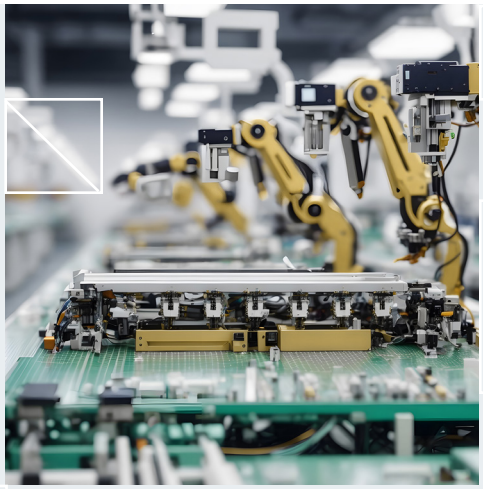


LIBRO ELECTRÓNICO

CONFIANZA DE LOS DISPOSITIVOS: UN CONCEPTO CLAVE PARA PROTEGER EL FUTURO DE LA TECNOLOGÍA INTELIGENTE

digicert®

ÍNDICE

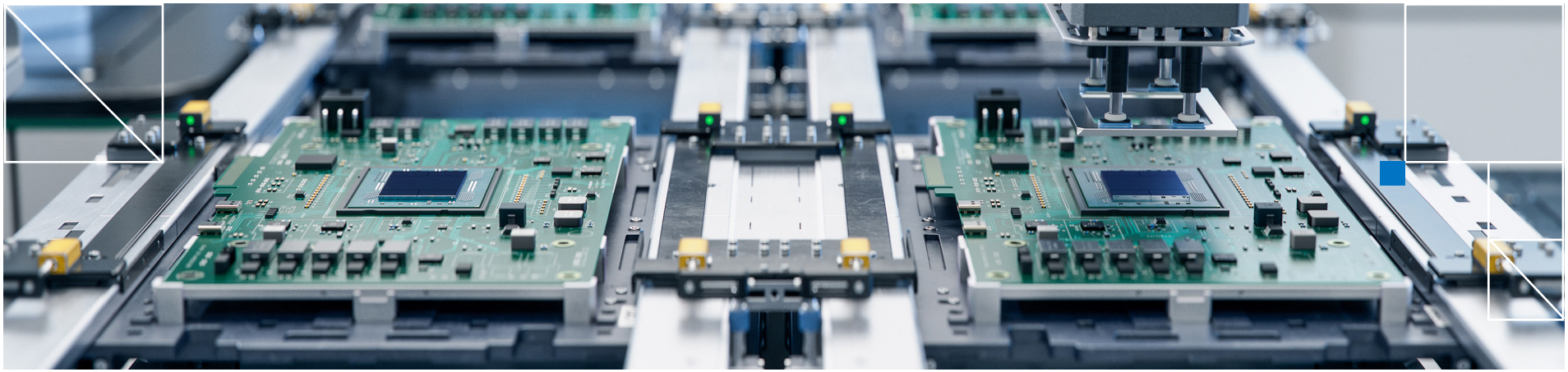
© 2023 DigiCert, Inc. Todos los derechos reservados. DigiCert es una marca registrada de DigiCert, Inc. en los Estados Unidos y otros lugares. El resto de las marcas comerciales y marcas registradas pertenecen a sus respectivos propietarios.

LA PROMESA Y EL PELIGRO DE UN MUNDO CADA VEZ MÁS CONECTADO

La creciente conectividad del mundo actual ha desplegado ante nosotros un panorama repleto de oportunidades, pero también de vulnerabilidades. Los peligros a los que se enfrenta el mercado de los dispositivos conectados evolucionan tan rápido como la tecnología, lo que supone una amenaza para los usuarios individuales y para la integridad de redes enteras.

