La seguridad de IdC en el sector sanitario: guía para CISO

Proteja todos sus dispositivos gestionando el flujo de trabajo de los dispositivos y entornos clínicos en 6 pasos

Contenido

Se dispara la adopción del IdC en el sector sanitario

El IdC (Internet de las cosas) da oxígeno al sector sanitario. La pandemia no ha hecho más que acelerar su adopción.

Esta tecnología está cambiando la atención sanitaria. La demanda de dispositivos IdC en áreas funcionales como la monitorización de pacientes a distancia y el rastreo de contactos se ha intensificado a raíz de la pandemia. Pero ya antes de este crecimiento exponencial, la adopción del IdC en la sanidad iba en aumento.

La transformación de la prestación de servicios sanitarios gracias al IdC se ha ido consolidando en la última década. Durante este tiempo, muchos usos prácticos de esta tecnología —como el seguimiento y la gestión de los pacientes, el diagnóstico a distancia, el cuidado de la higiene, la monitorización remota, el mantenimiento predictivo de los dispositivos médicos, etc.— se han ido abriendo paso en la línea de negocio de la atención sanitaria.

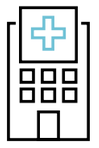
Así lo demuestra un estudio de Gartner publicado en enero de 2020, que revelaba que el 86 % de las organizaciones de servicios sanitarios ya contaban con una solución de IdC para la mayoría de las líneas de negocio.[1] Actualmente, Omdia calcula que en 2020 se introdujeron en el mercado global más de 250 millones de dispositivos médicos, y se espera que otros 500 millones hagan lo propio para 2025.[2]

48 %

Porcentaje de organizaciones de servicios sanitarios que utilizan el IdC en implementaciones a gran escala (diversos casos de uso y proyectos)[3]

31 %

Porcentaje de organizaciones de servicios sanitarios que utilizan el IdC en implementaciones con un solo caso de uso (o proyecto)[4]

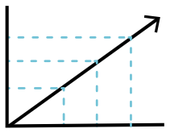


21 000 M

Gasto en IdC de los proveedores de servicios sanitarios en 2019[5]

54 000 M

Gasto previsto en IdC de los proveedores de servicios sanitarios en 2029[6]



10 %

Tasa de crecimiento anual compuesto[7]

El sector sanitario sigue apostando por el IdC sin signos de desaceleración. Pero ¿hasta qué punto está preparado para hacer frente a los graves problemas de seguridad que se derivan de esta tendencia?

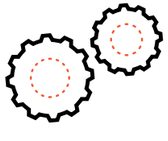
Fuentes:

1, 3-4 Gartner Survey Analysis: Healthcare Provider IoT Adoption Is Becoming Mainstream (disponible en inglés), 2020
2 Omdia IoT Devices Intelligence (disponible en inglés), 2020
5-7 Gartner Forecast Analysis, Healthcare Providers IoT Endpoint Electronics and Communications Revenue, Worldwide (disponible en inglés), 2020

La seguridad es el eslabón más débil

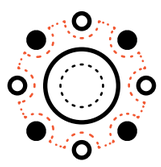
Los dispositivos IoMT representan una barrera de entrada extraordinariamente baja para los ciberdelincuentes, lo que obliga a instaurar un nuevo paradigma de seguridad.

Aunque el IdC está revolucionando la atención sanitaria, lamentablemente hay algunos problemas que solucionar. La seguridad es uno de esos escollos y sigue siendo el mayor impedimento a la adopción de la tecnología. La sanidad se ha convertido en un objetivo de interés estratégico para los ciberdelincuentes debido al valor de los datos que maneja. Eso hace que millones de dispositivos médicos conectados (lo que se conoce como «Internet de las cosas médicas» o «IoMT», por sus siglas en inglés) que recogen y almacenan esos datos sean vulnerables a los ataques. Al ser tan difíciles de proteger, estos dispositivos dan lugar a importantes riesgos para la seguridad, tal y como ocurre con los dispositivos IdC.



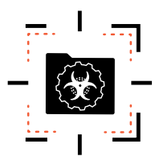
SISTEMAS OPERATIVOS OBSOLETOS

Los dispositivos IoMT suelen ejecutar sistemas operativos obsoletos y muchos de ellos ni siquiera fueron concebidos para conectarse a Internet, por lo que no incorporan sistemas integrados de prevención ni de aplicación de políticas.



