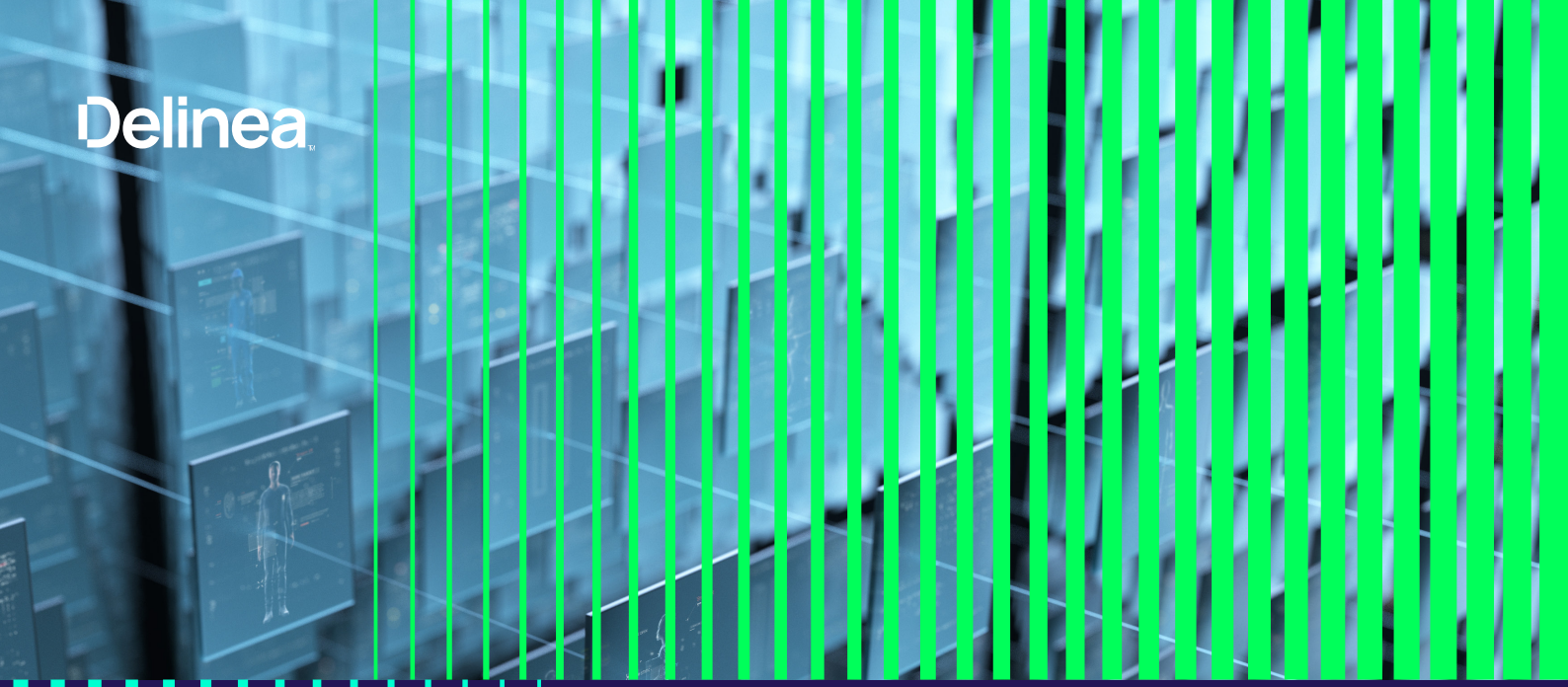
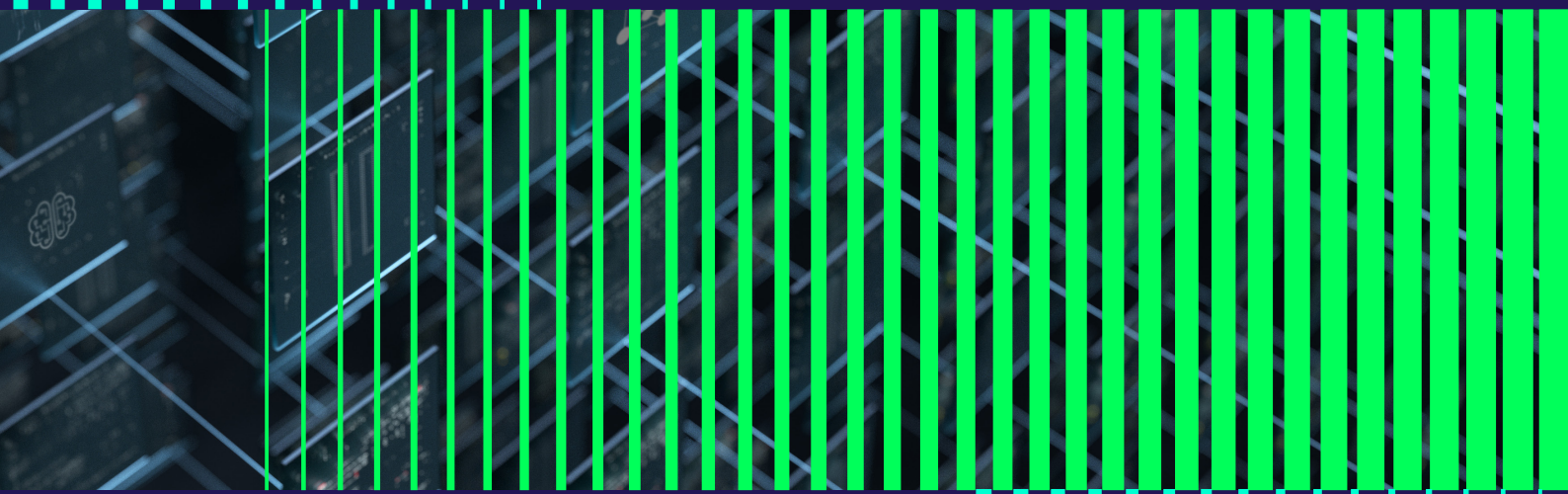


Delinea

Modelo de madurez de la gestión de accesos con privilegios



DOCUMENTO TÉCNICO

Modelo de madurez de la gestión de accesos con privilegios

Un marco para ayudar a las organizaciones a reducir sistemáticamente el riesgo de cuentas con privilegios, aumentar la agilidad empresarial y mejorar la eficiencia operativa

Introducción

El acceso con privilegios es el principal método que utilizan los atacantes para acceder a los sistemas sensibles. Proteger el acceso con privilegios en cada sistema se está convirtiendo en algo extremadamente importante para defenderse de estos ataques. El modelo de madurez de la gestión de accesos con privilegios (PAM) de Delinea es un marco que le ayuda a reducir sistemáticamente el riesgo de los accesos con privilegios, aumentar la agilidad del negocio y mejorar la eficiencia operativa.

El modelo está basado en las prácticas recomendadas del sector de la seguridad y en el trabajo de Delinea con más de 10 000 clientes de todo tipo, desde organizaciones que acaban de comenzar su experiencia de PAM hasta los usuarios más experimentados y avanzados de PAM.

Como líder en el mercado de PAM que trabaja para mejorar continuamente la postura de seguridad de nuestros clientes y reducir los riesgos empresariales, reconocemos la necesidad de actualizar y depurar la definición de madurez de PAM a medida que evoluciona el sector. Este último modelo es multidimensional y proporciona recomendaciones prácticas para la adopción de PAM paso a paso.

Puede aplicar las lecciones y orientaciones del modelo de madurez de PAM a su estrategia de ciberseguridad independientemente del tamaño de su empresa, su sector o el número y tipo de sistemas que necesite proteger. Le ayudará a navegar por su experiencia de PAM en función de sus propios factores de riesgo, presupuesto y prioridades.

