Windows 11 Pro

Cuaderno de estrategias de seguridad completo para las áreas de trabajo híbridas

La ciberseguridad es una prioridad El 88 % de las pymes encuestadas consideran que no está prepa-radas para hacer frente a las ciberamenazas.[1]

Aquí encontrarás algunas de las maneras con las que una infraestructura de TI segura y preparada para el futuro ayuda a proteger tu empresa contra ciberamenazas

Aplica un método de confianza cero

El modelo de seguridad de Confianza cero reduce los riesgos al verificar puntos de datos, como identidad de usuario, ubicación y estado del sistema, para cada solicitud de acceso, sin excepciones. Cuando se verifican, los usuarios y dispositivos tienen acceso limitado y solo a los recursos necesarios.

Los principios de Confianza cero tienen tres aspectos:

1 En primer lugar, verificar explícitamente. Esto significa autenticar y autorizar siempre según todos los puntos de datos disponibles, como la identidad de usuario, la ubicación, el estado del dispositivo, el servicio o carga de trabajo, la clasificación de los datos y las anomalías.

2 En segundo lugar, usar el acceso con el menor nivel de privilegios, que limitan el acceso de los usuarios con acceso cuando es necesario y que sea solo lo suficiente, directivas adaptables basadas en riesgos y protección de datos para ayudar a proteger tanto los datos como la productividad.

3 En tercer lugar, suponer la aparición de vulneraciones. Suponer la aparición de vulneraciones funciona de forma que minimiza el radio de alcance y segmenta el acceso. Verificar el cifrado de un extremo a otro y usar análisis para obtener visibilidad y mejorar la detección de amenazas y defensas.

Para implementar un método de Confianza cero, las organizaciones deben comprender sus propios datos y dónde residen estos.

Las empresas deben conocer el nivel de confidencialidad de los datos y los riesgos potenciales de exposición para determinar dónde se debe aplicar la Confianza cero. Para almacenamiento y aplicaciones basadas en la nube, como servicios de correo electrónico y almacenamiento de datos en la nube, establecer un entorno de Confianza cero tiene sentido y es fundamental para mitigar los riesgos. Sin este método, las contraseñas, los dispositivos y los datos confidenciales de la empresa corren riesgo de sufrir ataques.

Implementar métodos de autenticación avanzados

Una vulneración de seguridad se hace más probable si se ponen en riesgo los métodos de autenticación de usuario. Un acceso no autorizado al dispositivo de un usuario con frecuencia da acceso a un posible malhechor a toda la red de una organización. Implementar una manera segura de controlar que los usuarios son quienes dicen ser es fundamental en el entorno de trabajo híbrido de hoy en día. La autenticación multifactor puede contribuir en gran medida a crear un entorno más seguro. Las contraseñas ya no son suficientes para mitigar amenazas cada vez más sofisticadas, ya que con frecuencia se pueden poner en riesgo fácilmente. Las técnicas como la autenticación en dos fases, en combinación con las capacidades biométricas disponibles en muchos dispositivos modernos, como Windows Hello para empresas, son mucho más eficaces a la hora de proteger las organizaciones y sus redes contra ciberataques, especialmente cuando se fortalecen con una estrategia de seguridad de Confianza cero.

