Manual de mitigación de riesgos de seguridad

¡Los principales riesgos de seguridad de TI que debe eliminar cuanto antes utilizando Password Manager Pro!

ManageEngine
Password Manager Pro

Fortalezca los controles internos y mitigue los riesgos de seguridad

Funciones del producto frente a los riesgos mitigados

Resumen general

Password Manager Pro ofrece una solución completa para controlar, gestionar, monitorear y auditar todo el ciclo de vida del acceso privilegiado. En un solo paquete ofrece tres soluciones: gestión de cuentas privilegiadas, gestión de acceso remoto y gestión de sesiones privilegiadas.

Password Manager Pro básicamente consolida todas sus cuentas privilegiadas en una bóveda centralizada en forma totalmente cifrada. Aplica las mejores prácticas de gestión de contraseñas y protege las cuentas privilegiadas, que son las llaves de su reino. Ayuda a mitigar los riesgos de seguridad relacionados con el acceso privilegiado y a prevenir las violaciones de la seguridad y los problemas de cumplimiento.

Este documento enumera los riesgos de seguridad mitigados por Password Manager Pro.

Gestión de cuentas privilegiadas

Descubrimiento de cuentas, protección y gestión de contraseñas

Descubrimiento de cuentas privilegiadas

Password Manager Pro descubre automáticamente los activos de TI en la red (Windows, Linux, dispositivos de red y equipos virtuales) y enumera las cuentas privilegiadas asociadas a ellos, ayudando así a las empresas a proteger rápidamente todas sus identidades privilegiadas.

El proceso de descubrimiento mitiga los siguientes riesgos:

- **Identifique las cuentas o servicios no autorizados:** Password Manager Pro enumera todas las cuentas privilegiadas que se encuentran en sus activos de TI críticos. Puede realizar fácilmente una auditoría interna e identificar las no autorizadas.

- **Minimice la cantidad de cuentas privilegiadas:** El proceso de descubrimiento también le ayuda a identificar las cuentas obsoletas. Puede elegir conservar sólo las cuentas que sean absolutamente necesarias.

- **Prevenga el acceso no autorizado:** Al aleatorizar las contraseñas de las cuentas privilegiadas en el momento de su descubrimiento, se puede evitar el acceso no autorizado por parte de administradores actuales o pasados que hayan tenido acceso a esas contraseñas anteriormente.

Bóveda de contraseñas centralizada

Password Manager Pro consolida, almacena y organiza todas sus contraseñas en un repositorio seguro y centralizado.

La consolidación centralizada de las cuentas privilegiadas permite combatir los siguientes riesgos:

- **Evite que las contraseñas caigan en manos equivocadas debido a un almacenamiento inseguro:** Los administradores de red y de TI tienden a almacenar credenciales sensibles en archivos de texto y hojas de cálculo, e incluso en notas adhesivas. Estas prácticas de almacenamiento inseguras convierten a las organizaciones en un paraíso para los hackers. Password Manager Pro elimina las vulnerabilidades al establecer un repositorio seguro y centralizado de contraseñas.

- **Supere el bloqueo del sistema debido a contraseñas obsoletas:** Con múltiples copias de archivos electrónicos que contienen contraseñas sensibles flotando por allí en la organización, aumentarán los casos de contraseñas obsoletas y los problemas de coordinación, lo que afectará a la eficiencia operativa. Con Password Manager Pro como repositorio centralizado, usted puede eliminar los problemas de coordinación y de bloqueo del sistema debido a contraseñas obsoletas.

Aprovisionamiento y controles de acceso

Titularidad de las contraseñas y compartición detallada

El diseño básico de Password Manager Pro gira en torno al concepto de titularidad y compartición de contraseñas. Quien añade una contraseña al repositorio se convierte en el propietario de la misma y sólo él tendrá acceso a esa contraseña. Si el propietario quiere que otros lo vean, la contraseña tiene que ser compartida. En cualquier momento, todos los usuarios (incluidos los administradores) sólo verán las contraseñas que tienen y comparten.

