

Proofpoint Data Security Posture Management

SaaS 플랫폼, 클라우드 인프라 및 온프레미스 환경 전반에서 데이터 검색 및 보호

주요 이점

- AI 분류기는 수동 규칙 없이 SaaS, 클라우드 및 온프레미스 환경 전반에서 민감한 데이터와 비즈니스별 데이터를 식별합니다.
- **Data Risk Map**은 데이터 민감도, 액세스, 비즈니스 영향 및 이동을 기준으로 위험을 우선순위화합니다.
- 비즈니스 인식 액세스 거버넌스는 직접 및 위임된 수정 조치와 DLP 정책 생성을 효율화합니다.
- 내장형 AI 데이터 보안은 AI 애플리케이션 및 AI 교육 파이프라인에 노출된 민감한 데이터를 식별합니다.
- 규정 준수 대시보드는 실행 가능한 보고와 함께 25개 이상의 프레임워크 전반에 걸쳐 상태를 추적합니다.
- 통합 데이터 보안은 DSPM, 액세스 거버넌스, DLP 및 Data Security for AI 전반에 걸쳐 인텔리전스를 공유합니다.

엔터프라이즈 데이터의 폭발적 증가

AI, DBaaS(Database as a Service) 플랫폼 및 클라우드 스토리지의 부상은 SaaS(Software as a Service), 클라우드 및 온프레미스 환경 전반에서 데이터 확산을 가속화했습니다. 민감한 데이터가 시스템과 파이프라인 전반으로 확산됨에 따라 팀은 데이터가 어디에 있는지 파악하는 데 어려움을 겪고 있습니다. 이는 사각지대를 유발하고 노출 위험을 증가시키며 규정 준수를 복잡하게 만듭니다.

사람과 AI에 의한 통제되지 않은 데이터 액세스

데이터 확산은 누가, 그리고 무엇이 민감한 정보에 액세스할 수 있는지에 대한 통제 부족으로 인해 더욱 심화됩니다. 과도한 권한을 가진 사용자, 승인되지 않은 도구 및 위험한 공유는 사람으로 인한 위험을 초래합니다. AI 모델, 에이전트 및 자동화된 워크플로는 새로운 비인간 액세스 경로를 추가합니다. 강력한 거버넌스가 없으면 잘못된 구성, 과도한 권한 및 취약한 감독으로 인해 데이터 유출, 오용 및 규정 준수 위반이 발생할 수 있습니다.

55%

데이터의 21%~40%가 민감하다고 응답한 조직의 비율.

출처: Proofpoint

68%

부적절한 AI 사용으로 민감한 데이터가 노출되었다고 응답한 조직의 비율.

출처: Proofpoint

데이터 검색, 분류, 관리 및 보호

Proofpoint Data Security Posture Management(DSPM)는 팀이 방대하게 퍼진 데이터에 대한 통제권을 되찾고 사람과 시에 의한 위험한 액세스를 줄이도록 돕습니다. 민감한 데이터를 발견 및 분류하고, 누가 무엇에 액세스할 수 있는지 보여주며, 위험 순위를 지정합니다. 팀은 노출을 더 빠르게 수정하고 데이터 보안을 강화할 수 있습니다.

고유한 기능

Proofpoint Data Security의 일부로서, 통합 데이터 액세스 거버넌스를 갖춘 DSPM은 데이터 분류 프레임워크를 Proofpoint Enterprise DLP 및 Proofpoint Data Security for AI와 공유합니다. AI 분류기는 단순한 패턴이 아닌 문맥과 의미를 통해 민감한 문서 범주를 식별합니다. 이는 검색 및 분류 기능을 향상합니다. 또한 팀이 액세스를 관리하고, DLP(데이터 손실 방지) 정책을 생성하며, 클라우드, SaaS, 온프레미스 및 AI 환경 전반에서 데이터를 보호하도록 돕습니다.

