Microsoft

Tres maneras en que puede garantizar un trabajo remoto seguro y productivo

A medida que el trabajo remoto se vuelve cada vez más común, es necesario empoderar a los empleados para que sean productivos desde cualquier lugar. Al mismo tiempo, no se puede comprometer la seguridad. Estos objetivos son complementarios: el trabajo seguro es trabajo productivo. Con el enfoque tecnológico adecuado, puede proteger datos, dispositivos y aplicaciones, minimizar el impacto de la seguridad en los empleados y simplificar la TI.

Desafíos del trabajo remoto seguro

1. Acceso remoto a las aplicaciones

El acceso a aplicaciones basadas en VPN implica confianza en función del lugar donde se encuentra y puede afectar negativamente tanto la seguridad como la productividad.

¿Cómo puede ofrecer un acceso sin problemas a la vez que mantiene altos niveles de protección?

2. Administración de dispositivos y aplicaciones

Para los trabajadores remotos es necesario poder ser productivos en diversos dispositivos. Sin embargo, TI necesita tener visibilidad de las aplicaciones que se están usando y tener control sobre los datos confidenciales.

¿Cómo se puede simplificar la administración de ecosistemas de dispositivos y aplicaciones complejos?

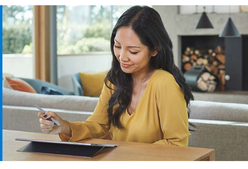
3. Protección de los datos

Con los trabajadores teniendo acceso a aplicaciones y datos de forma remota, los tradicionales métodos de seguridad basados en el perímetro no son los más adecuados.

¿Cómo puede proteger los recursos corporativos en cualquier lugar?

1 Permita el acceso remoto a las aplicaciones

Elimine la complejidad del acceso basado en VPN para proporcionar las herramientas que los empleados necesitan con una seguridad sólida y un alto rendimiento.



Comodidad y seguridad en un inicio de sesión único

Azure Active Directory (Azure AD)

Ofrezca acceso altamente seguro y con un clic a las aplicaciones, ya sea localmente o en la nube.

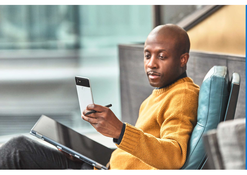
- Una identidad, miles de aplicaciones
- No se requiere VPN
- Funciona en todos los dispositivos

Seguridad inteligente que se adapta

Acceso condicional de Azure AD

Nunca confíe, siempre verifique. El acceso condicional aplica automáticamente el nivel de control adecuado en función del contexto, usando la información sobre el dispositivo, la ubicación, el rol del usuario, el riesgo y más.

Ubicación de inicio de sesión inusual → Problema de autenticación multifactor → ID de usuario confirmada / Inicio de sesión bloqueado



2 Administre dispositivos y aplicaciones

Desde equipos corporativos tradicionales hasta dispositivos móviles que se conectan a través de la nube, las soluciones modernas unifican la seguridad y administración para simplificar el soporte para los trabajadores remotos.

Unifique la administración de dispositivos

Microsoft Endpoint Manager

Reúna soluciones de administración de equipos locales tradicionales con herramientas en la nube avanzadas con tecnología de IA en una solución.

Endpoint Manager = Intune + System Center Configuration Manager

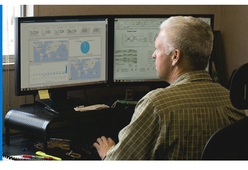
Proteja los datos en cualquier dispositivo

Garantice la productividad continua al proteger los datos corporativos tanto en dispositivos administrados como personales.

Microsoft Intune verifica el cumplimiento del dispositivo → Azure AD aplica la directiva de acceso condicional en función del estado del dispositivo → Solo los dispositivos que cumplan pueden tener acceso a las aplicaciones y los servicios

3 Proteja los recursos corporativos

Empodere a los usuarios para que tengan acceso a datos críticos para el negocio sin aumentar el riesgo de seguridad.



Descubra, administre y proteja sus datos confidenciales dondequiera que vaya

Microsoft Information Protection

En → Dispositivos, Servicios en la nube, Aplicaciones, Entorno local

Tome medidas como → Marcar, Restringir, Cifrar, Analizar

Descubra y controle el acceso a sus aplicaciones en la nube

Microsoft Cloud App Security

- Identifique qué aplicaciones están usando los empleados
- Evalúe los niveles de riesgo y el cumplimiento
- Detecte comportamientos inusuales en las aplicaciones en la nube

Proteja los recursos corporativos

Protección contra amenazas avanzada de Microsoft Defender + Protección contra amenazas avanzada de Office 365

- Descubra y corrija las vulnerabilidades y los errores de configuración en el punto de conexión
- Reduzca la superficie de ataque para fortalecer sus sistemas y regular el acceso a IP, dominios y URL potencialmente maliciosos
- Automatice el proceso de investigación y corrección de amenazas
- Proteja a los usuarios contra los ataques de suplantación de identidad (phishing) y malware

Empodere a los empleados para que sean productivos en cualquier lugar

Un lugar de trabajo eficaz y moderno requiere de un acceso remoto a las aplicaciones y los datos que sea altamente seguro y de alto rendimiento en todos los dispositivos y ubicaciones. Microsoft ofrece un conjunto completo de herramientas y soluciones que permiten la productividad en cualquier lugar.

Obtenga más información acerca de las soluciones de trabajo remoto seguro ›

Microsoft

© 2020 Microsoft Corporation. Todos los derechos reservados. Este documento se proporciona "tal cual". La información y las opiniones expresadas en este documento, incluidas las direcciones URL y otras referencias a sitios web de Internet, están sujetas a cambios sin previo aviso. Usted asume el riesgo de utilizarlo. Este documento no le otorga derecho legal alguno a ningún aspecto de propiedad intelectual de ninguno de los productos de Microsoft. Puede copiar y usar este documento para uso interno como referencia.