

Proofpoint Impersonation Protection

신뢰할 수 있는 파트너, 고객 및 공급업체와의 커뮤니케이션 보호

주요 이점

- 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)
- 사용자 및 응용 프로그램 이메일을 신뢰할 수 있도록 보호

대부분의 조직에서는 이메일에 의존하여 비즈니스를 수행합니다. 하지만 공격자들은 신뢰할 수 있는 비즈니스 커뮤니케이션을 가로챌 수 있는 방법을 알아냈습니다. 공격자는 고객, 고객 브랜드 또는 비즈니스 파트너를 사칭할 수 있습니다. FBI에 따르면 BEC(비즈니스 이메일 사기 공격)와 같은 사칭 공격으로 인해 기업에서 27억 달러 이상의 비용을 지불했다고 합니다. 손상된 공급업체가 포함된 데이터 유출 비용은 약 500만 달러에 달했습니다.¹

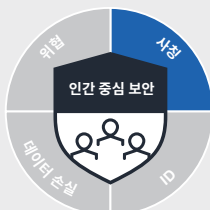
사칭 공격에서 스푸핑된 도메인, 유사 도메인, 손상된 공급업체 계정과 같은 전술이 함께 사용되는 경우도 있습니다. 신뢰할 수 있는 파트너, 고객 및 공급업체와의 커뮤니케이션을 이러한 위협으로부터 보호해야 합니다. Proofpoint가 위협을 완화할 수 있도록 도와드리겠습니다. 사용자 및 응용 프로그램 이메일을 인증하고 손상된 공급업체 계정으로부터 방어합니다.

Proofpoint는 고객과 고객 브랜드를 사칭 남용으로부터 보호하기 위해 총체적인 다중 계층 접근 방식을 채택합니다. Proofpoint는 이메일 인증을 활성화하고 위험하거나 손상 가능성이 있는 공급업체 계정을 식별할 수 있는 도구, 기술 및 리소스를 제공하며, 악의적인 유사 도메인을 모니터링하여 폐쇄할 수 있도록 도와줍니다. 사용자가 생성한 이메일을 보호하는 데 그치지 않고 타사 SaaS 파트너가 고객을 대신하여 전송하는 응용 프로그램 이메일 및 메시지를 처리하는 보안 솔루션도 제공합니다.

사칭 남용으로부터 고객 및 고객 브랜드 보호

가장 일반적인 사칭 전술 중 하나는 도메인 스푸핑입니다. 적절한 보안 제어가 없으면 공격자가 신뢰할 수 있는 도메인을 쉽게 도용할 수 있습니다. 그러면 고객, 파트너 및 직원을 표적으로 삼을 수 있습니다. 이메일 인증은 이러한 공격을 차단할 수 있는 가장

이 솔루션 세트는 Proofpoint의 통합 인간 중심 보안 플랫폼의 일부이며 사람에게서 비롯되는 위협 중 네 가지 주요 영역을 완화합니다.



¹ IBM. 데이터 유출 비용 보고서. 2023.

효과적인 방법입니다. Proofpoint Impersonation Protection은 사용자 이메일과 응용 프로그램 이메일을 모두 인증할 수 있도록 DMARC를 구현합니다. 배포의 각 단계를 안내하여 DMARC 구현을 단순화합니다. 저희 전문가가 고객과 함께 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. 신뢰할 수 있는 도메인을 스푸핑하는 인바운드 위협을 차단하도록 보안 계층을 강화합니다. 또한 합법적인 이메일을 차단하거나 허용 목록으로 보안을 훼손하지 않고 DMARC 정책을 재정의할 수 있습니다. 이 통합은 인바운드 및 아웃바운드 이메일 트래픽 모두에 대한 가시성을 제공합니다. 타사에서 발송한 이메일을 포함하여 신뢰할 수 있는 도메인을 사용하여 발송되는 모든 이메일을 표시할 수 있습니다.

손상된 공급업체 계정으로부터 보호

공격자들은 공급망을 또 다른 위협 벡터로 만들었습니다. 공격자들은 종종 손상된 공급업체 계정을 사용하여 고객과 비즈니스 파트너 간의 이메일 커뮤니케이션을 가로칩니다.

손상된 공급업체의 이메일이 항상 악의적인 페이로드를 전달하는 것은 아니며 인증을 통과합니다. 따라서 탐지하기가 어렵습니다. 엄청난 재정적 손실, 데이터 강탈 또는 랜섬웨어 공격으로 이어지는 경우도 있습니다.

