




ManageEngine

Suite de gestión de identidades privilegiadas

**UN ENFOQUE UNIFICADO
PARA PROTEGER LAS
IDENTIDADES
PRIVILEGIADAS Y
CONTROLAR EL ACCESO
PRIVILEGIADO**

[Solicite una demostración personalizada gratuita](#)



Una suite completa de nivel empresarial que permite a los administradores de TI gestionar las identidades privilegiadas, así como controlar y monitorear el acceso a los sistemas de información críticos desde una plataforma sencilla y consolidada.

1 Destruya los silos de datos

Reúna todas sus cuentas privilegiadas bajo un mismo techo y haga una mejor gestión de ellas. Suprima las bases de datos de credenciales específicas de los departamentos o equipos y establezca un control colectivo. Establezca una titularidad clara y no deje ninguna entidad privilegiada sin contabilizar.

2 Evite la fatiga de las contraseñas

Implemente una bóveda centralizada que se adapte al ritmo de su crecimiento digital. Dote a sus equipos con potentes programas de detección, almacenamiento ilimitado de recursos y flujos de trabajo de automatización para combatir la fatiga de las contraseñas a medida que proliferan las cuentas privilegiadas.

3 Combata el robo de identidad

Aísle y proteja las cuentas privilegiadas con un doble cifrado que utiliza AES-256 para evitar el acceso no autorizado. Vaya más allá de los flujos de trabajo de inicio de sesión básicos y aplique la autenticación multifactor o el inicio de sesión único; demuestre la identidad del usuario antes de permitir el acceso a credenciales sensibles.

4 Evite los fallos de seguridad

Refuerce la seguridad de las cuentas privilegiadas con contraseñas únicas e imprevisibles y pares de claves seguras. Aplique políticas estrictas para los requisitos de complejidad y la rotación periódica de credenciales, incluidas las actualizaciones de las contraseñas de las cuentas de servicio y las renovaciones oportunas de los certificados SSL.

5 **Impulse la productividad de las TI**

Agilice y automatice las rutinas de restablecimiento de contraseñas para una serie de sistemas de destino con el fin de reducir el trabajo manual. Supervise los próximos vencimientos de los certificados SSL y renuévelos con antelación para evitar el tiempo de inactividad del servicio. Obtenga acceso ininterrumpido a las credenciales de los activos de TI críticos con módulos de alta disponibilidad bien diseñados.

6 **Mitigue la amenaza interna**

Utilice controles granulares basados en roles para delegar adecuadamente el acceso permanente o puntual a las credenciales de cuentas privilegiadas. Proporcione al personal cualificado y a las entidades no humanas un acceso limitado en el tiempo a los sistemas de información críticos sin compartir las credenciales en texto plano.

7 **Establezca máxima visibilidad**

Manténgase informado de las necesidades de acceso privilegiado en su entorno con flujos de trabajo de solicitud y liberación de credenciales diseñados para necesitar su aprobación. Supervise constantemente el acceso y el uso de las cuentas privilegiadas con alertas instantáneas por correo electrónico, flujos de actividad en tiempo real y pistas de auditoría integrales. Genere traps SNMP y mensajes Syslog a los sistemas de gestión para detectar rápidamente las anomalías.

8 **Apruebe las auditorías de cumplimiento**

Demuestre el cumplimiento de las normas de control de acceso privilegiado establecidas por GDPR, NIST, FISMA, HIPAA y SOX, entre otras, a través de mecanismos de bóveda seguros, autenticación de usuarios, control de acceso y aprovisionamiento, e informes detallados, incluidos los informes listos para la auditoría de PCI-DSS, GDPR, ISO/IEC 27001 y NERC-CIP.

9 **Construya relaciones de confianza**

Ejecute un entorno SSL libre de vulnerabilidades con un análisis regular de certificados y servidores finales para detectar fallos de configuración como Heartbleed, POODLE, revocaciones de certificados y conjuntos de cifrado débiles. Aísle los certificados SHA-1 y migre de manera eficiente a SHA-2. Demuestre a los clientes que está preparado para la seguridad y gane su confianza.

