



ManageEngine
PAM360

Resumen de la solución



Automatizar. Orquestar. Controlar.

Una solución completa de gestión de accesos privilegiados para organizaciones

ManageEngine PAM360 es una solución ideal para las empresas que buscan incorporar la gestión de acceso privilegiado (PAM) en sus operaciones generales de seguridad de TI. Como solución unificada, ofrece:

- Gobernanza de cuentas privilegiadas
- **Flujos de trabajo detallados de control de acceso**
- Aprovisionamiento de acceso remoto seguro
- Gestión de sesiones privilegiadas
- Análisis avanzado del comportamiento de los usuarios
- Gestión de credenciales de DevOps
- **Gestión de certificados SSL/TLS**
- Auditoría e informes exhaustivos
- Integraciones con diversas plataformas de seguridad de TI

Uno de los retos más persistentes a los que se enfrentan hoy en día las organizaciones con sus soluciones PAM es la incapacidad de escalar a través de la dinámica infraestructura de TI de una organización. Aunque la seguridad de acceso privilegiado ha acaparado una atención significativa y los casos de uso de PAM se han diversificado en los últimos años, la mayoría de las ofertas de PAM en el mercado hoy en día se centran principalmente en las funciones básicas, como la bóveda de cuentas privilegiadas y la gestión de contraseñas. Otra limitación de las herramientas PAM heredadas es que están construidas para funcionar como un programa independiente y no se interconectan bien con las soluciones de seguridad de TI existentes en la red de la organización. Estos modelos en silos y confinados ya no sirven; en consecuencia, algunas organizaciones tienen sus operaciones de TI funcionando a niveles de riesgo inaceptablemente altos.

A medida que el entorno de TI se distribuye y extiende, las organizaciones modernas deben crear un programa PAM efectivo que proporcione una seguridad de acceso privilegiado completa en toda su infraestructura de TI y corrobore la estrategia de seguridad global mediante la integración con otras herramientas.

Los casos críticos de uso empresarial de PAM

1. Descubra, custodie y gestione cuentas y contraseñas privilegiadas

Las cuentas y contraseñas con privilegios son puertas de acceso a los sistemas críticos de una organización, y continuamente se añaden nuevas cuentas a su repositorio. Sin embargo, muchas organizaciones no tienen un registro del número y la lista de todas las cuentas privilegiadas utilizadas en su red, y siguen imprudentemente malas prácticas de gestión de contraseñas. Si no se gestionan y protegen, los ciberdelincuentes pueden explotar fácilmente las credenciales privilegiadas y destrozar las operaciones empresariales.

Las soluciones PAM pueden analizar automáticamente sus entornos on-premises y en la nube para descubrir todas las cuentas privilegiadas de su organización, y almacenarlas de forma segura en una bóveda de contraseñas centralizada, regida por sólidas políticas de cifrado y control de acceso. Descubrir, guardar en bóveda y rotar periódicamente todas las credenciales privilegiadas es uno de los pasos más importantes que hay que dar para reducir los riesgos que plantean las contraseñas.

2. Gestione las cuentas privilegiadas no humanas

Aunque es importante gestionar las cuentas de usuarios privilegiados debido a las amenazas internas y a su vulnerabilidad a los ataques de ingeniería social, es igualmente importante que las organizaciones gestionen las cuentas de servicio, las credenciales de las aplicaciones y las identidades de los equipos. Muchos equipos de TI, aunque comprenden los riesgos, suelen pasar por alto las cuentas no humanas debido a los riesgos operativos asociados a su gestión. Para empeorar las cosas, estas credenciales no suelen tener fecha de caducidad ni límite de intentos fallidos de inicio de sesión. También suelen almacenarse en archivos de

instalación o de script, lo que deja la infraestructura en un estado vulnerable. Dado que son estáticos y pueden permanecer inalterados durante mucho tiempo, los hackers pueden intentar aprovecharse de ellos para acceder a información confidencial de la empresa.

Una solución PAM puede ayudarle a gestionar estas cuentas y a rotar automáticamente sus contraseñas a intervalos regulares. También puede obtener estas credenciales de su bóveda para las comunicaciones de aplicación a aplicación y de aplicación a base de datos, sin ninguna interrupción del servicio ni tiempo de inactividad.

