ManageEngine
Password Manager Pro

8 cosas que hay que hacer para una estrategia perfecta de gestión de cuentas privilegiadas

Los expertos están de acuerdo:

La gestión de cuentas privilegiadas (PAM) es uno de los principales proyectos de seguridad de las organizaciones. Teniendo esto en cuenta, he aquí un conjunto de 8 cosas imprescindibles que todo jefe de TI debería implementar para impulsar un programa PAM sólido.

01 Reúna todas sus cuentas privilegiadas bajo un mismo techo.

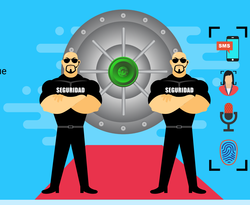
Ejecute un programa totalmente automatizado que analice regularmente su red, detecte nuevas cuentas y las añada a una bóveda central. Para evitar accesos no deseados, refuerce la protección en torno a la bóveda con algoritmos de cifrado conocidos, como AES-256.

02 Decida quién puede acceder a qué.

Establezca roles bien definidos con los privilegios de acceso mínimos requeridos para los miembros de su equipo de TI, y garantice que todas las actividades en torno a la bóveda sean trazables hasta los empleados autorizados.

03 Combine algo que usted sabe con algo que tiene.

Implemente la autenticación multifactorial tanto para los administradores de PAM como para los usuarios finales para garantizar que la persona que inicia sesión es quien dice ser. Conocer una contraseña ya no es suficiente para mantener seguros los recursos sensibles.



04 Piense antes de compartir.

Proporcione a los empleados o contratistas acceso a los activos de TI sin revelar las credenciales en texto plano. Permita a los usuarios iniciar conexiones con un solo clic a los dispositivos de destino desde la interfaz de su herramienta PAM, sin necesidad de ver o introducir manualmente las credenciales.

05 Inicie el restablecimiento automático de las contraseñas.

Haga que el restablecimiento automático de las contraseñas sea una parte integral de su estrategia PAM. Sustituya las contraseñas predeterminadas y no modificadas por contraseñas robustas y únicas que se restablezcan periódicamente.

06 Fomente una cultura de conocer solamente lo necesario.

Exija a los usuarios que envíen una solicitud al administrador de PAM de su organización siempre que necesiten credenciales de cuenta específicas para acceder a un activo remoto. También puede proporcionar a los usuarios un acceso temporal, basado en el tiempo, a estas credenciales, y restablecer automáticamente las credenciales una vez que expire el tiempo estipulado.

07 Deje que las API hablen.

Utilice API seguras para permitir que las aplicaciones consulten su herramienta PAM directamente y recuperen las credenciales de cuentas privilegiadas para comunicarse con otra aplicación o un activo remoto.

08 Asegúrese de que todo sea auditado.

Capture todas las operaciones de los usuarios y establezca la responsabilidad y la transparencia de todas las acciones relacionadas con las PAM. Vaya un paso más allá e integre su herramienta PAM con una herramienta de registro de eventos y consolide las actividades de PAM con otros eventos del resto de su organización para recibir consejos inteligentes sobre actividades inusuales.