proofpoint.

RESUMO DA SOLU-

SSO Password Guard

Detecte a exposição de senhas antes que ela se torne um sequestro de

Principais desta-

- **Detecta quando senhas corporativas são inseridas em sites não autorizados, sinalizando a exposição de credenciais antes que os atacantes possam usá-las.**
- **Oferece orientação em tempo real, no navegador, quando os usuários reutilizam suas senhas corporativas, promovendo correções rápidas e reduzindo a exposição repetida.**
- **Reduz comprometimentos relacionados a credenciais, o que significa menos incidentes de sequestro de contas, investigações e redefinições de senha.**

Visão geral

O sequestro de contas ocorre quando credenciais são expostas. Isso pode acontecer por meio de ataques que contornem controles de prevenção ou por um comportamento cotidiano do usuário que viole a política corporativa.

Os funcionários costumam reutilizar senhas corporativas em aplicativos de SaaS, ferramentas de IA e sites externos, estendendo o risco muito além do controle da organização. Uma vez expostas, essas credenciais permitem que os atacantes façam login como usuários legítimos, passando facilmente por defesas tradicionais. Os controles de segurança tradicionais concentram-se em impedir ameaças antes que cheguem ou em sinalizar atividades incomuns após uma violação. Isso deixa uma lacuna crítica no momento em que uma credencial é inserida em um site não autorizado ou malicioso.

O SSO Password Guard ajuda a fechar essa lacuna.

Operando diretamente no navegador, ele detecta a reutilização de senhas corporativas no ponto de entrada e orienta os usuários a mudarem seus hábitos inseguros. Parte do Proofpoint Collaboration Security Prime, ele estende a proteção a canais e estágios de ataque para reduzir o risco de sequestro de contas e a carga de trabalho da sua equipe.

Proteja-se contra exposição de credenciais no momento do risco

O SSO Password Guard atua em um ponto crítico da cadeia de ataque. Ele age após uma ameaça alcançar o usuário, mas antes que um sequestro de contas ocorra.

Quando os usuários inserem senhas corporativas em sites não autorizados ou maliciosos, o produto da Proofpoint identifica o comportamento em tempo real. Em seguida, ele oferece orientação imediata no navegador durante os fluxos de login e cadastro. Dessa forma, a exposição de credenciais é tratada quando acontece — antes que senhas possam ser reutilizadas ou exploradas em outros lugares.

Ao reduzir o uso indevido de senhas no ponto de entrada, as organizações cortam um dos caminhos mais confiáveis que os atacantes usam para obter acesso. Isso reduz o risco de sequestro de contas antes que este se torne um incidente.

Imponha políticas de credenciais e promova mudanças de comportamento

As políticas corporativas sozinhas não impedem os usuários de reutilizarem senhas corporativas.

O SSO Password Guard reforça comportamentos seguros ao intervir no momento exato em que os usuários tentam realizar ações inseguras. A orientação em tempo real, no navegador, conecta o comportamento do usuário diretamente ao risco, transformando ações inseguras em momentos de aprendizado imediato.

Ao mesmo tempo, as equipes de segurança ganham visibilidade sobre infratores

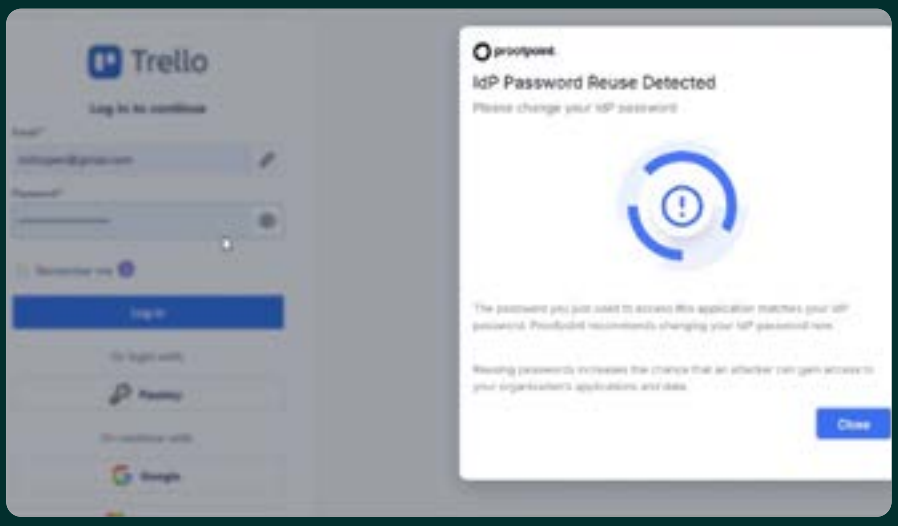

Figura 1. Exemplo de um alerta para o usuário final do SSO Password Guard.

Reduza a carga operacional e a complexidade

A maioria das equipes de segurança é forçada a investigar incidentes de sequestro de contas após as credenciais já terem sido expostas. Elas frequentemente carecem de uma visão clara de onde a exposição ocorreu ou quais usuários estão gerando o risco.

O SSO Password Guard reduz essa carga ao eliminar exposições de senha evitáveis antes que estas se tornem incidentes, enquanto oferece uma visão de alta fidelidade sobre reutilização de credenciais. As equipes de segurança podem ver em quais sites as senhas corporativas estão sendo utilizadas. Elas podem avaliar o risco desses sites e identificar

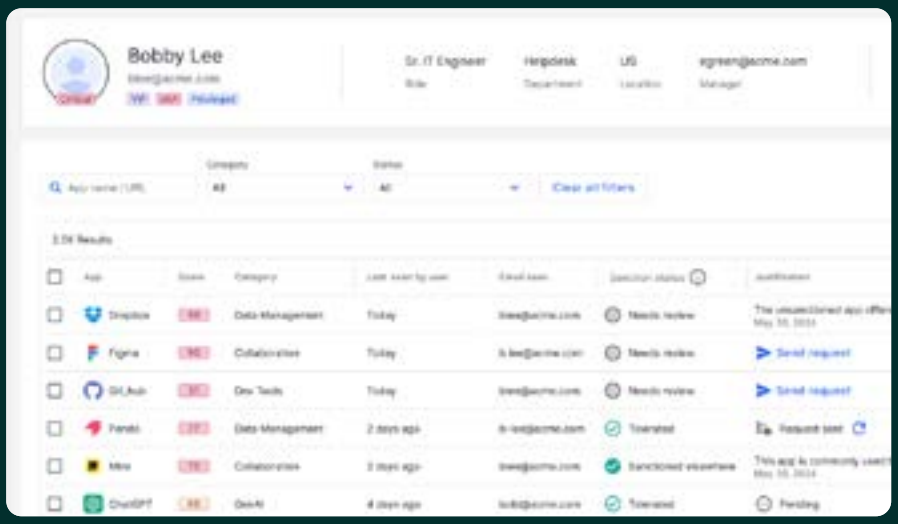

Figura 2. Insights sobre exposição de senhas no SSO Password Guard.

Isso resulta em menos casos de sequestro de contas, menos tempo gasto em investigações e menos tempo em redefinições de senha e limpeza. Quando ocorre uma exposição, as equipes têm o contexto necessário para responder imediatamente, sem adivinhação.

Ao integrar-se com o Proofpoint Collaboration Security Prime, o SSO Password Guard também reduz a dependência de soluções de detecção complexas baseadas em sinais. As equipes de segurança beneficiam-se de visibilidade centralizada, sinais de alta confiança e resposta simplificada. Isso ajuda a reduzir o custo total de propriedade enquanto melhora os resultados de segurança.

proofpoint.