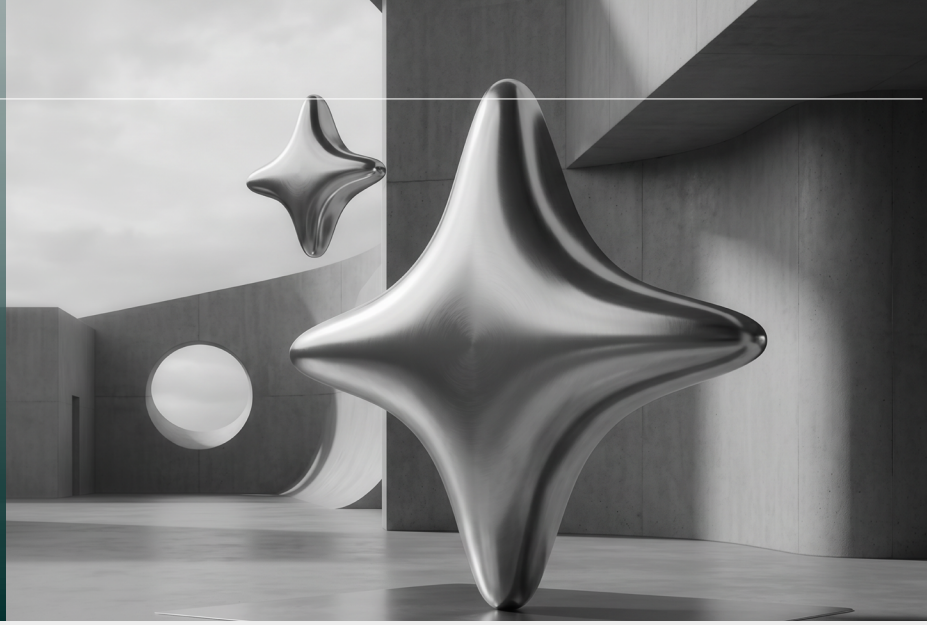
proofpoint



솔루션 요약

Proofpoint의 AI

AI는 사람들이 업무를 완료하도록 도와주는 새롭고 혁신적인 방법을 가능하게 하고 있습니다. 마찬가지로, AI는 위협 행위자가 생산성을 높이는 데에도 도움을 주고 있습니다. 오늘날 위협 행위자의 전술, 기술 및 절차(TTP)는 AI에 의해 증폭되어 세계적인 규모로 다단계, 다채널 공격을 수행할 수 있습니다. 이러한 위협은 종종 기존의 보안 방어를 우회하며 사용자가 스스로 식별하기가 더욱 어려워졌습니다.

동시에 위험은 외부 공격에서만 오는 것이 아닙니다. 데이터 노출은 조직 내 일상적인 사용자 행동에서 점점 더 많이 발생하고 있습니다. AI는 데이터 흐름을 모니터링하고 맥락에 따라 위험한 행동을 식별하는 데 도움을 줄 수 있습니다. 이는 보안 운영 센터(SOC) 팀의 부담을 크게 줄여줄 수 있습니다.

AI가 업무에 미치는 영향이 진화함에 따라, Proofpoint는 고객 보호를 위해 AI를 활용하는 데 있어 업계를 선도하고 있습니다. 지속적인 AI 기반 혁신과 뛰어난 위협 인텔리전스를 결합하여, Proofpoint 솔루션은 위협 행위자보다 앞서 나가고 민감한 데이터를 보호하며 AI가 점점 더 강화되는 세상에서 조직이 안전을 유지하도록 돕습니다.

2025년에 Proofpoint는 고객을 표적으로 하는 이메일 위협 수가 전년 대비

94%

증가한 것을 확인했습니다.

위협 행위자가 AI를 사용하여 공격을 확대하는 방법

Proofpoint는 악의적인 행위자가 AI를 사용할 때 나타나는 영향을 직접 목격했습니다. 2025년에 Proofpoint는 고객을 표적으로 하는 이메일 위협 수가 전년 대비 94% 증가한 것을 확인했습니다. 이는 AI 프롬프트 주입, 이메일 폭탄 공격, 합법적인 서비스 악용 공격을 포함하는 더욱 정교해진 위협 환경으로 이어지고 있습니다.

위협 행위자는 다양한 방식으로 AI를 활용하여 영향력을 확대하고 있습니다.

