Experience the power of a single platform

Purpose-built for long-term value, cybersecurity, and integration

AXIS COMMUNICATIONS

Powering your Axis network devices

AXIS OS is the Linux-based operating system used in most of your Axis network devices. It's the heartbeat of more than 200 Axis products and tens of millions of devices deployed at customer sites. AXIS OS reflects a commitment to innovation, reliability, and seamless integration. Axis software is the reason our devices are so dependable and why they provide such great image quality – and we make Axis software better with every release. In fact, 80% of our research and development revolves around software development.

We add new features and improve existing ones all the time. We also continuously increase security through vulnerability patching for devices built on AXIS OS, making them better, and allowing more use cases to be solved more securely.

AXIS OS is purpose-built to live up to the most important criteria for network devices: long-term value, high standards for cybersecurity, and ease of integration.

Purpose-built for Axis devices
Built by the AXIS OS development organization and rooted in the stability of Linux Yocto OpenEmbedded, AXIS OS surpasses generic builds because it's perfectly optimized for the unique demands of Axis edge devices such as cameras, speakers, and access control equipment.

Long-term value
AXIS OS ensures your devices are always on. Designed for 24/7 operation, it offers consistent and responsive performance that aligns with the demands of your applications for the long haul, be it day or night.

Robust cybersecurity
At the core of AXIS OS is dedication to cybersecurity. AXIS OS, with its built-in security architecture, helps you safeguard your devices. With secure software development practices and vigilant vulnerability management, AXIS OS ensures that your data and devices remain resilient against emerging threats.

Seamless integration
AXIS OS incorporates VAPIX, ONVIF, and more, helping your Axis network devices integrate easily into diverse ecosystems. This integrability provides a smooth, interconnected experience for users and developers.

AXIS OS in numbers

900 developers

24,000,000 lines of code written

4000 code commits daily

4,000,000 automated tests daily

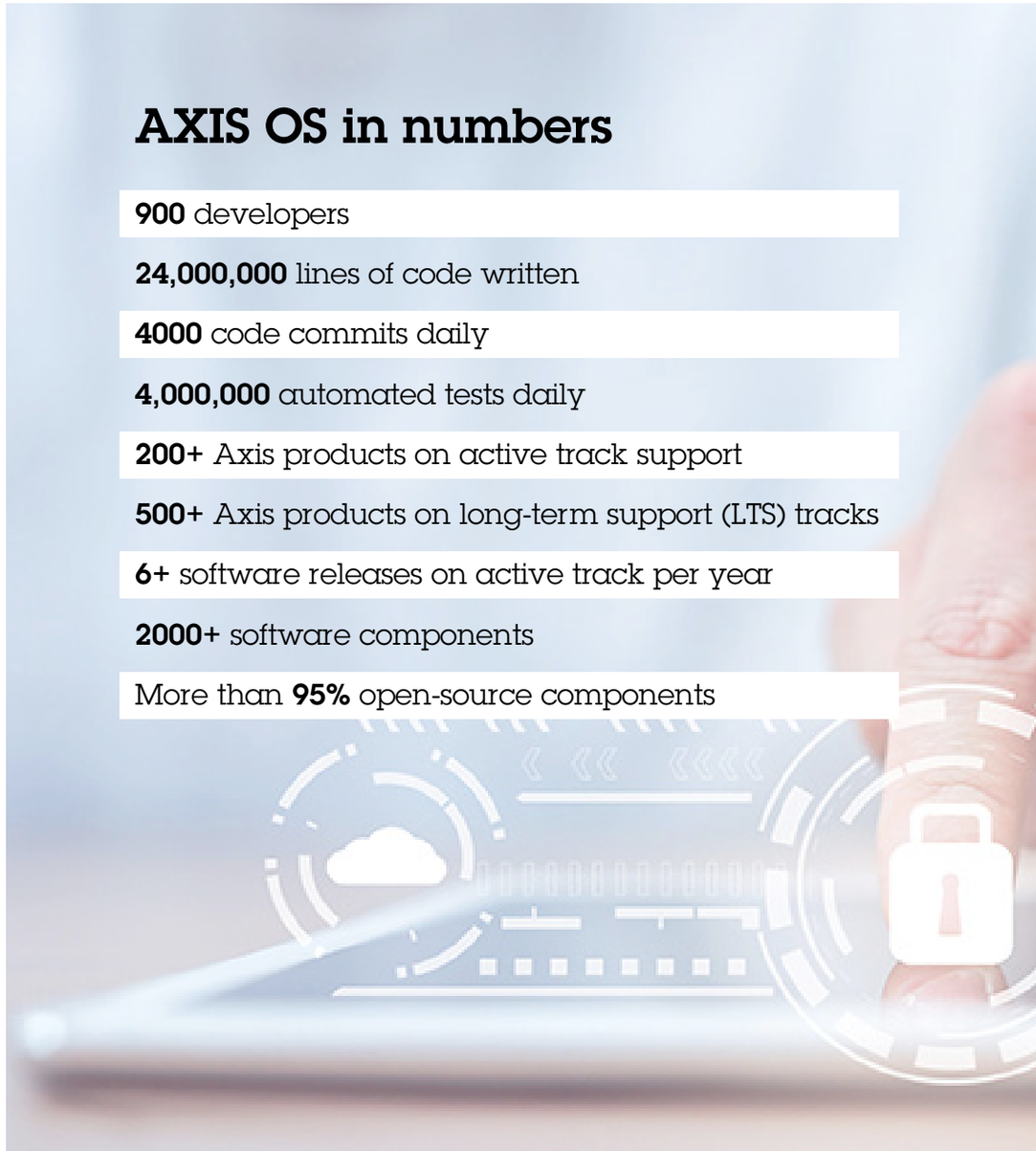
200+ Axis products on active track support

500+ Axis products on long-term support (LTS) tracks

6+ software releases on active track per year

2000+ software components

More than **95%** open-source components



Purpose-built for Axis devices

When we designed AXIS OS, we focused specifically on performance, integration, security, and software quality for edge devices.

