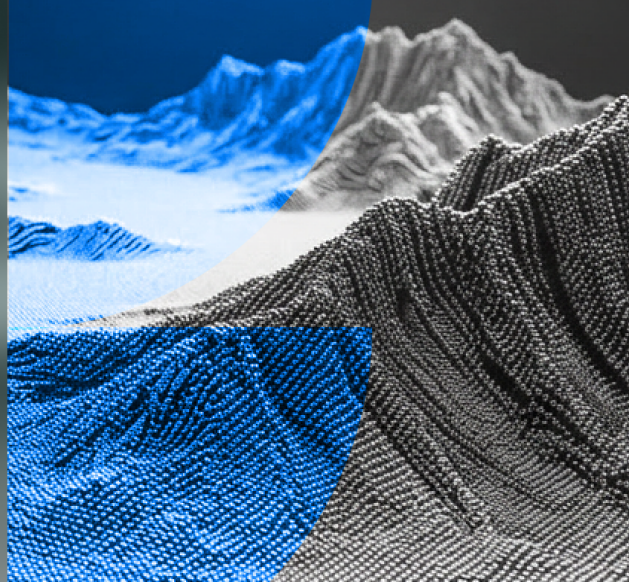
proofpoint.

솔루션 요약

# Proofpoint Core Email Protection

이메일 수명 주기 전반에 걸친 완전하고 지속적인 보호로 AI 확장 이메일 위협 차단



## 주요 이점

- 배송 전에 AI 기반 이메일 위협 차단
- 위협 탐지 효율 99.999%
- API 또는 보안 이메일 게이트웨이(SEG)를 통해 24시간 내에 배포
- 배송 전, 배송 후 및 클릭 시간 모두에 걸친 완전한 보호 제공
- 더 빠른 조사를 위한 통합 Threat Protection Workbench
- 최고 수준의 생태계 통합

## 과제: AI 기반 이메일 위협

공격자는 기계 속도로 반복 공격을 수행합니다. 최첨단 AI는 위협 행위자들이 피싱 미끼, BEC(비즈니스 이메일 사기 공격), 사회공학 캠페인을 빠르게 만들 수 있었던 제약을 제거했습니다. 이제 하나의 캠페인이 각 수신자에게 맞춤화된 무한하고 매우 타겟팅된 변형을 생성할 수 있습니다.

이러한 AI 생성 위협은 오타 없이, 재사용 템플릿도 없고, 익숙한 지문 없이 이메일과 협업 채널을 통해 도착합니다. 평판 목록과 정적 서명에 기반한 전통적인 방어는 따라갈 수 없습니다. 한편, 인간을 대상으로 한 사이버 공격의 94%는 여전히 이메일에서 시작됩니다.[1]

이러한 공격은 사전 배송 보호 기능이 누락된 점, 공급업체 침해 탐지의 사각지대, 분리된 클라우드 및 협업 환경, 계정 탈취 통제 부재 등 보안 허점을 악용합니다.

### AI는 힘을 배가시키는 요인임

공격자가 16시간 걸렸던 일이 이제는 5분이 걸립니다. AI 생성 피싱은 오류 없이 완벽하게 맞춤화된 미끼를 생성합니다.

**무한 변형**
두 개의 동일한 미끼가 없음

**기계 속도**
몇 분 만에 캠페인 실행

**멀티채널**
이메일, 음성 및 비디오

[1] 출처: Proofpoint 위협 연구.

# 솔루션:
# Proofpoint Core Email Protection

Proofpoint Core Email Protection은 이메일 전체 수명 주기에 걸쳐 완전하고 지속적인 보호를 제공하며, AI 기반 이메일 위협을 차단합니다. SEG 또는 API를 통해 배포하면 업계 최고 수준의 99.999% 위협 탐지 효율성을 달성할 수 있습니다.

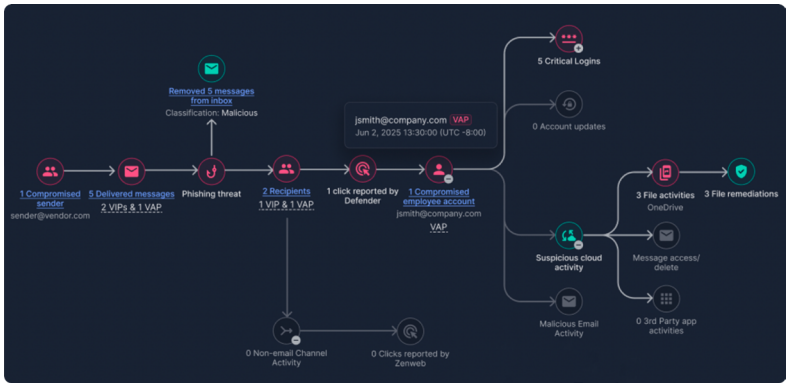



**그림 1.** Threat Protection Workbench는 위협을 종단 간 매핑합니다.

## 핵심 기능:

### Proofpoint Nexus AI 기반 탐지

Proofpoint Nexus는 언어 모델, 관계 그래프, 머신 러닝, 위협 인텔리전스, 컴퓨터 비전을 활용해 AI 의도 기반 탐지를 통해 가장 광범위한 고급 이메일 위협을 탐지합니다.