Fortalecer la seguridad por hardware

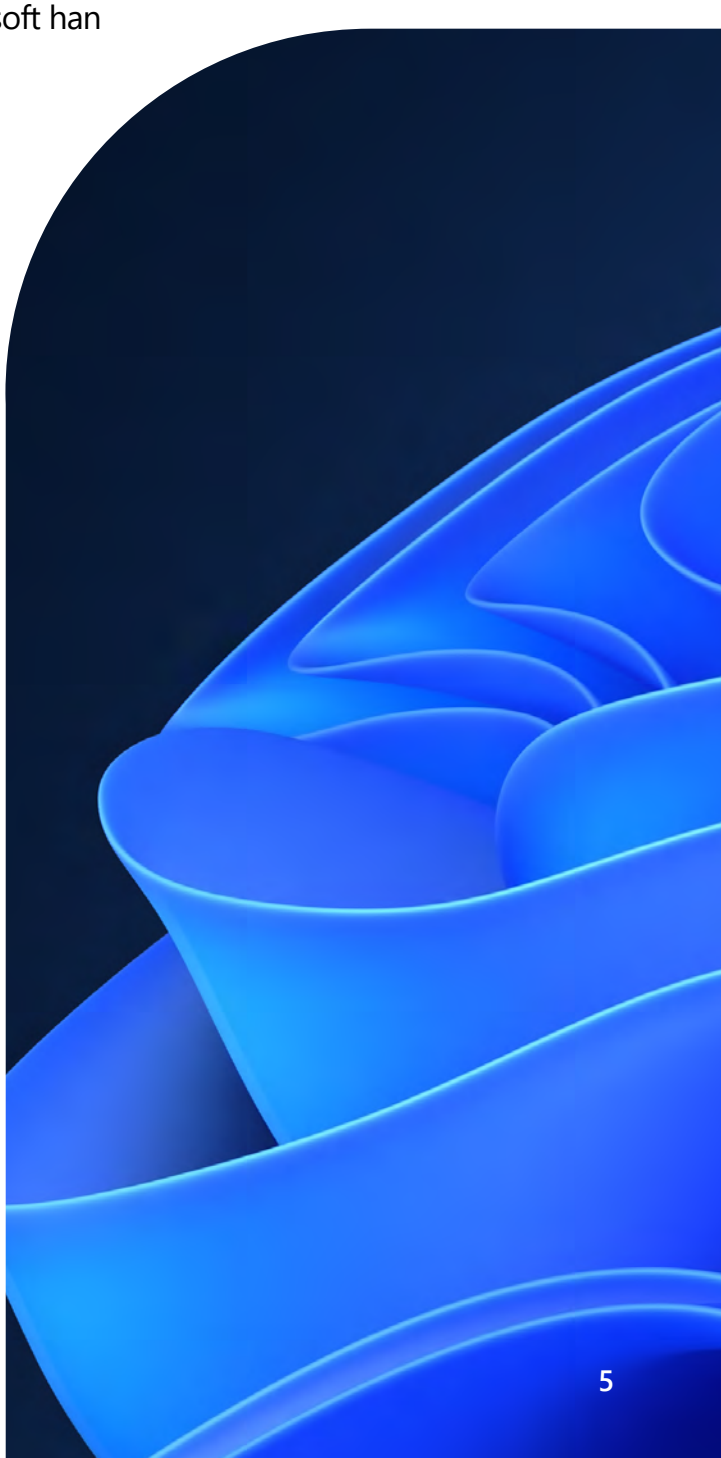
No se debe depender del sistema operativo solo para proteger contra una gran variedad de herramientas y técnicas que los ciberdelincuentes pueden usar para poner en riesgo a un equipo. Los intrusos, una vez que hayan obtenido acceso, pueden implementar malware difícil de eliminar en el firmware del dispositivo, o pueden robar datos confidenciales y credenciales importantes. Puede resultar difícil detectar estos intrusos una vez que hayan obtenido acceso. Debe haber una fuerte alineación entre la seguridad por hardware y las aplicaciones de seguridad basada en software. Las amenazas modernas requieren de hardware informático que sea seguro en el nivel de chip y procesador, protegiendo a la información confidencial de la empresa allí donde se almacena. Hay clases completas de vulnerabilidades que se pueden invalidar simplemente con capacidades de seguridad integradas en el nivel de hardware.

Dichas capacidades se pueden encontrar en todos los PC Windows 11 con núcleo protegido, por ejemplo. Además, se pueden lograr importantes mejoras de rendimiento en comparación con la implementación de capacidades de seguridad similares solo con software. Esto aumenta la posición de seguridad general del sistema, sin sacrificar el rendimiento del sistema.

Usar controles de acceso para la protección basada en identidad

En la nube, los administradores pueden controlar y administrar las identidades y acceder desde un solo lugar. Por ejemplo, con Microsoft Azure Active Directory (Azure AD), pueden administrar de manera centralizada las identidades del personal, así como configurar e implementar directivas para acceder a aplicaciones, sitios y grupos. Los administradores pueden incorporar requisitos de cumplimiento y las nuevas reglas se pueden incorporar a medida que surjan.

Los controles basados en la nube aumentan la seguridad y fortalecen el cumplimiento normativo. Las investigaciones de Microsoft han revelado que la autenticación multifactor sola puede bloquear más del 99,9 % de los ataques de puesta en riesgo de la cuenta.[2] El acceso condicional permite a los administradores crear reglas basadas en la actividad o ubicación, lo que reduce aún más la oportunidad para que los atacantes aprovechen las vulnerabilidades. Por ejemplo, los intentos de inicio de sesión provenientes de fuera del país o que llegan a hora extrañas se pueden rechazar. Además, los administradores pueden habilitar el inicio de sesión único, que permite a los usuarios acceder de forma seguro a las aplicaciones desde cualquier lugar, a la vez que facilita la administración de contraseñas para el departamento de TI.



