

Administre y audite el acceso remoto de empleados y proveedores con Privileged Remote Access

Hoy en día, las empresas necesitan administrar el acceso a redes cada vez más complejas con perímetros en infinita expansión. Los ecosistemas incluyen infraestructura como servicio (IaaS, por sus siglas en inglés), recursos internos en la nube y consolas web de administración a los cuales debe acceder una gran variedad de proveedores externos y empleados remotos. Los privilegios de acceso remoto mal administrados, en especial las VPN, son vectores de amenaza muy atractivos para actores maliciosos.

Privileged Remote Access de BeyondTrust les da a las personas adecuadas acceso a los sistemas apropiados en el momento indicado, y brinda visibilidad y control de todos los accesos remotos, incluidos los de administradores informáticos, proveedores externos, programadores e ingenieros de operaciones en la nube. Las organizaciones aprovechan la solución para brindar acceso continuo a recursos informáticos importantes sin dejar de cumplir con rigurosas exigencias de seguridad y cumplimiento normativo.

“Antes, la única manera que teníamos de darles acceso a los proveedores era establecer una VPN. Con BeyondTrust, podemos darles acceso limitado a nuestro entorno y grabar sus sesiones para tener un registro de auditoría exacto de lo que se haya hecho. Eso hace que nuestro entorno sea mucho más seguro”. - **Brian Bard, analista de empresas y tecnología, Universidad de Carolina del Norte, Charlotte**

Entre sus funciones más importantes están:

Control de Accesos Privilegiados

Elimine los accesos remotos radicales y permítalos a sus empleados y a terceros conectarse sin problemas ni riesgos a cualquier cosa, desde cualquier lugar —desde un servidor con Windows hasta un clúster Kubernetes— mediante acceso granular, basado en la función, con parámetros de sesión definidos.

Infraestructura como Código

Aproveche el poder de la automatización con API y herramientas fáciles de usar, como Terraform, que le permiten aumentar y reducir el uso de infraestructura en la nube, y brindar y quitar acceso.

Incorpore Sus Propias Herramientas (BYOT)

Permita a los usuarios emplear herramientas conocidas, como Putty y Data Studio de Azure, para hacer su trabajo y mantenga así flujos de trabajo seguros para su personal técnico, todo sin una VPN.

Integraciones Simples

Incorpore acceso remoto seguro y privilegiado a las herramientas SIEM que ya tenga, para establecer un único punto central que usen los analistas y los técnicos dentro de los flujos de trabajo con los que ya se sientan cómodos.

Promueva la Eficiencia

Proporcione acceso seguro y mantenga los flujos de trabajo con integraciones robustas que no pongan en peligro el cumplimiento normativo ni la seguridad.

Cumpla con los Requisitos Normativos

Dinamice las auditorías con registro avanzado de sesiones de toda la actividad de soporte remoto en un único repositorio central.

Reduzca Costos

Elimine la necesidad de usar VPN y maximice así su valor y mejore la seguridad de su red.

