proofpoint

FICHE SOLUTION

SSO Password Guard

Détectez les expositions de mots de passe avant qu'elles ne se transforment en prise de contrôle de comptes

Principaux atouts

- **Détecte les mots de passe d'entreprise saisis sur des sites non approuvés, et signale l'exposition d'identifiants de connexion avant que les cybercriminels ne puissent les utiliser.**
- **Fournit des conseils en temps réel dans le navigateur lorsque les utilisateurs réutilisent leur mot de passe d'entreprise, de façon à permettre une correction rapide et à réduire les expositions répétées.**
- **Réduit les compromissions liées aux identifiants de connexion, avec pour conséquence moins d'incidents de prise de contrôle de comptes, d'investigations et de réinitialisations de mot de passe.**

Présentation

Les prises de contrôle de comptes sont le résultat de l'exposition d'identifiants de connexion. Elles peuvent se produire au moyen d'attaques qui contournent les contrôles de prévention, ou par les comportements quotidiens des utilisateurs qui enfreignent les règles de l'entreprise.

Les collaborateurs réutilisent souvent des mots de passe d'entreprise sur des applications SaaS, des outils d'IA et des sites Web externes, étendant ainsi le risque bien au-delà du contrôle de l'entreprise. Une fois exposés, ces identifiants de connexion permettent aux cybercriminels de se connecter en tant qu'utilisateurs légitimes et de contourner facilement les défenses traditionnelles. Les contrôles de sécurité traditionnels se concentrent sur le blocage des menaces avant qu'elles ne se produisent, ou sur le signalement des activités inhabituelles après une compromission. Cette approche laisse une faille critique dès lors que les identifiants sont saisis sur des sites non approuvés ou malveillants.

SSO Password Guard aide à combler cette faille.

Fonctionnant directement dans le navigateur, Proofpoint SSO Password Guard détecte toute réutilisation de mots de passe d'entreprise au point d'entrée et guide les utilisateurs pour qu'ils modifient leurs comportements non sécurisés. Cet outil, qui fait partie de Proofpoint Collaboration Security Prime, étend la protection à l'ensemble des canaux et des phases d'une attaque pour réduire le risque de prise de contrôle de comptes et la charge de travail de votre équipe.

Protéger contre l'exposition des identifiants de connexion au moment du risque

SSO Password Guard intervient à un point critique de la chaîne d'attaque : après qu'une menace a atteint l'utilisateur, mais avant qu'une prise de contrôle de comptes ne se produise.

Dès lors que des utilisateurs saisissent des mots de passe d'entreprise sur des sites non approuvés ou malveillants, Proofpoint détecte ce comportement en temps réel. Il fournit alors des conseils immédiats dans le navigateur tant au moment de l'inscription que de la connexion. L'exposition des identifiants de connexion est ainsi prise en charge dès qu'elle se produit – avant que les mots de passe ne puissent être réutilisés ou exploités ailleurs.

En réduisant l'utilisation abusive de mots de passe au point d'entrée, les entreprises bloquent l'une des voies les plus fiables utilisées par les attaquants pour obtenir un accès. Cela réduit le risque de prise de contrôle de comptes avant que celui-ci ne se transforme en incident.

Appliquer des règles en matière d'identifiants de connexion et encourager un changement de comportement

Les règles d'entreprise à elles seules ne suffisent pas à empêcher les utilisateurs de réutiliser des mots de passe d'entreprise.

SSO Password Guard renforce les comportements sûrs en intervenant au moment précis où les utilisateurs exécutent des actions non sécurisées. Les conseils en temps réel dans le navigateur relient directement le comportement de l'utilisateur au risque, transformant ainsi les actions non sécurisées en moments d'apprentissage immédiats.

Dans le même temps, les équipes de sécurité bénéficient d'une visibilité sur les récidivistes et les schémas d'exposition. Cela leur permet de mettre en place des programmes de sensibilisation ciblés et basés sur des preuves. Les entreprises passent ainsi d'une formation générale à une action ciblée et à même de réduire la répétition des risques au fil du temps.

