

SSO Password Guard

암호 노출이 계정 탈취로 이어지기 전에
감지



주요 내용

- 승인되지 않은 사이트에 회사 암호가 입력될 때 이를 감지하여 공격자가 악용하기 전에 자격 증명 노출을 알려줍니다.
- 사용자가 회사 암호를 재사용할 때 실시간으로 브라우저 내에서 안내를 제공하여 신속한 수정을 유도하고 암호 중복 노출을 줄입니다.
- 자격 증명을 이용한 계정 침해를 줄여 계정 탈취 사건, 조사 및 암호 재설정 횟수를 감소시킵니다.

개요

계정 탈취는 자격 증명이 노출될 때 발생합니다. 이는 예방 조치를 우회하는 공격을 통해 발생하거나, 기업 정책을 위반하는 일상적인 사용자 행동을 통해 발생할 수 있습니다.

직원들은 SaaS 앱, AI 도구, 외부 웹사이트 등에서 회사 passwords를 재사용하는 경우가 많아 조직의 통제 범위를 훨씬 넘어 위험을 초래합니다. 이러한 자격 증명이 노출되면 공격자는 합법적인 사용자로 로그인하여 기존 보안 시스템을 쉽게 우회할 수 있습니다. 기존 보안 제어는 위협이 발생하기 전에 차단하거나 침해 발생 후 비정상적인 활동을 감지하는 데 중점을 둡니다. 이는 승인되지 않은 사이트나 악의적인 사이트에 자격 증명 입력되는 순간 치명적인 허점을 남깁니다.

SSO Password Guard는 이러한 격차를 해소하는 데 도움이 됩니다.

브라우저에서 직접 작동하는 이 기능은 로그인 시점에 회사 암호 재사용을 감지하고 사용자가 안전하지 않은 습관을 바꾸도록 안내합니다. Proofpoint Collaboration Security Prime의 일부인 이 솔루션은 채널 및 공격 단계 전반에 걸쳐 보호 기능을 확장하여 계정 탈취 위험과 팀의 업무 부담을 줄여줍니다.

위험 발생 순간에 자격 증명 노출로부터 보호

SSO Password Guard는 공격 과정의 핵심 지점에서 작동합니다. 이 기능은 위협이 사용자에게 도달한 후, 하지만 계정 탈취가 발생하기 전에 작동합니다.

사용자가 승인되지 않은 사이트나 악성 사이트에 회사 암호를 입력하면 Proofpoint는 해당 행위를 실시간으로 감지합니다. 그런 다음 로그인 및 회원가입 과정 전반에 걸쳐 브라우저 내에서 즉각적인 안내를 제공합니다. 이렇게 하면 자격 증명 노출이 발생했을 때 이를 즉시 해결할 수 있으므로 암호가 재사용되거나 다른 곳에서 악용되기 전에 조치를 취할 수 있습니다.

조직은 접속 시점에서 암호 오용을 줄임으로써 공격자가 접근 권한을 얻는 가장 확실한 경로 중 하나를 차단할 수 있습니다. 이를 통해 계정 탈취 위험이 실제 사건으로 이어지기 전에 줄일 수 있습니다.

자격 증명 정책 강화 및 행동 변화 유도

회사 정책만으로는 사용자가 회사 암호를 재사용하는 것을 막을 수 없습니다.

SSO Password Guard는 사용자가 안전하지 않은 행동을 시도하는 바로 그 순간에 개입하여 보안 행동을 강화합니다. 실시간 브라우저 내 안내는 사용자의 행동을 위협과 직접 연결하여 안전하지 않은 행동을 즉각적인 학습 기회로 전환합니다.

동시에 보안팀은 상습범과 노출 패턴을 파악할 수 있게 됩니다. 이를 통해 목표 지향적이고 증거 기반의 인식 개선 프로그램을 운영할 수 있으며, 조직이 광범위한 교육에서 집중적인 조치로 전환하고 시간이 지남에 따라 반복적인 위험을 줄일 수 있습니다.



그림 1. SSO Password Guard 최종 사용자 알림의 예시입니다.

운영 부담 및 복잡성 감소

대부분의 보안팀은 자격 증명이 이미 노출된 후에야 계정 탈취 사건을 조사할 수밖에 없습니다. 그들은 종종 위험 노출이 발생한 위치나 어떤 사용자가 위험을 유발하는지에 대한 명확한 통찰력이 부족합니다.

SSO Password Guard는 예방 가능한 암호 노출이 사고로 이어지기 전에 제거하여 이러한 부담을 줄이는 동시에 자격 증명 재사용에 대한 정확한 분석 정보를 제공합니다. 보안팀은 회사 암호가 어떤 웹사이트에서 사용되고 있는지 확인할 수 있습니다. 그들은 해당 사이트들의 위험성을 평가하고, 어떤 사용자가 반복적으로 자격 증명을 노출하여 가장 큰 위험을 초래하는지 파악할 수 있습니다.

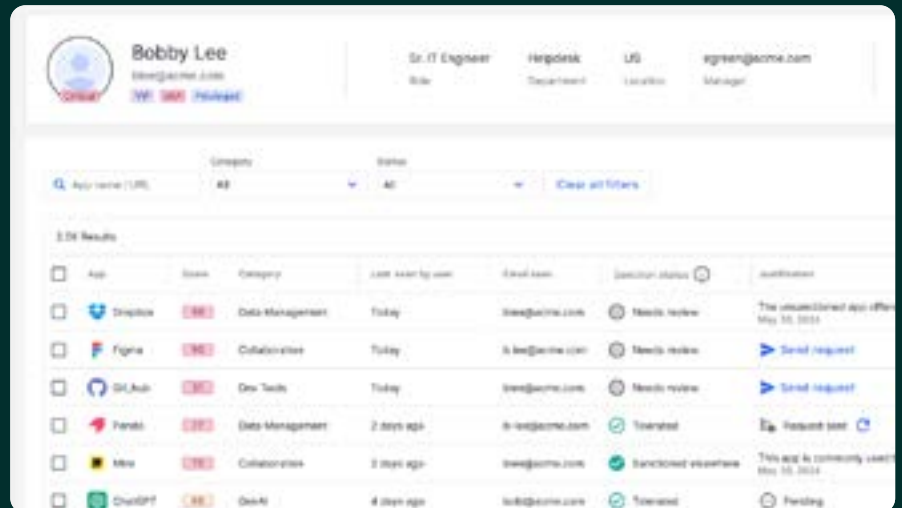


그림 2. SSO Password Guard에서 암호 노출에 대한 인사이트를 제공합니다.

이러한 조치를 통해 계정 탈취 사례가 줄어들고, 조사에 소요되는 시간과 암호 재설정 및 정리 작업에 소요되는 시간이 단축됩니다. 노출이 발생했을 때, 팀은 추측 없이 즉시 대응하는 데 필요한 맥락을 파악할 수 있습니다.

SSO Password Guard는 Proofpoint Collaboration Security Prime과 통합함으로써 복잡한 신호 기반 탐지 스택에 대한 의존도를 줄입니다. 보안팀은 중앙 집중식 가시성, 높은 신뢰도의 신호, 간소화된 대응을 통해 이점을 얻습니다. 이는 총 소유 비용을 낮추는 동시에 보안 결과를 개선하는 데 도움이 됩니다.

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 위협을 차단하고, 데이터 손실을 방지하며, 인력 및 AI 워크플로 전반에 걸쳐 회복력을 구축하기 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 연결하기: [LinkedIn](#)

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