DSPM은 과도한 권한, 위험한 액세스, 잘못된 구성, 오래된 데이터 및 공격 경로를 찾아냅니다. Data Risk Map은 민감한 데이터가 어디에 있는지, 얼마나 광범위하게 노출되어 있는지, 어떤 사용자, 앱 및 AI 도구가 액세스할 수 있는지 보여줍니다. 데이터 액세스 거버넌스 워크플로는 대량 및 위임된 수정 작업을 지원합니다. DSPM 결과는 클릭 몇 번으로 DLP 규칙으로 변환할 수 있습니다. 이는 팀이 노출을 줄이고 최소 권한 원칙을 시행하도록 돕습니다.

DSPM은 더욱 안전한 AI 도입을 가능하게 합니다. 코파일럿, 대규모 언어 모델(LLM) 및 AI 앱에 노출된 민감한 데이터를 찾아냅니다.

데이터 액세스 거버넌스, Enterprise DLP 및 Data Security for AI를 포함한 DSPM은 팀이 데이터 수명 주기 전반에 걸쳐 민감한 데이터를 발견, 관리 및 보호할 수 있는 단일 방법을 제공합니다.

비즈니스 중요 문서를 자율적으로 분류

DSPM은 시장을 선도하는 데이터 분류 기능을 제공합니다. 정규 표현식, 자연어 처리 및 LLM을 사용하여 성능을 향상하고 리소스 사용을 줄입니다.

Proofpoint Autonomous Custom Classification(ACC)은 수동 규칙이나 교육 없이도 조직별 문서를 식별합니다. 이는 팀이 독점 데이터를 찾아내고, 사각지대를 없애며, 위험 탐지 및 정책 시행을 개선하도록 돕습니다.

DSPM은 AI 분류기를 기반으로 Microsoft Information Protection(MIP) 민감도 레이블을 적용할 수도 있습니다. 이는 팀이 거버넌스 정책을 시행하고, 규정 준수를 지원하며, 무단 액세스나 오용으로부터 Microsoft 데이터를 보호하도록 돕습니다.

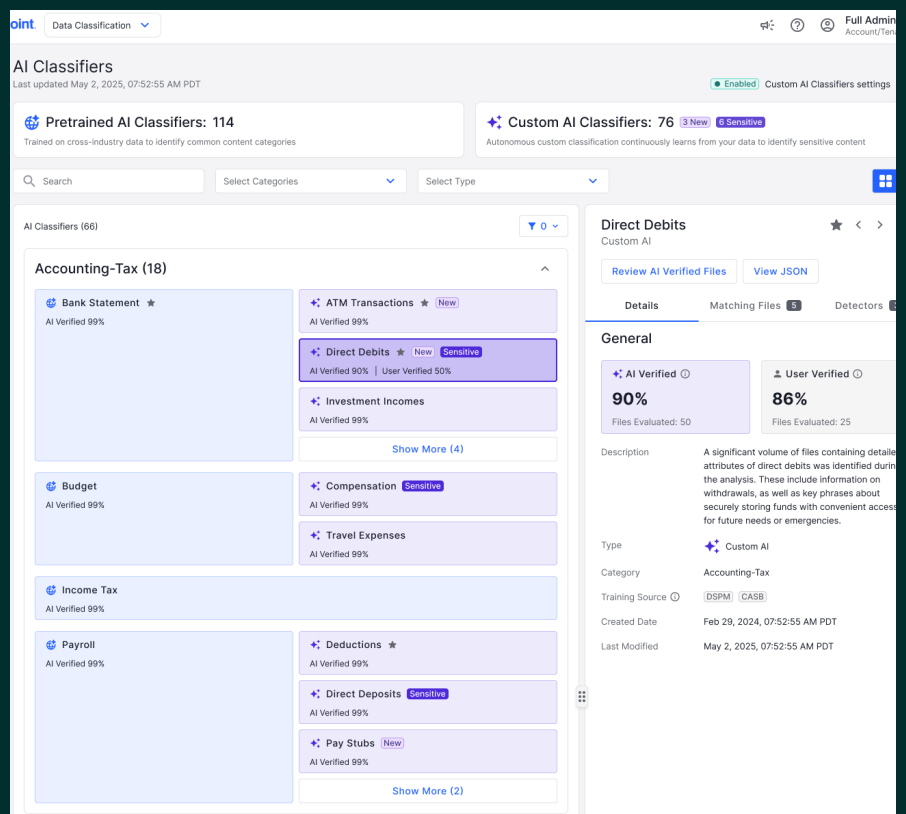


그림 1. DSPM의 사전 학습된 자율 AI 분류기는 계약서, 재무 기록, 소스 코드, 직원 기록을 포함한 표준 및 비즈니스별 문서를 식별합니다.

데이터 액세스 위험 매핑

Data Risk Map은 SaaS 및 온프레미스 시스템에서 민감한 데이터가 어디에 있는지 보여줍니다. 데이터가 얼마나 광범위하게 공유되는지, 그리고 어떤 사용자, 앱 또는 AI 도구가 데이터에 액세스할 수 있는지 보여줍니다. AI 분류와 액세스 및 사용 인사이트를 결합합니다.

보안 팀은 과도하게 노출된 데이터를 찾고, 위험 수준을 매기고, 수정 사항을 검증하며, AI 사용이 증가함에 따라 적절한 액세스 권한을 유지할 수 있습니다. 데이터 위험 결과는 데이터 민감도, 액세스 패턴 및 노출을 고려합니다. 이를 통해 팀은 높은 가치와 높은 위험을 모두 가진 데이터에 집중하는 동시에 비용을 절감하고 기업의 위험 영역을 줄일 수 있습니다.

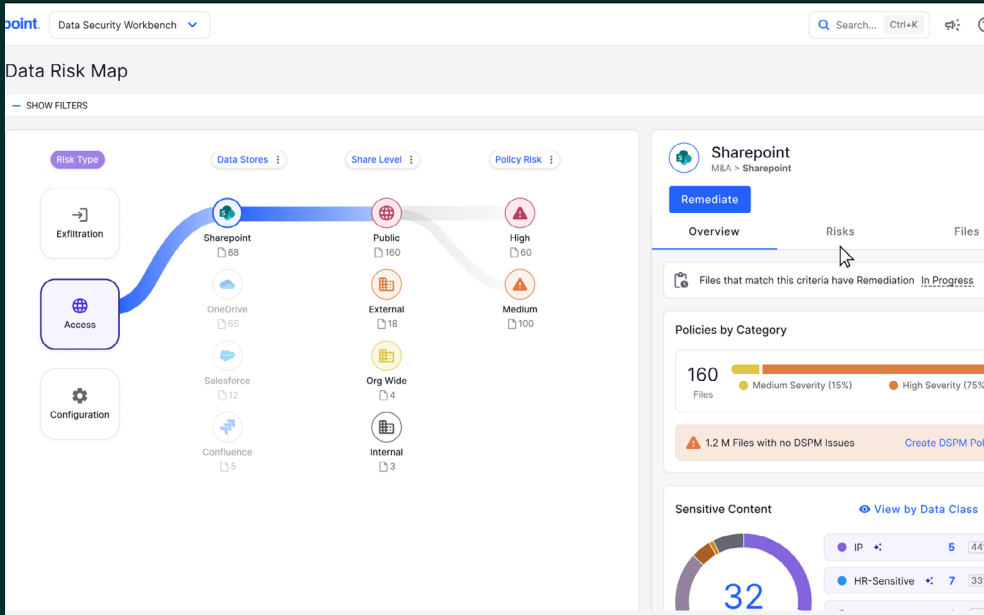


그림 2. Data Risk Map은 민감한 데이터가 포함된 리포지토리, 데이터 공유 범위, 사용자, 애플리케이션 및 AI 도구에 의한 액세스 현황을 보여줍니다.

데이터의 금전적 가치에 따른 위험 우선순위 지정

데이터 보안 팀은 많은 데이터 저장소를 보호해야 합니다. 하지만 모든 저장소가 동일한 가치나 위험을 가지는 것은 아닙니다. DSPM은 데이터 평가 기술을 사용하여 각 데이터 저장소에 대한 유출 비용을 추정합니다. 이를 통해 팀은 가장 중요한 것에 집중할 수 있습니다. 또한 DSPM에는 유해 조합 탐지 기능이 포함된 200개 이상의 사전 구축된 액세스 및 노출 결과가 포함되어 있습니다. 이 위험 매트릭스는 위험도가 높고 재정적 영향이 큰 저장소를 강조합니다.