REDES SIN SEGMENTAR

Las redes de los hospitales no suelen estar segmentadas, y eso permite a los atacantes infectar un dispositivo informático y desplazarse lateralmente para contaminar de forma cruzada los dispositivos IdC y viceversa.



VULNERABILIDADES PREEXISTENTES

Los dispositivos médicos suelen traer vulnerabilidades preexistentes que son difíciles de corregir. Con una larga vida útil, muchos no se retiran ni se sustituyen con la suficiente frecuencia.

En 2020, las instituciones sanitarias alertaron de 616 brechas de datos de 500 historiales o más, poniendo en riesgo 28 756 445 historiales clínicos.[8]

¿Sabía que...?

El 41 % de los ataques aprovechan vulnerabilidades en los dispositivos IdC

El 57 % de los ataques de gravedad media o alta se producen en dispositivos IoMT

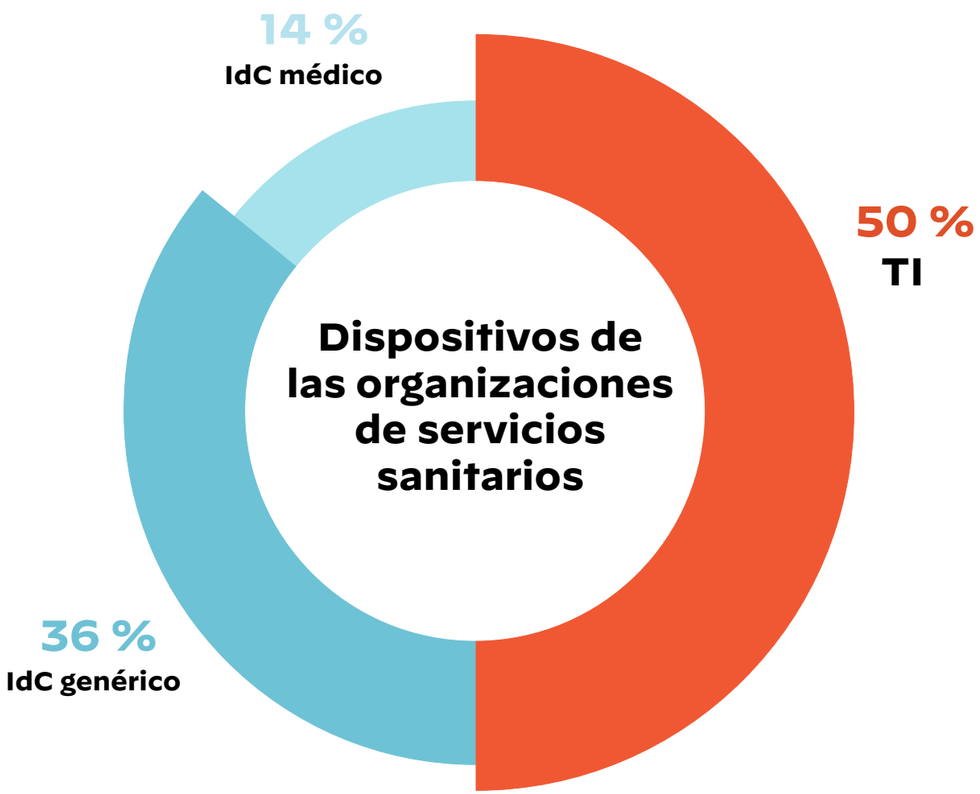
El 72 % de las redes VLAN del sector sanitario contienen una mezcla de dispositivos de TI y de IdC/IoMT

El 83 % de los dispositivos de obtención de imágenes diagnósticas incorporan sistemas operativos desfasados, un incremento del 56 % con respecto a 2018

Fuente:
Informe sobre las amenazas del IdC (Unit 42, 2020)
8 HIPAA Journal 2021 (disponible en inglés)

Dispositivos de las organizaciones de servicios sanitarios

Los dispositivos IoMT representan una barrera de entrada extraordinariamente baja para los ciberdelincuentes, lo que obliga a instaurar un nuevo paradigma de seguridad.