3. Proporcione a los usuarios un acceso controlado, limitado en el tiempo y menos privilegiado

En muchas organizaciones, los empleados suelen tener un exceso de privilegios de alto nivel y permisos de acceso que en realidad son innecesarios para sus roles, lo que prepara el camino al abuso de privilegios. Estos privilegios pueden pasar desapercibidos y no ser gestionados, invitando a varios riesgos de seguridad y poniendo en peligro a las empresas. A menudo, los equipos de TI no saben gestionar las consecuencias de un acceso excesivo, sobre todo cuando se trata de antiguos empleados. No anular la identidad y los permisos de acceso de un antiguo empleado permite a los empleados descontentos acceder a datos sensibles aunque ya no pertenezcan a la organización. En estos casos, es importante aplicar el principio del menor privilegio: proporcionar solo el permiso mínimo necesario para completar una tarea y revocar automáticamente los permisos una vez completada la tarea. Elevar los privilegios de los empleados solo cuando sea necesario también puede ayudar a evitar la acumulación de derechos de acceso no utilizados o innecesarios.

Puede integrar su sistema PAM con su herramienta interna de gobernanza de identidades para implementar controles basados en roles para usuarios privilegiados. También puede limitar los permisos de acceso, como el acceso específico a una aplicación durante una sesión RDP, o permitir solo determinados comandos en una sesión de terminal SSH. Una vez establecidos los controles necesarios, puede permitir a los usuarios privilegiados iniciar conexiones remotas directas y limitadas en el tiempo a los sistemas de destino sin revelar la contraseña.

4. Gestione el acceso remoto de terceros

Los proveedores remotos y los empleados subcontratados conforman la red empresarial ampliada de una organización. Suelen ser contratistas, consultores y proveedores de servicios que necesitan acceder a sus recursos de TI corporativos para diversas tareas contractuales. Esto significa que terceros tienen acceso a su red interna y, por lo tanto, suponen una amenaza igual de grave que las personas internas, lo que deja vulnerable a su organización. Según un informe de Ponemon Institute de 2020 (via [Security Boulevard](#)), el 53% de las organizaciones han sufrido al menos una violación de la seguridad de los datos causada por un tercero en los últimos dos años.

Cuando proporcione acceso remoto a terceros, una buena práctica es compartir las credenciales de acceso sin mostrar las contraseñas en texto plano. Una herramienta PAM le permite configurar otras políticas de seguridad, como límites de tiempo para el acceso con contraseña y un restablecimiento automático de la contraseña al final del periodo de uso. También le permite seguir continuamente las sesiones de terceros para detectar cualquier traza de comportamiento malicioso y adoptar al instante medidas correctoras.

5. Gestione las sesiones privilegiadas en tiempo real y establezca controles preventivos

Un atacante con acceso a una sola cuenta privilegiada mal gestionada podría escalar fácilmente su acceso a los sistemas más sensibles de la red de una organización sin dejar rastro. Estas sesiones privilegiadas maliciosas pueden evitar el escrutinio porque son lanzadas a través de cuentas privilegiadas legítimas por atacantes que se hacen pasar por usuarios privilegiados. Es más seguro asumir que incluso las personas con información privilegiada de confianza son una amenaza para el sistema porque cualquier actividad descuidada, deliberada o involuntaria, puede poner en peligro las actividades empresariales.

Una herramienta PAM ayuda a aumentar la supervisión y la transparencia, y mitiga el riesgo de uso indebido de privilegios mediante la gestión, el [monitoreo y la auditoría continuos de las actividades llevadas a cabo por los](#)

usuarios privilegiados, incluidos las personas con información privilegiada de confianza, los contratistas de terceros, las aplicaciones y los sistemas. También es una parte inseparable del modelo de confianza cero que anima a las organizaciones a no confiar automáticamente en que los usuarios utilicen siempre su acceso elevado para las acciones correctas. Su aplicación garantiza que se sigan conscientemente las mejores prácticas de seguridad.

6. Simplifique los informes de cumplimiento y las auditorías

Con el panorama de las amenazas en constante evolución, las organizaciones corren más riesgo que nunca de sufrir violaciones de la seguridad y la privacidad. La necesidad de proteger los datos críticos y lograr una transparencia total de las actividades privilegiadas exige un cumplimiento estricto de las normas de seguridad de TI y auditorías forenses, así como una forma de demostrar que las organizaciones se atienen a estos estándares. Sin embargo, muchas herramientas de seguridad heredadas permiten a los usuarios acceder a datos críticos y borrar sus huellas al instante sin tener que documentar sus acciones. Esto prepara el camino para una transparencia deficiente de las acciones privilegiadas y también hace que sea más difícil para las organizaciones anticipar, comprender y remediar una violación de la seguridad de los datos.