Rooted in the stability of Linux Yocto OpenEmbedded, AXIS OS provides a single unified platform for all your Axis network devices, offering a consistent experience across a diverse array of products.

On the following pages, you can read more about the valueof an operating system specifically made for edge devices and about the power of one platform.

Made for excellence at the edge

In a landscape dominated by general-purpose solutions, AXIS OS isn't just another Linux operating system. It transcends the conventions of generic Linux builds to provide a solution finely tuned to the specific needs of edge devices. This specialization supports performance, reliability, and security unique to Axis products.

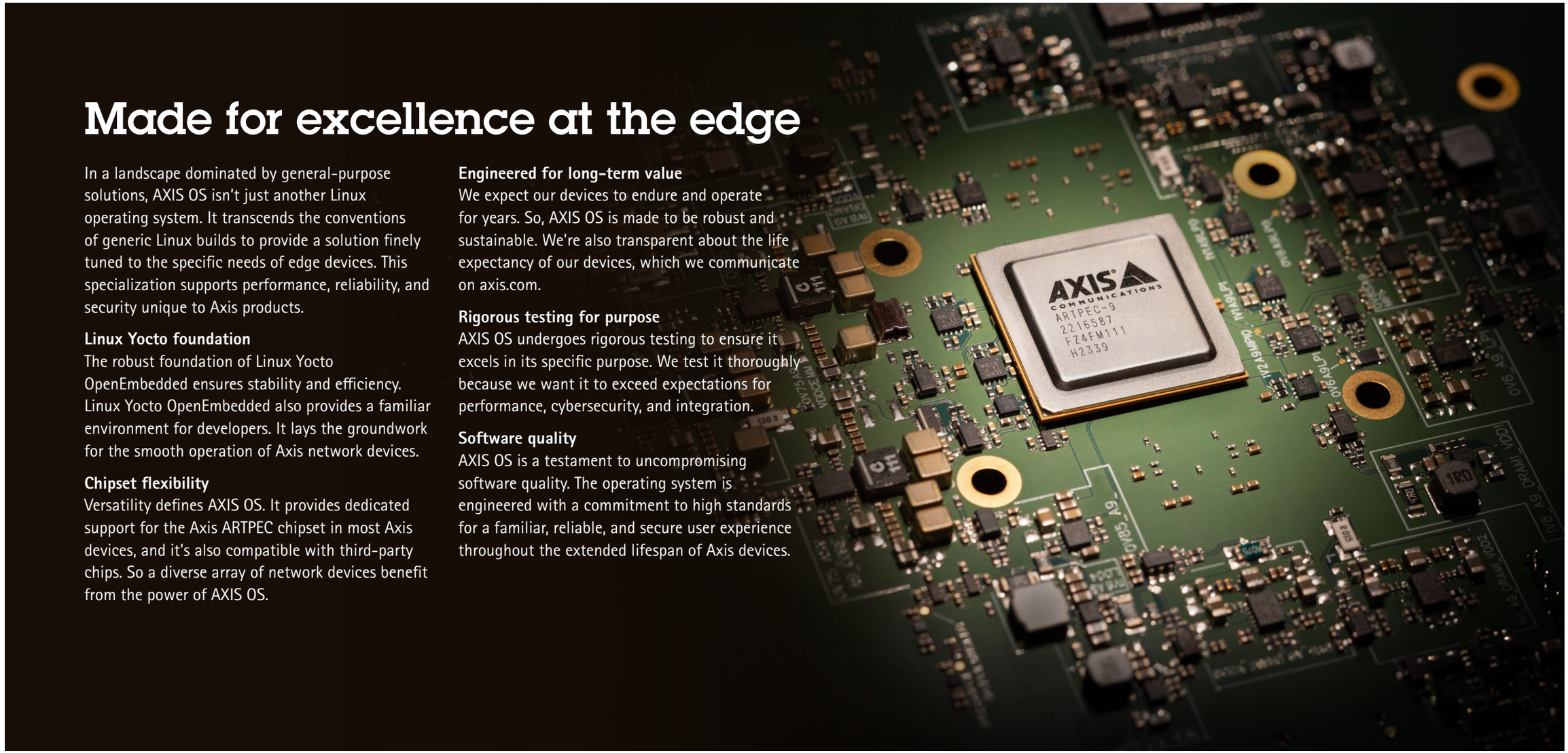
Linux Yocto foundation
The robust foundation of Linux Yocto OpenEmbedded ensures stability and efficiency. Linux Yocto OpenEmbedded also provides a familiar environment for developers. It lays the groundwork for the smooth operation of Axis network devices.

Chipset flexibility
Versatility defines AXIS OS. It provides dedicated support for the Axis ARTPEC chipset in most Axis devices, and it's also compatible with third-party chips. So a diverse array of network devices benefit from the power of AXIS OS.

Engineered for long-term value
We expect our devices to endure and operate for years. So, AXIS OS is made to be robust and sustainable. We're also transparent about the life expectancy of our devices, which we communicate on axis.com.

Rigorous testing for purpose
AXIS OS undergoes rigorous testing to ensure it excels in its specific purpose. We test it thoroughly because we want it to exceed expectations for performance, cybersecurity, and integration.

Software quality
AXIS OS is a testament to uncompromising software quality. The operating system is engineered with a commitment to high standards for a familiar, reliable, and secure user experience throughout the extended lifespan of Axis devices.



Experience the power of a single platform

Our commitment to excellence transcends product categories and is embodied in what we call the power of a single platform. With support for more than 200 products, from body worn cameras to explosion-proof solutions, from PTZ cameras to sirens, and from speakers to intercoms, our unified platform is meant to deliver for our partners and customers.