Estrategia

El modelo de madurez de PAM consta de cuatro fases:

Con un mayor nivel de madurez, mayor será la superficie de ataque que pueda controlar

A medida que avanza en las fases de la curva de madurez, puede ampliar la protección para incluir más tipos de usuarios con privilegios, sistemas sensibles y sus cuentas con privilegios.

La mayoría de las organizaciones tienen exponencialmente más cuentas y sistemas con privilegios como empleados. Un subproducto de la migración a la nube es una superficie de ataque mucho mayor debido al aumento exponencial de cuentas con privilegios y sistemas virtuales. Las cuentas con privilegios incluyen cuentas de administrador de dominio, cuentas locales y cuentas de servicio no humanas que ejecutan aplicaciones, bases de datos y otras comunicaciones e intercambios de datos entre sistemas.

En una estrategia de PAM madura, el término «usuario con privilegios» ya no equivale a «usuario de IT». También incluye a los usuarios empresariales que acceden a información financiera, personal u otra información sensible desde aplicaciones web, así como a los desarrolladores que crean productos en plataformas que utilizan AWS, Azure, Google Cloud Platform o su propia nube.

En cada fase del modelo, el alcance de los usuarios con privilegios y los casos de uso se amplía. Las organizaciones en la fase de Fundamentos se centran en los administradores que utilizan máquinas Windows. Las

que se encuentran en la fase Avanzado incorporan a los usuarios empresariales, desarrolladores y terceros que utilizan sus propias estaciones de trabajo, así como los endpoints que no son de Windows, como Unix/Linux. El nivel de madurez Experto abarca también las cuentas no humanas.

Cuanto mayor es el nivel de madurez, más dinámica, automatizada e integrada es la estrategia

El significado de «acceso con privilegios» incluye no solo quién puede acceder a qué, sino también qué puede hacer con ese acceso y cuándo.

La madurez de la PAM comienza con políticas y controles estáticos, y se vuelve más granular y dinámica con cada fase. Los controles operativos nativos no son lo suficientemente granulares. A medida que se avanza en la curva de madurez, se añaden controles más granulares y se aplican condiciones y límites de tiempo para el acceso. En última instancia, los controles de acceso se basan en el riesgo y se adaptan a medida que cambia el perfil de riesgo.

La inteligencia y la automatización también aumentan. Pasar de la creación y rotación de contraseñas manual a la automática es el primer cambio. A partir de ahí, se automatizan más funciones hasta que, en última instancia, la PAM aprende y se adapta de forma continua como sistema inteligente.

La integración con otras herramientas empresariales es un aspecto clave de la automatización. Como tal, a medida que aumenta la curva de la madurez, se integran más tecnologías, hasta el punto de que prácticamente todos los usuarios con privilegios acceden a la PAM a través de otro sistema (sus herramientas ITSM o IGA, herramientas CI/CD para DevOps, navegadores web, clientes nativos, etc.) haciendo que la PAM resulte prácticamente «invisible».

Dimensiones de la madurez

Una incorporación importante a este modelo actualizado es una vista multidimensional de la madurez de la PAM. Cada fase de madurez se caracteriza por la estrategia de una organización hacia la PAM en estas tres dimensiones:

- **Gobernanza, riesgo y cumplimiento normativo (GRC)**: ¿cuál es la solidez de la integridad de su sistema y cuánta visibilidad y control tiene?
- **Administración de privilegios**: ¿cómo crea, define y gestiona los privilegios en su organización?
- **Gestión de identidades y accesos**: ¿cuál es la solidez de sus controles de autorización y la granularidad de sus controles de acceso?

En la descripción detallada de cada fase de madurez que aparece a continuación, aprenderá a evaluar la madurez de su PAM según estas dimensiones. No resulta extraño que una organización sea más madura en una dimensión que en otra. Una vez que evalúe su propio nivel de madurez, podrá priorizar las actividades de seguridad para que una dimensión no se acelere en exceso sin el apoyo de las demás.