Una solución PAM ayuda a las organizaciones a implementar políticas de seguridad y controlar el acceso privilegiado, al tiempo que monitorea y registra todas las actividades privilegiadas de principio a fin. Proporciona una pista de auditoría impecable e informes completos sobre todas las actividades privilegiadas, lo que permite a los administradores de seguridad identificar de forma proactiva las actividades sospechosas o no autorizadas, respaldar las investigaciones forenses y demostrar fácilmente el cumplimiento de diversos estándares de seguridad como SOX, HIPAA, PCI DSS, GDPR y FISMA.

7. Gestione el acceso de emergencia y proporcione mecanismos de recuperación en caso de desastre

En caso de cualquier emergencia empresarial o interrupción del servicio, como un apagón prolongado o una violación de seguridad, la planificación y recuperación ante desastres es fundamental para el funcionamiento empresarial de una organización. En tales situaciones, la principal prioridad

de un administrador de seguridad es recuperar el acceso seguro a los sistemas críticos para restablecer los servicios empresariales. Una cuenta "break glass", o para casos de emergencia, proporciona a un usuario acceso inmediato a una cuenta a la que normalmente no estaría autorizado a acceder, y le otorga altos privilegios para eludir los procedimientos normales de control de acceso. Por lo tanto, es importante asignar permisos de emergencia a un administrador de confianza y limitar el uso de la cuenta a un periodo de tiempo estipulado que sea el justo para completar una tarea.

Una solución PAM permite a los equipos de TI configurar los controles de acceso para las cuentas de emergencia y predefinir quién puede acceder a qué recursos, con disposiciones para habilitar aprobaciones automáticas para la comprobación de contraseñas en caso de emergencia. Sin embargo, todas las actividades realizadas a través de la cuenta de emergencia y las políticas en torno a ella deben registrarse y gestionarse cuidadosamente por razones obvias de seguridad. Una solución PAM también puede intermediar sesiones a sistemas críticos sin revelar sus contraseñas al administrador de la cuenta de emergencia durante la comprobación.

8. Integre de forma nativa con las soluciones de seguridad existentes

Las organizaciones modernas necesitan algo más que una solución PAM aislada y heredada para hacer frente a las crecientes amenazas informáticas. Las soluciones PAM actuales deben ser capaces de integrarse con una serie de herramientas de ciberseguridad, recopilar datos de acceso privilegiado de todas las partes integrantes de la infraestructura de TI y correlacionar estos datos con las metodologías incorporadas para proporcionar una seguridad de acceso privilegiado completa en toda la TI de la organización. Por ejemplo:

- La integración de su herramienta PAM con su herramienta interna de registro de eventos puede ayudar a correlacionar los datos de los endpoints y de los accesos privilegiados.
- La asignación de las solicitudes de acceso privilegiado planteadas en su herramienta PAM a los problemas de red o incidentes en su mesa de servicio de TI puede ofrecer una comprensión más profunda de lo que está sucediendo en su entorno.
- La integración de la inteligencia artificial y las herramientas de detección de anomalías puede ayudar a identificar amenazas a partir de comportamientos inusuales y a detectar amenazas ocultas antes de que tomen forma.

- La integración con los servicios de gestión de identidades y las herramientas 2FA puede facilitar la incorporación y la autenticación de los usuarios.
- El estudio de los logs de auditoría de PAM en una plataforma de análisis avanzada proporciona información y una visión más inteligente de los riesgos basada en todos los datos disponibles.

Aproveche la combinación de automatización inteligente y potentes flujos de trabajo para crear una postura de seguridad inquebrantable en torno a su infraestructura de TI.

ManageEngine PAM360 es una solución diseñada de forma inteligente que permite a las organizaciones reforzar la seguridad en toda su infraestructura de TI, escalando varios departamentos y abarcando su creciente necesidad de acceso privilegiado. Las funciones de integración contextual de PAM360 permiten a las organizaciones crear una consola central para gestionar los datos de los distintos departamentos de su red de TI, al tiempo que controlan todos los accesos privilegiados y proporcionan eficacia empresarial.

