

Proofpoint Impersonation Protection

신뢰할 수 있는 파트너, 고객 및 공급업체와의 커뮤니케이션 보호



주요 내용

- 사칭 위협으로부터 신뢰할 수 있는 비즈니스 커뮤니케이션 보호
- 사칭 남용으로부터 고객 및 고객 브랜드 보호
- 악의적 유사 도메인 모니터링 및 폐쇄
- 위험한 공급업체 탐지 및 방어(손상된 공급업체 계정 포함)
- 애플리케이션, 장치, SaaS 플랫폼 및 AI 에이전트가 귀하를 대신하여 전송하는 보안 이메일
- Nexus® AI, 머신 러닝, LLM 및 행동 분석 기반

대부분의 조직에서는 이메일에 의존하여 비즈니스를 수행합니다. 하지만 공격자들은 신뢰할 수 있는 비즈니스 커뮤니케이션을 가로채는 방법을 알아냈으며, 생성형 AI는 이러한 공격을 더 빠르고 설득력 있게 만들고 규모를 확장하기 쉽게 만들었습니다. 공격자는 귀하의 조직, 브랜드 또는 비즈니스 파트너를 사칭하여 몇 시간 대신 몇 분 만에 신뢰할 수 있는 메시지와 웹사이트를 만들 수 있습니다.

FBI의 인터넷 범죄 신고 센터에 따르면, BEC(비즈니스 이메일 사기 공격)는 매년 수십억 달러의 손실을 지속적으로 발생시키며, 손실액은 매년 계속 증가하고 있습니다. 또한 FBI는 AI를 별도의 위협 요소로 추적하기 시작했으며, 확인된 AI 구성 요소가 포함된 공격으로 인한 BEC 손실액을 수천만 달러로 추산하고 있으며, 이 수치는 실제 규모보다 낮게 평가되었을 가능성이 있다고 경고합니다.

이러한 공격은 종종 스푸핑된 도메인, 유사 도메인, 손상된 공급업체 계정을 포함한 여러 사칭 전술을 결합합니다. 이러한 공격은 신뢰할 수 있는 파트너, 고객 및 공급업체와의 커뮤니케이션을 위험에 빠뜨리고 수신자가 합법적인 메시지와 사기성 메시지를 구분하기 어렵게 만듭니다.

당사는 귀하의 조직과 브랜드가 사칭 악용으로부터 보호받을 수 있도록 총체적이고 다층적인 접근 방식을 채택합니다. 당사는 사용자 생성 및 애플리케이션 이메일을 인증하고, 귀하를 대신하여 전송된 메시지를 보호하며, 위험하거나 잠재적으로 손상된 공급업체 계정을 식별하고, 악의적인 유사 도메인을 모니터링하여 제거할 수 있도록 도구, 기술 및 리소스를 제공합니다.

사칭으로부터 귀하의 브랜드 보호

가장 흔한 사칭 전술 중 하나는 도메인 스푸핑이며, 생성형 AI는 스푸핑된 메시지를 더 빠르게 생성하고 실제 메시지와 구분하기 어렵게 만들었습니다. 적절한 보안 제어가 없으면 공격자는 신뢰할 수 있는 도메인을 쉽게 도용하고 AI를 사용하여 매우 설득력 있는 메시지를 대규모로 작성할 수 있습니다. 이를 통해 공격자는 1년 전에는 존재하지 않았던 속도와 세련됨으로 고객, 파트너, 심지어 직원을 표적으로 삼을 수 있습니다. 이메일 인증은 이러한 공격을 차단할 수 있는 가장 효과적인 방법입니다.

Proofpoint Impersonation Protection은 배포의 각 단계를 안내하여 DMARC 구현을 간소화하고 사용자 및 애플리케이션 이메일을 모두 인증할 수 있도록 합니다. 당사 전문가가 귀하와 협력하여 합법적인 발신자를 식별합니다. 또한 타사 승인 발신자의 이메일을 포함하여 모든 이메일이 제대로 인증되도록 보장합니다.

Proofpoint Threat Protection과 통합하여 인바운드 메시지에 대한 DMARC 인증을 완벽하게 시행할 수 있습니다. 이는 신뢰할 수 있는 도메인을 스푸핑하는 AI 생성 사칭 시도에 대한 방어 계층을 추가합니다. 또한 합법적인 이메일을 차단하거나 허용 목록으로 보안을 훼손하지 않고 DMARC 정책을 재정할 수 있습니다. 이 통합은 인바운드 및 아웃바운드 이메일 트래픽 모두에 대한 가시성을 제공합니다. 제3자가 보낸 이메일과 점점 더 많이 귀하를 대신하여 행동하는 AI 에이전트가 보낸 이메일을 포함하여 귀하의 신뢰할 수 있는 도메인을 사용하는 모든 이메일을 확인할 수 있습니다.

손상된 공급업체 계정으로부터 보호

공격자들은 신뢰할 수 있는 비즈니스 커뮤니케이션을 손상시키기 위해 공급망을 점점 더 많이 악용하고 있습니다. 공격자들은 종종 손상된 공급업체 계정을 사용하여 귀하와 비즈니스 파트너 간의 이메일 스레드를 가로챍니다. 생성형 AI는 공격자가 이전 대화를 연구하고 공급업체의 글쓰기 스타일을 모방하도록 도와 사기성 메시지를 탐지하기 어렵게 만듭니다. 또한 이러한 이메일은 합법적인 공급업체 계정에서 올 수 있고 악성 페이로드가 포함되어 있지 않을 수 있으므로 기존의 인증 및 탐지 제어를 회피할 수 있습니다. 그 결과 상당한 재정적 손실, 데이터 도난, 금전탈취 또는 랜섬웨어가 발생할 수 있습니다.

Proofpoint Impersonation Protection은 잠재적으로 손상된 계정을 포함하여 위험한 공급업체를 탐지하고 방어하는 데 도움을 드립니다. 이 솔루션은 행동 기반 AI, 머신 러닝, 그리고 Proofpoint의 방대한 고객 기반에서 얻은 위협 인텔리전스를 사용하여 공급업체 침해 징후를 찾아내며, 여기에는 생성형 AI를 사용하여 더 설득력 있는 유인책을 만드는 공격도 포함됩니다. 자동 URL 격리와 같은 적응형 제어는 손상된 발송자로부터의 위협에 대한 노출을 줄이는 데 도움이 됩니다. 또한 Proofpoint Threat Protection과 발신자-수신자 관계에 대한 맥락을 결합하여 타사 사고 대응 및 조사를 간소화합니다.

유사 사이트를 포함한 악성 사이트 탐지 및 제거

악의적인 행위자들은 공격을 목적으로 웹사이트를 구축합니다. 일부 악의적인 행위자들은 다른 조직, 브랜드 또는 기관을 사칭하여 귀하의 직원, 고객 또는 파트너가 그들을 신뢰하도록 속이기도 합니다. 다른 악의적인 행위자들은 귀하의 로고, 레이아웃 및 브랜드 경험을 밀접하게 모방하는 도메인과 페이지를 사용하여 귀하의 조직을 모방하기도 합니다. 생성형 AI는 두 가지 유형의 공격을 모두 더 쉽게 생성하고, 더 발견하기 어렵게 만들며, 더 빠르게 확장할 수 있게 했습니다. 악의적인 행위자들은 이러한 사이트를 자격 증명 피싱, BEC, TOAD(전화 지향적 공격 전송) 및 기타 설득력 있는 디지털 공격 수법에 이용합니다.

Proofpoint Impersonation Protection을 통해 당사는 귀하의 조직을 사칭할 수 있는 신규 등록 도메인을 지속적으로 모니터링하며, 잠재적 위험을 평가하는 데 필요한 맥락을 제공합니다.

탐지는 첫 번째 단계일 뿐입니다. 귀하께서 의심스러운 사이트를 당사 Takedown 팀에 제출하시면, 당사가 이를 조사하고 가용한 증거를 수집하며 악의적인 활동을 완화하고 사이트를 제거하기 위해 노력합니다. 당사는 등록 기관, 호스팅 제공업체, 이메일 서비스 제공업체, 차단 목록 파트너 등을 포함한 광범위한 인터넷 인프라 제공업체 및 신뢰할 수 있는 파트너 네트워크와 관계를 유지하고 있습니다.

당사 팀이 귀하를 대신하여 Takedown 프로세스를 관리하므로, 귀하께서 누구에게 연락해야 할지 또는 어떤 문서가 필요한지 결정할 필요가 없습니다. 당사의 Takedown 서비스는 유사 도메인을 넘어 악의적인 하위 도메인 및 URL, 그리고 유사 도메인이 아닌 도메인에 대한 완화 지원까지 확장됩니다.

