ManageEngine
PAM360

Modelo de madurez de PAM

Cree su propia travesía de PAM

Introducción

Las identidades privilegiadas han proliferado en cada faceta del entorno empresarial. Ahora son prevalentes dentro de componentes fundamentales de la empresa, tanto en TI como en otros, incluyendo ingeniería, recursos humanos, nómina, sistemas operativos, sistemas directivos, hipervisores, aplicaciones en la nube, líneas CI/CD y rutinas de RPA. Con más y más identidades privilegiadas entretejidas en los flujos de trabajo corporativos de las organizaciones, ahora hay una necesidad de gestionar extensivamente la autenticación y controlar el acceso a cualquier aspecto colateral crítico del negocio mediante estas identidades privilegiadas.

Se ha aconsejado ampliamente la gestión de acceso privilegiado (PAM) como una adición obligatoria a su portafolio de gestión de TI, pero ya no es solo eso. La PAM ha sobrepasado su dominio y propósito como una simple estrategia de gestión de TI. Ahora es una necesidad en el proceso corporativo.

Con el fin de controlar el acceso privilegiado, se aconseja a las organizaciones que incorporen las mejores prácticas de PAM en cada parte del marco de procesos de su negocio. Sin embargo, esta implementación de la PAM diferirá según cada organización,

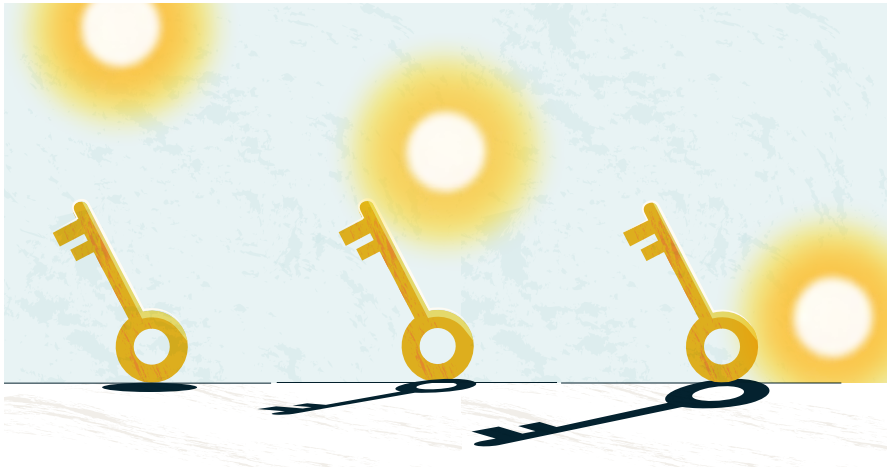
dependiendo de su fase de madurez debido al hecho de que distintas organizaciones tienen infraestructuras, perfiles de riesgo, prioridades financieras, requisitos de seguridad y casos de uso específicos únicos para el acceso privilegiado.

Potenciado con las decenas de años de experiencia de ManageEngine en investigación intrincada, las inferencias de miles de implementaciones de PAM, una base de clientes y nuestra experiencia como un jugador líder en el mercado global de PAM, traemos un modelo de madurez que es plenamente inclusivo, pero que al mismo tiempo es efectivo e inflexible.

Nuestro modelo de madurez de PAM lo ayudará a entender en qué fase de madurez se encuentra y le dará información sobre cómo emprender su travesía de PAM y aumentar su madurez de PAM con base en su perfil de riesgos, presupuesto, tipos y número de identidades privilegiadas, y prioridades de TI sin importar a qué mercado vertical pertenezca.

Identifique su método de madurez de PAM

Su madurez y superficie de ataque son inversamente proporcionales. Entre más madurez de PAM posea, menor es la superficie de ataque.

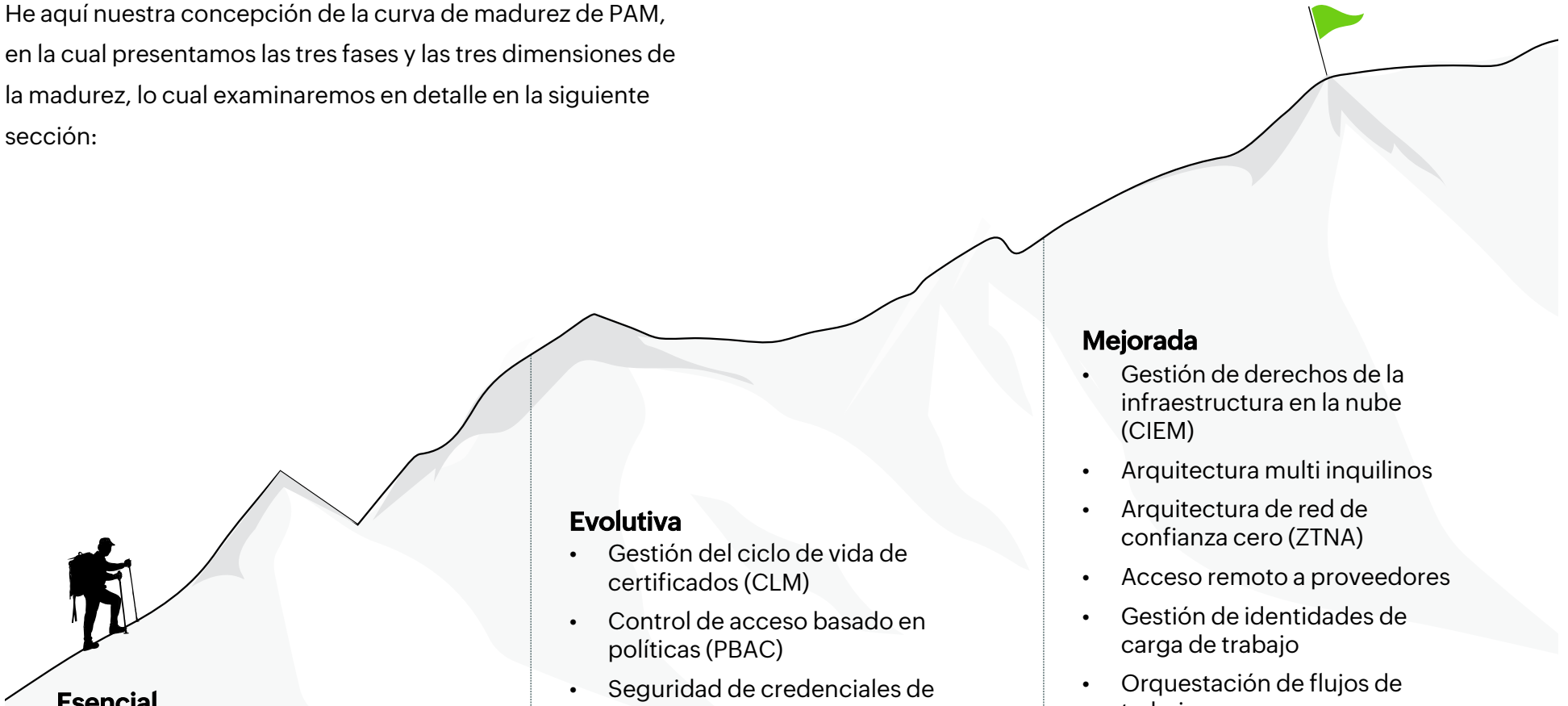


Notará que el amplio abanico de casos de uso que la PAM ofrece y el control que proporciona sobre su superficie de ataque aumentan según avanza por cada fase de madurez de PAM. Simultáneamente, también notará un aumento en la cantidad de automatización involucrada (mediante integraciones con otros flujos de trabajo corporativos y de TI) y la influencia de controles guiados por IA.

Varios analistas de la industria han establecido un consenso sobre dónde empieza y termina generalmente una travesía de PAM. Asimismo, han discutido ampliamente qué funciones de PAM debería adoptar una organización en el camino hacia la madurez de PAM.

Teniendo esto en cuenta y con base en nuestra extensiva investigación sobre las tendencias de los mercados, creemos que todas las organizaciones, según sus necesidades, pueden agruparse en tres fases: esencial, evolutiva y mejorada. Con base en esa interpretación, tenemos una gráfica de madurez que categoriza este enorme conjunto de funciones de PAM en tres dimensiones. Hemos determinado también que la fase de madurez de una organización se determina según cuánto ha implementado las funciones en cada dimensión de madurez.

He aquí nuestra concepción de la curva de madurez de PAM, en la cual presentamos las tres fases y las tres dimensiones de la madurez, lo cual examinaremos en detalle en la siguiente sección:



Esencial

- Control de acceso privilegiado
- Control de acceso basado en roles (RBAC)
- Auditorías y cumplimiento

Evolutiva

- Gestión del ciclo de vida de certificados (CLM)
- Control de acceso basado en políticas (PBAC)
- Seguridad de credenciales de aplicaciones
- Elevación de privilegios
- Análisis de amenazas privilegiadas
- Integraciones – IUTSM e IGA

Mejorada

- Gestión de derechos de la infraestructura en la nube (CIEM)
- Arquitectura multi inquilinos
- Arquitectura de red de confianza cero (ZTNA)
- Acceso remoto a proveedores
- Gestión de identidades de carga de trabajo
- Orquestación de flujos de trabajo

Al progresar más desde el origen de la curva de madurez, observará que la PAM no será más una estrategia de TI en silo que solo tiende a compartir secretos, sino que es una adición obligatoria a cualquier proceso corporativo.

Dimensiones

&

fases de la madurez de PAM

Definimos cada una de estas fases de madurez de esta manera para justificar la complejidad, efectividad y método de implementación de los controles contenidos en ellas. Estos controles y su forma de implementación definen la fase de madurez en sí y mapean dónde empieza y termina, por lo que esencialmente definen sus dimensiones. En consecuencia, estos son lo que nos gusta llamar las dimensiones de la madurez. Estas dimensiones de la madurez se basan en un consenso común de analistas populares de la industria.

Dimensiones de la madurez

Gobernanza, riesgo y cumplimiento

La gobernanza, riesgo y cumplimiento (GRC), en el contexto de la PAM, se refiere a controles que permiten a las organizaciones tomar un control completo de los procesos de creación, descubrimiento, intercambio y auditoría de identidades privilegiadas. La GRC no es solo una dimensión de la madurez de PAM, sino también una práctica de seguridad que las organizaciones normalmente siguen y que se incorpora en cualquier proceso corporativo. La dimensión de GRC se explora principalmente en la fase esencial de su travesía de PAM.

Zero Trust

Zero Trust es un marco de seguridad que exige los siguientes tres principios centrales y cualquier proceso corporativo que involucre el uso de identidades privilegiadas: siempre verificar, asumir violaciones y acceso de mínimos privilegios. Las medidas para el control del acceso que incorporan estos tres principios en sus esquemas de funciones, por tanto practicando la filosofía de Zero Trust en la gestión de acceso privilegiado y de endpoints, constituyen esta dimensión de nuestro modelo de madurez. Las organizaciones tienden a explorar mucho los controles de acceso de Zero Trust durante su fase evolutiva, lo que las impulsa más cerca que nunca al objetivo final:Zero Standing Privileges

Habilitación técnica

En nuestro modelo, la habilitación técnica es la solución que conecta el potencial abstracto de la TI de una empresa con su ejecución e implementación en tiempo real. Cuando las organizaciones aprovechan la habilitación técnica, mantienen el ritmo con respecto a los últimos avances tecnológicos y los aprovechan para un avance transformativo.

En el contexto de la PAM, los controles que permiten la colaboración entre su solución de PAM y otras aplicaciones de terceros para la orquestación de las rutinas de acceso privilegiado se categorizan generalmente como integraciones. Estas integraciones permiten la comunicación fluida entre varios procesos corporativos, entretejiendo la PAM a lo largo de cada nivel en la empresa. Mejorar aún más la fluidez de las integraciones, los controles de acceso y las estrategias de GRC al automatizarlas es solo la cereza del pastel.

Esto garantiza que los flujos de trabajo se ejecuten sin supervisión manual, deshaciéndose del error humano y, por tanto, satisfaciendo el estándar del mercado para un portafolio de PAM que demande cero privilegios permanentes. Las organizaciones en fases evolutiva y mejorada son las que en su mayoría buscan la habilitación técnica.

Fases de la madurez

En las siguientes secciones encontrará información detallada sobre cada fase, incluyendo aspectos específicos sobre qué ventajas puede buscar, retos que necesita abordar y oportunidades que debe explorar con el fin de avanzar a la siguiente fase.

¿Qué categorizamos como una ventaja?

Una organización que está en la vía de la transformación digital generalmente trata con preocupaciones amplificadas alrededor del riesgo y la seguridad. Si el efecto de un riesgo se reduce o elimina del todo al adoptar un control que es parte de cualquiera de las dimensiones de la madurez mencionadas, categorizamos este control como una ventaja.

¿A qué nos referimos con retos?

La confianza cero es un marco de seguridad que exige los siguientes tres principios centrales y cualquier proceso corporativo que involucre el uso de identidades privilegiadas: siempre verificar, asumir violaciones y acceso de mínimos privilegios.

Las medidas para el control del acceso que incorporan estos tres principios en sus esquemas de funciones, por tanto practicando la filosofía de confianza cero en la gestión de acceso privilegiado y de endpoints, constituyen esta dimensión de nuestro modelo de madurez. Las organizaciones tienden a explorar mucho los controles de acceso de confianza cero durante su fase evolutiva, lo que las impulsa más cerca que nunca al objetivo final: cero privilegios permanentes.

¿Qué consideramos oportunidades?

Abordar un reto al adoptar cualquier medida que haga parte de cualquiera de las dimensiones de la madurez en una fase particular de la madurez es una oportunidad que debe explorarse. Si dicha exploración resulta en una reducción de la supervisión administrativa manual o de la superficie de ataque, es posible acelerar su madurez de PAM y, a su vez, avanzar hacia una fase de madurez mayor.

PAM manual

Si su portafolio de TI de gestión de accesos e identidades no incorpora alguna de las dimensiones de PAM mencionadas arriba (GRC, confianza cero y habilitación técnica), eso significa que aún no ha iniciado su travesía de PAM. En este punto, no hay necesariamente ventajas que la organización pueda buscar. De hecho, las organizaciones con PAM manual tienen varios retos que abordar y una gran variedad de oportunidades por explorar.

Las organizaciones que aún no han iniciado su travesía de PAM tienden a practicar la gestión secreta mediante credenciales de código fuerte y otras identidades privilegiadas en archivos de texto y los comparten sin una solicitud y mecanismos de liberación adecuados, lo que da campo a amenazas críticas a las identidades y a horas administrativas improductivas.

En la siguiente tabla puede ver qué clase de controles le hacen falta en cada dimensión si está gestionando manualmente sus identidades privilegiadas.

Dimensión de la madurez	Controles
GRC	• No hay gestión centralizada de las identidades y usuarios privilegiados • No hay un inventario central para gestionar los endpoints y secretos privilegiados • No hay una regularización o rotación de identidades privilegiadas • No se implementan medidas para auditar el intercambio del acceso • No hay medios para grabar o revisar sesiones privilegiadas • No se cumple con los estándares de TI federales, tales como HIPAA, SOX y el PCI DSS
Zero Trust	• No hay medios para dar acceso efímero o periódico a un dominio privilegiado o cuentas root en Windows y Linux • Sin capacidad de compartir acceso restringido por tiempo a endpoints y secretos privilegiados • No se implementa un formulario de acceso de mínimos privilegios (controles de acceso basados en roles o políticas) • Mucha dependencia en el intercambio directo con el dominio privilegiado o cuentas root
Habilitación técnica	• Sin descubrimiento automático o vinculación de cuentas locales y de dominio • Sin integraciones a herramientas de TI internas, como ITSM, ITOM y herramientas para análisis de TI • Sin medios de análisis del acceso privilegiado usando UEBA • Sin integración de 2FA o MFA • Sin forma de gestionar la solicitud de credenciales aplicación a aplicación y aplicación a base de datos • Sin medios para gestionar secretos críticos pertenecientes a plataformas CI/CD, rutinas de RPA, contenedores en la nube o microservicios

Si se ajusta a la categoría anterior y se encuentra en las estribaciones de la travesía de PAM, eso es bueno, pues lo tenemos cubierto. Si desea verificar nuestra guía de compradores de PAM, que lo ayudará a empezar su travesía de PAM al tomar las decisiones correctas, puede hacerlo aquí.

Fase 1
Esencial

Todas las organizaciones empiezan su travesía de PAM en esta fase. En esta fase se espera que las organizaciones opten por soluciones para abordar sus necesidades de almacenamiento de identidades privilegiadas. Sin embargo, una organización de escala pequeña con un número pequeño de endpoints privilegiados e incluso menos administradores y usuarios que necesitan acceso privilegiado a dichos endpoints privilegiados tiende a aferrarse a esta fase de madurez hasta que su perfil de riesgos demande otra cosa.

Si implementa un mecanismo o herramientas para ayudarlo a reducir la codificación incrustada de sus identidades privilegiadas a través del descubrimiento automático y rotación de secretos, almacenamiento central e intercambio auditado del acceso a identidades privilegiadas, en la actualidad se encuentra en la fase esencial de su travesía de PAM.

Ventajas

Una organización que está en la vía de la transformación digital generalmente trata con preocupaciones amplificadas alrededor del riesgo y la seguridad. Si el efecto de un riesgo se reduce o elimina del todo al adoptar un control que es parte de cualquiera de las dimensiones de la madurez mencionadas, categorizamos este control como una ventaja.

Cuando está en la fase esencial de su travesía de PAM, hay varias ventajas que puede buscar obtener, especialmente de la dimensión de GRC.

- Ejerza control sobre usuarios y cuentas privilegiados al proteger sus credenciales en una consola de PAM accesible centralmente.
- Habilite la MFA para usuarios privilegiados que acceden al dashboard de PAM.
- Imponga limitaciones de acceso en términos de los roles de los usuarios privilegiados al asignar roles de usuarios privilegiados que aborden necesidades de acceso específicas y nada más.
- Aplique un proceso de solicitud y liberación que requiera la aprobación de todas las solicitudes de acceso por parte de administradores de TI específicos.
- Haga un inventario de las contraseñas y reduzca el código fuerte al encriptarlas usando una bóveda central. Implemente políticas complejas de contraseñas para todas las contraseñas en la empresa.
- Descubra automáticamente usuarios privilegiados, cuentas locales y de dominio de Windows, cuentas de servicios de Windows, cuentas root de Linux, dispositivos de red, equipos virtuales y mucho más desde varios directorios, como AD; LDAP y AWS.
- Establezca rutinas automáticas de restablecimiento de contraseñas de acuerdo con los estándares de TI organizacionales.
- Mantenga pistas de auditoría de extremo a extremo para controlar toda actividad privilegiada en la red.
- Registre todas las sesiones privilegiadas para la revisión del acceso, detección de amenazas y medidas de respuesta.
- Genere convenientemente informes que determinen la adherencia a estándares de cumplimiento, como HIPAA, el PCI DSS y SOX.

Retos

En su fase esencial, el reto principal que una organización enfrenta es la regularización del intercambio de secretos digitales. En esta fase, una organización típicamente tiene controles para gestionar el intercambio de secretos. Sin embargo, un administrador de TI debe revocar manualmente estos secretos tras su finalización. Así, un administrador debe rotar estos secretos o contraseñas.

Además, este intercambio de acceso no es efímero y no limita las oportunidades para abusar de los privilegios durante estas sesiones privilegiadas. Una vez se autentica una solicitud de acceso, el usuario tiene acceso ilimitado a todo el equipo y no está restringido por el tiempo o límites de acceso.

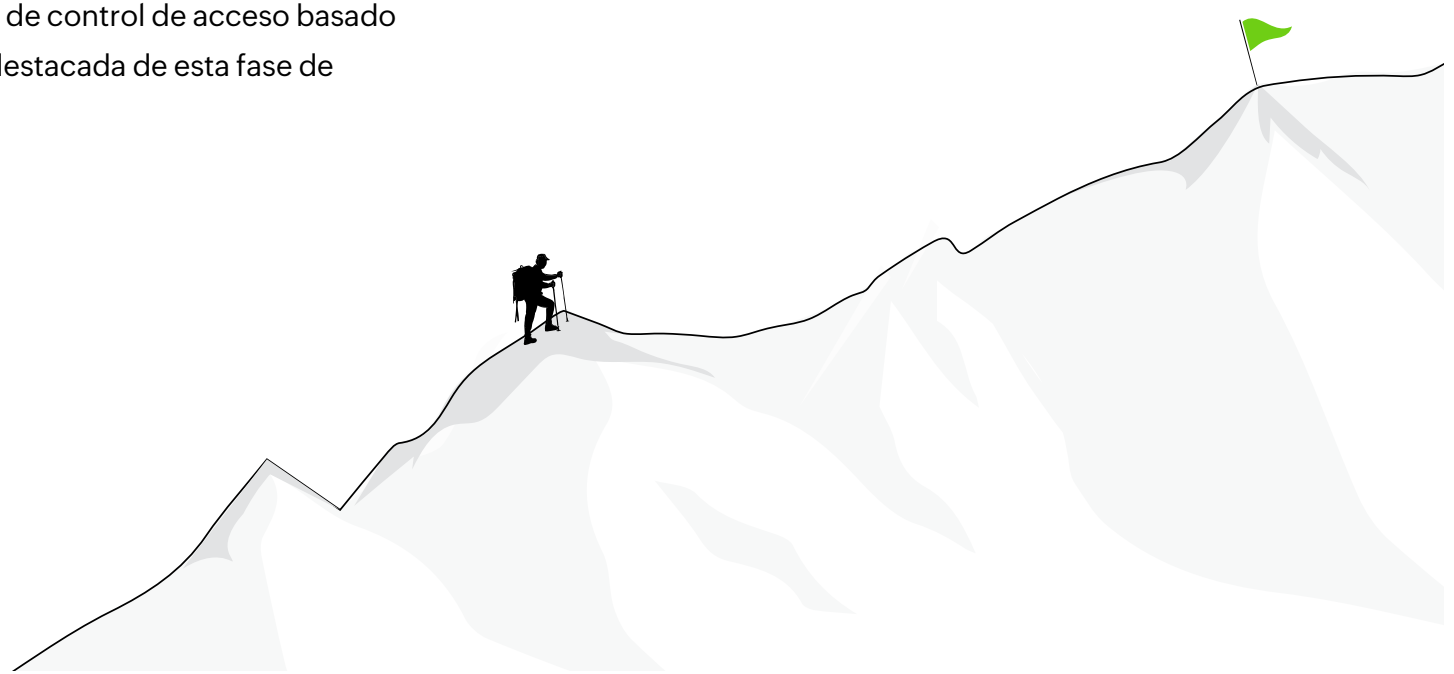
Oportunidades

Cuando progresa más, con el fin de superar los retos asociados con su fase de madurez, debe adoptar estrategias que escudriñen más si el intercambio de secretos es necesario para cada caso. Para limitar más el intercambio de acceso, adopte controles de confianza cero como controles de acceso basados en políticas, acceso y elevación de privilegios justo a tiempo (JIT) y controles de comandos y aplicaciones para endpoints de Windows y Linux.

Dimensión de la madurez	Controles
GRC	• Una bóveda central para gestionar las identidades privilegiadas de los usuarios • Un inventario central para gestionar los endpoints y secretos privilegiados • Regularización o rotación de identidades privilegiadas • Auditoría y grabación automatizadas de sesiones privilegiadas • Cumplimiento de los estándares de TI federales como HIPAA, SOX y el PCI DSS
Zero Trust	• Controles de acceso basado en roles para asignar el acceso según el perfil del empleado • Un proceso de solicitud y liberación para solicitudes de acceso con base en la aprobación del administrador
Habilitación técnica	• Descubrimiento automático y programado de cuentas privilegiadas desde directorios como AD y LDAP • Restablecimientos de contraseñas automatizadas y programadas de cuentas privilegiadas, incluyendo cuentas de servicios • Generación programada de informes personalizados para el inventario de cuentas privilegiadas • Revocación automática de acceso privilegiado con base en un periodo de tiempo estipulado previamente

Conclusión

Las organizaciones en esta etapa de su madurez de PAM con frecuencia establecen controles como y cuando lo consideran adecuado, reaccionando a incongruencias en sus redes de TI cuando se presentan. Su método de seguridad de TI es más reactivo que proactivo. Normalmente definen el intercambio de acceso sobre una base de todo o nada y tienen controles limitados para la detección, mitigación y respuesta ante amenazas. Sus implementaciones con frecuencia incluyen una función de descubrimiento automático de cuentas que descubre cuentas directamente desde los directorios de la organización, así como una función de control de acceso basado en roles que sirve como la función destacada de esta fase de madurez no pulida pero incipiente.



Fase 2
Evolutiva

El objetivo principal asociado con la fase 2 de la madurez de PAM es reducir el número de contraseñas privilegiadas compartidas y a su vez aumentar la cantidad de verificaciones y medidas implementadas para ellas. Esto es posible al explorar la dimensión de confianza cero más allá del método binario del intercambio de acceso contextual y al tratar con las solicitudes de acceso según cada caso. Además, en esta fase, las organizaciones implementan integraciones completamente funcionales entre su solución de PAM, otras herramientas para la gestión de TI (como herramientas de ITSM) y soluciones de seguridad secundarias (como la detección y respuesta extendidas (XDR) y herramientas de SIEM).

Si su organización ha dominado el intercambio de acceso mediante controles avanzados y detallados, como la elevación de privilegios JIT, controles de acceso guiados por puntuaciones de confianza y basados en políticas, y controles de aplicación y comando, entonces su madurez está evolucionando rápidamente.

Ventajas

En la cima de las varias ventajas que se disfrutan en la primera fase, las organizaciones en la fase evolutiva pueden añadir más capas a su manto de madurez de PAM, con un enfoque en la dimensión de la confianza cero.

- Mida las posturas de los usuarios y dispositivos usando evaluaciones de riesgos en tiempo real para aislar posibles actores maliciosos. Emplee un sistema de puntuación de confianza con base en las evaluaciones de riesgos e idee políticas de acceso adecuadas con base en las puntuaciones.
- Configure políticas de acceso que permitan o denieguen solicitudes de acceso automáticamente con base en las puntuaciones de confianza asociadas con los usuarios privilegiados y endpoints.
- Comparta el acceso temporal a cuentas privilegiadas como cuentas de dominio de Windows y cuentas root de Linux.
- Limite más las oportunidades de abusar de los privilegios durante sesiones privilegiadas al exigir controles de comandos y de aplicaciones.
- Extienda la PAM no solo a contraseñas sino también a identidades de equipos, como certificados y claves, mediante la gestión del ciclo de vida de los certificados.
- Controle la recuperación de credenciales aplicación a aplicación mediante API personalizadas.
- Regule el acceso a aplicaciones empresariales críticas mediante servidores de gateway de acceso seguro.
- Integre su solución de PAM con herramientas de ITSM para validar las solicitudes de acceso según la ID del ticket generado en la herramienta de ITSM.
- Integre con herramientas de UEBA para supervisar el comportamiento de usuarios y recursos a lo largo de su implementación de PAM y mitigue cualquier posible riesgo de seguridad.
- Integre con herramientas de proveedor de identidad (IdP) y de gobernanza y administración de identidades (IGA) para mapear los privilegios de los usuarios con base en sus atributos.
- Integre con soluciones de seguridad adyacentes, como soluciones de XDR, SIEM y SOAR, para facilitar el acceso privilegiado a endpoints y servidores con base en análisis de amenazas en tiempo real.

Retos

En la fase evolutiva el elefante en el cuarto que toda organización lucha por abordar es la adopción empresarial del principio de confianza cero de eliminar los privilegios permanentes. Este proceso de eliminación se cataliza mediante la incorporación de controles de acceso detallados para formular todas las posibles situaciones para escudriñar las solicitudes de acceso y garantizar cero privilegios permanentes en cada paso del camino.

Este reto va más allá del reino de la gestión de TI, extendiéndose a cualquier flujo de trabajo en la red empresarial que demande acceso privilegiado. En la fase evolutiva, las organizaciones luchan por expandir la aplicación de controles de acceso de confianza cero en todas las facetas de las operaciones de TI y operativas. Esto resulta en una falta de integradores y conectores, lo que permite la expansión de la seguridad del acceso privilegiado para las necesidades empresariales de PAM.

Oportunidades

Para superar los retos asociados con la fase evolutiva, debe ampliar la implementación de la PAM más allá de la TI. La automatización e integración son la grasa que su motor de PAM necesita, que por lo demás es completamente funcional.

Aunque se trate de adiciones aparentemente menores e invisibles, los esfuerzos de habilitación técnica que se concentran en la integración y automatización pulirán su implementación de PAM para ejecutarse fluidamente e implementar el principio de cero privilegios permanentes en todos los tipos de procesos corporativos. Esto se puede abordar desde distintos ángulos, como las integraciones con plataformas de contenedores y herramientas de DevOps, así como la automatización para procesos robóticos y corporativos.

Dimensión de la madurez	Controles
GRC	• Evaluaciones de riesgos en tiempo real (popularmente en la forma de puntuaciones de confianza) para todas las cuentas, según varias acciones privilegiadas realizadas • Gestión del ciclo de vida de los certificados • Gestión de credenciales aplicación a aplicación
Zero Trust	• Controles de acceso basados en políticas para validar el intercambio de accesos con base en el comportamiento de los usuarios y de los endpoints • Controles de aplicaciones y comandos para endpoints privilegiados • La elevación de privilegios JIT de cuentas privilegiadas como cuentas locales y de dominio de Windows y cuentas root de Linux • Aprovisionamiento de acceso mediante servidores de gateway de acceso seguro
Habilitación técnica	• Integraciones con sistemas de tickets para automatizar el aprovisionamiento del acceso • Integraciones con herramientas de IDP e IGA para lograr una seguridad holística en el acceso privilegiado al aplicar políticas de acceso a nivel detallado y mapear privilegios con base en el rol, departamento grupos de directorio y requisitos del usuario • Integración con herramientas de UEBA para determinar el comportamiento estándar del usuario y detectar posibles amenazas de actores internos • Integraciones con soluciones de seguridad adyacentes, como soluciones de XDR, SIEM y SOAR, para gestionar los privilegios de endpoints y permitir la correlación de eventos en tiempo real y así tomar mejores decisiones de seguridad

Conclusión

Las organizaciones en la fase evolutiva implementan una rutina robusta de PAM para repeler el abuso de privilegios mediante controles de acceso con confianza cero. Aunque la fase evolutiva es un buen lugar para estar, las organizaciones en esta fase tienden a perderse de las ventajas que da explorar la habilitación técnica mediante la integración y la automatización.

Fase 3
Mejorada

Cuando la rutina de PAM de una organización se extiende más allá de los confines de la infraestructura de gestión de TI para abarcar todas las identidades privilegiadas en el panorama corporativo digital, se equilibra para lograr la velocidad de escape. Los controles de acceso robustos desprovistos de credenciales de código incrustado cubren todos los niveles de operación, empleando medidas multi faceta y multi capa para detectar y evitar intrusiones en varios puntos. Las recomendaciones de la industria también abogan por funciones de PAM que regulen el acceso privilegiado para colaboradores externos, como auditores y proveedores.

En pocas palabras, cuando la PAM de una organización ha evolucionado para automatizar integralmente los controles de acceso, abarcando el aprovisionamiento, rotación, desaprovisionamiento y presentación de informes con un compromiso inflexible para lograr cero privilegios permanentes a escala empresarial, esa organización está en la fase de madurez mejorada de PAM. Además, las organizaciones en la etapa mejorada con frecuencia buscan aumentar su postura de seguridad con una solución para la gestión de derechos de la infraestructura en la nube (CIEM) con el fin de controlar los riesgos de acceso a la nube, especialmente en entornos híbridos y multi nube.

Ventajas

Mientras que dominar los controles de acceso puede ser ciertamente útil para que una organización obtenga un impulso considerable en su travesía de PAM, las ventajas que disfruta en la fase mejorada son lo que le permite alcanzar la meta definitiva de cero privilegios permanentes.

- Practique controles de identidad para sistemas heredados, infraestructuras multi inquilinos, SaaS y aplicaciones internas.
- Establezca mecanismos de autenticación para un método en capas para la seguridad del acceso privilegiado.
- Expanda la PAM a los niveles red, aplicación y base de datos al adoptar los principios de acceso a la red de confianza cero (ZTNA).
- Integre con plataformas de contenedores en la nube y DevOps para buscar y rotar automáticamente secretos encriptados de clusters y plataformas de contenedores de la nube, como Kubernetes, de acuerdo con políticas organizacionales personalizadas.
- Automatice e integre rutinas de acceso privilegiado en otras aplicaciones corporativas.
- Gestione centralmente los riesgos de acceso a la nube al implementar una solución de CIEM.

Retos

En la fase mejorada, su implementación ya no es responsable de solo la gestión de acceso; es una sombrilla que cubre cada forma de acceso privilegiado, incluyendo la TI y más. Una organización que se encuentre en esta fase de madurez generalmente batalla con escalar sus rutinas de seguridad de acceso privilegiado para sitios distribuidos geográficamente. Sugerimos optar por un proveedor de PAM que respalde el mejoramiento fácil de oportunidades sin elevar los costos de migración.

Cuando las operaciones de su empresa empiezan a abarcar varios puntos geográficos, lo más importante es maximizar los mecanismos de recuperación ante desastres al automatizar completamente servicios de failover al funcionar en situaciones adversas, de forma que no requieran intervención manual, lo que garantiza una continuidad corporativa eficiente.

Mientras que lograr un método inflexible de cero privilegios permanentes es necesario, también creemos que este método debe ser financieramente prudente. Todas las implementaciones de PAM deben tener un valor optimizado para evitar costos ocultos y eliminar las funciones innecesarias y excesivas que raramente se necesitan o que dañan su presupuesto de TI a largo plazo sin resultados reales.

Oportunidades

Mientras que se trata del fruto más importante de su travesía de PAM, la mejora que su organización puede incorporar en su perfil de TI es el mantenimiento sin errores, sobre todo ahora que se espera que todas sus rutinas de PAM funcionen autónomamente. El mantenimiento sin errores involucra actualizaciones constantes para descubrir cronogramas, restablecer cronogramas y acceder a ajustes de control, así como la supervisión constante de enlaces integrados entre su herramienta de PAM y otras aplicaciones corporativas.

Una oportunidad sobre la cual capitalizar que la mayoría de las organizaciones maduras en PAM tienden a ignorar es su ROI. Es importante optimizar los controles con el fin de lograr oportunidades rápido para dar valor a su ROI desde su solución de PAM.

Asimismo, resulta útil estar actualizado con las últimas tendencias del mercado y funciones de PAM con el fin de tomar la mejor decisión cuando se actualiza su solución de PAM.

Las organizaciones pueden aprovechar la extensión de la PAM más allá de las contraseñas y secretos a un abanico extensivo de identidades de equipos, como dispositivos de IoT, tecnología operativa (OT) y sistemas de control de supervisión y adquisición de datos (SCADA), y otras cargas de trabajo que no se gestionan convencionalmente dentro del alcance de la PAM.

Una organización es completamente madura en PAM si sus controles existentes satisfacen su perfil de riesgos existentes y posee cero privilegios permanentes en toda forma de acceso privilegiado a lo largo de la organización.

Dimensión de la madurez	Controles
GRC	• Control para sistemas heredados, infraestructuras multi-inquilinos, SaaS y aplicaciones internas • Control y monitoreo del acceso para derechos de la nube
Zero Trust	• Aumento de la autenticación por capas para políticas de acceso privilegiado por capas • ZTNA para gestionar el acceso privilegiado a nivel red, aplicación y base de datos • Acceso con un solo clic a través de la solución de PAM para proveedores externos y otros colaboradores que requieren acceso privilegiado
Habilitación técnica	• Integraciones con herramientas de DevOps y líneas CI/DI para gestionar secretos en rutinas de ingeniería • Integraciones con plataformas de contenedores como Kubernetes para automatizar la gestión de secretos basada en nube-cluster • Integraciones con herramientas de RPA para gestionar secretos que autentiquen rutinas de bots • Automatización de flujos de trabajo corporativos para entretejer la seguridad de acceso a lo largo de aplicaciones corporativas y rutinas de orquestación

Conclusión

Las organizaciones en la fase mejorada tienen todas las bases cubiertas igualmente. Tienen una práctica fluida de descubrimiento de cuentas que funciona por sí sola sin intervención manual para incorporar cuentas privilegiadas desde cualquier lugar, lo que satisface sus necesidades de GRC. Estas organizaciones también tienen controles de acceso detallados para contrarrestar el acceso no autorizado y el abuso de privilegios como resultado de explorar y adoptar la filosofía de confianza cero a lo largo de sus rutinas de seguridad. Estos controles también se automatizan y son capaces de integrarse contextualmente con otras aplicaciones de TI o corporativas.

¿Cuán rápido debe acelerar su madurez de PAM?

Ninguna organización tiene la misma paleta de colores cuando se trata de la aceleración de la madurez de PAM. Para organizaciones nuevas en el vagón de la transformación digital, proteger el acceso a su número limitado de identidades privilegiadas tendrá un impacto enorme sobre su perfil de riesgos, y las otras dimensiones (confianza cero y habilitación técnica) podrían seguirlo.

Sin embargo, cuando las organizaciones ya no dejan una huella digital tan grande, su perfil de riesgos también evoluciona para incorporar prioridades más complejas. Con la expansión también viene la necesidad de la escalabilidad y un mayor presupuesto de TI. Pero en ciertos casos, incluso si una compañía pudiera escalar digitalmente, su fuerza de trabajo podría permanecer estancada, llevando a que menos administradores gestionen un abanico más amplio diverso de endpoints críticos. Estas organizaciones tenderán naturalmente a priorizar la automatización sobre otros aspectos de la PAM.

En contraste, una compañía con endpoints críticos limitados pero que ahora expande su base de clientes tenderá a colaborar más con proveedores, contratistas y socios externos. Este tipo de organizaciones tiende a priorizar el gasto de TI en medidas de control de acceso de confianza cero.

¿Cuán rápido debe acelerar su madurez de PAM? Las organizaciones que realizan la travesía de PAM mediante una ruta que exige el cumplimiento tenderán a priorizar los controles de autenticación, grabación de sesiones privilegiadas y otras funciones que las ayuden a satisfacer los estándares de cumplimiento.

Al final del día, la aceleración de la madurez reduce el perfil de riesgos, el presupuesto de TI y las prioridades de cada organización.

¿Cómo puede ayudar ManageEngine?

El paquete de PAM empresarial de ManageEngine ayuda a las empresas a aplicar un control estricto en las rutas de acceso a endpoints y activos de misión crítica. Cargado con todos los aspectos esenciales de una PAM inteligente, nuestro paquete verifica todas las casillas para dar una postura de seguridad robusta mientras lo ayuda a alcanzar un ROI más rápido. Los productos para PAM de ManageEngine asumen un método holístico para la seguridad del acceso privilegiado al ofrecer integraciones contextuales con soluciones de gestión de TI, herramientas para desarrolladores y aplicaciones corporativas, lo que resulta en información útil, controles de acceso detallados y correcciones más rápidas.

Nuestra filosofía corporativa está profundamente enraizada en la investigación y desarrollo (I+D), a tal punto que nuestra compañía matriz, Zoho Corp., invierte 50% de sus ingresos en esfuerzos de I +D para generar y probar a futuro soluciones resilientes en seguridad de TI para las empresas de hoy y mañana. Creemos en generar soluciones, no adquirirlas.

Con dicha experiencia en el campo de la TI surge nuestro esquema preliminar sobre el que se construyen nuestros productos de PAM: la PAM no es una solución universal.

Los productos avanzados para PAM de ManageEngine están diseñados para arrancar donde y cuando los necesite, optimizados para acompañarlo a medida que progresa a través de la curva de madurez de PAM. Hemos comprobado nuestra experticia en generar soluciones extensivas para la gestión de TI que pueden integrarse nativa y contextualmente. En promedio, un cliente que usa una solución de PAM nuestra usa al menos otros cinco productos de ManageEngine, lo que elimina efectivamente la fatiga de proveedores.

Nuestra meta última no es hacerle una oferta que no pueda rehusar, sino hacer productos que de hecho use. Nuestra misión está definida por su progreso. Estamos aquí para suplirle las herramientas, recursos, estrategias y asesoría experta correctos que necesite para andar su travesía de PAM propia.

¿Por qué confiar en ManageEngine para su travesía de PAM?

El paquete de PAM empresarial de ManageEngine ayuda a las empresas a aplicar un control estricto en las rutas de acceso a endpoints y activos de misión crítica. Cargado con todos los aspectos esenciales de una PAM inteligente, nuestro paquete verifica todas las casillas para dar una postura de seguridad robusta mientras lo ayuda a alcanzar un ROI más rápido. Los productos para PAM de ManageEngine asumen un método holístico para la seguridad del acceso privilegiado al ofrecer integraciones contextuales con soluciones de gestión de TI, herramientas para desarrolladores y aplicaciones corporativas, lo que resulta en información útil, controles de acceso detallados y correcciones más rápidas.

He aquí algunas razones por las cuales más de un millón de administradores de TI confían a ManageEngine su PAM:

La solución para PAM del tamaño correcto para la empresa orientada al valor

ManageEngine ofrece un portafolio integral de PAM que aborda todos los casos de uso de PAM y niveles de madurez de la TI empresarial.

PAM360, nuestra solución de PAM insignia, realiza todas las funciones fundamentales de PAM para empresas de todos los tamaños. Con opciones de implementación flexibles y fáciles de usar, usted puede obtener valor más rápido con respecto a sus inversiones en seguridad.

Zero Trust por diseño, hasta el último detalle

ManageEngine ofrece un portafolio integral de PAM que aborda todos los casos de uso de PAM y niveles de madurez de la TI empresarial. PAM360, nuestra solución de PAM insignia, realiza todas las funciones fundamentales de PAM para empresas de todos los tamaños. Con opciones de implementación flexibles y fáciles de usar, usted puede obtener valor más rápido con respecto a sus inversiones en seguridad.

Fácil de implementar para lograr una rentabilidad rápida

Nuestros productos son más fáciles de instalar, configurar y gestionar, en comparación con otros programas que amplían las complejidades operativas y de mantenimiento. Con ManageEngine puede empezar a trabajar de inmediato. La mayoría de nuestros clientes pueden implementar completamente nuestros productos en cuatro semanas o menos. Además, proporcionamos modelos flexibles de implementación para ajustarnos mejor a sus necesidades.

Precio con valor optimizado con el fin de obtener un ROI más rápido

ManageEngine proporciona una estructura de precios transparente sin costos ocultos, add-ons inflados o contratos intrincados. PAM360 tiene licencias solo con base en el número de usuarios administrativos, sin límite alguno en el número de usuarios finales o endpoints. Ofrecemos todos los controles y funciones esenciales que desea en una solución de PAM sin afectar su presupuesto de TI.

Parte del entorno integral de gestión de TI en ManageEngine

En promedio, los clientes que usan un producto de ManageEngine también usan al menos otros cuatro productos de ManageEngine, incluyendo ITSM, UEBA y soluciones analíticas de TI. Nuestro entorno concentrado de TI ayuda a nuestros clientes a eliminar la fatiga de proveedores y crea una sinergia enorme para extender la PAM a la empresa, lo que los ayuda a progresar en las fases de su madurez rápida y coherentemente.

ManageEngine

PAM360