ManageEngine
PAM360

Guía del comprador PAM

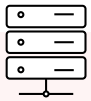
Todo lo que usted necesita saber a la hora de elegir una solución PAM para su empresa.

Introducción

En el panorama cibernético actual, los privilegios forman parte integral de los componentes críticos para el negocio de una empresa, como los sistemas operativos, los sistemas de directorio, los hipervisores, las aplicaciones en la nube, las herramientas de canalizaciones de CI/CD y la automatización robótica de procesos. Los delincuentes informáticos están interesados en estos privilegios porque pueden permitirles acceder fácilmente a los objetivos más críticos de una organización.

La superficie de ataque se está expandiendo rápidamente.

En 2022, más del **60%** de las violaciones de la seguridad en todas las industrias se implementaron a través de credenciales comprometidas, que tomaron un promedio de 341 días para identificar y contener. El abuso del acceso privilegiado y las identidades comprometidas se han convertido en los vectores clave de los ataques cibernéticos modernos. Con la rápida y desenfrenada adopción de modelos de trabajo híbridos, los perímetros de seguridad tradicionales han empezado a desvanecerse.



On-premises

Cuentas de administrador compartidas

Cuentas de servicio

Desktops, servidores y estaciones de trabajo

Dispositivos de red

Aplicaciones y bases de datos

Hipervisores y dispositivos virtuales

Identidades de equipos

Cloud infrastructure

Plataformas de gestión en la nube

Plataformas de gestión en la nube

Derechos basados en la nube

Internet of Things

Sistemas de control industrial, OT y SCADA

Estaciones de trabajo móviles

BYOD, impresoras, sensores y otros endpoints

DevSecOps

Herramientas

Canalizaciones de

CI/CD

Microservicios y plataformas de contenedores

Tipos y categorías de identidades privilegiadas modernas

Para protegerse frente a la evolución de las amenazas externas e internas, y satisfacer las crecientes exigencias de cumplimiento, es crucial controlar, monitorear y auditar los privilegios y el acceso privilegiado de empleados, proveedores, sistemas, aplicaciones y dispositivos IoT dentro de su entorno de TI.

Cómo utilizar esta guía

Para los responsables de I&O, los administradores de TI y los profesionales de la seguridad encargados de la seguridad de las identidades, la selección de la herramienta de gestión de acceso privilegiado (PAM) adecuada a los requisitos de su empresa puede ser una tarea difícil debido a la ampliación del panorama de amenazas. Proteger, monitorear, controlar y auditar el acceso privilegiado en toda la empresa es esencial para salvaguardar los activos de misión crítica frente a vectores de amenaza tanto internos como externos, y demostrar el cumplimiento de las leyes del sector, los organismos reguladores y las empresas de seguros de riesgos cibernéticos.

Pero, ¿por dónde empezar? Y una vez que haya empezado, ¿su herramienta se adaptará a la evolución de los niveles de madurez del mercado de las PAM?

La mayoría de los proveedores ofrecen suites PAM con ofertas sobredimensionadas, add-ons costosos y contratos con largos periodos de permanencia. Estos productos pueden estar muy lejos de las necesidades reales de su organización. Más eficiente es una suite PAM totalmente funcional que sea fácil de instalar, configurar y poner en marcha, que se pueda personalizar según los requisitos empresariales exclusivos de su organización, que ayude a garantizar el cumplimiento de la normativa y que aporte valor a sus inversiones en TI de forma casi inmediata.

Esta Guía del Comprador PAM le ayudará a comenzar su viaje PAM proporcionándole todos los detalles básicos y necesarios para ayudarle a elegir una solución PAM que tenga el tamaño adecuado para cada escenario empresarial, y que demuestre cómo usted puede reforzar su postura de seguridad, y cómo la herramienta PAM adecuada le ayuda a lograr resultados empresariales óptimos. Usted también recibirá una lista de control gratuita para ayudarle a comparar proveedores de PAM durante el proceso de evaluación.

Esta guía es el resultado de la vasta experiencia de ManageEngine con cientos de miles de implementaciones de PAM completadas a lo largo de los años, que consisten en una infinidad de escenarios y desafíos de seguridad. Creemos que todo viaje exitoso de PAM debe estar bien informado y ser imparcial.

