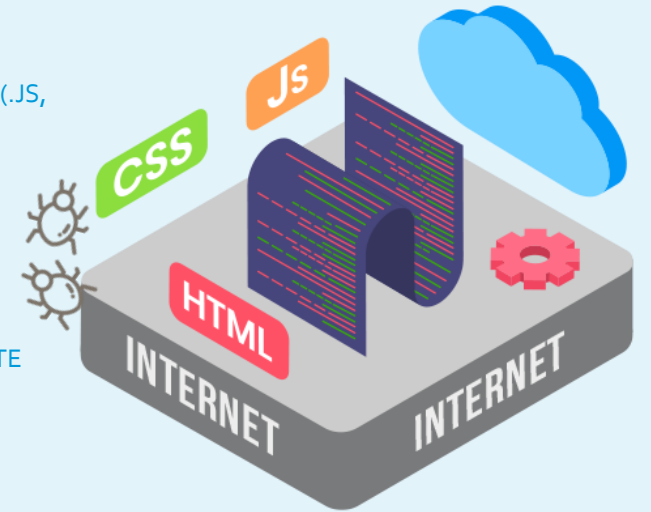
SECURE CONNECTION  
(HTTPS)



HIGH RISK CONTENTS (.JS,  
.EXE, ETC.)



ANONYMOUS WEBSITE  
TRAFFIC

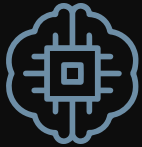


- Existing Browsers
- Easy Deployment

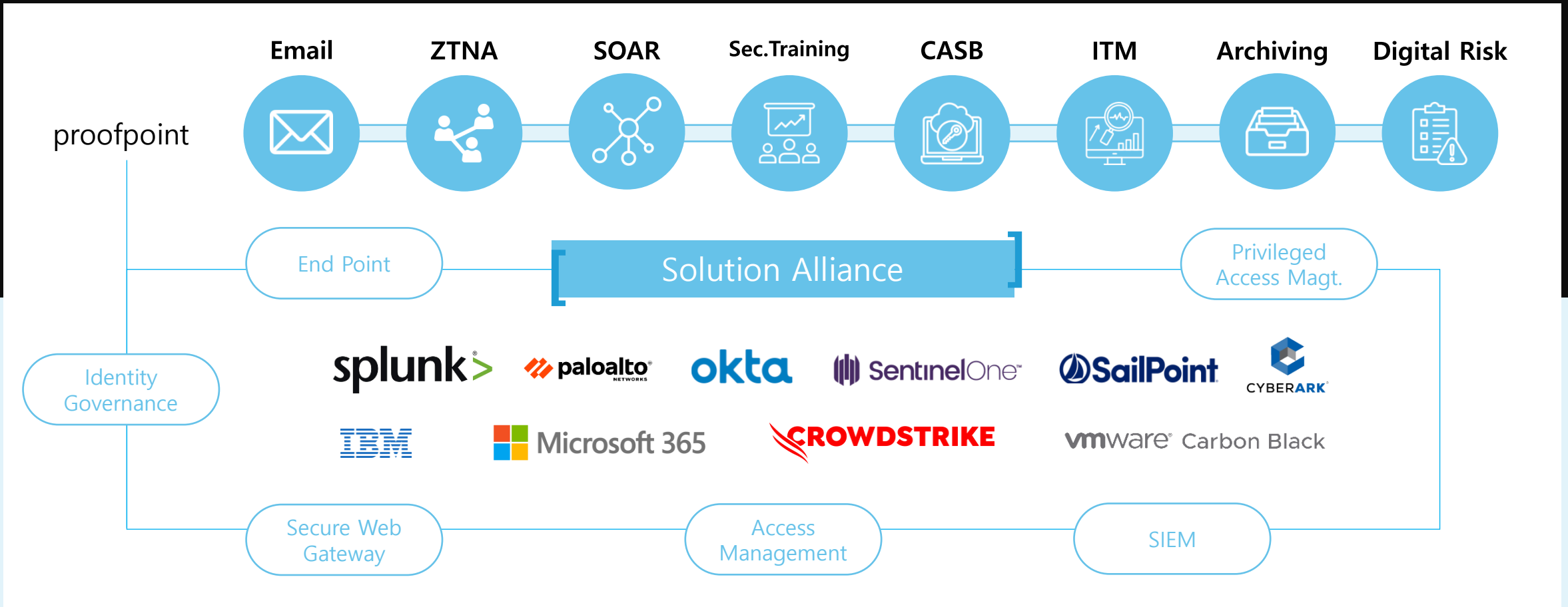
- Cloud Isolation Browsers
- Threat Protection  
(phishing, malware, code execution)
- Disposable

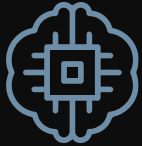
- Policy-based Browsing
- Anonymized





# 04 Eco System 통합을 통한 보안 운영 효율성





# 04 Proofpoint TAP – 사람 중심의 위협 가시성

proofpoint TAP Dashboard

DEMO Industrial Design Comp...

