ManageEngine
Device Control Plus

Los DIEZ MANDAMIENTOS

de la seguridad de los periféricos

Los dispositivos USB son pequeños pero poderosos en la era cibernética actual. Incluso cuando adoptan nuestras formas favoritas, como personajes de dibujos animados, divertidos emojis, frutas exóticas o, a veces, con lucecitas ¡no es ningún secreto que los USB son pequeños diablillos! Además de transferir datos, los dispositivos periféricos pueden facilitar la filtración de datos a través de las vulnerabilidades físicas de nuestros ordenadores: los puertos. Echando más leña al fuego, se han hecho grandes avances para perfeccionar los dispositivos periféricos con el fin de brindar mayor seguridad.

He aquí diez reglas divinas: los mandamientos de la seguridad de los dispositivos periféricos para salvaguardar la red de su empresa. También hablaremos de cómo puede aprovechar nuestra solución dedicada de control y gestión de dispositivos periféricos, Device Control Plus, para cada uno de los mandamientos

I No permitirás la entrada de periféricos no autorizados en tu organización

Un malware infectado USB, microcontroladores programados para robar PII de clientes y un rootkit que puede controlar remotamente puntos finales son algunas cosas que definitivamente no quieres cerca de tu organización. Device Control Plus puede actuar como guardián, moderando la entrada de dispositivos periféricos, permitiendo los buenos y rechazando los malo

II Deberás configurar la política adecuada para supervisar y gobernar los dispositivos periféricos.

Una política de control de dispositivos periféricos adaptada a tu organización es clave para establecer un ecosistema de Zero Trust. Pero un enfoque de talla única no es una estrategia de seguridad ideal, ya que la autoridad y los requisitos de cada usuario son diferentes. En su lugar, Device Control Plus puede desplegar políticas específicas para cada grupo de usuarios.

III Grupo de dispositivos periféricos de confianza.

La eliminación completa de los dispositivos periféricos puede hacer más mal que bien, ya que estos dispositivos son cruciales para la transferencia de datos. Las organizaciones a menudo son víctimas de a través de dispositivos periféricos y pagan cuantiosas sumas en virtud de la estricta legislación actual en materia de ciberseguridad. Crear una lista de dispositivos periféricos autorizados es imprescindible. La lista de dispositivos de confianza es la versión de Device Control Plus de reunir esta lista para proporcionar acceso

IV Vigilarás todas las solicitudes de acceso temporal y concederás el acceso únicamente a los justos.

La excepción que confirma la regla: la lista de dispositivos de confianza. Limitar el acceso utilizando únicamente la lista de dispositivos de confianza no es una opción práctica teniendo en cuenta el número de dispositivos de una empresa. Algunas situaciones pueden requerir que los usuarios soliciten acceso temporal a dispositivos periféricos que no están en la lista de dispositivos de confianza durante un periodo específico. Device Control Plus proporciona una plataforma para que los usuarios realicen estas solicitudes, y el administrador puede concederlas o denegarlas tras analizar la intención.

V Estarás atento a la presencia de dispositivos no autorizados.

No tengas piedad de los dispositivos periféricos. Bloquear estos dispositivos por defecto puede ayudar a mantener los riesgos. Con Device Control Plus, puedes crear una lista de dispositivos que bloquear, pero cualquier dispositivo que no esté incluido en la política bloqueará automáticamente para garantizar la seguridad de los dispositivos.

VI Tratarás el expediente de organización como un bien preciado.

Dado que los datos son la moneda de cambio de la nueva era, deben tratarse como un activo valioso en su empresa. Proporcionar acceso total a los archivos a todos los empleados acabará provocando un desastre, y la multitud de dispositivos periféricos que hay que gestionar y supervisar no hace sino aumentar la probabilidad de que se produzca un accidente o una amenaza interna. La gestión del acceso a los archivos es el proceso de regular quién puede hacer qué y cuándo. Establece un sistema sólido para gestionar el acceso a archivos a través de dispositivos periféricos utilizando Device Control Plus.

VII Dominarás la transferencia de archivos.

Los ataques internos son el segundo tipo de ciberataque de más rápido crecimiento, con un desastroso aumento del 15% a partir de 2022. Un control deficiente de la transferencia de archivos es el quid de un ataque interno. Device Control Plus te permite establecer límites claramente definidos para la transferencia de datos a través de dispositivos periféricos. Permite la transferencia de archivos en función del tipo, tamaño y extensión del archivo, y establece un límite de transferencia de archivos.

VIII Siempre asignarás un guerrero en la sombra.

Una vez que un archivo sale de la red de tu empresa, está sujeto a mayores niveles de riesgo. El contenido puede modificarse, copiarse o caer en las manos equivocadas. Para ir sobre seguro, recuerda siempre activar shadow copy. Una copia del archivo original se almacenará en una ubicación segura cada vez que se copie o modifique con dispositivos periféricos.

IX Aprovecharás el poder de los informes.

El arsenal de toda empresa debe estar repleto de potentes informes y perspectivas para dar marcha atrás en caso de accidente o percance. Las auditorías meticulosas y los informes disponibles al alcance de la mano pueden hacer algo más que dar marcha atrás; también pueden ayudar a detectar de forma proactiva acciones sospechosas que indiquen un ataque. Device Control Plus ofrece informes y auditorías muy informativos con opciones de personalización.

X ¡Confiarás en tus usuarios!

En ciberseguridad, la confianza da poder. Adopte una cultura de zero-blame en la notificación de incidentes. Nutre al usuario dando prioridad a la educación sobre las repercusiones de la ciberseguridad. Juntos podemos reforzar la cultura de la seguridad, fomentar comportamientos responsables y responder rápidamente a las amenazas. La confianza refuerza la resistencia frente a las ciberamenazas en evolución.

Siempre es prudente tener una solución a mano. Device Control Plus, la solución de dominio de dispositivos periféricos de ManageEngine, satisface todas tus necesidades.

Comienza aquí