El 50 % de los dispositivos de las organizaciones de servicios sanitarios no están gestionados

Fuente:
Informe de Zingbox de 2019 sobre amenazas a dispositivos médicos (disponible en inglés)
Informe sobre las amenazas del IdC (Unit 42, 2020)

Dispositivos IdC médicos más implementados

46 %
Bombas de infusión

19 %
Sistemas de obtención de imágenes diagnósticas

17 %
Sistemas de monitorización de pacientes

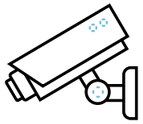
Dispositivos IdC médicos con más problemas de seguridad

51 %
Sistemas de obtención de imágenes diagnósticas

26 %
Sistemas de monitorización de pacientes

9 %
Puertas de enlace de dispositivos médicos

Dispositivos IdC genéricos con más problemas de seguridad en todas las organizaciones, incluidas las de servicios sanitarios



33 %
Cámaras de seguridad

24 %
Impresoras

10 %
Dispositivos de juego

Las soluciones actuales no protegen el IdC en el sector sanitario

Los mecanismos de seguridad obsoletos no están preparados para proteger todos los dispositivos, y esto aumenta la carga de trabajo de los equipos de seguridad, infraestructuras y dispositivos clínicos.

Los ciberdelincuentes aprovechan cualquier vulnerabilidad en el IoMT para perpetrar sus fechorías: tomar el control del dispositivo médico, robar datos confidenciales de los pacientes (tanto los personales como los relativos a su salud y seguro médico) e historiales clínicos, ofuscar el tráfico de la red, interrumpir procesos de la atención sanitaria y exigir un rescate por liberar el dispositivo. En el mercado empiezan a abundar las soluciones de seguridad de IdC, pero ninguna de ellas contempla una estrategia de seguridad exhaustiva e integral con todo lo necesario para proteger los dispositivos médicos de la red sin excepción.

Por qué las soluciones actuales no protegen el IoMT ni el IdC

LAS SOLUCIONES BASADAS EN FIRMAS

para identificar dispositivos ni son precisas ni pueden adaptarse la proliferación masiva de dispositivos —o variantes de dispositivos— que se implementan cada día.

LAS ESTRATEGIAS BASADAS SOLO EN ALERTAS

no pueden aplicar ni recomendar políticas, ni tampoco evitan las amenazas conocidas y desconocidas de los dispositivos IoMT e IdC.

LAS SOLUCIONES INDEPENDIENTES

introducen problemas y fricciones en la implementación, ya que obligan a cambiar la infraestructura de la red o a añadir nuevos sensores en ella para procesar el tráfico e identificar los dispositivos.

Una estrategia integral para proteger y gestionar los dispositivos clínicos

Los dispositivos médicos deben entenderse en el contexto de una metodología de gestión de dispositivos clínicos completa que minimice el riesgo para los pacientes y la red. La metodología ideal es la que libera a los equipos médicos y de seguridad de muchas de las tareas diarias relacionadas con la protección y la gestión de estos dispositivos.

Las superficies de ataque se están ampliando y los vectores de ataque son cada vez más elaborados. Ha llegado el momento de reforzar su seguridad de IoMT con un nuevo nivel de sofisticación.

Implemente une gestión segura del flujo de trabajo de los dispositivos y entornos clínicos en 6 pasos