Proofpoint Impersonation Protection을 사용하면 손상된 공급업체 계정을 포함하여 위험한 공급업체를 탐지하고 방어할 수 있습니다. 대규모 고객 기반에서 파생된 행동 기반 AI, 머신러닝 및 위협 인텔리전스를 사용하여 손상 가능성이 있는 공급업체 계정을 선제적으로 파악합니다. 노출을 완화하기 위해, 손상된 공급업체 계정으로부터 URL을 자동으로 격리하는 등과 같은 적응형 제어가 포함되어 있습니다. Proofpoint Threat Protection 및 발신인-수신인 관계에 관한 컨텍스트를 통합하여 타사 사고 대응 및 조사를 간소화합니다.

악의적 유사성 감지 및 제거

다른 일반적인 전술은 유사 도메인으로 수신자를 속이는 것입니다. 여기서 공격자는 합법적인 브랜드 또는 기관과 흡사한 도메인 이름을 등록합니다. 유사 도메인 스푸핑은 자격 증명 피싱, BEC 및 TOAD(전화 지향적 공격 전술)와 같은 공격에서 사용됩니다.

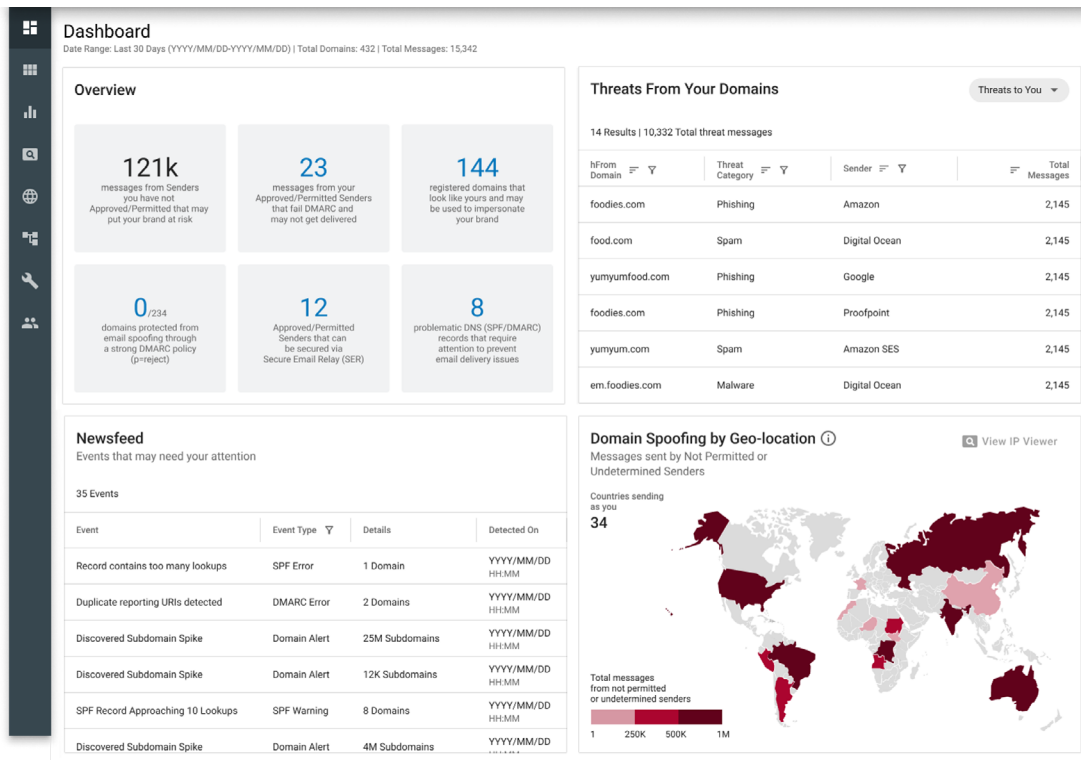


그림 1: Proofpoint는 도메인 스푸핑 위협, 고객 도메인의 악의적인 유사 도메인, 신뢰할 수 있는 도메인을 사용하여 전송되는 이메일에 대한 가시성을 제공합니다.