### Proofpoint Nexus AI

- **LM** — 언어 모델
- **RG** — 관계 그래프
- **ML** — 머신 러닝
- **TI** — 위협 인텔리전스
- **CV** — 컴퓨터 비전

### 독보적인 위협 데이터

| 2.1T | 20.4T | 8,900 | 100+ |
|---|---|---|---|
| 이메일 | URL | 캠페인 | 행위자 |

### 완전하고 지속적인 보호

Proofpoint Core Email Protection은 배송 전, 배송 후 및 클릭 시간 전반에 걸쳐 조정된 방어를 제공합니다. 정보는 실시간으로 각 통제 장치 간에 공유되므로, 배송 후에 드러난 위협이 차기 사전 전달 결정을 더욱 정교하게 만듭니다.


실시간으로 제어 장치 간에 공유되는 인텔리전스

**선택적 추가 기능:**

- 계정 탈취
- 메시징
- 공급업체
- 로그인 시간

### 통합 SEG 및 API 배포

Proofpoint는 시장을 선도하는 SEG와 API 기반 배포를 하나의 통합 아키텍처로 통합합니다. SEG는 이메일 게이트웨이에서 인바운드 및 아웃바운드 위협을 차단하며, API 기반 보호 기능은 내부 메일과 배송 후 위협에 대한 가시성과 대응을 확장합니다.

하나의 콘솔, 하나의 조사 워크플로우, 하나의 정책 세트가 개별 도구를 관리하는 운영 단편화를 대체합니다. 조직은 API를 통해 24시간 이내에 배포하거나, SEG와 API를 결합해 최대 범위를 달성할 수 있습니다.

### 효율적인 보안 운영

위협의 99.999%가 자동으로 차단되면서, 보안팀은 가장 우선순위가 높은 조사에 집중합니다. Threat Protection Workbench는 메시지, 사용자, 클릭, 복구 조치를 하나의 뷰에서 연결하는 시각적이고 종단 간 공격 체인 재구성을 제공합니다. 자동화된 워크플로, 통합 검색, 알림 기반 분류 시스템은 복구까지 평균 소요 시간을 단축합니다.

## 운영 영향

## Proofpoint에서 기대할 수 있는 점은 다음과 같습니다.

### 업계 최고 수준의 탐지 효율성

위협 탐지 효율은 99.999%로, 1,970만 건의 메시지당 1건의 오탐과 530만 건의 메시지당 1건의 미검출이 발생합니다.

### 가치 실현 시간 단축

API 배포는 24시간 이내에 완료됩니다. SEG와 API는 함께 심층 방어를 제공합니다.

### SOC 부담 감소

자동화된 워크플로와 시각적 공격 사슬 조사는 분석가가 수작업으로 상관관계를 처리하는 시간을 줄여줍니다.

### 더욱 광범위한 위협 보호 범위

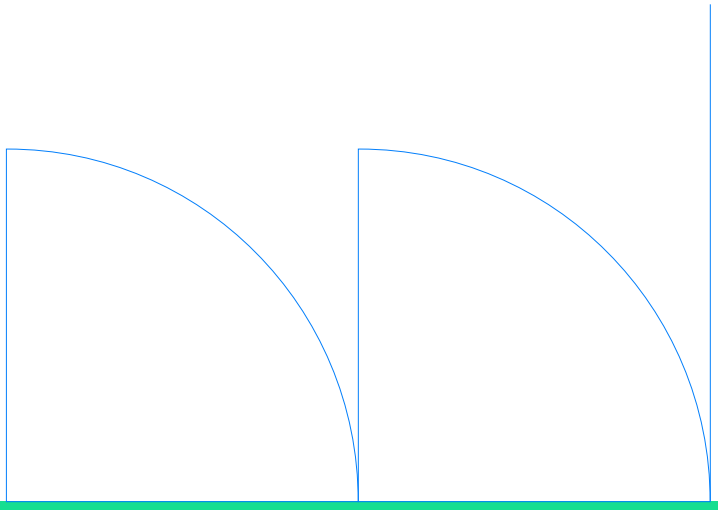
외부 위협, 배송 후 침해, 내부 간 피싱, 직접 전송에 대해 보호를 제공합니다.

### 미래를 대비한 아키텍처

통합 플랫폼은 새롭게 발견된 위협과 신흥 위협 행위자에 대한 자동 보호를 제공합니다.

### 최고 수준의 통합

CrowdStrike, Okta, Palo Alto Networks, Microsoft Defender, Splunk, Sentinel과의 생태계 통합.



자세한 내용은 **proofpoint.com/kr**에서 확인하십시오.



proofpoint.