1

Conozca todos los dispositivos IoMT de su organización de servicios sanitarios

Tener una visibilidad completa de la superficie de ataque de IoMT le ayudará a evaluar su estrategia de seguridad. Ahí empieza el ciclo de vida de la seguridad de IdC. La detección de dispositivos permite a todas las partes interesadas —equipos de TI, de seguridad y biomédicos— tener una visión global de los activos de IoMT de su organización de servicios sanitarios. Obtenga un inventario actualizado de todos los activos IoMT: los conocidos, los desconocidos e incluso los olvidados. Durante el proceso de detección de dispositivos, la solución de seguridad de IoMT recaba atributos esenciales del dispositivo para ofrecer el contexto completo de cada dispositivo médico.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Identificar al menos el 90 % de los dispositivos en segmentos visibles en un plazo de 48 horas.
- Detectar nuevos dispositivos —desconocidos hasta ese momento— con un sistema de aprendizaje automático y clasificarlos por proveedor, marca, modelo, tipo, sistema operativo, *firmware*, ubicación, subred, puntuación de riesgo, tipo de información sanitaria protegida, especificaciones contenidas en el formulario MDS2, etc.
- Detectar los dispositivos recién conectados en cuestión de minutos, y no en horas ni semanas.
- Distinguir los dispositivos IoMT e IdC no gestionados de los activos de TI gestionados.
- Registrar el total de dispositivos de TI para que los equipos informáticos y de seguridad puedan identificar los dispositivos de TI no gestionados.
- Actualizar automáticamente las soluciones de gestión de activos —como los sistemas de gestión de mantenimiento asistido por ordenador, los sistemas de gestión de servicios de TI o las bases de datos de gestión de la configuración (CMMS, ITSM y CMDB, respectivamente, por sus siglas en inglés)— con la información detallada de los dispositivos IoMT.
- Utilizar sensores multipropósito que se integren en la infraestructura existente.

2

Reduzca el riesgo de forma proactiva con la supervisión y evaluación continuas de los dispositivos IoMT

En la etapa de **evaluación de riesgos** del ciclo de vida de la seguridad de IdC, es preciso supervisar activamente los dispositivos IoMT en todo momento. La supervisión de riesgos, los informes y las alertas en tiempo real son fundamentales para que las organizaciones puedan reducir de forma proactiva tanto los riesgos que plantea el IoMT como la superficie expuesta a las amenazas. Las soluciones basadas en firmas son imprecisas y lentas, lo que limita su capacidad para proteger estos activos. Evaluar con precisión los riesgos del ciclo de vida de la seguridad de IdC le permite adoptar una estrategia mejor, porque sus equipos de seguridad de TI pueden examinar continuamente los dispositivos y supervisar los patrones de tráfico para favorecer la segmentación proactiva del control de acceso a la red (NAC, por sus siglas en inglés) y reducir la superficie expuesta a las amenazas. La evaluación de riesgos también hace que los equipos de TI analicen de forma proactiva la microsegmentación de la red por tipos y clases de dispositivos —IoMT, IdC o TI— para prevenir el movimiento lateral de las amenazas.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Integrarse con varias fuentes de información sobre amenazas (CVE, MDS2, RSSI, etc.) para establecer correspondencias entre las vulnerabilidades y el inventario de activos IoMT.
- Incluir especificaciones MDS2 (declaración de divulgación del fabricante para la seguridad de los dispositivos médicos) tales como las funciones antivirus, la información sanitaria electrónica protegida (ePHI), los productos retirados por la FDA y los avisos de los proveedores para la aplicación de revisiones.
- Detectar y notificar en tiempo real anomalías en los dispositivos IoMT que puedan afectar a las puntuaciones de riesgo.
- Calcular las puntuaciones de riesgo de los dispositivos IdC y las categorías de dispositivos.
- Hacer un seguimiento de los cambios en las puntuaciones de riesgo y almacenar el historial completo de riesgo de los dispositivos a efectos de cumplimiento normativo.
- Integrarse con los sistemas de gestión de vulnerabilidades y con los proveedores de dispositivos para gestionar los riesgos del IoMT de forma centralizada y proporcionar la información a los equipos de seguridad.

3

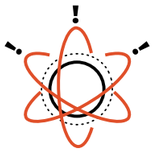
Utilice las recomendaciones y la aplicación de políticas de seguridad automatizadas basadas en el riesgo