10 **Haga que la seguridad sea utilizable**

Haga de la seguridad informática una experiencia positiva para sus empleados. Proporcione a ellos una plataforma sencilla pero potente que consiga un equilibrio entre seguridad y facilidad de uso. Acorte las curvas de aprendizaje y permita una realización más rápida de las rutinas diarias de la PAM.

Encárguese de las necesidades de gestión de identidades privilegiadas de su organización de principio a fin con una solución integrada hecha a conciencia para abarcar una amplia gama de servicios esenciales, todo ello desde una única consola centralizada.

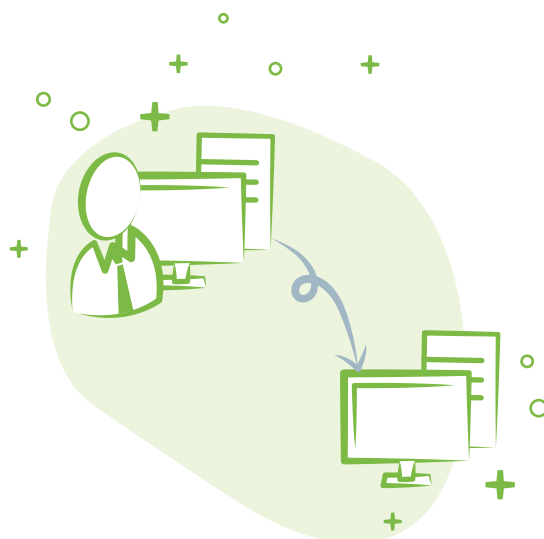


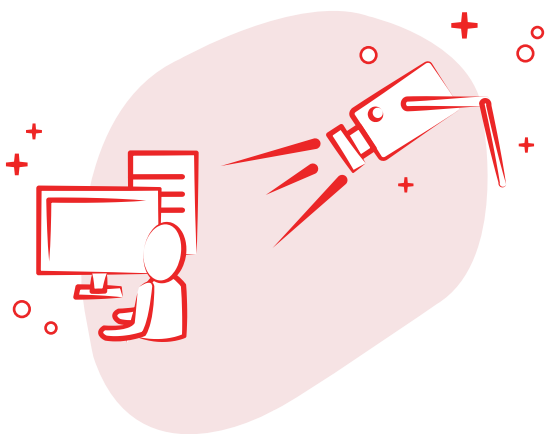
Gestión de cuentas privilegiadas

Adopte un enfoque de mejores prácticas para la gestión efectiva de las cuentas privilegiadas que forman el perímetro de seguridad alrededor de los servidores de datos de misión crítica y otros activos de TI en su entorno, ya sea que usen autenticación basada en contraseña o en clave, incluyendo las de sistemas operativos, bases de datos, servidores, aplicaciones, plataformas en la nube y dispositivos de red.

Gestión del acceso remoto

Establezca un control centralizado sobre las vías de acceso y defina cómo se conectan los usuarios a los sistemas de destino. Garantice la máxima seguridad en todas las conexiones privilegiadas con funciones de inicio de sesión con un solo clic en lugar de compartir las credenciales en texto claro. Haga conexiones de túnel a través de un gateway de canal cifrado, que no requiere conectividad directa entre el dispositivo del usuario y el host remoto.



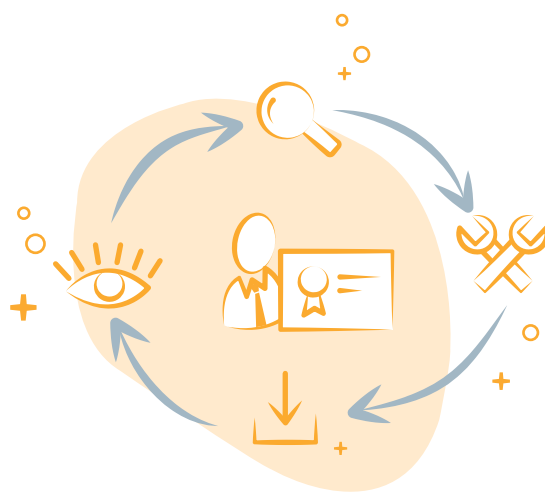


Gestión de sesiones privilegiadas

Esté al tanto de lo que hacen sus usuarios con su acceso privilegiado y evite el uso indebido. Facilite el monitoreo avanzado para comprobar si los usuarios, tanto empleados como terceros, se mantienen dentro de su ámbito de aprovisionamiento. Responda fácilmente a las preguntas sobre "quién", "qué" y "cuándo" del acceso privilegiado.

