El Internet de las cosas en la empresa

Construir una base segura para aprovechar las oportunidades del IoT en la empresa

Resumen de la solución

Alcatel·Lucent Enterprise

El IoT cambia en esencia la ecuación empresarial

El Internet de las cosas (IoT) tiene el potencial para transformar la empresa modificando profundamente la forma en que las organizaciones recopilan datos e información, reuniendo las principales tendencias técnicas y comerciales de la movilidad, la automatización y el análisis de datos. El IoT hace referencia a la puesta en red de objetos físicos, mediante sensores, accionadores y otros dispositivos incorporados que pueden recabar y transmitir información sobre la actividad en tiempo real dentro de la red. Los datos acumulados a partir de estos dispositivos podrán ser analizados por tanto por la organización para:

- **Optimizar los productos y procesos,** reduciendo los costes de explotación, aumentando la productividad y desarrollando nuevos productos y servicios
- **Conocer mejor las necesidades y preferencias de los clientes,** permitiendo a las empresas ofrecer productos y servicios más personalizados
- **Hacer que las empresas sean más inteligentes y eficientes,** supervisando de forma proactiva las infraestructuras críticas y creando procesos más eficientes
- **Mejorar las experiencias de los usuarios,** ofreciendo productos y servicios nuevos o mejorados para diferenciar de la competencia un negocio

El despliegue del IoT sigue creciendo

Los profesionales de TI de una variedad de sectores ya planean aumentar el uso de soluciones de IoT en un futuro próximo. En 2022, se espera que el mercado del Internet de las cosas crezca un 18 % hasta alcanzar los 14 400 millones de conexiones activas. Se prevé que para 2025, a medida que se reduzcan las limitaciones de la oferta y se acelere el crecimiento, habrá aproximadamente 27 000 millones de dispositivos de IoT conectados.

Fuente https://iot-analytics.com/number-connected-iot-devices

Desafíos del despliegue del IoT

basado en datos El IoT aporta flujos de datos sin precedentes, lo que plantea retos de rendimiento, funcionamiento y gestión a la infraestructura de red, además de mayores riesgos de seguridad desde todos los puntos de conexión. Para hacer frente a estos problemas, las organizaciones deben adaptar los diseños de red tradicionales para ofrecer nuevos niveles de inteligencia, automatización y seguridad de la red.

Las organizaciones necesitan una infraestructura de red rentable que pueda manejar con seguridad enormes flujos de datos, pero que también sea sencilla de gestionar y operar. La infraestructura debe:

- **Proporcionar un proceso sencillo y automatizado para la incorporación de dispositivos de IoT.** Los grandes sistemas de IoT pueden contener miles de dispositivos o sensores, y el aprovisionamiento y la gestión manuales de todos estos puntos de conexión son complejos y propensos a errores. La incorporación automática permite a la infraestructura de red reconocer dinámicamente los dispositivos y asignarlos a la red segura apropiada.
- **Suministrar los recursos de red correctos para que el sistema de IoT funcione de forma adecuada y eficiente.** Muchos dispositivos del sistema de IoT ofrecen información esencial que requiere un nivel específico de calidad de servicio (QoS). Por ejemplo, algunos casos de uso requieren reservas adecuadas de ancho de banda en una infraestructura de red de alto rendimiento para garantizar la fiabilidad y la prestación de servicios.
- **Proporcionar un entorno seguro contra los ciberataques y la pérdida de datos.** Dado que la gran cantidad de dispositivos y sensores conectados en red en el IoT provoca la correspondiente abundancia de posibles vectores de ataque, la seguridad es fundamental para mitigar los riesgos de la ciberdelincuencia. La seguridad es necesaria en múltiples niveles, incluida la segmentación de las propias redes de IoT.

El IoT acrecenta la exposición a la ciberdelincuencia

El crecimiento del IoT conlleva también una explosión de amenazas de ciberseguridad, ya que la proliferación de sensores y dispositivos conectados amplía enormemente la superficie de ataque de la red. El IoT es especialmente susceptible, ya que muchos dispositivos de IoT se fabrican sin tener en cuenta la seguridad o son creados por empresas que no entienden los requisitos de seguridad actuales. En consecuencia, los sistemas de IoT son cada vez más el eslabón más débil en la seguridad de la empresa.