Funciones críticas que usted debe buscar en una solución PAM

01 Gestión de cuentas privilegiadas

El primer paso, y el más crucial, para lograr un mayor control de los privilegios es obtener visibilidad sobre las identidades privilegiadas que están distribuidas por toda la organización, como las cuentas de usuario y las contraseñas. Según el Informe de Verizon sobre investigaciones de violaciones de la seguridad de los datos (DBIR) de 2023, más del **49%** de todas las violaciones de la seguridad de los datos se produjeron debido a credenciales débiles o robadas.

Las contraseñas incrustadas o codificadas que se utilizan en múltiples sistemas, aplicaciones y dispositivos IoT aumentan aún más la probabilidad de uso indebido de privilegios y acceso no autorizado. La gestión manual de contraseñas privilegiadas, incluida la detección periódica, la rotación y la aplicación de políticas, es poco fiable y engorrosa. Sin unas herramientas de gestión adecuadas, es difícil garantizar el control y la seguridad completos de las credenciales críticas.

Funciones críticas de gestión de contraseñas privilegiadas que se deben buscar en una solución PAM

Las soluciones PAM están diseñadas para mejorar la gestión del ciclo de vida de las cuentas y credenciales privilegiadas, incluidas las cuentas humanas y no humanas. Estas soluciones deben estar diseñadas específicamente para la gestión de contraseñas empresariales y ser capaces de automatizar la gestión del ciclo de vida de las identidades privilegiadas, como contraseñas, claves, certificados digitales, etc.

Este proceso incluye la detección automática, la incorporación, el almacenamiento en bóveda, la rotación periódica y la supervisión en tiempo real de las identidades.

Estas son algunas de las funciones obligatorias de gestión de cuentas privilegiadas que usted debe tener en cuenta si desea implementar una solución PAM en su organización:

Lista de control para la gestión de cuentas privilegiadas

- ☑ Realiza la detección, el análisis y la incorporación de extremo a extremo de todas las cuentas y credenciales críticas asociadas a los endpoints en toda la red corporativa.
- ☑ Almacena y gestiona automáticamente credenciales en múltiples plataformas (Windows,

- Linux, Cloud, Unix, hipervisores, dispositivos de red) en una bóveda digital cifrada en múltiples niveles mediante algoritmos, como AES-256, para garantizar un repositorio seguro de activos y credenciales altamente clasificados.

- Incluye API para obtener, gestionar y rotar automáticamente la contraseña de la aplicación para eliminar la codificación de credenciales en archivos y scripts.

- Ofrece controles integrados para gestionar el ciclo de vida de otras identidades privilegiadas, como claves SSH, certificados SSL/TLS, cuentas de servicio, cuentas de IIS App Pool, etc.

- Aplica un verdadero acceso de mínimo privilegio al ofrecer acceso justo a tiempo (JIT) y controles de solicitud y liberación de contraseñas.

- Aplica políticas de contraseñas estrictas que cubren la complejidad de las contraseñas, la frecuencia de los restablecimientos de contraseñas, la generación de pares de claves SSH sólidos, el acceso limitado en el tiempo a cuentas privilegiadas, el restablecimiento automático tras un único uso y otros controles robustos.

- Se integra con herramientas para desarrolladores, plataformas de contenedores y soluciones RPA para la obtención y gestión seguras de credenciales de aplicaciones críticas.

- Proporciona pistas de auditoría completas de todas las operaciones privilegiadas, como inicios de sesión de usuarios, uso compartido de contraseñas, intentos de acceso a contraseñas, acciones de restablecimiento, etc.
- Proporciona controles de acceso detallados basados en roles de usuario y políticas de acceso.
- Ofrece opciones flexibles de MFA compatibles con SAML y RADIUS.
- Proporciona opciones de rápido acceso para comprobaciones y controles de emergencia.
- Incluye opciones para gestionar y rotar credenciales pertenecientes a dispositivos personalizados, recursos en DMZ y entornos detrás de firewalls, así como aplicaciones internas y heredadas.

Al considerar una solución PAM para su empresa, la escalabilidad es un factor que no debe pasarse por alto. Dependiendo del tamaño de su repositorio de credenciales, es posible que necesite una solución PAM que pueda escalar para gestionar decenas o cientos de miles de credenciales de usuarios privilegiados, claves y certificados.