- **Elimine las cuentas huérfanas:** Las cuentas huérfanas son cuentas privilegiadas que permanecen activas pero no tienen dueño asociado. Estas cuentas suelen ser el resultado de un empleado que cambia de departamento o que deja la organización. No cerrar o transferir la titularidad de estas cuentas puede dar lugar a brechas en el control de acceso. Password Manager Pro resuelve este problema permitiendo que cualquier propietario de recursos que se vaya pueda transferir la titularidad de sus recursos a otro empleado autorizado.

- **Supere los riesgos de seguridad debido a la rotación de empleados:** Cuando un miembro del personal de TI que tiene acceso privilegiado a los recursos de TI deja la organización, todo el acceso a los sistemas de TI críticos que posee el miembro que se va debe ser inmediatamente desactivado. En ausencia de un sistema de gestión de contraseñas, resulta difícil identificar la lista de contraseñas a las que ha accedido ese usuario y cambiarlas todas. Password Manager Pro permite transferir la titularidad y aleatorizar las contraseñas después de la salida del personal de TI , eliminando así completamente los problemas de seguridad que podrían surgir debido a la rotación de empleados.

- **Evite la fuga de contraseñas por compartirlas de forma insegura:** El personal de TI tiende a compartir contraseñas comunes entre los miembros del equipo mediante el boca a boca, el correo electrónico o las llamadas telefónicas, lo que lleva a comprometer las contraseñas. Password Manager Pro ofrece un uso compartido seguro y detallado basado en las funciones del trabajo y ayuda a evitar la exposición o el compromiso de la contraseña.

- **Evite el acceso innecesario:** Password Manager Pro aplica estrictos controles de acceso y garantiza que los administradores sólo tengan acceso a las contraseñas que necesiten para sus funciones laborales. Por ejemplo, los administradores de Windows sólo tendrán acceso a las contraseñas de Windows y no a las de las bases de datos. De este modo, las organizaciones pueden evitar accesos innecesarios.

- **Elimine la visualización de contraseñas en texto plano:** Aunque se compartan las contraseñas con otras personas a través de los medios más seguros, las contraseñas pueden ser memorizadas o anotadas, lo que a su vez puede conducir a un acceso no autorizado. Para una mayor seguridad, Password Manager Pro permite a los administradores proporcionar acceso a los recursos de TI según sea necesario, sin revelar las contraseñas de los recursos en texto plano. Los usuarios podrán iniciar conexiones directas de RDP, SSH, Telnet, y consola SQL con recursos remotos e iniciar sesión automáticamente a sitios web y aplicaciones sin ver las contraseñas.

Integración de AD y LDAP

Password Manager Pro se integra con almacenes de identidades corporativas como Active Directory o LDAP para el aprovisionamiento y la autenticación de usuarios. Se sincroniza continuamente con el directorio y actualiza automáticamente la base de datos de usuarios cada vez que se añaden o eliminan usuarios en AD. Además, las funciones de autenticación de Active Directory pueden extenderse a Password Manager Pro, permitiendo a los usuarios iniciar sesión con sus credenciales de AD.

- **Supere los problemas de aprovisionamiento y desprovisionamiento de usuarios:** Password Manager Pro mantiene la misma estructura de grupos de usuarios que en AD. Dado que los permisos de acceso a las diferentes contraseñas pueden concederse en función de los grupos de AD, el aprovisionamiento y la desactivación del acceso a las contraseñas siguen los cambios en el propio AD. Esto ayuda a superar los problemas de seguridad que normalmente surgen debido al aprovisionamiento y la desactivación del acceso.

Control de liberación de contraseñas y flujo de trabajo avanzado

Password Manager Pro aplica una capa adicional de seguridad para las contraseñas al obligar a los usuarios a pasar por un flujo de trabajo de solicitud y liberación. Los usuarios que necesiten acceder a una contraseña sólo tienen que presentar una solicitud al administrador, junto con una razón creíble. Esto permite al administrador examinar las solicitudes de acceso antes de su aprobación y rechazar las solicitudes no válidas. Si es necesario, se pueden configurar aprobaciones dobles, que requieren que dos o más administradores aprueben una solicitud antes de que se liberen las contraseñas.