오래된 데이터 최소화

SaaS 및 온프레미스 시스템에서 DSPM은 최근 액세스되지 않은 파일을 찾아 제거합니다. AI 분류기는 팀이 비즈니스에 중요한 데이터를 필요할 때 보관할 수 있도록 돕습니다. IaaS(Infrastructure as a Service) 환경에서 DSPM은 불필요한 데이터 저장소를 찾아냅니다. 여기에는 오래된 백업 및 스냅샷과 같은 새도우 데이터, 중복 데이터, 방치된 데이터가 포함됩니다.

이는 스토리지 비용을 절감하고, 공격 표면을 축소하며, 데이터 관리를 간소화합니다. 팀은 관련성 있는 활성 데이터만 보관합니다.

최소 권한 액세스 적용

DSPM은 데이터 저장소 전반에 걸쳐 과도한 권한이 부여된 사용자, 미사용

액세스 및 위험한 계정을 찾아 최소 권한 액세스를 지원합니다. 이는 더 강력한 데이터 액세스 거버넌스와 제로 트러스트를 지원합니다.

DSPM은 사람 및 기계 ID에 대한 ID 및 액세스 관리(IAM) 역할, 권한, 데이터베이스 권한 부여 및 기타 액세스 제어를 분석합니다. 실시간에 가까운 속도로 누가 민감한 데이터에 접근할 수 있는지 보여줍니다. 팀은 불필요한 권한을 제거하고 노출을 줄일 수 있습니다.

DSPM은 또한 SaaS 및 PaaS(Platform as a Service) 환경 전반에 걸쳐 제대로 보호되지 않은 계정을 플래그합니다. 예로는 민감한 데이터에 접근할 수 있지만 다중 인증(MFA)을 사용하지 않는 사용자, 비활성 계정, 과도한 관리자 권한을 가진 앱 등이 있습니다.

클라우드 환경의 공격 경로 탐지

DSPM은 클라우드 제공업체 전반에 걸쳐 컴퓨팅 및 네트워킹 리소스와 PaaS 및 SaaS 서비스에 대한 정보를 수집합니다. 해당 리소스의 잘못된 구성과 취약성을 탐지합니다. 그래프는 공격자가 민감한 데이터에 도달하기 위해 사용할 수 있는 경로를 보여줍니다. 실시간에 가까운 모니터링은 팀이 노출을 증가시키는 변경 사항을 발견하도록 돕습니다.

데이터 민감도, 접근 패턴 및 위험에 대한 통찰력은 DLP 및 데이터 탐지 및 대응(DDR) 도구에도 도움이 됩니다.

액세스 직접 관리 또는 위임을 통한 관리

SaaS 및 온프레미스 시스템에서 DSPM 워크플로우는 노출에 대한 통찰력을 실행으로 전환합니다. Microsoft Copilot과 같은 AI 도구가 과도하게 공유된 콘텐츠의 영향력을 확대함에 따라, 불필요한 액세스 권한을 줄이는 것이 중요해졌습니다. 관리자는 Google Workspace 및 Microsoft 365 전반에서 공개 링크, 외부 공유 및 도메인 전체 액세스 권한을 취소할 수 있습니다. 이를 통해 기업 규모의 수정 작업이 가능해집니다.

보안 팀은 모든 파일에 대한 적절한 액세스 수준을 판단할 수 없습니다. 데이터 액세스 거버넌스 워크플로를 통해 보안 팀은 콘텐츠 소유자에게 액세스 검토를 할당할 수 있습니다. 자동화된 캠페인, 알림 및 추적 기능은 거버넌스를 더 쉽게 유지할 수 있도록 합니다.

Enterprise DLP와의 통합은 저장 데이터 이상의 보호 기능을 제공합니다. DSPM에 의해 분류된 민감한 데이터와 우선순위가 지정된 위험은 DLP 정책에 매핑될 수 있습니다. 이는 이메일, 엔드포인트, 클라우드 및 협업 채널 전반에서 일관된 보호와 자동화된 수정 작업을 지원합니다.