Consistency in action
AXIS OS delivers across a diverse array of products. The same APIs and behaviors are shared by all our products. One platform ensures that integrators and developers can incorporate new Axis devices into their systems without complex, device-specific drivers. This not only accelerates integration but also future-proofs solutions, allowing for the swift adoption of new products within the ever-expanding Axis ecosystem. It ensures a uniform experience for end customers. And it saves time and money for developers because every integration solution works on every AXIS OS device.

Versatility without complexity
The power of one platform is also about a single platform that allows for diversity without introducing complexity. Whether you're integrating a PTZ camera into a surveillance system or incorporating a speaker into an intelligent audio solution, the process is consistent. This versatility extends beyond compatibility to provide a harmonious experience and many possibilities for creating integrated solutions tailored to unique needs.

Unified security
In a world where cybersecurity is paramount, the power of one platform is also found in support for a unified solution across the entire product spectrum. Maintaining security isn't a product-by-product ordeal. When a vulnerability is identified and addressed, the fix is propagated across all supported products. This not only streamlines security management but also facilitates a swift, collective response to emerging threats. And it saves time and resources and reinforces the resilience of the entire Axis ecosystem.

Long-term value

AXIS OS supports predictable value throughout the lifecycle of your devices. Stable, robust architecture keeps downtime to a minimum.

We deliver software updates – including brand-new features – over many years. With extensive documentation, helpful tools, and intuitive interfaces, Axis devices are both easy to use and easy to maintain. And we offer transparent and dependable release schedules so you can plan maintenance to suit the needs of your organization.

On the following pages, you can read more about the quality of AXIS OS lifecycle management and software support.

Software you can depend on

The quality of AXIS OS is important to us. With approximately 900 developers and 4000 code commits into the AXIS OS main branch every day, our operating system is continuously transforming to adapt to market needs. Accommodating two builds per day for each of our over 200 products means we face a staggering 182,500 builds annually, allowing for iterative testing and added value.

Rigorous testing
Maintaining software stability also demands rigorous testing. In fact, our systems execute a remarkable 4 million diverse test cases daily. These are complemented by more than 4000 daily code commits to patch vulnerabilities and improve quality. It adds up to over 1 billion tests and more than 1,000,000 code commits annually. We also let customers and partners deliver direct feedback about AXIS OS through data sharing.

Continuous improvement
Imagine that your camera is getting smarter and faster, while consuming less and less power. AXIS OS isn't static, it's dynamic, as we continuously make improvements. Through regular updates and enhancements, Axis devices on the AXIS OS active track evolve with technological advancements. This means the product you buy today will gain new features and become more valuable throughout its lifetime.

Clear Support Lifecycles
Even before a customer buy an Axis device, we transparently communicate the End-of-support date. Until that date, we promise to continue to protect and maintain your device, providing stability, security, and the long-term peace of mind.

Supporting the device lifecycle

One of the benefits of using AXIS OS is that it supports the device lifecycle, from installation to maintenance to replacement. AXIS OS provides tools and resources to help you manage and optimize your Axis devices throughout their lifespan.

Easy installation and configuration
AXIS OS simplifies the installation and configuration of Axis devices by providing wizards, templates, and profiles that guide you through the process. You can also use Axis device management software to install and configure multiple devices at once, saving you time and effort..

Continuous monitoring and diagnostics
With your consent, AXIS OS monitors and analyzes the performance and status of Axis devices by collecting health monitoring data in the form of logs, reports, and alerts. This helps you identify and resolve any issue. And it lets us improve our software with each release.

Long-term support and compatibility
AXIS OS offers long-term support for Axis devices with regular security patches and bug fixes. Our long-term support tracks the compatibility of Axis devices and applications by minimizing changes and disruptions. Devices running on AXIS OS usually have a software support for around 8-12 years in average.

Trust and commitment
AXIS OS is designed to meet the expectations and needs of customers who value trust and quality. AXIS OS sets a clear and transparent life expectancy for each product and keeps it on track as much as possible. Axis also maintains long-term relationships by providing customers with the best possible service and support.

AXIS OS beta

AXIS OS beta is a benefit for developers and integrators who want to test and evaluate the latest features and functionalities of AXIS OS before they're officially released. AXIS OS beta can be used to perform early compatibility tests on selected devices, verify upcoming security updates, and access upcoming features.

Some of the benefits of using AXIS OS beta are that you:

> Get a preview of the new and improved features and functionalities AXIS OS will offer in the future, such as edge analytics, IoT connectivity, and platform modularization.
> Can provide feedback and suggestions to Axis that help shape the development and improvement of AXIS OS.
> Can prepare and adapt your applications and systems for upcoming changes and updates in AXIS OS to avoid potential issues.

You can read more about AXIS OS beta here.

