Las ventajas de una única plataforma

Valor a largo plazo, ciberseguridad y facilidad de integración: claves de un diseño a medida

AXIS COMMUNICATIONS

Al servicio de sus dispositivos de red Axis

AXIS OS es el sistema operativo Linux que utilizan la mayor parte de los dispositivos de red Axis. Es el cerebro de más de 200 productos Axis y de decenas de millones de dispositivos utilizados en las instalaciones de nuestros clientes. AXIS OS es garantía de innovación, fiabilidad y una integración sencilla. El software de Axis es la clave de la fiabilidad de nuestros dispositivos y también de su excelente calidad de imagen, y cada nueva versión introduce mejoras y avances. De hecho, el 80% de nuestros esfuerzos de investigación y desarrollo giran en torno al software.

Constantemente incorporamos nuevas prestaciones y mejoras. Y también reforzamos la seguridad a través de parches para corregir vulnerabilidades en los dispositivos que utilizan AXIS OS, con el objetivo de que puedan usarse en más situaciones y con las máximas garantías.

El diseño de AXIS OS tiene muy en cuenta lo que buscan los usuarios de dispositivos de red: valor a largo plazo, un elevado nivel de ciberseguridad y una integración sencilla.

Un diseño a medida para los dispositivos Axis
Diseñado por un equipo de desarrollo interno de Axis y basado en una plataforma tan estable como Linux Yocto OpenEmbedded, AXIS OS ofrece mucho más que cualquier plataforma genérica, ya que está optimizado pensando en las necesidades específicas de los dispositivos en el extremo de Axis, como cámaras, altavoces y sistemas de control de acceso.

Valor a largo plazo
Con AXIS OS, sus dispositivos están siempre en guardia. Diseñado para una vigilancia ininterrumpida, garantiza un funcionamiento estable y una respuesta ágil ahora y en el futuro, tanto de día como de noche.

Ciberseguridad avanzada
La firme apuesta por la ciberseguridad es uno de los pilares de AXIS OS: su arquitectura de seguridad integrada es el mejor aliado para proteger sus dispositivos. Con un proceso de desarrollo de software seguro y un estricto control de las vulnerabilidades, AXIS OS protege sus datos y dispositivos ante nuevas amenazas.

Integración sin problemas
AXIS OS es compatible con VAPIX, ONVIF y otros protocolos que le ayudarán a integrar fácilmente sus dispositivos de red Axis en diferentes ecosistemas. Y esta facilidad de integración se traduce en una experiencia ágil e interconectada, tanto para usuarios como para desarrolladores.

AXIS OS en cifras

900 desarrolladores

24.000.000 líneas de código escritas

4000 confirmaciones de código cada día

4.000.000 de pruebas automatizadas cada día

+200 productos Axis con modelo de soporte activo

+500 productos Axis con modelo de soporte a largo plazo (LTS)

+6 lanzamientos de software en modelo activo al año

+2000 componentes de software

Más del **95%** de componentes de código abierto

Un diseño a medida para los dispositivos Axis

En la fase de diseño de AXIS OS, definimos como principales prioridades el rendimiento, la integración, la seguridad y la calidad del software en los dispositivos en el extremo.

Gracias a la estabilidad de Linux Yocto OpenEmbedded, AXIS OS pone en sus manos una plataforma unificada para todos sus dispositivos de red Axis y permite disfrutar de una misma experiencia en un amplio abanico de productos.

En las siguientes páginas, veremos las ventajas de una plataforma unificada y de un sistema operativo diseñado específicamente para dispositivos en el extremo.

Al servicio de los dispositivos en el extremo

En un mundo dominado por productos cortados por un mismo patrón, el concepto de AXIS OS va más allá de un simple sistema operativo basado en Linux: ofrece una solución adaptada a las necesidades específicas de los dispositivos en el extremo. Este elevado nivel de especialización es lo que explica el rendimiento, la fiabilidad y la seguridad de los productos Axis.

Linux Yocto: la piedra angular
La plataforma basada en Linux Yocto OpenEmbedded garantiza unos excelentes niveles de estabilidad y eficiencia. Linux Yocto OpenEmbedded es, además, un entorno con el que los desarrolladores están ya familiarizados. Esta sólida plataforma es la clave del buen funcionamiento de los dispositivos de red Axis.

Compatibilidad con diferentes chips
La versatilidad es una de las palabras clave de AXIS OS. Por eso, no solo es compatible con el chip ARTPEC de Axis presente en la mayoría de los dispositivos de la marca, sino también con chips de terceros, para que el máximo número de dispositivos de red pueda disfrutar de las ventajas de AXIS OS.

Garantía de valor a largo plazo
Nuestros dispositivos tienen que poder funcionar durante muchos años. Por este motivo, AXIS OS tiene un diseño sólido y preparado para el futuro. Al mismo tiempo, hablamos con transparencia sobre la vida útil de nuestros dispositivos, una información que publicamos en axis.com.

Pruebas específicas de gran exigencia
AXIS OS se somete a rigurosas pruebas para garantizar que puede cumplir con nota su cometido. Este nivel de exigencia tiene una razón de ser: queremos que supere las más altas expectativas en cuanto a rendimiento, ciberseguridad e integración.

Un software de calidad
AXIS OS es la mejor prueba de nuestro inquebrantable compromiso con la calidad del software. El sistema operativo está diseñado para ofrecer a los usuarios una plataforma intuitiva, fiable y segura a lo largo de todo el ciclo de vida de los dispositivos Axis.

Las ventajas de una única plataforma

Nuestro compromiso con la excelencia abarca todas las categorías de productos y se plasma en nuestra firme apuesta por una plataforma unificada. Compatible con más de 200 productos, desde cámaras corporales hasta soluciones a prueba de explosiones, pasando por cámaras PTZ, sirenas, altavoces e intercomunicadores, nuestra plataforma ofrece todas las respuestas que nuestros socios y clientes necesitan.

La unión hace la fuerza
AXIS OS es compatible con un amplio abanico de productos. Todos nuestros productos comparten unas mismas API y unos mismos patrones de comportamiento. Con una única plataforma, todos los integradores y desarrolladores pueden añadir nuevos dispositivos Axis a sus sistemas, sin necesidad de complejos controladores específicos para cada dispositivo. El resultado no es solo una integración más rápida, sino también una infraestructura mejor preparada para el futuro, que podrá incorporar los nuevos productos del ecosistema Axis. Además, los clientes finales pueden disfrutar siempre de una misma experiencia, y los desarrolladores ahorran tiempo y dinero, ya que sus soluciones de integración son siempre compatibles con todos los dispositivos con AXIS OS.