EFFECTIVENESS LANDSCAPE PEOPLE

### Very Attacked People

You have **220 VAPs** that are **over 3.4x more** attacked than the average person in your organization.

**220명의 VAP**  
평균 3.4배의 공격을 받음

Attack Index Ranking  
2019/12/24 - 2020/01/22

Average Person 329

Very Attacked Person 1,103

lowest to highest attack index score

**TOP 위험 사용자**  
해당 사용자의 위협 노출 통계와 공격 비중 정보

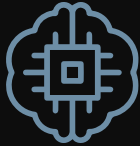
Person	Attack Index	Breakdown by Threat Family
1. <b>Ella Brown</b> - Senior Software Engineer	8,100	[Bar chart showing threat family breakdown]
2. <b>Benjamin Hill</b> - Director of Engineering	5,177	[Bar chart showing threat family breakdown]
3. <b>Alexander Garcia</b> - Director of Product Marketing	4,575	[Bar chart showing threat family breakdown]
4. <b>Ethan Baker</b> - Senior Corporate Counsel	4,470	[Bar chart showing threat family breakdown]
5. <b>Abigail Walker</b> - Major Accounts Manager	4,425	[Bar chart showing threat family breakdown]
6. <b>Michael Allen</b> - Senior Service Reliability Engineer	4,201	[Bar chart showing threat family breakdown]
7. <b>Aria Allen</b> - Country Manager	3,943	[Bar chart showing threat family breakdown]
8. <b>Alexander Anderson</b> - Director of Marketing Communications	3,915	[Bar chart showing threat family breakdown]
9. <b>Benjamin Hill</b> - Director of Engineering	3,847	[Bar chart showing threat family breakdown]

2019/12/24 - 2020/01/22

Sort by Attack Index Contribution

- Credential Phishing 61%
- RAT 12%
- Keylogger 9%
- Stealer 9%
- Corporate Credential Phishing 5%
- Malware 4%
- Banking <1%

Banking  
Consumer Credential Phishing  
Credential Phishing  
Malware  
Stealer  
Corporate Credential Phishing  
Keylogger  
RAT



# 04 BEC 위협을 발견하고 보고하도록 사용자 교육

## 보안인식교육

### Interactive Training

- 비즈니스 이메일 사기
- 피싱 소개
- 사회 공학 기법
- 스피어 피싱 위협
- 의도하지 않은 내부 위협
- 비디오: 비즈니스 이메일 침해
- 비디오: 피싱 소개
- 비디오: 내부자 위협 개요
- 비디오: 인보이스 사기 적발
- 비디오: BEC 사기

### Awareness Video

- 이메일 사기란 무엇입니까?
- 보안 강화를 위한 60초: BEC란?
- 15+ Posters, Infographics, Newsletters

## 지식 평가 및 피싱훈련

### Pre-defined Assessments in Cyberstrength

- 14개의 보안 도메인 평가
- 실제와 같은 피싱 훈련을 통한 평가

**Campaign**

**Business Email Compromise (BEC)**

SUGGESTED CAMPAIGN LENGTH: 1 Month

- Campaign Plan and Materials: Gather everything you need to run a successful campaign — done!
- Communication Tools: Use our talking points and notification emails to communicate about your BEC awareness training campaign.
- Virtual Meeting Background: Kick off your BEC campaign virtually if you can't meet with everyone in person.
- Poster and Social Image: Post themed content in digital channels or in the workplace.
- Article, Digital Signage, and Postcard: Share additional facts about BEC attacks and reinforce your key message.
- Training Modules and Videos: Assign security awareness training about BEC.

Consider These Additional Actions ...

- REDUCE EXPOSURE**: Implement our PhishAlarm® and CLEAR to automate email reporting and remediation.

### Take 5: Defending Against BEC/EAC Attacks

#### 5 Tips for Defending Against BEC and EAC Attacks

Proactive steps you can take to engage end users and prevent successful attacks

There is no escaping the fact that people are the last line of defense against business email compromise (BEC) and email account compromise (EAC) attacks.<sup>1</sup> Cybercriminals are using imposter emails, emails from compromised accounts, vishing (voice phishing) phone calls, pretexting, and other social engineering techniques to craft highly believable attacks designed to trick your end users into making costly mistakes.

Technical safeguards can only do so much. These types of attacks more easily evade perimeter defenses because they generally exclude hallmarks associated with other kinds of phishing emails, like spammy language, embedded links, and infected attachments. That's why security awareness training about this particular topic is so critical.

