ManageEngine
Access Manager Plus

Gestión de sesiones privilegiadas

Establezca un punto de apoyo sólido en la lucha contra el abuso del acceso privilegiado al controlar, monitorear y grabar sesiones privilegiadas de cuentas en alto riesgo.

¿Qué es una sesión privilegiada?

Una sesión privilegiada es una sesión de internet iniciada por un usuario con privilegios administrativos mientras accede a un sistema, dispositivo o aplicación en la infraestructura de TI —ya sea local o remotamente— y consta de todas las actividades realizadas durante dicha sesión.

Una sesión privilegiada puede ser una base de datos o un administrador de seguridad que accede a información corporativa confidencial en el centro de datos mediante una sesión RDP o SSH, un proveedor externo que accede remotamente a aplicaciones empresariales específicas mediante una herramienta de acceso remoto o un ingeniero de mantenimiento que accede a servidores críticos ubicados en varias plantas industriales y sistemas de automatización, como PLC y SCADA, para la resolución de problemas o el parcheo de software.

Los riesgos de seguridad asociados con las sesiones privilegiadas

Si es un administrador de TI, sabe que iniciar una sesión privilegiada hoy es un riesgo a la vez que una tarea inevitable. Aunque una mezcla de herramientas y tecnologías modernas y tradicionales puede ayudar a las empresas a facilitar el acceso remoto e impulsar la eficiencia operativa, el acceso privilegiado no verificado también introduce muchos nuevos retos en términos de seguridad y cumplimiento.

1. Las organizaciones con frecuencia restan importancia a las cuentas privilegiadas

Las cuentas privilegiadas y las credenciales que las protegen están dispersas en los sistemas más críticos de la organización, debido a que tienen los niveles de permiso más altos. No es sorpresa que las cuentas privilegiadas sigan siendo un objetivo claro para los criminales cibernéticos. Si un atacante obtiene acceso a solo una cuenta privilegiada mal gestionada,

podría fácilmente escalar su acceso a los sistemas más sensibles dentro de la red. Dichas sesiones maliciosas privilegiadas tienen la ventaja de la duda, ya que los atacantes que imitan a usuarios privilegiados las inician mediante cuentas privilegiadas legítimas.

2. Los resultados del Internet de las amenazas

Los datos corporativos sensibles, como cuentas privilegiadas, certificados, tokens, claves y contraseñas, son los objetivos principales de los criminales cibernéticos debido a que ofrecen acceso privilegiado ilimitado a todo recoveco de la infraestructura de TI. Para minimizar riesgos y equilibrar la seguridad de TI con respecto a la productividad, las organizaciones deben suministrar un acceso controlado y adecuado para que los usuarios privilegiados protejan los sistemas críticos. Si las sesiones privilegiadas no se gestionan con controles estrictos, los atacantes —externos o internos— pueden comprometerlas, causando un daño irreversible a los datos corporativos.

3. Los riesgos de las colaboraciones con terceros

Uno de los más grandes desafíos que las organizaciones enfrentan hoy es no entender sus relaciones con terceros y los riesgos asociados. De acuerdo con un informe de Ponemon Institute en 2020 (mediante Security Boulevard), 53% de las organizaciones ha experimentado al menos una violación de la seguridad de los datos por parte de un tercero en los últimos 2 años. Los atacantes también aprovechan los puntos de acceso de terceros para obtener una entrada y lanzar ataques a su debido tiempo. Con la creciente dependencia de proveedores remotos y el cambiante panorama de amenazas, es difícil identificar amenazas y vulnerabilidades de terceros sin implementar las herramienta correctas para el monitoreo.

4. No limitar el acceso a sistemas sensibles

En la mayoría de las organizaciones los empleados con frecuencia tiene un exceso de privilegios de alto nivel y de permisos de acceso que son de hecho innecesarios para sus roles, lo que allana el camino para el abuso de privilegios.

Generalmente estos privilegios pasan desapercibidos y no se gestionan, suponiendo varios riesgos de seguridad y amenazando la compañía. Los equipos de TI con frecuencia no manejan las consecuencias de demasiados accesos, especialmente cuando se trata de exempleados. No anular la identidad y permisos de acceso de un exempleado permite a empleados insatisfechos tener acceso a datos sensibles, incluso si ya no están en la organización.