- **Evite el acceso inseguro y permanente cuando las personas necesiten un acceso temporal:** A menudo, el personal de TI o los contratistas de terceros necesitan acceso temporal a ciertos recursos para realizar operaciones de resolución de problemas. En estos casos, las contraseñas se transmiten por correo electrónico o por teléfono y se olvidan después. De este modo, el personal de TI tendrá acceso permanente a esos recursos. Password Manager Pro permite a los administradores liberar las contraseñas durante un período de tiempo limitado, al final del cual la contraseña se restablecerá automáticamente y se revocará el acceso.

- **Evite la explotación del acceso privilegiado por parte de personas con información privilegiada malintencionada:** Al aplicar un doble control en el flujo de trabajo solicitud-liberación, las personas con información privilegiada malintencionadas que busquen explotar el acceso privilegiado autorizado serán objeto de escrutinio.

Control de liberación de contraseñas y flujo de trabajo avanzado

- **Elimine los problemas de coordinación y los cambios conflictivos:** Cuando más de un administrador accede a un recurso de TI, se pueden producir cambios conflictivos y problemas de coordinación. Password Manager Pro elimina esto proporcionando acceso exclusivo a usuarios específicos durante un período de tiempo determinado.

- **Elimine la falta de control sobre el acceso de terceros:** Los usuarios de terceros -incluidos los contratistas, el personal temporal, los socios comerciales y los proveedores que necesiten acceder a las contraseñas de los activos informáticos críticos- tendrán que plantear una solicitud de acceso a las contraseñas. Los administradores pueden conceder un acceso limitado en el tiempo; y cuando el límite de tiempo expire, el acceso será revocado y la contraseña será restablecida. Este proceso garantiza el control absoluto del acceso de terceros a los recursos de TI.

Restablecimiento remoto de la contraseña

Password Manager Pro restablece las contraseñas de los recursos de TI remotos automáticamente a intervalos periódicos o en cualquier momento a petición. Asigna contraseñas seguras y únicas a cada cuenta y es compatible con una amplia gama de endpoints y sistemas de destino en entornos físicos, virtuales y en la nube.

- **Elimine las contraseñas débiles y estáticas; supere los intentos de cracking:** Al aleatorizar las contraseñas de los recursos de TI remotos a intervalos periódicos y asignar contraseñas seguras y únicas, Password Manager Pro ayuda a eliminar las contraseñas estáticas e invariables en toda la red. Esto, a su vez, impide el acceso no autorizado y los intentos de cracking.

- **Elimine las cuentas de servicio estáticas:** Las cuentas de servicio muy potentes utilizadas por los programas del sistema para ejecutar servicios o procesos de software de aplicación suelen poseer privilegios elevados o incluso excesivos. Las contraseñas de las cuentas de servicio suelen estar configuradas para "no cambiar nunca", debido a la dificultad de descubrir todos los servicios dependientes y propagar el cambio de contraseña. Las cuentas de servicio estáticas convierten a la empresa en un paraíso para los hackers.

Password Manager Pro localiza automáticamente las cuentas de servicio identificando los diversos componentes del servidor de Windows que se ejecutan utilizando cuentas de dominio y asignando los servicios y las tareas programadas a las cuentas respectivas. Cuando se restablece la contraseña de una cuenta de servicio, Password Manager Pro propaga automáticamente el cambio en todos los servicios dependientes asociados a la cuenta para evitar cualquier interrupción del servicio.

- **Mitigue los ataques "pass-the-hash":** Las cuentas de administrador de dominio de Windows proporcionan privilegios administrativos en todas las estaciones de trabajo, servidores y controladores de dominio. Sólo unos pocos administradores de confianza deberían utilizar las cuentas de administrador del dominio. Y, deben utilizar la cuenta sólo para iniciar sesión en los sistemas de los controladores de dominio que son tan seguros como los controladores de dominio.