Steve Turner, analista de Forrester, dijo que su propia investigación indicó la existencia de una distribución relativamente uniforme de los ataques de rescate en los sectores verticales. Sin embargo, los incidentes de ransomware en determinados sectores, como las infraestructuras críticas y la sanidad, suelen ser los que más titulares generan.[1]

Los dispositivos de IoT representan riesgos para los activos en toda la red. Al establecer segmentos mediante la segmentación de red virtual, las aplicaciones y los dispositivos de IoT que los controlan están aislados, con lo que se reducen las amenazas sin el coste o la complejidad de redes separadas.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Cómo crear una infraestructura de red segura de IoT

Proteger el tráfico y los dispositivos de IoT es un reto que no puede resolver ninguna tecnología de seguridad por sí sola. Requiere un enfoque estratégico que aproveche las múltiples garantías de seguridad.

Para ayudar a las organizaciones a aprovechar las ventajas y mitigar los riesgos del despliegue del IoT, Alcatel-Lucent Enterprise (ALE) ofrece una estrategia de red de confianza cero con seguridad multinivel.

La estrategia de ALE ofrece protección en cada capa de la infraestructura, desde cada uno de los usuarios y dispositivos hasta la propia capa de la red. La macrosegmentación y microsegmentación de la red garantiza un forma sencilla y segura de incorporar dispositivos y ofrecer los recursos de red adecuados para que el sistema funcione de forma correcta y eficiente, todo ello en un entorno seguro para proteger las organizaciones frente a los ciberataques.

Segmentación del IoT

Para posibilitar la segmentación del IoT, se asignan perfiles a todos los usuarios, dispositivos y aplicaciones de la red de ALE. Estos perfiles, que definen las funciones, las autorizaciones de acceso, los niveles de calidad de servicio y otra información sobre directivas, se transmiten a todos los conmutadores y puntos de acceso de la red.

- Con la macrosegmemtación, los dispositivos se colocan en "segmentos virtuales" mediante técnicas de virtualización de redes que permiten que múltiples dispositivos y redes utilicen la misma infraestructura física y permanezcan aislados del resto de la red
- Con la microsegmentación, se pueden aplicar diferentes reglas de calidad de servicio y seguridad a los dispositivos dentro de cada segmento virtual. Esto añade una mayor granularidad y aumenta la seguridad de la red, impidiendo que diferentes tipos de dispositivos del mismo segmento interactúen entre sí cuando no están pensados para ello.
- Al segregar la red con la macrosegmentación y microsegmentación, si un dispositivo se ve comprometido en una parte de la red, la infracción no solo no afecta a los dispositivos o aplicaciones de otros segmentos virtuales, sino que no puede propagarse dentro del segmento afectado a otros tipos de dispositivos
- Cuando se conecta un nuevo dispositivo de IoT, la red reconoce automáticamente su perfil y asigna el dispositivo al entorno virtual correspondiente
- La comunicación se limita a los dispositivos dentro de ese entorno virtual y a la aplicación en el centro de datos que controla estos dispositivos
- Dado que todos los usuarios también tienen perfiles en la red de ALE, el acceso a los segmentos virtuales de IoT puede limitarse a las personas y grupos autorizados

Seguridad a fondo

- Además de la contención de IoT, las tecnologías de redes de ALE proporcionan seguridad por capas en varios niveles de la red
- A nivel de usuario, los perfiles garantizan que los usuarios estén autenticados y autorizados con los derechos de acceso adecuados
- A nivel de dispositivo, la red garantiza que los dispositivos estén autenticados y cumplan las reglas de seguridad establecidas
- A nivel de aplicación, la red puede establecer reglas relativas a cada aplicación o grupo de aplicaciones, como el bloqueo, la limitación del ancho de banda y el control de quién puede acceder a qué aplicaciones
- A nivel de red, los conmutadores ALE se benefician de un código seguro y diversificado. Protege las redes frente a vulnerabilidades intrínsecas, uso indebido de códigos, malware integrado y posibles puertas traseras que podrían poner en peligro los conmutadores, enrutadores y otros equipos fundamentales.
- El análisis inteligente de ALE utiliza la inspección pormenorizada de paquetes y otras tecnologías para detectar el tipo de datos y aplicaciones que se mueven a través de la red, lo que permite identificar patrones inusuales de tráfico en la red, actividad no autorizada e intrusiones en la red

Gestión de red y operativa de extremo a extremo

Las soluciones de red de Alcatel-Lucent Enterprise también proporcionan importantes ventajas operativas y de gestión.

- ALE permite que varias redes virtuales independientes funcionen en una única infraestructura común, lo que elimina la necesidad de invertir gastos de capital en varias infraestructuras físicas
- La solución de acceso unificado de ALE permite que las tecnologías alámbricas e inalámbricas funcionen juntas como una red única y sólida, con un conjunto común de servicios de red, un marco de directivas, un esquema de autenticación común y una única base de datos de autenticación
- Las soluciones de red de Alcatel-Lucent Enterprise también cuentan con un único sistema de gestión para todos los elementos de la infraestructura, incluida la gestión unificada de las redes LAN por cable y WLAN inalámbricas. El sistema de gestión de red Alcatel-Lucent OmniVista® 2500 y la gestión de red como servicio Alcatel-Lucent OmniVista® Cirrus para la gestión basada en la nube proporcionan un panel de vista única para gestionar entornos virtuales, conmutadores, puntos de acceso y todos los demás componentes de la red.

Una cartera de redes de alto rendimiento

Los conmutadores, puntos de acceso y controladores de ALE son compatibles con la última generación de capacidades de gran ancho de banda y baja latencia; además, pueden gestionar un gran número de dispositivos en entornos de alta densidad. Los productos y soluciones de red de ALE satisfacen las necesidades de red de organizaciones de todos los tamaños. ALE también ofrece una selección de conmutadores, puntos de acceso y enrutadores robustos para la implantación de redes en exteriores o en entornos hostiles.

Escenarios de IoT en sectores clave

Las soluciones de IoT prometen hacer que las organizaciones sean más inteligentes y tengan más éxito en lo que hacen. Estas ventajas son especialmente notables en determinados sectores verticales.

Sanidad

El IoT tiene el potencial de transformar la atención sanitaria modificando profundamente el modo en que los hospitales, las clínicas y otros centros sanitarios recopilan y utilizan los datos, reuniendo las principales tendencias técnicas y comerciales de la movilidad, la automatización y el análisis de datos para mejorar los cuidados al paciente. Los datos acumulados a partir de estos dispositivos podrán ser analizados por tanto por la organización para:

- Mejorar la atención al paciente, ofreciendo servicios y cuidados nuevos o mejorados que ayuden a diferenciar una organización sanitaria basada en datos
- Optimizar los procesos, desarrollando nuevos servicios, flujos de trabajo y soluciones que aumenten la eficacia y reduzcan los costes de explotación
- Conocer mejor las necesidades y preferencias de los pacientes, permitiendo a las organizaciones sanitarias ofrecer una atención y experiencias más personalizadas
- Hacer que las redes de los hospitales sean más inteligentes, supervisando de forma proactiva las infraestructuras críticas y automatizando la implementación y gestión de la infraestructura informática

El crecimiento del IoT en el sector sanitario también trae consigo una explosión de amenazas de ciberseguridad, ya que la proliferación de sensores y dispositivos conectados amplía enormemente la superficie de ataque de la red. El IoT del sector sanitario es especialmente susceptible, ya que muchos dispositivos de IoT se fabrican sin tener en cuenta la seguridad o son creados por empresas que no entienden los requisitos de seguridad actuales. En consecuencia, los sistemas de IoT pueden representar potencialmente el eslabón más débil de la ciberseguridad de hospitales, clínicas y centros sanitarios.

Educación

Las instituciones educativas no son una excepción en el mundo omnipresente del IoT; un mundo en el que las tecnologías se diseñan para todo tipo de producto imaginable. El IoT ofrece numerosas ventajas a universidades y colegios, dando muestras de una nueva generación de cosas inteligentes que pueden mejorar tremendamente la experiencia de aprendizaje y la seguridad y protección del campus. Los dispositivos de IoT, pequeños como un sensor de luz o grandes como las pizarras inteligentes, suponen cambios importantes en la gestión de los entornos académicos y en la forma de aprender de los alumnos. Los dispositivos de IoT:

- Crean nuevas formas de aprendizaje para los estudiantes favoreciendo experiencias de aprendizaje más personalizadas y dinámicas, como los libros de texto digitales inmersivos y el aprendizaje basado en juegos
- Modifican el modo en que los profesores imparten las clases y evalúan el rendimiento con equipos audiovisuales inteligentes, grabadoras de vídeo digitales para la captura de las clases y exámenes en línea
- Simplifican las operaciones para los administradores escolares supervisando de forma proactiva las infraestructuras críticas y creando procesos más eficientes y rentables para la gestión del sistema de HVAC, la iluminación y el entorno
- Ofrecen un entorno más seguro para alumnos y profesores con cámaras de vigilancia digital, cerraduras de puertas inteligentes y autobuses escolares conectados

En estos colegios y universidades

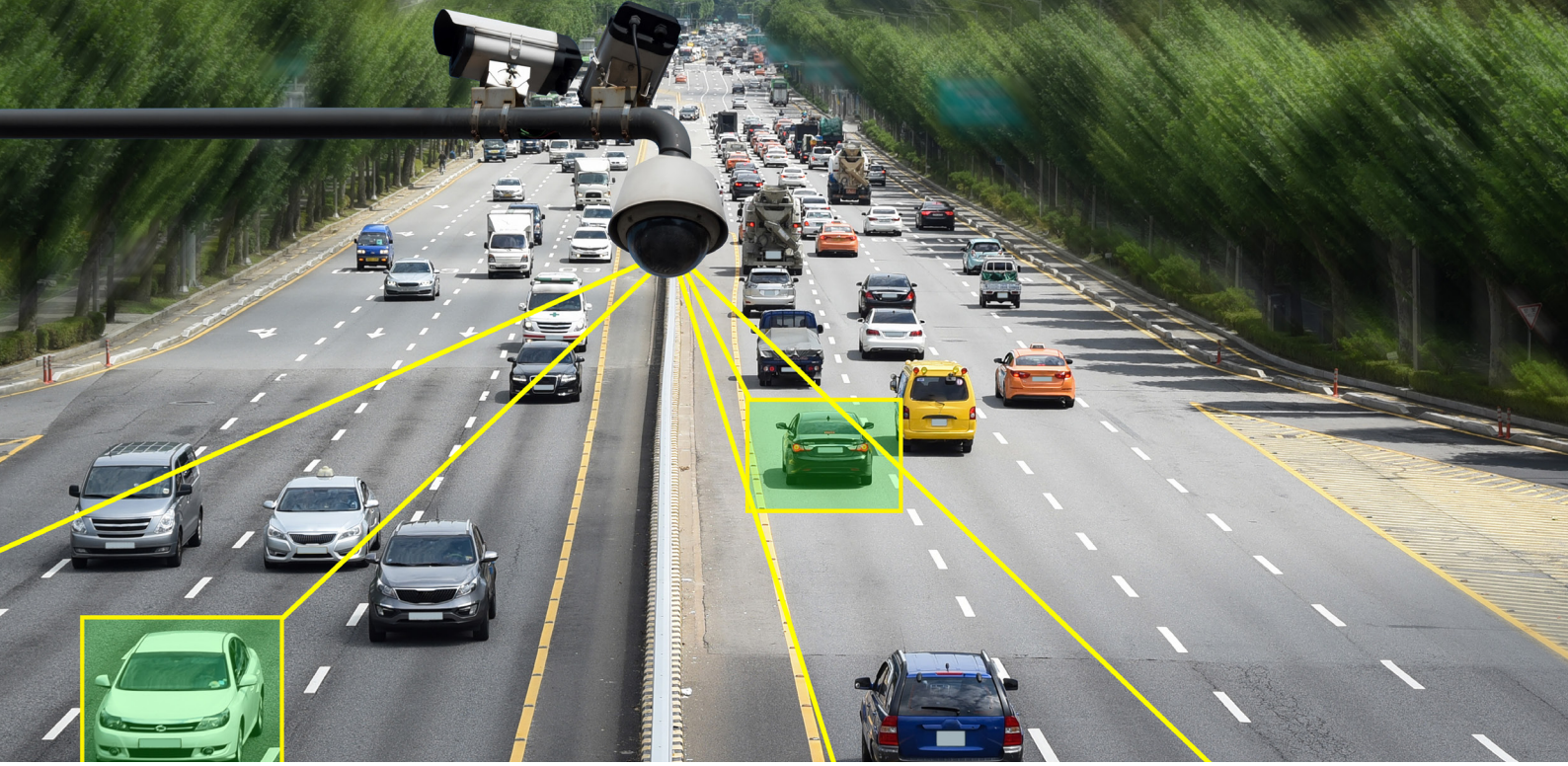
remodelados, los administradores pueden recabar, almacenar y analizar enormes cantidades de datos sobre el entorno y el rendimiento de los alumnos. Esto dotará a los centros educativos de la inteligencia que necesitan para mejorar los procesos encaminados al éxito académico y les permitirá identificar las deficiencias que deben subsanarse.

Estos cambios transformadores acarrean tanto amenazas como oportunidades. Es imprescindible emplear una estrategia de defensa avanzada que proporcione conexiones seguras a los dispositivos de IoT y evite las infracciones que puedan afectar a la privacidad de los datos de los estudiantes y a la seguridad de la investigación o poner en peligro la autenticidad e integridad de los datos.

Administración pública

Administraciones públicas y ayuntamientos se suman a la corriente del IoT. Las ciudades inteligentes presentan una gran oportunidad de negocio y nuevos medios para prestar servicio y proteger a los ciudadanos. En estas ciudades conectadas, las empresas de servicios públicos están fomentando los contadores inteligentes para crear sistemas de precios adaptables; por otro lado, los promotores están instalando sensores y componentes de automatización en los nuevos inmuebles. Los aparcamientos inteligentes ahorran tiempo a los ciudadanos y los hacen más eficientes; además, las papeleras inteligentes dan la voz de alarma cuando están casi llenas. El IoT ayuda a ayuntamientos y otras administraciones públicas a recopilar información sobre la movilidad y las tendencias de datos que proporcionan análisis críticos vitales para formular la estrategia urbana y planificar a largo plazo. El IoT aporta:

- Ciudadanos mejor conectados y contribuye a que las entidades públicas ofrezcan servicios y recursos de alta calidad, seguros y eficaces que mejoren la interacción y confianza entre la administración y la población aumentando la habitabilidad, la capacidad de trabajo y la sostenibilidad
- Mayor seguridad en el tránsito al comprender mejor el funcionamiento del sistema de transporte gracias a los datos de los sensores que lo rastrean todo, desde anomalías en la velocidad de los trenes ligeros hasta la temperatura de las carreteras y la ubicación en tiempo real de los autobuses de transporte colectivo
- Reducción de la congestión y el consumo de energía mediante tecnologías de ciudad inteligente que aprovechan los datos en tiempo real para mejorar la forma en que los funcionarios ajustan los recursos para satisfacer las demandas; también proporcionan la agilidad para reaccionar rápidamente a los patrones de tráfico en continuo cambio, las variaciones en el consumo de agua o energía o los cambios en la calidad del aire
- Mejora del rendimiento operativo y del mantenimiento mediante la supervisión proactiva de las infraestructuras públicas críticas y la creación de procesos más eficientes para reducir los costes operativos y mejorar la capacidad del sistema
- Mejora de la seguridad pública al responder de forma más rápida y eficaz a las emergencias Sin embargo, el listón de la ciberseguridad debe estar alto, muy alto. En las ciudades del IoT, donde no todas las aplicaciones, sensores y dispositivos están diseñados teniendo en cuenta la seguridad, se necesita una infraestructura inteligente y automatizada que pueda poner estos dispositivos en categorías separadas y evitar que hablen con lo que no deben hablar. Esta contenedorización mejorará significativamente la seguridad y pondrá a la entidad del sector público en el camino correcto para avanzar hacia un entorno de confianza cero, creando múltiples capas de protección en una estrategia cibernética de defensa exhaustiva.



Transporte

El Internet de las Cosas (IoT) está transformando la industria del transporte, al modificar profundamente la forma en que los sistemas recopilan datos e información combinando la automatización y el análisis de datos. Los sensores, accionadores y otros dispositivos pueden recabar y transmitir información sobre la actividad en tiempo real en la red. Estos datos pueden ser por tanto analizados por las autoridades de transporte para mejorar la experiencia y la seguridad de los viajeros, reducir la congestión y el consumo de energía y, al mismo tiempo, optimizar el rendimiento operativo.

El IoT es el eje de las fuerzas que están remodelando el transporte para ofrecer mayor seguridad, viajes más eficientes, mejor mantenimiento de vehículos y aeronaves y una gestión más estratégica del tráfico. Entre los ejemplos de aplicación del IoT en el transporte destacan los siguientes:

- Eficiencias, para aumentar la capacidad del sistema y mejorar la seguridad y la comodidad de los pasajeros, reduciendo al mismo tiempo costes y riesgos
- Señales de mensajes dinámicos en carretera, para sistemas de transporte inteligentes que muestran en tiempo real el estado de la carretera, las tarifas de peaje, los cierres de carriles y la marcha del tráfico
- Vehículos autónomos, con capacidad para percibir su entorno, predecir su comportamiento, comunicarse con otros vehículos y con su entorno, y reaccionar instantáneamente en determinados contextos viales.
- Videovigilancia, para proteger la circulación de personas y multitudes, para automatizar y proporcionar una detección temprana de comportamientos sospechosos y equipajes abandonados

Los ciberataques pueden afectar a las operaciones diarias durante largos períodos. No solo se interrumpe el servicio, sino que la exposición de datos altamente sensibles es también un gran riesgo cuando se trata de este sector. Si bien algunos ataques de ciberseguridad tienen un fin lucrativo, otros están pensados para causar el caos y el desorden apagando sistemas enteros. La interrupción de los semáforos, el bloqueo del acceso a archivos y datos importantes, la interrupción de los servicios de nómina y la puesta en peligro de las máquinas expendedoras de billetes y los torniquetes son solo algunos de ellos.

- En 2018, Bay & Bay Transportation fue víctima de un ataque masivo de ransomware que bloqueó los sistemas que utiliza para gestionar su flota de 300 camiones
- En 2018, los piratas informáticos apagaron 2000 ordenadores del Departamento de Transporte de Colorado, interrumpiendo las operaciones durante semanas. Más recientemente, los ciberdelincuentes se infiltraron en tres de los 18 sistemas informáticos de la Autoridad Metropolitana del Transporte de Nueva York.
- El primer semestre de 2020 reveló un asombroso aumento de los incidentes de ransomware, con un incremento global del 715 % interanual
- En 2020, se robaron las direcciones de correo electrónico y los datos de viaje de nueve millones de clientes de EasyJet. De ellos, 2208 vieron comprometida la información de sus tarjetas de crédito. Este ciberataque, junto con el golpe de la pandemia mundial, hizo que la aerolínea perdiera el 45 % de su valor en acciones y registrara su primera pérdida anual en sus 25 años de existencia.

Las redes y estrategias seguras de IoT ya están aquí

Los productos y soluciones de ALE construyen una base de red segura para ayudar a las organizaciones a desplegar sistemas de IoT que puedan revelar la información necesaria para optimizar productos y procesos, hacer que las empresas sean más inteligentes y eficientes y ofrecer mejores experiencias a los clientes. Las estrategias de contención de IoT y de seguridad en capas de Alcatel-Lucent Enterprise reducen los riesgos y simplifican la configuración de las redes de IoT facilitando la integración de dispositivos, proporcionando operaciones más eficientes y aumentando considerablemente la seguridad. ALE ayuda a las organizaciones a aprovechar todo el potencial del IoT proporcionando niveles reforzados de automatización, seguridad e inteligencia de red.

¿Desea obtener más información?

Para obtener más información sobre las soluciones de IoT de Alcatel-Lucent Enterprise, visite Seguridad de IoT de ALE.

Alcatel·Lucent Enterprise