proofpoint.

이메일보안 소개

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

S.Pin Technology | 솔루션 사업실 Cloud.solution@spintech.co.kr

proofpoint.

Agenda

01 – 배경 및 목적

02 – 주요위협 및 문제점

03 – proofpoint를 통한 해경방안

04 – 제품의 특장점

05 – 성공사례

06 – 기대효과 / TCO

07 – 구축방안 및 지원사항

S.Pin Technology

proofpoint.

01
배경 및 목적

S.Pin Technology

01

Enterprise DX환경에서 가장 걱정되는 부분은

보안

비용

가버넌스

리소스

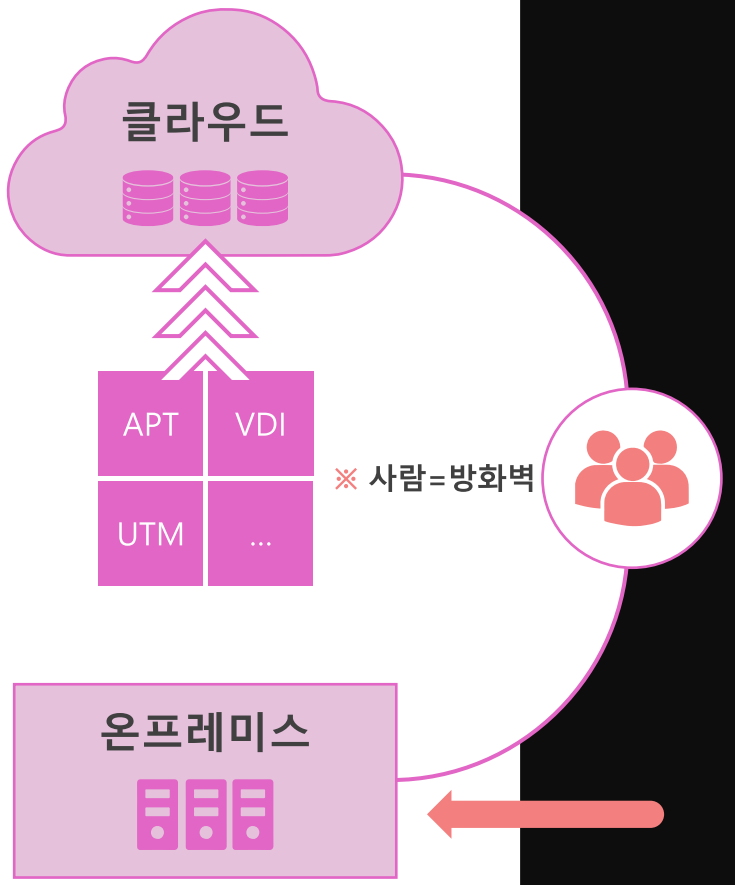
컴플라이언스

* 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

* Flexera, '2020 스테이트 오브 클라우드 리포트

우리 조직의 사이버 보안 위협 점검 필요성

피해사례	점검 포인트
기프트 카드 사기	BEC 변형의 조직 경험 있는지?
급여 전환	위험한 공급자가 누구인지?
공급업체 송장 사기	솔루션은 다단계 랜섬웨어 차단?
거래처 계좌 변경 메일 사기	클라우드 계정 및 앱(Office365) 보안이 안전?
퇴사자 메일 도용 정보 유출	현재 이메일 보안공급자가 교차공격 방어?
고객센터 안내 위장 메일	피싱 사용자를 어떻게 식별 & 치료?
지인 사칭 악성코드 첨부 메일	발견된 위협과 손실을 대처하는 프로세스가 있는가?

proofpoint.

02

주요위협 및 문제점

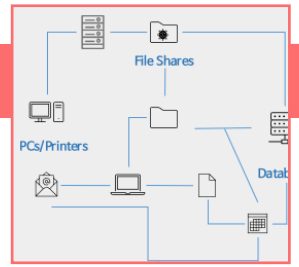
S.Pin Technology

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 부탁 드립니다.

ABC Bank : 123-456-789999

02

직면한 사이버 위협 즉시대응 필요

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

02

직면한 사이버 위협 즉시대응 필요

이메일

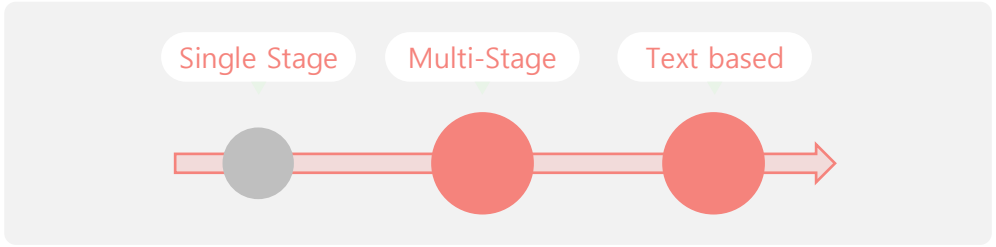
BEC

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

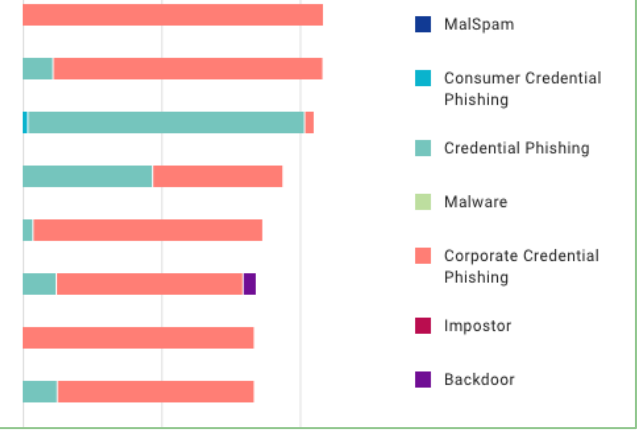
확인해본 실제 기업의 상황

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
1 Alexander Harris Director of Marketing Commu...	4,333	
2 William Lewis Senior Product Manager	4,325	
3 Daniel Walker QA Engineer	4,198	
4 Aria Moore Director of Engineering	3,745	
5 Jacob Scott Director of Finance	3,453	
6 Harper Martinez Senior Corporate Counsel	3,355	
7 Noah Brown Junior Sales Engineer	3,334	
8 Michael Brown Senior QA Engineer	3,330	



02

직면한 사이버 위협 즉시대응 필요

이메일 | BEC

랜섬웨어

User Activity (ITM)