Tenga en cuenta que las tres dimensiones de madurez no están vinculadas a roles de trabajo o funciones empresariales específicas. La gobernanza, por ejemplo, puede ser asumida por los responsables de la infraestructura de IT o los equipos de escritorio, y no necesariamente por una función central de GRC.

Tenga en cuenta que las tres dimensiones de madurez no están vinculadas a roles de trabajo o funciones empresariales específicas. La gobernanza, por ejemplo, puede ser asumida por los responsables de la infraestructura de IT o los equipos de escritorio, y no necesariamente por una función central de GRC.

¿Con qué rapidez debe acelerar su madurez?

La aceleración no es igual para todos. La madurez de su PAM debe reflejar su perfil de riesgo.

Para algunas organizaciones, la protección del acceso a un pequeño número de sistemas críticos tiene el mayor impacto en su perfil de riesgo general. Basándose en su tolerancia al riesgo, una empresa puede aplicar capacidades de PAM para un departamento, una región geográfica o un tipo de cuenta con privilegios, y nunca extenderlas a toda la organización.

Sin embargo, a medida que las organizaciones comienzan a escalar y a migrar más cargas de trabajo a la nube, el riesgo de seguridad aumenta, por lo que la madurez de la PAM debe seguir el ritmo. Por ejemplo, cuando las organizaciones hacen crecer las funciones de negocio, puede que no decidan, o no puedan, contratar personal de IT con experiencia, lo que significa que el mismo número de personas se encuentra bajo presión para gestionar un abanico más amplio y diverso de operaciones de IT y seguridad. La demanda de automatización de IT puede agilizar su aceleración a lo largo de la curva de madurez.

Del mismo modo, las organizaciones de rápido crecimiento tienden a trabajar con más proveedores, socios y contratistas a medida que se expanden a nuevos mercados y aumentan su oferta. Las organizaciones con un riesgo sustancial de terceros precisan una aceleración a lo largo de la curva de madurez más rápida que otras.

Por lo general, es probable que las organizaciones que están en proceso de transformación digital cuenten con más servicios en la nube y necesiten una gestión de privilegios madura de los servidores basados en la nube, las herramientas DevOps y las cuentas de servicio.

Aquellas que estén obligadas por regulaciones y normativa probablemente priorizarán la aplicación de políticas de mínimos privilegios, autenticación multifactor y monitorización de sesiones por encima de otras capacidades. A medida que aumenta su madurez, necesitarán personalizar y compartir fácilmente los informes con ejecutivos y auditores.

Las cuatro fases de madurez de la PAM

Los controles asociados a cada fase de madurez reflejan el orden que Delinea recomienda a las organizaciones para desplegar su estrategia de PAM. Este método de adopción de PAM paso a paso le ayuda a crear una base sólida que le brinda soporte a medida que escala.

FASE 0: punto de partida

La clave para las organizaciones en la fase 0 de madurez de la PAM es reconocer su riesgo y planificar la acción.

Las organizaciones en esta fase protegen sus cuentas con privilegios de manera limitada, si es que lo hacen. Por lo general, establecen los privilegios de forma manual y puede que lleven a cabo un seguimiento de los mismos mediante hojas de cálculo. Como resultado, a menudo proporcionan demasiados privilegios a personas que no los necesitan, comparten privilegios entre varios administradores y no eliminan los privilegios cuando los usuarios dejan la organización o cambian de función.

Suelen tener requisitos de complejidad mínimos para la creación de contraseñas y solo cuentan con autenticación de un solo factor, lo que abre la puerta al hackeo de las contraseñas.

Las cuentas de servicio se crean «a lo loco», lo que da lugar a una documentación deficiente, a una mala asignación a las aplicaciones o a los servicios principales, y a la «reutilización», en la que una misma cuenta se utiliza repetidamente para numerosos servicios.

También es común en entornos Linux/UNIX que los administradores creen sus propias cuentas con privilegios locales, ya que no disponen de una cuenta única/unificada (como una cuenta de Active Directory) para iniciar sesión en todas ellas. Esto hace que la superficie de ataque sea muy amplia.