#### To Defend Against BEC and EAC Attacks, You Must Engage Your Employees

When it comes to BEC prevention, the IT's have it. Keep these five points in mind:

1. Identify individuals within your organization (like controllers, accountants, HR representatives, etc.) who would be likely targets of BEC and EAC attacks. Also identify individuals and partner organizations that may legitimately request wire transfers, invoice payments, gift card purchases, and transfers of sensitive data (like employees' W-2 information).
2. Inform users—particularly those in key roles—about BEC/EAC attacks and the ways cybercriminals will try to mislead them. (Our [Infographic](#) can help, as can our Business Email Compromise training module.)
3. Instruct employees to be immediately suspicious of any requests like those outlined above—even if requests appear to come from someone they know and trust. Any requests that provide "updated" account or bank routing information—including those related to employee payroll—should immediately raise warning bells.
4. Insist that, prior to executing on a request like those outlined above, some form of "manual" two-factor authentication must happen. We suggest that the person who receives the request reach out and contact the requestor via a **known, trusted channel**—like a frequently used phone number—to receive voice-to-voice confirmation. No request of this nature should be fulfilled based on an inbound request (whether that comes via email, phone, text, or another form of communication).
5. Implement a code word or phrase as an additional layer of security for these types of transactions. The code word/phrase should be changed regularly and should never appear in email or text messages. Be sure to document all procedures for establishing and distributing code words/phrases, as well as processes for authenticating requests. You should also have an action plan in place for situations in which an employee suspects a fraudulent request has been made.

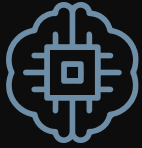
<sup>1</sup> BEC and EAC attacks are closely related; in fact, EAC attacks are often referred to as BEC attacks. At Proofpoint, we characterize the distinction this way: In the case of BEC, the attacker pretends to be a trusted contact; in the case of EAC, the attacker appears to BE the trusted contact. It's important for users to be aware that, in the case of EAC, a request could in fact originate from a known source and still be dangerous. You can read more about EAC on our [blog](#).

