Cuadrante Mágico para la Administración de Accesos Privilegiados (**PAM**)

Published: 3 December 2018 **ID:** G00356017
Analyst(s): Felix Gaehtgens, Dale Gardner, Justin Taylor, Abhyuday Data, Michael Kelley

La administración de Accesos Privilegiados es uno de los controles de seguridad más críticos, particularmente en los ambientes de TI actuales cuya complejidad aumenta de forma constante. Los líderes en Administración de Riesgos y Seguridad deben utilizar herramientas PAM en una estrategia a largo plazo para la mitigación de riesgos.

Supuestos de Planificación Estratégica

Para el año 2020, más del 50% de las compañías que utilizan herramientas de administración de acceso privilegiado (PAM) enfatizarán el acceso privilegiado **just in time** sobre el acceso privilegiado a largo plazo. Actualmente son menos del 25%.

Para el año 2021, el 40% de las organizaciones (en comparación con menos del 10% en 2018) que utilizan prácticas formales de gestión de cambios, tendrán herramientas PAM integradas dentro de ellas, reduciendo significativamente la superficie de riesgo general.

Para el año 2021, más del 50% de las organizaciones que utilizan DevOps adoptarán productos de administración de passwords secretos basados en PAM, aumentando significativamente desde menos del 10% en la actualidad.

Definición / Descripción del Mercado

Las herramientas PAM ayudan a las organizaciones a proporcionar acceso privilegiado seguro a los activos críticos, y a cumplir con los requisitos normativos al administrar y monitorear cuentas y acceso privilegiados. Las herramientas PAM ofrecen características que permiten a los líderes de seguridad y riesgos:

- En todos los casos
  - Descubrir e inventariar cuentas privilegiadas en sistemas, dispositivos y aplicaciones para su posterior administración.
  - Automáticamente administrar, guardar y generar contraseñas seguras y aleatorias, y otras credenciales para cuentas administrativas, de servicio y de aplicación.
  - Controlar el acceso a cuentas privilegiadas, incluidas las cuentas compartidas y cuentas de acceso de emergencia ("firecall").
  - Aislar, supervisar, registrar y auditar sesiones, comandos y acciones de acceso privilegiado.
- Para Usuarios:
  - Proporcionar un inicio de sesión único (SSO) para sesiones privilegiadas, comandos y acciones, de forma segura para no revelar las credenciales de la cuenta (contraseñas, claves criptográficas, etc.).

- Delegar, controlar y filtrar operaciones privilegiadas que un administrador puede ejecutar.
- Asegurar los niveles requeridos de confianza y responsabilidad para el acceso privilegiado, al proporcionar capacidades de autenticación sólidas e integrarse con productos y servicios de autenticación externos.

- Para Servicios y Aplicaciones:
  - Eliminar las contraseñas codificadas en programas fuentes al hacer que estén disponibles bajo demanda para las aplicaciones. Dos categorías distintas de herramientas han evolucionado como el foco predominante para los líderes de seguridad y gestión de riesgos que consideran la inversión en herramientas PAM:
    - **Gestión privilegiada de cuentas y sesiones (PASM)**. Las cuentas privilegiadas están protegidas mediante el almacenamiento de sus credenciales. El acceso a esas cuentas se promueve para usuarios humanos, servicios y aplicaciones. Las funciones de **administración de sesión privilegiada** (PSM) establecen sesiones con posible inyección de credenciales y grabación de sesión completa. Las contraseñas y otras credenciales para cuentas privilegiadas se administran de forma activa, como el cambio a intervalos definidos o la ocurrencia de eventos específicos. Las soluciones PASM también pueden proporcionar administración de contraseña de aplicación a aplicación (AAPM).
    - **Administración de elevación y delegación de Privilegios (PEDM)**. Los privilegios específicos en el sistema administrado se otorgan por los agentes basados en host para los usuarios que inician sesión. Esto incluye el control de comandos basado en el host (filtrado) y la elevación de privilegios, este último permitiendo que comandos particulares se ejecuten con un nivel más alto de privilegios.

Los proveedores analizados en este Cuadrante Mágico deben proporcionar al menos un producto PASM completamente funcional y, opcionalmente, también herramientas PEDM. En los comentarios sobre cada proveedor, mencionamos la calidad de los componentes individuales del producto y usamos términos como "muy por encima del promedio", "por encima del promedio", "promedio", "por debajo del promedio" y "muy por debajo del promedio". El promedio para un componente en particular se refiere al puntaje promedio para todos los proveedores evaluados en esta investigación para ese componente. Consulte la entrada de "Producto o servicio" en la sección Criterios de evaluación para obtener una descripción completa de estos componentes y lo que se evaluó.

Magic Quadrant

Figura 1. Cuadrante Mágico para Proveedores de Administración de Accesos Privilegiados

Source: Gartner (December 2018)

Proveedores: Fortalezas y Precauciones

BeyondTrust

BeyondTrust ofrece un conjunto completo de productos PAM bajo la marca PowerBroker. BeyondTrust PowerBroker Password Safe (PBPS) es una solución PASM que utiliza un enfoque de servidor intermedio para la administración de sesiones. La funcionalidad de administración y descubrimiento de cuentas de servicio está muy por encima del promedio, y BeyondTrust ofrece una herramienta integrada llamada PowerBroker Privilege Discovery and Reporting Tool (DART). La gestión de claves SSH está disponible. Se incluye la funcionalidad AAPM, se basa en aplicaciones para mantener una clave estática para la autenticación desde la bóveda.

BeyondTrust también ofrece una solución PEDM (Privileged Elevation & Delegation Management) para múltiples sistemas. PowerBroker para UNIX y Linux (PBUL) incluye bridges de Active Directory para sistemas UNIX / Linux, que también pueden adquirirse de manera independiente como PowerBroker Identity Services. PowerBroker for Sudo es una solución alternativa que extiende el sudo nativo para la administración centralizada de políticas. PowerBroker para Windows (PBW) y PowerBroker para Mac implementan el filtrado de comandos para los sistemas operativos respectivos. PowerBroker for Networks proporciona filtrado de comandos en base al protocolo para dispositivos de red y sistemas de control industrial, entre ellos IOT, ICS y SCADA.

Todos los productos se basan en un componente/consola llamado BeyondInsight, que se incluye con cada producto PowerBroker. BeyondInsight proporciona funciones de descubrimiento integrales y un entorno unificado de administración, informes y análisis de amenazas para varias soluciones de BeyondTrust.

Las funciones de gestión de vulnerabilidades se pueden agregar como una opción.

PBPS se entrega como software, o como un dispositivo virtual o de hardware (Appliance). También está disponible en varios mercados de IaaS (Amazon Web Services [AWS], Microsoft Azure y Google Cloud Platform) utilizando el mecanismo de “traer licencias propias”. BeyondTrust prefiere licenciar PBPS en función de cada dispositivo / objeto, pero permite que los clientes obtengan licencias para cada usuario administrador / operador. Todos los demás productos se licencian exclusivamente por dispositivo / objeto.

En octubre de 2018, Bomgar se fusionó con BeyondTrust. La nueva empresa conserva el nombre de BeyondTrust. Esta evaluación del Cuadrante Mágico refleja las capacidades de BeyondTrust antes de que se anunciara la fusión. La empresa combinada tiene muchos componentes y soluciones que, si están bien integradas, podrían crear **una de las soluciones más poderosas y atractivas** en términos de amplitud y profundidad dentro del mercado de PAM.

Fortalezas de BeyondTrust

- BeyondInsight, que se incluye con cada producto PowerBroker, puede integrar funciones de PAM como el descubrimiento, con la administración de activos y vulnerabilidades. La sinergia de esta integración puede ayudar a las organizaciones a reducir la superficie de ataque y el riesgo con mayor rapidez y precisión.
- La integración de PBPS con ServiceNow se destaca en funcionalidad y características avanzadas, como un conector inteligente de amenazas para la gestión de activos de ServiceNow, e integración con PBUL. Esto permite a los usuarios autorizados realizar acciones administrativas específicas desde ServiceNow sin iniciar sesión como administradores.

- BeyondTrust cuenta con monitoreo de integridad de archivos como parte de PBUL y PBW.
- El proveedor ofrece precios tanto para el usuario como para el dispositivo / objeto, y los precios para una serie de escenarios **fueron con frecuencia, por debajo de los promedios de la industria.**

Precauciones

Los clientes comentan que la configuración requiere experiencia en el producto.

PBPS incluye un repositorio de datos autocontenido para implementación de configuraciones simples, pero esto no es suficiente para implementaciones empresariales con necesidades de alta disponibilidad y recuperación ante desastres. Para esas necesidades, existe un mecanismo de configuración opcional que utiliza Microsoft SQL Server Always On como repositorio de datos.

La nueva empresa fusionada BeyondTrust puede sufrir cambios a medida que se consolidan las líneas de productos, canales y departamentos. Gartner no espera que BeyondTrust anuncie pronto el fin de la vida útil de ninguno de sus productos principales.

Características Adicionales de PBPS

- Pueden enviarse alertas y cuando se superan los umbral de riesgo, los usuarios con privilegios pueden ser bloqueados u obligados a volver a autenticarse.
- Se licencia por usuario o dispositivo y ofrece capacidades PASM, incluida la gestión de bóvedas y sesiones, y la grabación que funciona mediante un mecanismo proxy o servidor de salto (jump server). Las capacidades de descubrimiento y cuenta de servicio están muy por encima del promedio. Se incluye una interfaz de acceso HTML5 opcional para permitir el acceso privilegiado completo desde un navegador web sin herramientas en el cliente. También se incluye la gestión de claves SSH. La funcionalidad de AAPM es excelente.
- La Administración de sesiones privilegiadas admite varios protocolos en modo “proxy”, incluidos RDP, SSH Telnet y X11. También admite la supervisión de accesos a bases de datos Microsoft SQL Server, MySQL y Oracle, DB2, Sybase.
- La Administración de sesiones privilegiadas puede proporcionar reconocimiento de las acciones de teclado (para sesiones gráficas y de terminales) y mouse, archivos ejecutados para sesiones gráficas capturadas, identificando comandos ejecutados, de gran utilidad para las actividades de auditoría.
- Todas las funciones están incluidas en el producto base, y el proveedor tiene un historial de inclusión de nuevas capacidades como parte de las actualizaciones, en lugar de dividirlas en productos separados y cobrarlos por separado.
- A diferencia de la mayoría de los proveedores que requieren que las aplicaciones almacenen las claves en formatos vulnerables, se puede utilizar una API con certificados para las aplicaciones, lo que permite el uso de claves rotadas automáticamente. Este método puede eliminar efectivamente cualquier credencial estática de aplicaciones o scripts.
- Es compatible con RDP, SSH, Telnet, y múltiples aplicaciones utilizando una función de conexión remota basada en proxy. Se pueden configura la inyección de credenciales en aplicaciones basadas en Web (como los paneles de control SaaS), en aplicaciones legacy, aplicaciones de

conexión a bases de datos, etc. Los comandos se pueden filtrar en sesiones Telnet y SSH para que la solución pueda enviar alertas cuando se realizan intentos de ejecutar comandos críticos o peligrosos.

- Fuerte soporte y distribución local en el mercado Latinoamericano, en contraste con muchos otros proveedores por los cuales se pasa por alto o no se respalda a América Latina.
- Provee integración con Remedy, y ServiceNow.

Notas

- En esta edición del cuadrante mágico no se incluyeron nuevos proveedores.
- También se evaluó:
- Características para la administración de contraseñas de aplicación a aplicación, y si los proveedores podrían eliminar cualquier tipo de secreto codificado (contraseña o clave de aplicación).
- La compatibilidad con protocolos como SSH y RDP, así como protocolos adicionales como HTTPS, ICA, TDS, Telnet, VNC, X11, etc.
- La capacidad de filtrar comandos u operaciones sobre la base de un protocolo.
- Capacidades de grabación y reproducción de sesiones: lo que podría grabarse y lo fácil que sería revisar rápidamente sesiones, buscar eventos particulares o visualizar rápidamente lo que se ha hecho.

Ver el informe completo Analyst-Report-2018-Gartner-Magic-Quadrant-for-PAM

Ver el informe completo The Forrester Wave™: Privileged Identity Management, Q4 2018