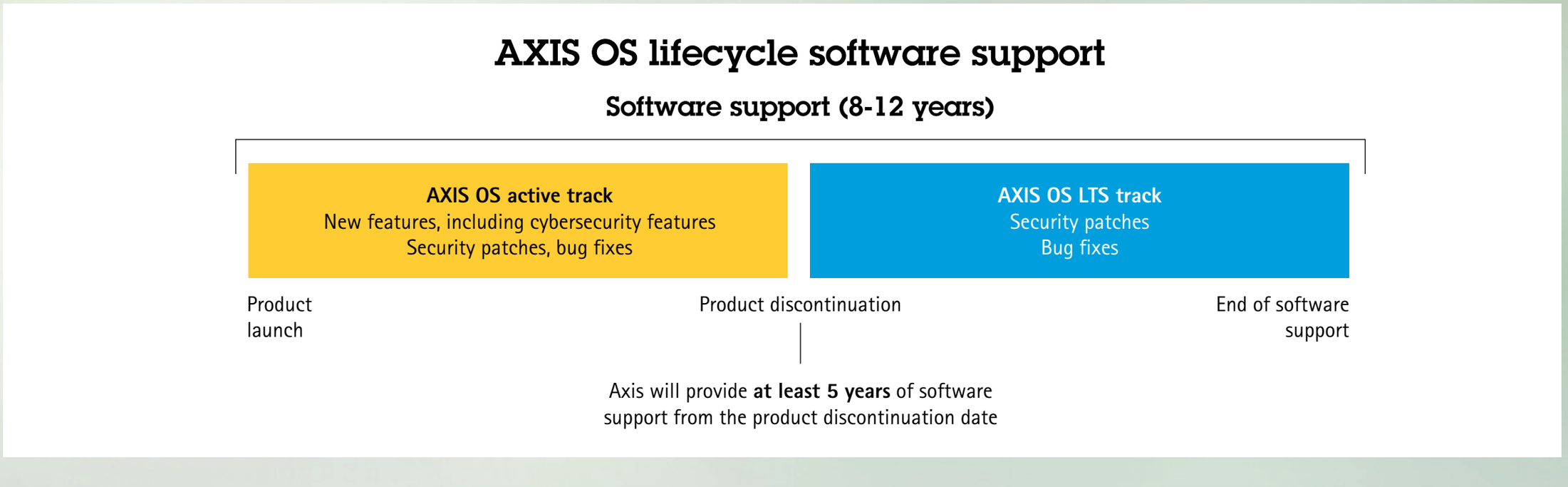
AXIS OS lifecycle software support*

AXIS OS lifecycle support consists of various tracks. Active and long-term support are the main tracks. There are also product-specific support (PSS) tracks to serve individual product lifecycles.

The minimum lifetime of an Axis device exceeds industry standards. A robust 5-year hardware warranty is complemented by AXIS OS software support over many years. Most devices have an impressive AXIS OS lifetime of 8-12 years.

It works like this:

1. When Axis releases a new device, only the AXIS OS active track is available. During the initial post-release period, you benefit from continuous updates and improvements, including new features.
2. A long-term support (LTS) track becomes available as an alternative to the active track within two years of product release. At this point, you can choose either the active track or the long-term support track. Products on the long-term support track are supported with patches and bug fixes.
3. Two to four years after release when a device is discontinued, the active track for that device is discontinued as well. At this point, all devices are automatically moved to the long-term support (LTS) track, where they are supported with patches and bug fixes for a minimum of 5 years.



* *AXIS OS email notification service – Subscribe to AXIS OS email notification service to get regular updates of the releases and other important information.*

Which software support track is right for you?

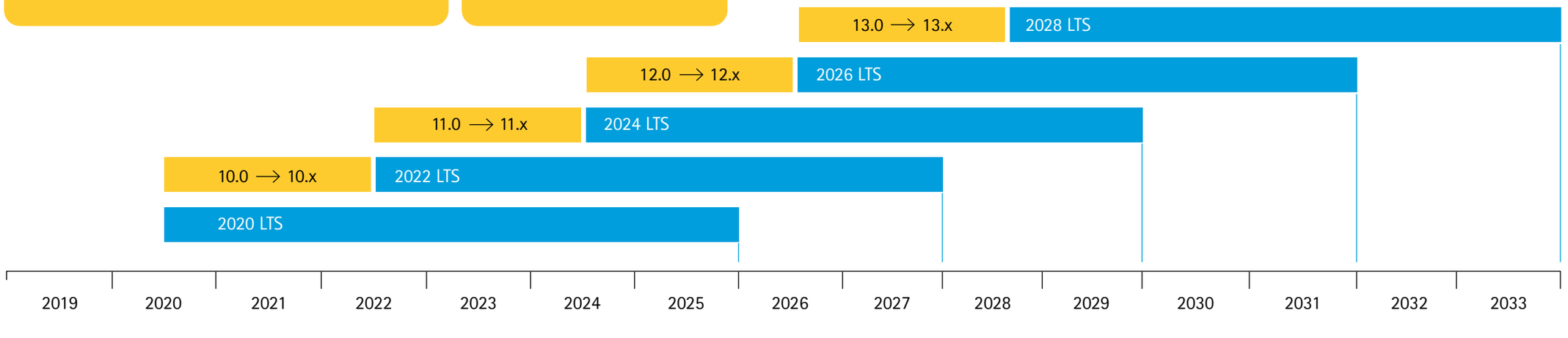
Once both active and LTS tracks are available, customers can choose the track best suited to their needs with guidance from Axis.

Active track
AXIS OS active track delivers the most up-to-date, feature-rich experience for the AXIS OS operating system. Tailored for customers who want to benefit from immediate access to the latest features and enhancements, this is the only track available for newly released devices. It helps users stay on top of evolving device capabilities: New cybersecurity features are added for even more secure operation and existing features receive ongoing enhancements. With devices on the AXIS OS active track, you get more from your products without extra cost even years after you purchase them. If you don't have compatibility dependency, this is the track for you for as long as it is available.

Long-term support (LTS) track
If you're looking for API consistency and compatibility, you should choose the long-term support (LTS) track once it becomes available. The LTS track is focused on backward compatibility and provides regular security patches and bug fixes. It maintains cybersecurity rather than delivering new cybersecurity features. Likewise, it doesn't add new features or functionality but rather minimizes changes to reduce disruption. The LTS track is suitable for customers who want a well-integrated third-party system. Each LTS track is supported for 5 years, and LTS tracks are issued every 24 months, based on a regular active track release. All devices are automatically moved to the LTS track when they are discontinued.

The illustration shows the AXIS OS active track side by side with the LTS tracks introduced throughout the years. Roughly every 24 months, a new LTS track is created and the major AXIS OS version is incremented. For example, in 2026 we create the new AXIS OS 2026 LTS, and then switch from AXIS OS 12 to AXIS OS 13.

