ManageEngine
Password Manager Pro

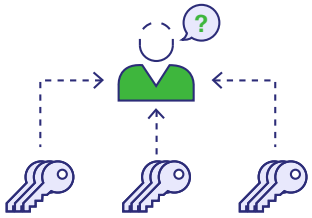
¿Está protegiendo sus identidades privilegiadas no humanas?

Obtenga más información sobre los posibles riesgos de seguridad y las formas de mitigarlos.

Las cuentas privilegiadas son cuentas poderosas dentro de una organización que los equipos de información y comunicaciones utilizan para ajustar la infraestructura de TI, instalar nuevo hardware y software, ejecutar servicios críticos y realizar operaciones de mantenimiento. Sirven como llaves maestras para los activos empresariales altamente críticos de la organización que albergan información sensible. Las soluciones de gestión de cuentas privilegiadas ayudan a los administradores de TI a proteger el acceso a estos activos de misión crítica al permitirles almacenar, compartir, gestionar, monitorear y auditar el ciclo de vida de todo tipo de cuentas privilegiadas desde una única consola unificada.

Sin embargo, la mayoría de las soluciones de gestión de cuentas privilegiadas ofrecen conjuntos de funciones que se limitan a proteger y gestionar las contraseñas de las cuentas privilegiadas, como las cuentas de servicio, las cuentas de aplicaciones y otras similares. Las contraseñas, sin duda, son credenciales de acceso privilegiado dignas de mención. Sin embargo, la constante evolución de la tecnología y la ampliación del perímetro de seguridad informática exigen que las empresas observen más de cerca las otras identidades que facilitan el acceso privilegiado, especialmente las claves criptográficas, que a pesar de servir como credenciales de acceso para enormes volúmenes de cuentas privilegiadas, a menudo se ignoran.

Estos son algunos de los posibles riesgos de seguridad que se plantean a los activos privilegiados dentro de su entorno de TI debido a la orfandad de las identidades de acceso no humanas como las claves SSH y los certificados SSL/TLS.

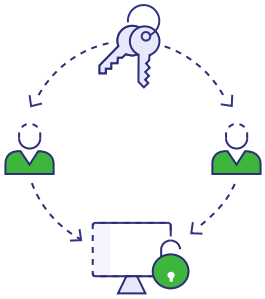


1. El número incontrolado de claves SSH dispara ataques basados en la confianza

Un informe reciente, State of machine identity management, señala que el 53% de las organizaciones no tienen un programa centralizado de gestión de claves SSH, y el 38% de las organizaciones declaran la probabilidad de que se produzcan incidentes de seguridad debido al robo de claves SSH. Sin un enfoque de gestión de claves centralizado, cualquiera en la red puede crear o duplicar cualquier número de claves. Estas claves suelen generarse aleatoriamente en función de las necesidades y se olvidan pronto una vez que se ha realizado la tarea a la que están asociadas. Las personas infiltradas maliciosas pueden aprovecharse de este océano masivo de claves SSH huérfanas para hacerse pasar por administradores, ocultarse cómodamente utilizando el cifrado y tomar el control completo de los sistemas de destino.

2. Las claves estáticas crean puertas traseras permanentes

Las empresas deberían rotar periódicamente sus claves SSH para evitar el abuso de privilegios, pero los enormes volúmenes de claves SSH no gestionadas hacen que la rotación de claves sea una tarea intimidante para los administradores de TI. Además, debido a la falta de visibilidad adecuada sobre qué claves pueden acceder a qué, existe una aprensión generalizada a la hora de rotar las claves por miedo a bloquear accidentalmente el acceso a los sistemas críticos. Esto conduce a una oleada de claves SSH estáticas, que tienen el potencial de funcionar como puertas traseras permanentes.

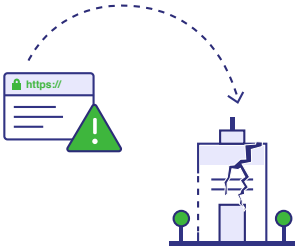


3. La duplicación involuntaria de claves aumenta la posibilidad de abuso de privilegios

En aras de la eficiencia, las claves SSH suelen duplicarse y circular entre varios empleados de una organización. Esta duplicación involuntaria de claves crea una relación clave-usuario de muchos a muchos, lo que aumenta enormemente la posibilidad de abuso de privilegios. Esto también hace que la corrección sea un reto, ya que los administradores tienen que pasar una buena cantidad de tiempo revocando claves para desenredar las relaciones existentes antes de crear e implementar nuevos pares de claves dedicadas.