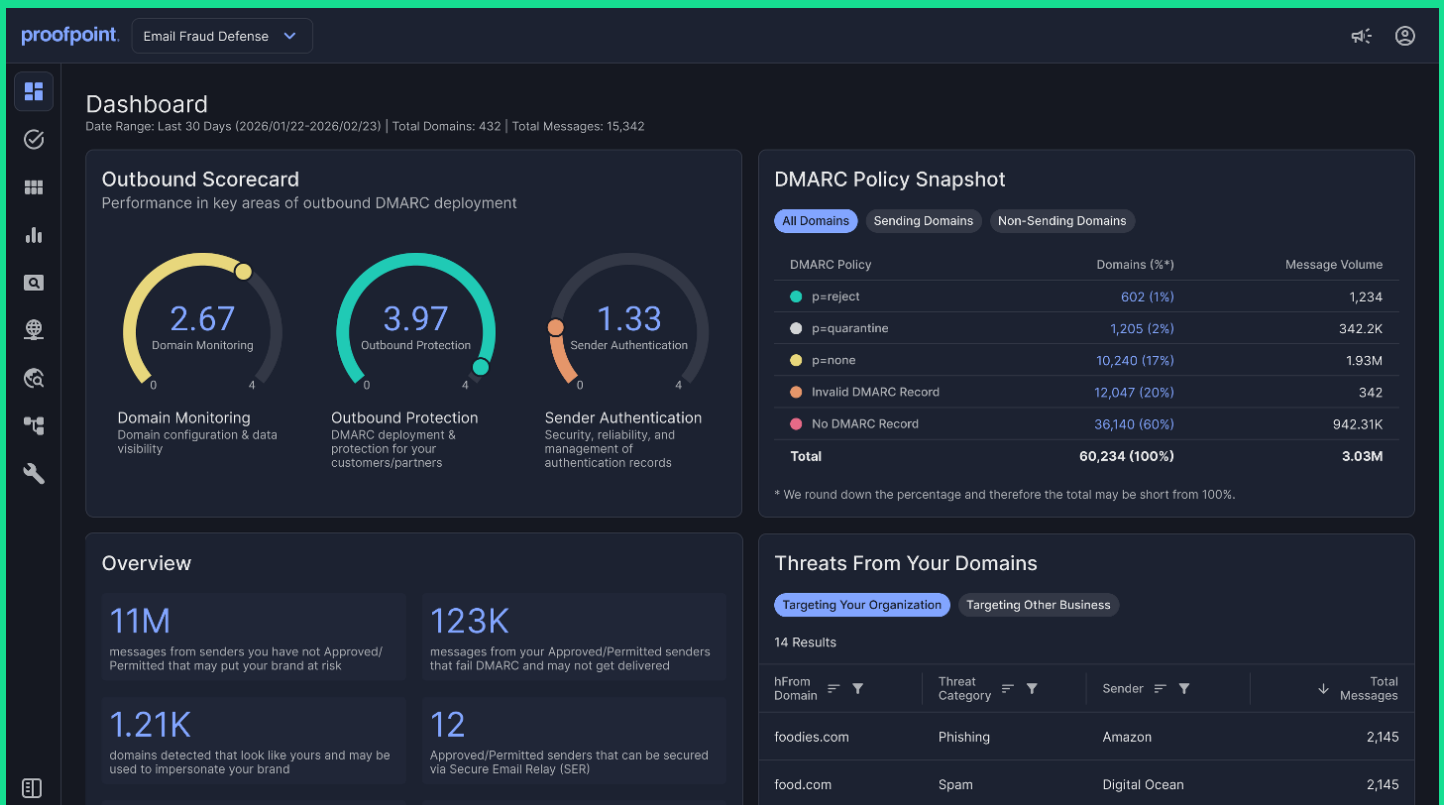


그림 1 Proofpoint는 도메인 스푸핑 위협, 고객 도메인의 악의적인 유사 도메인 및 신뢰할 수 있는 도메인을 사용하여 전송되는 이메일에 대한 가시성을 제공합니다.