Gestión de certificados SSL

Obtenga completa visibilidad y control de su entorno SSL. Aléjese de los riesgos relacionados al descuido con respecto a la caducidad de los certificados, de los algoritmos de hashing obsoletos y de los conjuntos de cifrado débiles que le cuestan la confianza de sus clientes. Experimente una gestión integral y sin complicaciones de los ciclos de vida de los certificados.



Resumen general de funciones



Descubra rápidamente contraseñas, claves SSH y certificados SSL implementados en su red y almacénelos de forma segura en una bóveda centralizada.



Genere fácilmente pares de claves SSH y asócielas a los usuarios. Asigne contraseñas nuevas y seguras para los sistemas remotos.



Rote regularmente las contraseñas y los pares de claves con un estricto cumplimiento de la política. Establezca una sólida rutina de gestión de contraseñas para las cuentas de servicio.



Elimine las credenciales codificadas en los archivos de configuración y los scripts con API seguras para la gestión de contraseñas de aplicación a aplicación (A-to-A) y de aplicación a base de datos (A-to-DB).



Importe los certificados asignados a las cuentas de usuario en su servicio de Active Directory. Automatice completamente la gestión de su ciclo de vida mediante la integración con su propia autoridad de certificación.



Comparta de forma segura las contraseñas o las claves SSH con los usuarios durante un tiempo determinado y revoque el permiso automáticamente.



Programe análisis periódicos para detectar contraseñas débiles, vulnerabilidades en la configuración de SSL, etc.



Actualice remotamente las contraseñas de una amplia gama de sistemas de destino mediante la compatibilidad out-of-the-box, los creadores de plugin personalizados y los flujos de trabajo de restablecimiento basados en comandos SSH.



Mejore la seguridad de DevOps con plugins nativos de gestión de cuentas privilegiadas para Jenkins y Ansible, y sustituya las contraseñas incrustadas por flujos de trabajo de solicitud-liberación para los procesos de automatización de SDLC.



Automatice completamente la adquisición, la implementación, la renovación y la revocación de certificados SSL para dominios públicos mediante la integración out-of-the-box con Let's Encrypt, GoDaddy, Microsoft CA y The SSL Store.



Conecte dispositivos (RDP, SSH, SQL) a recursos sensibles con un solo clic a través de túneles seguros y sin contraseña.



Grabe y almacénelas como archivos de vídeo para futuras consultas.



Refuerce la autenticación de los usuarios con servicios de segundo factor seguros como RSA SecurID, Duo Security, YubiKey, Google Authenticator, RADIUS y OTP por email.



Monitoree estrechamente las sesiones activas en tiempo real, supervise la actividad de los usuarios y finalice las sesiones al detectar actividades sospechosas.



Realice un control continuo de todas las operaciones de los usuarios con un extenso log de auditoría y con información sobre la actividad en tiempo real.



Integre sin problemas los servicios basados en Active Directory/LDAP, los sistemas de tickets de la empresa, las herramientas SIEM, los servidores de syslog y los proveedores de servicios SAML 2.0.

About us

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 90+ products and free tools cover everything your IT needs, at prices you can afford. From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.

[Download now](#)

[Video demo](#)

180,000+
companies around the world trust

ManageEngine

manageengine.com/pim

For questions: sales@manageengine.com
Toll-free number: +1 888 720 9500



Zoho Corporation
4141 Hacienda Drive
Pleasanton, CA 94588
USA
Phone: +1-925-924-9500