Solución: ManageEngine PAM360 ofrece un completo módulo de gestión de cuentas que comprende una gestión integral de credenciales privilegiadas pertenecientes a múltiples tipos de endpoints y recursos de TI. PAM360 ofrece diversas funciones de gestión de cuentas, como la detección de cuentas, el almacenamiento de credenciales en bóveda, los flujos de trabajo de control de acceso, la gestión remota de contraseñas, la gestión del ciclo de vida de los certificados SSL/TLS, el acceso remoto seguro, etc., todo ello integrado en una única plataforma.

02 Acceso con privilegios mínimos y controles de acceso granulares

El acceso con menos privilegios pretende reducir la superficie de ataque concediendo a los usuarios permiso para acceder únicamente a los sistemas de misión crítica necesarios para su rol actual, minimizando el riesgo de uso indebido o abuso. Esta estrategia solo eleva los privilegios cuando es necesario, reduciendo la superficie de amenaza y el potencial de movimiento lateral, y minimizando riesgos como el phishing, la ingeniería social y el ransomware.

El acceso de los administradores está estrictamente controlado y auditado para salvaguardar los activos críticos. Sin embargo, depender de conjuntos de herramientas nativas o internas para gestionar los privilegios de los usuarios puede ser engorroso y llevar mucho tiempo. A pesar de los riesgos, algunas aplicaciones requieren privilegios elevados para ejecutarse. Para minimizar estos riesgos sin obstaculizar la productividad de TI o bombardear la mesa de ayuda con solicitudes de permisos, la mayoría de las soluciones PAM están equipadas con controles de mínimo privilegio que pueden automatizar todo el flujo de trabajo de aprovisionamiento de acceso.

Una solución PAM que incorpore la confianza cero y el principio de mínimo privilegio permite a los administradores de TI restringir los privilegios de los usuarios en función de sus roles, lo que reduce la superficie de ataque y limita los daños potenciales causados por cuentas comprometidas. Lo ideal sería que estas soluciones eliminaran el acceso.

Estos son algunos de los principales controles de acceso con menos privilegios que se deben buscar en una solución PAM:

Lista de control de los controles de acceso granular y de mínimo privilegio

- ☑ Realiza auditorías periódicas para descubrir e identificar cuentas con privilegios excesivos que no tienen propietarios asociados.
- ☑ Otorga privilegios mínimos y adecuados a los usuarios en función de sus roles. Concede privilegios elevados de forma temporal en función de sus necesidades.
- ☑ Aplica las políticas de control de acceso a nivel de aplicación, servicio y dispositivo.
- ☑ Elimina los derechos de acceso administrativo a todos los servidores de la red y convierte a todos los usuarios en usuarios estándar de manera predeterminada.
- ☑ Proporciona un manejo detallado de las aplicaciones mediante controles como las listas de aplicaciones permitidas, los entornos de pruebas y la elevación de privilegios de autoservicio.
- ☑ Permite a los administradores aplicar el filtrado de comandos SSH mediante listas de permisos y agrupación de comandos seleccionados.
- ☑ Asigna controles de acceso y elevación JIT para cuentas de dominio, root y locales mediante privilegios administrativos temporales.

- Asigna controles de acceso y elevación JIT para cuentas de dominio, root y locales mediante privilegios administrativos temporales.
- Rota automáticamente las contraseñas de los dispositivos críticos después de cada uso.
- Incluye mecanismos de control de acceso adaptables, como la puntuación de confianza y los controles de acceso basados en políticas.
- Aplica restricciones a la ejecución de comandos privilegiados, la instalación de aplicaciones y los cambios en el sistema operativo.
- Graba en tiempo real sesiones privilegiadas. Proporciona pistas de auditoría detalladas de las actividades de los usuarios para facilitar las auditorías de cumplimiento y los análisis forenses.

Solución: Las funciones integradas de acceso de confianza cero de PAM360 permiten a los equipos de TI implementar el acceso JIT y de mínimo privilegio, los controles de aplicaciones y comandos, y el aprovisionamiento de acceso basado en políticas a través de múltiples tipos de recursos y sistemas operativos, garantizando así que los usuarios correctos tengan acceso administrativo a los recursos sensibles.