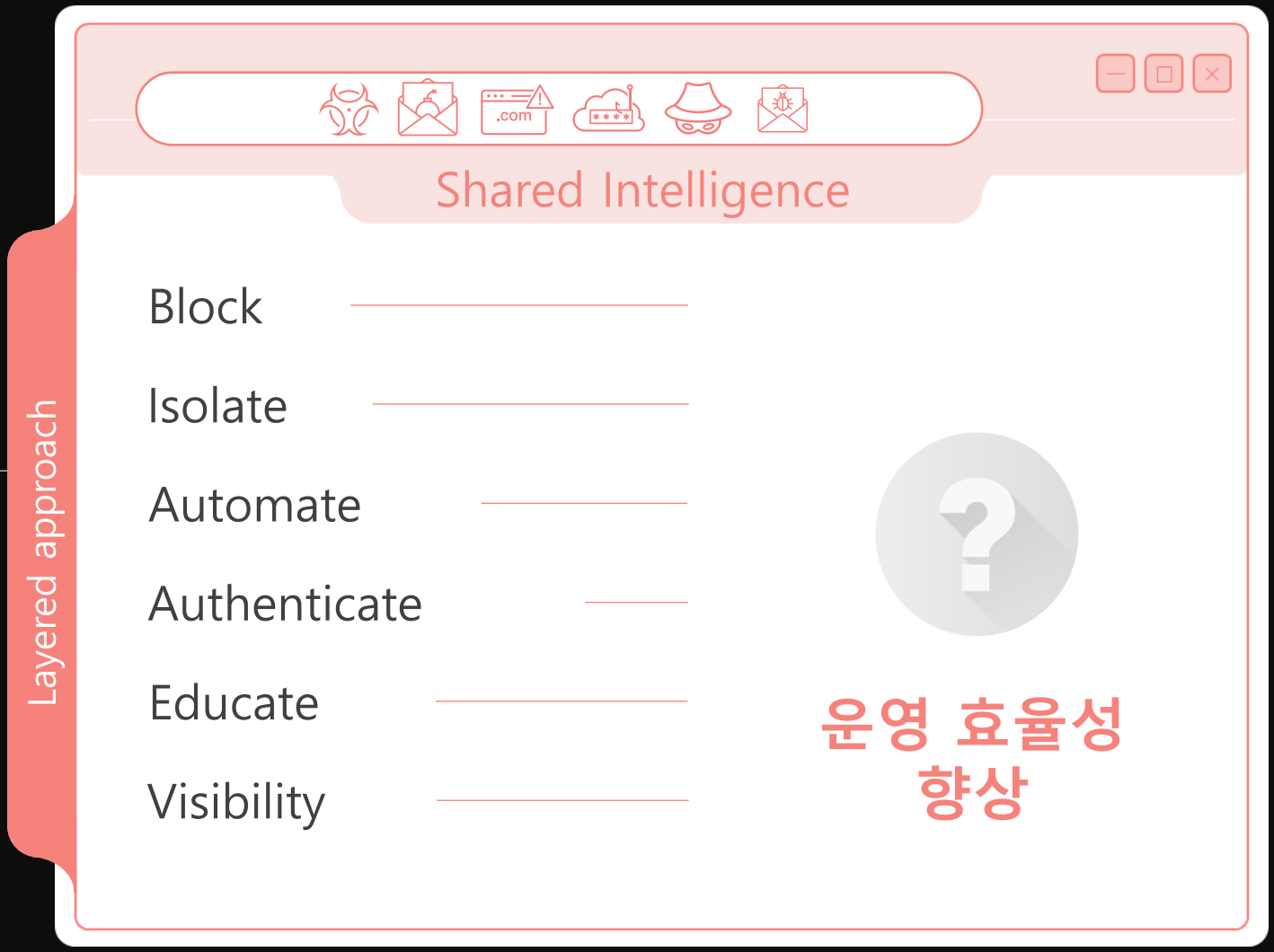
BEC와 랜섬웨어

동시에
방어할 수 있는
솔루션은?

02

직면한 사이버 위협 즉시대응 필요

점점 많아지고 위중해지는
CISO & 보안 운영
관리자의 미션



proofpoint.

03

Email Protection - Powerful Email Gateway

S.Pin Technology

03 Proofpoint 이메일 보안 제품 Line-up

BEC까지 방어할 수 있는 유일 솔루션

이메일 GW(PPS/POD)

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

샌드박스(TAP)

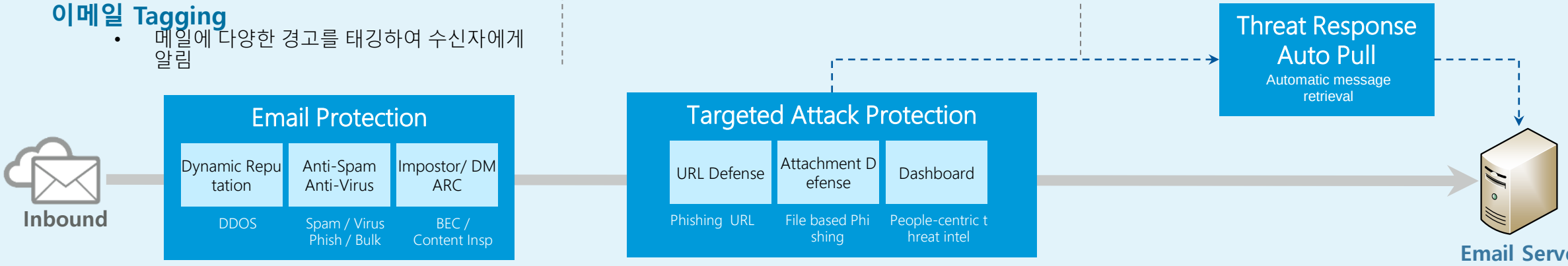
Cloud 샌드박스
- URL Defense : 메일 내의 URL 주소를 재설정 하여 추후 해당 URL이 악성으로 변경되어도 실시간으로 검사 및 탐지
- Attachment Defense : 메일 첨부파일에 대한 행위 분석 수행

VAP(Very Attacked People) 리스트
- 위험에 노출 된 사용자에 대한 가시성 제공

이메일 위협 사후 대응(TRAP)

mSoar
- 이메일 전달 후 악성으로 확인된 메일을 Mailbox에서 자동 격리

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

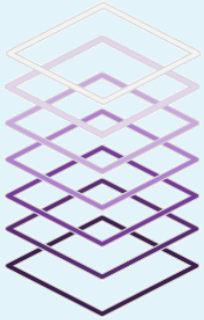


03 Proofpoint 이메일 보안 제품 Line-up

BEC까지 방어할 수 있는 유일 솔루션

악성 URL 탐지

Proofpoint URL Defense



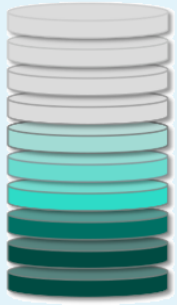
- Reputation Analysis
- Predictive Sandbox Engine
- Static Analysis
- Dynamic Analysis (URLs & files)
- ML Feedback Loop
- Automated Expert Systems
- Browser Isolation

Microsoft Safe Links

- Reputation Analysis
- Static File Analysis
- Dynamic File Analysis

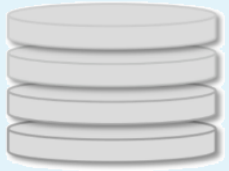
악성 첨부파일 탐지

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

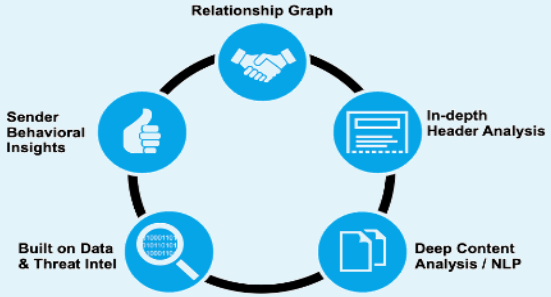
Microsoft Safe Attachments



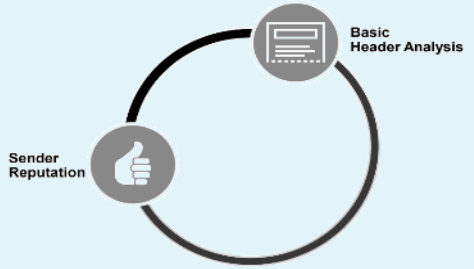
- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection

이메일 사기 탐지

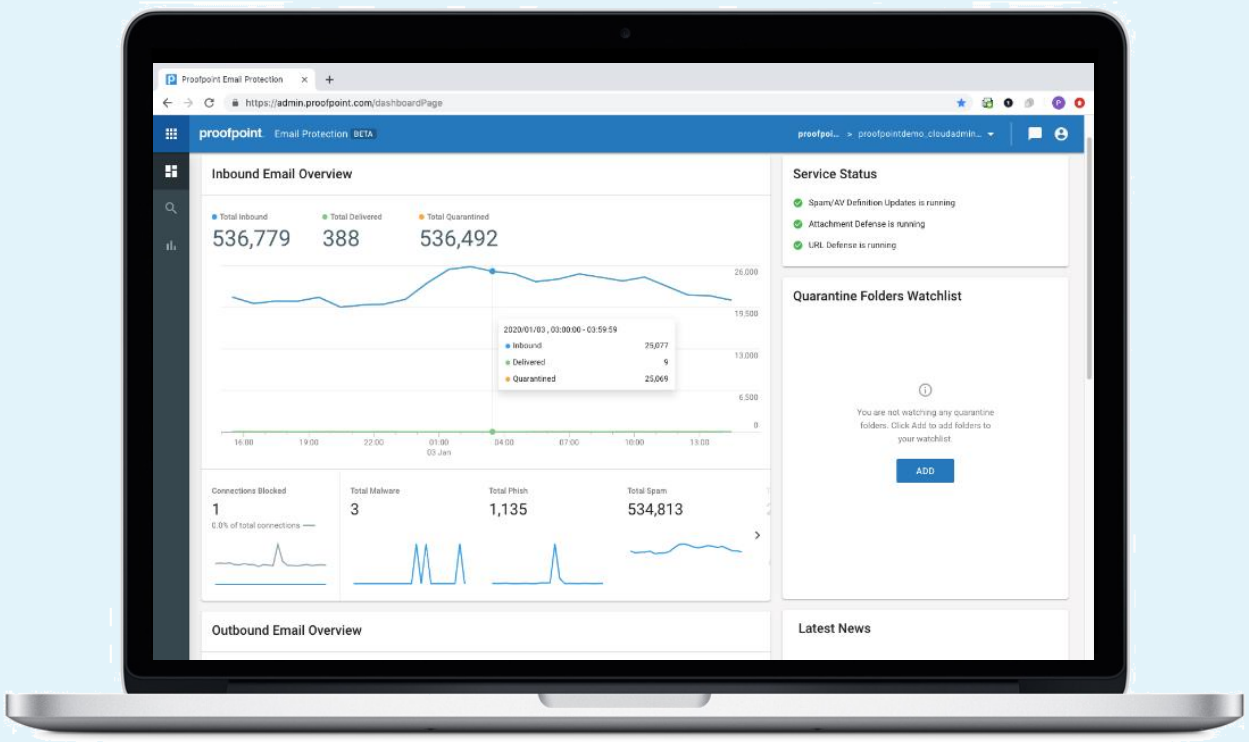
Proofpoint Supernova



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

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: SCBLXHXXK

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.