Versatilidad máxima, complejidad mínima
Otra de las ventajas de una plataforma unificada es que abre la puerta a una gran diversidad de usos sin necesidad de complicar las cosas. Tanto si quiere integrar una cámara PTZ en un sistema de vigilancia como incorporar un altavoz a una solución de audio inteligente, el proceso siempre es el mismo. Esta versatilidad va más allá de la compatibilidad, ya que se traduce también en una experiencia unificada y en un enorme potencial para crear soluciones integradas adaptadas a necesidades específicas.

Seguridad unificada
En un mundo en el que la ciberseguridad es cada vez más imprescindible, disponer de una sola plataforma facilita la adopción de soluciones unificadas para todo el abanico de productos. Para mantener el nivel de seguridad no hace falta proteger cada producto uno a uno, sino que cuando se detecta una vulnerabilidad puede aplicarse la corrección a todos los productos compatibles. Esta fórmula no solo agiliza la gestión de la seguridad, sino que también permite una respuesta rápida y colectiva ante nuevas amenazas, además de ahorrar tiempo y recursos, y reforzar la seguridad de todo el ecosistema Axis.

Valor a largo plazo

AXIS OS ayuda a conservar el valor de sus dispositivos en todo su ciclo de vida, gracias a una arquitectura sólida y estable que minimiza los tiempos de inactividad.

El software de nuestros productos sigue actualizándose (e incorporando nuevas funciones) aunque pasen los años. Con una completa documentación, prácticas herramientas y unas interfaces intuitivas, los dispositivos Axis son garantía de una utilización y un mantenimiento extremadamente sencillos. Y como nuestros calendarios de publicación de versiones son transparentes y fiables, puede planificar el mantenimiento según las necesidades de su organización.

En las páginas que siguen podrá ver más detalles sobre la calidad del software de Axis, la gestión del ciclo de vida de AXIS OS y el soporte de software.

Un software de toda confianza

La calidad es el santo y seña de AXIS OS. Con aproximadamente 900 desarrolladores y 4000 confirmaciones de código cada año en la estructura principal de AXIS OS, nuestro sistema operativo no deja de evolucionar en respuesta a las necesidades del mercado. Y con dos compilaciones diarias para cada uno de nuestros más de 200 productos, la cifra anual se eleva hasta las 182.500 compilaciones, lo que permite un proceso de pruebas iterativo que aporta un gran valor añadido.

Pruebas con la máxima exigencia

Para garantizar la estabilidad del software hacen falta unas pruebas muy rigurosas. Tanto es así que nuestros sistemas ejecutan cada día 4 millones de situaciones de prueba de diferentes tipos. Estas pruebas se complementan con más de 4000 confirmaciones de código diarias para corregir vulnerabilidades y mejorar la calidad. Al final del año, todo esto equivale a más de 1000 millones de pruebas y un millón de confirmaciones de código. Asimismo, animamos a nuestros clientes y socios a compartir datos con nosotros para saber cómo valoran AXIS OS.

Mejoras constantes

AXIS OS no es una plataforma estática: es un entorno dinámico, que evoluciona constantemente. A través de actualizaciones regulares y mejoras, los dispositivos Axis con modelo de soporte activo de AXIS OS pueden beneficiarse de los últimos avances tecnológicos. Por lo tanto, el producto que compra hoy irá integrando nuevas funciones y ganando valor a lo largo de su ciclo de vida.

Soporte en todo el ciclo de vida

Una de las ventajas de AXIS OS es que acompaña los dispositivos en todo su ciclo de vida, desde la instalación hasta el mantenimiento y su sustitución. AXIS OS pone en sus manos herramientas y recursos para ayudarle a gestionar y optimizar sus dispositivos Axis a lo largo de todo su camino.

Instalación y configuración sencillas
AXIS OS simplifica la instalación y la configuración de los dispositivos Axis, a través de asistentes, plantillas y perfiles que le guían en todo el proceso. También puede recurrir a AXIS Device Manager (ADM) y AXIS Device Manager Extend (ADMX) para instalar y configurar varios dispositivos a la vez y ahorrarse así tiempo y esfuerzo.

Supervisión y diagnósticos continuos
Siempre que otorgue su consentimiento, AXIS OS supervisa y analiza el funcionamiento y el estado de los dispositivos Axis, a través de la recopilación de datos de registros, informes y alertas. El objetivo no es otro que ayudarle a identificar y atajar cualquier posible problema. Además, también nos sirve para mejorar nuestro software en cada nuevo lanzamiento.

Soporte a largo plazo y compatibilidad
AXIS OS ofrece soporte a largo plazo para los dispositivos Axis, con parches de seguridad y correcciones de errores. Nuestro modelo de soporte a largo plazo permite garantizar la compatibilidad de los dispositivos y aplicaciones Axis con unas interrupciones y cambios mínimos. Los dispositivos que utilizan AXIS OS suelen tener un ciclo de vida de hasta 10 años o más. En algunos casos, nuestro soporte puede prolongarse hasta los 13 años.

Confianza y compromiso
AXIS OS está diseñado para dar respuesta a las expectativas y las necesidades de los clientes que más valoran la confianza y la calidad. AXIS OS define de forma clara y transparente la vida útil prevista para cada producto y le ofrece soporte durante el máximo tiempo posible. Además, Axis ofrece a los clientes los máximos niveles de servicio y asistencia para mantener unas relaciones de largo recorrido.

Beta de AXIS OS

La beta de AXIS OS ofrece a desarrolladores e integradores la posibilidad de probar y evaluar las últimas funciones y prestaciones de AXIS OS antes de su lanzamiento oficial. Pueden utilizarla, por ejemplo, para realizar pruebas de compatibilidad en determinados dispositivos, comprobar las actualizaciones de seguridad o acceder a nuevas prestaciones.

Estas son algunas de las ventajas que le ofrece la beta de AXIS OS:

> Acceso a las funciones y prestaciones nuevas y mejoradas que AXIS OS incorporará en el futuro, relacionadas por ejemplo con la analítica en el extremo, la conectividad IoT o la modularización de la plataforma.

> Posibilidad de enviar valoraciones o sugerencias a Axis para contribuir al desarrollo y la mejora de AXIS OS.

> Preparación y adaptación de sus aplicaciones y sistemas ante próximos cambios y novedades en AXIS OS para anticiparse a posibles problemas.

Consulte aquí más información sobre la beta de AXIS OS.