Una solución de seguridad IoMT sencilla no requiere infraestructuras ni inversiones adicionales y, con ella, sus equipos de seguridad de TI podrán aprovechar la inversión existente en cortafuegos de nueva generación para establecer una estrategia de seguridad exhaustiva e integrada. Utilice una solución que, en combinación con las funciones del cortafuegos, **recomiende automáticamente políticas de seguridad** basadas en el nivel de riesgo y en los comportamientos no fiables de los dispositivos IdC y las aplique de forma nativa. Teniendo en cuenta que la confianza no es sino una vulnerabilidad, la solución de seguridad de IoMT debe acogerse directamente a los principios del modelo Zero Trust (confianza cero) para aplicar políticas de control de acceso basadas en el criterio del mínimo privilegio. De este modo, se reduce drásticamente el número de vías de acceso para los atacantes, tanto internos como externos, a los activos IdC cruciales de la organización.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Ofrecer mecanismos para convertir los patrones de comportamiento de los dispositivos IoMT en políticas que solo permitan comportamientos de confianza.
- Automatizar la aplicación de políticas con la identificación de dispositivos y aplicaciones.
- Admitir tanto listas de permitidos como listas de bloqueados.
- Llevar un control de los dispositivos y aplicaciones para aplicar las políticas con independencia de dónde se encuentren en la red.
- Actualizar las políticas automáticamente para limitar las actualizaciones manuales cada vez que se produce un cambio.
- Integrarse con la solución NAC y facilitar automáticamente información sobre los dispositivos IdC para aplicar controles a los dispositivos y habilitar la segmentación contextualizada.

4



Tome medidas preventivas rápidamente frente a las amenazas conocidas

Por su gran diversidad, los dispositivos IoMT crean un entorno muy distribuido en la red con numerosos puntos de peligro. Para que la estrategia de seguridad resulte eficaz, la cuarta fase del ciclo de vida de la seguridad de IdC requerirá información útil para **detectar y bloquear las amenazas conocidas** que acechan a sus dispositivos IoMT. Busque un mecanismo de prevención de amenazas que emplee firmas basadas en la carga útil para bloquear las amenazas avanzadas. Así conseguirá que tanto su estrategia de seguridad como sus mecanismos de defensa estén actualizados para responder en tiempo real a las vulnerabilidades que afecten a los dispositivos IoMT y a posibles deficiencias en la red. Es la mejor manera de ahorrar tiempo y de evitar quebraderos de cabeza sin sobrecargar a sus equipos de seguridad con alertas de detección que podrían detenerse.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Habilitar protecciones contra amenazas de forma selectiva basándose en la estrategia de seguridad del grupo de dispositivos IoMT.
- Detectar y bloquear las amenazas conocidas del *malware*, el *spyware* y los *exploits* dirigidos al IoMT.
- Detener los ataques al IoMT derivados de URL y sitios web maliciosos.
- Frenar los ataques de comando y control y de robo de datos que se valen del protocolo DNS para poner en peligro los dispositivos IoMT.
- Prohibir las amenazas IoMT desconocidas distribuidas mediante cargas útiles.

5

Detecte las amenazas desconocidas y responda a ellas rápidamente

A la hora de **detectar y bloquear amenazas verdaderamente desconocidas**, las soluciones heredadas aíslan los datos de amenazas que recibe y genera cada organización, lo que crea silos y reduce el margen de prevención. En aras de cumplir los requisitos del último paso del ciclo de vida de la seguridad de IdC, la solución de seguridad de IoMT que elija debe ser capaz de adaptarse a un nuevo enfoque que se nutra de un motor de inteligencia sobre amenazas colectiva para hacer análisis de *malware* en tiempo real y ofrecer protección inmediata frente a los ataques de día cero dirigidos a los dispositivos IoMT. Utilizar datos recopilados de forma colaborativa por una comunidad internacional de suscriptores no solo brinda inmunidad a todos, sino que también ahorra un tiempo valiosísimo a su equipo de seguridad informática, ya que facilita información sobre la identidad de los dispositivos IoMT afectados, calificaciones de riesgo, datos de vulnerabilidades y análisis de comportamiento para investigar amenazas nunca vistas que afectan particularmente a su entorno de IoMT. Este último paso también destapará posibles amenazas que se quedaron sin detectar previamente y favorece la implantación de un proceso cíclico de mejora continua.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Detectar comportamientos anómalos en diferentes niveles: primero, en el nivel de categoría del dispositivo; después, en el nivel de modelo/fabricante del dispositivo y, por último, en el nivel de instancia del dispositivo.
- Aprovechar la inteligencia recopilada de forma colaborativa gracias al aprendizaje automático mejorado con tecnología de modelado de amenazas para detectar amenazas desconocidas o ataques y enviar notificaciones o tomar medidas de forma anticipada.
- Integrarse con los sistemas SIEM y SOAR con un método simplificado basado en un libro de estrategias para orquestar acciones de respuesta a incidentes y prevención de amenazas.
- Allanar el camino de los investigadores de seguridad de IdC para descubrir nuevas amenazas que afecten al entorno IdC.