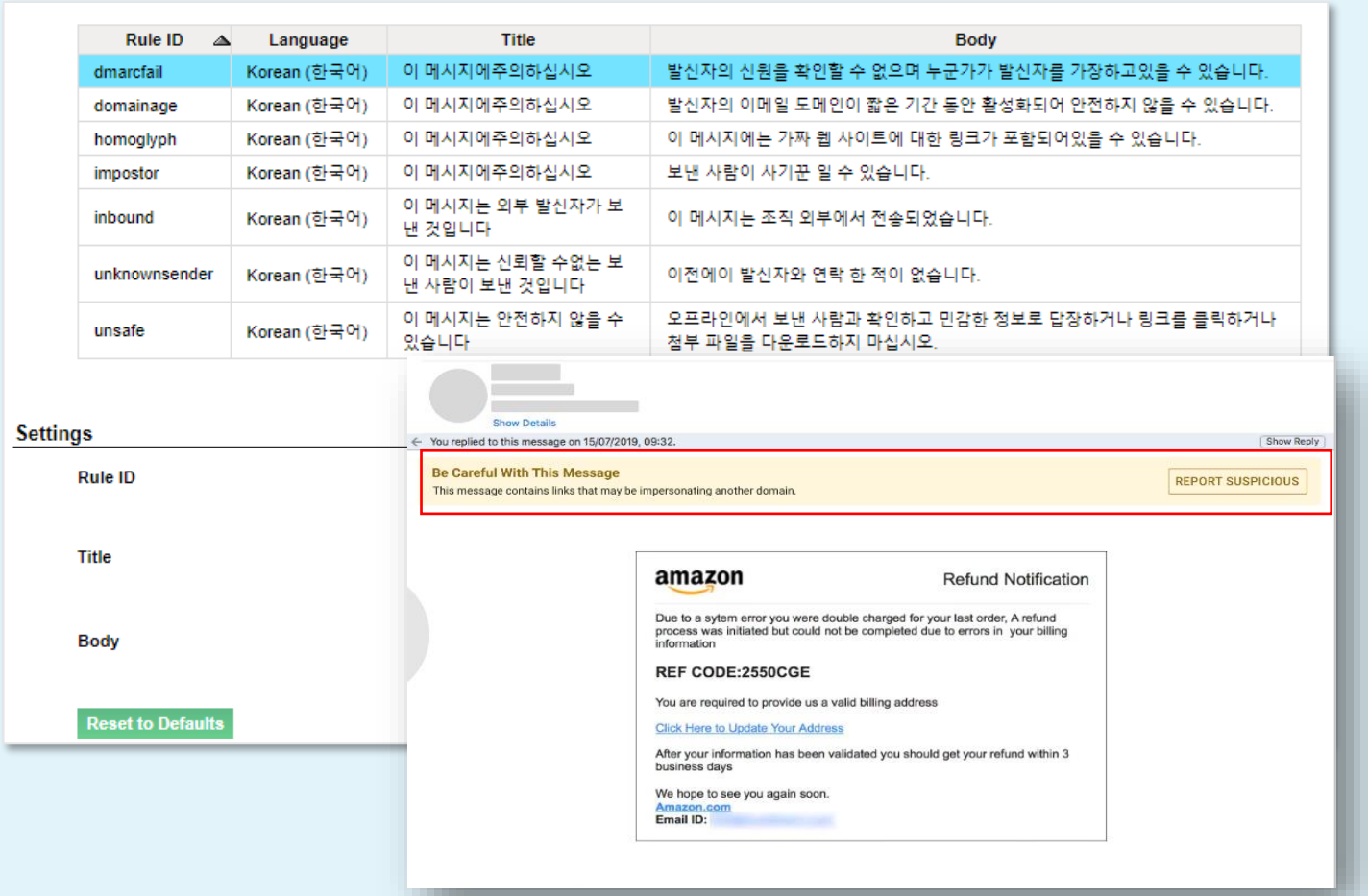
메세지 구문 분석

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 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 수없는 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 답장하거나 링크를 클릭하거나 첨부 파일을 다운로드하지 마십시오.

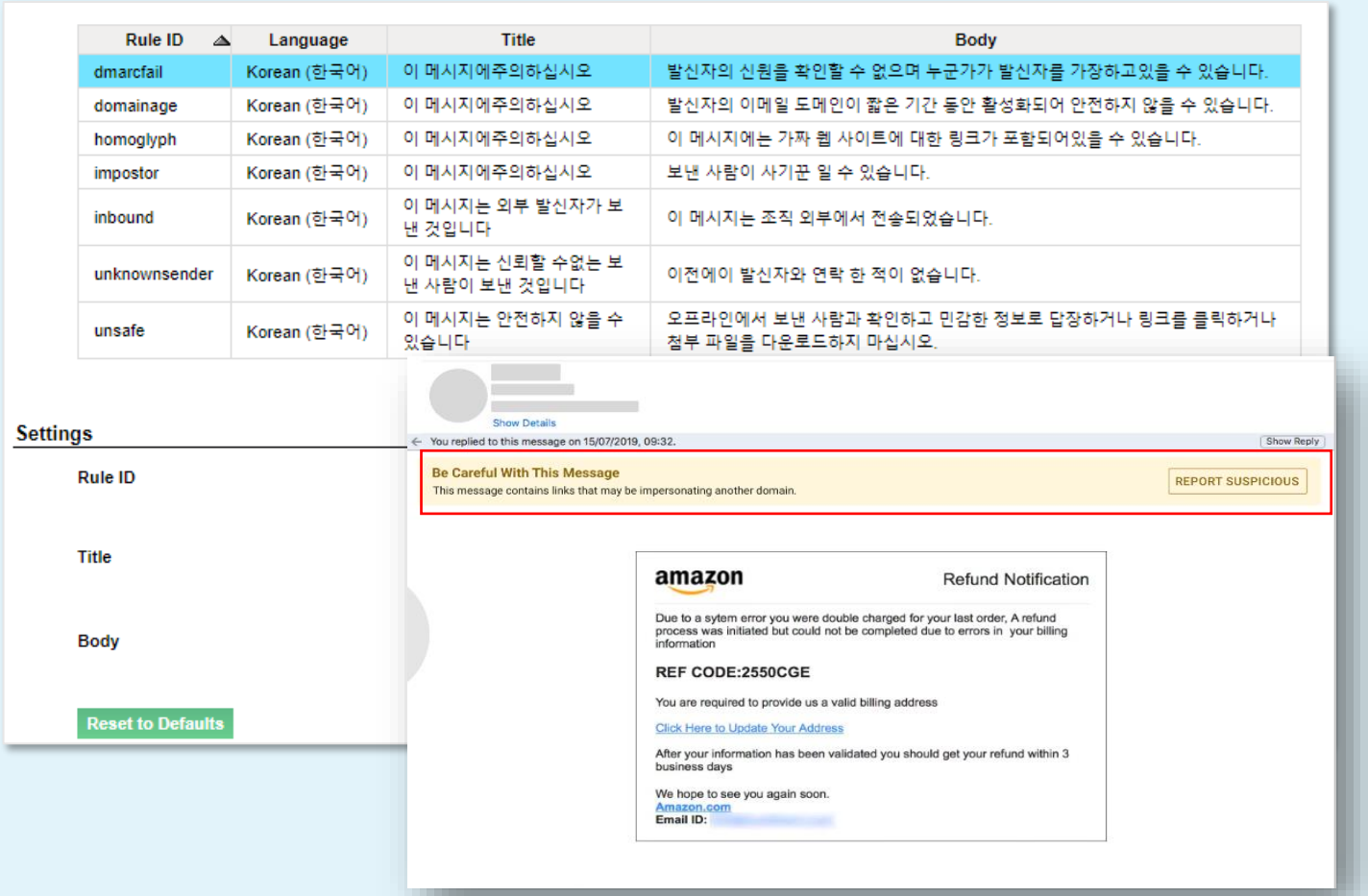


- 최종 사용자가 좀 더 정보에 입각한 결정을 내릴 수 있도록 하여 잠재적인 침해 위험 완화
- 사용자가 경고 태그에서 바로 조치를 취할 수 있도록 함
- BEC 및 EAC 공격 전략에 맞서 보호
  - 이메일 스푸핑
  - 유사 도메인
  - 자격 증명 피싱
- 위험 요소에 관한 간략한 설명 제공

