ADVANTECH

Enabling an Intelligent Planet

Las Novedades en Ciberseguridad que Windows 11 IoT Implementó para la Industria

ADVANTECH
Enabling an Intelligent Planet

Introducción

En la industria, si bien los dispositivos de IoT pueden parecer demasiado pequeños o especializados para representar un peligro, existe el riesgo de que un atacante pueda hackear computadoras en red realmente comunes y causar problemas más allá del alcance del IoT (Problemas de seguridad en Internet). Simplemente en estos últimos 3 años hemos presenciado ataques cibernéticos enormes, claros ejemplos como la filtración de la base de datos de la Policía Nacional de Shangai la cual contenía muchos datos e información sobre miles de millones de ciudadanos chinos, otro caso es Syniverse empresa que forma parte de la infraestructura global de telecomunicaciones utilizada por AT&T, T-Mobile, Verizon y varias otras en todo el mundo, está informó que hackers estuvieron dentro de sus sistemas durante años, afectando a gran porcentaje de sus clientes el cual representa un estimado de millones de usuarios de teléfonos móviles en todo el mundo.

En esos ejemplos los atacantes cibernéticos obtienen el control, pueden robar datos, interrumpir servicios o cometer cualquier otro tipo de delitos cibernéticos relacionados con la informática. Los ataques que comprometen la infraestructura de IoT no solo provocan la filtración de datos y operaciones no confiables, sino que también causan daños físicos a las instalaciones.

Windows 11 es el Windows con mayor seguridad, con amplias soluciones diseñadas para evitar suplantación de identidad, alteraciones, revelación de información, denegación de servicio y elevación de privilegios. Las soluciones que se incluyeron en Windows 11 son: cifrado avanzado y protección de datos integrados, seguridad sólida de la red y del sistema, y medidas de seguridad inteligentes frente a amenazas en constante evolución.

Diferencias entre Windows IoT y Windows Pro

Antes de presentarte las nuevas implementaciones de seguridad que se incluyen en Windows 11, te explicaremos la diferencia entre Windows IoT y Windows Pro. Si bien ambos sistemas operativos comparten una base en común, presentan diferencias significativas en sus enfoques y aplicaciones.

Windows IoT se ha diseñado específicamente para impulsar dispositivos conectados y sistemas embebidos, mientras que Windows Pro se ha optimizado para brindar un entorno de trabajo y productividad eficiente en equipos de escritorio y portátiles.

Windows Pro	Windows IoT Enterprise
Aplicaciones de uso general, como ordenadores personales	Aplicaciones específicas, como sistemas embebidos
Ciclo de vida más corto (2-3 años, luego actualización forzosa)	Ciclo de vida más largo (más de 10 años)
Menor tiempo de soporte (18-30 meses)	Mayor tiempo de soporte (10 años)
De mayor costo (Actualizaciones constantes y flexibilidad para uso comercial)	De menor costoso (Sin actualizaciones constantes y para aplicaciones específicas)
Actualizaciones automáticas	El usuario controla las actualizaciones
Claves de producto únicas por dispositivo	Sólo tiene una clave de producto

Novedades en Seguridad de Windows 11 IoT Enterprise

A continuación explicaremos las novedades que Microsoft ha implementado en Windows 11 IoT Enterprise, enfocándonos en aspectos como:

1. Programa de seguridad y actualización de datos
2. El arranque seguro
3. Mejoras específicas para dispositivos IoT
4. El Antivirus de Microsoft Defender
5. La reducción de la superficie expuesta a ataques (ASR)
6. El acceso controlado a carpetas
7. Acceso Directo

Estas innovaciones representan un paso adelante en la protección de los sistemas y datos en los dispositivos IoT basados en Windows 11, permitiendo a las empresas abordar los desafíos de seguridad de manera más efectiva en un entorno cada vez más conectado.

1. Programa de seguridad y actualización de datos

Windows 11 IoT ha mejorado las funciones VBS, HVCI y Secure Boot para garantizar la integridad y seguridad de los programas y datos de los usuarios. La seguridad basada en virtualización (VBS) utiliza funciones de virtualización de hardware para crear zonas de memoria aisladas de forma segura e independientes de los sistemas operativos comunes. Windows puede utilizar el "Modo seguro virtual" para cargar varias soluciones de seguridad que mejoran la protección de las zonas de memoria aisladas.