6

Obtenga inteligencia operativa para los equipos clínicos y biomédicos

Aunque la mayoría de los dispositivos médicos nunca alcanzan su plena utilización a pesar del exceso de inventario, a menudo requieren gastos operativos y de capital que provocan un desembolso innecesario. Aparte de eso, como los dispositivos médicos están regulados por la FDA, todas las actualizaciones de software requieren una revisión por parte del fabricante de equipos originales (OEM, por sus siglas en inglés) para validar que los cambios en el software sigan garantizando que es seguro utilizar el dispositivo con pacientes. Los equipos clínicos biomédicos que se ocupan de estos aspectos del uso o la gestión de los dispositivos médicos necesitan, por un lado, información útil y práctica sobre el negocio y las operaciones que reduzca la complejidad de las tareas de planificación de capital y de mantenimiento preventivo y, por el otro, saber en todo momento cuándo hay que aplicar revisiones y actualizaciones de software a los dispositivos. De ahí la necesidad de contar con una solución de seguridad de IdC que facilite la toma de decisiones importantes. La información operativa derivada de la solución ayuda a los equipos a **identificar** dispositivos, **incorporarlos** para utilizarlos cuando sea necesario, **optimizar** su rendimiento en función de los datos de uso y **retirarlos** de forma segura conforme a la normativa del sector.

Una solución de seguridad de IoMT eficaz debe ser capaz de desempeñar estas funciones:

- Realizar un seguimiento y elaborar informes de las estadísticas de uso de cada dispositivo médico para ayudar a decidir cuándo sustituirlo o comprar uno nuevo.
- Determinar los picos de uso para planificar el mantenimiento preventivo y las actualizaciones de software, garantizando que la programación de los servicios médicos críticos o la atención al paciente no se vean afectadas.
- Proporcionar datos analíticos sobre el uso de dispositivos de obtención de imágenes diagnósticas, indicando qué miembros del personal están utilizando los dispositivos y cómo lo están haciendo para asegurarse de que los recursos de personal se encuentren cerca de los dispositivos con los que trabajan.
- Gestionar rápidamente los avisos de los fabricantes, las retiradas de la FDA y los problemas de forma centralizada sin necesidad de investigaciones manuales.
- Actualizar los sistemas de inventario para mantener un log continuo de los dispositivos, garantizando que todos los demás departamentos estén al tanto de los dispositivos nuevos y de los que ya se han retirado.
- Proteger los historiales de los pacientes revelando cómo utiliza y almacena los datos cada dispositivo para facilitar la incorporación y retirada de dispositivos conforme a la normativa HIPAA.

IoT Security para el sector sanitario de Palo Alto Networks

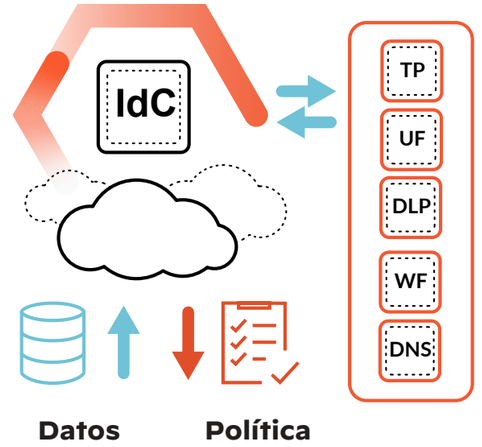
La solución de seguridad de IdC más completa para el sector sanitario

IoT Security de Palo Alto Networks es la solución de seguridad de IdC más completa para el sector sanitario. Incorpora en una sola plataforma funciones de visibilidad, prevención, aplicación de políticas e información operativa con aprendizaje automático.

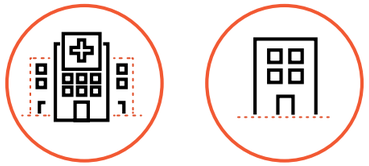
Descubra todo lo que IoT Security puede hacer por su organización:

- Es la única solución dotada de **aprendizaje automático colaborativo** que detecta rápidamente y con precisión todos los dispositivos, incluso los desconocidos.
- Es la única solución con **prevención integrada.** A diferencia de los sistemas basados únicamente en alertas, IoT Security mantiene los dispositivos no gestionados a salvo de todas las amenazas y vulnerabilidades conocidas y desconocidas mediante la prevención de amenazas y el bloqueo de vulnerabilidades para evitar que entren en la red.
- IoT Security también reduce el coste de la atención al paciente con **información operativa** para el personal sanitario y **aplica automáticamente las políticas directamente o por medio de integraciones.** Esto reduce la carga de trabajo de sus equipos de operaciones de seguridad y de red, mantiene todos los dispositivos protegidos y aumenta el tiempo de actividad y disponibilidad.
- IoT Security es una plataforma centralizada que **se implementa fácilmente** y sin necesidad de infraestructura adicional.

A día de hoy, IoT Security de Palo Alto Networks es la única solución del mercado que rentabiliza al máximo la inversión y optimiza la experiencia del paciente, gracias a que ofrece visibilidad completa, información operativa específica y una mayor seguridad para los dispositivos médicos. Y todo, en una sola plataforma. **Ya protegemos a 1 de cada 5 hospitales de EE. UU.**



Opciones de implementación flexibles



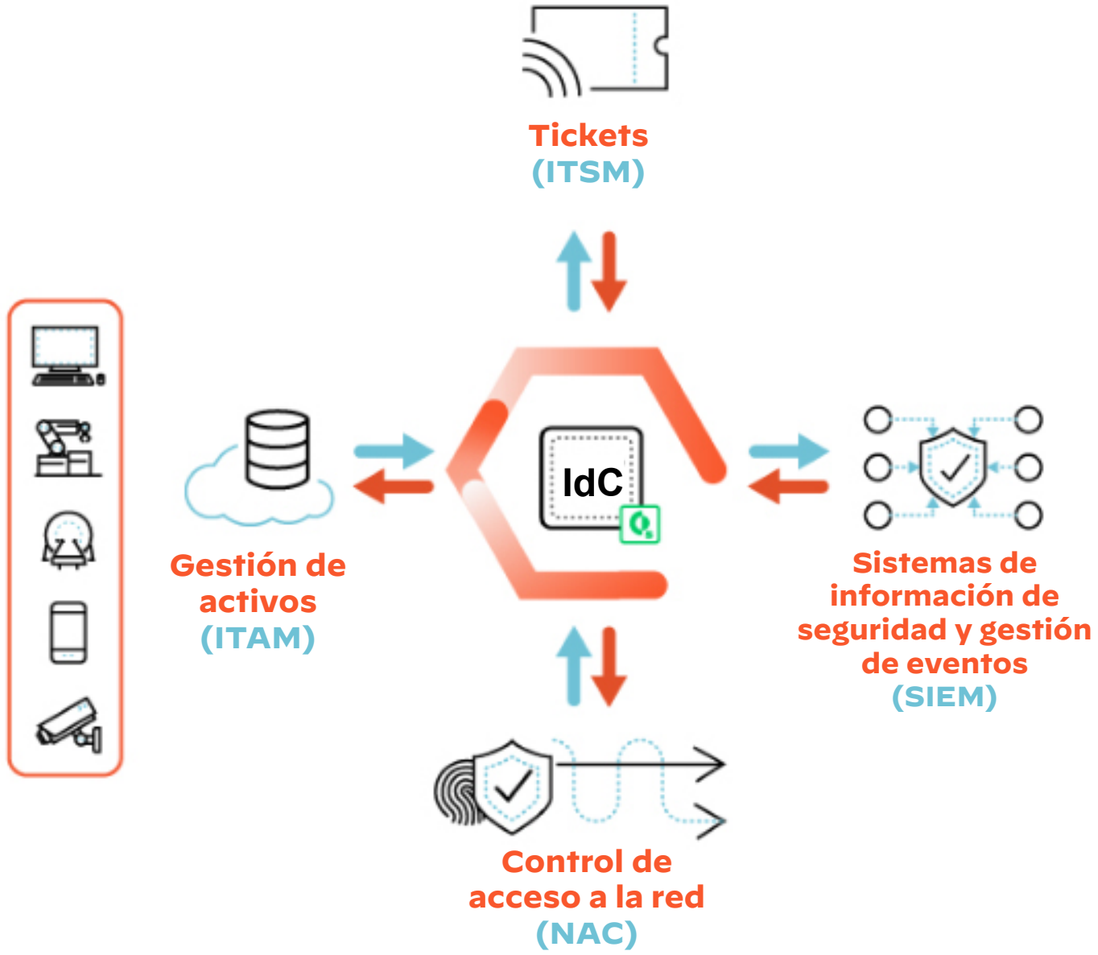
Integración con terceros

Con tecnología XSOAR integrada

Nuestra solución IoT Security se integra perfectamente con los flujos de trabajo de su organización y evita las integraciones vía API que tantos recursos consumen, lo que reduce la carga de trabajo de los equipos de infraestructuras y de seguridad.

Aproveche integraciones nativas con los flujos de trabajo de TI y de seguridad existentes para reforzar sus sistemas de gestión de servicios de TI, de control de acceso a la red y de información de seguridad y gestión de eventos (ITSM, NAC y SIEM, respectivamente, por sus siglas en inglés), entre otros casos de uso.

Con nuestra orquestación modular y personalizada basada en libros de estrategias, su equipo de seguridad podrá mejorar las ineficiencias operativas, enriquecer los inventarios de activos, incorporar con precisión los dispositivos IoMT, aplicar controles a los dispositivos y automatizar las respuestas a los incidentes sin necesidad de crear integraciones desde cero.

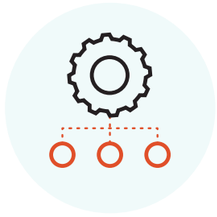


Aproveche su equipo de seguridad de TI actual

Sin necesidad de formar un nuevo equipo, implementar una nueva infraestructura ni cambiar los procesos operativos que ya tiene en marcha.

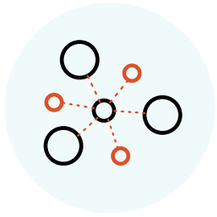
Visibilidad y protección sin precedentes

- Detección de dispositivos IdC basada en el aprendizaje automático
- Evaluación automatizada de riesgos
- Aplicación de políticas de seguridad nativa
- Segmentación de la red basada en el contexto



Implementación sencilla con opciones de formato flexibles

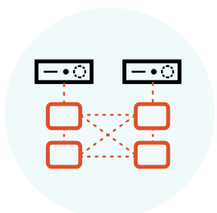
- Cortafuegos de hardware
- Cortafuegos de software
- Cortafuegos en la nube



Protección completa de dispositivos IdC , IoMT y de TI

- Dispositivos IoMT no gestionados
- Dispositivos IdC no gestionados
- Dispositivos de TI gestionados

Aproveche la prevención avanzada de otros servicios de seguridad



Adapte linealmente los sistemas al crecimiento de su empresa con una infraestructura en la nube elástica de varios inquilinos

Automatice los flujos de trabajo con integraciones basadas en libros de estrategias

Piense en IoT Security para el sector sanitario.

Piense en Palo Alto Networks.

En Palo Alto Networks, nuestra misión es ser el socio de confianza en materia de ciberseguridad y proteger nuestro estilo de vida digital. Decenas de miles de organizaciones nos han encomendado la tarea de proteger sus nubes, redes y dispositivos, y ayudamos a afrontar los mayores desafíos del mundo en materia de seguridad con innovaciones constantes que recurren a los últimos avances en inteligencia artificial, análisis, automatización y orquestación.

Palo Alto Networks, fundada en 2005, está afincada en el condado de Santa Clara (California) y presta sus servicios a clientes internacionales con oficinas repartidas por el mundo entero.

Para obtener más información, visite: www.paloaltonetworks.es

¿Quiere saber más? **Vea la demostración del producto**

Nuestros clientes opinan

«IoT Security de Palo Alto Networks es una solución sencilla basada en la nube que se implementa rápidamente. Gracias a esta herramienta, tenemos una visibilidad completa de más de 4000 dispositivos IoT y médicos, aproximadamente un 30 % más que antes.»

Miroslav Belote
Director de Seguridad de la Información
Valley Health System

Valley Health System

www.paloaltonetworks.es

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883