BeyondTrust

Los 5 Principales Problemas de los Accesos Remotos

Con el creciente número de dispositivos conectados, y las vulnerabilidades que rodean a las herramientas y contraseñas de acceso remoto, los departamentos de TI se enfrentan a la gestión de los riesgos de seguridad mientras mantienen la productividad de los empleados. Se espera que continúe la rápida expansión del trabajo remoto y los requisitos de seguridad relacionados con el acceso remoto seguro son más críticos que nunca.

¿Su equipo cuenta con las herramientas seguras adecuadas para manejar los problemas más urgentes relacionados con el gran volumen de proveedores externos, usuarios internos privilegiados y trabajadores remotos que se conectan de forma remota a su red?

1 GESTIONANDO LOS ACCESOS DE LOS PROVEEDORES

En promedio, los profesionales de TI informan que casi 182 proveedores externos acceden a su red interna semanalmente[1]. Estos terceros van desde proveedores de hardware hasta fabricantes de software o subcontratistas de TI. A menudo tienen Active Directory u otras credenciales privilegiadas, y muy probablemente una VPN, lo que les permite iniciar sesión en su red en cualquier momento y permanecer conectados todo el tiempo que quieran.

[1]BeyondTrust, "Privileged Access Threat Report", 2019

2 ACCESO PRIVILEGIADO "TODO O NADA"

La mayoría de sus empleados o proveedores solo necesitan acceso a sistemas muy específicos. El uso de una VPN permite el acceso en la capa de red, lo que comúnmente proporciona más acceso del necesario, resultando en un acceso "sobrante" cuando los usuarios son eliminados o reemplazados. Esto ocurre especialmente cuando una gran cantidad de usuarios y proveedores internos dependen del acceso remoto para funciones de trabajo críticas. Las herramientas como las VPN carecen de controles granulares y solo pueden habilitar el acceso "todo o nada" en la capa de red, carecendo de funcionalidades para administrar aplicaciones o sesiones.

Mi organización está sujeta a estrictos mandatos de cumplimiento que debemos cumplir.

3 CUMPLIMIENTO DE LAS DIRECTRICES DE CONFORMIDAD

Muchas organizaciones están sujetas a estrictos estándares de cumplimiento como PCI, GDPR e HIPAA. Existen procedimientos de auditoría para garantizar que se cumplan los requisitos de cumplimiento, y el trabajo de la organización es proporcionar evidencias de que están siguiendo los estándares. Muchas herramientas de acceso heredadas, como RDP o VNC, no pueden realizar un seguimiento adecuado o auditar la actividad durante las sesiones remotas.

Necesito mantener la productividad de los trabajadores remotos, y ofrecer acceso a los activos de TI que necesitan para hacer su trabajo.

4 HABILITACIÓN DE TRABAJO REMOTO

Las VPNs simplemente no se crearon para la seguridad de la capa de aplicaciones, la visibilidad del usuario final, los escritorios compartidos y las aplicaciones web modernas. Además del riesgo de seguridad, el rendimiento de la VPN puede deteriorarse cuando muchos empleados remotos están conectados. Las empresas buscan alternativas para que los empleados puedan trabajar sin interrupciones, al tiempo que brindan una mejor experiencia de acceso remoto.

Necesito bloquear las contraseñas de las cuentas de administrador compartidas y hacer cumplir las políticas de contraseñas corporativas.

5 LAS CONTRASEÑAS SE ALMACENAN DE MANERA MANUAL Y NO SEGURA

Las cuentas de usuarios privilegiados son un punto de entrada de red común para los hackers. Dado que muchos profesionales de TI utilizan varias cuentas privilegiadas para acceder a los endpoints en la red, el volumen de credenciales para administrar y proteger es alto. Estas credenciales a menudo se almacenan y comparten de forma insegura mediante archivos de excel o notas. A menudo son olvidadas, se repiten y rara vez o nunca se cambian.

Las herramientas heredadas carecen de características adecuadas de seguridad y productividad

Las tecnologías de gestión de accesos heredadas, como las VPN o RDP, solo abordan un número limitado de casos de uso, lo que puede resultar en el uso de diferentes herramientas para hacer cumplir todas las tareas. La falta de flujos de trabajo automatizados puede ralentizar aún más a los equipos de TI.

También tienen brechas de seguridad significativas, como resultado de la falta de niveles granulares de acceso o la incapacidad de crear registros para auditorías de cumplimiento.

Controle, Administre y Audite el Acceso Remoto con BeyondTrust

Privileged Remote Access

Las soluciones de acceso remoto privilegiado permiten a las organizaciones brindar a sus empleados remotos y proveedores externos el acceso a su red sin la necesidad de una conexión VPN. Los usuarios tienen acceso granular a diferentes segmentos de red o sistemas específicos usando privilegios. Esta capacidad no solo mitiga los riesgos de un enfoque amplio para la asignación de privilegios en capas de red, sino que también ayuda a las organizaciones a lograr mandatos de cumplimiento o marcos que especifican controles de acceso.

El uso de BeyondTrust Privileged Remote Access, ya sea en conjunto con su VPN corporativa o como reemplazo de esta, permite a su organización eliminar los puntos ciegos del acceso remoto, reducir la superficie de ataque e impulsar la productividad de las siguientes maneras:

- Haciendo cumplir una política de privilegios mínimos, dando a usuarios específicos el nivel adecuado de acceso a aplicaciones, sesiones y protocolos;
- Dando responsabilidad individual de las cuentas compartidas, proporcionando una pista de auditoría para el acceso;
- Definiendo a qué endpoints pueden acceder los usuarios, cuándo pueden acceder a ellos y qué aplicaciones o acciones pueden usar durante esas sesiones;
- Eliminando la carga administrativa de configuración e instalación de una VPN para proveedores, usuarios privilegiados y trabajadores remotos que usan dispositivos no administrados (BYOD);
- Controlando y monitoreando sesiones a través de un agente seguro o usando protocolos estándar para conexiones RDP, VNC, Web y SSH.

Además, el Privileged Remote Access de BeyondTrust incluye una bóveda de contraseñas que garantiza que las cuentas administradas tengan sus contraseñas rotadas de forma regular. Para las cuentas más confidenciales, uno puede implementar contraseñas de un solo uso, lo que significa que cada vez que se usa una contraseña, se cambia a una nueva.

Permita que los profesionales de seguridad controlen, supervisen y administren el acceso a los sistemas críticos de todos los usuarios privilegiados, tanto internos como externos, con BeyondTrust.

Obtenga más información y vea una demo de nuestra solución Privileged Remote Access en

beyondtrust.com/remote-access

BeyondTrust es líder mundial en Gestión de Accesos Privilegiados (PAM), que permite a las empresas proteger y administrar todo su universo de privilegios. El enfoque de Gestión Universal de Privilegios de BeyondTrust asegura y protege los privilegios a través de contraseñas, endpoints y accesos, brindando a las organizaciones la visibilidad y el control que necesitan para reducir el riesgo, lograr el cumplimiento y aumentar el rendimiento operativo.

beyondtrust.com/es

2020_11_PRT