Internet de las Cosas en sanidad

Constituya una base segura para aprovechar las soluciones IoT y optimizar los cuidados

Informe de la solución
IoT en sanidad

Alcatel·Lucent
Enterprise

IoT cambia fundamentalmente la ecuación de la sanidad

Internet de las Cosas (Internet of Things, IoT) tiene potencial para transformar la sanidad ya que altera profundamente la forma de recoger los datos en hospitales, clínicas y otros centros sanitarios al combinar las principales tendencias técnicas y de negocio en movilidad, automatización y análisis de datos para mejorar la atención al paciente. IoT recurre a redes de objetos físicos mediante el uso de sensores embebidos, actuadores y otros dispositivos que pueden captar y transmitir información sobre la actividad de la red en tiempo real. Los datos obtenidos a través de estos dispositivos pueden ser analizados luego por la organización para:

- Mejorar la atención al paciente ofreciéndole unos cuidados y un servicio nuevos o mejorados que ayuden a diferenciar una organización sanitaria impulsada por los datos.
- Optimizar los procesos mediante el desarrollo de nuevos servicios y soluciones que aumenten la eficiencia y reduzcan los costes operativos.
- Conocer mejor las necesidades y preferencias de los pacientes para permitir que las organizaciones sanitarias ofrezcan una atención y unas preferencias más personalizadas.
- Lograr que las redes de los hospitales sean más inteligentes mediante la supervisión proactiva de la infraestructura crítica, junto con el despliegue y la gestión de la infraestructura TI.

Posibilidades de IoT en sanidad

Las soluciones IoT para sanidad prometen lograr que las organizaciones médicas sean más inteligentes y más exitosas en lo que hacen. IoT tiene el potencial de redefinir cómo interaccionan las personas, la tecnología y los dispositivos y cómo se conectan entre sí en los entornos sanitarios, ayudando así a promover una mejor atención, reducir costes y mejorar resultados. Estos son algunos ejemplos de soluciones IoT para sanidad:

- Dispositivos médicos conectados, como equipos de resonancia magnética y tomografía computerizada, que generan enormes flujos de datos que se conectan a infraestructuras informáticas para proporcionar análisis y visualización.
- Dispositivos médicos portátiles y de monitorización remota del paciente, que ofrecen una atención sanitaria más segura y efectiva mediante la monitorización de las constantes vitales del paciente en tiempo real, la recuperación tras una operación y el cumplimiento de los tratamientos, tanto en el hospital como de forma remota. Con los sensores portátiles, los doctores realizan un seguimiento remoto y responden al estado de la salud de los pacientes en tiempo real.
- Videocámaras de seguridad y puertas de seguridad con identificación electrónica que aumentan la seguridad y evitan amenazas así como entradas y salidas no autorizadas.
- Seguimiento de activos médicos con etiquetas Bluetooth Low Energy (BLE) para la localización de dispositivos médicos, medicinas y suministros.
- Soluciones de mantenimiento preventivo para el equipamiento médico con el fin de reducir las reparaciones imprevistas de instrumentos, dispositivos y sistemas médicos esenciales.

Desafíos del despliegue de IoT

IoT aporta un flujo de datos sin precedentes, lo cual genera desafíos en cuanto a prestaciones, operativos y de gestión a la infraestructura de la red, así como mayores riesgos de seguridad desde todos los puntos. Para solucionar estas cuestiones, las organizaciones necesitan adaptar los diseños de la red tradicional para ofrecer nuevos niveles de inteligencia, automatización y seguridad a la red.