  Esto se debe a que los sistemas Windows son vulnerables a los ataques "pass-the-hash". La funcionalidad de inicio de sesión único de Windows permite a los usuarios introducir las credenciales una vez y no tener que volver a introducir la contraseña. En realidad, Windows almacena en caché los detalles del inicio de sesión dentro del sistema en forma de hashes de contraseñas. Si un atacante consigue acceder a un sistema en el que el administrador del dominio haya iniciado sesión en el pasado utilizando sus credenciales de administrador del dominio, el atacante podría obtener fácilmente el hash y perpetrar una transacción no autorizada.

  Como mejor práctica, las cuentas de administrador de dominio no deben utilizarse para iniciar sesión en ningún sistema que no sean los controladores de dominio. Si hay una fuerte necesidad de hacerlo, el acceso a la contraseña debe pasar por un flujo de trabajo para su uso por una sola vez, después de lo cual se debe restablecer. Aunque las cuentas de administrador del dominio se utilicen prudentemente desde sistemas de confianza, deben cambiarse periódicamente. Password Manager Pro aleatoriza periódicamente las credenciales del administrador del dominio y mitiga los ataques de tipo pass-the-hash.

API para la gestión de contraseñas entre aplicaciones y bases de datos

Password Manager Pro ofrece tres tipos de API para la gestión de contraseñas entre aplicaciones: SSH-CLI, XML-RPC y REST. Las aplicaciones pueden consultar mediante programación a Password Manager Pro y obtener las credenciales.

- **Elimine las credenciales codificadas:** Normalmente, diversas aplicaciones requieren acceso a bases de datos y otras aplicaciones con frecuencia para consultar información relacionada con el negocio. Este proceso de comunicación se suele automatizar incrustando las credenciales de la aplicación en texto claro dentro de los archivos de configuración y los scripts. Los administradores suelen tener dificultades para identificar, cambiar y gestionar estas contraseñas. Como resultado, las credenciales no se modifican, lo que puede conducir a un acceso no autorizado a los sistemas sensibles. Así, las credenciales codificadas pueden facilitar el trabajo de los técnicos, pero esta práctica crea un punto de partida fácil para los hackers.

  Password Manager Pro elimina la práctica de la codificación de contraseñas con API seguras para la gestión de contraseñas de aplicación a aplicación y de aplicación a base de datos. Las credenciales de acceso no necesitan estar incrustadas en los archivos de configuración, sino que pueden almacenarse en la base de datos de Password Manager Pro. Siempre que una aplicación necesite conectarse con otras aplicaciones o bases de datos, puede consultar y recuperar las contraseñas de Password Manager Pro utilizando las API. De esta manera, las contraseñas también pueden estar sujetas a las mejores prácticas de seguridad, incluyendo la rotación periódica de contraseñas y la asignación de contraseñas seguras y únicas, sin la necesidad de realizar copiosas actualizaciones manuales.

- **Reduzca los riesgos de seguridad en los entornos DevOps:** Los entornos DevOps abarcan varias etapas, como el entorno de pruebas, el desarrollo, las pruebas unitarias, la integración, el control de calidad, las pruebas de aceptación del usuario, la producción y la recuperación de desastres. También requieren un acceso automatizado a las identidades privilegiadas por parte de los distintos interesados. Las aplicaciones, los scripts y las bases de datos que se ejecutan en entornos DevOps requieren acceso a identidades privilegiadas sin ninguna intervención humana. La codificación de las credenciales es la práctica de programación más peligrosa e invita a los problemas de seguridad. Las API de Password Manager Pro ayudan a conceder acceso automatizado a las contraseñas a las aplicaciones autorizadas, además de aplicar las prácticas de contraseñas estándar eliminando los problemas de seguridad en los entornos DevOps.