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 수없는 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 답장하거나 링크를 클릭하거나 첨부 파일을 다운로드하지 마십시오.



- 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

S.Pin Technology

04 Proofpoint TAP

URL 또는 첨부파일을
이용한 피싱 위협

Proofpoint TAP Module

URL Defense

- Reputation Analysis
- Predictive Sandbox Engine
- Static Analysis
- Dynamic Analysis
- ML Feedback Loop
- Automated Expert Systems
- Browser Isolation

Comprehensive Detection Improves Protection from Advanced & Emerging Threat Tactics

Attachment Defense

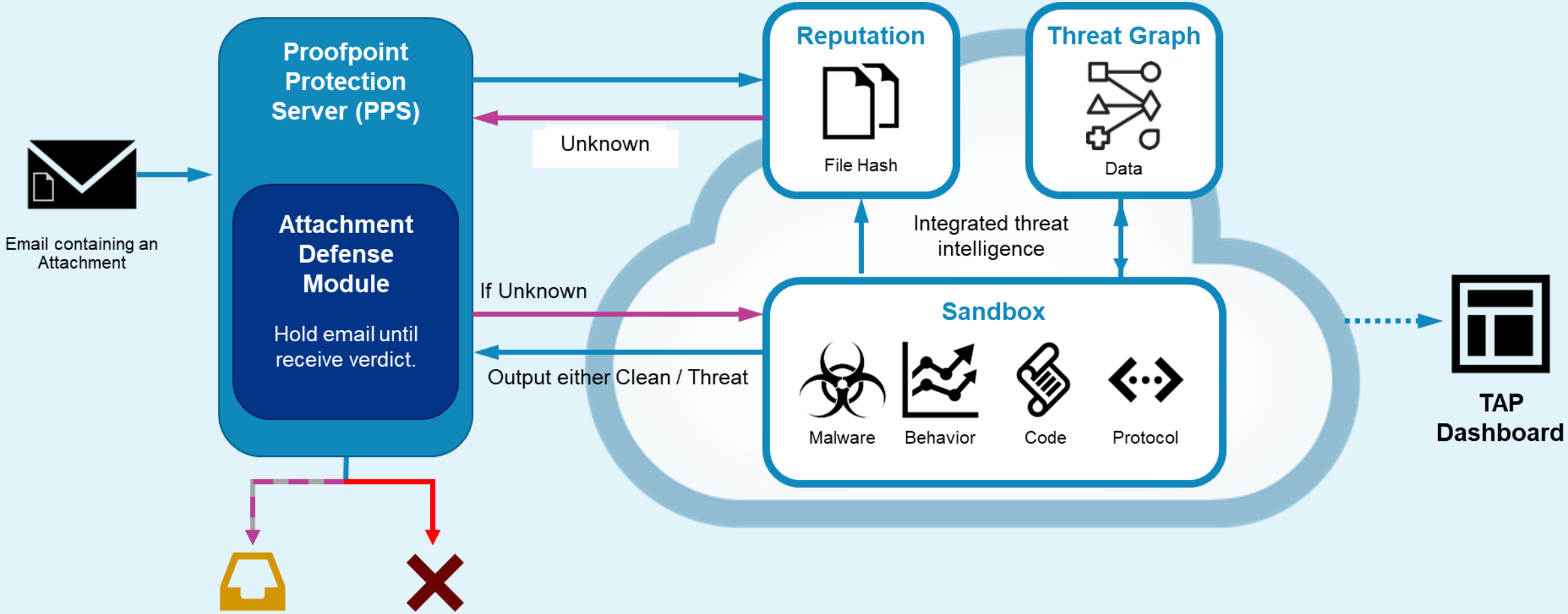
- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection
- Evasion Detection
- URL Extraction
- Network & Protocol Analytics
- Ecosystem Partnerships
- ML Feedback Loop
- Automated Expert Systems

Protection Against Sophisticated Attacks Requires a Layered & Sophisticated Detection Stack