03 Acceso remoto seguro para empleados y usuarios de terceros

Para desempeñar efectivamente su trabajo, los empleados, contratistas y proveedores externos necesitan acceso privilegiado a sistemas remotos. Sin embargo, las organizaciones suelen tener dificultades para monitorear las actividades de los proveedores cuando acceden a su red. Las soluciones tradicionales de acceso remoto, como las VPN, conceden un acceso excesivo y a menudo carecen de ajustes de seguridad contextuales, pistas de auditoría exhaustivas y compatibilidad con diversos sistemas operativos y escenarios, lo que conlleva riesgos potenciales para la seguridad.

El acceso remoto seguro es una parte integral de la solución PAM, ya que permite a los usuarios administrativos obtener acceso sin VPN ni contraseña a endpoints de TI críticos, como servidores, aplicaciones, bases de datos, hipervisores, etc. Las soluciones PAM deben estar bien equipadas con motores de gestión de sesiones para monitorear las sesiones y las actividades de los usuarios en tiempo real, identificando y finalizando las sesiones anómalas y habilitando opciones de reproducción para auditorías forenses y organizativas.

Lista de control de la gestión de sesiones privilegiadas

- ☑ Elimina el aprovisionamiento de accesos sobre la base de "todo o nada". Implementa el verdadero privilegio mínimo autorizando el acceso JIT para sesiones remotas.
- ☑ Proporciona acceso instantáneo y sin contraseña a sistemas y aplicaciones remotas mediante protocolos estándar como RDP, VNC, HTTPS y SSH.
- ☑ Incluye controles granulares de gestión de sesiones, como el seguimiento de sesiones, la grabación y la transferencia bidireccional de archivos.
- ☑ Permite el acceso remoto a usuarios y proveedores de terceros a través de un cliente complejo.
- ☑ Genera pistas de auditoría exhaustivas de todas las actividades de los usuarios durante las sesiones privilegiadas, además de ayudar a cumplir los requisitos de cumplimiento.
- ☑ Proporciona acceso seguro a centros de datos remotos con opciones de servidor de salto.
- ☑ Incluye opciones para ofrecer acceso solo a la aplicación, en lugar de proporcionar acceso a todo el equipo.

Solución: PAM360 cuenta con un módulo integrado de gestión de sesiones que permite el acceso seguro a endpoints remotos con un solo clic, sin revelar contraseñas. La consola registra y graba todas las sesiones iniciadas a través de PAM360, y los administradores pueden realizar un control de la actividad de los usuarios y finalizar las sesiones si detectan algún comportamiento sospechoso. PAM360 también ofrece acceso instantáneo y seguro a centros de datos remotos a través de servidores de acceso. Además, PAM360 permite a los usuarios iniciar conexiones RDP y SSH a equipos de destino a través de un cliente desktop nativo.

04 Análisis de confianza en tiempo real para garantizar el privilegio de Zero Trust

Las actividades sospechosas, como los intentos fallidos de inicio de sesión, el tráfico procedente de IP bloqueadas, etc., pueden pasar desapercibidas cuando se producen de forma aislada. A la hora de conceder acceso a sistemas sensibles, los administradores suelen enfrentarse a la onerosa tarea de sancionar los privilegios basándose en los méritos de las solicitudes de los usuarios.

Con los controles de acceso adecuados, se conceden a los usuarios los privilegios necesarios para sus roles. Sin embargo, las herramientas PAM deben proporcionar mecanismos adecuados para evaluar las solicitudes de acceso en función de múltiples parámetros, ayudando así a los administradores a identificar y contener las actividades anómalas de los usuarios en tiempo real. Estas herramientas deben evaluar los posibles parámetros de riesgo antes de conceder el acceso, y hacer que el aprovisionamiento de acceso sea más contextual y estricto. Por ejemplo, ¿cómo proporcionan los administradores a sus usuarios acceso privilegiado a aplicaciones críticas que residen en sistemas y redes aislados? La respuesta es verificar la confianza del usuario y el dispositivo basándose en varios parámetros de seguridad críticos.

Dicho esto, ¿cómo empezar con el aprovisionamiento de acceso basado en la puntuación de riesgos en tiempo real y el análisis de amenazas? Aquí hay algunos elementos esenciales mínimos que una herramienta PAM debe tener para garantizar el privilegio de Zero Trust.

