Ivanti Neurons for Healthcare:

Mejorar la visibilidad de los activos y la mitigación de los riesgos de seguridad de los dispositivos médicos

Millones de dispositivos de TI médica y de IoT médica se utilizan para atender a los pacientes y agilizar los flujos de trabajo clínicos en las organizaciones clínicas, pero sus vulnerabilidades inherentes a programas malignos y a los ciberataques ponen en riesgo a hospitales y a pacientes. Los dispositivos médicos conectados representan un gran reto para las organizaciones de TI, biomédicas y de seguridad. Debido a su papel fundamental en la atención al paciente y en las infraestructuras de red de TI deben permanecer conectados, y las soluciones de TI estándar no pueden protegerlas. Esto deja a los hospitales expuestos y pone en peligro la seguridad de los pacientes, la confidencialidad de los datos y la disponibilidad del servicio.

- El **50%** de los hospitales no cumple las directrices del NIST (NIST por sus siglas en inglés, National Institute of Standards and Technology).
- El **65%** de los hospitales tiene poca confianza en la visibilidad de los activos.
- El **40%** de los dispositivos médicos conectados ejecutan un sistema operativo no soportado.
- Aumento del **300%** de los ciberataques en el sector médico desde principios de 2020.

Ivanti Neurons for Healthcare mejora la visibilidad de los activos y la mitigación de los riesgos de seguridad de los dispositivos médicos. La solución descubre y define de forma inteligente los dispositivos médicos y el Internet de las Cosas Médicas (IoMT), evaluando los riesgos de seguridad, informando de las amenazas y conciliando la información de los dispositivos a través de múltiples fuentes de datos. Conozca con más detalle los distintos dispositivos específicos de la entidad y de sus instalaciones, incluyendo la clasificación de los dispositivos y la información de uso, con los detalles para reducir el riesgo de seguridad o para atender las anomalías. Recopile y concilie los datos de los proveedores, creando una única fuente de confianza para todos sus dispositivos médicos.

Identificar dispositivos médicos, IoT y sistemas OT

El reto de los dispositivos médicos conectados no es fácil de entender para los equipos de TI, para biomédicos y personal de seguridad de los hospitales y organizaciones médicas debido a una visibilidad extremadamente limitada. Es fundamental comprender el entorno completo.

El escaneo activo de la red puede interrumpir el funcionamiento de los dispositivos médicos, por lo que debe utilizar la detección pasiva. Las herramientas tradicionales no descubrirán la gran mayoría de los dispositivos médicos conectados, o pueden indicar falsamente que el dispositivo es una estación de trabajo de Windows.

La mayoría de los dispositivos médicos conectados no anuncian su información, y detectarlos a través de la red requiere un detallado análisis del tráfico en la capa de aplicación. Con Ivanti Neurons for Healthcare se puede descubrir fácilmente qué dispositivos médicos y de TI existen, clasificarlos con precisión, comprender su contexto clínico e identificar sus necesidades de red para conocer su grado de exposición a las amenazas externas e internas.

Evaluar y priorizar el riesgo

En cuanto conozca mejor sus dispositivos médicos conectados y haya construido un inventario de los dispositivos, su contexto y su comportamiento en la red, podrá utilizar este inventario para evaluar los riesgos de seguridad que afectan a cada dispositivo y su impacto en la organización. Con la evaluación de riesgos a nivel de toda la organización y de los dispositivos, la detección de anomalías, las alertas en tiempo real y los conocimientos clínicos, Ivanti Neurons for Healthcare prioriza los planes de acción en función del impacto y la importancia del riesgo.

La ventaja de un proceso estructurado de descubrimiento y evaluación de riesgos es que puede clasificar los dispositivos en función de los riesgos que representan.

Asegure más rápido y cubra todos los factores de amenaza

Ivanti Neurons for Healthcare identifica las vulnerabilidades de los dispositivos y los riesgos relacionados con la red; asigna a cada dispositivo un índice de riesgo para la seguridad del paciente, la privacidad y la interrupción del servicio; y proporciona recomendaciones para la corrección. Su organización puede definir un

nivel de riesgo aceptable, y el equipo de seguridad puede centrarse en proteger los dispositivos con puntuaciones de riesgo superiores al nivel aceptable y aplicar las medidas de seguridad adecuadas a los dispositivos con diferentes puntuaciones de riesgo. Desde el acceso a proveedores hasta el acceso a la nube y segmentación virtual, Ivanti Neurons for Healthcare automatiza la reducción de riesgos ofreciendo la ruta de solución óptima. Empezando por los riesgos más críticos que tienen el mayor impacto en su organización, puede llegar a una postura de seguridad rápida y sostenible.

Reduzca los riesgos, prevenga las amenazas y mejore el cumplimiento de la normativa

Ivanti Neurons for Healthcare ofrece a los ingenieros biomédicos y clínicos la información y las soluciones que requieren para tener un control total de sus activos y estar sincronizados con sus homólogos de seguridad de TI con descubrimiento automatizado, inventario, ePHI y localización, clasificación de activos, paneles de utilización y capacidad de los dispositivos, y evaluaciones de riesgo adaptados a los flujos de trabajo y las arquitecturas exclusivas de los centros médicos. Las organizaciones médicas pueden aprovechar la información clínicamente contextualizada y en tiempo real para identificar y gestionar los riesgos de seguridad, optimizar el rendimiento de los dispositivos y lograr las ventajas rápidas y duraderas necesarias para garantizar la seguridad de los pacientes y la fluidez de las operaciones.