La existencia de una mayor cantidad de dispositivos implica un aumento en el número de vectores de ataque. Una única filtración de datos puede causar una enorme pérdida de datos y dinero que acabe repercutiendo en la confianza de los clientes y haga tambalearse los cimientos de empresas de cualquier tamaño. Además, mientras los fabricantes y los desarrolladores saquen provecho del ansia de conectividad de los consumidores, aquellos que resten importancia a la seguridad seguirán alimentando el floreciente negocio de las filtraciones de datos de dispositivos, un mercado ilegal que se espera que reporte 10 billones de dólares a los atacantes en 2025.

Por lo tanto, la pregunta que debe hacerse no es si puede permitirse invertir en la seguridad de sus dispositivos, sino si puede permitirse no hacerlo. La confianza de los dispositivos ha dejado de ser una función y se ha convertido en una necesidad. Los cuatro aspectos clave que indicamos a continuación le ayudarán a enfrentarse a los atacantes y a diferenciarse del resto de la competencia.



CAPÍTULO 1

MARKETING CENTRADO EN LA SEGURIDAD

Los fabricantes de dispositivos conectados son cada vez más conscientes de la importancia de la seguridad y reconocen la necesidad de una defensa sólida que sea capaz de detener una creciente variedad de amenazas y cubra aspectos como la identidad, la protección frente a la manipulación y el cumplimiento normativo.

Implementación de una identidad digital inmutable

Un dispositivo será de confianza si su identidad está protegida desde el momento de su creación y, por tanto, puede garantizarse su integridad durante todas las etapas de su ciclo de vida. Las identidades inmutables ofrecen protección frente a diferentes ataques y proporcionan una base segura que refuerza el proceso de fabricación de principio a fin.

Integración de la protección frente a la manipulación

Una buena protección frente a la manipulación es importante porque impedirá que se produzcan modificaciones no autorizadas que puedan poner en riesgo tanto a dispositivos individuales como a redes enteras. La confianza de los dispositivos integra en estos la protección frente a la manipulación mediante varias capas de seguridad, como anclas de confianza de hardware y procesos de arranque seguro. Estas funciones sirven como elemento disuasorio contra la manipulación física y protegen la integridad del software del dispositivo, así como la propiedad intelectual del fabricante y los datos del usuario.

Adhesión a los estándares globales de cumplimiento normativo

La confianza de los dispositivos ayuda a cumplir la normativa, por difícil que sea, mediante funciones que ayudan a los fabricantes a adherirse a los protocolos de seguridad internacionales. Con plantillas de cumplimiento predefinidas que se ajustan a las normativas y otras medidas, se puede reducir el riesgo de cometer errores relacionados con el incumplimiento.

Marketing centrado en la seguridad aplicado al mundo real

La eficacia de estas medidas de seguridad ya se ha demostrado mediante aplicaciones prácticas, como las que se indican a continuación:

- Una empresa de electrónica utilizó la confianza de los dispositivos para integrar identidades inalterables en sus productos de domótica. De esta manera, logró garantizar la autenticidad y la protección del origen y las actualizaciones del firmware de cada dispositivo desde la fase de producción hasta el uso por parte del cliente.
- Un fabricante de sensores industriales usó funciones de protección frente a la manipulación para proteger los dispositivos que operan en infraestructuras esenciales, con lo que mejoró la resiliencia de sus productos.
- La confianza de los dispositivos permitió a un fabricante internacional de electrodomésticos abordar el complejo entramado de leyes sobre privacidad de los datos en diferentes regiones. Al adaptar los perfiles de seguridad a los distintos mercados, la empresa se aseguró de que todos los dispositivos cumplieran con los estándares locales sin que fuera necesario rediseñarlos y, de ese modo, ahorró tiempo y recursos.

La confianza de los dispositivos ofrece un completo marco de seguridad que se aplica desde la concepción de cada dispositivo conectado. Al integrar las identidades inmutables, garantizar la protección frente a la manipulación y facilitar el cumplimiento normativo a nivel global, refuerza el proceso de fabricación y mejora la confianza que tienen los usuarios en los dispositivos *in situ*.