Lista de control de las medidas de acceso adaptables de Zero Trust

- ☑ Formula puntuaciones de confianza de referencia para usuarios y dispositivos en función de parámetros críticos, como intentos de inicio de sesión, dirección IP, estado de MFA, etc.
- ☑ Crea políticas de acceso dinámicas basadas en factores contextuales como puntuaciones de confianza, controles de acceso existentes, etc.
- ☑ Procesa automáticamente las solicitudes de acceso y concede acceso a los usuarios en función de la mejor política aplicable.
- ☑ Aísla a los usuarios y dispositivos que no cumplen las políticas de acceso, eliminando así cualquier riesgo potencial para la seguridad.
- ☑ Inicia acciones de runtime para poner fin a actividades anómalas basándose en las puntuaciones dinámicas de confianza.
- ☑ Proporciona pistas de auditoría detalladas de todas las actividades privilegiadas desde el momento en que se generan las puntuaciones de confianza hasta que finaliza la sesión del usuario.

Solución: El enfoque de PAM360 hacia Zero Trust es el primero de su clase en el sector. Implica aprovechar un mecanismo dinámico y automatizado de puntuación de la confianza para evaluar en tiempo real las amenazas que plantean los usuarios y los dispositivos. Usted puede establecer puntuaciones de confianza de referencia personalizables para diversos factores de riesgo en función de los parámetros de usuario y dispositivo que considere vitales para la seguridad de su organización. Posteriormente, usted puede establecer políticas de control de acceso basadas en estas puntuaciones de confianza y otros factores cruciales, y activar acciones de seguimiento automatizadas.

05 Gestión del ciclo de vida de los certificados

Las empresas confían en los certificados SSL/TLS para las comunicaciones y la transmisión de datos seguras, y en ausencia de un sistema de gestión de certificados adecuado, las empresas podrían experimentar interrupciones imprevistas y exponerse a posibles exploits. Los administradores de TI deben monitorear y gestionar diariamente numerosos certificados, lo que incluye la detección de vulnerabilidades, el control del uso y las fechas de caducidad.

De hecho, las interrupciones relacionadas con los certificados aumentaron un 26% en los últimos tiempos, lo que supuso un total de 2,4 millones de horas de inactividad empresarial.

El proceso de gestión de certificados suele estar aislado, lo que dificulta la visibilidad de la creación, la implementación y la caducidad de los certificados. Las herramientas PAM deberían estar equipadas con un módulo nativo para gestionar todo el ciclo de vida de los certificados SSH/TLS. Esto incluye controles para descubrir, crear, implementar, renovar y gestionar claves de cifrado y certificados junto con cuentas privilegiadas.

Estas son algunas de las funciones críticas de gestión del ciclo de vida de los certificados que debe buscar en una solución PAM:

Lista de control para la gestión del ciclo de vida de los certificados

- ☑ Descubre y enumera certificados SSL/TLS en múltiples entornos y endpoints.
- ☑ Implementa automáticamente certificados en aplicaciones y dispositivos de destino.
- ☑ Proporciona alertas puntuales de caducidad de los certificados para una solución más rápida.
- ☑ Ofrece integraciones con CA de terceros para una gestión efectiva de los ciclos de vida de los certificados.

Solución: PAM360 proporciona un módulo nativo para la gestión de claves SSH y certificados SSL/TLS, que son una parte integral de su entorno PAM. Este módulo permite a los administradores de TI descubrir, gestionar, implementar y realizar un control automático de todo el ciclo de vida de las claves SSL/TLS asignadas a endpoints de misión crítica en todo el entorno de TI. Esto elimina la necesidad de una solución independiente de otros proveedores para gestionar sus certificados SSL/TLS y claves SSH.

06 Análisis unificado del comportamiento de los usuarios privilegiados, auditoría e informes de cumplimiento

Las herramientas PAM deben ofrecer un módulo integral de análisis de comportamiento de los usuarios privilegiados (PUBA), que aprovecha la IA y el machine learning para analizar y derivar patrones de comportamiento de los usuarios, y correlacionar los datos de acceso privilegiado con otros eventos en toda la empresa para mitigar las amenazas de seguridad en tiempo real. Esto ayuda a los administradores a comprender las actividades anómalas de los usuarios, realizar análisis detallados de la causa raíz y remediar los incidentes de seguridad para minimizar el riesgo de violación de la seguridad de los datos mediante la extracción de inferencias procesables a partir de los datos de los eventos.