5. Aprovisionamiento y gestión descentralizados del acceso remoto

Muchas organizaciones hoy aún dependen de varias herramientas y de estrategias manuales y fragmentadas para proveer de acceso remoto a empleados, debido a las limitaciones presupuestarias o a la ignorancia flagrante sobre los riesgos de métodos de acceso inseguros. Dicho sistema descentralizado puede causar enormes disparidades en las políticas y flujos de trabajo del acceso remoto en la organización, lo que deja varias brechas de seguridad atrás y complica a los equipos de TI gestionar todo en las sesiones privilegiadas de una organización.

Cómo proteger el acceso privilegiado a sistemas confidenciales

¿Cómo puede, como administrador de TI, sobreponerse a este panorama moderno de amenazas y establecer de manera segura una estrategia para dar acceso privilegiado a empleados, proveedores externos, aplicaciones y dispositivos? ¿Cómo gestiona y monitorea cada actividad privilegiada que sucede en su infraestructura on-premise, híbrida y en la nube, y garantiza que ninguna actividad maliciosa pase desapercibida? ¿Cómo bloquea todas las puertas traseras fabricadas por atacantes para permanecer seguro sin disminuir la productividad?

El calvario de tratar con dichas preguntas puede parecer un desafío tedioso para muchos equipos de TI hoy. Aquí es donde la gestión de sesiones privilegiadas resulta útil.

Gestión de sesiones privilegiadas: un proceso de seguridad de TI para controlar y supervisar el acceso privilegiado

La gestión de sesiones privilegiadas (PSM) es un componente fundamental de la seguridad de TI en un programa de gestión de accesos e identidades que regula el acceso privilegiado a sistemas críticos, mientras controla estrictamente las sesiones mediante grabaciones y auditorías de sesiones.

Una herramienta de PSM ayuda a aumentar la supervisión y la transparencia, además de mitigar el riesgo del abuso del acceso privilegiado al gestionar, monitorear y auditar continuamente las actividades realizadas por usuarios privilegiados, incluyendo miembros de confianza, contratistas externos, aplicaciones y sistemas. Asimismo, es una parte inseparable del emergente modelo de confianza cero que fomenta en las organizaciones no confiar automáticamente en que los usuarios están usando su acceso elevado para hacer lo correcto y garantizar que se siguen rigurosamente las mejores prácticas de seguridad.

Ventajas de usar una herramienta de PSM efectiva

Una herramienta de PSM monitorea y registra las actividades de cada usuario privilegiado desde el momento en que inicia una sesión privilegiada hasta cuando dicha sesión termina, lo que permite a los administradores de seguridad identificar y terminar proactivamente actividades sospechosas o no autorizadas en tiempo real. Proporciona una pista de auditoría intachable de todas las actividades privilegiadas que permite el cumplimiento y facilita las investigaciones forenses. Implementar una solución de PSM como parte de su programa de seguridad informática ayuda a las empresas a mitigar los riesgos de seguridad, reducir la complejidad operativa, mejorar la visibilidad del acceso privilegiado y adherirse a los estándares de cumplimiento.

1. Da un acceso centralizado a activos geográficamente restringidos

Un administrador de sesiones privilegiadas permite a los líderes de TI y seguridad tener un punto de control central para gestionar el acceso a recursos críticos desde cualquier lugar en el globo, tener controles detallados sobre rutas de acceso y definir cómo otros usuarios remotos privilegiados se conectan a sistemas críticos.

2. Permite el acceso detallado a interesados y terceros

Una herramienta robusta de PSM proporciona un flujo de trabajo fácil de usar que permite el aprovisionamiento y desaprovisionamiento sencillo del acceso privilegiado, mientras crea una total transparencia para los usuarios privilegiados. Permite el acceso temporal basado en roles a terceros —como contratistas proveedores y empleados subcontratados— para acceder a sistemas o aplicaciones empresariales específicos sin la necesidad de credenciales de cuentas privilegiadas.

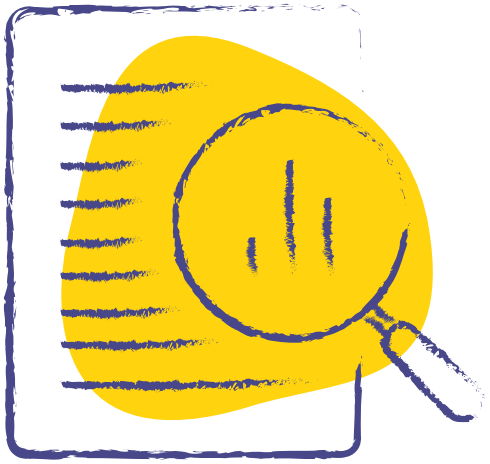
3. Aumenta la productividad y simplifica la administración

Implementar una solución de PSM facilita la administración centralizada de activos de TI distribuidos remotos mediante un solo punto de control. Los usuarios privilegiados pueden actualizar, resolver problemas y gestionar sistemas de centros de datos de forma centralizada, lo que facilita una administración rápida y eficaz. Esto también garantiza una mejora en la calidad laboral y una mejor rendición de cuentas mediante políticas estandarizadas y una supervisión eficaz.

4. Refuerza el gobierno general del acceso

Además de dar acceso detallado, las soluciones de PSM también dan a los administradores los controles correctos para monitorear y gestionar activos distribuidos geográficamente. El monitoreo en tiempo real de sesiones remotas privilegiadas promueve la transparencia organizacional y da a los administradores de TI la capacidad de mitigar proactivamente ataques internos mediante la grabación y seguimiento de sesiones.

5. Ayuda a cumplir con varios estándares de cumplimiento para acceso remoto



Una herramienta de PSM ayuda a las organizaciones a cumplir con las normas de cumplimiento de la industria, como SOX, HIPAA, ICS CERT, GLBA, PCI DSS, FDCC y FISMA, y permite proteger todos sus datos. Implementar PSM como parte de una estrategia integral de seguridad informática permite a las organizaciones registrar todas las actividades relacionadas con la infraestructura de TI y el acceso privilegiado críticos, lo que les ayuda a adherirse sin esfuerzo a los requisitos de auditoría y cumplimiento.

6. Mejora la seguridad y reduce los riesgos

Un administrador de sesiones privilegiadas ayuda a proteger sistemas críticos al eliminar el acceso directo a ellos. Funciona como un servidor del gateway proxy para canalizar conexiones privilegiadas desde el dispositivo del usuario al sistema objetivo. Esto evita el acceso inesperado desde sistemas no autorizados, limita todas las vías de acceso a sistemas corporativos a esta herramienta y permite comunicaciones más seguras sin la necesidad de dar contraseñas confidenciales.

Access Manager Plus: la solución de ManageEngine para la gestión de sesiones privilegiadas

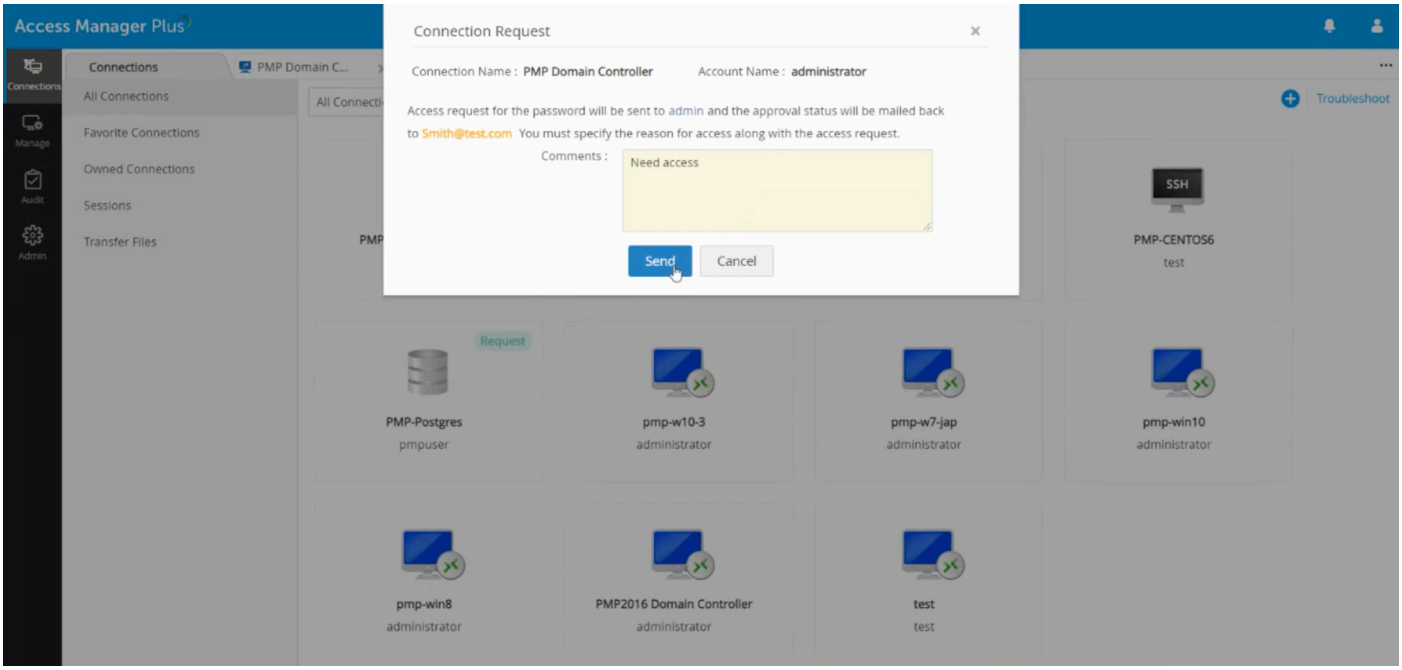
Access Manager Plus es una herramienta para la gestión de acceso remoto seguro y de sesiones privilegiadas de ManageEngine que ayuda a regular y monitorear todos los accesos privilegiados en su organización. Funciona como un servidor proxy entre los dispositivos de los usuarios finales y los sistemas objetivo, mientras que simultáneamente evita la exposición de credenciales y el acceso directo a sistemas críticos mediante rutas inseguras y no autorizadas.

Access Manager Plus ayuda a mejorar la supervisión y transparencia de las actividades de los usuarios privilegiados mediante el seguimiento, grabación y auditoría de sesiones.

Flujos de trabajo para el control de acceso privilegiado

A diario un equipo de TI por lo general maneja muchas solicitudes de acceso permanente y temporal que los usuarios y proveedores externos generan, para acceder a varios sistemas corporativos. Para garantizar la gestión efectiva de estas solicitudes de acceso privilegiado y el funcionamiento ininterrumpido de las rutinas corporativas, los equipos de TI deben mantener un flujo de trabajo optimizado como parte de su estrategia de PSM.

