BeyondTrust

Rompiendo los 6 mitos de PAM

Gestión de Acceso Privilegiado:
Separación de Hechos de Ficción

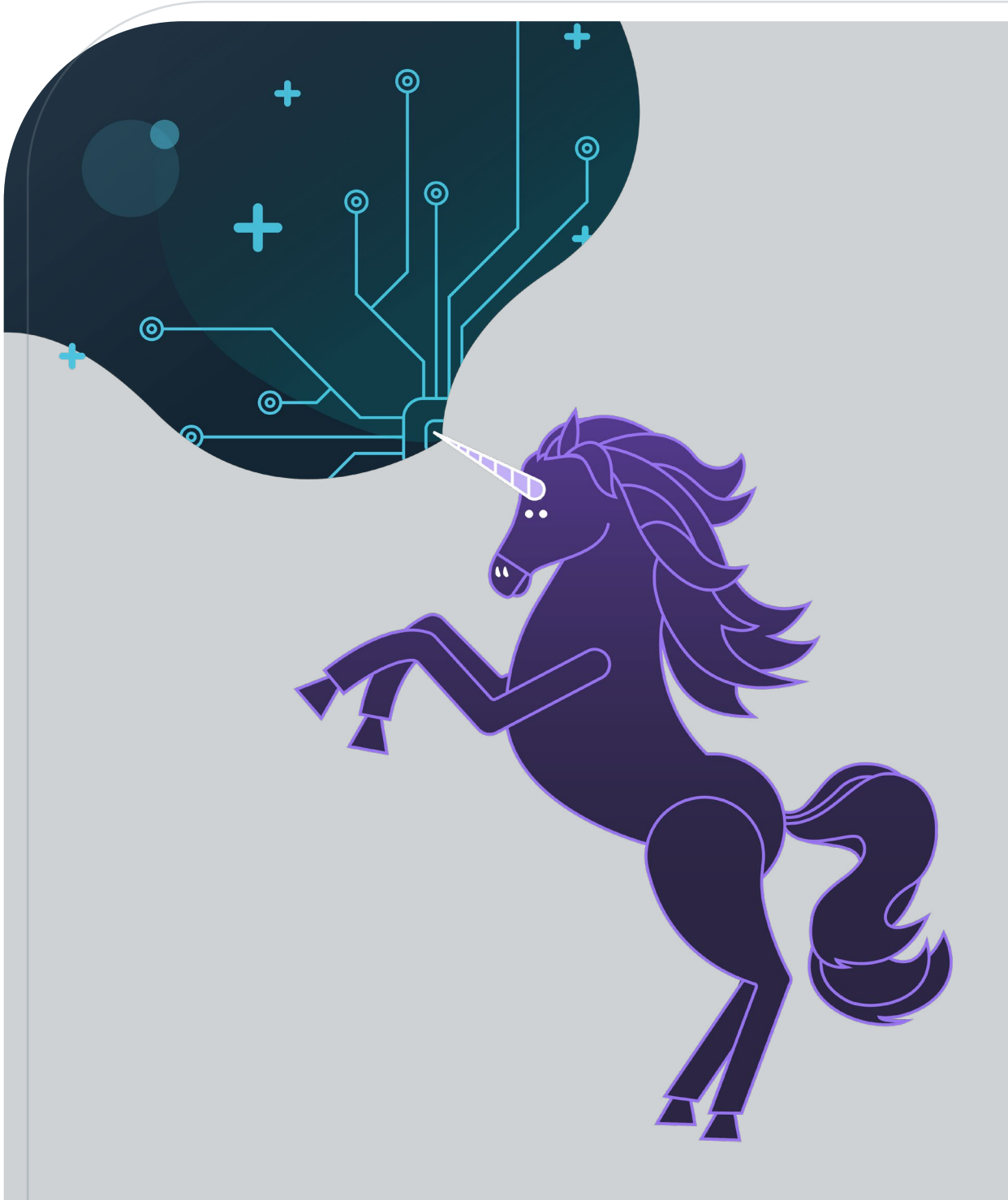
CONTENIDO

INTRODUCCION

Los mitos son cosas curiosas, ¿no? Creencias falsas ampliamente defendidas que ganan impulso con el tiempo, pueden crecer y propagarse rápidamente. La línea entre el mito y el hecho pronto se vuelve borrosa, y muchos optan por creer en un mito porque generalmente es una realidad "más agradable" o más atractiva, o simplemente porque han escuchado lo suficiente.

Aquí en BeyondTrust, tratamos de creer en los unicornios, pero todavía nos están engañando. Y si bien nos negamos a descartarlos, hay algunos mitos que queremos disipar.

En este documento técnico, descubrirá seis creencias populares sobre la Gestión de acceso privilegiado (PAM) que, de hecho, son incorrectas. Explicaremos por qué, aclararemos la verdad y brindaremos consejos prácticos para desarrollar su viaje hacia una organización más segura y libre de creencias regionales.



EL INCREMENTO DE AMENAZAS PARA UNA BRECHA DE FUGA DE DATOS

Antes de llegar a los mitos, comencemos con algunos hechos. La fuga de datos no se están desacelerando. Parece que con cada mes que pasa se produce una nueva violación de alto perfil. Y cientos suceden cada mes que no aparecen en los titulares. Como empresa, se ha convertido en un caso de cuándo, y no si, la seguridad se ve comprometida, por lo que es importante tener una estrategia para enfrentar este riesgo y tenerlo en cuenta.

La siguiente es una descripción general de las estadísticas clave para
Informes recientes publicados sobre violaciones de datos.

Según el estudio de Ponemon: El costo de una violación de datos en 2019

El reciente informe Cost of a Data Breach patrocinado por el Instituto Ponemon, patrocinado por IBM Security, revela algunas estadísticas desgarradoras sobre lo que enfrentan las víctimas de violación cibernética en el camino de la pérdida.
Actualmente, el costo total promedio general de una violación de datos es de alrededor de $ 4 millones, con un volumen promedio de aproximadamente 25,575 registros.
de una Brecha de perdida de datos. Con el tiempo promedio para identificar y contener una brecha de casi 10 meses, es obvio que se necesita una solución rápida.

Fuentes: 1. 2019 Cost of a Data Breach Report, Ponemon Institute;
2. 2019 MidYear QuickView Data Breach Report, Cyber Analystic, Agosto 2019

EL "HACKEO" HOY ES MÁS FÁCIL QUE NUNCA

Una de las principales razones por las que se producen tantos incidentes y brechas de seguridad es simplemente porque la superficie de ataque ha crecido exponencialmente en los últimos 20 años. Si bien las redes de TI solían consistir principalmente en activos locales, el número de cuentas y puntos finales explotó. Las organizaciones de TI necesitan aprender a administrar identidades humanas, así como cuentas de administrador compartidas, servidores, equipos de escritorio, IoT y credenciales de máquina en una variedad de entornos, que pueden incluir locales, en la nube e híbridos, así como DevOps. Los ciberataques y las estafas que aprovechan la IA también se perciben cada vez más de la ciencia ficción a la realidad de hoy.

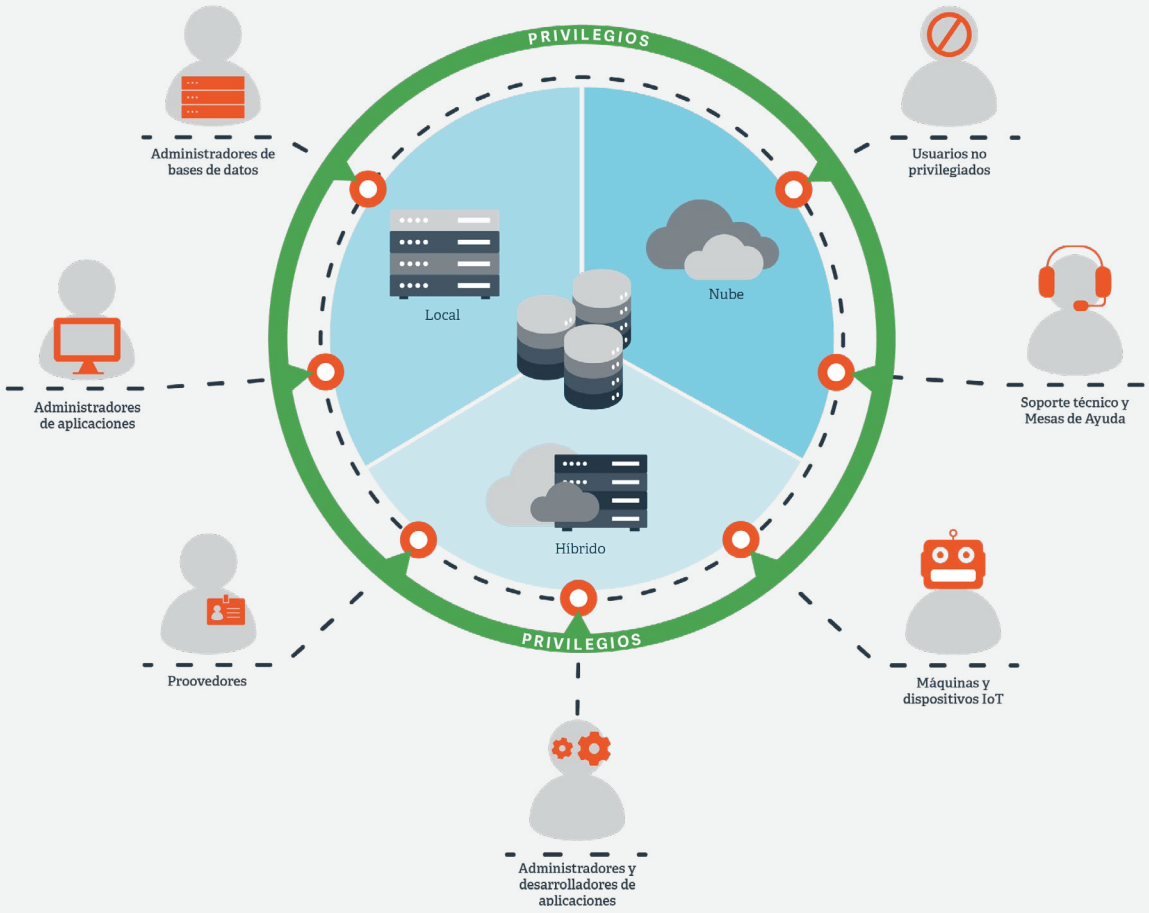
Ponga todo junto y el problema es generalizado, complejo y potencialmente difícil de resolver. El campo de juego de los hackers siempre está creciendo y, si bien continuar puede significar nuevas inversiones en seguridad y una evolución de sus estrategias, la pérdida de espacio finalmente puede ser catastrófico para su negocio.

Un problema relacionado con el aumento de los ataques es la necesidad de productividad. A medida que aumenta el número de aplicaciones, sistemas y nuevas tecnologías, también lo hace la necesidad de acceso privilegiado.

Los empleados de las empresas modernas necesitan activos de TI críticos y datos comerciales valiosos. Y dependiendo de la posición, lugar o sistema operativo, darles el acceso necesario sin riesgo a menudo parece imposible.

Debido a que muchos equipos de TI temen afectar negativamente la productividad, otorgan derechos de administrador y privilegios de aprovisionamiento excesivo sin abordar el riesgo de seguridad relacionado.

¿Cómo se accede a sus redes?



BROWSE UP VS. BROWSE DOWN: APROXIMACIONES DE GESTIÓN DE LA SEGURIDAD

Aproximación de Seguridad “Browse up”

Browse Up Security es un concepto mediante el cual los sistemas de TI se administran desde dispositivos de ‘baja confianza’ que corren un mayor riesgo de verse comprometidos, como una computadora personal doméstica. Desafortunadamente, este es un escenario típico hoy, lo que demuestra que la práctica común. No siempre es una buena práctica. Un dispositivo de usuario final utilizado por un administrador puede ser una de las rutas más fáciles hacia el sistema de destino.

En sistemas informáticos donde la integridad de los datos es importante (como los servicios de almacenamiento en la nube que manejan datos personales o pagos, o sistemas de control industrial), si no confía en los dispositivos que se utilizan para administrar u operar un sistema, no puede tener confianza en la integridad de este sistema.

Aproximación de Seguridad “Browse Down”

En todo el espectro, la seguridad de Browse Down es la mejor práctica para mitigar los riesgos en su entorno. La seguridad de Browse Down implica tener estaciones de trabajo de administración remota dedicadas que residen en una red segregada con el sistema operativo bloqueado, junto con el correo electrónico bloqueado y la navegación web.

La idea es que si la estación de trabajo / entorno menos confiable se ve comprometida, no estará directamente debajo del entorno limpio, y sería difícil para el operador de malware obtener acceso a su entorno limpio ya que viven en una estación de trabajo separada.

Sin embargo, este enfoque tiene varias desventajas. Aunque es muy seguro, no es práctico. Imagine un trabajador remoto: ¿suelen tener acceso a un sistema secundario en una VPN aislada?

Una alternativa mucho mejor es la Gestión de acceso privilegiado (PAM).

Según lo declarado por el Centro Nacional de Seguridad Cibernética (NCSC, parte de GCHQ), “Examinar es un mal modelo de seguridad, pero a menudo se usa ya que facilita la administración del equipo. Privileged Access Management (PAM) ayuda a mitigar algunos de estos riesgos. Browse Down es mejor y, junto con la administración de acceso privilegiado, realmente puede ayudarlo a ganar confianza en sus interfaces de administración.“

“La aproximación de seguridad “Browse Down” por sí solo no es escalable y no mitiga el riesgo.”

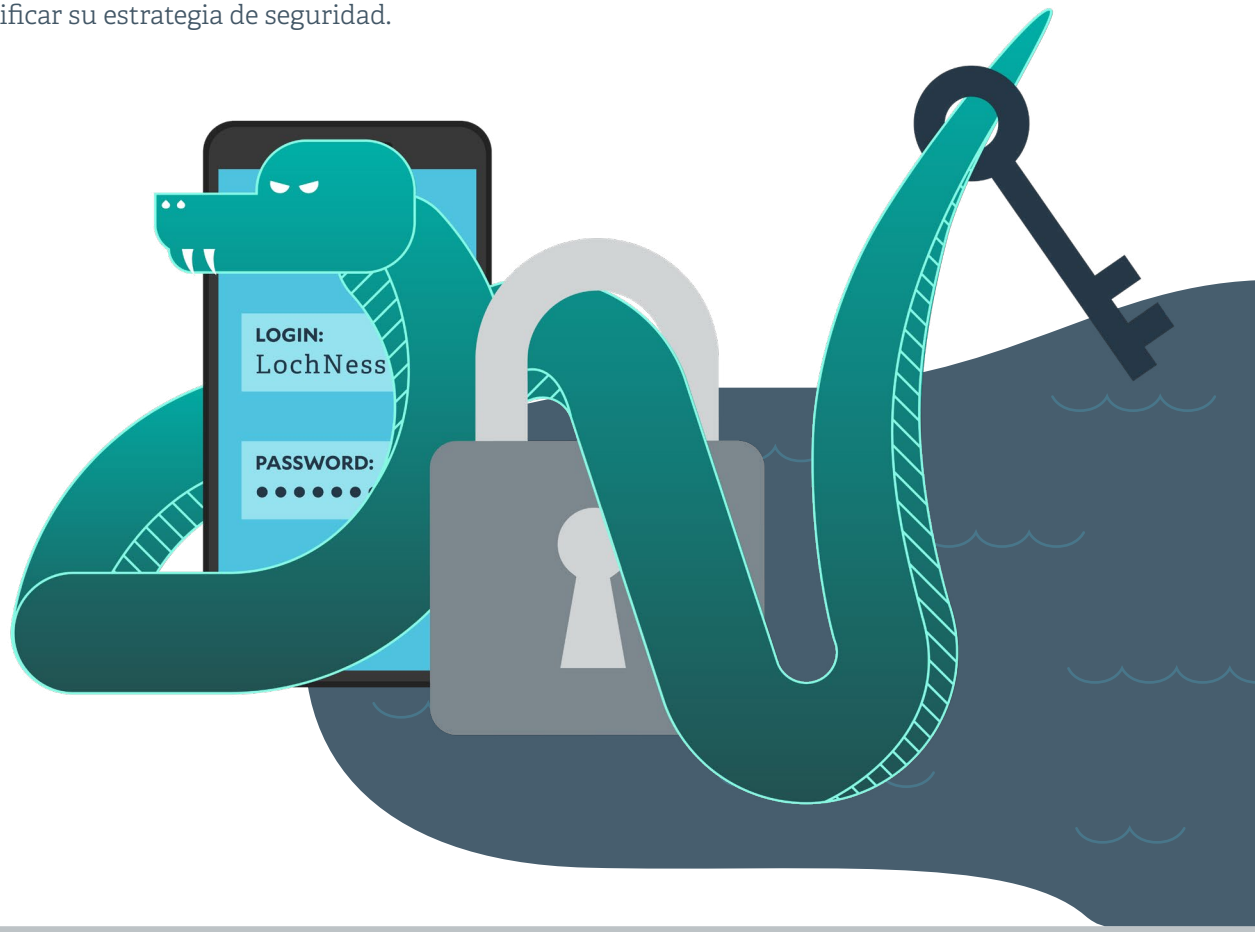
PAM: PRIORIDAD NUMERO NO.1 PARA LOS PROYECTOS DE SEGURIDAD EN 2019

¿Por qué Gartner nombró a PAM su proyecto de seguridad número uno en el año? Debido a que la implementación de PAM no solo tiene un fuerte impacto comercial (positivo), también reduce significativamente el riesgo de incidentes de seguiridad por pérdida de datos.

La administración de acceso privilegiado ayuda a las organizaciones a administrar y controlar el acceso privilegiado sin comprometer la productividad.
PAM puede garantizar un alto nivel de seguridad administrando credenciales privilegiadas a través del almacenamiento centralizado de contraseñas, controlando actividades y accesos privilegiados, y monitoreando cualquier actividad sospechosa.

A finales de 2018, Gartner lanzó su primer cuadrante mágico para PAM. El informe evalúa el escenario de amenazas internas, proporciona un análisis exhaustivo de 14 proveedores de PAM y destaca cuáles Las funciones de administración de acceso privilegiado son indispensables.

Sin embargo, abundan los malentendidos sobre el PMA. BeyondTrust ha identificado seis de los mejores mitos sobre la administración de acceso privilegiado y los ha dividido para facilitarle la vida a la hora de planificar su estrategia de seguridad.



> **"Para 2022, el 90% de las organizaciones reconocerán que la mitigación del riesgo PAM es un control de seguridad fundamental, representando un incremento del 70% en comparación con los días de hoy."**
>
> ***— Gartner "Mejores Prácticas para la Gestión de Accesos Privilegiados a través de los quatro pilares de PAM", 28 de Enero de 2019***

MITO 1: "ZERO TRUST" ES LOGRABLE

¿Qué es el modelo de confianza cero?

Creado por primera vez en 2010 por John Kindervag, analista principal de Forrester Research, se ha convertido en un concepto muy popular entre muchas organizaciones que buscan reducir el riesgo de violación de datos.

El principio detrás de la confianza cero es que requiere medidas de verificación estrictas para todos los dispositivos y personas que acceden a los recursos en un red privada, independientemente de si están dentro del perímetro de la red. No existe una tecnología específica asociada con cero confianza, múltiples tecnologías (con autenticación multifactorial o MFA como principio básico) para lograr el estado óptimo de seguridad. Por lo tanto, se considera un enfoque holístico y un ideal para el que trabajan muchas empresas.

Tres razones por las cuales la confianza cero es un ideal poco realista

Si bien la confianza cero se ha convertido en un eslogan de moda en TI, en la práctica, este modelo a menudo es poco práctico y poco realista de implementar. Aunque Forrester ha proporcionado una hoja de ruta de cinco pasos para lograr una confianza cero, y aunque muchos de los enfoques recomendados tienen mérito y parecen lógicos, se hacen varias suposiciones poco realistas debido a Los siguientes problemas que enfrentan casi todas las organizaciones:

1 Deuda Técnica

Si su organización desarrolla su propio software de consumo y las aplicaciones tienen más de unos pocos años, entonces está en deuda. Rediseñar, recodificar y volver a implementar aplicaciones internas puede ser costoso y potencialmente perjudicial. Es necesario que haya un negocio serio para emprender este tipo de iniciativas. No siempre es posible agregar parámetros de seguridad a las aplicaciones existentes para que sean confiables con cero. Es muy probable que su organización use aplicaciones existentes que no pueden acomodar la confianza cero.

2 Sistemas Legados o Heredados

Es poco probable que las aplicaciones, la infraestructura y los sistemas operativos heredados reconozcan la confianza. Es posible que no tengan los conceptos de privilegio mínimo y movimiento lateral y que no tengan modelos de autenticación que permitan dinámicamente modificaciones basadas en el uso contextual. Cualquier implementación de confianza cero requiere un enfoque por capas para habilitar estos sistemas. Sin embargo, un enfoque por capas implica romper el acceso externo al recurso y rara vez puede interactuar con el sistema en sí. Esto derrota la premisa de Cero confianza.

3 Transformación Digital

Incluso para las organizaciones que pueden construir un nuevo centro de datos, implementar un modelo de acceso basado en roles y adoptar un 100% de confianza cero, las consideraciones de transformación digital pueden dificultar la adopción de la teoría. Cloud, DevOps y la transformación digital impulsada por IoT no son compatibles inherentemente con el modelo de confianza cero porque requiere tecnología adicional para segmentar y aplicar el concepto. Para implementaciones grandes, esto puede ser prohibitivo e incluso puede afectar la capacidad de las soluciones para interactuar correctamente con el acceso multiusuario.

"Realidad"

Un modelo que puede ayudar a superar el límite es la administración de acceso privilegiado just in time (JIT PAM). La parte JIT se origina en la industria manufacturera y es una estrategia que minimiza los costos al reducir el nivel de inventario en proceso. Está impulsado por una serie de señales que le indican a la línea de producción que realice la siguiente parte del producto y cuando sea necesario.

JIT PAM puede ayudar a condensar drásticamente la superficie de amenazas privilegiadas y reducir los riesgos en toda la empresa al garantizar que las identidades solo tengan los privilegios apropiados cuando sea necesario y durante el menor tiempo posible. Este proceso puede ser totalmente automatizado y, por lo tanto, el usuario final no lo nota.

Según Gartner en su Cuadrante Mágico PAM 2018, "para 2022, más de la mitad de las empresas que usan herramientas de administración de acceso privilegiado (PAM) enfatizarán el acceso privilegiado just in time sobre el acceso privilegiado a largo plazo, hoy el número representa un poco más del 25%."

Lea una descripción más detallada de la administración de acceso privilegiado just in time.

MITO 2: LAS CUENTAS COMPARTIDAS SON NECESARIAS PARA HABILITAR PAM

Muchas organizaciones de TI usan cuentas compartidas para usuarios privilegiados, administradores o aplicaciones para darles el acceso que necesitan para realizar su trabajo. Si se maneja mal, esta práctica presenta riesgos significativos de seguridad y cumplimiento derivados del uso intencional, accidental o indirecto de privilegios compartidos.

Incluso para el personal de TI más experimentado, la administración de cuentas compartidas presenta complejidades y riesgos.

Las cuentas compartidas son difíciles de auditar

Según un informe reciente del Monitor ICS-CERT, las cuentas compartidas "dificultan la identificación real del usuario y permiten que terceros maliciosos las usen de forma anónima. Las cuentas utilizadas por un grupo compartido de usuarios a menudo tienen contraseñas malas que los actores maliciosos pueden adivinar fácilmente y que los usuarios no cambian con frecuencia o cuando un miembro del grupo se va."

Es difícil cambiar los hábitos de los empleados comprometidos

Incluso una amplia capacitación y conciencia de seguridad no siempre es suficiente, y los piratas informáticos atacan nuestra naturaleza humana. La ingeniería social sigue siendo una técnica popular y exitosa cuando se trata de obtener acceso a sistemas y datos importantes. Todo lo que se necesita es que un empleado haga clic en un enlace de phishing o visite un website inseguro para abrir una puerta a los piratas informáticos. El empleado puede incluso estar al tanto de este tipo de ataques, pero si lo atrapan en un momento ocupado o se somete a un phishing sofisticado, puede convertirse en una víctima. Y si una cuenta de superusuario se ve comprometida, el hacker puede tener acceso instantáneo a las joyas de la corona.

"Realidad"

Si una cuenta privilegiada compartida se ve comprometida, conlleva riesgos potencialmente devastadores porque las cuentas compartidas a menudo se utilizan en múltiples aplicaciones y recursos. Si ocurre una violación, el atacante podría abarcar múltiples cuentas de empleados y acceso Múltiples ubicaciones en una sola empresa. Identificar quién ha sido comprometido se vuelve más difícil y a menudo requiere muchos sistemas que deben usarse para "solucionar" el problema.

Una cuenta compartida comprometida es como el día de Navidad para un hacker. La buena noticia es que no tiene que cambiar a cuentas compartidas para habilitar PAM.

MITO 3: SOLAMENTE LAS CUENTAS PRIVILEGIADAS SON GESTIONADAS POR PAM

PAM hace más que administrar sus cuentas privilegiadas

La administración de cuentas privilegiadas es la punta del iceberg PAM. Privileged Access Management se compone de varios componentes, cada uno con un propósito en el camino para lograr el equilibrio óptimo entre seguridad y productividad. Un objetivo central es la imposición de privilegios mínimos, definidos como la restricción de derechos de acceso y permisos para usuarios, cuentas, aplicaciones, sistemas, dispositivos (como IoT) y procesos informáticos al mínimo absoluto necesario para realizar actividades autorizadas de rutina.

También conocido como gestión de cuenta privilegiada, gestión de identidad privilegiada (PIM) o simplemente privilegios, muchos analistas y tecnólogos consideran que PAM es uno de los proyectos de seguridad más importantes para reducir el riesgo cibernético y lograr un ROI de alta seguridad.

"Realidad"

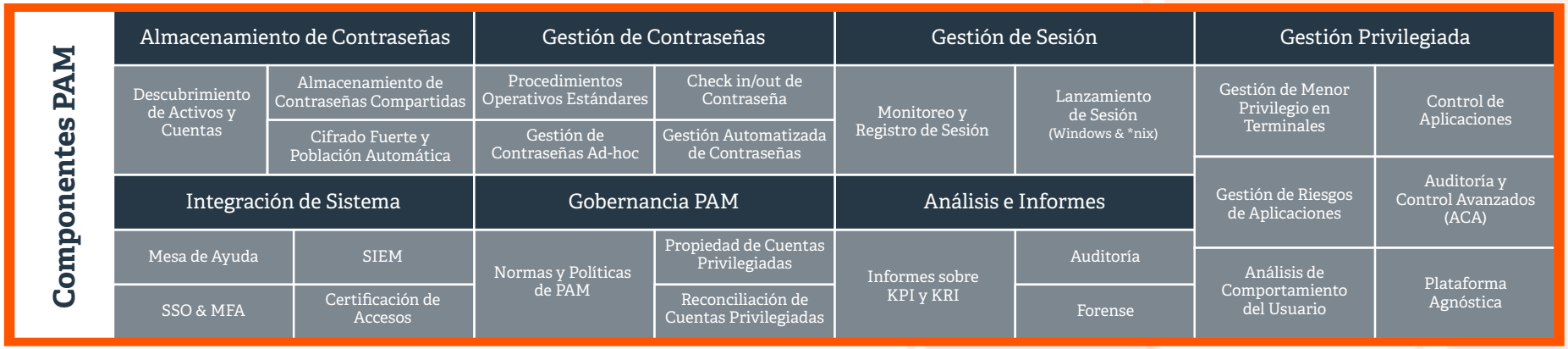
Una plataforma PAM integral incluye mucho más que solo una cuenta privilegiada y gestión de sesión (PASM), aunque sigue siendo un componente esencial. PAM también consiste en una administración de elevación y delegación privilegiada (PEDM), también conocida como administración de privilegios de terminal, acceso remoto seguro (para proveedores y empleados) y más. Algunas de las características clave de PAM incluyen:

- Descubrimiento de cuentas / credenciales privilegiadas en sistemas, dispositivos y aplicaciones e integración para una gestión continua.
- Aleatoriza y almacena automáticamente contraseñas para identidades humanas y no personales privilegiadas.
- Eliminación de los privilegios de administrador y root y simplificación de la aplicación de políticas menos privilegiadas.
- Asegurar rutas de acceso remoto para proveedores y empleados.
- Integre los datos de vulnerabilidad para tomar decisiones privilegiadas de elevación y delegación basadas en el riesgo en tiempo real
- Registre todos los accesos privilegiados para auditoría e informes
- Proporcionar comportamiento de usuario privilegiado y análisis de amenazas.

Integración con soluciones de gobierno de identidad para una visibilidad y gestión continuas de identidades privilegiadas y no privilegiadas en toda la empresa.

En pocas palabras, PAM cubre un área mucho más grande de controles de seguridad y mitigación de amenazas de lo que la gente puede imaginar.

- La estructura MITER ATT & CK
- Los 20 mejores controles críticos



MITO 4: PAM SOLO GESTIONA Y CONTROLA EL DIRECTORIO ACTIVO

La administración de acceso privilegiado trata mucho más que las cuentas de Active Directory (AD). Active Directory (AD) es un servicio de directorio desarrollado por Microsoft para redes de dominio de Windows. Autentica y autoriza a todos los usuarios y computadoras en una red de tipo de dominio de Windows, asignando y aplicando políticas de seguridad para todas las computadoras e instalando o actualizando software.

"Realidad"

Sin embargo, para 2018, el 52.2% del tráfico de Internet provino de dispositivos móviles y se espera que aumente al 63.4% para fines de 2019. El cóctel de los crecientes desafíos de BYOD y la expansión de los servicios en la nube es parte de varias plataformas a las que se mueven los entornos de TI. También es importante tener en cuenta que las empresas que utilizan redes DMZ (que a menudo quedan fuera de los límites de AD) presentan riesgos de seguridad adicionales que PAM también puede ayudar a mitigar.

Otro objetivo de alto valor para los atacantes son los sistemas Unix y Linux, ya que alojan los datos y aplicaciones más críticos. Sin una protección y control completos de las credenciales privilegiadas y la responsabilidad de las acciones de los usuarios, las organizaciones podrían estar expuestas a brechas de riesgo.

Una solución PAM integral para Unix y Linux mitiga todos estos riesgos al proteger, auditar y monitorear todas las cuentas y actividades privilegiadas en sus sistemas más críticos. Active Directory es solo una de las muchas consideraciones que las organizaciones deben tener en cuenta para su estrategia de seguridad.

Además, PAM también ayuda en otras áreas de riesgo menos convencionales en su organización, como las cuentas corporativas de redes sociales. Las contraseñas para sus cuentas corporativas de Facebook, Twitter o LinkedIn deben considerarse privilegiadas; Si las credenciales caen en las manos equivocadas, el mal uso puede provocar daños considerables a largo plazo en la marca y la reputación.

MITO # 5: EL ACCESO AL PROVEEDOR PUEDE GARANTIZARSE UTILIZANDO LA CONFIGURACIÓN DE LA GESTIÓN DE SESIONES DEL GESTOR DE CONTRASEÑAS

El rol de los administradores de contraseñas

Los administradores de contraseñas son herramientas útiles para los usuarios sobrecargados de contraseñas que necesitan saber para acceder a una multitud de sistemas, portales y muchas otras aplicaciones en la organización. Por lo tanto, la idea de tener una bóveda digital encriptada que pueda almacenar toda esta información para usted, así como generar contraseñas únicas y seguras para diferentes servicios, a menudo es una herramienta esencial (y a veces gratuita) que muchas personas usan.

Sin embargo, los administradores de contraseñas orientados al consumidor como LastPass, 1Password y Dashlane tienen limitaciones significativas. Muchos creen erróneamente que este tipo de administradores de contraseñas ofrecerán capacidades de administración de sesión que pueden proteger el acceso del proveedor. Este no es el caso.

Las limitaciones de VPN

El acceso VPN no es lo mismo que el monitoreo de sesión. Saber que se ha iniciado una sesión VPN no ayuda a determinar si las acciones en la sesión son apropiadas. Para seguridad y auditabilidad, los equipos de TI deben ir más allá de las capacidades de administración de VPN, lo que significa monitoreo de sesión con registro de pulsaciones de teclas, indexación y filtrado de comandos para sesiones remotas verdaderamente seguras.

"Realidad"

La administración de sesión por sí sola no protege los protocolos utilizados para el acceso del proveedor. Se requiere una puerta de enlace, proxy, host o punto de salto como middleware para garantizar que la sesión no se use como cabeza de puente para actividades maliciosas adicionales.

Las soluciones como el acceso remoto privilegiado no solo protegen, administran y auditan al proveedor y el acceso privilegiado remoto interno sin una VPN, sino que también funcionan en entornos híbridos y le permiten cumplir requisitos de cumplimiento más complejos a través de pistas de auditoría integrales y Análisis forense de sesiones.

Es importante destacar que las herramientas gratuitas (como RDP) no son lo suficientemente robustas, para una mirada en profundidad al documento técnico: El verdadero costo del software de soporte remoto gratuito.

MITO 6: UN GRAN EQUIPO DE TI ES NECESARIO PARA LA IMPLEMENTACIÓN Y GESTIÓN DE PAM

El concepto de implementar la administración de acceso privilegiado puede ser desalentador para muchos, especialmente si su entorno está compuesto por una variedad de sistemas operativos, software heredado y ubicaciones globales distantes. O tal vez tiene un pequeño personal de TI que ya está al límite. Sin embargo, una buena solución PAM será fácil de implementar y mantener con el tiempo. Implementar PAM es más fácil de lo que piensas.

"Realidad"

PAM consta de tres componentes principales, con diferentes esfuerzos requeridos para cada uno, enumerados a continuación, los más pequeños para el mayor esfuerzo y mantenimiento:

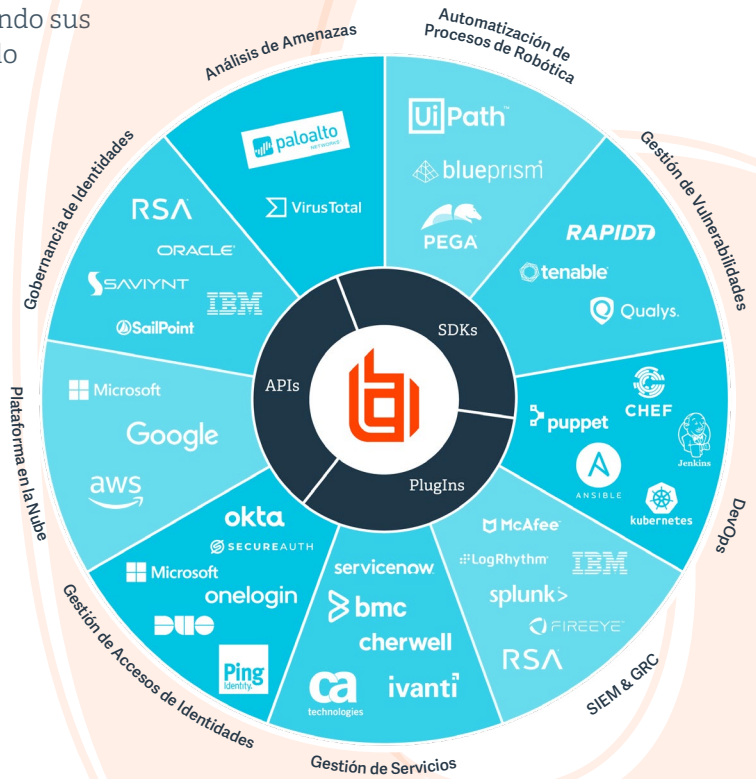
- Acceso remoto seguro (SRA): proteja, administre y audite el acceso privilegiado remoto interno y del proveedor sin una VPN. Necesita poco o nada de mantenimiento.
- Endpoint Privilege Management (EPM): elimine los privilegios innecesarios y eleve los derechos a Windows, Mac, Unix, Linux y dispositivos de red sin sacrificar la productividad. Se requiere mantenimiento limitado cuando ocurren cambios ambientales o de aplicación.
- Administración de cuentas y sesiones privilegiadas (PASM): descubra, administre, audite y monitoree cuentas privilegiadas de todo tipo. Se requiere mantenimiento de nivel medio cuando se producen cambios en los procedimientos, el entorno o el personal.

Una vez que se instala el entorno para cada componente, se proporciona automatización interna (incluido el mantenimiento de la base de datos) en una solución PAM líder.

Implementación facilitada a través de integraciones

En términos de implementación, debe consultar con socios, proveedores y expertos en integración de sistemas. Tienen experiencia en la instalación de PAM y pueden transformar una curva de aprendizaje potencialmente empinada en un proyecto muy manejable. Los principales proveedores de PAM proporcionarán un amplio conjunto de integraciones, lo que significa que puede beneficiarse de las tecnologías que trabajan juntas de forma inmediata, maximizando sus inversiones de TI existentes y haciendo que todo el proceso sea aún más uniforme y eficiente. Por ejemplo, BeyondTrust se integra con una amplia variedad de soluciones de terceros. Consulte la figura a continuación para obtener una descripción general de nuestro ecosistema de socios.

Para reducir los gastos generales y los requisitos de infraestructura, las soluciones PAM se pueden implementar en la nube utilizando software como servicio (SaaS) o una solución alojada como AWS o Azure. La administración de credenciales en la nube puede hacer que la administración de acceso privilegiado sea más fácil y rentable. Para las organizaciones que buscan reducir los riesgos de acceso privilegiado mientras enfrentan escasez continua de personal y recursos, las soluciones en la nube PAM proporcionan cargas administrativas reducidas y una implementación rápida.



CONCLUSIÓN

Es importante poder separar los mitos de los hechos al determinar el enfoque de su organización para mitigar los riesgos de una violación cibernética. Comprender los verdaderos beneficios y los casos de uso de la administración de acceso privilegiado es un paso importante que puede tomar para mejorar significativamente la estrategia de seguridad de su organización.

La guía integral para compradores de acceso privilegiado integral de BeyondTrust proporciona una guía más detallada sobre cómo seleccionar la solución PAM adecuada para su negocio. Aquí descubrirá cómo evaluar de manera integral sus necesidades de seguridad de acceso privilegiado y asignarlas a soluciones modernas de administración de privilegios. Esto lo ayudará a identificar dónde comenzar su proyecto de administración de acceso privilegiado, cómo avanzar hacia una mejor postura de seguridad de TI y qué resultados comerciales esperar.

LA PLATAFORMA DE BEYONDTRUST

La plataforma de administración de acceso privilegiado BeyondTrust es una solución integrada para proporcionar control y visibilidad sobre todas las cuentas y usuarios privilegiados en todas las plataformas corporativas. Al reunir las mejores características que ofrecen muchos proveedores alternativos como herramientas desconectadas, la plataforma de administración de acceso privilegiado BeyondTrust simplifica las implementaciones, reduce los costos, mejora la seguridad del sistema y cierra los agujeros de seguridad para reducir el riesgo.

Sobre BeyondTrust

BeyondTrust es el líder mundial en gestión de acceso privilegiado, que ofrece el enfoque más perfecto para prevenir incidentes y brechas de seguridad sobre los datos relacionadas con credenciales robadas, privilegios mal utilizados y acceso remoto comprometido. Nuestra plataforma extensible permite a las organizaciones escalar fácilmente la seguridad de los privilegios a medida que las amenazas evolucionan en entornos de punto final, servidor, nube, DevOps y dispositivos de red. BeyondTrust ofrece a las organizaciones la visibilidad y el control que necesitan para mitigar el riesgo, lograr objetivos de cumplimiento y aumentar el rendimiento operativo. 20,000 clientes confían en nosotros, incluidos más de la mitad de Fortune 100 y una red global de socios.

Acerca de la gestión de privilegios de terminales

Las soluciones de administración de privilegios de punto final de BeyondTrust le brindan el poder de imponer menos privilegios y eliminar los derechos de administrador local. Elimine los privilegios excesivos del usuario final y las aplicaciones de control en Windows, Mac, Unix, Linux y dispositivos de red, todo sin comprometer la productividad del usuario final.

Sobre la gestión de contraseñas

BeyondTrust Password Safe unifica la contraseña privilegiada y la administración de sesión privilegiada al proporcionar descubrimiento, administración, auditoría y monitoreo seguros para cualquier credencial privilegiada. Password Safe permite a las organizaciones obtener un control y responsabilidad completos sobre las cuentas privilegiadas.

Acerca del acceso remoto privilegiado

BeyondTrust Privileged Remote Access proporciona visibilidad y control sobre el acceso de terceros, así como el acceso remoto interno, lo que permite a las organizaciones ampliar el acceso a activos importantes pero sin comprometer la seguridad.

beyondtrust.com/es/

V2020_07_SPA