BeyondTrust

PRIVILEGE MANAGEMENT FOR UNIX & LINUX

Implemente seguridad de accesos privilegiados sin igual *con* Privilege Management for Unix & Linux

Los sistemas Unix y Linux presentan blancos de mucho valor para hackers y personal interno que haga uso malicioso de información privilegiada. Lo mismo sucede con los dispositivos conectados en red, como IoT, ICS y SCADA.
Conseguir las credenciales root y otras credenciales privilegiadas les facilita a los hackers pasar inadvertidos y acceder a sistemas y datos críticos.

Privilege Management for Unix & Linux de BeyondTrust es una solución empresarial de gestión de privilegios de primer nivel que ayuda a las organizaciones de seguridad y de informática a cumplir con la normativa, controlar el acceso privilegiado y prevenir y contener vulneraciones de datos que puedan afectar a sistemas Unix y Linux. Amplíe las funcionalidades mucho más allá de sudo con administración centralizada, control y administración de sesiones, control de integridad de archivos y una poderosa mejora de la productividad.

"La implementación de Privilege Management for Unix & Linux de BeyondTrust nos dio excelentes resultados. El acceso a todos los servidores es limitado, incluso por SSH. Los auditores pueden ver con facilidad que se siguen los procedimientos, y nuestro personal de informática puede mantener su productividad".

SVP Systems / Recuperación, CTO, DCI

Entre sus funciones más importantes están:

Auditoría y Gobernanza

Recopile, guarde en un lugar seguro e indexe diversos tipos de registro, grabaciones de sesiones y otros eventos privilegiados para analizar el comportamiento de sus usuarios.

Políticas Granulares con Privilegios Mínimos y Acceso Dinámico

Eleve privilegios de usuarios comunes en Unix y Linux mediante controles específicos basados en políticas y utilice factores tales como la hora, el día, la ubicación y el estado de vulnerabilidad de la aplicación o el recurso para tomar decisiones de elevación de privilegios.

Control de Aplicaciones y Sistema Remoto

Permita a los usuarios ejecutar comandos específicos y mantener sesiones remotas basadas en reglas, sin iniciar sesión como administrador o root.

Control de Integridad de Archivos y de Políticas

Audite e informe cambios hechos a políticas, sistemas, aplicaciones y archivos de datos críticos.

Limite el Acceso a Root

Establezca reglas detalladas de elevación de privilegios para ejecutar solo tareas o comandos específicos.

Audite Toda la Actividad de los Usuarios

Protéjase contra cambios no autorizados en archivos, secuencias de comandos y directorios.

Controle Registros y Sesiones

Detecte actividades sospechosas de usuarios, cuentas y recursos en tiempo real.

Detalles y Demostración de Privilege Management for Unix & Linux

beyondtrust.com/products/privilege-management-for-unix-and-linux