Los equipos de seguridad y operaciones no suelen ser conscientes de la amplitud de las aplicaciones web que se utilizan y permiten a los usuarios tomar decisiones independientes en cuanto a los accesos y permisos con privilegios.

Estas organizaciones tienen un alto grado de riesgo cibernético. Si un atacante externo o una persona malintencionada tiene acceso a cuentas con privilegios, puede robar información confidencial, interrumpir la infraestructura de IT (incluso cerrarla) y acarrear costes millonarios.

Dimensiones de la madurez de la PAM	Características típicas
Gobernanza, riesgo y cumplimiento normativo	• No hay almacenes de PAM. • No hay inventario centralizado de todos los activos del entorno. • No hay una forma fácil de informar sobre los permisos y privilegios de acceso de los usuarios. • No hay una forma fácil de conciliar quién tiene acceso a qué, quién hizo qué ni quién aprobó el acceso. • Auditorías fallidas.
Administración de privilegios	• Gestión de la administración de los servidores Windows mediante la pertenencia al grupo de administradores de dominio. • Gestión de cuentas locales en cada sistema Unix/Linux y edición de archivos locales /etc/sudoers. • Los usuarios suelen ser administradores de sus propias estaciones de trabajo.
Gestión de identidades y accesos	• No hay controles de acceso centralizados. • La gestión de identidades no está centralizada. • Los administradores acceden utilizando cuentas de administrador locales. • Es difícil saber quién tiene acceso y qué privilegios tiene.

FASE 1: fundamentos

La clave para las organizaciones en la fase 1 de madurez de la PAM es obtener visibilidad sobre su superficie de ataque y comenzar a reducirla.

Una vez que han abierto los ojos, las organizaciones comienzan a tomar el control mediante la protección de las cuentas con privilegios compartidos. Se centran primero en las cuentas con privilegios gestionadas por los administradores de dominio y otros usuarios de IT.

Aunque las organizaciones son más maduras en esta etapa, siguen operando en modo reactivo. Suelen contar con numerosas herramientas y prácticas desconectadas, en lugar de un sistema integrado gestionado de forma centralizada y controlado por políticas. No diferencian el acceso en función de las funciones, no tienen suficiente visibilidad sobre el uso de las cuentas y no pueden producir de forma fácil o automática informes o documentación de cumplimiento normativo.

Las organizaciones que se encuentran en esta fase deben hacer esfuerzos periódicos para redescubrir nuevas cuentas en la red. Ocasionalmente, las aplicaciones críticas para el negocio experimentan tiempos de inactividad o fallan porque los nuevos usos de las cuentas de servicio no se han asociado

con la correspondiente cuenta de servicio gestionada en la solución PAM. Esto puede llevar a una interrupción de las operaciones del negocio, experiencias negativas de los clientes y una atmósfera de desconfianza entre los equipos, dificultando la adopción completa de una solución PAM.

Dimensiones de la madurez de la PAM	Características típicas
Gobernanza, riesgo y cumplimiento normativo	• Establezca un inventario preciso de cuentas y contraseñas administrativas con privilegios. • Clasifique las credenciales y los secretos.
Administración de privilegios	• Almacene con seguridad y automatice la rotación periódica de todas las cuentas administrativas. • Almacene con seguridad las cuentas con privilegios de Active Directory y Azure y gestione los grupos de cuentas con privilegios. • Descubra y almacene con seguridad las cuentas administrativas locales. • Establezca un entorno administrativo seguro para las sesiones locales y remotas. • Establezca el flujo de trabajo de acceso con privilegios inicial.
Gestión de identidades y accesos	• Aplique autenticación multifactor para el acceso al almacén, incluida la comprobación secreta y el inicio de la sesión remota. • Establezca cuentas de administración alternativa para evitar el uso de identidades públicas. • Aplique la administración alternativa y la autenticación multifactor para el acceso remoto.

FASE 2: avanzado

La clave para las organizaciones en la fase 2 de madurez de la PAM es ampliar las políticas de PAM con el fin de reducir el número de usuarios con exceso de privilegios. Se trata de una combinación de normalización (reducir los privilegios excesivos) y consolidación (eliminar las cuentas con privilegios locales adicionales para los administradores, de modo que solo tengan una única cuenta (AD) para el acceso).

Las organizaciones que se encuentran en esta fase incluyen a los usuarios empresariales, desarrolladores y proveedores, además de los administradores de dominio, en su definición de usuarios con privilegios que deben ser gestionados. Además de implementar un almacén central, amplían los controles granulares de PAM a los endpoints, incluidos los servidores y las estaciones de trabajo. Para hacer frente a los retos de la seguridad de las aplicaciones web y SaaS, empiezan a gestionar el acceso a estas aplicaciones de forma centralizada y aplican un control de acceso granular basado en roles (RBAC) a los permisos de los usuarios.

Durante esta fase y la siguiente, PAM se convierte en una prioridad principal dentro de la estrategia de seguridad de una organización. En este nivel, las organizaciones están comprometidas con la mejora continua de las prácticas de seguridad con privilegios.

Dimensiones de la madurez de la PAM	Características típicas
Gobernanza, riesgo y cumplimiento normativo	• Descubra, clasifique y gestione las cuentas locales, los servidores, los grupos, los roles y los archivos de configuración de seguridad que podrían conceder privilegios en todos los activos. • Ejecute políticas de control de acceso de seguridad y supervisión de sesiones en tiempo real para los endopoints. • Lleve a cabo auditorías de sesiones, archivos y procesos basadas en host con integración en SIEM. • Integración con ITSM para impulsar los flujos de trabajo de solicitud de control de acceso vinculados a los tickets de soporte técnico.
Administración de privilegios	• Establezca políticas básicas de elevación de privilegios para todos los endpoints (estaciones de trabajo y servidores). • Establezca solamente los privilegios necesarios y cuando sea necesario. • Almacene con seguridad las credenciales administrativas locales y de Linux (contraseñas y claves SSH). • Amplíe el control de acceso remoto a proveedores y contratistas sin crear cuentas de AD.
Gestión de identidades y accesos	• Imponga la autenticación multifactorial en los endpoints para el inicio de sesión directo y la elevación de privilegios. • Elimine las cuentas locales mediante la consolidación de identidades para Unix y Linux. • Elimine las credenciales codificadas y los datos de configuración de las aplicaciones y los scripts. • Automatice la seguridad de los privilegios en los flujos de trabajo y las herramientas de DevOps.

FASE 3: experto

La clave para las organizaciones en la fase 3 de madurez de la PAM es aumentar la automatización y la inteligencia, llevando el concepto de mejora continua a un nivel superior.

De este modo, gestionan de forma completa y automática todo el ciclo de vida de una cuenta con privilegios, desde el aprovisionamiento hasta la rotación, pasando por el desaprovisionamiento y los informes. En esta fase, los sistemas PAM están totalmente integrados para una estrategia de seguridad automatizada de defensa en profundidad. Los controles de la PAM están estratificados para romper la cadena de ataque en múltiples puntos. Si un atacante supera uno, se encuentra con el siguiente. La supervisión continua permite identificar automáticamente el comportamiento anómalo de las cuentas con privilegios y pone en marcha las actividades adecuadas para la respuesta ante incidentes.

Los programas de PAM más maduros procuran una cultura de seguridad holística. No mantienen las prácticas de PAM dentro del silo del equipo de seguridad o de operaciones de IT, sino que la integran a la perfección en otras áreas de IT y de desarrollo de software, incluso dentro de un entorno DevOps de alta velocidad. Consideran cada cuenta como una cuenta con privilegios y tienen una visión consolidada de todas las cuentas, credenciales, accesos y permisos de usuario, para todos los tipos de cuentas con privilegios en toda la organización.