Además, las herramientas PAM deben tener opciones integradas para generar logs y auditorías en tiempo real que puedan enviarse a herramientas SIEM para su posterior análisis. Estas auditorías deben cubrir todo el "quién", "qué" y "cuándo" de cada actividad de acceso privilegiado, que los equipos de TI pueden utilizar para comprender comportamientos sospechosos y tomar decisiones informadas en el futuro.

Lista de control del análisis del comportamiento de los usuarios privilegiados

- ☑ Incluye funciones UEBA nativas para analizar y crear patrones de comportamiento de los usuarios para una detección efectiva de anomalías.
- ☑ Ofrece dashboards interactivos para controlar y monitorear en tiempo real las actividades de acceso de los usuarios privilegiados.
- ☑ Genera exhaustivas pistas de auditoría para profundizar en los patrones de acceso privilegiado y poner fin rápidamente a las acciones de los usuarios que se desvían del comportamiento habitual.
- ☑ Comparte datos como mensajes syslog y traps SNMP con herramientas SIEM y soluciones de gestión de red para su posterior correlación.
- ☑ Proporciona informes instantáneos para los mandatos de cumplimiento, como HIPAA, PCI DSS, SOX, el GDPR, etc.
- ☑ Proporciona datos históricos para obtener información desde múltiples perspectivas.

Solución: PAM360 ofrece un PUBA nativo para detectar y acabar con usuarios y actividades sospechosas en sistemas privilegiados de forma efectiva. Las funciones de PUBA de la solución están impulsadas por el deep learning y el machine learning para monitorear y establecer patrones de comportamiento exhaustivos de los usuarios. Esto permite a los equipos de TI tomar decisiones de seguridad fundamentadas en datos anteriores. PAM360 ofrece alertas en tiempo real para eventos registrados, como actividades de sesiones privilegiadas, cambios de contraseña y actualizaciones de políticas. Estas alertas pueden enviarse a los sistemas de gestión de logs para su posterior análisis y correlación.

07 PAM para identidades de carga de trabajo

Los equipos de DevSecOps suelen necesitar credenciales para autenticar sus flujos de trabajo y microservicios. Por lo general, estas credenciales están codificadas en archivos y scripts en formatos de texto plano, y con frecuencia son utilizadas por varias partes interesadas que trabajan en canalizaciones de CI/CD, procesos de RPA y flujos de trabajo de ingeniería. Si estas credenciales se alteran sin planificación ni aviso previos, podría producirse un fallo en cascada de múltiples procesos críticos simultáneamente. Además, si estas credenciales quedan expuestas, aunque sea por casualidad, cualquier persona malintencionada podría aprovecharlas para vulnerar los sistemas de información críticos de una organización.

Si bien está claro que es necesario integrar la PAM en los procesos DevSecOps, ¿cómo pueden lograrlo los equipos de TI sin comprometer la velocidad y la agilidad?

Solución: PAM360 proporciona integraciones out-of-the-box con plataformas de contenedores, soluciones DevSecOps CI/CD y herramientas RPA para garantizar una gestión segura de las credenciales de las aplicaciones. Esta integración permite que los procesos y las aplicaciones recuperen automáticamente las credenciales de la bóveda de PAM360 y realicen acciones sensibles como el aprovisionamiento de acceso, los cambios periódicos de contraseña, el control granular y la auditoría, sin interrumpir los flujos de trabajo internos.

Factores adicionales a tener en cuenta a la hora de implementar una solución PAM en su empresa

Además de todas las funciones críticas descritas anteriormente, las organizaciones también deben tener en cuenta estos factores cruciales a la hora de buscar una solución PAM.

¿Es más rápida la creación de valor con la herramienta?

La mayoría de las soluciones PAM vienen con funcionalidades recargadas y complejidades de implementación, mientras que algunas de ellas requieren consultores o técnicos calificados para adaptar su solución a su entorno. Así, usted tendrá que orientar sus esfuerzos y su presupuesto a unas funciones que podrían distar mucho de sus necesidades reales. Las herramientas de PAM deben ser capaces de ponerse en marcha sin atascarse en un ciclo de implementación o en ciclos que duren meses.

¿Su organización se ve gravada por bloqueos contractuales y barreras de salida?