**Verify**

**PAYMENTS AND WIRE TRANSFER REQUESTS**

**FACE-TO-FACE OR VOICE-TO-VOICE**

☑



## 04 사람 중심 위협평가 방법제공

### PROOFPOINT ATTACK INDEX

공격자

목표 형태

공격 형태



#### 샘플#1

공격자	TA470 분류된 공격자 그룹	HIGH
목표형태	NGO 관련 조직 대상	HIGH
공격형태	서플라이체인 Invoice BEC	MID

평가 점수

**960** / 1000

#### 샘플#2

공격자	Small crime	LOW
목표형태	Widespread	LOW
공격형태	계정 탈취 피싱	LOW

평가 점수

**50** / 1000

# proofpoint.

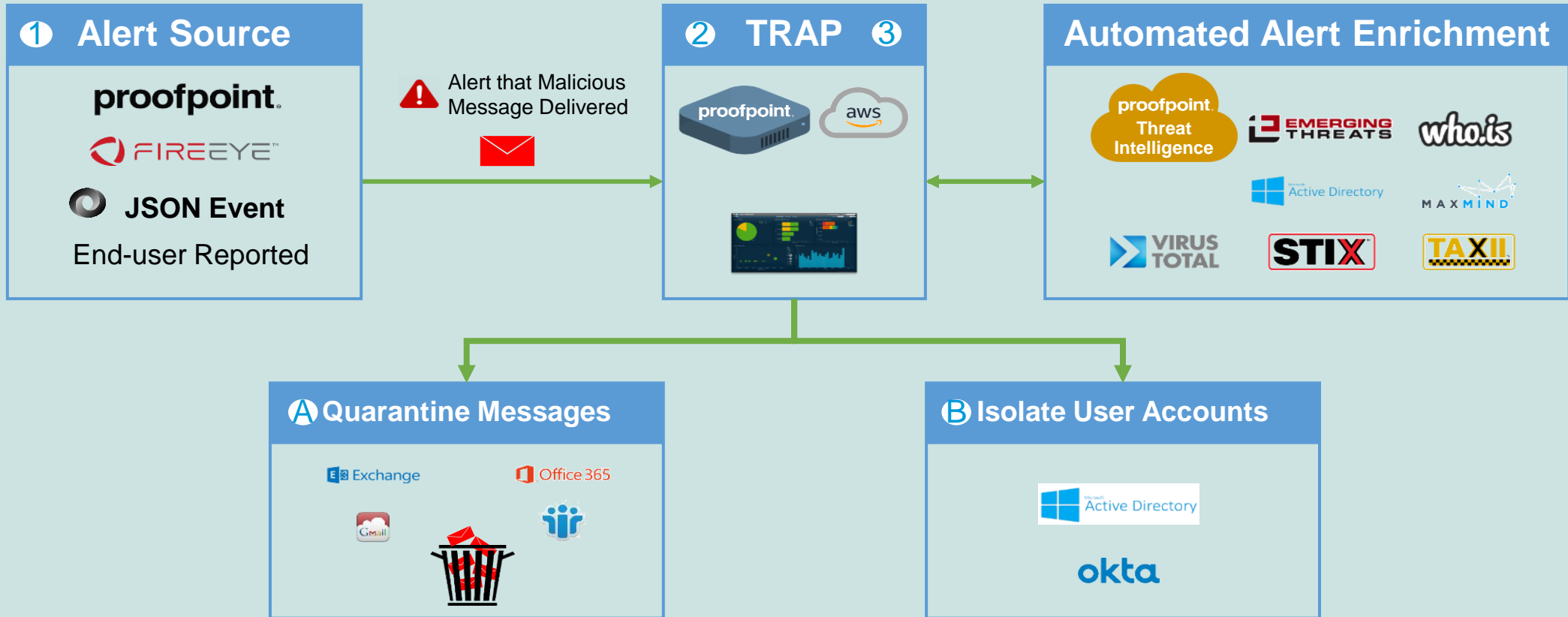
05

**TRAP** Threat Response Auto Pull



# 05 TRAP 소개

Retroactive 경고를 통해 메시지 자동 삭제

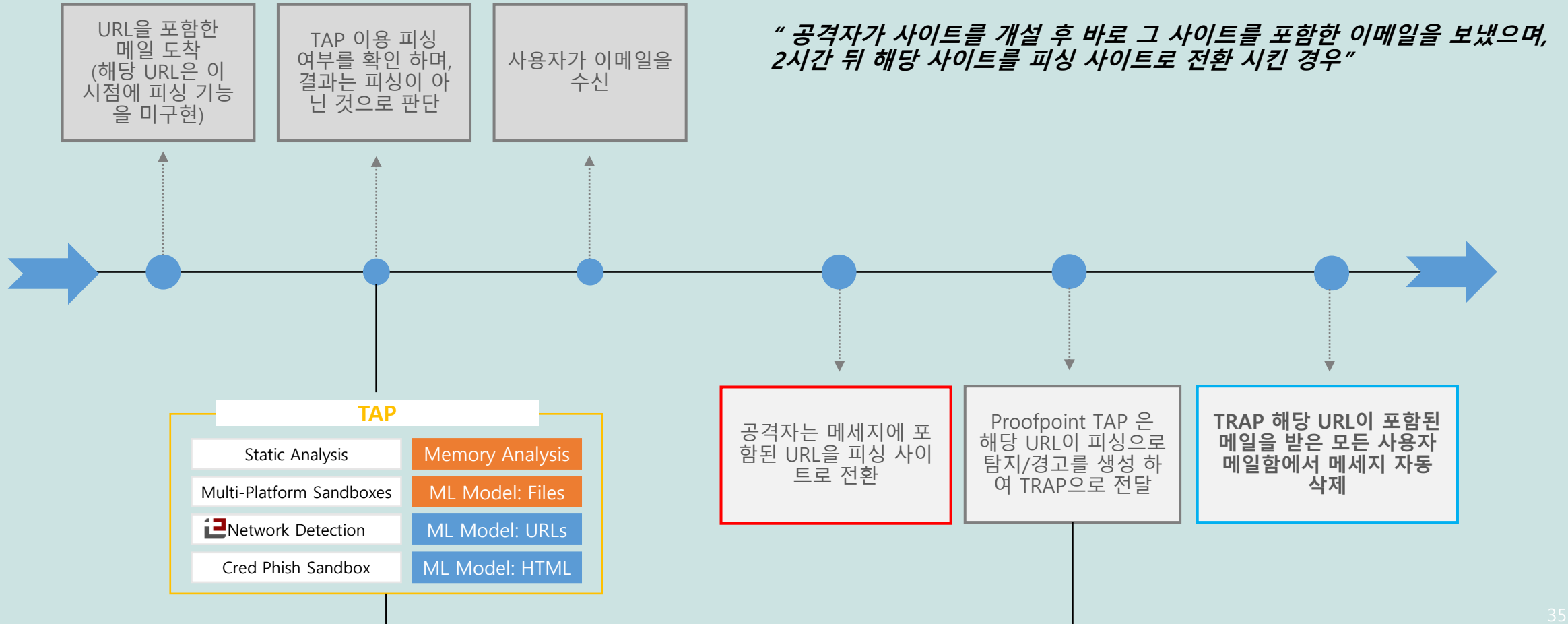






# 05 TRAP 소개

## Use Case



# proofpoint.

06

# Email Fraud Defense – Outbound BEC 대응

---



# 06 Outbound BEC

이메일 인증 - 기업 브랜드 보호

## 브랜드 이미지 실추

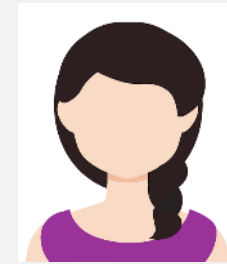


**e**lim.net 사칭

- 도메인 스푸핑
- 유사 도메인
- Display Name 스푸핑

조직의 고객, 파트너 대상 BEC

Outbound BEC