AXIS OS: soporte de software en todo el ciclo de vida

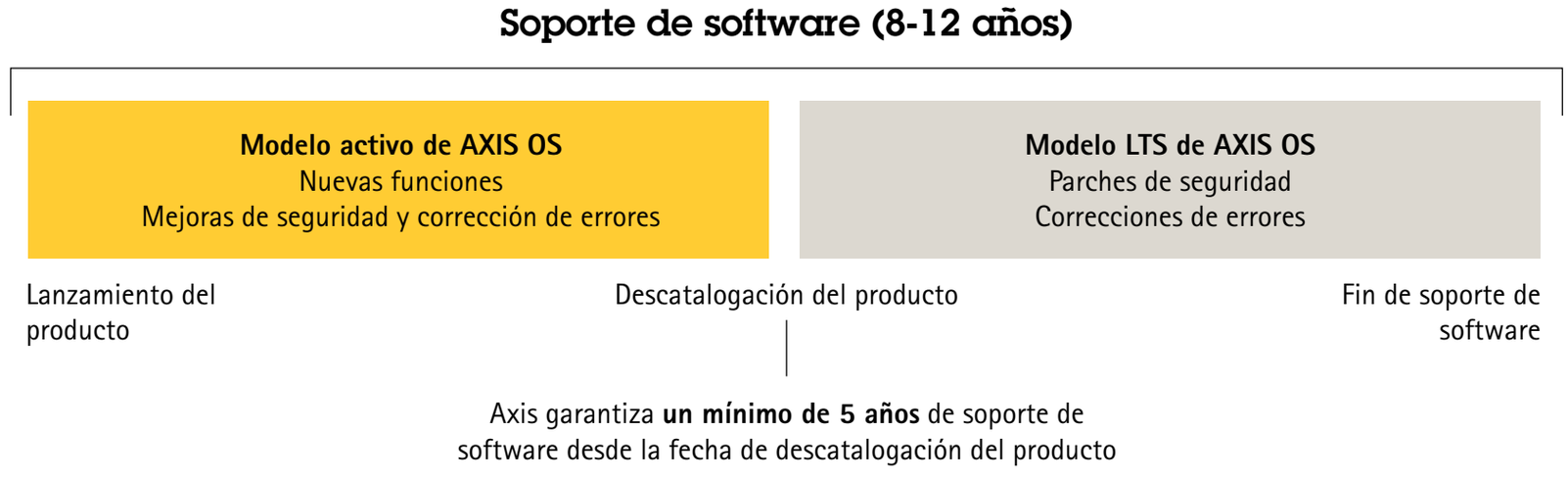
El soporte durante el ciclo de vida de AXIS OS está disponible en diferentes modelos. Los principales modelos son el activo y el de soporte a largo plazo (LTS). También hay modelos de soporte específicos de productos (PSS), adaptados a ciclos de vida de productos concretos.

El ciclo de vida mínimo de un dispositivo Axis está por encima de la media del sector. La completa garantía de hardware de 5 años se complementa con un soporte de software AXIS OS que se prolonga durante varios años más. El ciclo de vida de AXIS OS en la mayoría de los dispositivos se sitúa entre los 8 y los 12 años.

Así funciona:

1. Cuando Axis presenta un nuevo dispositivo, el único modelo de soporte de AXIS OS disponible es el activo. Durante la fase posterior al lanzamiento podrá disfrutar de actualizaciones y mejoras continuas, así como nuevas funciones.
2. A los dos años del lanzamiento del producto puede optar por un modelo de soporte a largo plazo (LTS) en sustitución del modelo activo. En este punto, puede elegir entre el modelo activo o el modelo de soporte a largo plazo. Los productos con modelo de soporte a largo plazo solo tienen acceso a parches y correcciones de errores.
3. Entre dos y cuatro años después del lanzamiento, cuando se descataloga un producto, también deja de estar disponible el modelo activo para dicho dispositivo. A partir de este punto, se aplica el modelo de soporte a largo plazo (LTS) a todos los dispositivos, que siguen recibiendo parches y correcciones de errores durante un mínimo de 5 años.

AXIS OS: soporte de software en todo el ciclo de vida



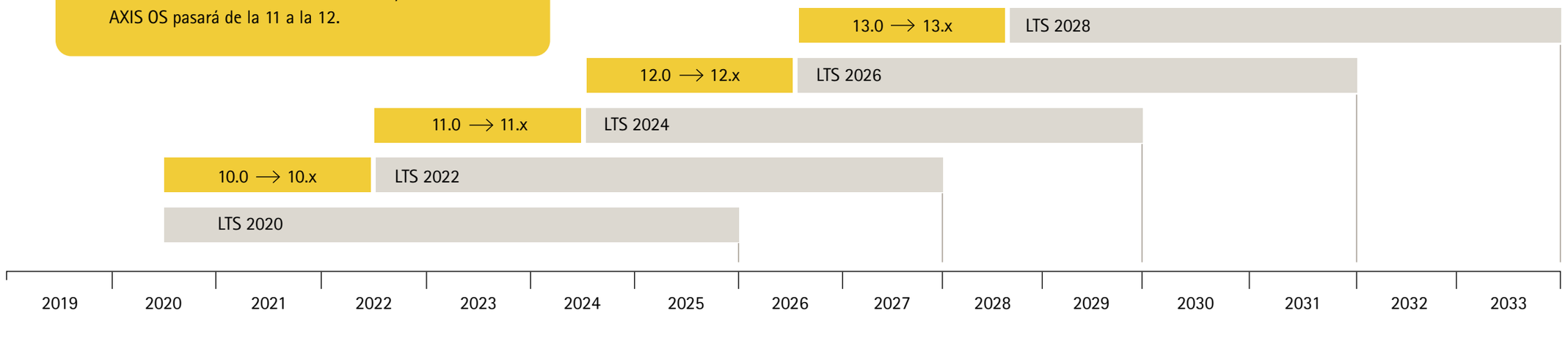
¿Cuál es el modelo de soporte que necesita?

Cuando están disponibles tanto el modelo activo como el de soporte a largo plazo, los clientes pueden elegir el que mejor se ajuste a sus necesidades, con el asesoramiento de Axis.