CAPÍTULO 2

FABRICACIÓN ÁGIL

Las opciones de implementación flexible se han convertido en un elemento clave para obtener la agilidad que exige el vertiginoso mundo de los dispositivos conectados, ya que permiten a los fabricantes adaptarse a diferentes entornos y requisitos con rapidez y eficacia. La capacidad de implantar medidas de seguridad que no se vean limitadas por un enfoque estándar permite diseñar una estrategia de seguridad personalizada que se adapte al modelo único de cada entorno de fabricación. Además de adaptarse a diferentes espacios físicos, esta flexibilidad también da cabida a las distintas circunstancias tecnológicas con las que tienen que lidiar los fabricantes.

Adhesión a distintas leyes regionales de protección de datos

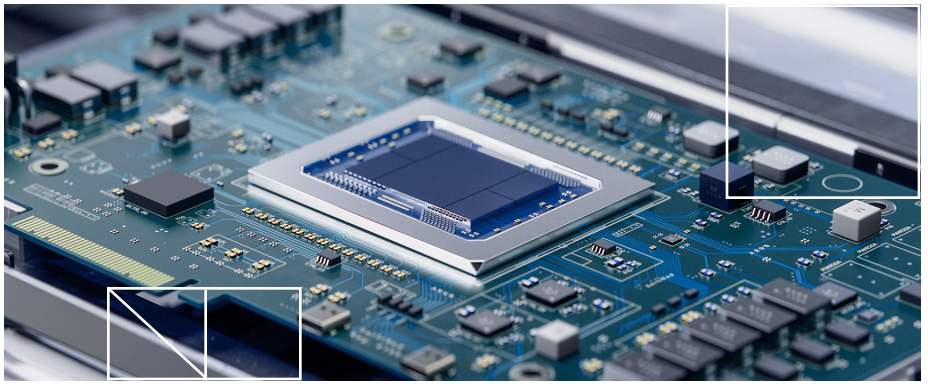
Uno de los principales desafíos que los fabricantes deben abordar a escala global es mantener un mismo estándar de seguridad que también se adhiera a las distintas leyes regionales de protección de datos. Para ir ampliando las operaciones a nivel internacional, es necesario orquestar las prácticas de seguridad minuciosamente y asegurarse de que respeten con las diferentes normativas de cumplimiento normativo de cada región, sin mermar por ello la velocidad y la escalabilidad de la implementación.

Por lo tanto, los fabricantes deben utilizar una solución de seguridad que proporcione las herramientas necesarias para ampliar las operaciones, en lugar de aplicar un marco rígido. De esa forma, garantizarán el crecimiento de su presencia global sin comprometer la seguridad de sus dispositivos.

Adopción de un enfoque equilibrado con respecto a la disponibilidad de la memoria y los recursos de los dispositivos

Los dispositivos del Internet de las cosas (IoT, por sus siglas en inglés) presentan una gran variedad de requisitos de recursos y memoria, por lo que es indispensable contar con una solución de seguridad que se adapte a los recursos. Del mismo modo que un dispositivo con una capacidad limitada de memoria o potencia de procesamiento puede provocar problemas en un sistema de seguridad que consuma muchos recursos, un sistema demasiado básico puede quedarse corto y no ofrecer la protección adecuada en los dispositivos más potentes.

Es necesario adoptar un enfoque equilibrado que se ajuste al perfil de recursos de cada dispositivo y que ofrezca una seguridad óptima sin generar una sobrecarga innecesaria. Esta adaptabilidad es clave para asegurarse de que la seguridad sea lo suficientemente sólida para los dispositivos más exigentes y lo suficientemente eficiente sin que se despilfarren recursos en el caso de los dispositivos con características más limitadas.



Al integrar estos principios de implementación flexible en sus procesos de fabricación, las empresas pueden abordar las complejidades del IoT moderno con confianza.

Fabricación ágil en entornos IoT reales

Las aplicaciones prácticas de los procesos de fabricación que integran estos principios demuestran su eficacia:

- Una empresa de artículos electrónicos de consumo empleó soluciones de seguridad flexibles y escalables para gestionar una gran variedad de productos, desde televisores inteligentes de gama alta hasta dispositivos IoT básicos para el hogar. La posibilidad de adaptar las medidas de seguridad a las capacidades de cada producto y los requisitos del mercado fue fundamental para que la implantación global de la empresa tuviera éxito.
- En el sector industrial, una empresa que produce sensores para la agricultura inteligente siguió estos principios para gestionar dispositivos implantados en diferentes continentes, cada uno con sus propias condiciones medioambientales y requisitos normativos. Gracias a la solución de seguridad y su capacidad para adaptarse a los recursos, la empresa se aseguró de que los dispositivos con capacidades informáticas mínimas pudiesen funcionar de forma segura, incluso en entornos lejanos y con recursos limitados.

Al integrar estos principios de implementación flexible en sus procesos de fabricación, las empresas pueden abordar las complejidades del IoT moderno con confianza. La combinación de la agilidad que proporciona la implementación flexible, la escalabilidad global garantizada y la precisión de la seguridad adaptable a los recursos da lugar a un ecosistema de fabricación resiliente que es capaz de satisfacer la demanda del presente y anticiparse a las necesidades del futuro.

CAPÍTULO 3

EXCELENCIA OPERATIVA

En los procesos de fabricación donde se utilizan tecnologías IoT, la excelencia operativa gira en torno a una interacción perfecta entre los procesos automatizados y unas buenas medidas de seguridad. El elemento central de esta estrategia operativa es la gestión automatizada de los certificados que sientan los cimientos de la identidad y la seguridad de los dispositivos en el ámbito del IoT. Al automatizar este ciclo de vida —que abarca desde la emisión hasta la renovación y la revocación de un certificado— los fabricantes pueden asegurarse de que las identidades de los dispositivos que producen se gestionan con precisión y no están expuestas a riesgos derivados de errores humanos.

Esta gestión de certificados automatizada también se aplica al ámbito de las operaciones de los dispositivos in situ. Una vez implementados, los dispositivos pueden recibir actualizaciones y revisiones de seguridad de forma remota, con una interrupción mínima y sin necesidad de intervención física. Los beneficios de la eficiencia operativa son notables: los dispositivos permanecen en uso durante más tiempo y se reduce la necesidad de retirarlos o hacer actualizaciones manuales, lo que supone un ahorro de tiempo y dinero.

Gestión de certificados automatizada aplicada al mundo real

Gracias a la amplia adopción de la tecnología inteligente, la confianza de los dispositivos permite incorporar la excelencia operativa en un amplio abanico de contextos:

- En un programa de ciudades inteligentes, se utilizan miles de sensores y dispositivos para recopilar y transmitir datos con el objetivo de gestionar el tráfico, el consumo de energía y la seguridad de los ciudadanos. Gracias a la gestión de certificados automatizada que ofrecen estos dispositivos, es posible autenticar la identidad de cada uno de ellos y los datos se transmiten de forma segura. Así, se puede garantizar que la información utilizada para tomar decisiones importantes sea fiable y segura.
- En el sector de la atención sanitaria, donde los dispositivos abarcan desde equipos de monitorización hospitalaria hasta dispositivos portátiles para hacer un seguimiento de la salud, es imperativo establecer unas medidas de seguridad estrictas y contar con dispositivos que funcionen de forma fiable. La automatización de la gestión de identidades y certificados permite actualizar estos dispositivos rápidamente para que tengan las credenciales de seguridad más recientes. De este modo, los datos de los pacientes están protegidos en todo momento y los proveedores de asistencia sanitaria pueden confiar en la integridad de los datos que reciben.
- En las operaciones de fabricación, la gestión de la seguridad automatizada se refleja en la capacidad de los dispositivos para adaptarse a los cambios que se producen en los entornos de seguridad. La estrategia de seguridad de los dispositivos in situ evoluciona conforme lo hacen las amenazas, con una interrupción de las operaciones mínima. Esta adaptabilidad es esencial para mantener la confianza de los consumidores y proteger la reputación de los fabricantes.

La integración de la gestión automatizada del ciclo de vida de los certificados y la gestión de identidades en las operaciones de los dispositivos IoT supone un importante avance para la excelencia operativa. Dicha integración mejora la seguridad, reduce los riesgos operativos y refuerza la fiabilidad general de los ecosistemas de IoT, para así satisfacer las demandas de la infraestructura y la sociedad modernas.

CAPÍTULO 4

FABRICACIÓN PREPARADA PARA EL FUTURO

El panorama de la seguridad del IoT cambia constantemente, por lo que los fabricantes no pueden centrarse únicamente en las preocupaciones de hoy en día, sino que también deben anticiparse a los desafíos del futuro.

Preparación para la informática cuántica

Se espera que la amenaza emergente de la informática cuántica ponga en jaque los métodos tradicionales de cifrado, lo que podría generar nuevas vulnerabilidades en los dispositivos actuales. La incorporación estratégica de la criptografía poscuántica (PQC, por sus siglas en inglés) prepara a los dispositivos para esa posibilidad, protegiéndolos de las capacidades de descifrado de los ordenadores cuánticos y garantizando la privacidad de los datos y la integridad del dispositivo a largo plazo.

Adopción de tecnologías emergentes

Las tecnologías como MQTT 5.0 ofrecen funciones mejoradas para las colas de mensajes en la comunicación entre dispositivos, lo que brinda un mayor nivel de seguridad, una gestión mejorada de los datos y una comunicación entre dispositivos más eficiente. Del mismo modo, Kubernetes —un sistema de código abierto destinado a automatizar la implementación, la ampliación y la gestión de aplicaciones alojadas en contenedores— proporciona agilidad y escalabilidad para la gestión de dispositivos.

Gracias a la integración de MQTT 5.0, Kubernetes y otras tecnologías emergentes, los fabricantes pueden gestionar dispositivos IoT de manera más eficaz, así como garantizar la solidez, la capacidad de respuesta y la adaptabilidad de la infraestructura a los rápidos avances tecnológicos.

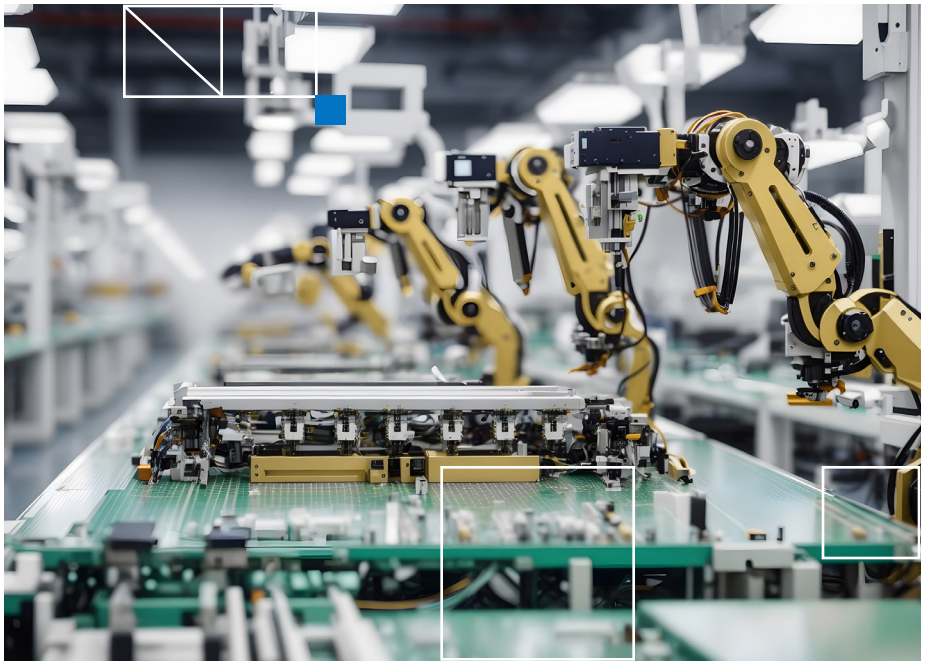
Se espera que la amenaza emergente de la informática cuántica ponga en jaque los métodos tradicionales de cifrado, lo que podría generar nuevas vulnerabilidades en los dispositivos actuales.