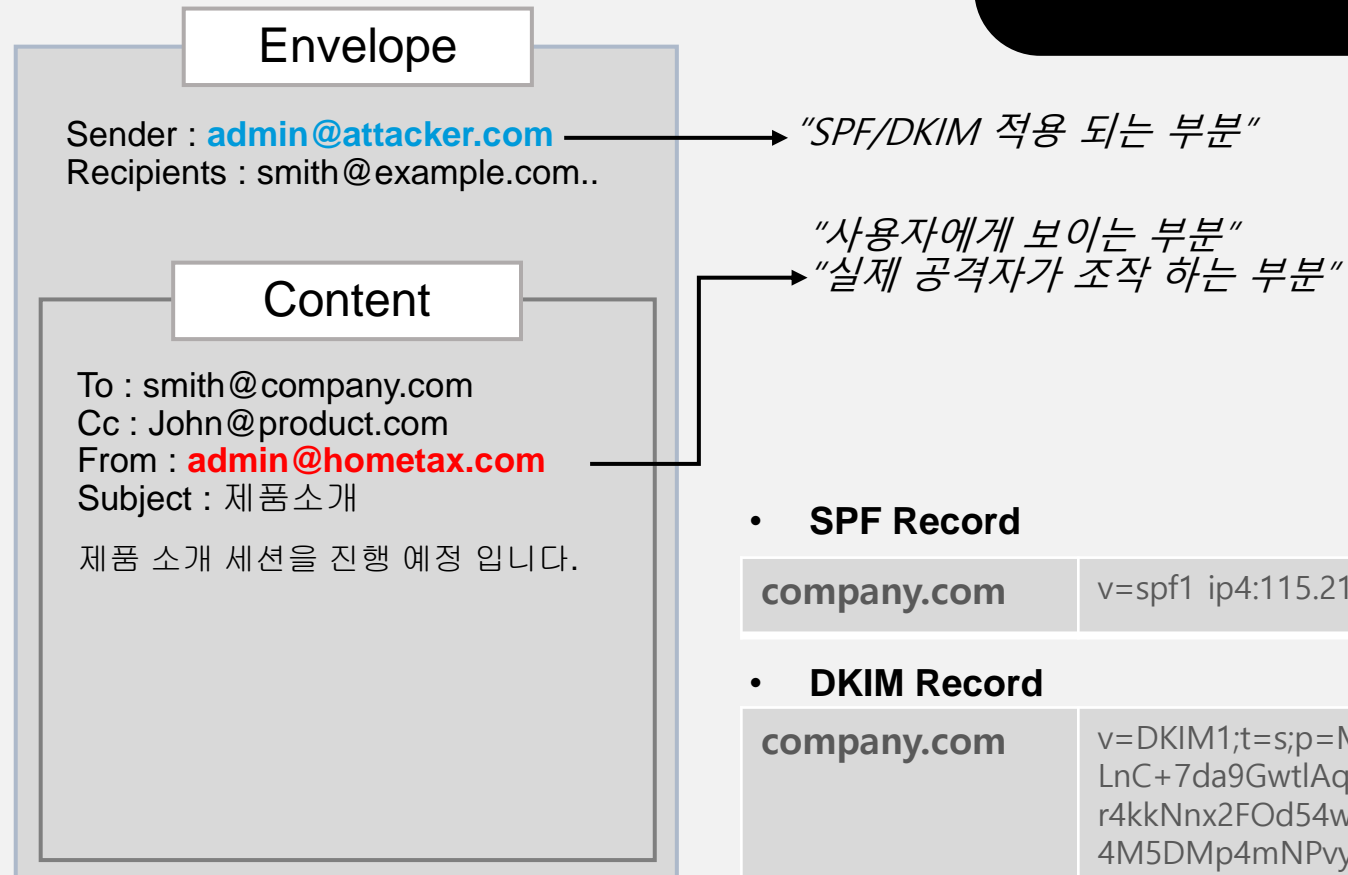


파트너, 고객



## 06 Outbound BEC

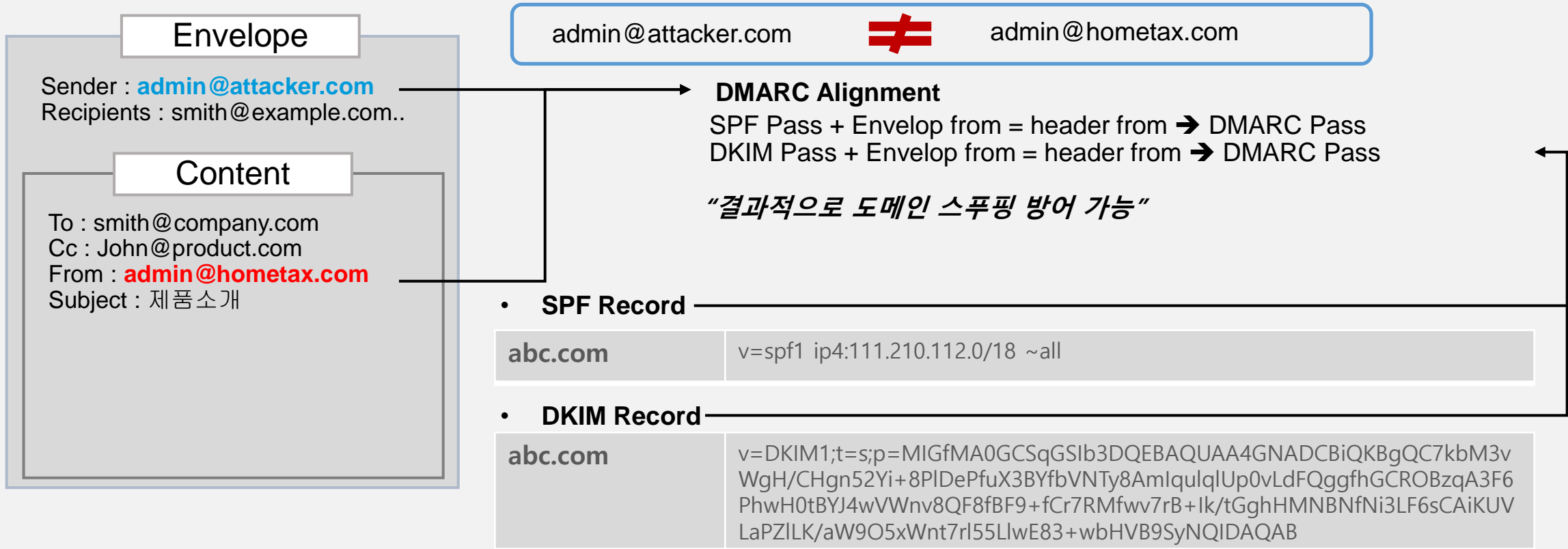
### SPF, DKIM 의 한계





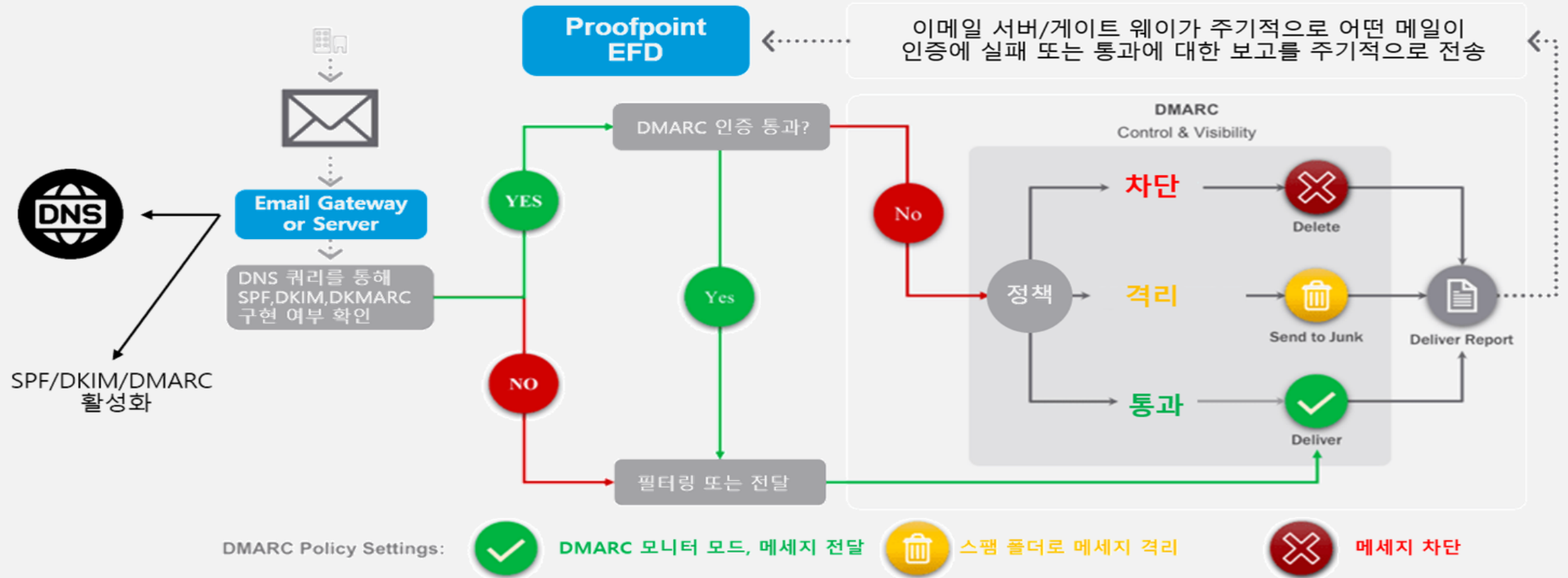
# 06 Outbound BEC

## DMARK 의 필요성



# 06 Outbound BEC

## EFD(Email Fraud Defense) 아키텍처





## 06 Outbound BEC

### 이메일 트래픽에 대한 완전한 가시성 제공

The screenshot displays the Proofpoint Email Fraud Defense dashboard for 'Foodies Corp.'. The main view is 'North America BU1\_Sending', showing emails sent to consumer mailbox providers in the last 7 days. The interface is divided into several sections:

- My Domains:** A table listing 10 domains with their FQDN(s) and DMARC Po... status. Domains include FOODIES.COM, foodies.com, em.foodies.c..., reply.foodies..., foodie.co.uk, yumyumfood.c..., and LISFOODIES.C.