Descubrimiento, gobernanza y automatización de cuentas de servicio

No es hasta la etapa de madurez del Experto que la mayoría de las organizaciones obtienen una imagen precisa de las cuentas de servicio con privilegios y sus dependencias.

Tras las actividades de descubrimiento y automatización, la gobernanza se extiende al aprovisionamiento de nuevas cuentas de servicio sin fisuras y de forma automática. Esto se puede gestionar de forma centralizada en Active Directory o a través de una

plataforma PAM SaaS para aumentar la eficiencia y el control. Las cuentas también se dan de baja automáticamente en función de las políticas, sin causar interrupciones en los servicios críticos o en los procesos empresariales. Las organizaciones establecen flujos de trabajo que precisan la aprobación antes de la creación de nuevas cuentas de servicio. La certificación y los derechos impuestos a las cuentas de servicio garantizan la rendición de cuentas y la propiedad. Los intentos fallidos de actualizar las nuevas credenciales tienen como resultado una reversión automática a las credenciales anteriores.

Dimensiones de la madurez de la PAM	Características típicas
Gobernanza, riesgo y cumplimiento normativo	• Integre herramientas de gobernanza y administración de la identidad (IGA) para la elaboración de informes de certificación y aprobaciones basadas en el riesgo. • Aproveche los datos de auditoría, el aprendizaje automático, el análisis del comportamiento y la automatización para detectar, rastrear y alertar sobre cualquier amenaza. • Integre herramientas de análisis del comportamiento de usuarios y entidades (UEBA). • Descubra y clasifique cuentas de servicio. Aplique el descubrimiento, el aprovisionamiento y la gobernanza de las cuentas de servicio entre los proveedores de identidad y de servicios en la nube. • Endurezca los sistemas operativos y los componentes de las aplicaciones.
Administración de privilegios	• Establezca políticas más granulares para la elevación de privilegios. • Automatice la incorporación de nuevos activos gestionados.
Gestión de identidades y accesos	• Garantice que todas las conexiones necesarias para las operaciones con privilegios se autentifiquen mutuamente con credenciales criptográficas. • Aumente la autenticación multifactor del nivel 1 de garantía de autenticación del NIST (autenticación con un ID y una contraseña) al nivel 2 de garantía de autenticación del NIST (AAL2). El AAL2 ofrece mayor garantía de identidad debido a la presencia de un segundo factor. • Restrinja el acceso con privilegios a los endpoints registrados y propiedad de la empresa. • Prohíba el acceso con privilegios a cualquier sistema cliente no conocido, autenticado, debidamente protegido y de confianza. • Exija una doble autorización para las operaciones con privilegios en los sistemas críticos o sensibles.

Cómo puede ayudar Delinea

A medida que avanza hacia la madurez, Delinea le ofrece las herramientas, los recursos y el asesoramiento de expertos que necesita en cada paso del camino.

Sabemos que la PAM no es una solución sencilla y que su estrategia no es la misma para todas las organizaciones. Convergemos con usted en su punto de madurez de PAM y le ayudamos a acelerar su progreso. Nuestra solución de seguridad modular está diseñada para crecer con usted.

Nuestra misión es convertirle en un campeón de la seguridad autosuficiente para que pueda ser dueño de su propia experiencia de PAM.

Delinea

Defining the boundaries of access

Delinea es un proveedor líder de soluciones de gestión de accesos con privilegios (PAM) que proporciona una seguridad sin fisuras para la empresa moderna e híbrida. Delinea Platform amplía sin problemas PAM proporcionando autorización para todas las identidades, controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles para ayudar a reducir el riesgo, garantizar el cumplimiento y simplificar la seguridad. Delinea pone fin a la complejidad y define las limitaciones de acceso para miles de clientes en todo el mundo. Nuestros clientes comprenden desde pequeñas empresas hasta las mayores instituciones financieras del mundo, agencias de inteligencia y empresas de infraestructuras críticas. **delinea.com/es/**