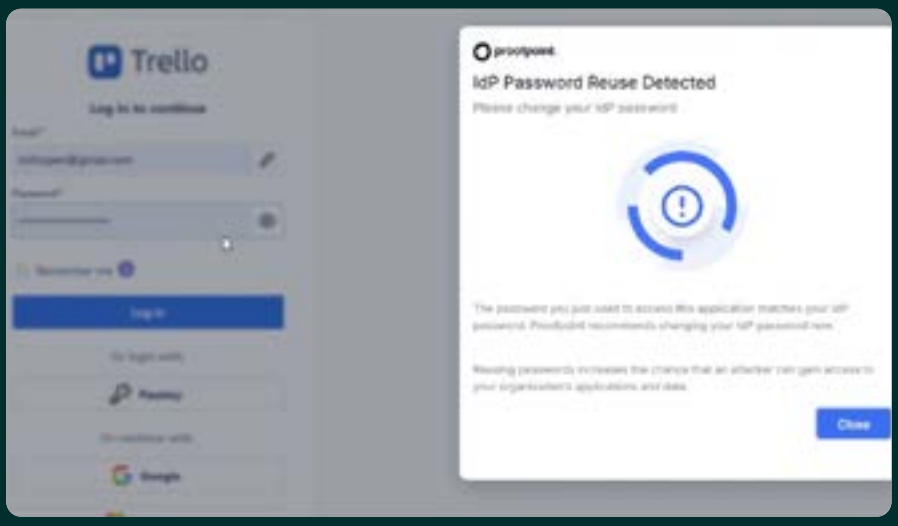

Figure 1. Exemple d'alerte de SSO Password Guard destinée à un utilisateur final

Réduire la charge opérationnelle et la complexité

La plupart des équipes de sécurité sont contraintes d'enquêter sur des incidents de prise de contrôle de comptes suite à l'exposition d'identifiants de connexion. Elles manquent souvent d'informations claires sur l'endroit où l'exposition s'est produite ou sur les utilisateurs à l'origine des risques.

SSO Password Guard réduit la charge de travail en mettant fin aux expositions de mots de passe évitables avant qu'elles ne se transforment en incidents, tout en fournissant des informations très précises sur la réutilisation des identifiants de connexion. Les équipes de sécurité peuvent voir sur quels sites Web les mots de passe d'entreprise sont utilisés. Elles peuvent évaluer les risques associés à ces sites et identifier les utilisateurs qui exposent de manière répétée leurs identifiants de connexion et posent le plus grand risque.

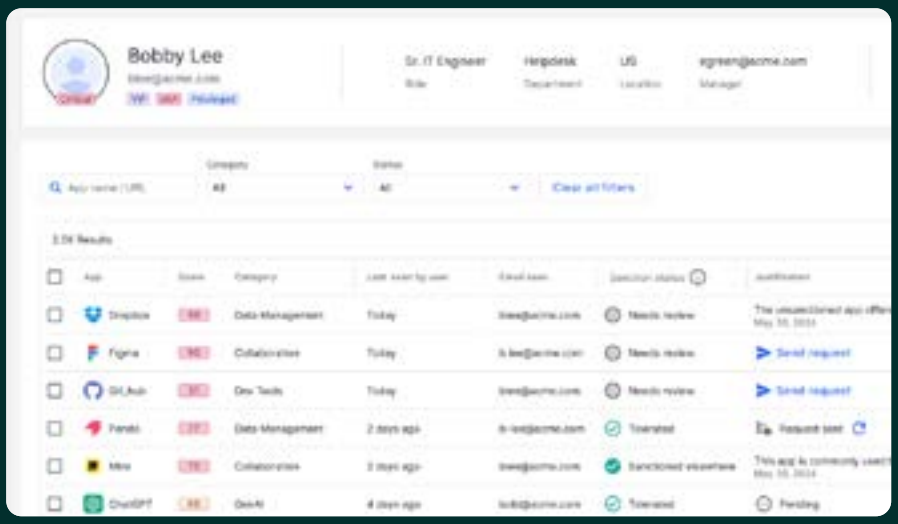

Figure 2. Informations sur l'exposition des mots de passe dans SSO Password Guard

Cela se traduit par une diminution des prises de contrôle de comptes, ainsi que par une réduction du temps consacré aux investigations, aux réinitialisations de mots de passe et au nettoyage. Lorsqu'une exposition se produit, les équipes disposent du contexte nécessaire pour réagir immédiatement, sans se lancer dans des conjectures.

Étant intégré à Proofpoint Collaboration Security Prime, SSO Password Guard réduit également la dépendance à l'égard de piles de détection complexes et basées sur des signaux. Les équipes de sécurité bénéficient d'une visibilité centralisée, de signaux extrêmement fiables et d'un workflow de réponse rationalisé. Tout cela contribue à réduire le coût total de possession tout en améliorant les résultats en matière de sécurité.

proofpoint.