ManageEngine
PAM360

Prepárese para el seguro de riesgos cibernéticos con ManageEngine PAM360

Checklist de PAM para todas sus necesidades de seguro de riesgos cibernéticos

El seguro de riesgos cibernéticos protege los intereses de las organizaciones en caso de incidentes cibernéticos relacionados con su infraestructura y seguridad de red de TI.

En los últimos 3 años, las indemnizaciones por seguros de riesgos cibernéticos han aumentado un considerable 200%, y el número máximo de reclamaciones ascenderá a 8.100 solo en 2021. Aunque la cantidad de reclamaciones puede parecer desorbitada, un estudio de mercado sugiere que solo el 55% de todas las organizaciones cuentan con seguros de riesgos cibernéticos.

En consecuencia, los seguros de riesgos cibernéticos se han vuelto más estrictos, con primas más elevadas y la obligación de vigilar la seguridad de todas las entidades de TI.

Los proveedores de seguros de riesgos cibernéticos reconocen que los controles de gestión de acceso privilegiado (PAM) son fundamentales para la seguridad de una organización. Estos controles desempeñan un rol fundamental a la hora de impedir diversas amenazas cibernéticas y reducir las ramificaciones de una violación de la seguridad de los datos.

En este folleto, exploraremos cómo una solución de PAM puede ayudarle a cumplir estos complejos requisitos de seguro de riesgos cibernéticos. Nos centraremos específicamente en cómo PAM360 implementa ideologías de PAM críticas que optimizarán su próxima compra de seguro de riesgos cibernéticos, para garantizar que se le considere elegible para minimizar los costos de las primas y las reclamaciones de seguros más grandes.

Requisitos del seguro de riesgos cibernéticos	Mejores prácticas recomendadas	How PAM360 helps
¿Dispone su organización de medidas para gestionar las identidades privilegiadas?	Descubra, agrupe, regule y comparta todas las identidades privilegiadas en toda la red de TI de la organización de forma segura.	PAM360 puede descubrir, consolidar e incorporar a la solución usuarios y endpoints de una amplia gama de servicios de directorio empresarial. A continuación, asigna roles y responsabilidades específicas a dichos usuarios privilegiados y endpoints, respectivamente, y los agrupa en función de los requisitos exigidos por la política de acceso de la organización. Utilizando PAM360, usted puede compartir de forma selectiva y segura dichas cuentas privilegiadas en endpoints remotos a usuarios privilegiados
¿Utilizan todos los empleados de su organización la autenticación multifactor (MFA) al iniciar sesión en los activos y software de TI de su empresa?	Autentique a los usuarios que inician sesión en la solución con credenciales almacenadas en el directorio correspondiente y aplique la MFA a todos los usuarios del activo o software de TI.	PAM360 ofrece una amplia gama de integraciones con todas las soluciones MFA para empresas, como Google Authenticator, Microsoft Authenticator, Okta Verify, RSA SecurID, YubiKey, por nombrar algunas. PAM360 también viene con una aplicación TOTP nativa, Zoho OneAuth, que es compatible con la autenticación de usuarios basada en biometría.

Requisitos del seguro de riesgos cibernéticos	Mejores prácticas recomendadas	How PAM360 helps
¿Qué pasos sigue su organización para prevenir, detectar y mitigar ataques de ransomware?	Evite la manipulación de programas maliciosos implementando un acceso regulado a los endpoints, aplique el principio de los cuatro ojos para las solicitudes de acceso a los endpoints, estandarice las prácticas de mínimo privilegio y aplique una segmentación de red estricta.	PAM360 permite compartir de forma selectiva cuentas con privilegios en endpoints remotos a usuarios individuales o a un grupo de usuarios mediante la verificación de los roles y responsabilidades de los usuarios. PAM360 permite compartir esta información privilegiada mediante flujos de trabajo de solicitud y liberación de contraseñas. Estas solicitudes de acceso son generadas en primer lugar por el usuario con un propósito mencionado y, a continuación, reciben la aprobación de un administrador seleccionado. Los administradores pueden establecer un acceso temporal, monitoreado y justo a tiempo (JIT) a recursos altamente privilegiados mediante controles nativos de gestión de elevación y delegación de privilegios (PEDM) que pueden finalizar la sesión en caso de actividad sospechosa. Con el módulo de control de acceso basado en políticas (PBAC) de PAM360, los administradores pueden crear políticas de acceso personalizables basadas en puntuaciones de confianza de usuarios y dispositivos y otros factores vitales. Las puntuaciones de confianza se obtienen dinámicamente en función de diversos parámetros de seguridad, como la legitimidad de la red, el comportamiento de los usuarios y los endpoints, etc. Por cada privilegio que se otorga a un usuario, nuestra solución coloca un dispositivo de seguridad que monitorea, previene, detecta y disuade de que se haga un uso indebido de tales privilegios

Requisitos del seguro de riesgos cibernéticos	Mejores prácticas recomendadas	How PAM360 helps
¿Su organización lleva un control de toda la actividad privilegiada en la red?	Audite y registre toda la actividad privilegiada en relación con quién, cuándo y dónde se inició una sesión privilegiada, y registre qué actividades se realizaron durante dichas sesiones privilegiadas. El "qué" puede incluir, entre otras cosas, cambios de contraseña, solicitudes de acceso aprobadas y denegadas, sesiones remotas y usuarios y recursos vinculados y desvinculados.	Las auditorías e informes de PAM360 constituyen un archivo exhaustivo de toda la actividad realizada por todos los usuarios de la solución. Las auditorías e informes abarcan desde informes de actividad de endpoints y usuarios e informes de sesiones privilegiadas (activas y registradas) hasta informes de claves SSH y operaciones con certificados SSL/TLS. Además, PAM360 ofrece a los usuarios la posibilidad de generar informes utilizando el lenguaje de consulta estructural (SQL). El esquema completo de la base de datos de PAM360 está disponible para que los administradores de la base de datos lo aprovechen, en función del cual, los usuarios pueden regular la generación de informes con consultas a la base de datos para cumplir los requisitos de SOX e HIPAA. PAM360 permite a las empresas registrar toda la actividad privilegiada realizada a través de la solución, que los equipos de seguridad utilizan para auditorías y fines de análisis forenses
¿Todos sus empleados tienen acceso de administrador?	Segregue el acceso administrativo para los usuarios privilegiados y conceda el acceso con menos privilegios a los demás usuarios.	PAM360 funciona según el principio del menor privilegio. Cada control, por defecto, se deshabilita funcionalmente para proporcionar el menor privilegio requerido para un usuario específico. Esta funcionalidad es totalmente personalizable y permite a las organizaciones implementar roles de usuario únicos para aplicar un control de acceso basado en roles.

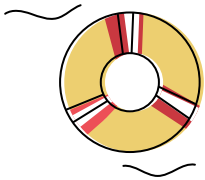
Requisitos del seguro de riesgos cibernéticos	Recommended best practices	Cómo ayuda PAM360
		Todas las características y funcionalidades se ajustan de forma coherente para reflejar el principio de mínimo privilegio en toda la empresa, limitando así el acceso de administración a los usuarios seleccionados que lo necesiten, cuando lo necesiten.
¿Dispone su organización de controles para realizar copias de seguridad y recuperación en caso de un incidente cibernético?	Realice copias de seguridad de los datos críticos, implemente medidas de emergencia y garantice una rápida restauración de los datos en función de criterios predefinidos	La configuración de emergencias repentinas de PAM360 ayuda a los usuarios a realizar copias de seguridad de todas las identidades privilegiadas y garantiza la activación automática de mecanismos a prueba de fallos basados en criterios seleccionados por el administrador. Los servicios de failover de PAM360 están totalmente automatizados para funcionar en situaciones adversas; no requieren intervención manual. Inevitablemente, si ocurre lo imprevisto, utilice el servidor de copia de seguridad de solo lectura de PAM360 para disponer de acceso ininterrumpido a todos sus datos críticos.. Estas funciones de emergencia repentina y acceso sin conexión también son accesibles de forma remota a través de aplicaciones móviles para dispositivos portátiles Android e iOS. Tenga en cuenta que a estas funciones y procedimientos de copia de seguridad solo pueden acceder usuarios con privilegios elevados, evitando así la activación no autorizada de medidas de emergencia.

Requisitos del seguro de riesgos cibernéticos	Mejores prácticas recomendadas	Cómo ayuda PAM360
¿Sus soluciones de TI de la organización cumplen con las normas de software más recientes?	Aborde los requisitos de TI críticos, como las directrices gubernamentales o las normas de TI reconocidas, teniendo en cuenta las recomendaciones establecidas por la normativa de protección de datos.	PAM360 ofrece generación de informes out-of-the-box para normativas gubernamentales e industriales como PCI DSS, ISO/IEC 27001, NERC CIP y GDPR. Estos informes pueden obtenerse por cláusulas o en su totalidad en función de las necesidades. La solución de PAM analiza sus endpoints para validar si cumplen o infringen la norma correspondiente. En caso de infracción, PAM360 propondrá medidas correctivas
¿Cómo evita su organización que caduquen inadvertidamente los certificados de sitios web y las claves de dispositivos de red?	Cree, proteja, implemente y gestione certificados SSL/TLS para sitios web, otros endpoints y claves SSH de red.	El módulo nativo de gestión de certificados y claves de PAM360 ofrece una gestión integral del ciclo de vida de los certificados SSL/TLS y las claves SSH a través de amplias integraciones con autoridades de certificación de terceros como GoDaddy, Verisign, DigiCert, Thawte, etc. PAM360 también avisa a los administradores antes de que caduquen los certificados y claves críticos, lo que les permite controlar y gestionar completamente los certificados y claves. Esto reduce significativamente la sobrecarga administrativa que surge naturalmente al gestionar certificados y claves manualmente. PAM360 elimina la necesidad de una solución de TI independiente para gestionar las claves SSH y los certificados SSL/TLS

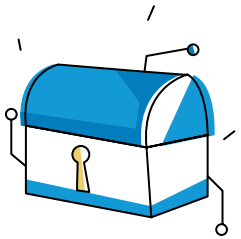
Las preguntas anteriores se derivan de los requisitos críticos de los seguros de riesgos cibernéticos que las aseguradoras utilizan para comprobar la elegibilidad de sus clientes potenciales para tarifas de primas más bajas y reclamaciones de seguros más altas.

En resumen, se espera que las organizaciones apliquen:

Autenticación multi-factor



Medidas estatutarias contra los ataques cibernéticos



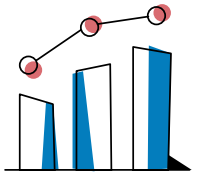
Bóveda secreta de acceso centralizado

Intercambio secreto monitoreado

Certificación regulada de activos de TI

Software que facilita el cumplimiento de las normas

Mecanismos de copia de seguridad fiables



Pistas de auditoría obligatorias de todas las actividades privilegiadas

Optimice su proceso de seguro de riesgos cibernéticos con PAM360

ManageEngine PAM360 es el producto estrella de la suite de gestión de accesos privilegiados de ManageEngine. PAM360 goza del reconocimiento de los analistas del sector por sus flexibles opciones de implementación, su facilidad de uso y mantenimiento y sus funciones de uso rápido diseñadas para reducir la fatiga operativa y dar prioridad a la seguridad por encima de todo lo demás.

PAM360 se ajusta y se audita periódicamente para cumplir los requisitos anuales del seguro de riesgos cibernéticos y está actualizado con las métricas de seguro de 2023. Dicho esto, más de 5.000 clientes de todo el mundo confían en la suite de PAM de ManageEngine para cumplir con los requisitos de elegibilidad de sus seguros de riesgos cibernéticos para reducir las primas de seguros y aumentar los pagos.

Reduzca su superficie de ataques cibernéticos y satisfaga efectivamente sus necesidades de seguro de riesgos cibernéticos con PAM360

Hablar con nuestros expertos

Iniciar una prueba gratuita