HOJA DE DATOS

Password Manager

Autorizaciones para los usuarios, reducción de los costos de soporte y mayor seguridad

Beneficios

- Reduce la participación de mesa de ayuda y del área de TI en la administración rutinaria de contraseñas.
- Reduce drásticamente los tiempos de inactividad del usuario.
- Ofrece un rendimiento de la inversión inmediato.
- Mejora la satisfacción del usuario y del área de TI debido a la facilidad de uso y la implementación simple.
- Aumenta la seguridad de la red.
- Permite la sincronización de las contraseñas entre sistemas dispares.
- Se integra en la autenticación multifactor de Defender para una mayor seguridad.

Información general

La mayoría de las solicitudes de asistencia que llegan a mesa de ayuda están relacionadas con el restablecimiento de contraseñas. Y a medida que las organizaciones intentan obtener políticas de seguridad más firmes, el problema de la administración de contraseñas se generaliza cada vez más. Requerir contraseñas más complejas que deben cambiarse con mayor frecuencia aumenta la probabilidad de que los usuarios las olviden y soliciten soporte. El problema se magnifica cuando las empresas aplican contraseñas a múltiples sistemas y aplicaciones dispares. Como resultado, muchas empresas deben elegir entre aumentar la seguridad y reducir los costos de soporte técnico.

Password Manager ofrece una solución de autoservicio simple y segura que permite a los usuarios finales restablecer las contraseñas olvidadas y desbloquear sus cuentas. Permite que los administradores implementen políticas de contraseñas más seguras y, al mismo tiempo, reduzcan la carga de trabajo de mesa de ayuda. Las organizaciones ya no tienen que comprometer la seguridad para reducir los costos.

Características

Mayor seguridad

Password Manager permite a las empresas adoptar políticas más seguras de acceso a los datos, más allá del control que se ofrece de manera nativa en Microsoft® Active Directory®. La seguridad es mayor debido a que se eliminan los errores en mesa de ayuda y se reduce la necesidad de que los usuarios escriban sus contraseñas y hagan que las tareas de descifrado de contraseñas y las intrusiones sean más difíciles. El cifrado de los datos integrado soporta el acceso global y mantiene la seguridad de los datos.

La participación del usuario garantiza su retorno de inversión

Password Manager permite que los usuarios administren las tareas de contraseña más básicas por sí solos, lo que reduce el presupuesto del área de TI y permite un rendimiento sobre la inversión más rápido.

Haga una inversión inteligente

Password Manager es una solución de largo plazo para un problema creciente. Es una inversión inteligente para cualquier empresa que busque aumentar la eficiencia operativa del área de TI y aumentar la seguridad.

- Rentabilidad en el uso de la infraestructura actual de Active Directory: Password Manager le permite obtener más de su infraestructura actual

de Active Directory. También puede implementarla rápidamente y obtener un rendimiento sobre la inversión de inmediato. Además, ofrece una política de contraseña basada en grupo y más granular que la de Windows Server.

- Reducción en los costos y la carga de trabajo de mesa de ayuda, y aumento de la productividad de los usuarios: con Password Manager, los usuarios pueden restablecer sus propias contraseñas y desbloquear sus propias cuentas sin la asistencia de mesa de ayuda ni del soporte administrativo.
- Ayuda al usuario a pedido: Password Manager ofrece explicaciones en línea sobre políticas de contraseña. Además, proporciona comentarios a los usuarios de manera automática si no se cumple con las reglas de configuración de contraseña, y puede generar contraseñas aptas para los usuarios, sin la asistencia de mesa de ayuda.
- Extensiones de GINA para el cuadro de diálogo de inicio de sesión en Windows: Para simplificar los restablecimientos de contraseña para los usuarios, los administradores pueden hacer que en la pantalla de inicio de sesión de Windows se muestre un botón para el restablecimiento de contraseñas antes del inicio de sesión. Esto elimina la necesidad de configurar quioscos públicos o sistemas telefónicos costosos.

Aplique las normas organizativas

Password Manager adapta el mayor rango posible de políticas organizativas y las normas de seguridad de los datos.

- Cumplimiento estricto de políticas: Password Manager aplica las normas definidas por los administradores, registra los intentos fallidos de autenticación y bloquea las cuentas correspondientes si es necesario.
- Aplicación de inscripción: Password Manager ofrece varios mecanismos que aseguran que los usuarios se inscriban y usen el software, lo cual garantiza su eficacia.
- Autenticación confiable: Los perfiles personales de Preguntas y respuestas para usuarios contienen preguntas con respuestas únicas fáciles de recordar para los usuarios pero difíciles de adivinar para otros. Además, Password Manager puede implementarse con Defender para requerir una autenticación de contraseña de un solo uso (OTP) más segura junto con el perfil de Preguntas y respuestas o como un reemplazo de este.
- Seguridad y simplicidad: Password Manager se integra perfectamente en Windows, lo que le permite prestar servicio a usuarios de múltiples dominios, con o sin relaciones de confianza. Se proporcionan un sólido cifrado de los datos y una comunicación segura a través de la compatibilidad con tecnologías de seguridad líderes, como CryptoAPI de Microsoft y SHA-256.

Monitoree la actividad del sistema

Password Manager ofrece a los administradores funciones sólidas de inicio de sesión e informes, lo que facilita el monitoreo de la actividad del sistema y la corrección de las anormalidades.

Soporte para las iniciativas de administración de identidades

Password Manager tiene una interfaz web receptiva y ofrece administración de contraseñas para cualquier sistema conectado a Microsoft Identity Integration Server (MIIS). Además, se extiende a sistemas operativos que no son de Microsoft, como Unix y Linux, a través de Authentication Services; la incorporación de la autenticación de dos factores mediante Defender.

Suscripción híbrida a One Identity

Expanda las capacidades de Password Manager con la suscripción híbrida a One Identity, que ofrece servicios y características adicionales en la nube. Acceda a la autenticación ilimitada de dos factores de Starling para proteger el acceso administrativo y de los usuarios finales en Password Manager, al reemplazar el adicional de verificación telefónica. Una única suscripción permite todas las implementaciones de la solución de One Identity.

Acerca de One Identity

One Identity, una empresa de Quest Software, permite que las empresas implementen una estrategia de seguridad centrada en las identidades, ya sea localmente, en la nube o en un entorno híbrido. Con nuestro portafolio exclusivamente amplio e integrado de propuestas de gestión de identidades que incluyen administración de cuentas, gobernanza de identidades y gestión de accesos privilegiados y administración, las empresas son capaces de alcanzar su máximo potencial donde la seguridad se logra al ubicar las identidades en el centro del programa, lo que posibilita un acceso adecuado desde todos los tipos de usuarios, sistemas y datos. Obtenga más información en OneIdentity.com.

Datasheet_2019_PasswordManager_US_RS_55939