IaaS 및 PaaS 환경에서 실행 가능한 인사이트와 권장 사항은 팀이 노출 위험을 신속하게 줄일 수 있도록 돕습니다. 티켓팅, 알림 및 자동화 플랫폼과의 통합을 통해 보안 운영자는 기존 워크플로우를 활용하여 DevOps 및 플랫폼 엔지니어링 팀과 협업할 수 있습니다.

규정 준수 프레임워크와의 정렬 유지

DSPM은 25개 이상의 규정 준수 프레임워크 전반에서 개인정보 보호 및 보안 격차를 찾아냅니다. 여기에는 EU AI 법령, GDPR, HIPAA, NIST, CMMC, SOC 2 등이 포함됩니다.

위반 사항은 프레임워크와 통제 항목별로 태그가 지정되므로 분석가는 규정 준수에 미치는 영향을 확인할 수 있습니다.

보고서는 계정, 리소스 및 프레임워크별 보기와 함께 인프라 전반의 규정 준수 상태를 보여줍니다. 이는 팀이 취약성을 수정하고, 감사를 준비하며, 규정 준수 상태를 유지할 수 있도록 돕습니다.

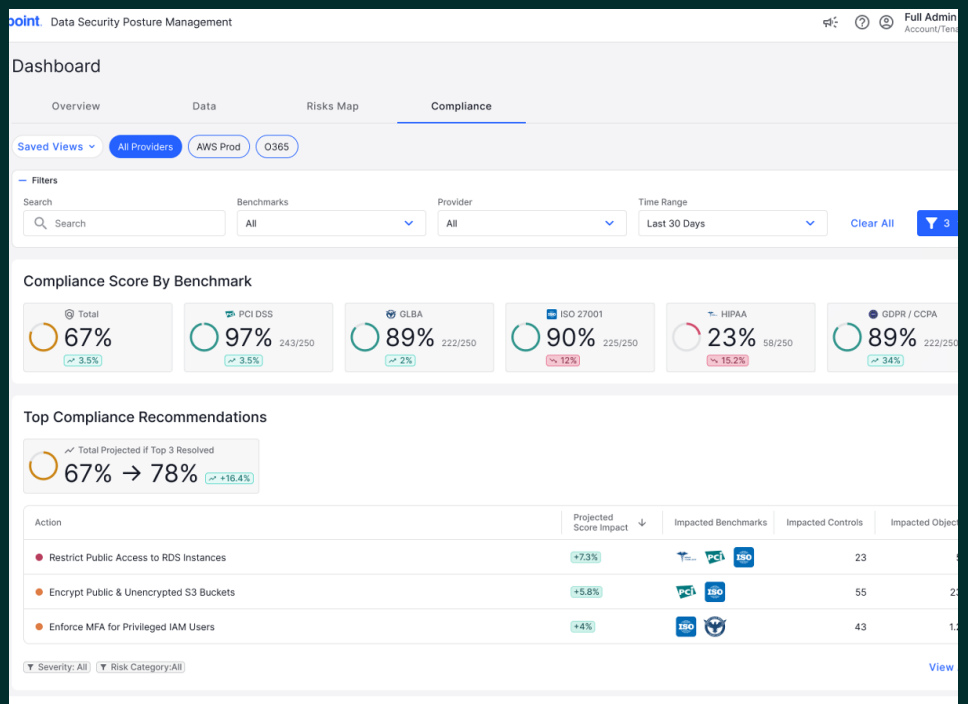


그림 3. 규정 준수 상태를 강조하는 대시보드.

AI 데이터 노출 위험 최소화

DSPM은 AI 앱과 워크플로에 노출된 민감한 데이터를 찾아내어 조직이 AI를 확장할 수 있도록 지원합니다.

Proofpoint DSPM은 노출 인사이트를 Proofpoint Data Security for AI 대시보드에 공급합니다. 대시보드는 승인된 AI 앱과 승인되지 않은 AI 앱 전반의 데이터 위험에 대한 중앙 집중식 보기를 제공합니다. 또한 DSPM은 AI 앱의 잘못된 구성을 모니터링하고 팀이 이를 수정할 수 있도록 돕습니다. 이는 유출 위험을 줄이고, AI 데이터 거버넌스를 강화하며, 안전한 도입을 지원합니다.