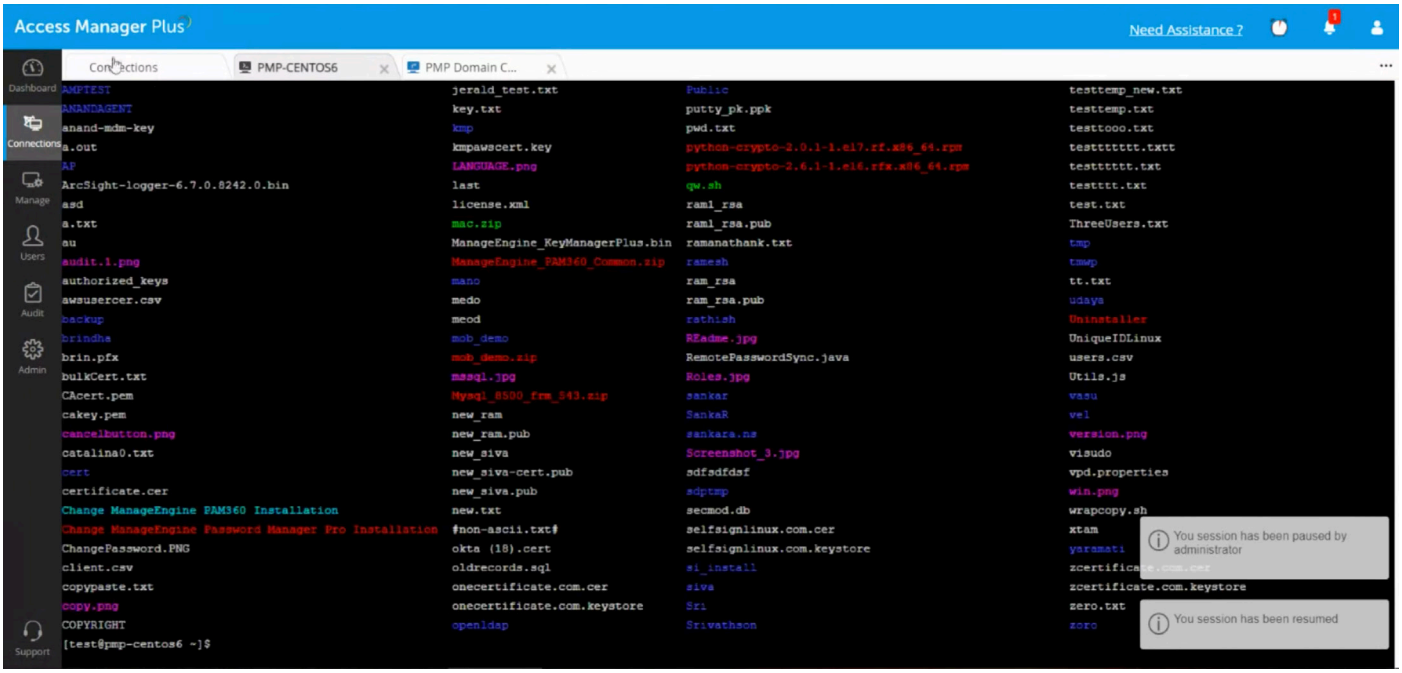
Configure controles de acceso en Access Manager Plus al establecer requisitos de aprobación para sesiones privilegiadas, obligar a los usuarios a dar una razón y/o la ID del ticket correspondiente que se pueda integrar con un sistema de tickets existente. También puede asociar ciertos recursos o aplicaciones a un usuario que está facultado para solicitar acceso y garantizar que se le otorgue solo el acceso mínimo requerido durante el menor tiempo.



Aprovisionamiento seguro de acceso remoto

Access Manager Plus sirve como un proxy a través del cual se inicia una sesión privilegiada y se pasa a los sistemas objetivo. Ya que no hay una conectividad directa entre el dispositivo del usuario y los sistemas objetivo, la red empresarial está protegida contra el acceso no autorizado y cualquier virus o malware que pueda haber en el sistema del usuario.

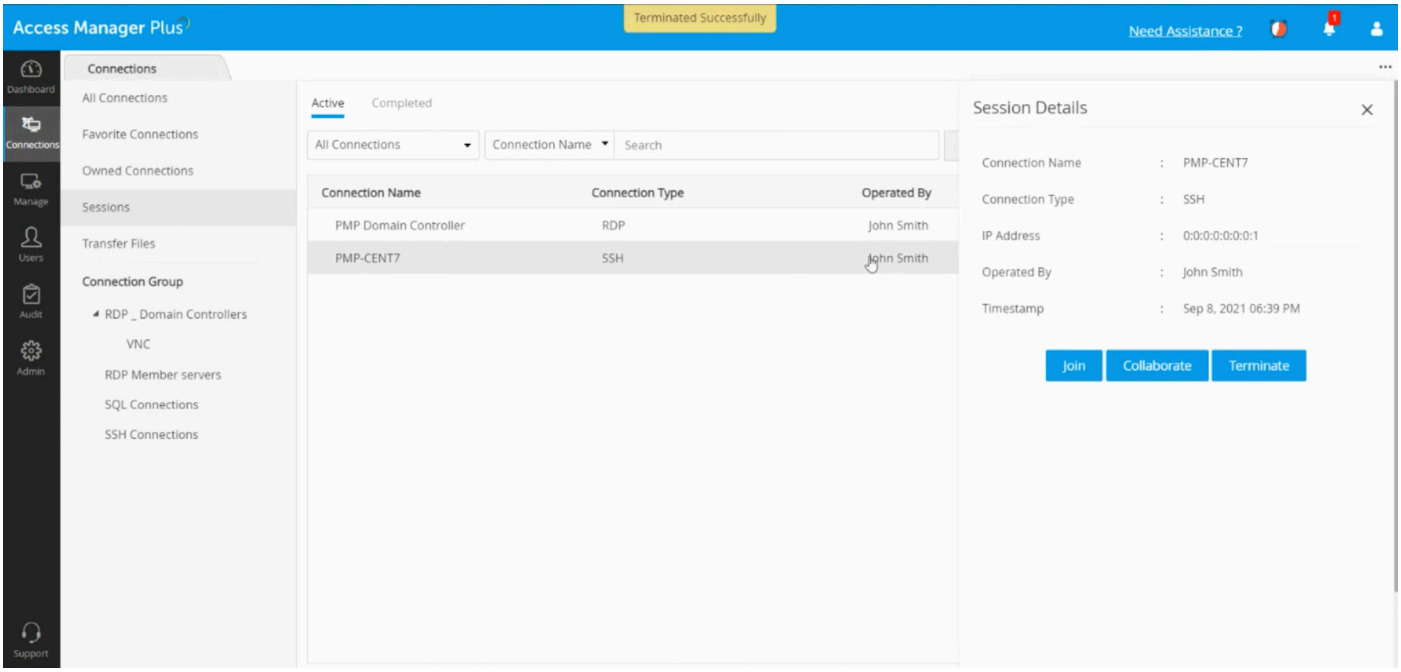
Dé a los empelados e interesados externos acceso RDP, SSH, SQL o VNC seguro y controlado a sistemas sensibles en su infraestructura on-premise, híbrida o en la nube sin exponer credenciales privilegiadas. Permita a los usuarios iniciar varias sesiones remotas simultáneamente para mejorar la productividad.



Colaboración, seguimiento y terminación de sesiones

Access Manager Plus le permite colaborar con usuarios en una sesión remota activa para compartir conocimiento, monitorear la actividad del usuario para garantizar el cumplimiento de las políticas de seguridad establecidas o ayudar con la resolución de problemas.

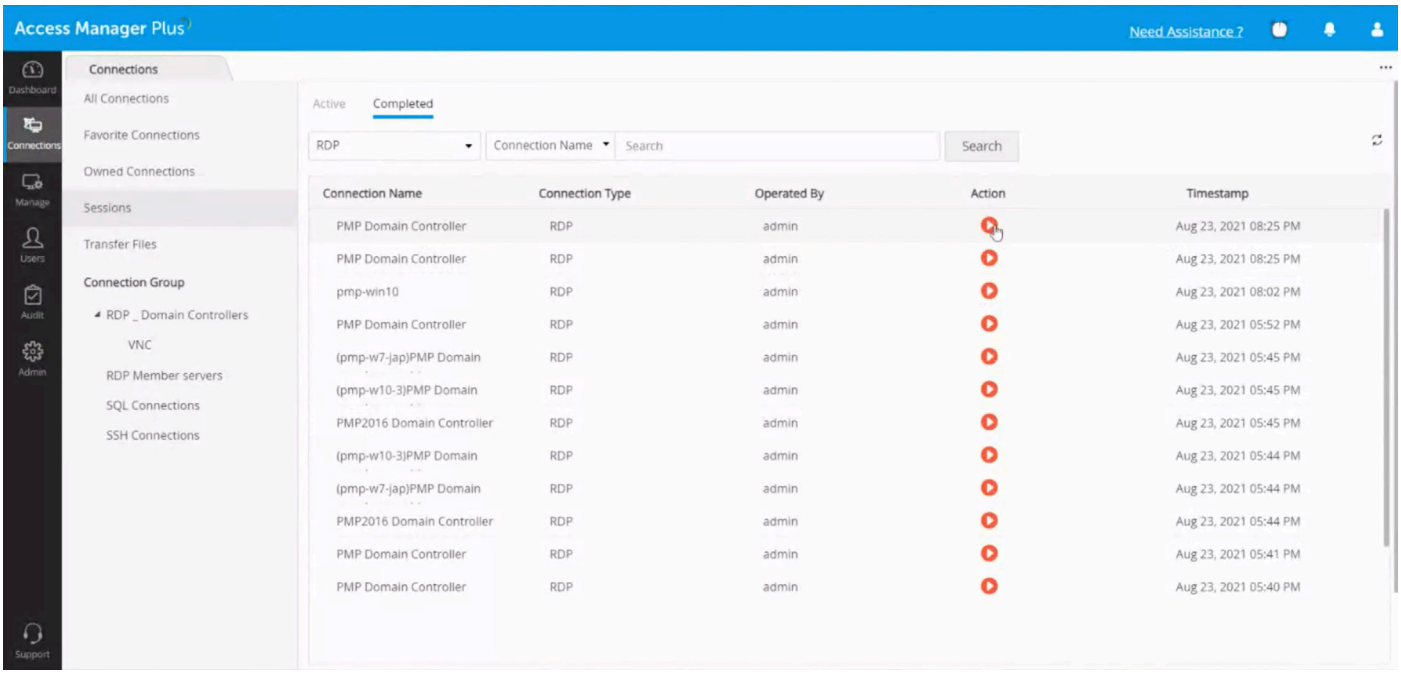
Siga sesiones privilegiadas que involucran sistemas críticos y proveedores externos para descubrir proactivamente actividades fraudulentas y garantizar que solo los usuarios autorizados accedan a sistemas confidenciales de acuerdo con el alcance de las actividades que les están permitidas realizar. Si detecta una actividad sospechosa o no autorizada durante una sesión privilegiada, usted puede terminar la sesión inmediatamente y alertar a los equipos de seguridad correspondientes.



Registro y repetición de sesiones

Las grabaciones de sesiones privilegiadas ofrecen evidencias a prueba de alteraciones sobre el acceso privilegiado de un usuario. Si un atacante penetra sus defensas y accede a sus sistemas, usted puede filtrar y revisar fácilmente grabaciones de sesiones pasadas para descubrir la fuente y ajustar políticas para evitar otro ataque.

Predeterminadamente, Access Manager Plus graba todas las sesiones RDP, VNC, SSH y SQL iniciadas desde la aplicación. Las sesiones grabadas pueden encontrar usando cualquier detalle, como el nombre de la conexión, el usuario que lanzó la sesión o la hora en que se lanzó la sesión.

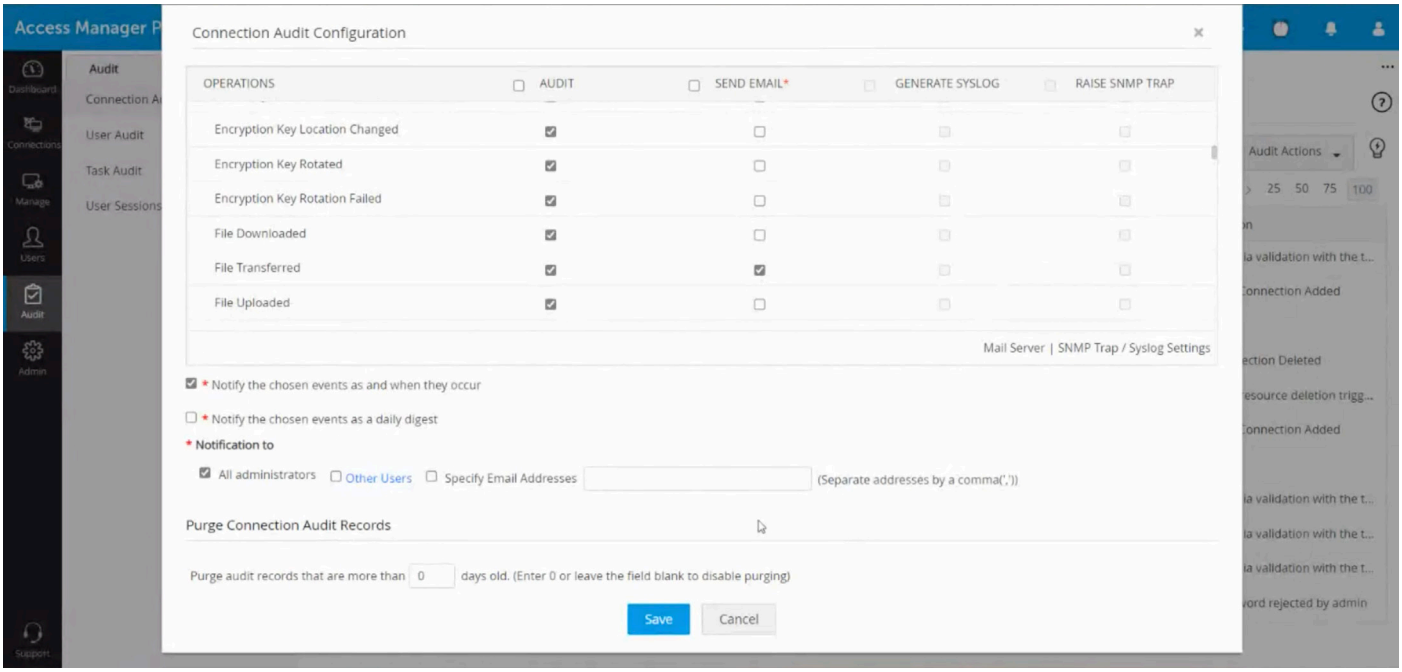


Auditorías integrales

Las pistas de auditoría ayudan a identificar comportamientos sospechosos. Los logs de auditorías automatizados permiten a los administradores identificar problemas en la implementación del sistema, problemas operativos, actividades inusuales o sospechosas, y otros errores del sistema. Varias normas de cumplimiento, tales como HIPAA, SOX y PCI DSS, buscan que las organizaciones monitoreen y registren todas las acciones realizadas por cuentas privilegiadas; la gestión de sesiones proporciona un log de auditoría inmutable que se puede compartir con los auditores para demostrar el cumplimiento.

Los logs de auditorías inmutables de Access Manager Plus contienen el registro de todos los eventos alrededor de las actividades de las cuentas privilegiadas, tareas programadas y completadas, y accesos remotos. Estos datos ayudan a cumplir con auditorías internas regulares e investigaciones forenses, demostrando quién accedió a qué recurso o archivo, dónde, cuándo y por qué.

Asimismo, puede integrar Access Manager Plus con su herramienta existente para la gestión de eventos e información de seguridad y así exportar datos de accesos privilegiados por mensajes de syslog o con su herramienta para la gestión de redes con el fin de recibir logs relacionados con el acceso mediante SNMP traps. Hacerlo le permite notificar a los equipos correspondientes de posibles vulneraciones y priorizar y ejecutar acciones correctivas de conformidad.



Obtenga más información sobre la gestión de sesiones privilegiadas

Debido a que los ataques cibernéticos se están haciendo cada vez más sofisticados y peligrosos, es el tiempo propicio para que los administradores de TI sepan cómo proteger la información crítica de su organización. Implementar las mejores prácticas de seguridad y las prácticas altamente recomendadas para PSM ayudará a su organización a lograr un mecanismo de defensa sólido contra amenazas de acceso no autorizado.

Si desea ver la gestión de sesiones privilegiadas en acción, puede registrarse para una prueba gratuita de Acces Manager Plus, donde puede probar todas las funciones de la herramienta. También puede probar la versión de demostración donde puede obtener de primera mano conocimiento de cómo funciona la herramienta.

https://www.manageengine.com/latam/privileged-session-management/

Technical support

Email: tech-latam@manageengine.com

ManageEngine
Access Manager Plus