이메일 시스템

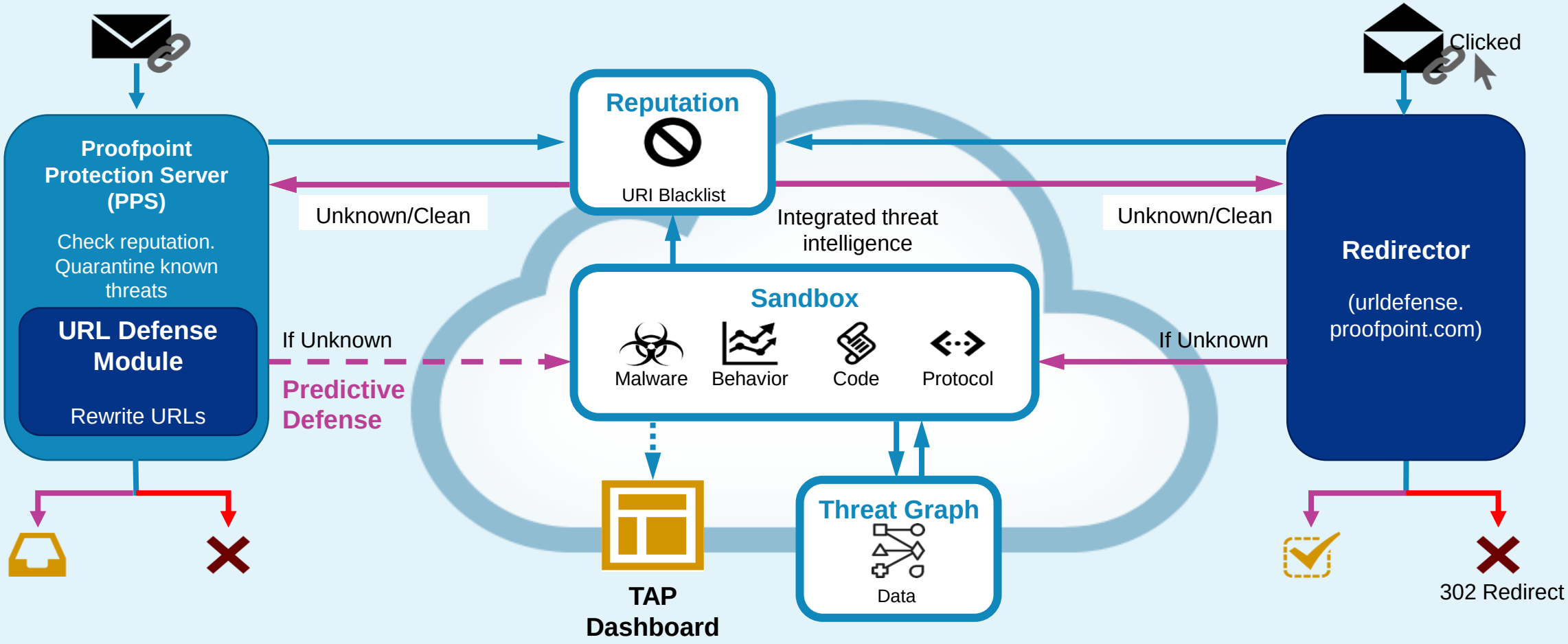
04 Proofpoint TAP

첨부파일 검사



04 Proofpoint TAP

URL 검사

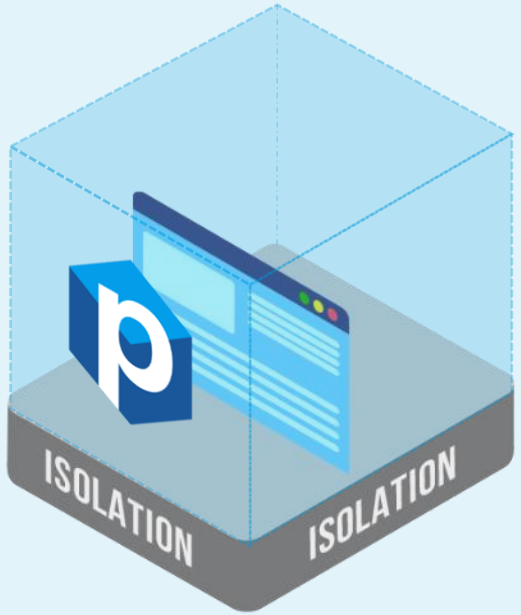


04 Proofpoint TAP

피싱 및 악성코드 피해방지를 위한 웹 격리

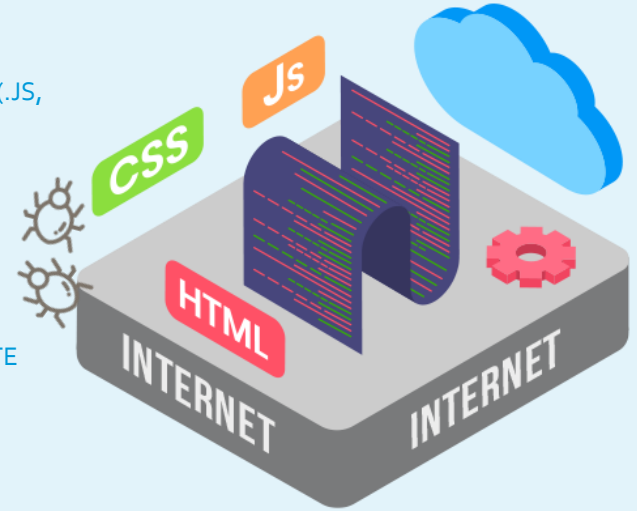
ONLY SAFE CONTENTS
(HTML-CSS)

SECURE CONNECTION
(HTTPS)



