

SSO Password Guard

Detecte la exposición de contraseñas antes de que deriven en la usurpación de cuentas

Características principales

- **Detecte las contraseñas corporativas introducidas en sitios web no autorizados y advierta de la exposición de las credenciales antes de que los ciberdelincuentes puedan utilizarlas.**
- **Proporciona avisos en tiempo real en el navegador cuando los usuarios reutilizan contraseñas corporativas, facilitando una corrección inmediata y reduciendo el riesgo de exposición reiterada.**
- **Reduce los riesgos relacionados con las credenciales, lo que se traduce en menos incidentes de usurpación de cuentas, investigaciones y restablecimientos de contraseña.**

Descripción general

La usurpación de cuentas es el resultado de la exposición de credenciales. Pueden producirse a través de ataques que eluden los controles de prevención, o por comportamientos cotidianos de los usuarios que incumplen las políticas de la empresa.

Los empleados suelen reutilizar las contraseñas de la empresa en aplicaciones SaaS, herramientas de IA y sitios web externos, lo que amplía el riesgo mucho más allá del control de la organización. Una vez que se han filtrado, estos datos de acceso permiten a los ciberdelincuentes iniciar sesión como usuarios legítimos y, de este modo, eludir fácilmente las defensas tradicionales. Los controles de seguridad tradicionales se centran en bloquear las amenazas antes de que se produzcan o en detectar actividades inusuales tras un ataque. Este enfoque presenta una vulnerabilidad crítica cuando los datos de acceso se introducen en sitios web no autorizados o maliciosos.

SSO Password Guard cierra esa brecha de seguridad.

SSO Password Guard, que funciona directamente en el navegador, detecta cualquier reutilización de contraseñas de la empresa en el punto de acceso y guía a los usuarios para que modifiquen sus hábitos poco seguros. Esta herramienta, que forma parte de Proofpoint Collaboration Security Prime, amplía la protección a todos los canales y fases de un ataque para reducir el riesgo de que se produzcan usurpaciones de cuentas y la carga de trabajo de su equipo.

Protéjase contra la exposición de credenciales en momentos de riesgo

SSO Password Guard interviene en un punto crítico de la cadena de ataque. Entra en acción después de que una amenaza haya afectado al usuario, pero antes de que se produzca la usurpación de cuentas.

Cuando los usuarios introducen contraseñas de la empresa en sitios web no autorizados o maliciosos, Proofpoint detecta este comportamiento en tiempo real. A continuación, ofrece consejos inmediatos en el navegador, tanto al registrarse como al iniciar sesión. De este modo, se gestiona la exposición de credenciales en cuanto se produce, antes de que las contraseñas puedan reutilizarse o aprovecharse en otros lugares.

Al reducir el uso indebido de contraseñas en el punto de acceso, las organizaciones bloquean una de las vías más fiables que utilizan los atacantes para obtener acceso. Esto reduce el riesgo de que se produzca usurpación de cuentas antes de que esto se convierta en un incidente.

Aplique políticas relativas a las credenciales e impulse un cambio de comportamiento

Las políticas de la empresa por sí solas no bastan para evitar que los usuarios reutilicen las contraseñas de la empresa.

SSO Password Guard promueve hábitos seguros interviniendo en el momento exacto en que el usuario comete una imprudencia. La orientación en tiempo real en el navegador relaciona el comportamiento del usuario directamente con el riesgo, y transforma las acciones inseguras en momentos de aprendizaje inmediato.

Al mismo tiempo, los equipos de seguridad disponen de información sobre los infractores reincidentes y los patrones de exposición. Esto habilita programas de concienciación específicos y basados en datos, llevando a las organizaciones de la formación genérica a la acción concreta y reduciendo los riesgos a largo plazo.

Reduzca la carga operativa y la complejidad

La mayoría de los equipos de seguridad se ven obligados a investigar incidentes de usurpación de cuentas tras la filtración de credenciales. A menudo carecen de información clara sobre el lugar en el que se produjo la exposición o sobre los usuarios que originaron los riesgos.

SSO Password Guard reduce la carga de trabajo al poner fin a las exposiciones evitables de contraseñas antes de que se conviertan en incidentes, al tiempo que proporciona información muy precisa sobre la reutilización de credenciales. Los equipos de seguridad pueden ver en qué sitios web se utilizan las contraseñas de la empresa. Pueden evaluar los riesgos asociados a estos sitios e identificar a los usuarios que exponen repetidamente sus credenciales y suponen el mayor riesgo.

SSO PASSWORD GUARD | RESUMEN DE LA SOLUCIÓN



Figura 1. Ejemplo de alerta de SSO Password Guard dirigida a un usuario final

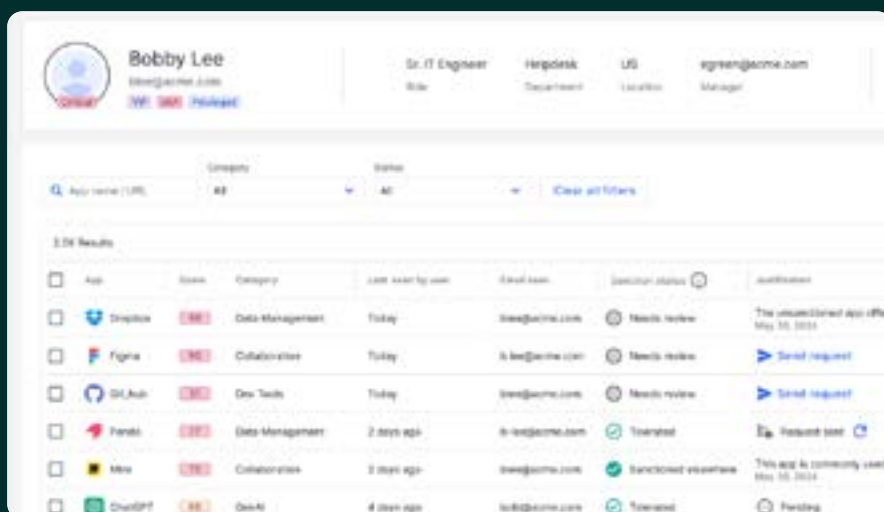


Figura 2. Información sobre la exposición de contraseñas en SSO Password Guard.

Esto se traduce en una disminución de los casos de usurpación de cuentas, así como en una reducción del tiempo dedicado a las investigaciones, al restablecimiento de contraseñas y a la limpieza. Cuando se produce un incidente, los equipos disponen de la información necesaria para reaccionar de inmediato, sin conjeturas.

Al estar integrado en Proofpoint Collaboration Security Prime, SSO Password Guard también reduce la dependencia de pilas de detección complejas y basadas en señales. Los equipos de seguridad disponen de una visibilidad centralizada, alertas extremadamente fiables y un flujo de trabajo de respuesta optimizado. Todo ello contribuye a reducir el coste total de propiedad, al tiempo que mejora los resultados en materia de seguridad.

Acerca de Proofpoint, Inc. Proofpoint, Inc. es un líder mundial en ciberseguridad centrada en las personas y los agentes, que protege la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un partner de confianza para más de 80 de las empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear las amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y empoderar a su personal mientras adoptan la inteligencia artificial de forma segura y con confianza. Más información en www.proofpoint.com/es

Conecte con Proofpoint: [LinkedIn](#)

Proofpoint es una marca comercial o marca comercial registrada de Proofpoint, Inc. en Estados Unidos y/o en otros países. Todas las demás marcas comerciales contenidas en el presente son propiedad de sus respectivos propietarios.

proofpoint.