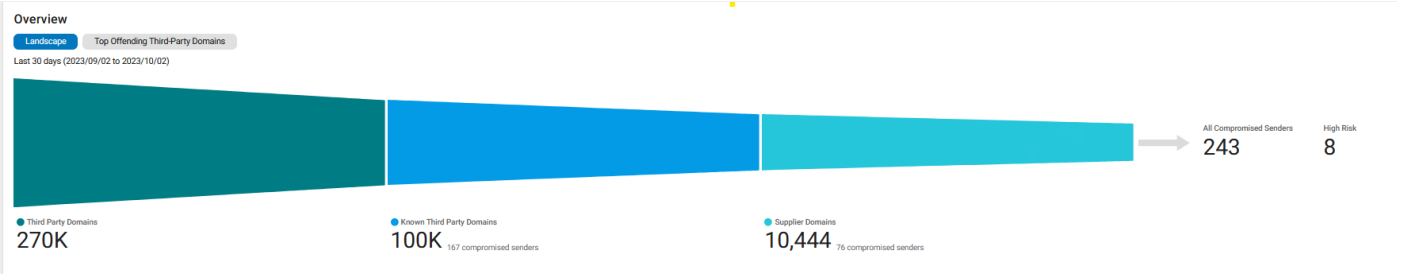


그림 2: Proofpoint는 비즈니스를 수행하는 손상 가능성이 있는 타사 계정을 탐지하고 고위험 공급업체에 대한 가시성을 제공합니다.

Proofpoint는 신뢰할 수 있는 파트너를 흉내 낸 악의적 유사 도메인을 파악할 수 있도록 도와줍니다. 당사는 이메일 공격 또는 피싱 웹사이트에서 고객의 브랜드로 가장한 새로 등록된 도메인을 동적으로 검출합니다. Proofpoint는 의심스러운 도메인을 전체적으로 보여주고 무기화된 사기성 도메인 및 웹사이트를 빠르게 제거할 수 있도록 지원합니다. 고객의 도메인에만 국한되지 않고 공급업체 도메인과 유사한 악의적 도메인을 탐지하는 데에도 도움이 됩니다. 메시지 볼륨과 공급업체의 유사 도메인에서 수신된 메시지를 공개하여 사칭될 수 있는 고위험 공급업체를 선제적으로 처리할 수 있도록 도와줍니다.

고객 이름으로 전송되는 응용 프로그램 이메일 보호

'고객 이름으로' 전송되는 이메일이 제어 권한이 없는 타사 응용 프로그램에서 발송될 수 있습니다. 예를 들어 조직에서는 Workday를 사용하여 직원 급여 관련 이메일을 전송할 수

있습니다. 또한 Salesforce를 사용하여 고객 뉴스레터를 전송할 수 있습니다. 제어하지 않으면 신뢰할 수 있는 도메인을 사용하는 응용 프로그램 이메일이 취약해질 수 있습니다. 타사 응용 프로그램 또는 SaaS 파트너가 손상된 경우 공격자는 고객이 보낸 것처럼 보이는 트랜잭션 이메일에 멀웨어를 주입할 수 있습니다. 최악의 경우 오염된 트랜잭션 이메일이 이메일 인증을 통과할 수 있습니다.

Proofpoint Impersonation Protection은 응용 프로그램 이메일과 고객 대신 발송되는 이메일을 모두 보호합니다. Proofpoint는 신뢰할 수 있는 도메인을 사용하는 트랜잭션 이메일에 보안 및 규정 준수 제어를 적용합니다. 이러한 이메일을 인증하고 업계 최고의 위협 탐지를 적용하여 멀웨어 또는 위협을 찾아냅니다. 그러면 고객, 비즈니스 파트너 및 직원은 인증된 깨끗한 응용 프로그램 이메일만 수신합니다. 또한 타사 응용 프로그램 및 SaaS 파트너의 트랜잭션 이메일을 중앙 집중식으로 제어할 수 있습니다. 고객 도메인을 사용하는 손상된 타사 파트너의 악의적인 응용 프로그램 이메일 트래픽을 언제든지 차단할 수 있습니다.

자세히 알아보기

자세한 내용은 proofpoint.com을 참조하십시오.

Proofpoint 정보

Proofpoint, Inc.는 조직의 최대 자산과 최대 위험인 사람을 보호하는 업계 최고의 사이버 보안 회사입니다. 통합된 클라우드 기반 솔루션 제품군을 통해 Proofpoint는 전 세계 기업이 타겟 위협을 차단하고, 데이터를 보호하고, 사이버 공격에 대한 사용자의 회복력을 강화하도록 지원합니다. Fortune 100대 기업의 85%를 비롯한 모든 규모의 선도적인 조직들이 Proofpoint의 사람 중심 보안 및 규정 준수 솔루션을 활용하여 이메일, 클라우드, 소셜 미디어 및 웹을 통해 전파되는 가장 중요한 위협을 완화하고 있습니다. 자세한 내용은 www.proofpoint.com에서 확인할 수 있습니다.