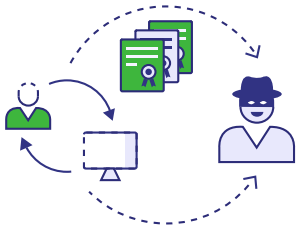
4. Las renovaciones fallidas de certificados SSL perjudican la credibilidad de su marca

Los certificados SSL, a diferencia de las claves, tienen una fecha de caducidad determinada. No renovar los certificados SSL a tiempo puede tener enormes consecuencias para los propietarios de los sitios web y para los usuarios finales. Los navegadores no se fían de los sitios web con certificados SSL caducados; lanzan mensajes de error de seguridad cuando los usuarios finales intentan acceder a esos sitios. Un certificado SSL caducado puede ahuyentar a los clientes potenciales en un instante o, lo que es peor, provocar el robo de datos personales de los visitantes del sitio.



5. Las implementaciones inadecuadas de SSL ponen en riesgo a las empresas

Muchas empresas confían completamente en el SSL para la seguridad en Internet, pero a menudo no se dan cuenta de que la mera implementación del SSL en su red no es suficiente para eliminar las amenazas a la seguridad. Los certificados SSL deben ser examinados minuciosamente en busca de vulnerabilidades de configuración después de ser instalados. Cuando se ignoran, estas vulnerabilidades actúan como brechas de seguridad que los delincuentes informáticos aprovechan para manipular el tráfico SSL y lanzar ataques de tipo man-in-the-middle (MITM).



6. Las firmas de certificados débiles no se tienen en cuenta

El grado de seguridad que proporciona cualquier certificado SSL depende de la fuerza del algoritmo hash utilizado para firmar el certificado. Las firmas débiles de los certificados los hacen vulnerables a los ataques de colisión. Los delincuentes informáticos aprovechan estas vulnerabilidades para lanzar ataques MITM e interceptar la comunicación entre los usuarios y los servidores web. Las organizaciones deben aislar los certificados que lleven firmas débiles y sustituirlos por certificados nuevos que contengan firmas más fuertes.

Incorporación de una estrategia de gestión de claves cifradas en toda la empresa

Todos los escenarios anteriores ponen de manifiesto la importancia de ampliar el alcance de su estrategia de seguridad de acceso privilegiado más allá de la gestión de contraseñas. Incluso con un sólido gestor de contraseñas, los delincuentes informáticos tienen mucho margen para eludir los controles de seguridad y obtener acceso a las cuentas de superusuario explotando diversas identidades de autenticación no gestionadas, incluidas las claves SSH y los certificados SSL. Descubrir y reunir todas esas identidades que pueden conceder acceso privilegiado, bajo un mismo techo, es un paso importante que las empresas deben dar para acortar las diferencias de su estrategia de seguridad de acceso privilegiado.

A continuación se presentan algunas de las mejores prácticas para empezar, que ayudan a su departamento de TI a gestionar efectivamente las identidades no humanas junto con las contraseñas privilegiadas, para aplicar una gobernanza completa sobre todo tipo de acceso privilegiado dentro de la red corporativa.

Descubra

Descubra las claves SSH y los certificados SSL/TLS implementados en entornos heterogéneos.

Consolide

Consolide las claves y certificados descubiertos en un repositorio seguro y centralizado.

Centralice

Evite la proliferación de claves SSH y certificados SSL/TLS centralizando su creación e implementación.

Automatice

Agilice y automatice la gestión del ciclo de vida de los certificados públicos, desde la generación de CSR, el aprovisionamiento, la implementación y la renovación.

Rote

Aplique la rotación automática de las claves SSH a intervalos de tiempo periódicos mediante la creación de tareas programadas.

Analice

Analice y corrija las vulnerabilidades de la configuración de SSL con regularidad, después de que se hayan implementado los certificados.

Monitoree

Establezca el tipo adecuado de mecanismo de alerta, preparando el camino para la renovación proactiva de los certificados mucho antes de su vencimiento.

Proteja y gobierne su entorno SSH y SSL/TLS con Password Manager Pro

Password Manager Pro es una solución de gestión de cuentas privilegiadas de nivel empresarial que ayuda a las organizaciones a obtener una visibilidad y un control completos de las credenciales privilegiadas, como las contraseñas, las claves SSH y los certificados SSL, desde un único lugar y sin tener que navegar entre varias consolas. A través de una perfecta integración con Key Manager Plus - que es la solución de gestión de claves SSH y certificados SSL/TLS de ManageEngine-, Password Manager Pro permite a los equipos de TI estar al tanto de la detección, la implementación, la rotación, la renovación, la auditoría y la gestión holística de todo tipo de credenciales de autenticación que facilitan el acceso privilegiado.

Tome el control de sus claves y certificados huérfanos hoy mismo

Programe una demo personalizada

www.passwordmanagerpro.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro