BeyondTrust

Habilite y Proteja su Fuerza de Trabajo Remota

Mantenga a los Empleados Remotos Productivos sin Sacrificar la Seguridad

INTRODUCCIÓN

Los departamentos de TI están bajo una presión increíble para mantener la productividad del negocio para una fuerza de trabajo remota expandida que es exponencialmente más grande que hace unas semanas.

Como muchos equipos de TI trabajan horas extras para permitir a los trabajadores remotos, mantener las prácticas de seguridad y el cumplimiento pueden no ser lo más importante, pero **los actores de amenazas buscan activamente oportunidades para beneficiarse de las circunstancias actuales.**

Si bien la habilitación de una fuerza de trabajo remota suele ser una práctica común, **se están aplicando algunas consideraciones particularmente urgentes** y únicas a las organizaciones y sus empleados durante la crisis del coronavirus.

Los atacantes son en gran parte oportunistas. **Los piratas informáticos buscan explotar empresas con grandes superficies de ataque debido a políticas de seguridad obsoletas o una menor adherencia a las mejores prácticas de seguridad durante esta crisis.**

No son solo las grandes. **Las pequeñas y medianas empresas (PYMES) y las organizaciones gubernamentales estatales y locales, como las escuelas, han sido las más afectadas por los brotes de malware y los ataques de ransomware en los últimos años.**

TABLA DE CONTENIDO

EL IMPACTO COVID-19

¿Cuáles son los desafíos más apremiantes para habilitar una fuerza de trabajo remota segura?

EL IT SERVICE DESK

¿Están equipados para manejar el pico?

VPN

¿Quién está en su red y qué están haciendo?

ACCESO REMOTO SIMPLIFICADO

Use cualquier plataforma o dispositivo personal

CIBER-HIGIENE

Las contraseñas son como gérmenes — ¡No las compartas!

GESTIÓN DE PRIVILEGIOS EN LOS TERMINALES

Proteja los terminales remotos de ataques y malware

EL TIEMPO ES AHORA

Habilite a los trabajadores remotos hoy

EL IMPACTO DE COVID-19

¿Cuáles son los desafíos más apremiantes para habilitar una fuerza de trabajo remota segura?

Muchas empresas se vieron obligadas a trabajar de manera remota en un período muy corto de tiempo. Algunos han podido proporcionar a los empleados computadoras emitidas por la compañía que están estrechamente administradas y bloqueadas, pero este no suele ser el caso.

Las siguientes prácticas relacionadas con el trabajo remoto crean riesgos:

Prácticas de creación de riesgos

- Flexibilizar la política BYOD (bring your own device)
- Realizar negocios personales en computadoras portátiles emitidas por empresas, como la educación en el hogar
- Uso de herramientas de acceso remoto inseguras u obsoletas para conectarse a la red
- Utilizando "VPN siempre activas" para todas las conexiones de usuarios, incluso cuando algunos usuarios solo necesitan acceso a aplicaciones y datos basados en la nube
- Apertura de correos electrónicos de phishing, que están en aumento debido a la pandemia
- Descargar software potencialmente malicioso, introduciendo malware en su entorno corporativo desde casa

Gartner recién publicó un estudio, "Solving the Challenges of Modern Remote Access,"* para ofrecer orientación a los líderes de seguridad y riesgo sobre los desafíos de escalar rápidamente el acceso remoto moderno a gran escala. Concluye que **la mayoría de las organizaciones solo tienen capacidad y licencias para manejar un pequeño subconjunto de usuarios y no están preparadas para permitir que todos los empleados trabajen a distancia durante eventos críticos a más largo plazo**, como COVID-19. Además, las organizaciones a menudo carecen del ancho de banda requerido para admitir a todos los usuarios que trabajan de forma remota de forma simultánea.

Gartner, "Solving the Challenges of Modern Remote Access", Rob Smith, Steve Riley, Nathan Hill, Jeremy D'Hoinne, 25 de marzo de 2020

Las malas prácticas de higiene de ciberseguridad, que pueden ser mejor administradas por los empleados durante un entorno empresarial más normalizado, pueden poner en riesgo a su organización, que incluye:

- Uso de conexiones a Internet inalámbricas inseguras
- Reutilizando o compartiendo contraseñas
- Dispositivo compartido
- Abrir correos electrónicos que contienen ransomware
- Almacenar contraseñas en ubicaciones no seguras o en notas adhesivas
- Descarga de software que podría contener malware

?

¿Cómo pueden las organizaciones habilitar a los trabajadores con herramientas seguras para mantener la continuidad del negocio y evitar ser víctimas de ataques cibernéticos?

EL IT SERVICE DESK

¿Están Equipados para Manejar el Pico?

LA PRESIÓN EN LOS EQUIPOS DE SOPORTE DE TI

Las políticas obligatorias de trabajo desde el hogar imponen inmensas demandas a la infraestructura y los sistemas de TI, a medida que los empleados recurren al trabajo remoto en masa. Esto tiene un gran impacto en los empleados de la mesa de servicio, que intentan habilitar y apoyar a los trabajadores remotos mientras trabajan desde casa. Las herramientas de soporte remoto efectivas impactan directamente el éxito del trabajo remoto. Estas soluciones deben escalar y adaptarse para cumplir con los rigurosos requisitos de seguridad y al mismo tiempo impulsar la productividad del técnico.

Además, la solución debe ser:

CASOS DE USO POTENCIALES

Las organizaciones necesitan una solución segura de acceso remoto que pueda cubrir una amplia lista de casos de uso, al tiempo que hace que toda la experiencia de la service desk sea más eficiente y segura. Algunos casos de uso comunes incluyen:

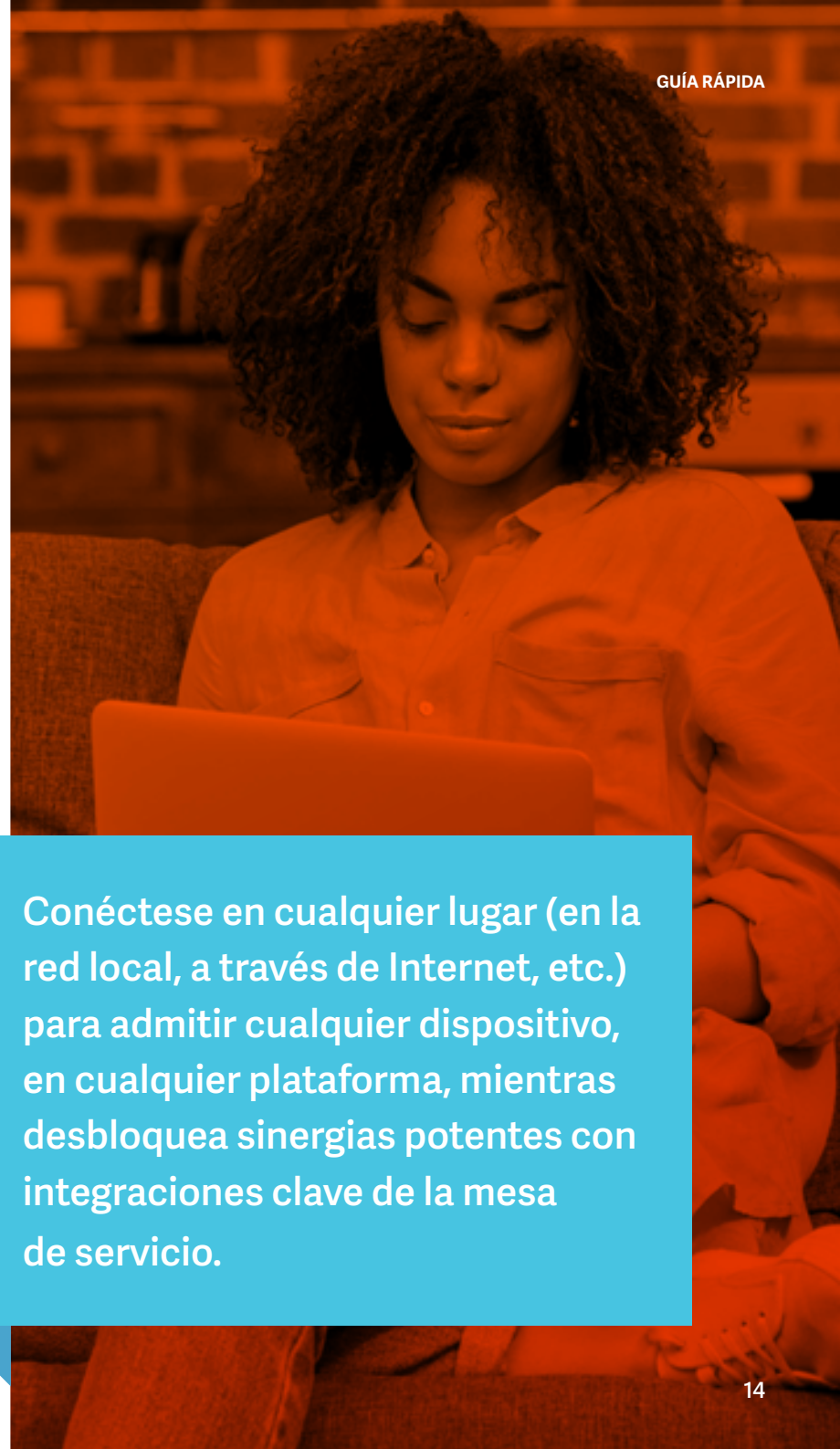
Durante estos tiempos difíciles, elegir el software de soporte remoto adecuado es fundamental para la productividad y la seguridad de su mesa de servicio.

SOPORTE CUALQUIER DISPOSITIVO O SISTEMA, EN CUALQUIER LUGAR

BeyondTrust Remote Support

Habilite el soporte remoto seguro y confiable para los empleados dentro y fuera de su red. Vea su pantalla, chatee, eleve privilegios y acceda a la cámara de su dispositivo móvil para solucionar problemas de periféricos. Admite dispositivos Windows, Mac, Linux, iOS, Android y de red con una única solución.

El "Remote Support" de Beyond Trust está diseñado para hacer que todo su servicio técnico funcione mejor. Nuestra solución cubre la gama más amplia de casos de uso de soporte remoto, al tiempo que ofrece la seguridad de acceso remoto más sólida disponible. BeyondTrust tiene la única solución de soporte remoto que cumple con los rigurosos requisitos de FIPS Nivel 2.



Conéctese en cualquier lugar (en la red local, a través de Internet, etc.) para admitir cualquier dispositivo, en cualquier plataforma, mientras desbloquea sinergias potentes con integraciones clave de la mesa de servicio.

VPN

¿Quién está en su red y qué están haciendo?

LAS CONEXIONES VPN

Ofrecer acceso remoto es obligatorio para casi todas las organizaciones. Los empleados deben poder acceder a sus sistemas desde fuera del firewall. Sin embargo, el acceso remoto, por su propia naturaleza, crea exposición a riesgos de ciberseguridad. Para establecer conexiones remotas para los empleados, las organizaciones a menudo usan alguna forma de Virtual Private Network (VPN) para permitir a los usuarios interactuar con sus sistemas. Las VPN funcionan bien cuando los empleados remotos tienen computadoras portátiles corporativas en casa. Pero para los empleados que se conectan a una computadora de escritorio corporativa desde una computadora portátil o dispositivo personal, o para los contratistas y proveedores que se conectan a sus sistemas, administrar y proteger las VPN presenta un desafío.

Riesgos de seguridad de VPN

- Las VPN permiten el acceso a la capa de red proporcionando más acceso del necesario
- Las VPN son difíciles de mantener y a menudo resultan en demasiado acceso y acceso "sobrante" cuando los hosts se eliminan o reemplazan
- Las VPN solo permiten el acceso "todo o nada" que está siempre activado sin niveles de acceso granulares

MITIGAR EL RIESGO DE VPN

Los hackers generalmente necesitan días o semanas para encontrar lo que buscan. Si los actores de amenazas obtienen acceso VPN de un sistema explotado a una red interna, a menudo pueden moverse sin ser detectados y usar técnicas de pivote para encontrar su objetivo final. Lo más probable es que los hackers apunten a trabajadores remotos o proveedores externos que usan dispositivos personales con acceso VPN sabiendo que pueden ser más fáciles de comprometer.

182

Número promedio de terceros proveedores * que los profesionales de TI informan que acceden a su red interna semanalmente.

Muchos de ellos tienen más privilegios con más acceso del requerido para sus roles.

*BeyondTrust, "Informe de Amenazas de Accesos Privilegiados de 2019"

BeyondTrust Privileged Remote Access

BeyondTrust "Privileged Remote Access" permite la administración segura de sesiones, con la capacidad de acceso proxy a RDP, SSH y hosts Windows / Unix / Linux, sin la necesidad una VPN. La asignación dinámica de privilegios just-in-time a través de flujos adaptativos de aprobación permitiendo a las organizaciones bloquear el acceso a los recursos según el día, la fecha, la hora y la ubicación. Por ejemplo, si espera que sus trabajadores remotos inicien sesión desde sistemas particulares, puede asegurarse de que el acceso solo se permita desde rangos de direcciones predefinidos. Del mismo modo, puede configurar políticas para controlar cuándo se puede acceder a las cuentas y alertar cuando se invocan políticas de acceso específicas.

El uso del BeyondTrust Privileged Remote Access junto con su VPN corporativa le permite a su organización reducir la superficie de ataques e impulsar la productividad **de las siguientes maneras:**

1. Aplique una política de privilegios mínimos al dar a ciertos usuarios el nivel de acceso correcto
2. Habilite la responsabilidad individual para las cuentas compartidas
3. Defina a qué puntos finales pueden acceder los usuarios y cuándo incluir en la lista blanca y en la lista negra las aplicaciones
4. Elimine la carga administrativa de configurar e instalar VPN para proveedores o trabajadores remotos que usan dispositivos personales
5. Controle y monitoree sesiones a través de un agente seguro o usando protocolos estándar para conexiones RDP, VNC, web y SSH

CONSIDERACIONES ADICIONALES

Rendimiento VPN

La mayoría de las implementaciones de VPN corporativas, incluso utilizadas con dispositivos emitidos por corporaciones, no están diseñadas para admitir que toda la empresa trabaje de forma remota. Permitir que ciertos usuarios, como proveedores o empleados de terceros en dispositivos domésticos, accedan a los sistemas a través del Privileged Remote Access puede ayudar a reducir la tensión en su VPN y aumentar el rendimiento.

Además de introducir problemas de seguridad en el entorno corporativo, el movimiento a las VPN en masa puede dar lugar a graves problemas de rendimiento de la red.

Riesgos de VPN a Gran Escala

- Las tecnologías VPN a menudo carecen de escalabilidad rápida, y cuando un número significativo de empleados o trabajadores externos de repente necesitan acceso, la solución puede no funcionar a un nivel aceptable
- Las VPN dependen en gran medida del ancho de banda disponible para el hogar del usuario que se conecta y de cuánto ancho de banda requiere la aplicación
- Las VPN generalmente no están configuradas para permitir el acceso a todos los recursos disponibles cuando alguien está físicamente sentado en una red confiable dentro de un edificio de oficinas

ACCESO REMOTO SIMPLIFICADO

Use cualquier plataforma o dispositivo personal

UN CAMINO SENCILLO PARA LOS USUARIOS

BeyondTrust Privileged Remote Access

Los empleados que dejaron sus computadoras de escritorio o portátiles en la oficina pueden aprovechar el BeyondTrust Privileged Remote Access para conectarse de forma segura a la estación de trabajo que usan todos los días. Pueden hacerlo desde una computadora personal o tableta usando solo un navegador web.

Si bien muchos trabajadores remotos usarán una computadora portátil emitida por la compañía, aquellos que no tienen acceso a una pueden estar usando cualquiera de los siguientes dispositivos para conectarse a su red:

BeyondTrust facilita a los trabajadores remotos el acceso a los recursos que necesitan para mantenerse productivos, utilizando dispositivos personales y emitidos por la empresa.

- **Empleados en dispositivos personales.**
- **Proveedores o contratistas que usan computadoras portátiles personales o de la empresa.**

Si bien los empleados en dispositivos emitidos por la compañía se consideran confiables, los otros trabajadores remotos representan un riesgo de seguridad significativo para su organización si están conectados a su VPN. Los piratas informáticos pueden utilizar estos dispositivos para infiltrarse en su red y establecer una presencia persistente.

Para todos estos escenarios, **BeyondTrust permite a los equipos de TI hacer lo siguiente:**

- Ofrecer acceso remoto granular basado en roles con autenticación de múltiples factores
- Proporcionar una ruta simple para que los usuarios remotos accedan de manera segura a los recursos de red, incluida una computadora que se deja en el trabajo, utilizando una consola web HTML5 sin configuraciones especiales
- Provisionar y desaprovisionar privilegios de usuario para empleados remotos que se conectan a su sistema

CIBER HIGIENE

Las contraseñas son como gérmenes — ¡No las compartas!

EL PAPEL DE LA GESTIÓN DE CONTRASEÑAS

Además de lavarse las manos para evitar compartir gérmenes con otros durante la crisis del coronavirus, los trabajadores remotos también deben dejar de compartir contraseñas. Las contraseñas que no se gestionan o controlan adecuadamente representan un riesgo de seguridad significativo para las organizaciones. Los usuarios tienen demasiadas contraseñas. Como resultado, muchos empleados a menudo comparten, reutilizan o almacenan contraseñas de forma insegura. Estos hábitos crean amenazas importantes que hacen que sus sistemas sean vulnerables a los ataques.

Cuando los empleados tienen problemas para recordar contraseñas, a menudo recurren a:

Al considerar las soluciones de acceso remoto, la integración con una bóveda de contraseñas es otro factor clave.

Hábitos de contraseña incorrecta que crean riesgo

- Escribir sus contraseñas
- Olvidar sus contraseñas
- Elegir contraseñas muy simples y fácilmente comprometidas o reutilizar contraseñas antiguas

PROTEGER CREDENCIALES PRIVILEGIADAS

BeyondTrust Vault (Bóveda de credenciales)

Incluido con el Privileged Remote Access y el Remote Support, BeyondTrust Vault unifica la administración de sesión integral y el almacenamiento de credenciales esenciales para usuarios privilegiados internos y de terceros con una solución simple y rápida basada en la nube.

BeyondTrust Password Safe

Para funcionalidades más avanzadas de Password Management ,BeyondTrust Password Safe combina contraseña privilegiada y administración de sesión para descubrir, administrar y auditar todas las actividades de credenciales privilegiadas. Password Safe lo ayuda a proteger cuentas de usuario privilegiadas, aplicaciones, claves SSH, cuentas de administrador en la nube, cuentas RPA y más, con un seguimiento de auditoría de búsqueda para cumplimiento y análisis forense.

Obtenga flexibilidad para proteger y controlar la administración de credenciales privilegiadas y el monitoreo de sesiones con modelos que se adaptan a sus necesidades comerciales específicas.

GESTIÓN DE PRIVILEGIOS EN LOS TERMINALES

Proteja los terminales remotos de ataques y malware

El cambio abrupto a gran escala al trabajo remoto no solo ha interrumpido los flujos y procesos de trabajo normales del usuario final, sino que también ha causado estragos en los procesos y políticas de seguridad. Muchas organizaciones no están preparadas adecuadamente para admitir fuerzas de trabajo totalmente remotas, pero la continuidad del negocio requiere que encuentren una manera de hacerlo funcionar.

Los trabajadores que se encuentran repentinamente obligados a trabajar de forma remota, pueden enfrentar estos desafíos:

- Desplazado de sus entornos normales
- Desconectado de la red corporativa segura
- Expuesto al riesgo de amenazas externas e internas
- Se espera que de repente use nuevas tecnologías para mantenerse conectado y ser productivo

Como resultado, estos empleados confían en el Service Desk para hacer más. Si sienten que no están obteniendo lo que necesitan de TI, o simplemente quieren intentar resolverlo por sí mismos, estos trabajadores a menudo aprovisionarán las herramientas y aplicaciones, lo que creará aún más riesgos de seguridad.

Los usuarios no tienen derechos de administrador y no pueden hacer nada en absoluto o tienen derechos de administrador completos y demasiado control.

ASEGURAR LA SEGURIDAD Y LA PRODUCTIVIDAD

Con el aumento de los ataques cibernéticos contra los trabajadores remotos, es imperativo que las organizaciones aseguren las máquinas de los usuarios finales y eviten que se introduzca malware y ransomware en su entorno corporativo.

Las soluciones BeyondTrust de gestión de privilegios en los terminales imponen el menor privilegio en todos los escritorios y servidores, permitiendo el nivel exacto de acceso privilegiado que necesitan los usuarios finales, al tiempo que evitan la introducción de malware y ransomware en su red corporativa. Esto permite a los usuarios realizar actividades cotidianas, como instalar y actualizar aplicaciones e impresoras, cámaras, etc. aprobadas, sin otorgarles derechos administrativos completos y sin abrumar al servicio técnico.

Evite los ataques perdidos por el software antivirus eliminando los derechos de administrador, implementando el menor privilegio, habilitando la elevación de privilegios y asegurando las aplicaciones con protección total de la aplicación.

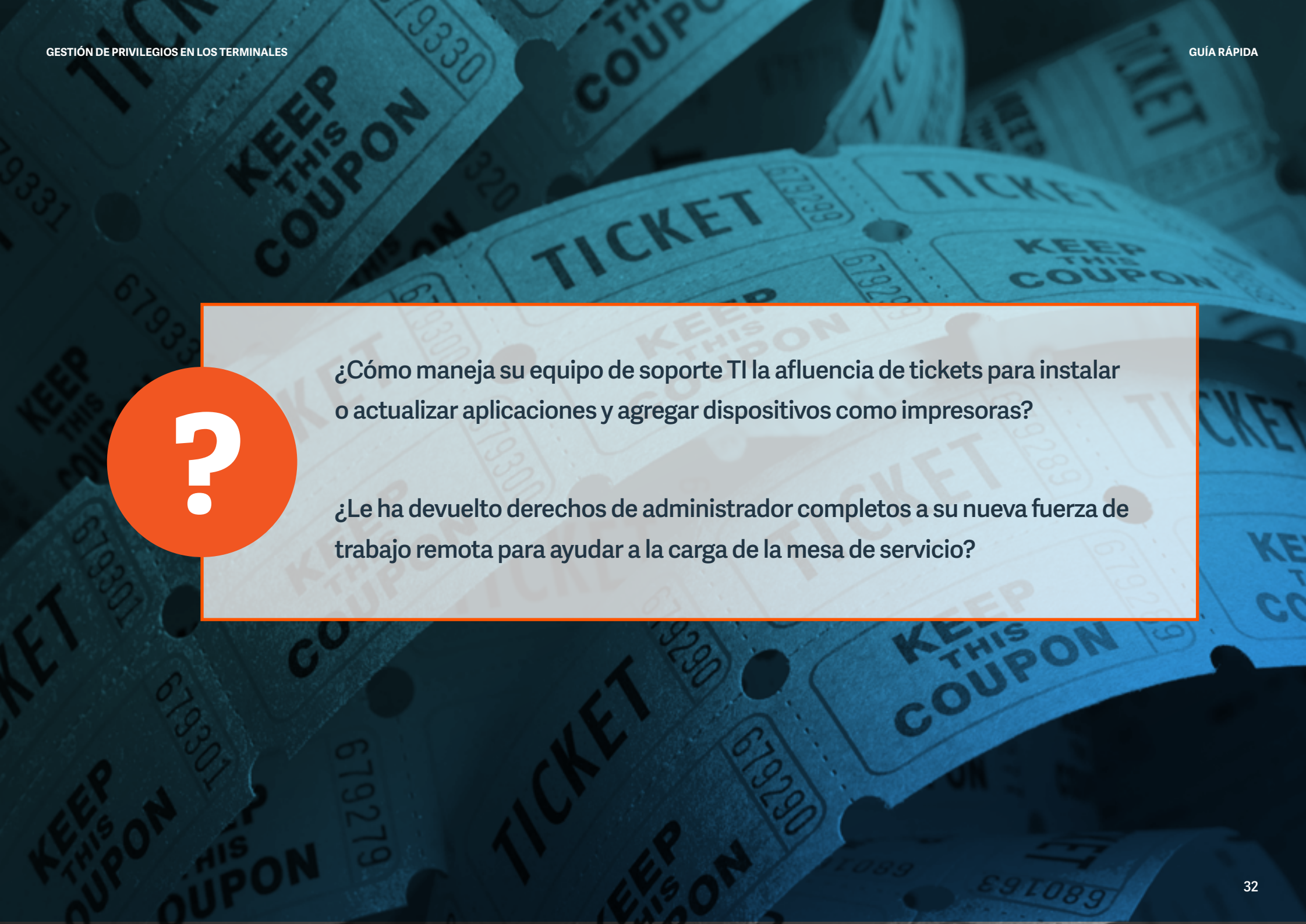
Con Endpoint Privilege Management, las organizaciones pueden implementar rápidamente políticas en todos los usuarios o grupos de usuarios. Además, nuestras políticas únicas de inicio rápido que aprovechan los datos de miles de implementaciones, permiten a los administradores de TI implementar plantillas de estilo de trabajo flexibles y ponerlas en funcionamiento rápidamente.

Con implementaciones globales que abarcan más de 50 millones de puntos finales y una miríada de industrias, nuestra experiencia ha ayudado a crear un enfoque probado que proporciona un tiempo de valor inigualable en toda la industria.

“Mis clientes más grandes han medido una reducción del 75% en la cantidad de tickets de la mesa de servicio después de eliminar los derechos de administrador.”

*- Sami Laiho, MVP de Microsoft y pirata informático ético **

**BeyondTrust, "Informe de vulnerabilidades de Microsoft 2020"*



?

¿Cómo maneja su equipo de soporte TI la afluencia de tickets para instalar o actualizar aplicaciones y agregar dispositivos como impresoras?

¿Le ha devuelto derechos de administrador completos a su nueva fuerza de trabajo remota para ayudar a la carga de la mesa de servicio?

REDUCCION DEL ALTO VOLUMEN DE REQUERIMIENTOS DE TI

BeyondTrust Privilege Management para Windows y Mac

Elimine privilegios innecesarios y eleve los derechos para los usuarios de Windows y Mac sin obstaculizar la productividad. Hemos combinado la mejor gestión de privilegios y control de aplicaciones en su clase, haciendo que la eliminación de derechos de administrador sea simple para garantizar el cumplimiento, la seguridad y la eficiencia.

Las características y beneficios incluyen:

- Desviar los tickets de la mesa de servicio y capacitar a los usuarios para que instalen y ejecuten sus propias aplicaciones aprobadas previamente, con políticas listas para usar
- Otorgar a los usuarios derechos de elevación ad hoc para instalar solo aplicaciones aprobadas / seguras
- Integrarse con ServiceNow y otras herramientas de ITSM para automatizar el envío de un ticket al servicio de asistencia, de modo que puedan tomar una decisión informada y expedita sobre la solicitud del usuario de ejecutar una aplicación, instalación, script o tarea
- Solución rápida de un problema una vez, para todos los usuarios, a través de amplias actualizaciones de políticas
- Empoderar a los usuarios para autoinstalar impresoras y otro hardware aceptado

?

¿Cómo puede evitar que los usuarios introduzcan malware y ransomware en su entorno?

BeyondTrust Privilege Management para Windows y Mac reduce la superficie de ataque de las siguientes maneras:

1. Haciendo cumplir los mínimos privilegios en el entorno de escritorio, así como en los servidores, manteniendo la seguridad, la productividad del usuario y la eficiencia operativa
2. Detenendo los ataques que involucran aplicaciones confiables, capturar scripts malos y archivos adjuntos de correo electrónico infectados en tiempo real
3. Usando una lista blanca automatizada y un elegante manejo de excepciones para proporcionar un control completo sobre lo que los usuarios pueden instalar o ejecutar
4. Proporcionando una única pista de auditoría de toda la actividad del usuario para agilizar el análisis forense y simplificar el cumplimiento
5. Correlacionando el comportamiento del usuario con los datos de vulnerabilidad de activos y la inteligencia de seguridad para evaluar el riesgo del usuario final con análisis de amenazas avanzados

EL TIEMPO ES AHORA

Habilite a los trabajadores remotos hoy

IMPLEMENTACIÓN SIMPLE Y DE MANERA RÁPIDA

Las soluciones BeyondTrust están disponibles en múltiples opciones de implementación, incluidos dispositivos virtuales y SaaS, que pueden estar en funcionamiento muy rápidamente. Con las soluciones de acceso remoto seguro de BeyondTrust, no se requieren descargas de agentes de escritorio; los usuarios pueden iniciar sesión a través de una consola web desde cualquier navegador. Para Endpoint Privilege Management (EPM), los agentes se implementan rápidamente en los puntos finales, con políticas aplicadas, sin interrupción para los usuarios.

La administración simplificada y los flujos de trabajo simplificados o automatizados también alivian la carga de sus equipos de TI. Los siguientes son los beneficios del uso de las soluciones de BeyondTrust:

LOS BENEFICIOS

Vías de acceso consolidadas	Seguimiento y trazabilidad del acceso	Aplicaciones móviles	Auditoría	Políticas de inicio rápido (EPM)
Intermedia todas las conexiones a través de una única vía de acceso, reduce la superficie de ataque y proporciona una lista única de puntos finales autorizados disponibles para cada usuario	Establezca las preferencias para recibir alertas cuando un proveedor / usuario privilegiado esté accediendo a su red / sistemas, o cuando ocurra una sesión iniciada por acceso remoto	Los administradores pueden usar sus dispositivos móviles para aprobar solicitudes y monitorear el uso de acceso desde cualquier lugar	Registre todas las sesiones para satisfacer los requisitos de cumplimiento y para su uso en sesiones forenses y otras necesidades de informes	Mantenga la seguridad, la productividad del usuario y la eficiencia operativa de TI mediante la aplicación de menos privilegios en el entorno de escritorio

BeyondTrust permite a las organizaciones aplicar controles de auditoría con privilegios mínimos y robustos a todos los accesos remotos requeridos por empleados, proveedores y service desks. Los usuarios pueden acceder de forma rápida y segura a cualquier sistema remoto, ejecutar cualquier plataforma, ubicarse en cualquier lugar, y aprovechar una bóveda de contraseñas integrada para descubrir, incorporar y administrar credenciales privilegiadas.

Obtenga visibilidad y control absolutos sobre el acceso remoto interno y externo, conectividad segura a los activos administrados y cree una pista de auditoría completa e impecable que simplifique su camino hacia el cumplimiento.

Además, evite que los usuarios descarguen software malicioso y abran archivos adjuntos de phishing peligrosos que podrían provocar daños abrumadores en su entorno corporativo.

Todo mientras reduce la afluencia de tickets de la mesa de servicio y continúa cumpliendo con las regulaciones de cumplimiento.

Nuestro enfoque crea una experiencia sin fricción para los usuarios, permitiendo el nivel correcto de acceso en el momento justo.

BeyondTrust

ACERCA DE BEYONDTRUST

BeyondTrust es el líder mundial en Privileged Access Management (PAM), capacitando a las organizaciones para asegurar y administrar todo su universo de privilegios. Nuestros productos y plataforma integrados ofrecen la solución PAM más avanzada de la industria, lo que permite a las organizaciones reducir rápidamente su superficie de ataque en entornos tradicionales, en la nube e híbridos.

El enfoque de BeyondTrust Universal Privilege Management asegura y protege los privilegios en contraseñas, puntos finales y acceso, brindando a las organizaciones la visibilidad y el control que necesitan para reducir el riesgo, lograr el cumplimiento y aumentar el rendimiento operativo. 20,000 clientes confían en nosotros, incluido el 70 por ciento de Fortune 500, y una red global de socios.

Obtenga más información en beyondtrust.com/es/remote-workers