Funciones clave

Descubrimiento y gestión de activos automatizados

El descubrimiento de dispositivos médicos en tiempo real encuentra, carga inventario y clasifica cada dispositivo, rastrea las ubicaciones y proporciona:

- Datos completos sobre el tipo de dispositivo, el proveedor, el sistema operativo, el departamento, el número de serie y mucho más.

- Datos sobre los dispositivos que reciben y envían información de salud electrónica, además de evaluaciones de riesgo continuas, seguimiento de retiros y alertas.
- Perfecta integración con Ivanti Asset Management y otras soluciones de gestión de activos de terceros para gestionar eficazmente los activos médicos y optimizar su rendimiento.

Planificación de recursos y preparación para emergencias

La información operativa y la visibilidad continua de los patrones de utilización de los dispositivos le ayudan a tomar decisiones rápidas y fundamentadas con:

- Desglose del uso, el impacto médico y la importancia de los dispositivos individuales y de los tipos de dispositivos por sala y centro.
- Alertas sobre la capacidad de los dispositivos y la ubicación en tiempo real (por sala, departamento, ubicaciones externas).
- Información sobre cuándo se pueden programar los dispositivos para el tiempo de inactividad y el mantenimiento sin interrumpir los servicios clínicos.
- Resolución de problemas para entender qué ha fallado y cómo solucionarlo.

Rastreo de ePHI y alertas de retirada de dispositivos

El seguimiento continuo de los dispositivos con ePHI y las alertas de retirada de dispositivos permiten una alineación perfecta entre los equipos de ingeniería biomédica y clínica con sus homólogos de seguridad informática para:

- Identificar los dispositivos que pueden ser vulnerables a los ciberataques.
- Identifique inmediatamente los dispositivos con funcionalidad o seguridad y recibir planes de mitigación paso a paso.
- Garantizar el cumplimiento del seguimiento de las comunicaciones ePHI y la seguridad a nivel de dispositivo.

Adquisición y gestión del ciclo de vida

Acceso a la biblioteca MDS2 digitalizada y con capacidad de búsqueda, además de la inteligencia interna sobre amenazas, combinada con el poder de la IA, promueve la alineación entre equipos con la seguridad de TI y el ahorro de costes en la adquisición de dispositivos:

- Fácil acceso a los formularios MDS2, incluso para los dispositivos que aún no están en su inventario, para garantizar que los dispositivos se adhieren a las políticas de seguridad de la organización antes de la compra.
- La capacidad de aplicar fácilmente los datos del MDS2 a las políticas de seguridad a nivel de dispositivo para garantizar los servicios de mantenimiento y asistencia necesarios y una funcionalidad óptima (y prolongada) del dispositivo.
- Identificación de vulnerabilidades que ahorra a los equipos el tiempo que tardarían en comunicarse directamente con proveedores de dispositivos.
- Datos en tiempo real extraídos de fuentes externas para garantizar la funcionalidad del dispositivo, la seguridad y cumplimiento de la información de la FDA, la JCAHO y la HIPAA.
- La evaluación comparativa del rendimiento de los dispositivos que permite a los equipos crear programas de parcheo y mantenimiento para garantizar la continuidad del flujo de trabajo clínico y de los servicios médicos.

Gestión del acceso de los proveedores

El control del acceso de proveedores y terceros a los dispositivos de las redes informáticas del hospital garantiza:

- Visibilidad de los proveedores que se conectan, cuándo y por qué.
- Los proveedores y otros terceros solo se conectan a los dispositivos para los servicios de mantenimiento y asistencia necesarios.
- Cumplimiento con escaneo pasivo de las normas reglamentarias y alertas en tiempo real sobre cambios y violaciones.

Cuadros de mando modulares y basados en funciones

Los cuadros de mando configurables y modulares muestran variedades de datos para dar a los equipos la perspectiva que necesitan con la información correcta en el momento adecuado:

- Inventario y conocimientos sobre el funcionamiento de los dispositivos, las vulnerabilidades y las retiradas.
- Profundización en las comunicaciones que involucran la ePHI.
- Vistas de varios sitios para los hospitales de la red.

Sobre Ivanti

Ivanti hace que sea posible trabajar desde “cualquier parte”. En el teletrabajo, los empleados utilizan un sinfín de dispositivos para acceder a las aplicaciones de TI y a los datos a través de varias redes para seguir siendo productivos mientras trabajan desde cualquier lugar. La plataforma de automatización Ivanti Neurons conecta las soluciones líderes del sector de gestión unificada de puntos finales, seguridad de confianza cero y gestión de servicios empresariales, proporcionando una plataforma de TI unificada que permite a los dispositivos autorestablecerse y autoprotegerse y capacita a los usuarios para el autoservicio. Más de 40.000 clientes, entre los que se encuentran 78 de las 100 empresas de la lista Fortune, han optado por Ivanti para descubrir, gestionar, proteger y dar servicio a sus activos de TI desde la nube hasta el borde, y ofrecer excelentes experiencias de usuario final a los empleados, donde quiera y como quiera que trabajen. Para más información, visite ivanti.com

ivanti Neurons

ivanti.lat
+57 315 5718981
contact-latam@ivanti.com

ivanti.es
+34 91 049 66 76
contact@ivanti.es