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

ANONYMOUS WEBSITE
TRAFFIC



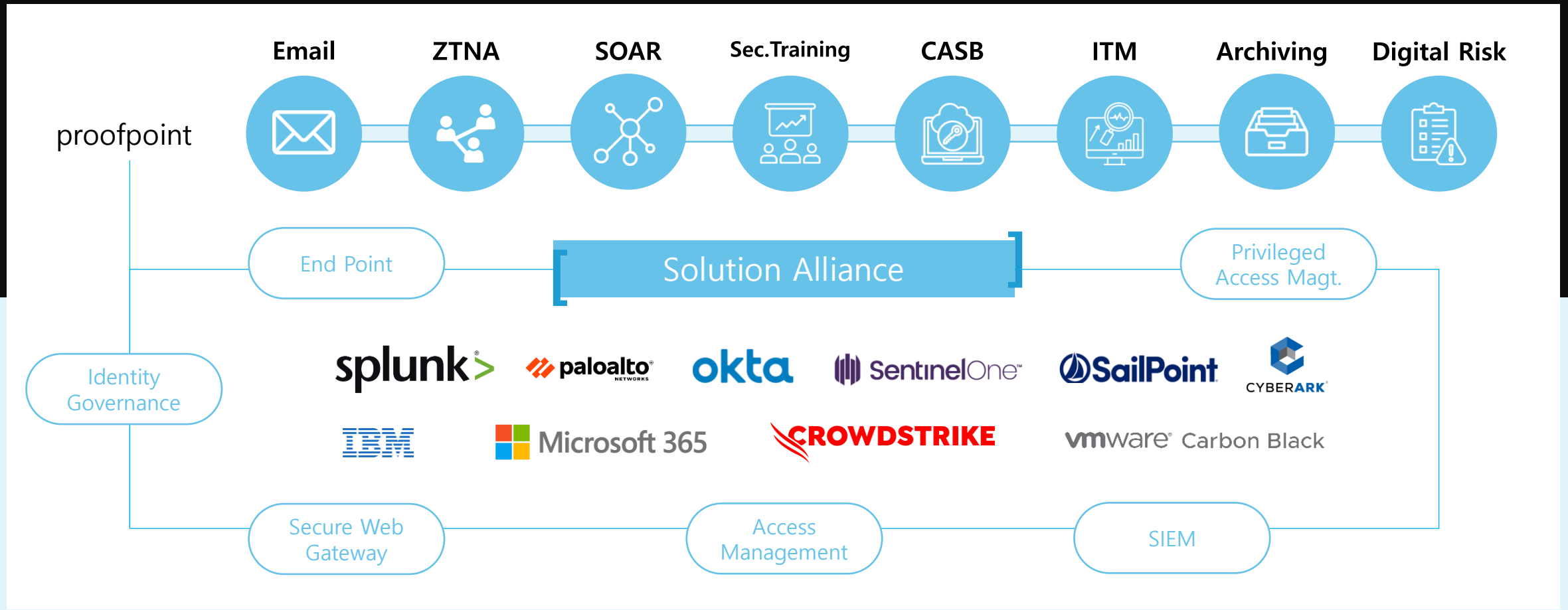
- Existing Browsers
- Easy Deployment

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

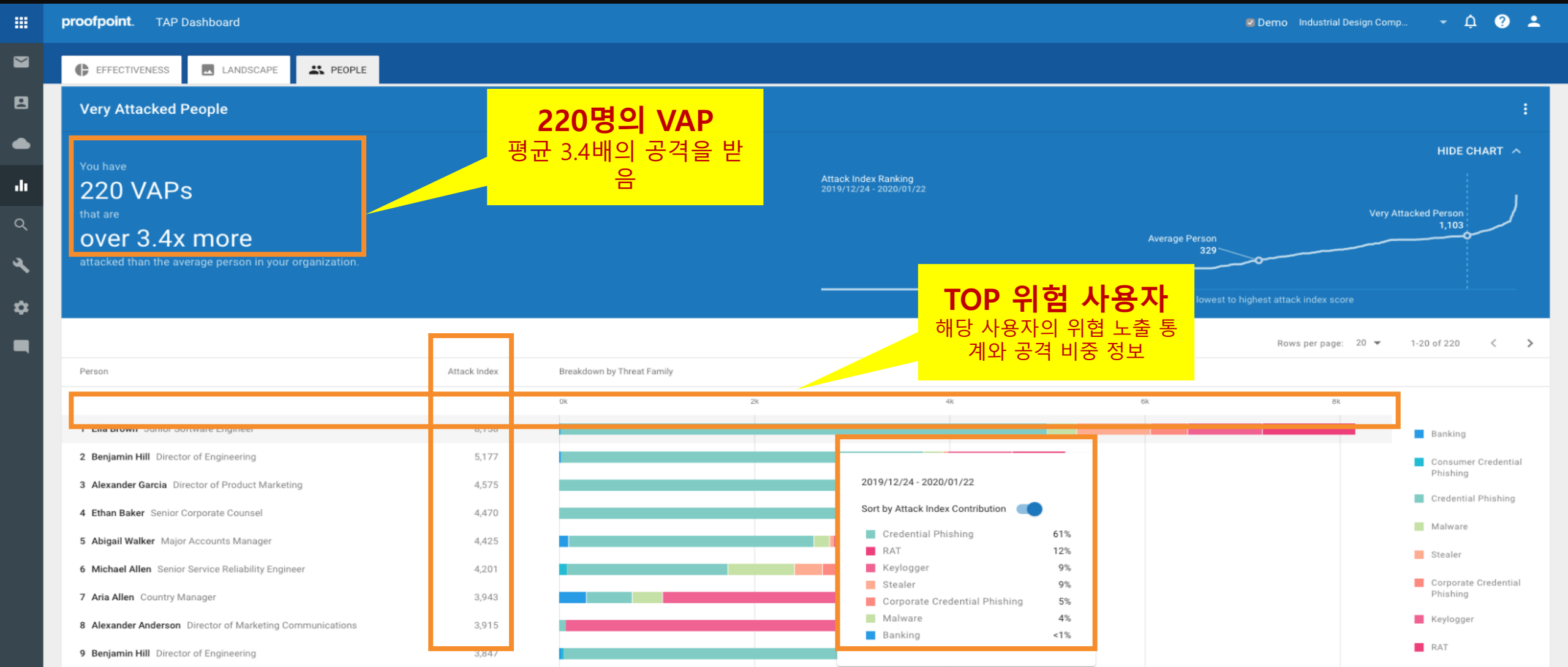
- Policy-based Browsing
- Anonymized

Demo-Isolation

04 Eco System 통합을 통한 보안 운영 효율성



04 Proofpoint TAP – 사람 중심의 위협 가시성



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

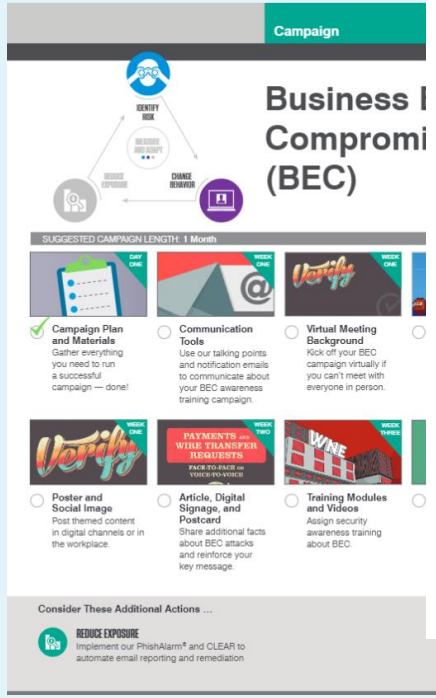
- 이메일 사기란 무엇입니까?
- 보안 강화를 위한 60초: BEC란?

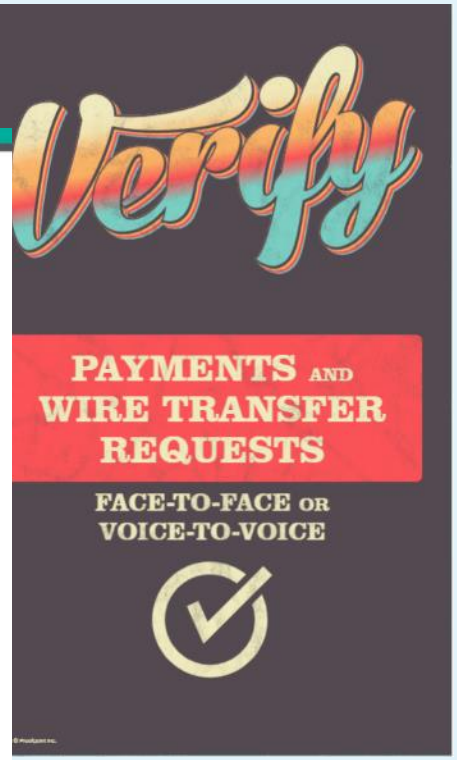
15+ Posters, Infographics, Newsletters

지식 평가 및 피싱훈련

Pre-defined Assessments in Cyberstrength

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





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.