귀하를 대신하여 발송된 보안 이메일

귀하의 도메인에서 나가는 모든 이메일이 사람이 직접 작성한 메시지는 아닙니다. HR 플랫폼은 급여 알림을 보내고, CRM 도구는 고객 영수증을 보내며, 사무 장치는 스캔-투-이메일 및 팩스 알림을 보내고, AI 에이전트는 귀하를 대신하여 메시지를 생성하기 시작했습니다. 각 소스는 악용의 통로가 될 수 있습니다. 애플리케이션, 장치 또는 발송 서비스가 손상되면 공격자는 해당 신뢰할 수 있는 채널을 사용하여 귀하가 보낸 것처럼 보이고 인증 확인을 통과하며 생성형 AI로 강화되어 그 어느 때보다 설득력 있게 보이는 악성 이메일을 보낼 수 있습니다.

Proofpoint Impersonation Protection은 내부 앱과 사무용 장치부터 SaaS 플랫폼 및 AI 에이전트에 이르기까지 귀하의 도메인을 사용하는 자동화된 발신자를 위한 안전한 전용 릴레이를 통해 이러한 격차를 해소합니다. 검증되고 인증된 소스에서 메일을 수락하고, 모든 메시지에 고급 스팸 방지 및 바이러스 백신 검사를 적용하며, 승인된 메일에 DKIM 서명을 합니다. 이는 귀하의 아웃바운드 소스가 합법적인 메일 흐름을 방해하지 않으면서 DMARC 정렬 및 SPF 규정 준수를 지원하도록 돕습니다. 또한 SER은 이 트래픽을 신뢰할 수 있는 전용 IP 뒤에 격리하여, 귀하의 도메인이 가진 신뢰에 무임승차할 수 있는 악의적인 행위자로부터 귀하의 발신 인프라와 브랜드 평판을 보호하도록 돕습니다.

가시성, 제어 및 규정 준수 지원 확보

Proofpoint Impersonation Protection은 Amazon SES와 같은 대량 발신 서비스에 대한 중앙 집중식 가시성과 제어 기능을 제공합니다. 귀하는 도메인에서 대량으로 발송되는 내용을 확인하고 메시지를 보낸 애플리케이션, 장치 또는 AI 에이전트를 추적할 수 있습니다. 선택적인 암호화 및 데이터 손실 방지 기능은 트랜잭션 메시지에 포함된 개인 식별 정보 (PII) 및 보호 대상 건강 정보 (PHI)를 포함한 민감한 데이터를 보호하는 데 도움을 줍니다. 이러한 제어 기능은 HIPAA, SEC 및 FINRA 요구 사항과 같은 프레임워크 및 규정 준수를 지원할 수 있습니다.

Proofpoint Impersonation Protection은 또한 대량 발신자를 위한 발신자 신원 및 메시지 무결성에 관한 주요 받은 편지함 제공업체의 요구 사항을 준수하도록 지원합니다. 수신 거부 헤더 및 중앙 집중식 목록 관리에 대한 지원을 통해 합법적인 이메일이 계속해서 받은 편지함에 도달하도록 돕습니다.

자세히 알아보기

자세한 내용은 proofpoint.com/kr을 참조하십시오.

Proofpoint, Inc. 소개 Proofpoint, Inc.는 사람 중심 및 에이전트 중심의 사이버 보안 분야의 글로벌 리더로서 이메일, 클라우드 및 협업 도구 전반에 걸쳐 사람, 데이터 및 AI 에이전트가 연결되는 방식을 보호합니다. Proofpoint는 Fortune 100대 기업 중 80개 이상, 14,000개 이상의 대기업, 그리고 수백만 개의 소규모 조직이 위협 차단, 데이터 손실 방지, 그리고 사람 및 AI 워크플로우 전반에 걸친 회복력 구축을 위해 선택한 신뢰받는 파트너입니다. Proofpoint의 협업 및 데이터 보안 플랫폼은 모든 규모의 조직이 AI를 안전하고 자신감 있게 채택하면서 직원을 보호하고 역량을 강화할 수 있도록 도와줍니다. www.proofpoint.com/kr에서 자세히 알아보십시오.

Proofpoint에 문의하기: [LinkedIn](#)

Proofpoint는 미국 및/또는 기타 국가에서 Proofpoint, Inc.의 등록 상표 또는 상호입니다. 여기에 포함된 모든 다른 상표는 해당 소유주의 재산입니다.