De hecho, el Modo Seguro Virtual mitiga las debilidades del sistema operativo e impide el uso de código malicioso/ejecutable por parte de los hackers. Además, Hypervisor-enforced Code Integrity (HVCI) (también conocida como integridad de memoria) utiliza VBS para reforzar la integridad del código. Kernel-Mode Code Integrity funciona comprobando los controladores y binarios del modo kernel antes de habilitarlos. Kernel-Mode Code Integrity sólo habilita ejecutables firmados por firmantes aprobados. Esto evita que se carguen en la memoria del sistema controladores o archivos de sistema no firmados.

2. El arranque seguro

Es una importante función de seguridad diseñada para evitar que se cargue malware al arrancar el ordenador. Aunque la mayoría de los ordenadores nuevos pueden ejecutar Secure Boot, algunos ajustes pueden impedir que el ordenador arranque de forma segura en algunos casos. Estas configuraciones pueden ajustarse en el arranque a través de la Configuración de la BIOS antes de ejecutar Windows en el ordenador por primera vez. Los usuarios deben cambiar el modo de arranque del ordenador a UEFI/BIOS y activar la opción Secure Boot para mejorar su seguridad.

3. Mejoras específicas para dispositivos IoT

Configurar un Gatekeeper en los puntos de acceso de los usuarios es clave para la seguridad en el uso de la nube. Los Gatekeepers pueden bloquear los intentos de inicio de sesión no autorizados y aprovechar las credenciales TPM X.509 con Azure DPS para una red de inicio segura. Para la autenticación de identidades y la privacidad, Windows 11 IoT ha mejorado la entrada sin contraseña. En consecuencia, admite mecanismos de inicio de sesión por voz y huella dactilar para mejorar la privacidad personal.

Además, Windows 11 IoT es compatible con innumerables aplicaciones como Microsoft Teams. Teams permite a los empleados colaborar y comunicarse utilizando el paquete Office.

4. El Antivirus de Microsoft Defender

Antivirus de Microsoft Defender es una solución de protección incluida en todas las versiones de Windows. Desde el momento en que arranca Windows, Antivirus de Microsoft Defender supervisa continuamente el malware, los virus y las amenazas de seguridad. Las actualizaciones se descargan automáticamente para ayudar a proteger el dispositivo frente a amenazas. Antivirus de Microsoft Defender incluye protección antivirus en tiempo real, basada en comportamiento e investigación.

La combinación de análisis de contenido siempre activado, supervisión del comportamiento de archivos y procesos y otras heurísticas evita de forma eficaz las amenazas de seguridad. Antivirus de Microsoft Defender examina continuamente el malware y las amenazas, y también detecta y bloquea aplicaciones potencialmente no deseadas (PUA), que son aplicaciones que se consideran que afectan negativamente al dispositivo, pero que no se consideran malware.

5. La Reducción de la superficie expuesta a ataques (ASR)

Las reglas de reducción de la superficie expuesta a ataques (ASR) ayudan a evitar comportamientos de software que a menudo se usan para poner en peligro el dispositivo o la red. Al reducir el número de superficies expuestas a ataques, puede reducir la vulnerabilidad general de su organización.

Los administradores pueden configurar reglas de ASR específicas para ayudar a bloquear ciertos comportamientos, como iniciar archivos ejecutables y scripts que intentan descargar o ejecutar archivos, ejecutar scripts ofuscados o sospechosos, y realizar comportamientos que las aplicaciones no suelen iniciar durante el trabajo diario normal.

6. Acceso controlado a carpetas

Puede proteger su información valiosa en carpetas específicas administrando el acceso de la aplicación a carpetas específicas. Solo las aplicaciones de confianza pueden acceder a carpetas protegidas, que se especifican cuando se configura acceso controlado a carpetas. Las carpetas usadas habitualmente, como las usadas para documentos, imágenes y descargas, suelen incluirse en la lista de carpetas controladas. El acceso controlado a carpetas funciona con una lista de aplicaciones de confianza. Las aplicaciones que se incluyen en la lista de software de confianza funcionan según lo previsto. Las aplicaciones que no están incluidas en la lista de confianza no pueden realizar cambios en los archivos dentro de carpetas protegidas.

El acceso controlado a carpetas te ayuda a proteger los datos importantes del usuario de las aplicaciones malintencionadas y amenazas, como ransomware.

7. Acceso directo

DirectAccess permite la conectividad de los usuarios remotos a los recursos de red de la organización sin necesidad de conexiones de red privada virtual (VPN) tradicionales.

Con las conexiones de DirectAccess, los dispositivos remotos siempre están conectados a la organización y no es necesario que los usuarios remotos inicien y detengan las conexiones.

FAQ'S sobre actualizar a Windows 11

Las reglas de reducción de la superficie expuesta a ataques (ASR) ayudan a evitar comportamientos de software que a menudo se usan para poner en peligro el dispositivo o la red. Al reducir el número de superficies expuestas a ataques, puede reducir la vulnerabilidad general de su organización.

Los administradores pueden configurar reglas de ASR específicas para ayudar a bloquear ciertos comportamientos, como iniciar archivos ejecutables y scripts que intentan descargar o ejecutar archivos, ejecutar scripts ofuscados o sospechosos, y realizar comportamientos que las aplicaciones no suelen iniciar durante el trabajo diario normal.

1. ¿Cuáles son los requisitos básicos de entorno para el hardware y el software de Windows 11 IoT?

Estos son los requisitos básicos de hardware para Windows 11 IoT y la tabla de asignación para Windows 10 IoT:

Windows 11 IoT	Requisitos del Sistema
Procesador	1 GHz con 2 o más núcleos en un procesador de 64 bits compatible o sistema en un chip (SoC).
RAM	4 GB.
Almacenamiento	Dispositivo de almacenamiento de 64 GB o más.
Firmware del sistema	UEFI, compatible con Arranque seguro.
TPM	Módulo de plataforma segura (TPM) versión 2.0.
Tarjeta Gráfica	Compatible con DirectX 12 o posterior con controlador WDDM 2.0.

2. ¿En qué circunstancias es adecuada la actualización de Windows 10 IoT a Windows 11 IoT?

La actualización es ideal para los usuarios que desean aprovechar el TPM para mejorar la seguridad de los dispositivos. La actualización también es ideal para usuarios con aplicaciones que interactúan con los clientes. Windows 11 IoT también proporciona mejoras de IA e IU.

TPM (Módulo de plataforma segura) permite crear y almacenar claves criptográficas de forma segura, todo esto para confirmar que el sistema operativo y el firmware del dispositivo no hayan sufrido algún cambio por ataque cibernético. Es por ello que el TPM 2.0 tiene un papel importante en todas las novedades en ciberseguridad que presentamos con anterioridad en Windows 11.

3. ¿Qué sectores específicos se benefician más de la adopción de Windows 11 IoT y por qué?

Windows 11 IoT está diseñado para dispositivos especializados y casos de uso en los que la funcionalidad y las características permanecen constantes durante la vida útil del dispositivo. Normalmente, estos dispositivos se encuentran en sectores como, entre otros, la banca, la atención sanitaria, la hospitalidad, la fabricación y el comercio minorista. Los dispositivos que requieren la certificación normativa y los dispositivos que realizan una función empresarial crítica no pueden aceptar actualizaciones de características durante años a la vez.

4. ¿Qué factores debo tener en cuenta antes de adoptar Windows 11 IoT?

Windows 11 IoT es un sistema operativo en desarrollo constante, por lo que cuenta con funciones embebidas que aún no están disponibles para su personalización. Además, sugerimos comprobar si los controladores de sus dispositivos periféricos están preparados para soportar este software. Hacia la segunda mitad de 2024 habrá una actualización con soporte mundial a largo plazo, pero mientras es necesario verificar que nuestros dispositivos y aplicaciones sean compatibles con Windows 11 IoT. En Advantech, con gusto podemos orientarte.

Productos Advantech para aprovechar al máximo Windows 11 IoT Enterprise

Las reglas de reducción de la superficie expuesta a ataques (ASR) ayudan a evitar comportamientos de software que a menudo se usan para poner en peligro el dispositivo o la red. Al reducir el número de superficies expuestas a ataques, puede reducir la vulnerabilidad general de su organización.

Los administradores pueden configurar reglas de ASR específicas para ayudar a bloquear ciertos comportamientos, como iniciar archivos ejecutables y scripts que intentan descargar o ejecutar archivos, ejecutar scripts ofuscados o sospechosos, y realizar comportamientos que las aplicaciones no suelen iniciar durante el trabajo diario normal.