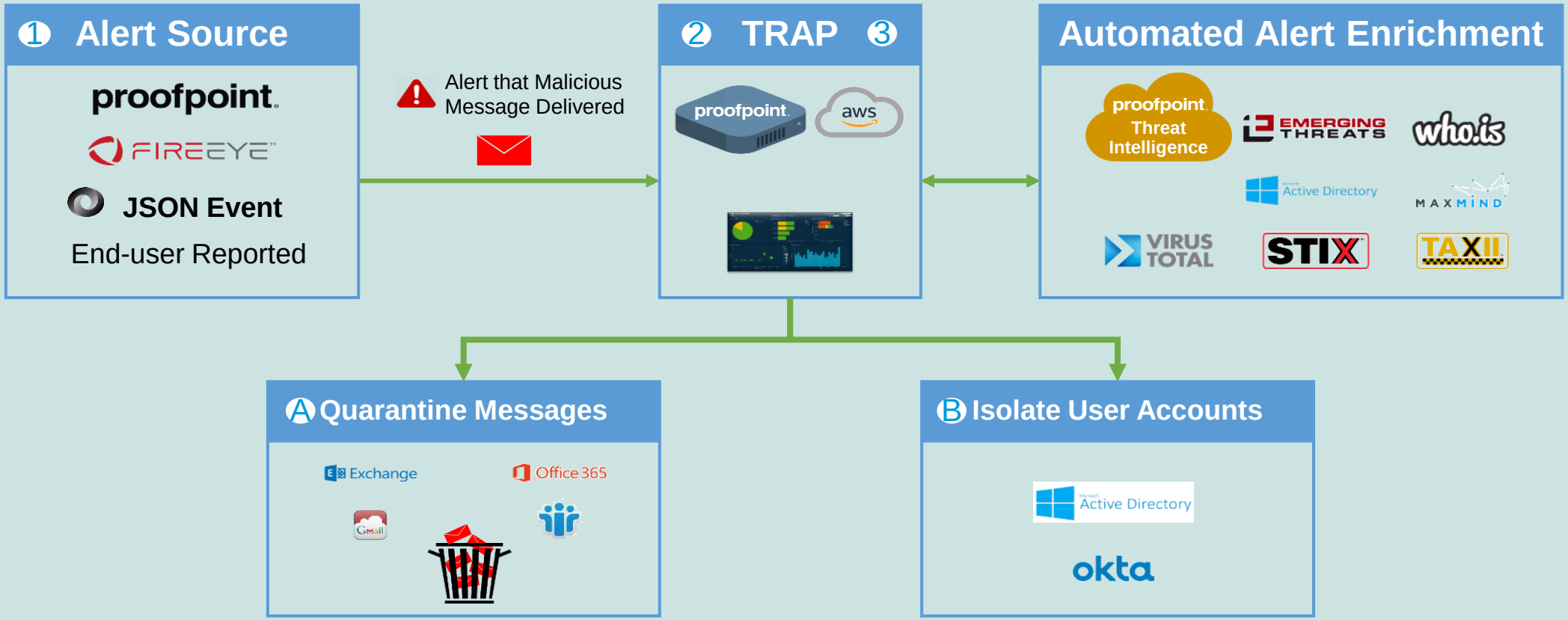
05

TRAP Threat Response Auto Pull

S.Pin Technology

05 TRAP 소개

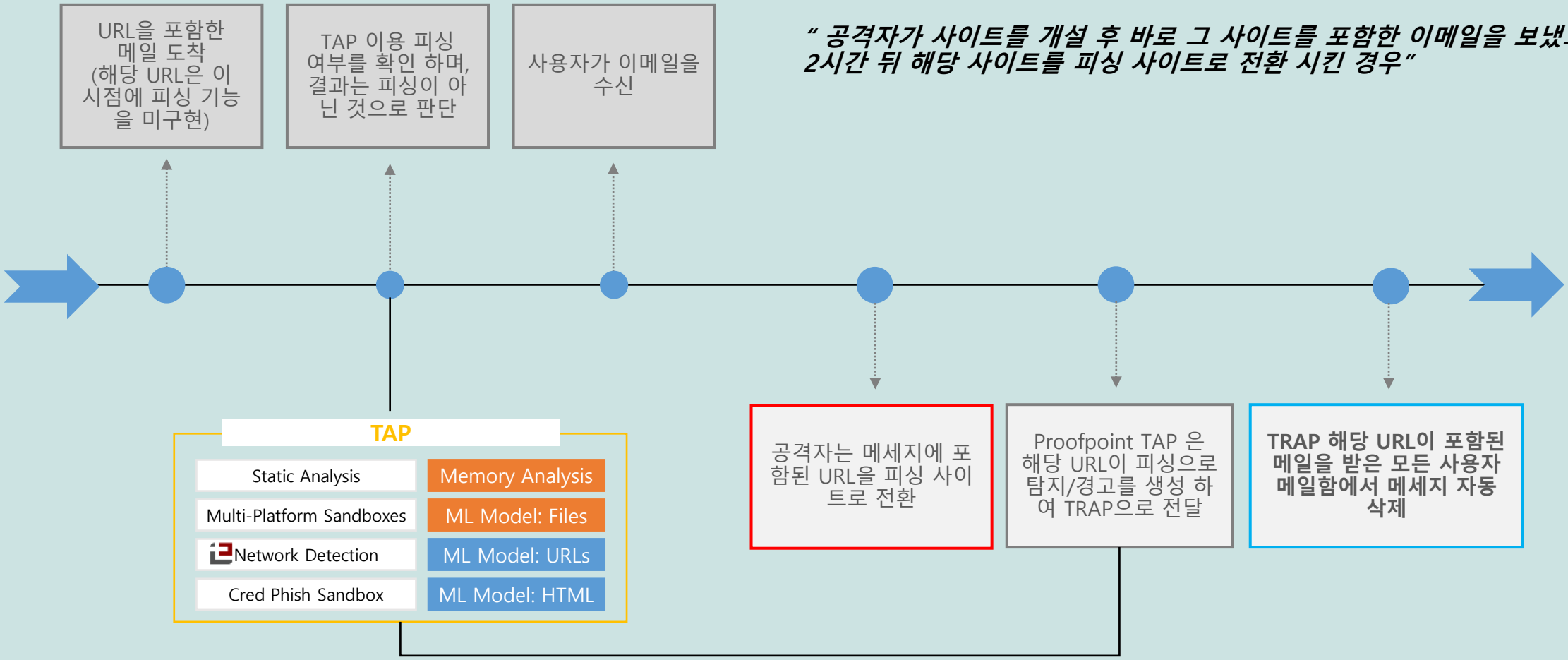
Retroactive 경고를 통해 메시지 자동 삭제



05 TRAP 소개

Use Case

" 공격자가 사이트를 개설 후 바로 그 사이트를 포함한 이메일을 보냈으며, 2시간 뒤 해당 사이트를 피싱 사이트로 전환 시킨 경우"



proofpoint.

06

Email Fraud Defense – Outbound BEC 대응

S.Pin Technology

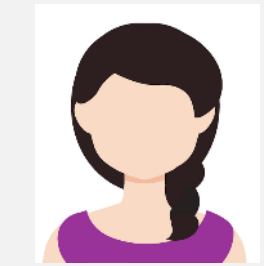
06 Outbound BEC

이메일 인증 – 기업 브랜드 보호

브랜드 이미지 실추

조직의 고객, 파트너 대상 BEC

Outbound BEC



파트너, 고객

elim.net 사칭

- 도메인 스푸핑
- 유사 도메인
- Display Name 스푸핑

06 Outbound BEC

SPF, DKIM 의 한계

Envelope

Sender : **admin@attacker.com** → *"SPF/DKIM 적용 되는 부분"*
Recipients : smith@example.com..

Content

To : smith@company.com
Cc : John@product.com
From : **admin@hometax.com** → *"사용자에게 보이는 부분"*
Subject : 제품소개 → *"실제 공격자가 조작 하는 부분"*

제품 소개 세션을 진행 예정 입니다.

- **SPF Record**

company.com	v=spf1 ip4:115.219.112.0/18 ~all

- **DKIM Record**

company.com	v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0toCYOI LnC+7da9GwtlAqvsso9ojZKXAD/NDWlMSFVghxFAyoPRandeRhDsjQgCOKe+ET r4kkNnx2FOd54wWA2XUKbvkYLOgo6ReBLYXEplqxExl9qkStvLocN0aFNNq0eaajj 4M5DMp4mNPvyw07y06bKxwEc/hRtwIDAQAB

*SPF: Sender Policy Framework / *DKIM: DomainKeys Identified Mail

06 Outbound BEC

DMARK 의 필요성

admin@attacker.com ≠ admin@hometax.com

Envelope

Sender : **admin@attacker.com**
Recipients : smith@example.com..

Content

To : smith@company.com
Cc : John@product.com
From : **admin@hometax.com**
Subject : 제품소개

DMARC Alignment

SPF Pass + Envelop from = header from ➔ DMARC Pass
DKIM Pass + Envelop from = header from ➔ DMARC Pass

"결과적으로 도메인 스푸핑 방어 가능"

- **SPF Record**

abc.com	v=spf1 ip4:111.210.112.0/18 ~all

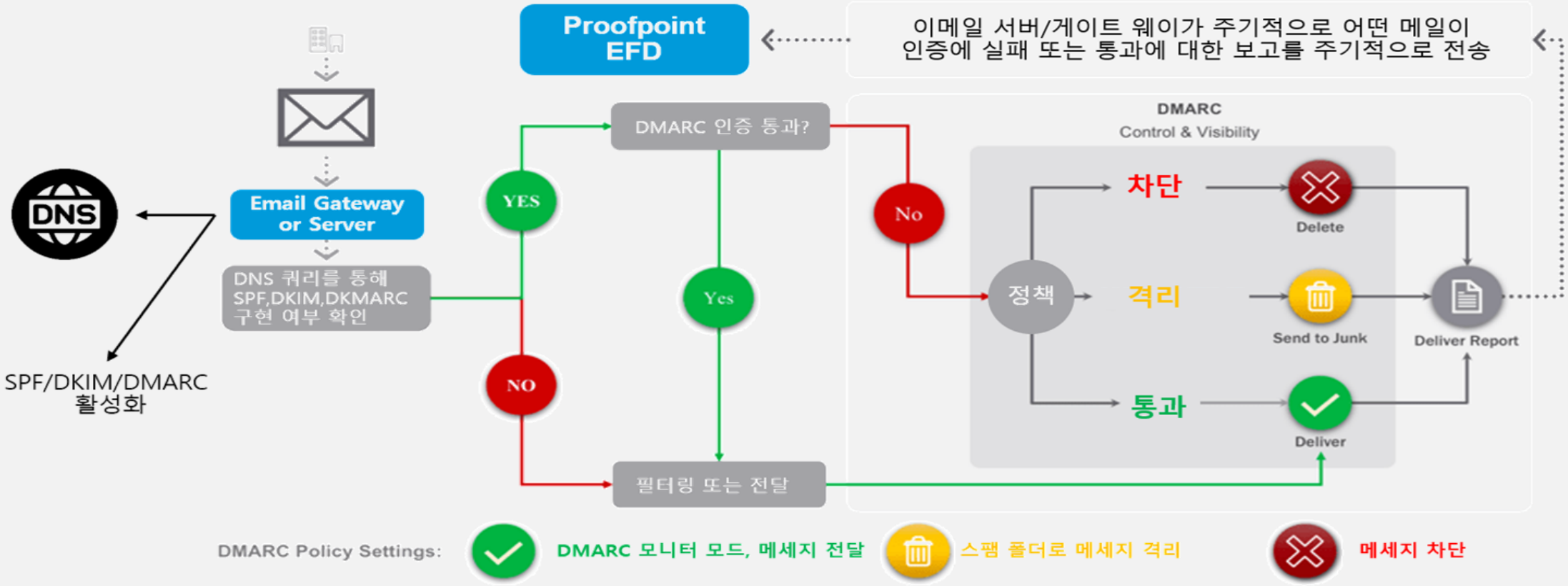
- **DKIM Record**

abc.com	v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7kbM3v WgH/CHgn52Yi+8PlDePfuX3BYfbVNTy8AmIqulqlUp0vLdFQggfhGCROBzqA3F6 PhwH0tBYJ4wVWnv8QF8fBF9+fCr7RMfwv7rB+Ik/tGghHMNBNfNi3LF6sCAiKUV LaPZILK/aW9O5xWnt7rl55LlwE83+wbHVB9SyNQIDAQAB

*DMARK (Domain-based Message Authentication, Reporting&Conformance)

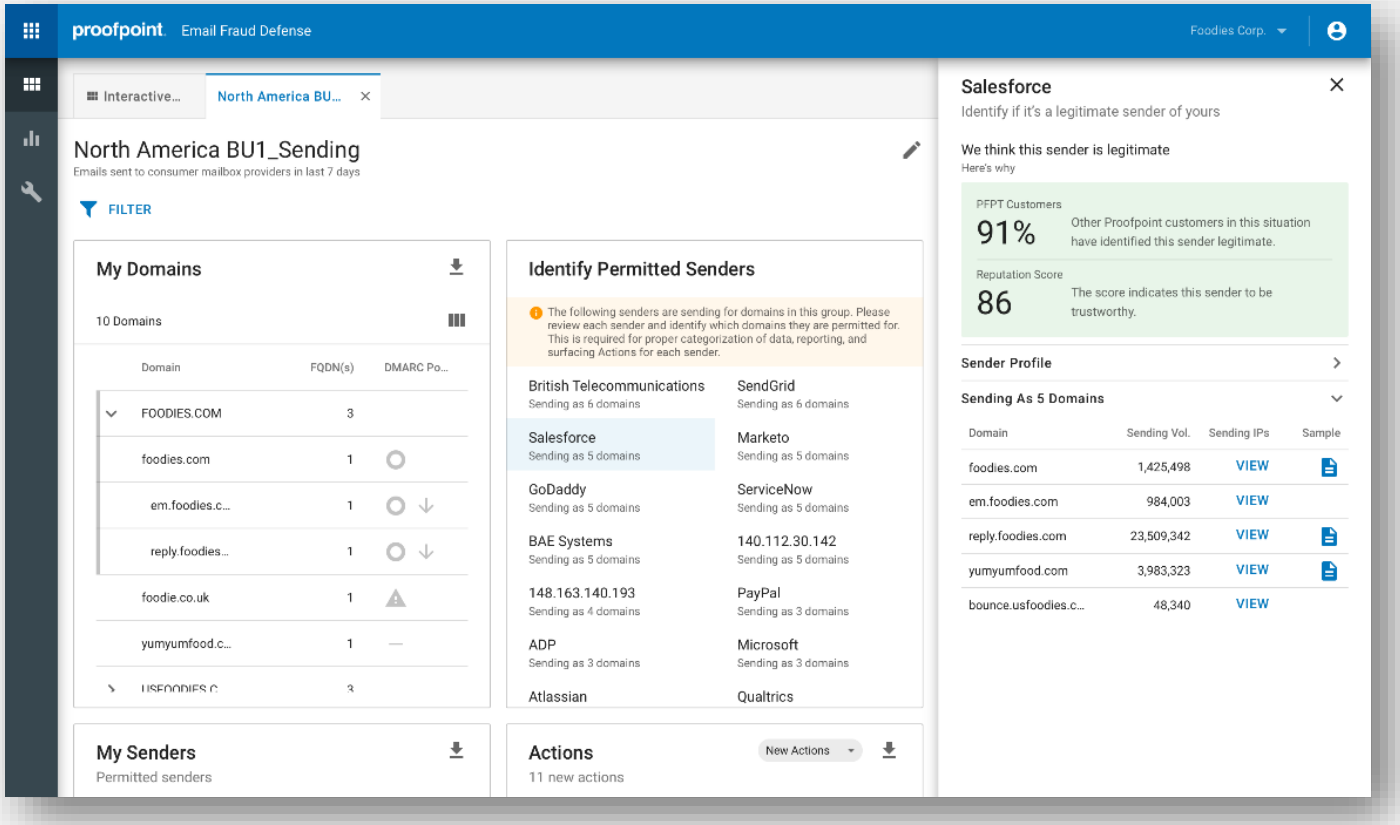
06 Outbound BEC

EFD(Email Fraud Defense) 아키텍처



06 Outbound BEC

이메일 트래픽에 대한 완전한 가시성 제공



- 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

S.Pin Technology

07 Summary

Proofpoint Solution Bundles

P1+

P1

P0

- Email Protection
- Email Warning Tags
- Targeted Attack Protection (TAP)
- TAP URL Isolation (VAP Only)
- TAP SaaS Defense
- Threat Response Auto Pull
- CLEAR

- Security Awareness Training

- Email Fraud Defense (Unlimited)
- Supplier Risk Explorer
- Hosted SPF
- TAP URL Isolation (All Users)
- SPF Hosting

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

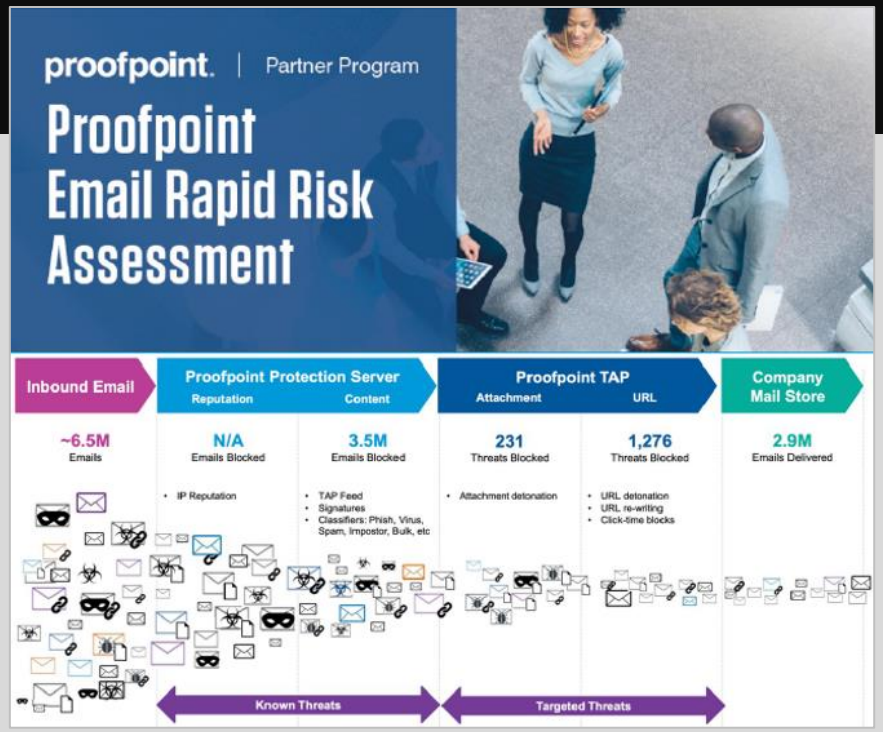
Crowd strike, Paloalto, Cabonblack, Okta, Sailpoint, CyberArk 등과 통합

07 Summary

An Email Rapid Risk Assessment for M365 고객

- Microft365 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
- 지속적인 기술지원 및 개선활동 수행
- 30년+ 전문 총판기술지원체계 노하우
- 전문적 품질관리 지원 조직
- proofpoint 한국지사의 기술지원체계
- 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

paloalto NETWORKS, okta, splunk>, CROWDSTRIKE

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

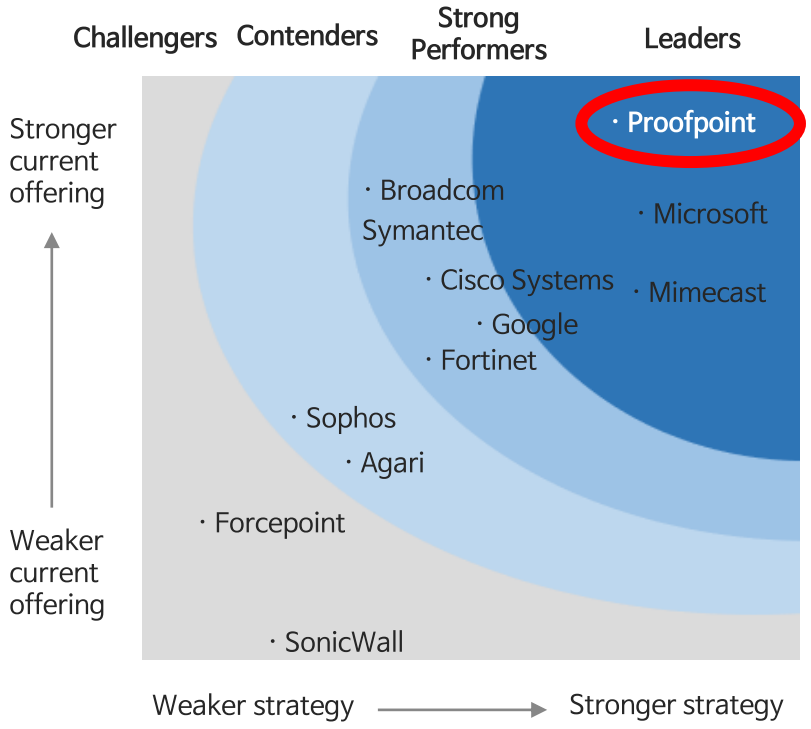
proofpoint

“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

paloalto NETWORKS okta splunk> CROWDSTRIKE



[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

Magic Quadrant 리더십

※ Security Awareness Training
6년 연속 리더

※ Information Archiving
10년 연속 리더

※ Cloud Access Security Broker
Leading Challenger

8,000+
Enterprise Customers

200,000+
SMB Customers

99.999%+
업계 최고의 효율성