

# OFREZCA ACCESO. NO UNA VPN

La solución de gestión de accesos privilegiados de BeyondTrust permite a los profesionales de seguridad controlar, monitorear y administrar el acceso a sistemas críticos por parte de usuarios privilegiados, incluidos proveedores externos. Con BeyondTrust, puede:

- \* Eliminar el punto de entrada que los atacantes pueden ganar dentro de su entorno
- \* Mantener control granular de los accesos a su red
- \* Supervisar y auditar sesiones de acceso en tiempo real
- \* Registrar los datos de seguridad de sesiones directamente en su herramienta SIEM
- \* Mitigar los ataques de suplantación de identidad
- \* Disminuir los tiempos de respuesta a incidentes
- \* Realizar investigaciones forenses efectivas
- \* Cumplir con lineamientos de auditoría

## ¿Sabías?



Los hackers generalmente necesitan días y semanas para encontrar lo que buscan. Si obtienen acceso VPN desde un sistema explotado hacia una red interna, a menudo pueden moverse sin ser detectados y usar técnicas de pivote para encontrar su objetivo final. Los hackers suelen elegir a proveedores externos con métodos de acceso como VPN y RDP hacia una red segura, sabiendo que son más fáciles de comprometer. BeyondTrust brinda a los usuarios externos acceso a los sistemas sin el uso de una VPN.

1 9 7 días

En promedio, ese es el tiempo que le toma a una organización darse cuenta que ha tenido una brecha de seguridad. En el caso que se comprometiera el acceso de un externo, cualquier actividad maliciosa se detendría una vez que se agote el tiempo de espera de una sesión de BeyondTrust, en comparación con una VPN en la que el hacker tenga total dominio hasta que sea detectado.



El 80% de las brechas de seguridad involucran una cuenta privilegiada que es explotada. La postura de seguridad de sus proveedores externos puede no cumplir con los mismos estándares de su organización. Para los hackers, los usuarios externos suelen ser una forma más fácil de atacar su red.

62%

Cerca de dos tercios de las empresas creen que administrar la identidad y los accesos en su organización es complejo. En promedio, las compañías tienen 1.200 solicitudes de acceso por mes. BeyondTrust aborda esta complejidad al permitir que los administradores gestionen, monitoreen y auditen de manera centralizada el acceso sin interrumpir los procesos.

## ÉRASE UNA VEZ...

el mayor riesgo de seguridad era un ataque MitM (Man in the Middle) en una conexión remota a su red.

EMPLEADO / OFICINA REMOTA



INTERNET

RED CORPORATIVA



Las empresas comenzaron a implementar VPNs para proporcionar un túnel encriptado para que oficinas y empleados remotos accedan a la red, deteniendo los ataques MitM.

EMPLEADO / OFICINA REMOTA



ALTO NIVEL DE CONFIANZA

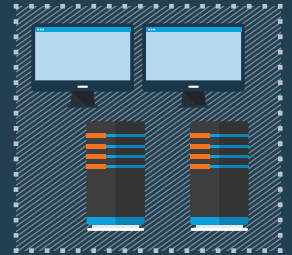


VPN



INTERNET

RED CORPORATIVA



A medida que terceros y proveedores comenzaron a requerir acceso privilegiado a sus redes, las empresas les dieron acceso utilizando la mejor herramienta disponible: VPN.

USUARIO REMOTO



BAJO NIVEL DE CONFIANZA

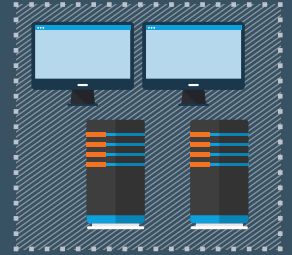


VPN



INTERNET

RED CORPORATIVA



Los ciberdelincuentes aprendieron que un proveedor con una conexión VPN es el medio perfecto para obtener acceso a una red segura. Con este punto de entrada por VPN, tienen el acceso y el tiempo para encontrar y atacar sistemas sensibles.

PROVEEDOR COMPROMETIDO



BAJO NIVEL DE CONFIANZA



VPN



INTERNET

RED CORPORATIVA



## ¡BRINDE A LOS PROVEEDORES EXTERNOS ACCESO SIN VPN!

La solución de gestión de accesos privilegiados de BeyondTrust le permite dar a los proveedores y terceros acceso a su red sin una conexión VPN y sin conectarse directamente a sus sistemas internos de mayor valor.

USUARIO REMOTO

INTERNET

GESTIÓN DE ACCESOS PRIVILEGIADOS BEYONDTTRUST

RED CORPORATIVA



Evitamos los ataques MitM



BeyondTrust le permite aplicar y solicitar controles de acceso granulares a proveedores externos. También captura registros de auditoría y grabación de videos de toda la actividad del proveedor.



Sin modificaciones en el firewall. El proveedor remoto está conectado a través de una conexión de solo salida al appliance BeyondTrust, NO al sistema de destino.



Con BeyondTrust, puede establecer qué proveedores pueden acceder a los sistemas, cuándo y durante cuánto tiempo, para que no permanezcan en su red.