Algunos proveedores de PAM presumen de sus elevados índices de retención, pero eso suele deberse a sus largos y complejos contratos, que restringen las opciones de sus clientes. En tiempos de dificultades económicas, los presupuestos de TI de muchas empresas se reducen, por lo que es importante elegir una solución PAM que no venga acompañada de largos periodos de bloqueo y contratos complicados.

¿La herramienta incluye un complejo sistema de precios?

Su herramienta PAM no debe obligarle a navegar por un complejo laberinto de ofertas. El enfoque de precios a la carta para funciones críticas, junto con implementaciones costosas y prolongadas, puede hacer mella en su presupuesto y retrasar la obtención de valor.

¿Está la herramienta preparada para el cumplimiento de la normativa y el seguro de riesgos cibernéticos?

Dado que el cumplimiento de las normativas y los seguros de riesgos cibernéticos se están convirtiendo en una necesidad innegociable para muchas empresas, las herramientas PAM deben incluir todas las funciones necesarias para ayudarle a cumplir fácilmente las normas del sector y los requisitos de los seguros.

¿Qué diferencia a ManageEngine PAM360?

PAM360 es la suite PAM empresarial de ManageEngine, que ayuda a las empresas a aplicar un control estricto en las vías de acceso a los endpoints y activos de misión crítica. Cargado con todos los elementos esenciales de PAM inteligente, PAM360 cumple todos los requisitos para ofrecer una sólida postura de seguridad y, al mismo tiempo, rentabilizar más rápidamente sus inversiones. PAM360 adopta un enfoque holístico de la seguridad de los accesos privilegiados, ofreciendo una integración contextual con las soluciones de gestión de TI, las herramientas para desarrolladores y las aplicaciones empresariales, lo que se traduce en una información ingeniosa, controles de acceso granulares y soluciones más rápidas.

He aquí algunas razones por las que más de 5.000 empresas como usted confían su PAM a ManageEngine.

- **La solución PAM adecuada para la empresa orientada al valor**

  ManageEngine ofrece una cartera completa de PAM que satisface todos los casos de uso de PAM y los niveles de madurez de TI de la empresa. PAM360, nuestra solución PAM estrella, cuenta con todas las funciones PAM esenciales para empresas de todos los tamaños. Gracias a sus opciones de implementación flexibles y fáciles de usar, usted podrá rentabilizar más rápidamente sus inversiones en seguridad.

Zero Trust por diseño, hasta el último detalle

PAM360 ofrece multitud de controles de seguridad granulares de confianza cero para regular sus rutinas de acceso. Se trata, entre otros, de flujos de trabajo de solicitud-liberación, aprovisionamiento de acceso basado en roles y políticas, y puntuación dinámica de la confianza de usuarios y endpoints. Con estas completas funciones, ¡tenemos su actividad de acceso cubierta y protegida!

Fácil de implementar y rápida rentabilización

PAM360 es más fácil de instalar, configurar y gestionar que otros programas que sobrepasan los límites de la complejidad operativa y de mantenimiento. Con PAM360, usted puede empezar a trabajar de inmediato. La mayoría de nuestros clientes pueden implementar completamente PAM360 en cuatro semanas o menos. Además, ofrecemos modelos de implementación flexibles para adaptarnos mejor a sus necesidades.

Precios con valor optimizado, obtenga un ROI más rápido

PAM360 ofrece una estructura de precios transparente, sin costos ocultos, add-ons excesivos ni contratos complicados. La licencia del producto se basa únicamente en el número de usuarios administradores, sin ningún límite en el número de usuarios finales o endpoints. PAM360 ofrece todos los controles esenciales y las funciones que usted desea en una solución PAM, sin hacer mella en su presupuesto de TI.

- **Forme parte del completo entorno de gestión de TI de ManageEngine**

  En promedio, los clientes que utilizan PAM360 también utilizan al menos otras cuatro soluciones de ManageEngine, como ITSM, UEBA y soluciones de análisis de TI. Nuestro unido entorno de TI ayuda a nuestros clientes a eliminar la fatiga de los proveedores y a crear una inmensa sinergia para extender PAM a toda la empresa.

- **Asociarse con una empresa cuya filosofía empresarial está profundamente arraigada en la I +D.**

  Zoho Corp., nuestra empresa principal, invierte el 50% de sus ingresos en actividades de I+D para crear soluciones de seguridad de TI resistentes y preparadas para el futuro, para las empresas de hoy y de mañana. Creemos en construir soluciones, no en adquirirlas.