Acceso remoto y gestión de sesiones privilegiadas

Password Manager Pro permite a los usuarios autorizados iniciar sesiones directas de RDP, SSH, Telnet y consola SQL desde cualquier navegador compatible con HTML5 sin agentes de endpoint, plug-ins de navegador o programas de ayuda. Las conexiones se canalizan a través del servidor de Password Manager Pro y no requieren una conectividad directa entre el dispositivo del usuario y el host remoto.

Además de una fiabilidad superior, la conexión por túnel proporciona una seguridad extrema, ya que las contraseñas necesarias para establecer sesiones remotas no necesitan estar disponibles localmente en el navegador del usuario. Las sesiones iniciadas desde la interfaz web de Password Manager Pro pueden ser grabadas, almacenadas y reproducidas para apoyar las auditorías forenses. Además, Password Manager Pro permite a los administradores hacer seguimiento de las sesiones privilegiadas iniciadas por otros usuarios.

- **Reduzca los riesgos al conceder acceso remoto a terceros:** Al proteger y aleatorizar periódicamente las credenciales expuestas a terceros, las organizaciones pueden reducir los riesgos debidos al robo de identidad en la cadena de suministro.

- **Reduzca el riesgo de infección en los endpoints con la configuración del servidor de acceso:** En entornos de alta seguridad, como los centros de datos, el acceso remoto a los endpoints sensibles puede concederse a través de un servidor de salto intermedio. Password Manager Pro centraliza la gestión de todas las credenciales, incluyendo el servidor de salto y maneja el acceso. La configuración del servidor de acceso evita que los endpoints se infecten a través de equipos de conexión inseguros en ubicaciones de terceros.

- **Evite las actividades maliciosas o sospechosas mediante controles duales:** Supervise las sesiones privilegiadas altamente sensibles iniciadas por terceros o usuarios internos en tiempo real y termine las sesiones sospechosas.

- **Elimine los problemas de repudio:** En caso de violaciones o problemas de seguridad, los contratistas de terceros o los administradores internos no pueden negar haber realizado una actividad porque Password Manager Pro registra las sesiones privilegiadas en su totalidad.

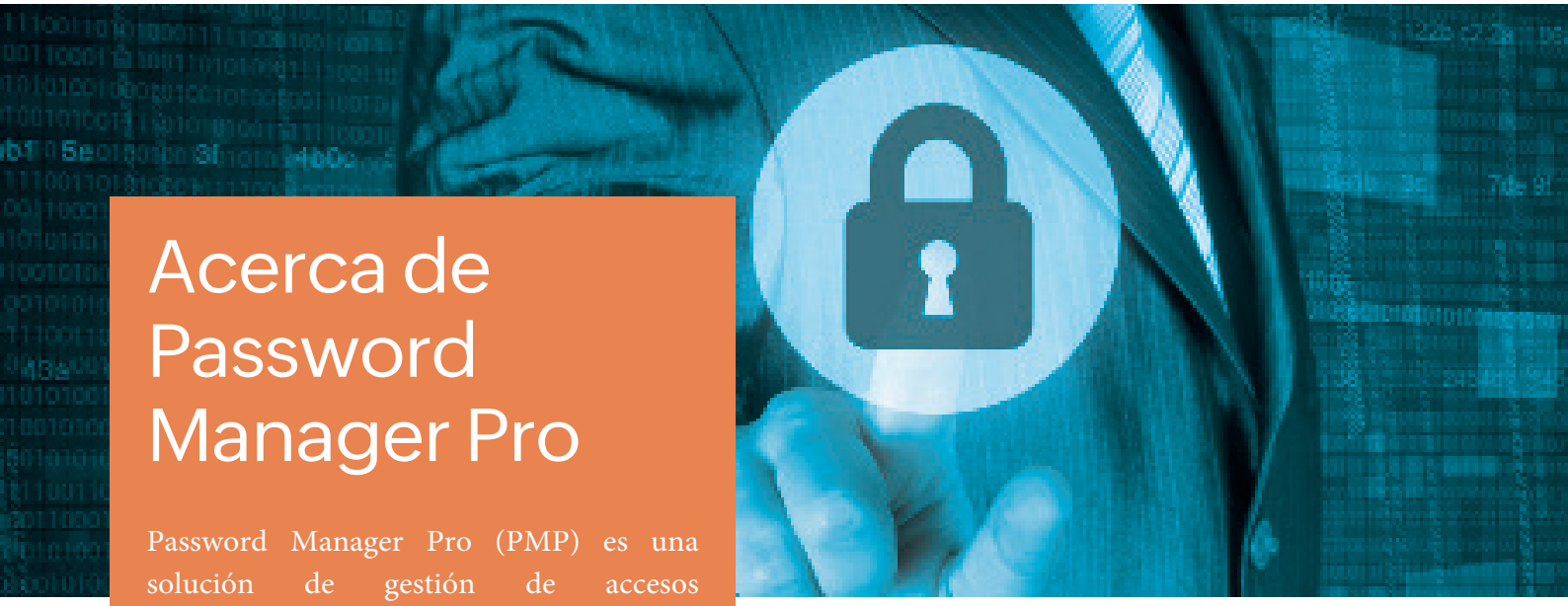
Auditoría, gestión en tiempo real, informes