Modelo activo
El modelo activo de AXIS OS permite utilizar el sistema operativo en su versión más actualizada y completa. Está pensado especialmente para clientes que quieren un acceso inmediato a las últimas funciones y mejoras, y es el único modelo disponible en el caso de los dispositivos de reciente lanzamiento. Con este modelo los usuarios pueden sacar el máximo partido a sus dispositivos, gracias a las nuevas funciones de ciberseguridad o a las mejoras en las funciones existentes. El modelo activo de AXIS OS permite exprimir todo el potencial de los dispositivos sin ningún coste extra, incluso años después de su compra. Si no tiene problemas de compatibilidad, es recomendable mantener este modelo mientras esté disponible.

Modelo de soporte a largo plazo (LTS)
Si lo que quiere es trabajar con las mismas API y asegurarse la compatibilidad, lo mejor es apostar por el modelo de soporte a largo plazo (LTS) una vez que esté disponible. El modelo LTS busca garantizar la compatibilidad con soluciones anteriores y ofrece parches de seguridad y correcciones de errores. En lugar de introducir nuevas funciones de seguridad, su finalidad es mantener la ciberseguridad. Por lo tanto, no incorpora nuevas prestaciones o funcionalidades, sino que intenta minimizar los cambios y los posibles desajustes. El modelo LTS es ideal para los clientes que valoran especialmente la fiabilidad y la calidad y quieren un sistema de terceros perfectamente integrado. Cada modelo LTS ofrece 5 años de soporte y los modelos LTS se introducen cada 24 meses, según el calendario regular del modelo activo. Una vez descatalogados, todos los dispositivos pasan a estar cubiertos por el modelo LTS.

La ilustración presenta cada modelo activo de AXIS OS junto con los modelos LTS introducidos a lo largo de los años. Aproximadamente cada 24 meses se introduce un nuevo modelo LTS y se avanza un nivel en la versión principal de AXIS OS. Por ejemplo, en 2024 se introducirá el nuevo LTS AXIS OS 2024 y la versión de AXIS OS pasará de la 11 a la 12.



En el foco: ciberseguridad

AXIS OS apuesta por el concepto de seguridad por diseño. Nuestro Axis Security Development Model (ASDM) define una serie de procesos y herramientas que reducen el riesgo de vulnerabilidades durante el desarrollo de software y también en las fases posteriores.

Axis Edge Vault, nuestra plataforma de ciberseguridad basada en hardware, garantiza un arranque seguro y un entorno a prueba de manipulaciones para el almacenamiento de claves criptográficas cargadas por los clientes. El software esencial de AXIS OS está formado por componentes de código abierto totalmente verificados. Además, cada nueva versión se complementa con una lista de materiales de software (SBOM) que demuestra que AXIS OS está al día y con los correspondientes parches para las vulnerabilidades conocidas.

AXIS OS cuenta, además, con la certificación ETSI EN 303 645, centrada específicamente en la seguridad de los dispositivos en el extremo. A través de la norma FIPS 140 se garantiza también la conformidad de AXIS OS con las últimas normas criptográficas publicadas por el National Institute of Standards and Technology (NIST) de EE. UU. Por último, por nuestra condición de Autoridad de Numeración CVE, aplicamos las prácticas recomendadas para la identificación, la gestión y la divulgación de vulnerabilidades.

En las páginas que siguen encontrará más detalles sobre nuestro Axis Security Development Model, Axis Edge Vault, la gestión de vulnerabilidades y nuestro concepto de seguridad unificada.

La seguridad, el pilar del proceso de desarrollo

El Axis Security Development Model (ASDM) integra la ciberseguridad en el ciclo de vida de desarrollo del software. Para hacerlo, define las actividades de seguridad que deben tenerse en cuenta durante las diferentes fases de desarrollo del software. El objetivo es reducir las vulnerabilidades y también los costes de desarrollo, definiendo un punto de referencia para la ciberseguridad y proporcionando orientaciones.

ASDM: con el sello de Axis
El Axis Security Development Model no es una arquitectura estándar de tipo genérico, sino que es fruto del análisis de diferentes normas y arquitecturas de ciberseguridad, como ISO 27001, IEC 62443, NIST, BSIMM y CMMC. El nexo de unión de todos estos instrumentos es la integración de la seguridad en todas las fases del desarrollo. Partiendo de esta premisa, adaptamos el modelo a la filosofía de nuestra empresa, nuestros procesos de desarrollo y el tipo de productos que diseñamos.

Las herramientas del ASDM
Las herramientas del ASDM están pensadas para dar respuesta a diferentes problemas de seguridad. Algunas de estas herramientas son la evaluación de riesgos, el modelado de amenazas, las pruebas de modelos de amenaza, los análisis de código estático, el análisis de vulnerabilidades y la evaluación de proveedores. Los equipos de desarrollo eligen los recursos empleados en función del tipo de software que van a desarrollar. El objetivo es reforzar la ciberseguridad en lugar de limitarse a seguir un proceso definido.

El papel clave de los especialistas externos
En nuestro proceso de desarrollo de un software seguro, el grueso del trabajo recae en el departamento de I+D de Axis y en nuestros ingenieros de software. Sin embargo, también somos conscientes de la importancia de recurrir a los conocimientos y la experiencia de otros expertos. Por este motivo, contratamos a empresas especializadas para realizar pruebas de penetración. Y también ofrecemos el programa de recompensas por la detección de fallos en AXIS OS, con compensaciones económicas para los analistas de seguridad que nos ayuden a identificar vulnerabilidades.

Gobernanza | capacitacion | Reunión de equipo de ASDM | Evaluación de ASDM | Cumplimiento y normas de seguridad

Requisitos	Diseño	Implementación	Verificación	Despliegue
Evaluación del riesgo Evaluación de proveedores Privacidad de la información Evaluación de seguridad de código abierto	Modelado de amenazas	Análisis del código estático Análisis de composición del software	Pruebas de modelos de amenazas Prueba de penetración externa Análisis de vulnerabilidades Evaluación de seguridad interna	Gestión de las vulnerabilidades Gestión de incidentes Estado de seguridad producto/solución Programa de recompensas por detección de errores

Ciberseguridad integrada de serie

Protección de dentro hacia fuera
Axis Edge Vault es nuestra plataforma de ciberseguridad basada en hardware, una sólida base que garantiza que sus dispositivos Axis son de confianza y pueden desempeñar su misión con garantías dentro de su red. Sin embargo, esta sólida infraestructura de hardware no servirá de nada sin un sistema operativo que ayude a explotar todo su potencial. AXIS OS utiliza la plataforma Edge Vault para reforzar la seguridad en los dispositivos locales en cualquier caso de uso.

Estas son algunas de las funciones de Edge Vault:

Almacenamiento seguro de claves
Un almacén seguro de claves utiliza módulos de computación criptográficos para el almacenamiento y procesamiento seguros de las claves criptográficas. Estos módulos protegen la identidad del dispositivo y otra información confidencial contra accesos no autorizados, aunque el dispositivo haya quedado expuesto. Los módulos de computación criptográficos empleados son el Trusted Execution Environment integrado en el sistema en chip (SoC) y también un elemento seguro específico o un Trusted Platform Module (TPM 2.0), que tienen sus propios chips en la placa de circuitos impresos (PCB).

SO firmado y arranque seguro
En un SO firmado se aplica una firma de código a la imagen de software del dispositivo. Gracias a la combinación del SO firmado y el arranque seguro, los dispositivos pueden descargar y ejecutar únicamente el sistema operativo AXIS OS original. Este mecanismo aporta un nivel adicional de protección contra manipulaciones en las cadenas de suministro del software y el hardware.

ID de dispositivo de Axis
El ID de dispositivo de Axis cumple con la norma IEEE 802.1AR y permite la identificación segura del dispositivo y su incorporación a una red, como si de un pasaporte se tratara.

Sistema de archivos cifrado
El cifrado del sistema de archivos protege los datos del sistema de archivos de extracciones o manipulaciones mientras el dispositivo no está en uso, por ejemplo durante su transporte de un integrador de sistemas al cliente final.

Vídeo firmado
Con el vídeo firmado, los usuarios pueden verificar la autenticidad del vídeo grabado y asegurarse de que no se ha manipulado.

Plataforma de ciberseguridad Axis Edge Vault

Módulos de computación criptográfica	Prestaciones	Aplicaciones
Elemento seguro TPM 2.0 Seguridad del SoC (TEE)	Arranque seguro SO firmado ID de dispositivo de Axis Almacén de claves seguro Vídeo firmado Sistema de archivos cifrado	Identidad de dispositivos validada Almacenamiento seguro de claves Detección de manipulación del vídeo Protección de la cadena de suministro

* Nota: no todos los modelos de dispositivos admiten todas las funciones de Axis Edge Vault. Consulte la hoja de datos o el selector de productos de Axis para confirmar las funciones admitidas por un producto concreto.

Gestión de las vulnerabilidades

Para minimizar el riesgo de exposición de nuestros clientes, aplicamos las prácticas recomendadas del sector para gestionar y corregir las vulnerabilidades de forma transparente.

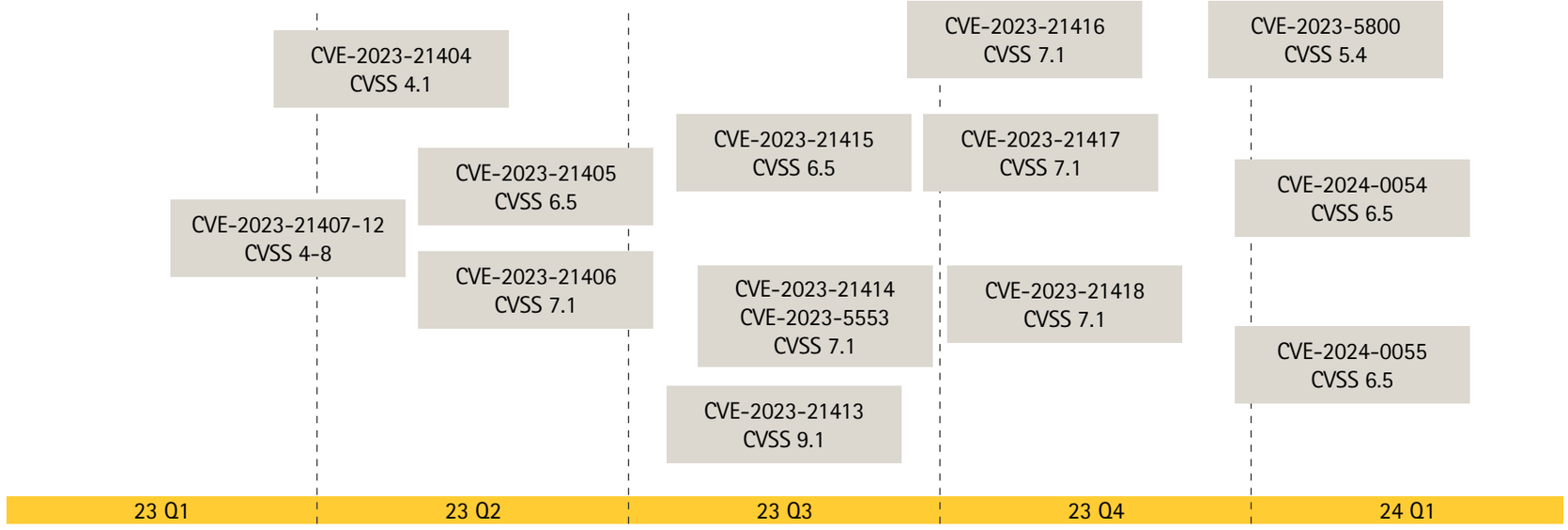
Una gestión de vulnerabilidades de primer nivel
No hay forma posible de garantizar que los productos y servicios de Axis están totalmente a salvo de vulnerabilidades. Y no ocurre solo con Axis, sino con todo tipo de software y servicios. Sin embargo, dedicamos un importante esfuerzo a identificar y mitigar posibles vulnerabilidades en sus fases iniciales, con el objetivo de reducir los riesgos al implantar productos y servicios Axis en los entornos de los clientes.

Autoridad de Numeración CVE
Axis es una Autoridad de Numeración CVE (CNA). Nuestra participación en el programa CVE nos ha permitido colaborar con empresas con valores compartidos para mejorar la gestión de las vulnerabilidades. La forma en que gestionamos, divulgamos y corregimos las vulnerabilidades se ajusta a los criterios internacionales definidos por esta organización sin ánimo de lucro y a nuestra propia política sobre gestión de vulnerabilidades.

Una gestión transparente y fiable
Axis utiliza el sistema de puntuación CVSS (sistema de puntuación de vulnerabilidad común) para evaluar las vulnerabilidades vinculadas a código desarrollado por Axis o código abierto desarrollado por terceros. Evaluamos las vulnerabilidades del código abierto teniendo en cuenta su relevancia para nuestros productos aplicando las prácticas recomendadas. Puede suscribirse al Servicio de notificaciones de seguridad de Axis para recibir información sobre vulnerabilidades y otras cuestiones relacionadas con la seguridad que afectan a los productos Axis.

Alianzas con analistas y organizaciones de seguridad
Valoramos y reconocemos el trabajo de los analistas de seguridad y las organizaciones de análisis de seguridad que nos trasladan las vulnerabilidades detectadas. Y no dudamos en hacerlas públicas y corregirlas. Al final, lo realmente importante es gestionar correctamente y con transparencia las vulnerabilidades, aplicando un proceso de difusión ético y responsable, más allá de cómo se hayan detectado.

Vulnerabilidades en AXIS OS



Vulnerabilidades en AXIS OS comunicadas por Axis.

Una infraestructura de seguridad integral

En los dispositivos de red con AXIS OS, los componentes de hardware y software funcionan como un engranaje perfecto para que los clientes puedan controlar de forma segura los dispositivos, sus servicios y los sistemas a los que están conectados. La protección integral por capas empieza con una base segura y una plataforma de seguridad basada en el hardware, y sigue en el software. Este modelo de ciberseguridad por capas y desde la raíz es el que protege los dispositivos que funcionan con AXIS OS y el que garantiza una mayor seguridad global de los datos, las aplicaciones y los procesos.

Puede tener la tranquilidad de saber que en cualquier dispositivo Axis la protección y la comunicación segura están siempre garantizadas, lo que permite una integración segura y sin fisuras en sistemas externos.

Control de acceso

Gestión del control de acceso
Gestión local de dispositivos de los usuarios con indicador de la complejidad de la contraseña
Gestión federada de dispositivos de usuarios mediante OpenID Connect (RFC6749, 1.3.1 Authorization Code) para la integración con ADFS, lo que abre la puerta a funciones como imposición de la complejidad de la contraseña, rotación, bloqueo automático de la cuenta, autenticación multifactor (MFA) o la administración de derechos en Microsoft AD.

Privacidad
Uso de datos de diagnóstico
Estrategia minimalista sobre la cantidad de datos del cliente que deben almacenarse

Aplicación

Seguridad de la aplicación
Seguridad de la aplicación basada en TLS (MQTT, SFTP, NTS, HTTPS, WebRTC)
Transmisión de vídeo cifrada (RTSPS/SRTP, HTTPS), registro del sistema remoto seguro

Sistema operativo

Cifrado y protección de los datos
OpenSSL 1.1.1 y 3.0
PKI con certificado X.509 y criptografía
Capa de seguridad de transporte (TLS 1.2/TLS 1.3)
Cifrado de tarjeta SD (AES-XTS-Plain64 de 256 bits)
Sistema de archivos cifrado (AES-XTS-Plain64 de 256 bits)
Vídeo firmado

Seguridad predeterminada
HTTPS activado de forma predeterminada
Protección de ralentización en ataques de fuerza bruta
Cortafuegos basado en host
Network Time Security (NTS)
Versiones poco seguras de TLS desactivadas
Puerto UART/depuración desactivado

Seguridad de la red de la empresa
IEEE 802.1X (control de acceso a la red)
IEEE 802.1AR (identidad del dispositivo seguro)
IEEE 802.1AE (seguridad MAC, MACsec)

Sistema operativo AXIS OS
Sistema operativo basado en Linux con más del 95% de los componentes de software de código abierto y conformes con los estándares del sector, como OpenSSL, Apache y Curl, entre otros.
Modelo de soporte activo para la incorporación de funciones y modelos de soporte a largo plazo (LTS) durante 5 años para la integración de sistemas de terceros y compatibilidad con tecnologías anteriores.

Seguridad basada en chip

Raíz de confianza del hardware
Seguridad del sistema en chip (SoC) basado en ARM
Entorno de ejecución de confianza (TEE/OP-TEE)
Módulo de plataforma de confianza (TPM 2.0), elemento seguro

Almacenamiento seguro de claves
Almacenamiento y uso con protección antimanipulación de claves criptográficas, como claves privadas cargadas por el cliente, claves para firmar vídeo y el ID de dispositivo Axis.

Modelo de seguridad

Axis Security Development Model
Axis Security Development Model (ASDM)
Pruebas de penetración de terceros
Programa de recompensas por detección de errores con Bugcrowd
Lista de materiales del software (SBOM)

Cumplimiento normativo
Niveles de garantía de evaluación de Common Criteria
FIPS 140
ETSI EN 303 645

Identidad de dispositivos validada
Plataforma de ciberseguridad Axis Edge Vault
Arranque seguro con SO firmado (firma de código)
ID de dispositivo Axis (IEEE 802.1AR)

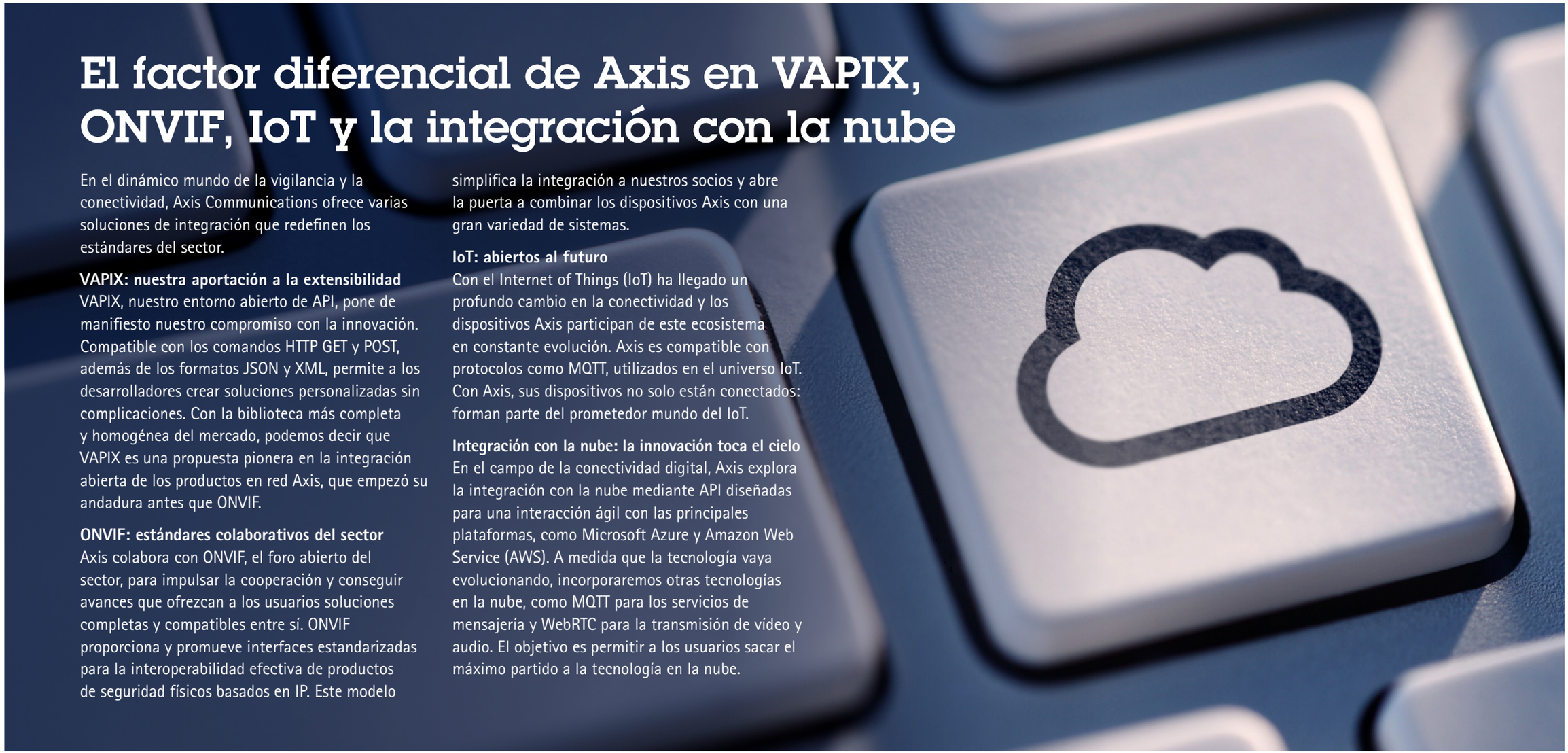
Integración avanzada

La integración es esencial en los productos Axis. Tenemos el compromiso de crear API sólidas y fiables que faciliten la integración de un amplio abanico de aplicaciones.

Nuestro objetivo no es otro que ayudarle a crear soluciones completas que le permitan exprimir al máximo el potencial de sus dispositivos Axis.

En las siguientes páginas, podrá saber más sobre VAPIX (nuestra API), nuestro trabajo con ONVIF e IoT, la modularización de la plataforma con ACAP y la automatización para la integración en redes.

El factor diferencial de Axis en VAPIX, ONVIF, IoT y la integración con la nube



En el dinámico mundo de la vigilancia y la conectividad, Axis Communications ofrece varias soluciones de integración que redefinen los estándares del sector.

VAPIX: nuestra aportación a la extensibilidad
VAPIX, nuestro entorno abierto de API, pone de manifiesto nuestro compromiso con la innovación. Compatible con los comandos HTTP GET y POST, además de los formatos JSON y XML, permite a los desarrolladores crear soluciones personalizadas sin complicaciones. Con la biblioteca más completa y homogénea del mercado, podemos decir que VAPIX es una propuesta pionera en la integración abierta de los productos en red Axis, que empezó su andadura antes que ONVIF.

ONVIF: estándares colaborativos del sector
Axis colabora con ONVIF, el foro abierto del sector, para impulsar la cooperación y conseguir avances que ofrezcan a los usuarios soluciones completas y compatibles entre sí. ONVIF proporciona y promueve interfaces estandarizadas para la interoperabilidad efectiva de productos de seguridad físicos basados en IP. Este modelo simplifica la integración a nuestros socios y abre la puerta a combinar los dispositivos Axis con una gran variedad de sistemas.

IoT: abiertos al futuro
Con el Internet of Things (IoT) ha llegado un profundo cambio en la conectividad y los dispositivos Axis participan de este ecosistema en constante evolución. Axis es compatible con protocolos como MQTT, utilizados en el universo IoT. Con Axis, sus dispositivos no solo están conectados: forman parte del prometedor mundo del IoT.

Integración con la nube: la innovación toca el cielo
En el campo de la conectividad digital, Axis explora la integración con la nube mediante API diseñadas para una interacción ágil con las principales plataformas, como Microsoft Azure y Amazon Web Service (AWS). A medida que la tecnología vaya evolucionando, incorporaremos otras tecnologías en la nube, como MQTT para los servicios de mensajería y WebRTC para la transmisión de vídeo y audio. El objetivo es permitir a los usuarios sacar el máximo partido a la tecnología en la nube.

Modularización de la plataforma a través de ACAP

Uno de los rasgos distintivos de AXIS OS es que permite la modularización de la plataforma a través de la Plataforma de aplicaciones de cámaras AXIS (ACAP). ACAP es un entorno en el que los desarrolladores pueden crear e implantar aplicaciones y servicios, como analítica de vídeo, analítica de audio y otras extensiones personalizadas para dar respuesta a las necesidades concretas de una empresa. Las aplicaciones ACAP son independientes de las funciones esenciales de AXIS OS y pueden instalarse, actualizarse y eliminarse sin que ello afecte al resto del sistema. Además, pueden comunicarse entre sí y con sistemas externos usando protocolos estándar y API.

Escalabilidad y rendimiento
ACAP utiliza la arquitectura de microservicios del sistema operativo en los dispositivos Axis. Es posible ampliar o reducir de forma independiente cada servicio en función de la demanda o la carga. Este modelo mejora el rendimiento y la disponibilidad globales del sistema y también garantiza una mayor eficiencia en el uso y la asignación de los recursos.

Adaptabilidad y personalización
Con ACAP, los dispositivos Axis son más versátiles, adaptables y personalizables, porque admiten diferentes tipos de integraciones, analítica y dispositivos. Además, ACAP reduce el nivel de interdependencia y aumenta la cohesión de la plataforma, porque cada aplicación presenta un bajo nivel de interdependencia con AXIS OS y un alto nivel de cohesión interno.

Fiabilidad y fácil mantenimiento
Cada servicio se puede probar, supervisar y depurar de forma independiente y aislada. Esta fórmula facilita el diagnóstico y la solución de los problemas, además de mejorar la resiliencia del sistema y la tolerancia en caso de fallos. Y pone en relieve la calidad de AXIS OS.

AXIS OS para equipos de TI

Crear unos mecanismos adecuados de automatización e integración en la infraestructura de TI permite tener los controles de seguridad correctos y ahorrarse tiempo y dinero. Además, se minimiza toda complejidad innecesaria en el sistema. Estas son algunas de las ventajas que puede obtener al combinar dispositivos Axis y software integrado en la infraestructura de TI de la empresa:

> Minimice la complejidad del sistema eliminando las redes provisionales de dispositivos físicos dedicados.

> Ahorre costes con procesos de incorporación y gestión de dispositivos automatizados

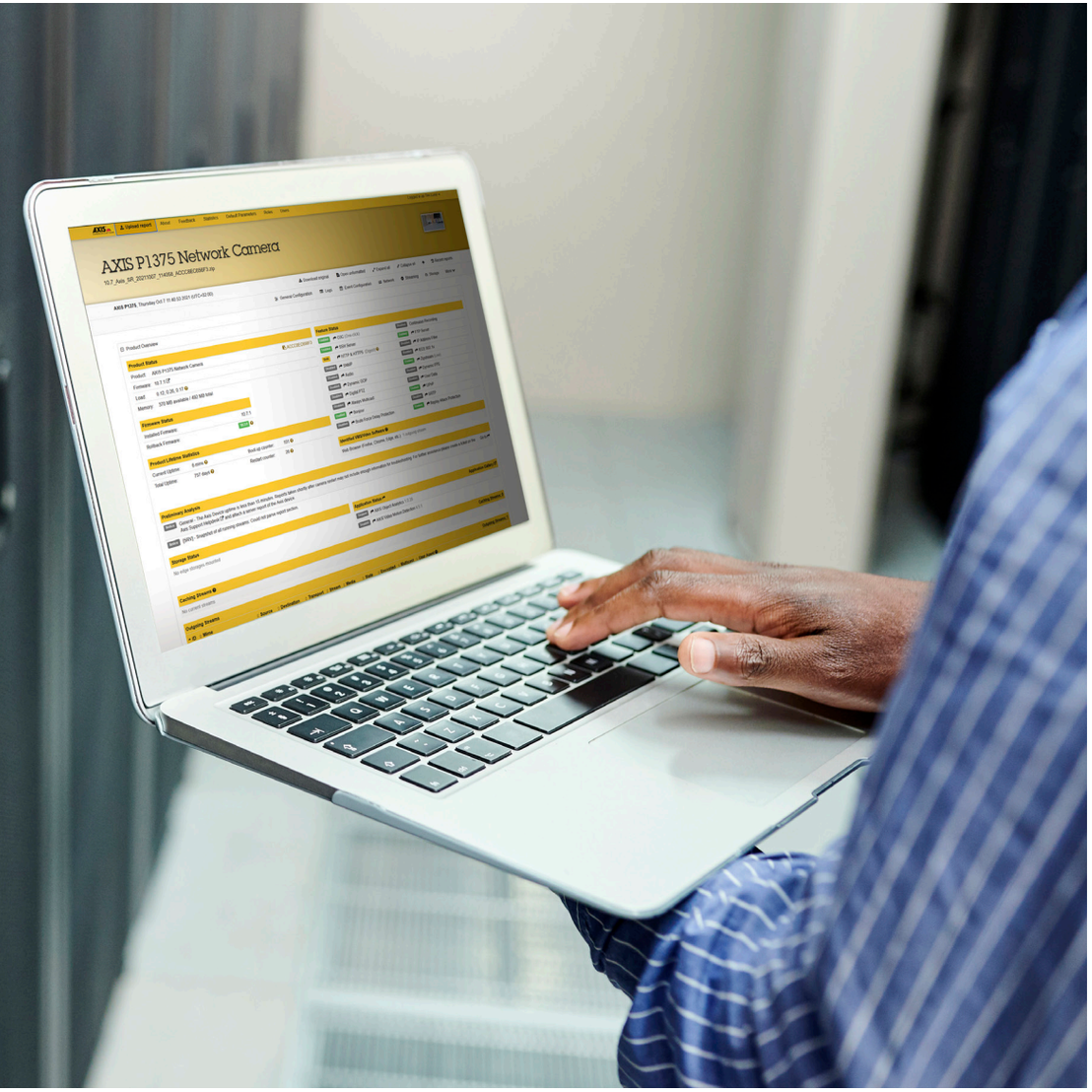
> Aproveche el potencial de los controles de seguridad de las redes de confianza cero como IEEE 802.1X e IEEE 802.1AR

> Aumente la seguridad general de la red introduciendo el cifrado de datos en la raíz con la ayuda de IEEE 802.1AE MACsec. De este modo, el dispositivo Axis puede contribuir a la seguridad de la red, por ejemplo.

> Supervise el dispositivo Axis con protocolos estandarizados como Remote Syslog para tener registros y controlar su estado, por ejemplo.

Redes seguras basadas en principios de confianza cero
Crear redes seguras multiservicio basadas en principios de confianza cero es clave para eliminar los sistemas aislados que funcionan por su cuenta. La integración de dispositivos Axis en la infraestructura de TI de la empresa usando protocolos y estándares de red abiertos y bien definidos abre la puerta a una mejora de la seguridad, unos costes de configuración y mantenimiento más bajos, y un mayor control a través de políticas de TI.

Un gran aliado de los departamentos de TI
Los departamentos de TI son los que velan por la seguridad de las redes de TI y los dispositivos Axis son grandes aliados para ellos. Son fáciles de integrar, mantener y controlar gracias a su versatilidad y también a su similitud con las soluciones de TI, definidas por protocolos de red IEEE e IETF abiertos y estandarizados y un diseño compartido. Los dispositivos Axis son como "ciudadanos de confianza" en las redes de los clientes y contribuyen a la mejora de la seguridad.



¿Hablamos?

AXIS OS es el secreto detrás de la fiabilidad de los dispositivos Axis. Es lo que explica su excelente calidad de imagen y de audio, entre muchas otras cosas.

Su diseño tiene muy en cuenta lo que buscan los usuarios de dispositivos de red: valor a largo plazo, un elevado nivel de ciberseguridad y una integración sencilla.

Nos encantaría tener la oportunidad de explicarle exactamente el valor añadido que pueden aportar los dispositivos Axis a su empresa u organización.

¿Hablamos hoy?

O descubra nuestros dispositivos en axis.com

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones diseñadas para mejorar la seguridad y la operatividad de las empresas. Como líder del sector y empresa especializada en tecnología de redes, Axis crea soluciones de videovigilancia, control de acceso, intercomunicadores y sistemas de audio. Su valor se multiplica gracias a las aplicaciones inteligentes de analítica y una formación de primer nivel.

Axis cuenta aproximadamente con 4.000 empleados especializados en más de 50 países y proporciona soluciones a sus clientes en colaboración con sus socios de tecnología e integración de sistemas. Axis fue fundada en 1984 y su sede central se encuentra en Lund (Suecia).