proofpoint.

SOLUTION BRIEF

SSO Password Guard

Detect password exposure before it becomes account takeover

Key Highlights

- **Detects when corporate passwords are entered on unsanctioned sites, flagging credential exposure before attackers can use them.**
- **Provides real-time, in-browser guidance when users reuse their corporate password, driving quick correction and reducing repeat exposure.**
- **Reduces credential-driven compromises, which means fewer account takeover incidents, investigations, and password resets.**

Overview

Account takeover occurs when credentials are exposed. This can happen through attacks that bypass prevention controls, or through everyday user behavior that breaks corporate policy.

Employees often reuse corporate passwords across SaaS apps, AI tools, and outside websites, extending risk far beyond the organization's control. Once exposed, these credentials let attackers sign in as legitimate users, easily slipping past traditional defenses. Traditional security controls focus on stopping threats before they arrive, or on flagging unusual activity after a breach. This leaves a critical gap at the moment a credential is entered into an unsanctioned or malicious site.

SSO Password Guard helps to close that gap.

Operating directly in the browser, it detects corporate password reuse at the point of entry and guides users to change their unsafe habits. Part of Proofpoint Collaboration Security Prime, it extends protection across channels and attack stages to reduce account takeover risk and your team's workload.

Protect Against Credential Exposure at the Moment of Risk

SSO Password Guard works at a critical point in the attack chain. It acts after a threat reaches the user, but before an account takeover occurs.

When users enter corporate passwords on unsanctioned or malicious sites, Proofpoint spots the behavior in real time. It then provides immediate, in-browser guidance across both login and sign-up flows. This way, credential exposure is addressed when it happens—before passwords can be reused or exploited elsewhere.

By reducing password misuse at the point of entry, organizations cut off one of the most reliable paths attackers use to gain access. This lowers account takeover risk before it becomes an incident.

Enforce Credential Policies and Drive Behavior Change

Corporate policies alone do not stop users from reusing corporate passwords.

SSO Password Guard reinforces secure behavior by stepping in at the exact moment users attempt unsafe actions. Real-time, in-browser guidance connects the user's behavior directly to the risk, turning unsafe actions into immediate learning moments.

At the same time, security teams gain visibility into repeat offenders and exposure patterns. This enables targeted, evidence-based awareness programs, shifting organizations from broad training to focused action and reducing repeat risk over time.

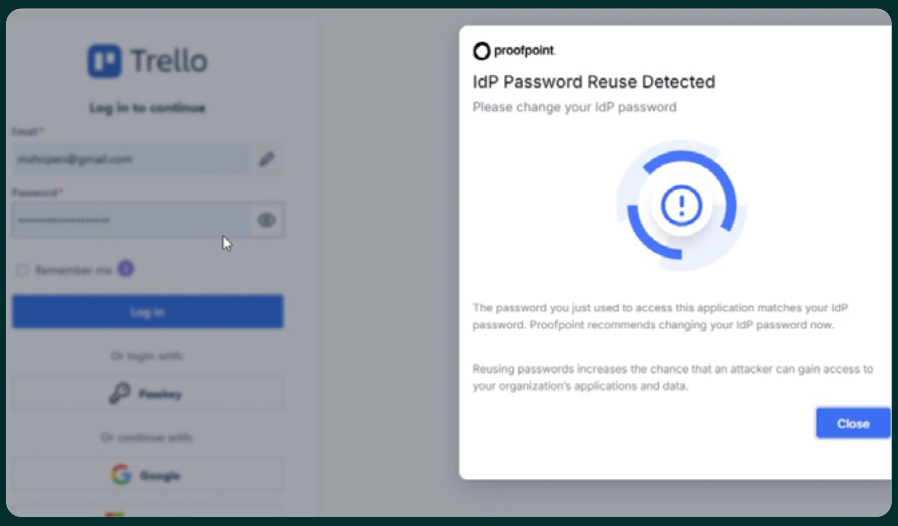

Figure 1. Example of an SSO Password Guard end-user alert.

Reduce Operational Burden and Complexity

Most security teams are forced to investigate account takeover incidents after credentials are already exposed. They often lack clear insight into where the exposure occurred, or which users are driving the risk.

SSO Password Guard reduces this burden by removing preventable password exposures before they become incidents, while providing high-fidelity insight into credential reuse. Security teams can see which websites corporate passwords are being used on. They can weigh the risk of those sites, and identify which users are repeatedly exposing credentials and pose the greatest risk.

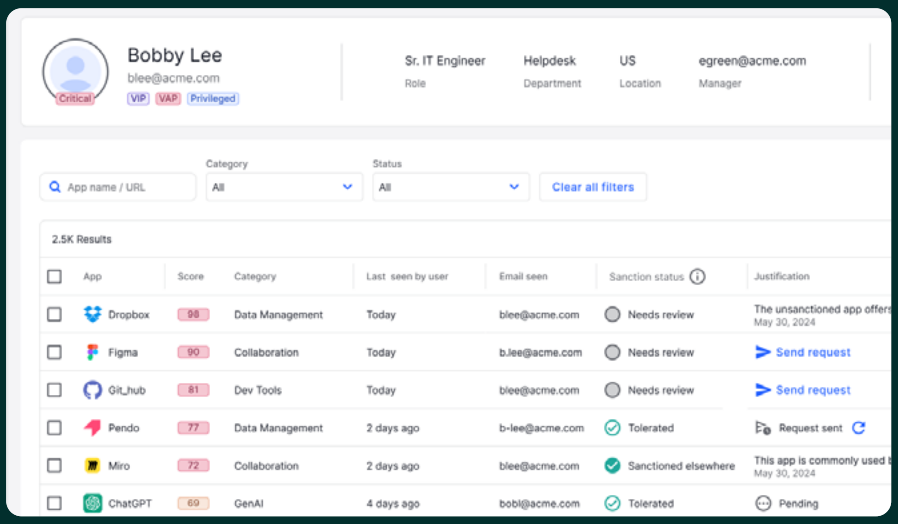

Figure 2. Password exposure insights in SSO Password Guard.

This results in fewer account takeover cases, less time spent on investigations, and less time on password resets and cleanup. When exposure does occur, teams have the context they need to respond right away, without guesswork.

By integrating with Proofpoint Collaboration Security Prime, SSO Password Guard also reduces reliance on complex, signal-driven detection stacks. Security teams benefit from centralized visibility, high-confidence signals, and streamlined response. This helps drive lower total cost of ownership while improving security outcomes.

proofpoint.