With Axis device software upgrade guide, you simply state your current and target version, and the guide will give you a step-by-step instruction for recommended upgrade path.



Cybersecurity in focus

AXIS OS adheres to security-by-design approach. Our Axis Security Development Model (ASDM) defines processes and tools that reduce the risk of vulnerabilities during software development and beyond.

Our hardware-based cybersecurity platform, Axis Edge Vault, ensures secure boot and a tamper-protected environment for the storage of customer-loaded cryptographic keys. The AXIS OS core software consists of well-tested open-source components. And every release is complemented by a software bill of materials (SBOM) showing that AXIS OS is up to date and patched for known vulnerabilities.

AXIS OS also complies with and is certified to ETSI EN 303 645, which focuses specifically on edge-device security. FIPS 140 compliance ensures AXIS OS adheres to the latest cryptographic standards defined by the National Institutes of Technologies (NIST). And finally, as an approved CVE Numbering Authority, we follow best practices for identifying, managing, and disclosing vulnerabilities.

On the following pages, you can read more about our Axis Security Development Model, Axis Edge Vault, vulnerability management, and the concept of unified security.

Developed and maintained with cybersecurity in mind

The Axis Security Development Model (ASDM) effectively integrates cybersecurity into the software development lifecycle. It describes security activities to consider during the phases of software development. The purpose is to reduce vulnerabilities – as well as development costs – by establishing a baseline for cybersecurity and by providing guidance.

ASDM: made by Axis
The Axis Security Development Model is not a standard "off-the-shelf" framework. Instead, we reviewed many cybersecurity standards and frameworks – such as ISO 27001, IEC 62443, NIST, BSIMM, and CMMC. The common thread between them is that security is incorporated into all the development phases. With that as our starting point, we adapted our model to fit our company culture, development practices, and the type of products we provide.

The ASDM toolbox
The ASDM toolbox prescribes a range of activities that address a variety of security problems. Some examples are risk assessment, threat modeling, threat model testing, static code analysis, vulnerability scanning, and vendor assessment. Development teams choose which activities to engage in depending on the kind of software to be developed. The goal is better cybersecurity rather than just compliance with a process.

The added benefit of outside expertise
Most of the heavy lifting of secure software development is carried out within Axis, but we also recognize that we can benefit from the knowledge and expertise of others. So, we hire specialized companies for penetration testing. And we have the public AXIS OS bug bounty program, where we offer financial rewards to security researchers for helping us identify vulnerabilities.

Governance	Training	ASDM line meeting	ASDM assessment	Security compliance and standards

Requirements	Design	Implementation	Verification	Deployment
Risk assessment	Threat modeling	Static code analysis	Threat model test	Vulnerability management
Vendor assessment		Software composition analysis	External penetration test	Incident management
Data privacy			Vulnerability scanning	Product/solution security status
Open source security assessment			Internal security assessment	Bug bounty program

Visit Axis Trust Center | *Find out how Axis and its products support cybersecurity and security compliance with various regulations and standards. Access a wide range of information, from cybersecurity practices and measures, to certificates, guides and reports.*

Built-in cybersecurity

Protection from the inside out
Axis Edge Vault is our hardware-based cybersecurity platform. It provides a solid foundation for ensuring your Axis devices are a trusted and reliable part of your network. But this strong hardware-based foundation would be useless without an operating system that supports its full potential. AXIS OS uses the Edge Vault platform to provide enhanced security on the edge for every use case.

Edge Vault includes features such as:

Secure key storage
Secure keystore involves cryptographic computing modules for the secure storage and computing of cryptographic keys. They safeguard device identity and other sensitive information from unauthorized access – even if the device is compromised. The cryptographic computing modules used are the Trusted Execution Environment (TEE) built into the system-on-chip (SoC) as well as a dedicated secure element or a Trusted Platform Module (TPM 2.0), which are separate chips on the printed circuit board (PCB).

Signed OS and secure boot
Signed OS means we code-sign the device software image. Together, signed OS and secure boot mean devices can download and run only the genuine AXIS OS operating system. This adds an extra layer of protection against tampering in the software and hardware supply chains.

Axis device ID
Axis device ID is IEEE 802.1AR-compliant and enables secure device identification and onboarding on a network. It acts as a genuine passport for every Axis device manufactured.

Encrypted file system
File system encryption protects data in the file system from being extracted or tampered with while the device is not in use, such as during transit from a system integrator to the end customer.

Signed video
Signed video lets users verify the authenticity of captured video and that it hasn't been tampered with.

Axis Edge Vault cybersecurity platform

Cryptographic computing modules	Features	Use cases
Secure element TPM 2.0 SoC security (TEE)	Secure boot Signed OS Axis device ID Secure keystore Signed video Encrypted file system	Trusted device identity Secure key storage Video tampering detection Supply-chain protection

*Note: Not all device models support all the Axis Edge Vault features. Check the datasheet or the Axis product selector for confirmation of the features supported by specific products.

Vulnerability management

To minimize our customers' risk of exposure, we implement industry best practices in managing and responding transparently to vulnerabilities.

Best-in-class vulnerability management
There's no way to guarantee that products and services delivered by Axis are entirely free from vulnerabilities. This is not unique for us, but rather a shared condition for all software and services. But we make a concerted effort to identify and mitigate potential vulnerabilities at every stage, reducing the risk of deploying Axis products and services in customer environments.

A CVE Numbering Authority,
Axis is a CVE Numbering Authority (CNA). We joined the CVE Program to work with like-minded companies on improving vulnerability management. We align the way we handle, disclose, and patch vulnerabilities with the international framework provided by this non-profit organization and with our public vulnerability management policy.