La importancia de adelantarse a los cambios normativos

El cumplimiento de los estándares del sector es una labor continua, ya que los parámetros de referencia cambian continuamente, conforme emergen nuevas amenazas de seguridad y evolucionan las normativas. Si las empresas quieren ir un paso por delante en el ámbito del cumplimiento normativo, no pueden limitarse a cumplir los estándares actuales, sino que también deben participar en los debates que se mantienen para diseñar estas normativas.

Al colaborar con los órganos normativos y los grupos de trabajo técnicos, los fabricantes pueden obtener información útil sobre los cambios que se avecinan y preparar sus productos en consecuencia. Abordar el cumplimiento normativo de manera proactiva facilita la transición cuando los nuevos estándares entran en vigor, lo que permite evitar costosas revisiones y garantizar que los productos sigan las prácticas de seguridad más recientes.

Además, cuando los fabricantes se adaptan a la evolución de los estándares, obtienen una ventaja estratégica que les ayuda a posicionarse como líderes del sector, así como a estar preparados para satisfacer las exigencias de los clientes que dan importancia a la seguridad y para abordar la complejidad de los mercados globales con diferentes requisitos normativos. Esta actitud también es una forma de demostrar a las partes interesadas que el fabricante se ha comprometido a mantener los estándares de seguridad más elevados, lo que refuerza la confianza y mejora la reputación de la marca.



La clave para garantizar el futuro de la fabricación en el ámbito del IoT

Al anticiparse a las amenazas emergentes, adoptar tecnologías innovadoras y abordar el cumplimiento normativo de manera proactiva, los fabricantes tendrán la seguridad de que sus productos no solo están protegidos para el presente, sino que están preparados para superar los desafíos del futuro. Esta visión de futuro estratégica será un aspecto diferenciador entre los líderes del IoT y les permitirá ofrecer productos seguros, fiables y vanguardistas que resistan al paso del tiempo y los avances tecnológicos.

CAPÍTULO 5

LOS RESULTADOS DE LA CONFIANZA DE LOS DISPOSITIVOS SALTAN A LA VISTA

La mejor forma de evaluar el efecto que tiene un marco sólido de seguridad de dispositivos es observar cómo lo han aplicado los clientes y analizar cómo han comprobado el potencial transformador de la confianza de los dispositivos. En los siguientes casos prácticos, se muestran diferentes formas de aplicar este marco haciendo hincapié en su impacto en el negocio, lo que permite entender mejor las ventajas estratégicas que proporcionan estas soluciones.

Caso práctico n.º 1

Cliente: Fabricante líder de dispositivos de domótica

Solución: Implementar un marco de seguridad en todo el catálogo de productos

Resultado: El cliente observó una reducción drástica de las brechas de seguridad, además de un aumento de la confianza de los consumidores que se tradujo en un incremento considerable de la cuota de mercado y una mejor reputación de la marca. El fabricante obtuvo un rendimiento de la inversión que superó con creces sus expectativas iniciales y logró cuantificar los beneficios.

Caso práctico n.º 2

Cliente: Multinacional especializada en dispositivos IoT para el ámbito industrial

Solución: Optimizar los procesos de cumplimiento normativo

Resultado: Al integrar una solución sofisticada de seguridad de dispositivos, la empresa optimizó sus procesos de cumplimiento normativo, ahorró costes y redujo el plazo de comercialización de los nuevos productos. El marco de seguridad le permitió automatizar aspectos esenciales de la gestión de la seguridad de los dispositivos, además de ayudarle a reducir la carga de trabajo de sus equipos de TI y minimizar el riesgo de cometer errores humanos al gestionar los certificados.

Caso práctico n.º 3

Cliente: Importante fabricante del sector automovilístico

Solución: Desarrollar una solución de seguridad personalizada

Resultado: Al desarrollar una solución de seguridad personalizada, la empresa pudo crear una plataforma de coches conectada y muy segura. El éxito de esta asociación no solo afianzó la posición del fabricante como agente innovador en tecnología automovilística, sino que también demostró su compromiso y experiencia a la hora de abordar los desafíos propios del sector.

En una época en la que las filtraciones de datos y las vulnerabilidades de seguridad acaparan titulares, la capacidad de demostrar un enfoque de seguridad proactivo y exhaustivo es algo muy preciado.

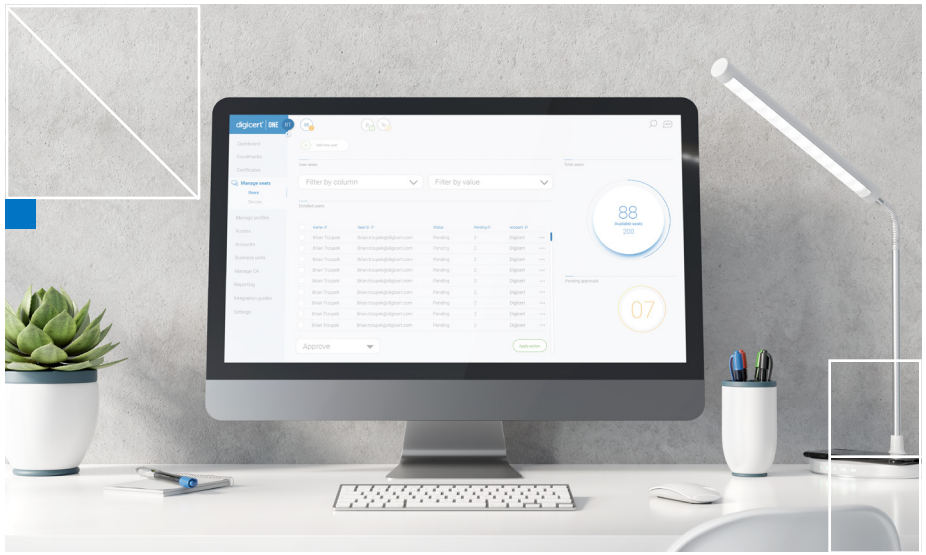
Soluciones de seguridad con un impacto duradero

El impacto empresarial de las soluciones implementadas en estos casos prácticos va más allá del aspecto operativo; también tiene un efecto a nivel estratégico, ya que influye en la manera en la que el sector percibe a estas empresas. En una época en la que las filtraciones de datos y las vulnerabilidades de seguridad acaparan titulares, la capacidad de demostrar un enfoque de seguridad proactivo y exhaustivo es algo muy preciado.

LA PROTECCIÓN DE SU NEGOCIO EMPIEZA POR LOS DISPOSITIVOS

La protección de su negocio empieza por los dispositivos

Garantizar la seguridad de los dispositivos y la excelencia operativa es más importante que nunca. Para los fabricantes que quieran superar las dificultades que conlleva el panorama de la seguridad actual, solo hay dos opciones: adoptar una postura proactiva con respecto a la seguridad de los dispositivos o correr el riesgo de quedarse atrás.



DigiCert® IoT Trust Manager pone la confianza de los dispositivos al alcance de todo el mundo. Visite digicert.com/es/contact-us para obtener más información sobre cómo este concepto puede proteger sus dispositivos, sus datos y, en definitiva, su negocio frente a las amenazas del presente y del futuro.

Acerca de DigiCert

DigiCert es el proveedor líder de confianza digital. Gracias a él, los usuarios individuales, las empresas, las administraciones públicas y los consorcios pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida.

La plataforma DigiCert® ONE, garantía de confianza digital, protege los sitios web, los accesos y comunicaciones empresariales, el software, las identidades, el contenido y los dispositivos, entre otros elementos, para que las empresas respondan a toda una gama de necesidades en materia de confianza digital con una visibilidad y un control centralizados. Su galardonado software y su liderazgo en el sector de los estándares, la asistencia y las operaciones convierten a DigiCert en el proveedor al que recurren las grandes empresas de todo el mundo que apuestan por la confianza digital.