Password Manager Pro registra cada acción del usuario mediante logs basados en texto, además de grabar las sesiones. También genera alertas y notificaciones en tiempo real sobre diversos eventos relacionados con las contraseñas, como el acceso, la modificación, la eliminación, los cambios en los permisos de uso compartido y otros eventos específicos. Password Manager Pro también genera mensajes syslog y traps SNMP, que pueden ser enviados a herramientas SIEM y sistemas de monitoreo respectivamente.

- **Elimine los problemas de responsabilidad:** Las cuentas administrativas no suelen estar vinculadas a una persona y se utilizan sobre todo en entornos compartidos. Esto podría dar lugar a problemas de responsabilidad cuando algo va mal. Cuando Password Manager Pro actúa como bóveda de contraseñas centralizada, los administradores tendrán que depender sólo de Password Manager Pro para acceder a los recursos de TI. Las pistas de auditoría generadas por Password Manager Pro permiten trazar el acceso a las personas.

- **Combata las amenazas persistentes avanzadas:** Password Manager Pro genera mensajes syslog, que pueden enviarse a herramientas SIEM para correlacionarlos con los eventos del resto de la empresa. Como los ataques informáticos avanzados normalmente abarcan un período de tiempo, la correlación de los datos de varios activos de TI con los datos de acceso privilegiado de Password Manager Pro ayuda a detectar los ataques informáticos que están en curso o que están a punto de producirse.

- **Reduzca la explotación del acceso privilegiado por parte de personas con información privilegiada:** Las alertas y notificaciones en tiempo real sobre el acceso privilegiado de Password Manager Pro ayudan a las organizaciones a detectar actividades no autorizadas y la explotación del acceso privilegiado por parte de personas con información privilegiada malintencionada.



Acerca de Password Manager Pro

Password Manager Pro (PMP) es una solución de gestión de accesos privilegiados basada en la web para empresas. Ofrece una solución completa para controlar, gestionar, monitorear y auditar todo el ciclo de vida del acceso privilegiado. En un solo paquete ofrece tres soluciones: gestión de cuentas privilegiadas, gestión de acceso remoto y gestión de sesiones privilegiadas. Los beneficios de la implementación de Password Manager Pro incluyen la eliminación de la fatiga de las contraseñas y los fallos de seguridad mediante la implementación de una bóveda segura y centralizada para el almacenamiento y el acceso a las contraseñas; la mejora de la productividad de TI mediante la automatización de los cambios frecuentes de contraseñas requeridos en los sistemas críticos; el aprovisionamiento de controles de seguridad preventivos y detectivos a través de flujos de trabajo de aprobación y alertas en tiempo real sobre el acceso a las contraseñas; y el cumplimiento de las auditorías de seguridad y el cumplimiento normativo como SOX, HIPAA y PCI.

Demo en línea:
http://demo.passwordmanagerpro.com

Asistencia técnica:
passwordmanagerpro-support@manageengine.com

Página web:
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro