

# 모든 인터넷 트래픽을 위협으로부터 검증하는 ETP

Solution Engineer  
김 채하 차장

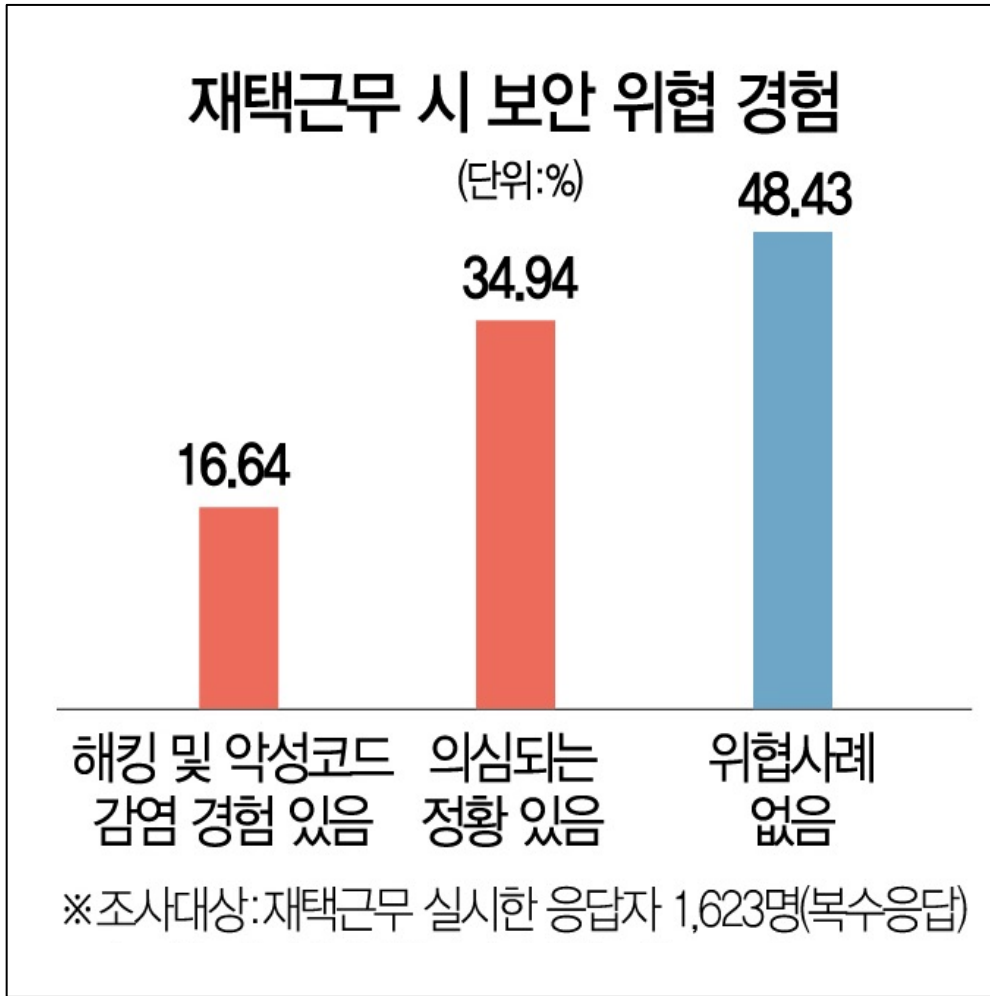




2022년은 어떤 준비를 해야할까?



# 2021 재택근무 보안 위협 트렌드



출처 : 한국인터넷진흥원 사이버 위협 동향 보고서



출처 : 2021년 사이버 위협 시그널 포스터 [이미지=한국인터넷진흥원]



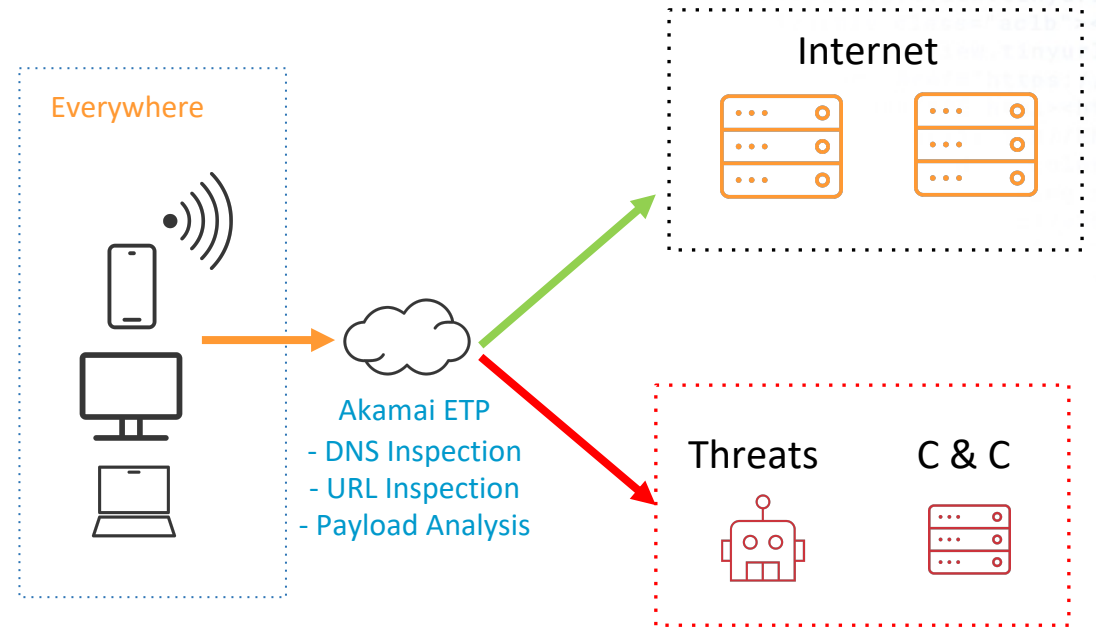
# Akamai Enterprise Threat Protector(ETP)

# ETP

## Enterprise Threat Protector

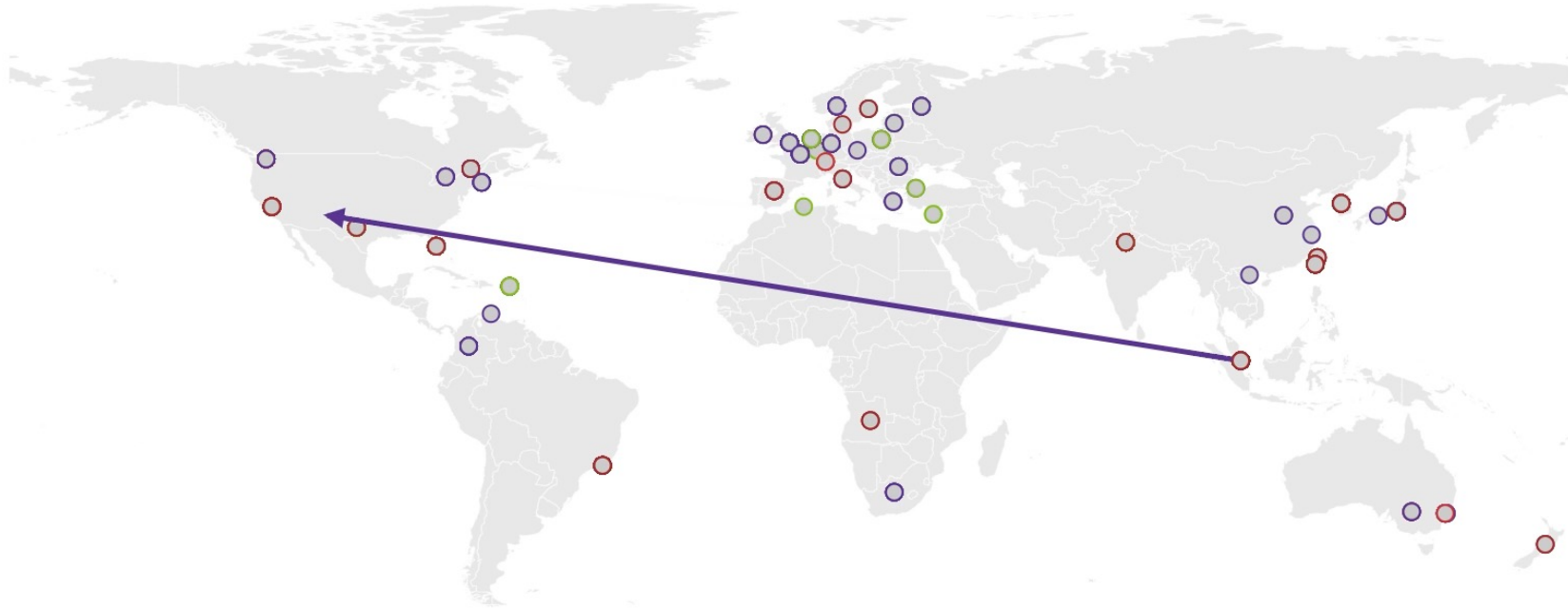
### 기업 직원의 안전한 인터넷 접속 관리

DNS 쿼리 과정부터 Payload 분석까지 지속적으로 변하는 악성 사이트를 선제적으로 탐지하고 차단합니다.



# Akamai ETP 고객대상 위협 트렌드

Enterprise Threat Monitor   피싱  멀웨어  C&C(명령 및 제어)



## 위협 로그

**MALWARE** (245 requests)

**COMMAND & CONTROL** (1 Request)

**MALWARE** (3 Requests)

**PHISHING THREAT** (1 Request)

**COMMAND & CONTROL** (2 Requests)

**MALWARE** (1 Request)

**MALWARE** (1 Request)

**MALWARE** (3 Requests)

# Akamai ETP 고객대상 위협 트렌드

2020년 Enterprise Threat Protector가 차단한 DNS 위협 쿼리

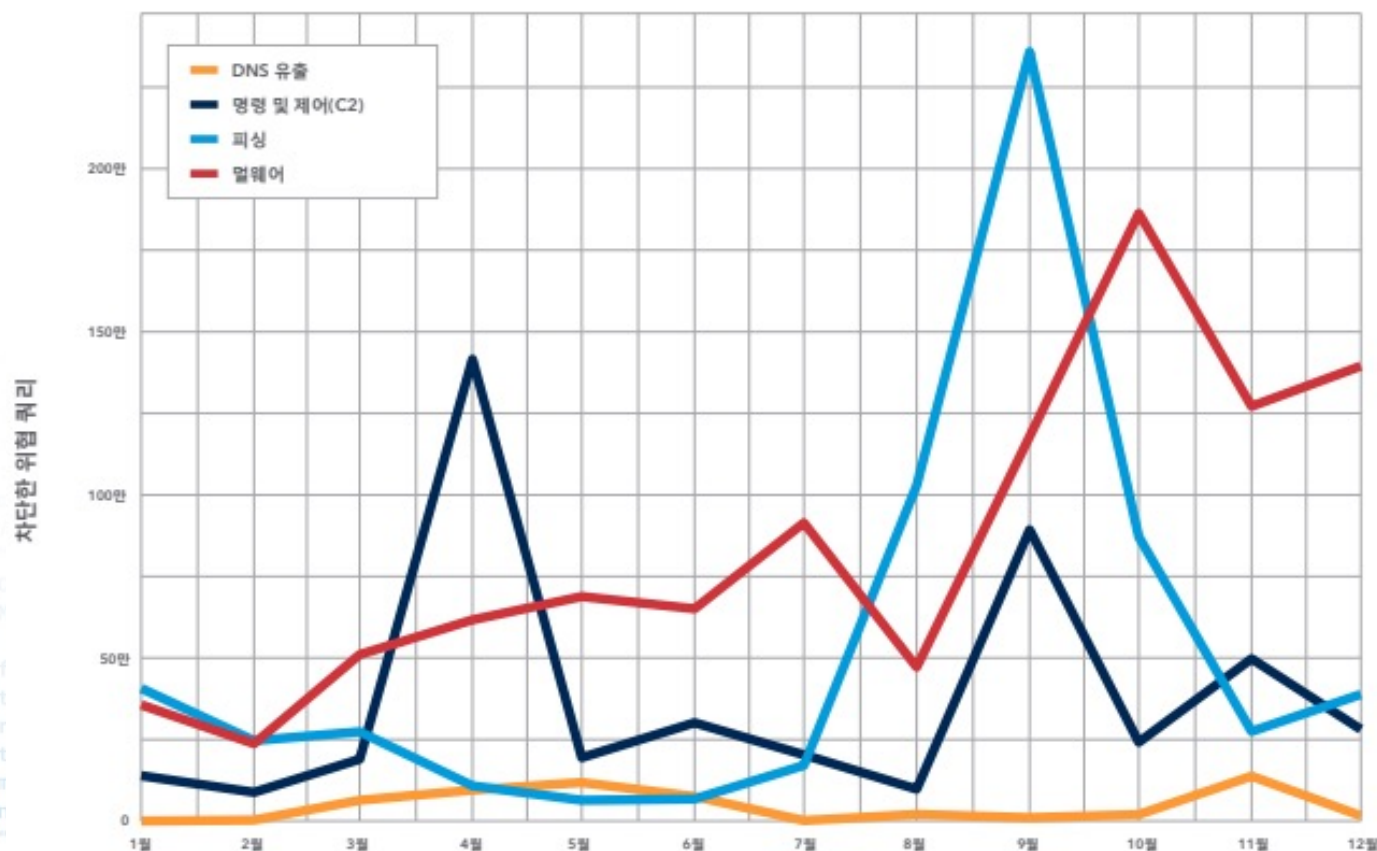


그림 2: 2020년 3분기와 4분기에 피싱 및 멀웨어 공격이 급증했음을 보여주는 Enterprise Threat Protector 로그

Akamai와 관련된 주목할 만한 수치: 2020년 ETP가 차단한 위협



**1091억3000만**  
전체 DNS 처리 건수



**2151만8050**  
차단한 DNS 위협



**454만2524**  
C2



**1015만5209**  
멀웨어

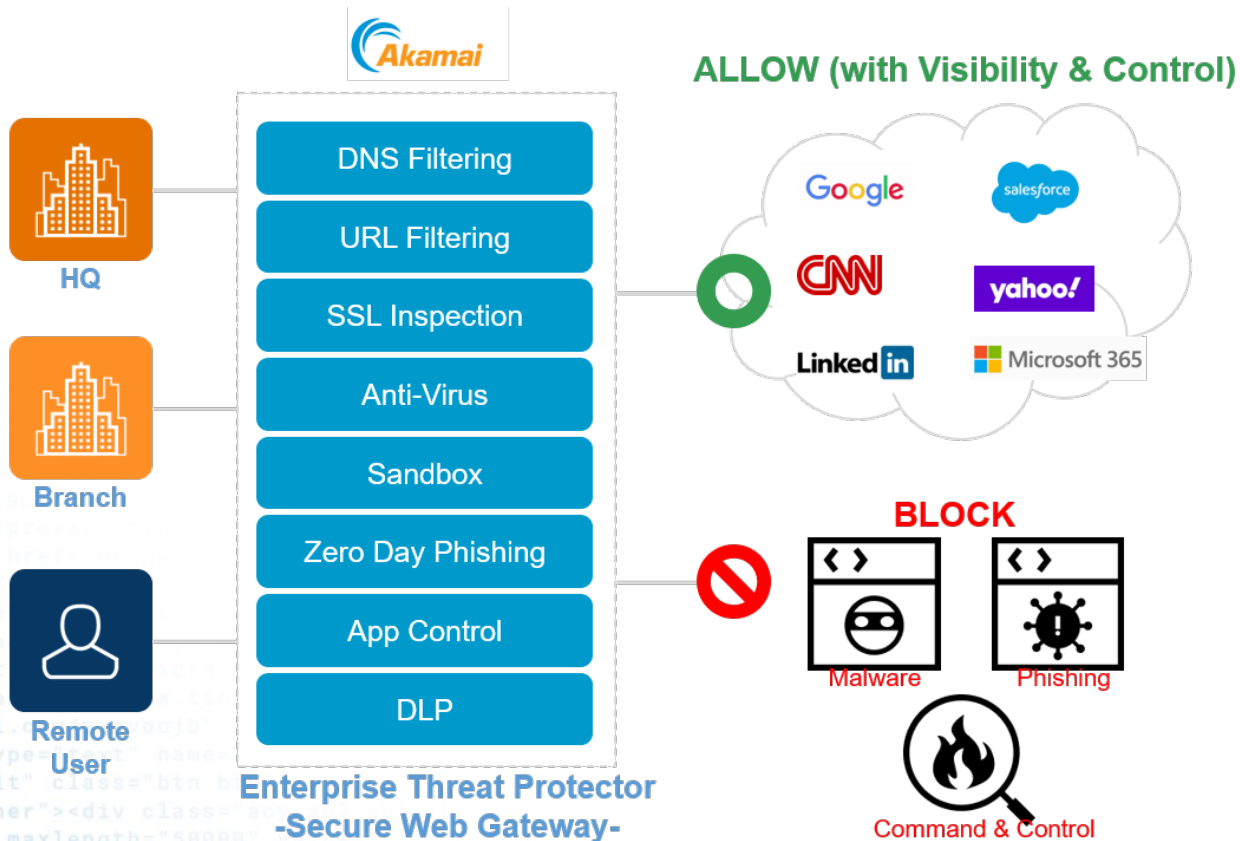


**56만1469**  
DNS 유출



**625만8597**  
피싱

# ETP의 차별성

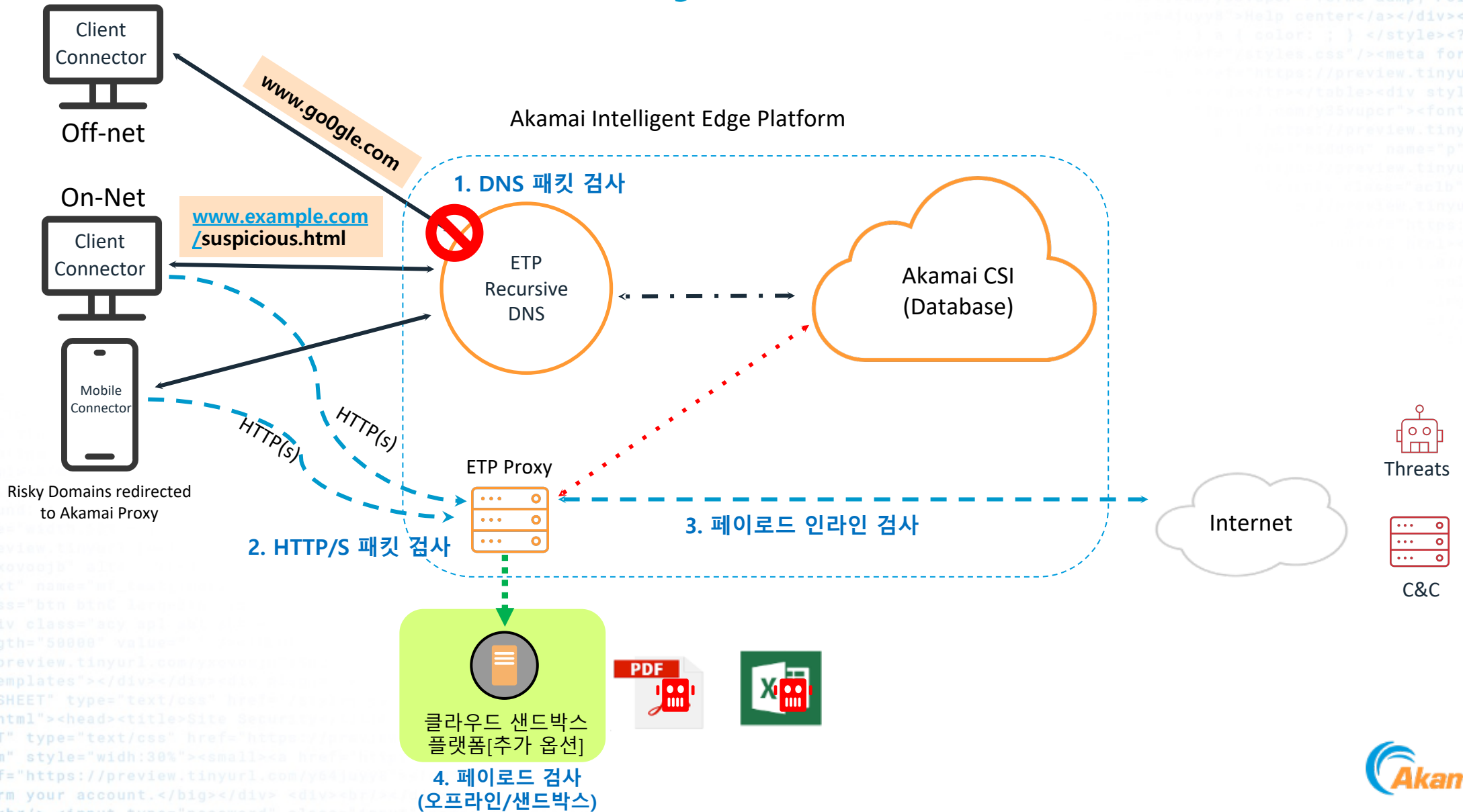


## Akamai 인텔리전트 엣지 플랫폼에서 제공되는 클라우드 DNS & Web 보안 게이트웨이 서비스

- DNS 트래픽을 매일 실시간 AI 분석하여 글로벌 최대 Database 생성 (\*Akamai CSI Intel)
- 사용자 및 단말의 위치에 상관없이 동일한 웹 보안 정책 사용
- 국제 특허 받은 인증된 제로데이 피싱 공격 실시간 방어 엔진
- DLP 지원, 데이터 유출방지 기능 제공 (글로벌 템플릿 제공)



# ETP Secure Web Gateway 워크 플로우





# 요약하면..



## 모든 위치&장치 타입에 단일 보안정책 적용

사내/외부에 상관없이 모든 사용자와 단말을 탐지 및 구분  
기업에서 적용하고자 하는 WEB 관련 보안 정책 적용  
사용자 위치에 따라 단일/차별화된 정책을 유연하게 적용



## 악성 멀웨어 탐지 및 클라우드에서 자동차단

멀웨어, 랜섬웨어, 스파이웨어 등의 악성 스크립트를  
실시간으로 탐지 하여 클라우드 상에서 다운로드 패킷  
차단하여 단말의 감염 원천방지



## 제로데이 피싱 공격 실시간 방어

해커가 사용자를 피싱사이트로 접속하도록 유도하고  
사용자가 접속하여 계정 및 개인정보 유출되는 사고를  
실시간으로 클라우드 상에서 트래픽 차단 및 사이트 접속  
불가



## CnC 서버 접속을 클라우드에서 자동차단

내외부에서 악성 스크립트에 감염되어 외부 해커의 CnC  
서버로 접속을 시도하는 경우, Akamai ETP 서버에서 해당  
트래픽을 흡수 및 자동 차단



## 실시간 Payload 분석 및 악성 웹 패킷 차단

Full SWG(보안 웹 게이트웨이) 모드를 지원하며, 패킷 사이즈에  
따라 인라인/오프라인/샌드박스 등으로 모든 웹 패킷을 클라우드  
상에서 검사 및 차단



## 컨텐츠 및 애플리케이션 기반 유해사이트 차단

사용자가 접속하는 웹사이트의 컨텐츠를 분석하여 접속 차단  
(e.g. 성인물/게임/금융/불법도박 등)  
애플리케이션 기반 분석으로 비인가 패킷(다운로드/업로드) 차단



## 데이터 유출방지 기능 제공(DLP)

악성 멀웨어에 감염된 단말 및 악성사용자가 데이터를 단말에서  
외부로 유출하려고 시도 할 때, DLP 정책을 적용하여 패킷 차단  
(e.g. 개인정보, 신용카드 정보, 금융정보 등)

# 더 자세한 정보가 필요하신가요?

모든 인터넷 트래픽을 위협  
으로 부터 검증하는  
ETP



Akamai ETP 솔루션 문의

korea-marketing@akamai.com