- Identify Permitted Senders:** A section with a warning icon and text: 'The following senders are sending for domains in this group. Please review each sender and identify which domains they are permitted for. This is required for proper categorization of data, reporting, and surfacing Actions for each sender.' It lists various senders like British Telecommunications, Salesforce, GoDaddy, BAE Systems, 148.163.140.193, ADP, Atlassian, SendGrid, Marketo, ServiceNow, 140.112.30.142, PayPal, Microsoft, and Qualtrics.
- Sender Profile:** A detailed view for 'Salesforce' showing a 91% PFPT Customers score and an 86 Reputation Score. It includes a 'Sender Profile' section and a 'Sending As 5 Domains' table with columns for Domain, Sending Vol., Sending IPs, and Sample. The table lists domains like foodies.com, em.foodies.com, reply.foodies.com, yumyumfood.com, and bounce.usfoodies.c... with their respective sending volumes and 'VIEW' links.
- My Senders:** A section for 'Permitted senders'.
- Actions:** A section for '11 new actions'.

- 자신의 도메인 이용한 모든 이메일 트래픽 및 어떤 3rd Party 자신의 도메인을 이용해 메일을 보내는지에 대한 가시성 제공
- 자신의 도메인을 대신하여 보낸 의심스러운 이메일 식별/발신자 평판 확인

# proofpoint.

# 07

## Summary

---



## 07 Summary

### Proofpoint Solution Bundles

<b>P1+</b>	<b>P1</b>	<b>P0</b>	<ul style="list-style-type: none"> <li>Email Protection</li> <li>Email Warning Tags</li> <li>Targeted Attack Protection (TAP)</li> <li>TAP URL Isolation (VAP Only)</li> <li>TAP SaaS Defense</li> <li>Threat Response Auto Pull</li> <li>CLEAR</li> </ul>
			<ul style="list-style-type: none"> <li>Security Awareness Training</li> </ul>
			<ul style="list-style-type: none"> <li>Email Fraud Defense (Unlimited)</li> <li>Supplier Risk Explorer</li> <li>Hosted SPF</li> <li>TAP URL Isolation (All Users)</li> <li>SPF Hosting</li> </ul>