Transparent management you can rely on
Axis uses the well-known CVSS rating system (Common Vulnerability Scoring System) to rate vulnerabilities related to either code developed by Axis or third-party open-source code. We assess vulnerabilities in open-source code according to how relevant they are for our products when best practice recommendations are applied. In our Security Advisories we transparently disclose all CVE related to AXIS OS. You can LSO subscribe to the Axis Security Notification Service to receive information about vulnerabilities and other security-related matters for Axis products.

Partnerships with security researchers and organizations
We embrace and appreciate the work of individual security researchers and security research organizations who contact us to report vulnerability findings. We don't hesitate to disclose and patch them. Handling vulnerabilities correctly and transparently with an ethical, responsible disclosure process is what's important – no matter how the vulnerability is discovered.

An all-in-one security experience

In network devices powered by AXIS OS, hardware and software components work together to enable customers to securely operate the devices, their services, and the systems they are connected to. Layer upon layer of comprehensive protection starts with a security foundation and a hardware-based security platform and continues up to the software. Devices powered by AXIS OS are guarded by this layered, defense-in-depth approach to cybersecurity. It increases the cumulative security of data, applications, and processes.

So, you can rest assured that no matter what an Axis device is used for, protection and secure communication is available, allowing for proper and secure integration into third-party systems.

Access control

Access control management
Local user device management with password complexity indicator
Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality

Privacy
Use of diagnostics data
Minimalistic approach to how much customer-specific data should be stored

Application

Application security
TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC)
Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog

Operating system

Encryption and data protection
OpenSSL 1.1.1 and 3.0
X.509 certificate PKI and cryptography
Transport layer security (TLS 1.2/TLS 1.3)
SD card encryption (AES-XTS-Plain64 256bit)
Encrypted file system (AES-XTS-Plain64 256bit),
Signed video

Default security
HTTPS enabled by default
Brute-Force Delay Protection
Host-based Firewall
Network time security (NTS)
Insecure TLS versions disabled
UART/Debug port disabled

Enterprise network security
IEEE 802.1X (network access control)
IEEE 802.1AR (secure device identity)
IEEE 802.1AE (MAC security, MACsec)

AXIS OS Operating System
Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others.
Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.

Silicon assisted security (chip)

Hardware root-of-trust
ARM-based system-on-chip (SoC) security
Trusted Execution Environment (TEE/OP-TEE)
Trusted platform module (TPM 2.0), Secure element

Secure key storage
Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.

Security foundation

Axis Security Development Model
Axis security development model (ASDM)
3rd party penetration tests
Bug bounty program with Bugcrowd
Software Bill of Material (SBOM)

Compliance
Common Criterial EAL
FIPS 140
ETSI EN 303 645

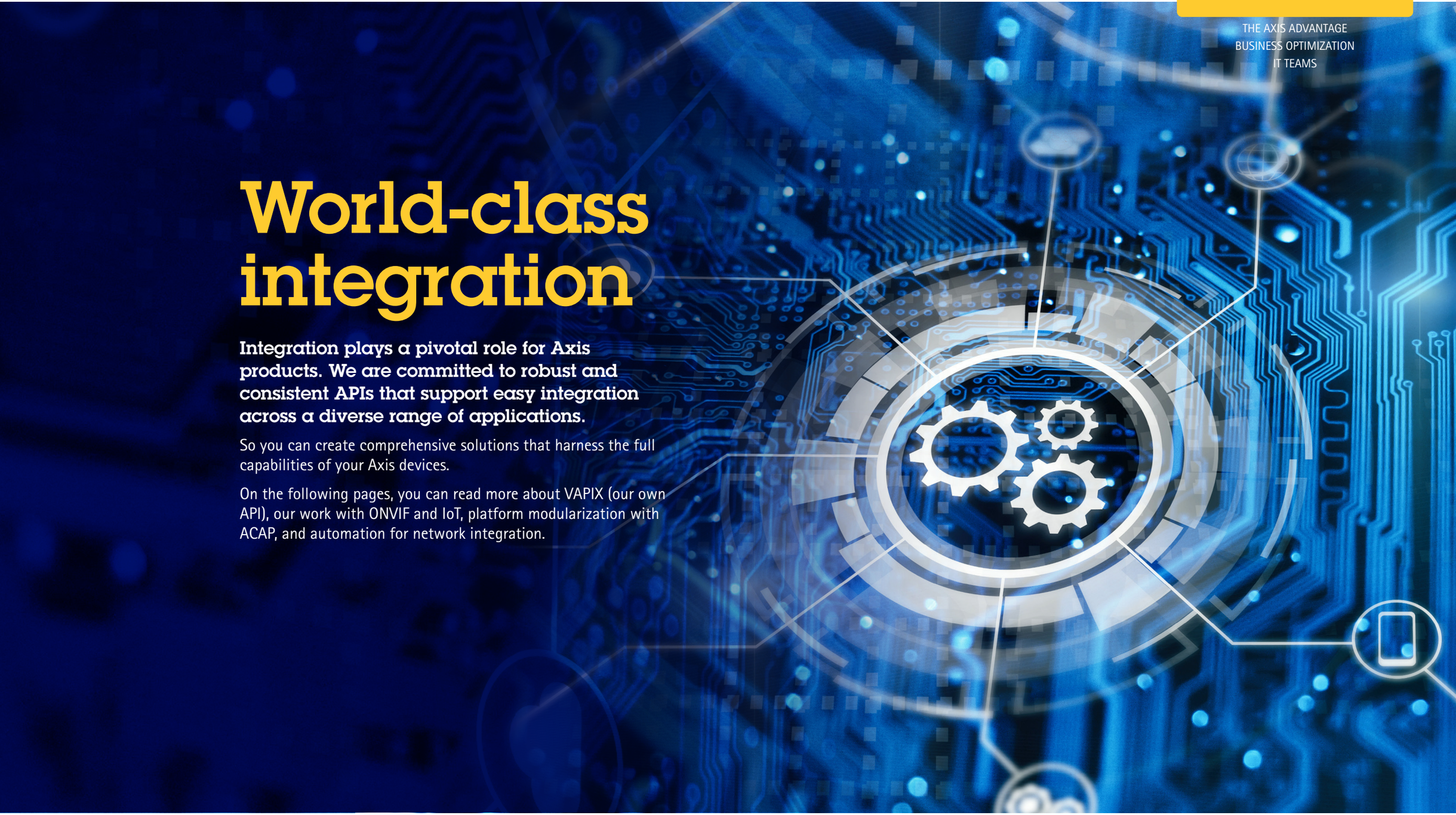
Trusted device identity
Axis Edge Vault cybersecurity platform
Secure boot with Signed OS (code-signing)
Axis Device ID (IEEE 802.1AR)