Hospitales, clínicas y centros sanitarios necesitan una infraestructura de red económica capaz de cumplir las exigencias de seguridad y privacidad y de gestionar enormes flujos de datos, además de ser fácil de gestionar y manejar. La infraestructura debe:

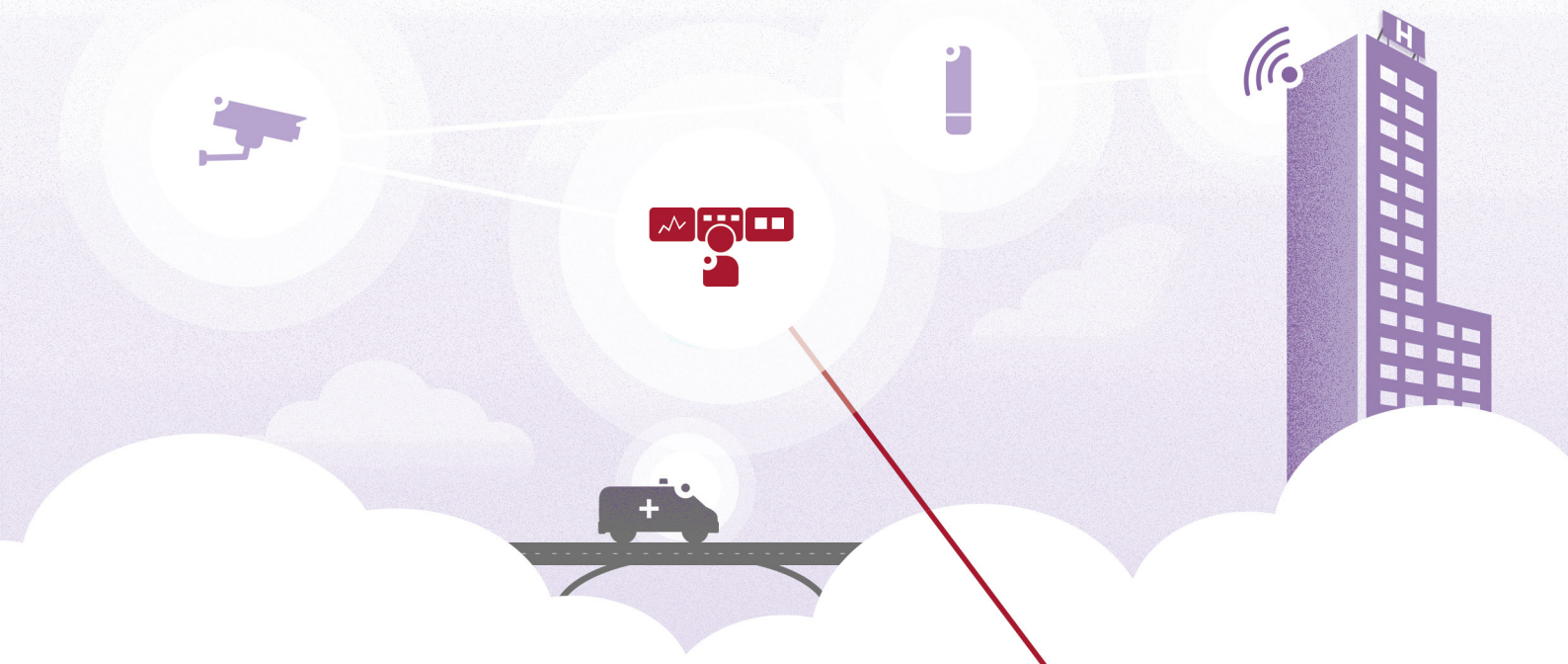
- Ofrecer un proceso sencillo y automatizado para la incorporación de dispositivos IoT. Los grandes sistemas IoT pueden contener miles de dispositivos o sensores, y el suministro y la gestión manual de todos estos puntos aumenta la complejidad y la posibilidad de errores. La incorporación automatizada permite que la infraestructura de la red reconozca los dispositivos dinámicamente, así como asignarlos a la red segura más apropiada.
- Suministrar los recursos correctos a la red para que el sistema IoT funcione de manera adecuada y eficiente. Muchos dispositivos en el sistema IoT aportan información crítica que exige un determinado nivel de calidad del servicio. Por ejemplo, algunos sistemas médicos, como sistemas de imágenes 3D y en color, exigen reservar el ancho de banda adecuado en una infraestructura de red de altas prestaciones para garantizar la prestación y fiabilidad del servicio.
- Proporcionar un entorno seguro frente a ciberataques y pérdida de datos. Debido que los numerosos dispositivos y sensores de la red IoT conllevan un gran número de vectores de ataque potencial, la seguridad es fundamental para aminorar los riesgos de cibercrimen. La seguridad es necesaria a múltiples niveles, incluyendo el confinamiento de las propias redes IoT.

Los profesionales de TI tienen previsto potenciar IoT

Los profesionales de TI en diversos sectores ya tienen previsto potenciar el uso de soluciones IoT en el próximo futuro. De acuerdo con el estudio de 451 Research sobre tendencias en Internet de las Cosas, un 67% de los profesionales de TI que respondieron al cuestionario dijeron que sus compañías ya han implementado una solución IoT o tenían un sistema IoT en fase de pruebas. Un 21% de los encuestados dijeron que sus compañías prevén implementar soluciones IoT en los próximos 12 meses, y un 11% afirma que sus compañías planean implementar IoT en un plazo superior a un año.

IoT acrecienta la exposición de las organizaciones a ciberdelitos

El crecimiento de IoT también conlleva una explosión de las amenazas de ciberseguridad ya que la proliferación de sensores y dispositivos conectados aumenta enormemente la exposición de la red a ataques. IoT es especialmente susceptible ya que muchos dispositivos IoT se fabrican sin tener en cuenta la seguridad, o bien son construidos por compañías que no comprenden los actuales requisitos de seguridad. En consecuencia, los sistemas IoT se han ido convirtiendo en el eslabón débil para la ciberseguridad en hospitales, clínicas y centros sanitarios.



- El ataque del ransomware WannaCry em mayo de 2017, perpetrado en redes de hospitales europeos y norteamericanos, suspendió la atención y los tratamientos médicos durante varios días en dieciséis hospitales públicos de Gran Bretaña.[1]
- St. Jude Medical, un fabricante de marcapasos, desfibriladores y otros dispositivos cardíacos, se vio forzado a introducir parches en el software de sus dispositivos en febrero de 2017 cuando se informó que los dispositivos implantables fabricados por la compañía eran vulnerables a potenciales ciberataques de tipo catastrófico. Los infiltrados podían aprovechar la vulnerabilidad para cambiar las configuraciones y provocar el mal funcionamiento de los dispositivos cardíacos, así como de alterar el ritmo cardíaco hasta niveles peligrosos, o bien suministrar shocks dañinos. Los ataques, según el informe, estaba al alcance de piratas informáticos con unas habilidades relativamente bajas.[2]
- Johnson & Johnson advirtió a los clientes sobre una vulnerabilidad de la seguridad en una de sus bombas de insulina conectadas en 2016, que los piratas informáticos pudieron explotar para suministrar sobredosis de insulina a pacientes diabéticos.[3]

El ciberataque MedJack permitió que los piratas informáticos introdujeran malware en dispositivos médicos, que a continuación distribuyeron por la infraestructura de la red sanitaria. Los datos médicos robados en este tipo de ataques se utilizó para fraude fiscal o robos de identidad, e incluso para el seguimiento de recetas de medicamentos, permitiendo así que los piratas realizaran pedidos de medicamentos en línea para venderlos en la web oscura.[4]

Construcción de una infraestructura segura de la red IoT para sanidad

La protección del tráfico y los dispositivos de IoT es un desafío que no se puede superar con una sola tecnología de seguridad. Exige un enfoque estratégico que aproveche diversas protecciones de seguridad.

Para ayudar a las organizaciones sanitarias a aprovechar las ventajas y a mitigar los riesgos de la implantación de IoT, Alcatel-Lucent Enterprise (ALE) proporciona una estrategia de seguridad multinivel. La estrategia de ALE ofrece protección en cada capa de la infraestructura, desde cada usuario y cada dispositivo hasta la propia capa de la red. También proporciona una estrategia de confinamiento de IoT para simplificar y proteger la incorporación de dispositivos y suministrar los recursos adecuados a la red para el funcionamiento correcto y eficiente del sistema, todo ello en un entorno seguro que proteja a las organizaciones frente a ciberataques.

Confinamiento de IoT

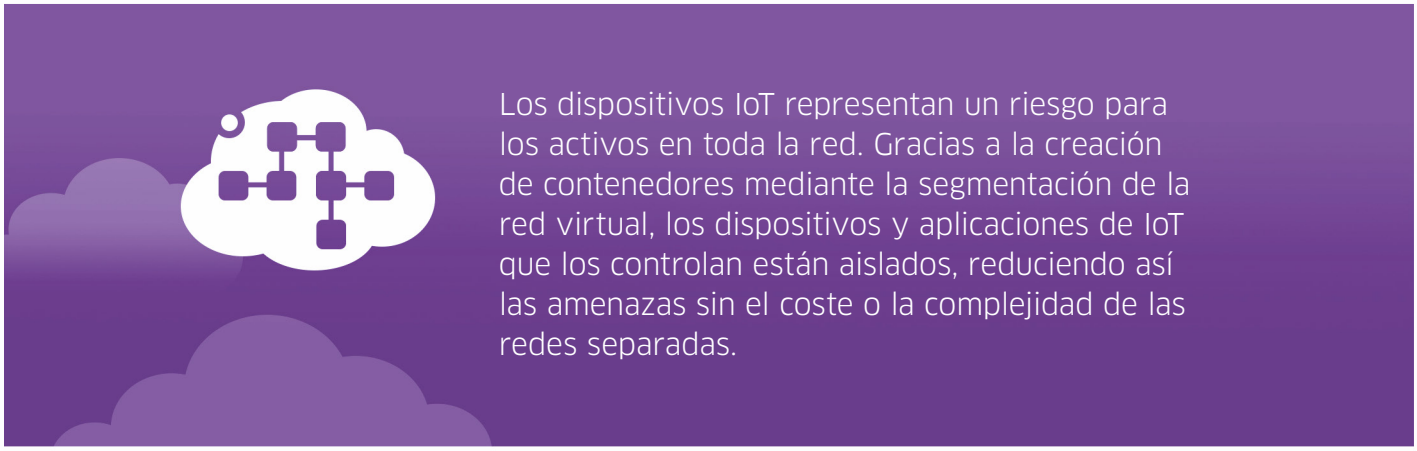
Para permitir el confinamiento de IoT, todos los usuarios, dispositivos y aplicaciones de la red de ALE son perfiles asignados. Estos perfiles, que definen funciones, autorizaciones de acceso, niveles de calidad de servicio y otro tipo de información relacionada, se transmite a todos los conmutadores y puntos de acceso de la red.

- Los dispositivos se encuentran en “contenedores virtuales”, que aplican técnicas de virtualización de la red de manera que diversos dispositivos y redes pueden utilizar la misma infraestructura física mientras permanecen aislados del resto de la red.
- En estos contenedores virtuales se aplican normas de calidad de servicio y seguridad.
- Al dividir la red mediante contenedores virtuales, si se produce una brecha en una parte de la red virtual ello no afecta a otros dispositivos o aplicaciones en otras redes virtuales.
- Cuando se conecta un nuevo dispositivo IoT, la red reconoce automáticamente su perfil y asigna al dispositivo al entorno virtual apropiado.
- La comunicación se limita a los dispositivos de este entorno virtual y a la aplicación en el centro de datos que controla estos dispositivos.
- Debido a que todos los usuarios también tienen perfiles dentro de la red de ALE, el acceso a los contenedores virtuales de IoT se pueden limitar a las personas y grupos autorizados.

Máxima seguridad

Además del confinamiento de IoT, las tecnologías de red de ALE proporcionan seguridad por capas en varios niveles de la red.

- Al nivel del usuario, los perfiles aseguran que los usuarios obtengan la autenticación y autorización con los derechos de acceso apropiados.
- Al nivel del dispositivo, la red asegura que los dispositivos tengan autenticación y cumplan las normas de seguridad establecidas.
- Al nivel de la aplicación, la red puede establecer normas relativas a cada aplicación o grupo de aplicaciones, como bloqueo, máximo ancho de banda y control de quien accede a cada aplicación.
- Al nivel de la red, los conmutadores de ALE aprovechan las ventajas de un código diversificado y seguro. Éste protege las redes frente a vulnerabilidades intrínsecas, código oculto, malware embebido y potenciales puertas traseras que puedan afectar a conmutadores, enrutadores y otro hardware de misión crítica.
- El análisis inteligente de ALE utiliza inspección avanzada de paquetes y otras tecnologías para detectar el tipo de datos y aplicaciones que se mueven por la red, posibilitando así la identificación de patrones inusuales de tráfico en la red y actividad no autorizada.



Gestión operativa y de la red de extremo a extremo

Las soluciones de ALE para redes también ofrecen ventajas significativas de tipo operativo y para su gestión a las operaciones en el sector sanitario.

- ALE permite el funcionamiento de varias redes virtuales separadas como una sola infraestructura, lo cual supone un ahorro de gasto de capital en varias infraestructuras físicas.
- La solución ALE Unified Access permite el funcionamiento conjunto de redes cableadas e inalámbricas como una sola red robusta, con un conjunto común de servicios de red, un marco normativo común, una técnica común de autenticación y una sola base de datos de autenticación.
- Las soluciones de ALE para redes también tienen un solo sistema de gestión para todos los elementos de la infraestructura, incluyendo la gestión unificada de redes LAN y WLAN. El paquete de gestión Alcatel-Lucent OmniVista® 2500 proporciona un solo panel para gestionar entornos virtuales, conmutadores, puntos de acceso y otros componentes de la red. La gestión de la red también se encuentra disponible «como servicio» con OmniVista Cirrus, una solución de gestión de la red basada en la nube de ALE.

Gama para redes de altas prestaciones

Los conmutadores, puntos de acceso y controladores de ALE ofrecen capacidades de elevado ancho de banda y baja latencia de última generación y pueden gestionar un gran número de dispositivos en entornos de alta densidad. Los productos y soluciones para redes de ALE pueden cubrir la necesidades de las redes en organizaciones sanitarias de cualquier tamaño. ALE también suministra una selección de conmutadores, puntos de acceso y enrutadores robustos para el despliegue de redes en el exterior o en los entornos adversos en los que trabajan los equipos médicos de ambulancias y urgencias.

Ya están aquí las redes y las estrategias para una IoT segura

Los productos y soluciones de ALE constituyen la base de una red segura para ayudar a hospitales, clínicas y centros sanitarios a implementar sistemas IoT que puedan crear nuevos métodos para optimizar productos y procesos, ahorrar tiempo al personal, lograr que los flujos de trabajo sean más eficientes y mejorar las experiencias de los pacientes. El confinamiento de IoT de ALE y las estrategias de seguridad por capas reducen los riesgos y simplifican la configuración de las redes IoT al facilitar la incorporación de dispositivos, proporcionando así un funcionamiento más eficiente y una enorme mejora de la seguridad. ALE ayuda a las organizaciones a aprovechar al máximo las ventajas de IoT a través de mayores niveles de inteligencia, automatización y seguridad de la red.

¿Desea más información?

Para más información sobre las soluciones IoT de ALE, visite Seguridad de IoT de ALE.

Sanidad conectada

«En Alcatel-Lucent Enterprise le ayudamos a conectar a sus pacientes, su personal y su ecosistema sanitario. Suministramos una tecnología que funciona, en todas sus instalaciones y más allá. Con una cobertura global y un enfoque local, suministramos redes y comunicaciones especializadas para sanidad con el fin de optimizar la atención sanitaria y los resultados para el paciente.»

1 Hacked Cameras Were Behind Friday's Massive Web Outage
2 St. Jude Patches Additional Cardiac Device
3 J&J warns diabetic patients: Insulin pump vulnerable to hacking
4 Medical Devices Are the Next Security Nightmare

www.al-enterprise.com/es-es El nombre y el logotipo Alcatel-Lucent son marcas registradas de Nokia que se usan bajo licencia por ALE. Para saber de otras marcas utilizadas por las empresas filiales de ALE holding, visite: https://www.al-enterprise.com/es-es/legal/marcas-comerciales-copyright. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios. La información incluida puede modificarse sin previo aviso. ALE Holding no asume ninguna responsabilidad por las posibles inexactitudes del contenido. © 2019 ALE International. Todos los derechos reservados. 00030918ES (Diciembre 2019)