Recientemente Microsoft presentó la disponibilidad general del soporte técnico de seguridad multinube. Ahora, las empresas pueden incorporar recursos multinube en Azure Security Center, como Google Cloud Platform (GCP) y Amazon Web Services (AWS), así como proteger los servidores con Azure Defender para servidores en Azure Arc.

Proteger dispositivos remotos

La nube de Microsoft facilita la administración de los dispositivos y aplicaciones. Por ejemplo, con Microsoft Intune, la implementación de dispositivos se puede administrar de forma segura y remota, mientras que las aplicaciones se pueden escalar para responder a la demanda.

Microsoft Windows Autopilot utiliza la configuración de seguridad y otros controles para ayudar a proteger los dispositivos antes de que un empleado se conecte a cualquier recurso.

Aplicaciones seguras

Consigue mayor protección contra orígenes que no sean de confianza al abrir archivos y sitios web en un contenedor aislado con Protección de aplicaciones de Microsoft Defender. El diseño con prioridad en la nube facilita la extensibilidad con Microsoft 365, Microsoft Defender for Cloud y Microsoft Defender para puntos de conexión.[3]

Simplifica la administración de la seguridad entre distintas ubicaciones y extiende la seguridad hacia la nube. Ayuda a proteger dispositivos, datos, aplicaciones e identidades en cualquier lugar. Implementa con confianza, sabiendo que el 99,6 % de las aplicaciones son compatibles con Windows 11.[4]

Automatizar el mantenimiento de la seguridad

Las tecnologías basadas en la nube permiten a los administradores de TI aplicar actualizaciones, parches y copias de seguridad entre varios sistemas y dispositivos, todo de forma automática. De este modo, se reducen los errores de configuración y se limitan los tiempos de inactividad a la vez que se protegen los sistemas contra nuevas amenazas. Se pueden automatizar las tareas rutinarias, lo que permite a los administradores dedicar su tiempo en tareas importantes que realmente necesitan de sus conocimientos.

Protege tu empresa con dispositivos Windows 11 Pro

Transformar la posición de seguridad de tu organización debería ser una prioridad, y proporcionar a tu personal dispositivos seguros es el pilar del éxito. Los nuevos dispositivos Windows 11 Pro, en combinación con Microsoft 365, están diseñados para el trabajo en entornos híbridos.

- Protege a tus empleados contra malware, virus, intentos de suplantación de identidad (phishing) y vínculos malintencionados, y ayuda a proteger los datos críticos para la empresa.
- Obtén capas de seguridad potente entre dispositivos, datos, identidades, aplicaciones y la nube.
- Simplifica la TI con herramientas unificadas y basadas en la nube para la administración de puntos de conexión, como Microsoft Endpoint Manager, Azure Active Directory y Windows Autopilot. Establece y aplica directivas de TI, administra apps e identidades, e implementa fácilmente dispositivos listos para la empresa.
- Supera los obstáculos relacionados con la colaboración mediante una solución única que incluye videoconferencias, apps de productividad, uso compartido de archivos y mucho más. Asegúrate de que tus empleados tengan acceso seguro a aplicaciones e información críticas del trabajo con una solución de colaboración unificada.
- Para las personas que trabajan en sectores o escenarios empresariales en los que se tratan datos confidenciales, los PC con núcleo protegido son los dispositivos Windows más seguros y se ofrecen con todas las características de seguridad avanzada de Windows 11 habilitadas.

Reduce significativamente los riesgos de ciberataques al reemplazar los PC más antiguos con nuevos dispositivos modernos optimizados para la seguridad y el trabajo en entornos híbridos. Windows 11 Pro y Microsoft 365 unen hardware y software para ofrecer protección potente, desde el primer instante, que protegen tus dispositivos, datos, aplicaciones, identidades y servicios.

Windows 11 Pro

[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Se vende por separado.*

[4] *Datos del programa Asesoría de aplicaciones de octubre de 2018 hasta febrero de 2022. Desde 2018, el programa Asesoría de aplicaciones ha trabajado con miles de clientes y evaluó más de 1,1 millones de apps, con una compatibilidad de aplicaciones del 99,6 %. Para más información, visita el sitio web de Asesoría de aplicaciones y la entrada del Windows IT*