World-class integration

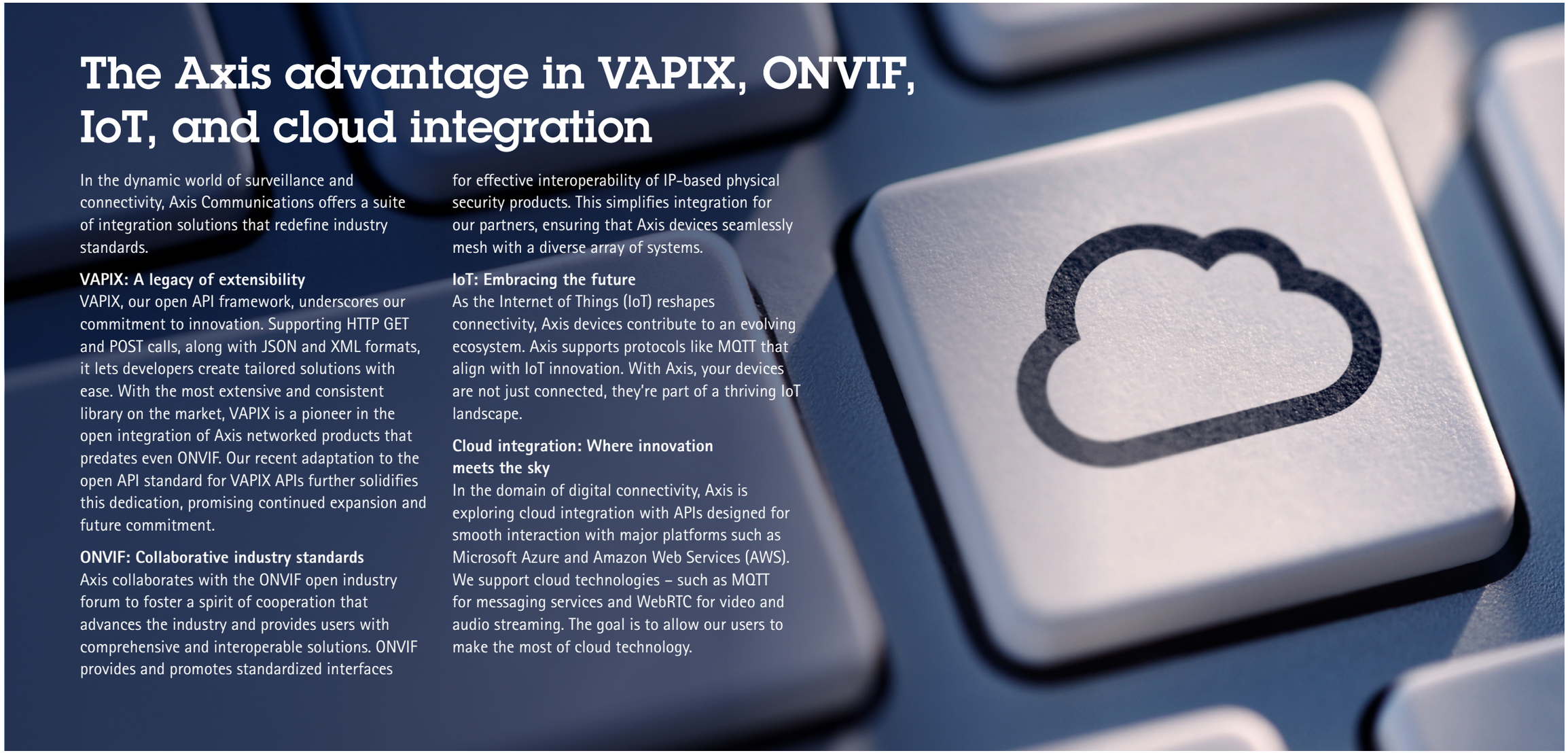
Integration plays a pivotal role for Axis products. We are committed to robust and consistent APIs that support easy integration across a diverse range of applications.

So you can create comprehensive solutions that harness the full capabilities of your Axis devices.

On the following pages, you can read more about VAPIX (our own API), our work with ONVIF and IoT, platform modularization with ACAP, and automation for network integration.



The Axis advantage in VAPIX, ONVIF, IoT, and cloud integration



In the dynamic world of surveillance and connectivity, Axis Communications offers a suite of integration solutions that redefine industry standards.

VAPIX: A legacy of extensibility
VAPIX, our open API framework, underscores our commitment to innovation. Supporting HTTP GET and POST calls, along with JSON and XML formats, it lets developers create tailored solutions with ease. With the most extensive and consistent library on the market, VAPIX is a pioneer in the open integration of Axis networked products that predates even ONVIF. Our recent adaptation to the open API standard for VAPIX APIs further solidifies this dedication, promising continued expansion and future commitment.

ONVIF: Collaborative industry standards
Axis collaborates with the ONVIF open industry forum to foster a spirit of cooperation that advances the industry and provides users with comprehensive and interoperable solutions. ONVIF provides and promotes standardized interfaces for effective interoperability of IP-based physical security products. This simplifies integration for our partners, ensuring that Axis devices seamlessly mesh with a diverse array of systems.