# 07 Summary

## Proofpoint Email 보안 솔루션 도입효과

### 업계 최고의 인텔리전스

20년간 이메일 보안 선두기업의 위협 인텔리전스

진화하는 이메일 위협에 대한 포괄적인 보호

### 완벽한 이메일 위협 차단 대응 시스템

Email Protection, TAP, TRAP

이메일 위협에 대한 예방, 탐지, 대응의 완벽한 시스템 구현

### Supernova ML

BEC 공격에 특화된 엔진

최근 피해 규모가 증가하는 BEC 공격에 대한 솔루션 제공

### 사람 중심의 보안 구현

차원이 다른 가시성 제공, 교육을 통한 보안 인식 향상

위협 중심이 아닌 사람 중심의 위협 가시성을 제공하여 중요 취약 인력에 대한 보안 강화

### 업계 리더 제품과의 통합

보안 업계 리더 제품과의 통합으로 보안, 운영 효율 강화

Crowd strike, Paloalto, Cabonblack, Okta, Sailpoint, CyberArk 등과 통합

## 07 Summary

### An Email Rapid Risk Assessment for M365 고객

- Microsoft365 전자메일 고객을 위한 테스트
- 지능적 위협에 노출된 2주간의 내용을 24시간 내 결과 도출 후 보고서 제공
- RRA를 위한 고객사의 설정은 5분 미만 소요 (M365 API 활용)

proofpoint PoC의 결과를 위협분석 관점에서  
더 빠르게 수행



# 07 Tech Support



- 고객사 환경을 이해하는 파트너사
- 30년+ 전문 총판기술지원체계 노하우
- proofpoint 한국지사의 기술지원체계
- 지속적인 기술지원 및 개선활동 수행
- 전문적 품질관리 지원 조직
- Global proofpoint 기술지원 연계

## 고객사 맞춤형 기술지원 제공

# proofpoint.

EOF.

S.Pin Technology

# proofpoint.

감사합니다.

S.Pin Technology



# proofpoint

“ 지능형 위협과 컴플라이언스 위험으로부터 사람을 보호하는데 앞장서는 선도 기업 ”

#1

Fortune 100대, Fortune 1000대 및 글로벌 2000대 기업에서 가장 많이 배포한 솔루션

5대

매출(>\$10억) 및 시장 자본 면에서 글로벌 사이버 보안 기업



주요 위협 벡터 차단을 위한 가장 신뢰할 수 있는 글로벌 보안 벤더

People-centric Security라는 독특한 메시지를 가진 정보보안 회사

다른 선도업체와 원활한 통합 가능

## proofpoint 고객



# proofpoint

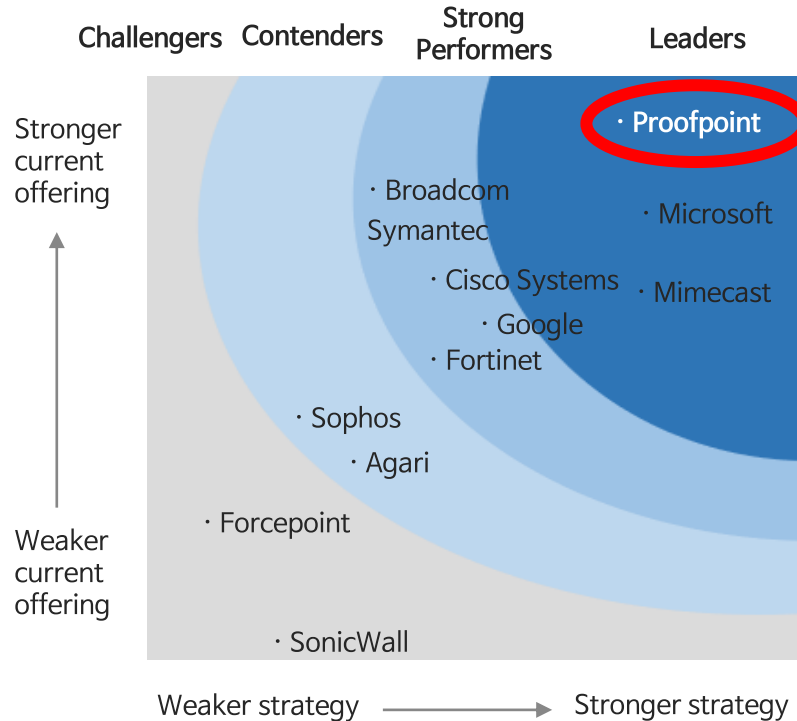
## “Global 경쟁력 No.1 솔루션”

# #1

Fortune 100대, Fortune 1000대 및 글로벌 2000대 기업에서 가장 많이 배포한 솔루션

# 5대

매출(>\$10억) 및 시장 자본 면에서 글로벌 사이버 보안 기업



[Q2 2021 Forrester Wave : Leader in Email Security]

### 7년 연속 이메일 시장 1위

Fortune 100대 기업의 80% 이상

Fortune 1,000대 기업의 60% 이상

Global 2,000대 기업의 45% 이상

# 8,000+

Enterprise Customers

# 200,000+

SMB Customers

# 99.999%+

업계 최고의 효율성

### Magic Quadrant 리더십

※ Security Awareness Training  
6년 연속 리더

※ Information Archiving  
10년 연속 리더

※ Cloud Access Security Broker  
Leading Challenger