UNO-2484 V2

- Procesador Intel® Core™ 11th i7/i5/i3 con memoria DDR4 3200Mb/s de 8 GB.
- 4 x GbE, 3 x USB 3.2 Gen2, 1 x USB2.0, 1 x HDMI 1.4, 1 x DP 1.4a, 4 x RS232/422/485.
- La 2ª pila opcional admite hasta 2 extensiones iDoor para ampliar la conectividad inalámbrica, el bus de campo industrial o más E/S.
- Diseño compacto sin ventilador.
- Diseño robusto sin cables y con E/S bloqueables.
- Admite almacenamiento NVME con alta eficiencia de transmisión de datos.
- Compatible con las tecnologías TPM.

MIC-770-V3

- CPU Intel® Core™ i de 12ª generación tipo zócalo (LGA1700) con chipset Intel® R680E/ H610E.
- Amplia temperatura de funcionamiento (-20 ~ 60 °C); salida VGA y HDMI;
- 2 x GigaLAN, 2 x USB 3.2 (Gen2) y 6 x USB 3.2 (Gen1); 2 x RS-232/422/485 y 4 x puertos serie RS232 (opcional) 1 x HDD/SSD de 2,5", 1 x mSATA y 1 x NVMe M.2; rango de alimentación de entrada de 9 ~ 36 VDC.
- IP40 a prueba de polvo para el despliegue en entornos difíciles.
- Soporta tecnología FlexIO e iDoor, configuración flexible de HDMI adicional, DP, DVI, puerto COM, DIO, IO de conmutación remota.
- Soporta Advantech i-Modules; Soporta Advantech SUSIAPI y APIs de software embebido.
- Compatible con las tecnologías Intel® vPro™/AMT y TPM.

ARK-1250

- Core i5/i3 de 11ª generación de Intel
- Sistema DIN-Rail con puertos de E/S esenciales en el bisel frontal
- 3 x Intel GbE, 4x RS-232/422/485
- 3 x USB 3.2 y 3 x USB 2.0, pantallas duales independientes con un HDMI 4K y un VGA
- 3 ampliaciones: M.2 E-Key 2230, M.2 B-Key 2280, 1 x mSATA de tamaño completo compartido con ranura mPCIe.
- mSATA y 1 dispositivo de almacenamiento SATA de 2,5.
- Entrada de alimentación de amplio rango de 12 V ~ 24 V.
- Temperatura de funcionamiento ampliada de -40 ~ 60 °C.
- Compatible con WISE-DeviceOn para una rápida implantación de IA a gran escala.
- Compatible con las tecnologías TPM.

ACP-4000 / AIMB-788

- Procesador Intel® Core™ i9/i7/i5/i3 y Pentium®/Celeron® de 12ª/13ª generación con chipset Q670E.
- Cuatro ranuras DIMM de hasta 128 GB DDR4 3200.
- Triple pantalla DP/HDMI/VGA y LAN GbE dual.
- M.2, SATA RAID 0, 1, 5, 10, USB 3.2 Gen 2.
- Solución de gestión remota de energía fuera de banda iBMC de Advantech en DeviceOn.
- Calificado para AWS (Amazon Web Service) IoT Greengrass.
- Compatible con las tecnologías TPM.

Advantech cuenta con sistemas, software y hardware, para implementar soluciones de Internet Industrial de las Cosas (IIoT), desde nuestra llegada a México en 2020, hemos adaptado nuestra misión de habilitar un planeta inteligente para la Industria mexicana. Estamos seguros que podemos co-crear grandes innovaciones y soluciones para el mercado mexicano.

¡Contáctanos!

800 467 2415 julio.mora@advantech.com.mx www.advantech.com/es-mx

ADVANTECH

Enabling an Intelligent Planet

Sobre Advantech

Fundada en 1983, Advantech es un proveedor líder de cómputo industrial así como soluciones innovadoras en IIoT. Advantech ofrece integración completa de sistemas, hardware, software, servicios de diseño centrados en el cliente, sistemas integrados, productos de automatización y soporte logístico global. Colaboramos estrechamente con nuestros socios para proporcionar soluciones completas para una amplia gama de aplicaciones en diversos sectores. Nuestra misión es hacer posible un planeta inteligente desarrollando productos y soluciones informáticas automatizadas e integradas que faciliten un trabajo y una vida más inteligentes. Con los productos Advantech, el potencial de aplicación e innovación se vuelve ilimitado.
(Sitio Corporativo: www.advantech.com/es-mx)