DSPM은 AWS Bedrock 및 Azure ML과 같은 플랫폼에서 사용자 지정 LLM

및 AI 앱을 보호합니다. 파운데이션 모델, 사용자 지정 모델 및 검색 증강 생성(RAG) 워크플로에 입력되는 민감한 데이터를 탐지합니다.

또한 DSPM은 LLM 보안을 위한 특수 API를 제공합니다. 이 API는 LLM으로 유입되고 유출되는 민감한 데이터를 실시간으로 분석합니다. 또한 데이터 사용에 대한 거버넌스와 가시성을 제공하며 고객 워크플로와 통합됩니다.

지원되는 플랫폼 및 기술

DSPM은 다양한 플랫폼과 서비스 전반에서 데이터를 검색하고 분류합니다. 관계형 데이터베이스부터 NoSQL 및 키-값 저장소에 이르기까지 광범위한 데이터 저장소를 지원합니다. 이를 통해 팀은 정형, 비정형 및 반정형 데이터에 대한 가시성을 확보할 수 있습니다.

주요 클라우드 및 SaaS 플랫폼을 포괄적으로 지원합니다. 예로는 AWS, Azure, Google Cloud Platform(GCP), Snowflake, Salesforce, ServiceNow, Workday, LLM 및 코파일럿 등이 있습니다.

공통 검색 및 분류 프레임워크를 통해 Proofpoint는 새로운 데이터 저장소 지원을 신속하게 추가할 수 있습니다.

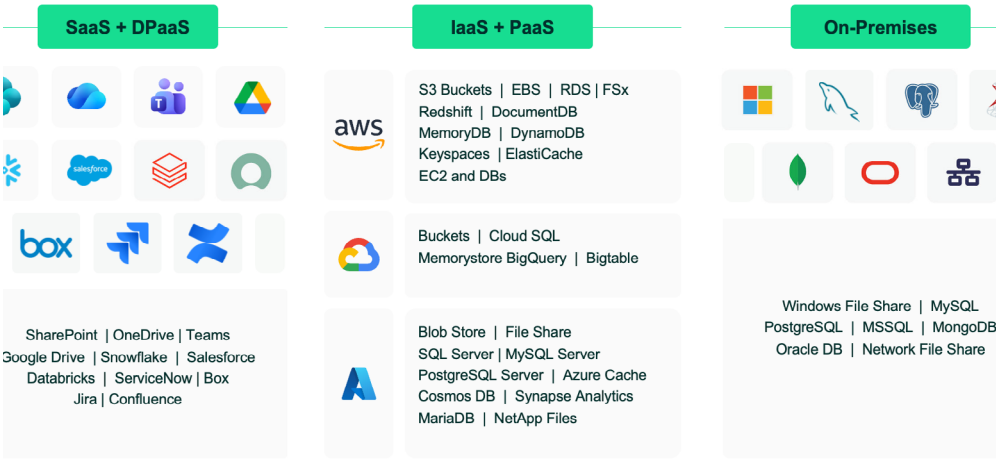


그림 4. DSPM은 광범위한 플랫폼과 서비스 전반에서 데이터 검색 및 분류.

결론

조직이 AI를 도입하고 더 많은 데이터를 관리함에 따라 민감한 데이터가 어디에 있는지, 누가 액세스할 수 있는지, 어떻게 사용되는지 파악해야 합니다. Proofpoint DSPM은 클라우드, SaaS, 온프레미스 및 AI 환경 전반에서 민감한 데이터를 분류하고, 위험 수준을 지정하며, 과도한 액세스를 찾고, 최소 권한 액세스를 적용하여 노출을 줄입니다.

Proofpoint Data Security의 일부로서 Proofpoint DSPM은 Proofpoint Enterprise DLP와 함께 작동합니다. 이들은 함께 팀이 민감한 데이터를 검색, 분류, 관리 및 보호할 수 있도록 돕습니다. 조직은 규정 준수를 강화하고, 안전한 AI 도입을 실현하며, 위험을 줄이고, 가장 가치 있는 정보를 보호할 수 있습니다.

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, 10,000개 이상의 대기업, 그리고 수백만 개의 소규모 조직이 위험 차단, 데이터 손실 방지, 그리고 사람 및 AI 워크플로 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.