Gestión de cuentas privilegiadas

PAM360 sirve como una bóveda segura y cifrada para almacenar, rotar y gestionar todas las contraseñas, claves, certificados y otros datos confidenciales de la organización. Descubre automáticamente todas las cuentas privilegiadas de su organización, es compatible con el restablecimiento periódico de contraseñas para más de 70 tipos de recursos y proporciona sólidas funciones de gestión de usuarios junto con autenticación robusta y compatibilidad con SAML SSO. PAM360 también ayuda en la gestión de contraseñas de aplicación a aplicación y de aplicación a base de datos, y en las automatizaciones DevOps mediante la integración con varias herramientas CI/CD.

Gestión de sesiones privilegiadas para el acceso remoto

PAM360 permite a los administradores aplicar estrictas políticas de control de acceso y permitir el acceso privilegiado justo a tiempo a una cuenta

perteneciente a un sistema crítico, como una base de datos, un dispositivo de red, una aplicación o un servidor, sin revelar la contraseña. Es compatible con servidores de salto para conectarse a sistemas Windows y Linux situados en zonas de seguridad distintas, la función RemoteApp para poner en la lista blanca aplicaciones específicas de Windows durante las sesiones RDP y diversos ajustes de configuración para mejorar la experiencia del usuario durante las sesiones remotas. PAM360 proporciona funciones avanzadas de gestión de sesiones privilegiadas y ayuda a los administradores a registrar y reproducir todas las sesiones privilegiadas, dando apoyo a auditorías forenses e internas. También permite a los administradores monitorear y seguir las sesiones de los usuarios en tiempo real con disposiciones para terminar las sesiones sospechosas, junto con auditorías e informes completos de todas las actividades.

Gestión de claves SSH y certificados SSL/TLS

PAM360 proporciona a los administradores de TI una visibilidad completa y un control centralizado sobre los entornos SSH y SSL de una organización, garantizando una seguridad total de los activos criptográficos y minimizando las posibilidades de posibles violaciones de la seguridad de los datos y problemas de cumplimiento. El módulo de gestión del ciclo de vida de los certificados SSL/TLS de PAM360 incluye el descubrimiento y el almacenamiento en bóveda de todos los tipos de certificados X.509 implementados en la red. Mediante el flujo de trabajo de solicitud de certificados integrado, los usuarios pueden solicitar a los administradores que creen e implementen certificados autofirmados para uso interno o aprovechar las integraciones con CA de terceros para obtener certificados públicos. PAM360 también permite implementar certificados en bloque y analizar vulnerabilidades SSL/TLS, funciona con sistemas de monitoreo de logs para activar alertas oportunas de caducidad de certificados.

Análisis del comportamiento de los usuarios privilegiados

PAM360 se integra con herramientas de análisis de usuarios privilegiados y de comportamiento como ManageEngine Analytics Plus, que simplifica el análisis de datos, y Log360, que cuenta con sólidas funciones UEBA que permiten a las organizaciones responder a actividades anómalas al instante.

Estas herramientas pueden recopilar todos los datos relevantes de inteligencia basados en amenazas de todas las redes individuales y correlacionar esta inteligencia con los datos de acceso privilegiado obtenidos de toda la red, mejorando la transparencia y la visibilidad de todas las actividades privilegiadas. Los responsables de seguridad pueden entonces tomar decisiones empresariales bien informadas o modificar las políticas de seguridad existentes para adaptarlas mejor a las circunstancias.

Integración con SIEM y otras herramientas de seguridad

PAM360 ayuda a las organizaciones a integrar de manera eficiente las soluciones SIEM en su estrategia de seguridad de acceso privilegiado. Las herramientas SIEM pueden detectar y evaluar las amenazas en tiempo real correlacionando los logs de auditoría de PAM360 con los datos de red de cada solución implementada en la red. PAM360 ofrece un dashboard consolidado para asignar el acceso privilegiado con las operaciones generales del sistema, y proporciona a los equipos de TI una visión más profunda de los incidentes de seguridad que se producen en todo el entorno distribuido e híbrido.

PAM360 también se integra con la detección de anomalías basada en inteligencia artificial para identificar amenazas a partir de comportamientos inusuales. Una vez establecida una línea de base de comportamiento para las operaciones privilegiadas dentro de una red, PAM360 incorpora una puntuación de riesgo para cada acción del usuario, y recopila las desviaciones de la línea de base en función de la ubicación, la hora o el rol. Cuando la puntuación ponderada de riesgo de una acción es superior a la norma, activa alertas automatizadas al administrador de TI para detener cualquier actividad potencialmente dañina en el acto.

Obtenga más información sobre las ofertas de seguridad de acceso privilegiado de ManageEngine

Solicitar una demostración personalizada