- **전력 증강.** AI를 통해 위협 행위자는 더 넓은 공격 표면에서 더욱 정교한 공격을 수행할 수 있습니다. 올해 당사는 AI 에이전트를 표적으로 삼아 위협 행위자를 대신하여 행동하도록 유도하는 수천 건의 이메일을 관찰했습니다.
- **진입 장벽 축소.** AI는 공격 사슬의 80~90%를 자동화할 수 있습니다. 이를 통해 위협 행위자는 더욱 복잡한 공격에 시간을 할애할 수 있습니다. 당사는 수천 건의 원치 않는 메시지가 포함된 다단계, 다채널 공격이 증가하는 것을 관찰했습니다.
- **지능형 타겟팅.** AI 이전에는 위협 행위자들이 공격을 위해 예측 가능하고 일반적인 템플릿에 의존했습니다. AI를 활용하여 각 피해자에 대한 개인 맞춤형 공격을 생성할 수 있습니다.

올해 당사는 합법적인 서비스를 악용하는 개인 맞춤형 공격이 증가하는 것을 확인했습니다.

이러한 모든 발전으로 인해 이메일 위협을 정확하게 식별하는 것이 더 어려워졌습니다.

대규모 언어 모델을 기반으로 하는 의미론적 분석과 기타 방법이 도움이 될 수 있습니다.

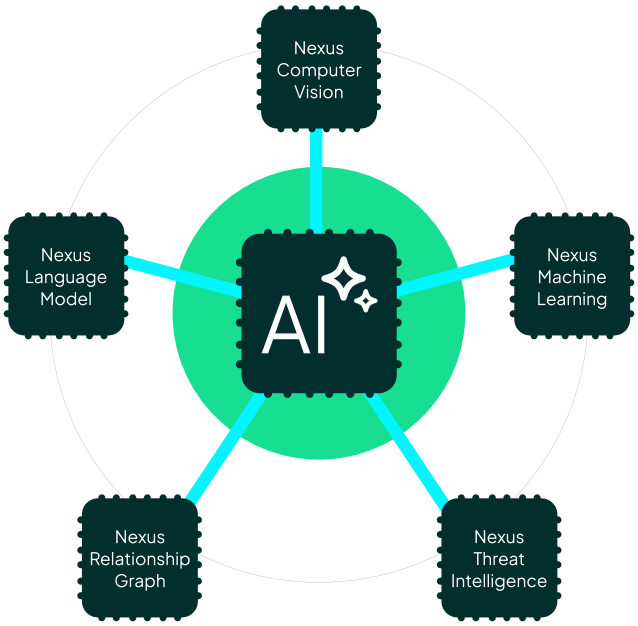
협업 보안을 위한 Proofpoint Nexus AI

Proofpoint의 Collaboration Security Prime 솔루션은 다중 계층 위협 탐지 방식을 사용하는 Nexus™ AI 플랫폼을 활용합니다.

위협 행위자가 AI를 사용하여 공격을 확대하는 방법

Nexus는 99.999% 탐지 효율을 제공하기 위해 함께 작동하는 AI 기반 엔진의 통합체입니다. 이 플랫폼은 머신 러닝, 컴퓨터 비전, 관계 그래프, 위협 인텔리전스 및 언어 모델을 결합하여 공격을 정확하게 탐지하고 차단합니다.

Proofpoint Nexus의 AI 모델은 매년 **2.1조 건의 이메일**을 처리하며, **100개 이상의 고유한 위협 행위자 그룹**과 **8,900개 이상의 위협 캠페인**을 추적하는 위협 인텔리전스 팀의 지원을 받습니다.



Nexus LM™(Language Model)은 고급 언어 분석(트랜잭션 언어, 긴급성, 맥락 및 의도 포함)을 활용하여 숨겨진 위협과 알려지지 않은 데이터 위험을 찾아냄으로써 BEC 및 정교한 피싱 위협을 탐지합니다.

Nexus RG™(Relationship Graph)는 사용자 통신의 미묘한 행동 변화를 식별하여 정상적인 사용자 행동의 편차, 용량 변화, 민감한 회사 데이터 공유를 탐지함으로써 데이터 유출 위험을 줄이고 행동 기반 사이버 위험으로부터 보호합니다.

Nexus TI™(Threat Intelligence)는 실시간 인텔리전스를 사용하여 새롭게 등장하는 공격자의 전술과 시스템 취약점을 식별하고 의심스러운 URL 및 첨부 파일에 대한 샌드박스 에뮬레이션을 트리거함으로써 공격자의 전술을 파악하고 새로운 사이버 위협에 선제적으로 대응합니다.

Nexus CV™(Computer Vision)는 시각 기반 위협을 식별하고 무력화합니다. Nexus Cv는 고급 컴퓨터 비전 기술을 통해 피싱 사이트, QR 코드, 악의적 첨부 파일, 스푸핑된 이메일 등의 시각 요소에 숨겨진 위협을 탐지합니다.

Nexus ML™(Machine Learning)은 감독되는 학습, 감독되지 않는 학습, 조합 방법과 같은 동적이고 적응적인 학습 기술을 사용합니다. 이러한 기술을 알려진 공격 행동을 매핑하기 위한 예측 위협 탐지 기능 및 알려지지 않은 이상 징후를 탐지하기 위한 감독되지 않는 학습 기술과 결합합니다.

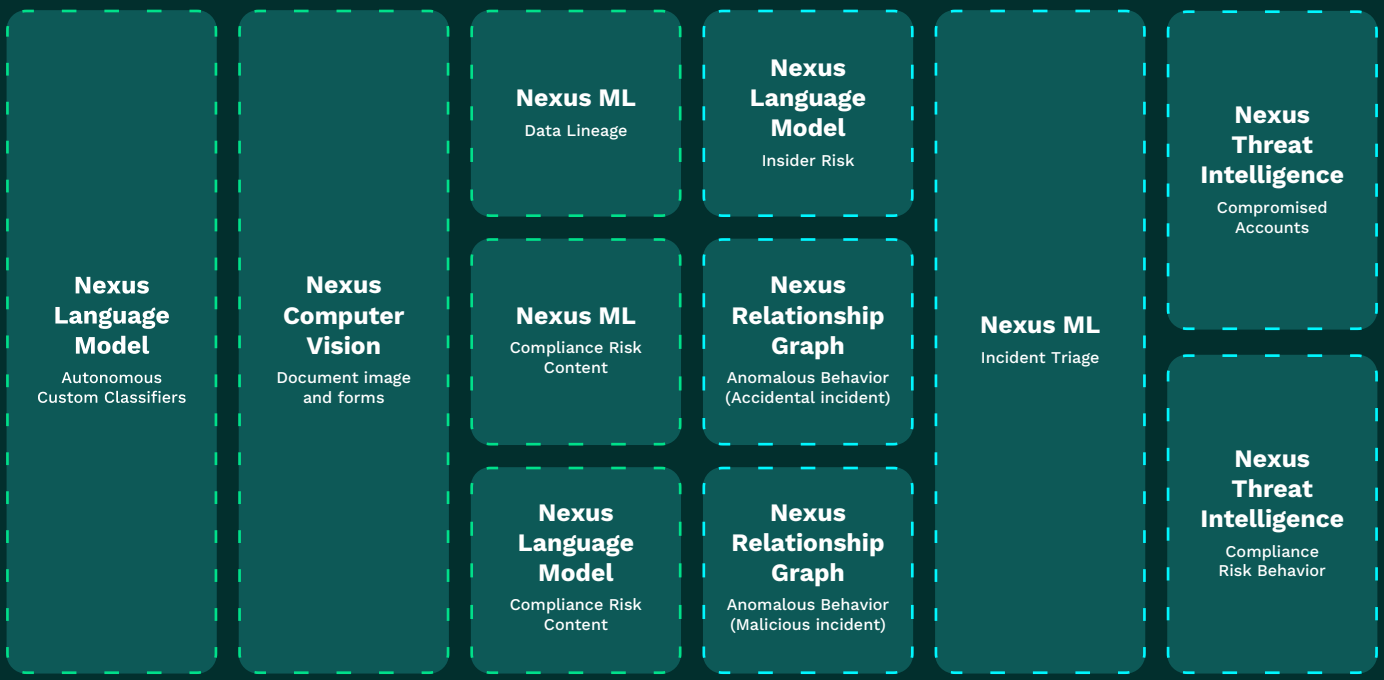
데이터 보안 및 거버넌스를 위한 Proofpoint Nexus AI

Proofpoint는 동일한 업계 최고 수준의 강력한 Nexus 엔진을 사용하여 데이터 보안 및 거버넌스 솔루션을 구동합니다.

데이터 유출 방지를 위한 AI

Nexus는 데이터의 경로와 흐름을 분류하고 추적합니다. 수신자가 조직 내부에 있는지 외부에 있는지는 중요하지 않습니다.

- **Nexus LM™(Language Model)**은 거래 자료, 예측, 제품 설계와 같은 조직의 실제 비즈니스 문서 유형을 학습합니다. 학습된 클래스를 실행 가능한 정책 컨텍스트로 전환하여 수동 조정 없이 민감한 데이터를 신속하게 검색하고 우선순위를 지정하며 보호합니다.
- **Nexus RG™(Relationship Graph)**는 관계를 파악하여 잘못 전달된 이메일 및 데이터 유출 시나리오로 인한 우발적이거나 의도적인 데이터 손실을 방지합니다.
- **Nexus TI™(Threat Intelligence)**는 내부와 외부 모두에서 피싱 이메일을 발송하는 손상된 계정으로부터 보호합니다.
- **Nexus CV™(Computer Vision)**는 이메일과 문서 내의 이미지에 포함된 민감한 콘텐츠를 탐지합니다.
- **Nexus ML™(Machine Learning)**은 파일이 리포지토리와 대상 간에 생성, 복사, 이름 변경, 공유, 이동되는 방식에 대한 엔드투엔드 가시성을 제공합니다. 이 활동을 추적 가능한 출처 타임라인으로 연결하여 더 빠른 조사, 출처 기반 제어, 데이터 보호 프로그램을 위한 감사 대비 증거를 지원합니다.



Proofpoint의 에이전트형 AI

에이전트형 AI 작업 공간과 관련하여 Proofpoint는 두 가지 핵심 영역에 투자하고 있습니다.

1: Proofpoint Satori™ 에이전트

당사는 기존 Proofpoint 솔루션과 통합할 AI 에이전트를 구축하고 있습니다. Satori Agents는 작업을 자동화하고 SOC 팀의 수동 작업을 줄여줍니다.

- **Abuse Mailbox Agent**는 신고된 메시지에 대한 수동 검토를 자동화합니다. 이를 통해 실제 위협과 안전한 이메일을 구분해야 하는 SOC의 부담이 완화됩니다.
- **DLP Triage Agent**는 데이터 손실 방지(DLP) 솔루션에 대한 알림 및 활동 모니터링을 관리합니다.
- **Phishing Simulation Agent**는 AI 자동화를 사용하여 보안 인식 프로그램을 운영하고 인간의 회복력을 강화합니다.

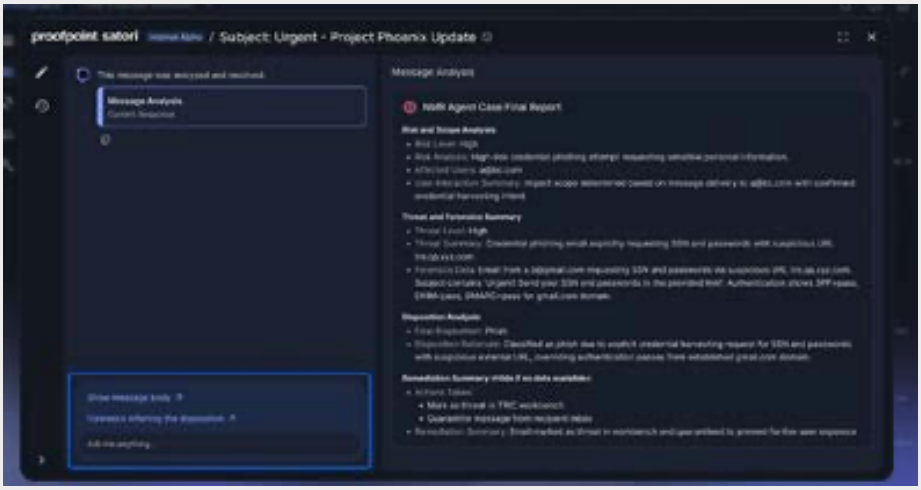


그림 2: Proofpoint Satori Abuse Mailbox Agent 적용 사례.

2: Proofpoint AI Security

Proofpoint는 사용자, 에이전트 및 엔터프라이즈 시스템 전반에 걸쳐 AI가 빠르게 도입되면서 발생하는 보안 위험을 잘 이해하고 있습니다. 따라서 전체 에이전트형 업무 공간을 관리하고 보호하기 위해 Human-Centric Security 플랫폼을 확장했습니다.

Proofpoint AI Security는 모든 AI 상호 작용에서 통합된 가시성, 제어 및 보호 기능을 제공하여 AI 기술을 안전하고 규정을 준수하며 사용할 수 있도록 보장합니다.

- **기업 전반에서 사용자, 에이전트, 시스템이 AI**와 상호 작용하는 방식을 보호합니다.
- **AI 사용, 에이전트 및 모델 상호 작용 전반에 걸쳐 엔드투엔드 가시성과 거버넌스**를 제공합니다.
- AI 워크플로 내에서 **데이터 유출, 도구 오용, 과도한 접근 권한 부여를 방지합니다.**

proofpoint.