IoT: Embracing the future
As the Internet of Things (IoT) reshapes connectivity, Axis devices contribute to an evolving ecosystem. Axis supports protocols like MQTT that align with IoT innovation. With Axis, your devices are not just connected, they're part of a thriving IoT landscape.

Cloud integration: Where innovation meets the sky
In the domain of digital connectivity, Axis is exploring cloud integration with APIs designed for smooth interaction with major platforms such as Microsoft Azure and Amazon Web Services (AWS). We support cloud technologies – such as MQTT for messaging services and WebRTC for video and audio streaming. The goal is to allow our users to make the most of cloud technology.

Platform modularization through ACAP

One of the key features of AXIS OS is that it enables platform modularization through the AXIS Camera Application Platform (ACAP). ACAP is a framework that lets developers create and deploy applications and services, such as video analytics, audio analytics, and other custom-tailored extensions to meet business requirements. ACAP applications are independent of the core AXIS OS functionalities and can be installed, updated, and removed without affecting the rest of the system. ACAP applications can also communicate with each other and with external systems using standard protocols and APIs.

Scalability and performance
ACAP uses the microservices architecture of the operating system on Axis devices. Each service can be scaled up or down independently according to the demand and load. This improves the overall performance and availability of the system and allows for efficient resource use and allocation.

Adaptability and customization
With ACAP, Axis devices are more versatile, adaptable, and customizable because they support different types of integrations, analytics, and devices. ACAP also reduces the coupling and increases the cohesion of the platform because each application is loosely coupled with the AXIS OS and highly cohesive within itself.

Maintainability and reliability
Each service can be tested, monitored, and debugged independently and in isolation. This simplifies troubleshooting and diagnostics and enhances the system's resilience and tolerance for faults. And it makes AXIS OS stand out when it comes to software quality.

Secure and easy integration and 24/7 monitoring of Axis devices

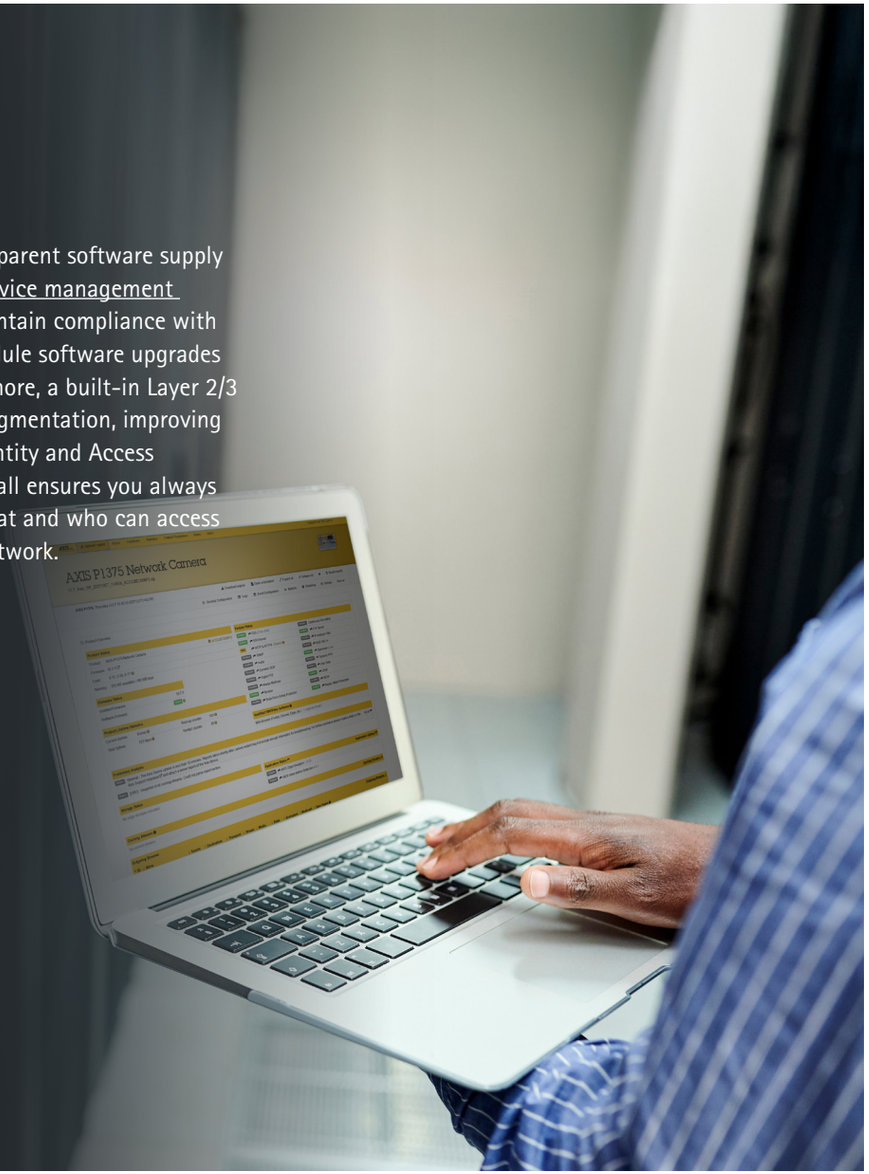
Axis has a strong track record of delivering IT-relevant features and remains committed to ongoing innovation, transparency, and industry best practices. AXIS OS enables secure onboarding and integration of Axis devices into your IT infrastructure, so you can manage and monitor them just like your other IT equipment. It's easy to schedule software upgrades and ensure you always maintain software compliance with your IT policies. With robust cybersecurity, Axis devices are preconfigured from factory and there's no vendor lock-in.

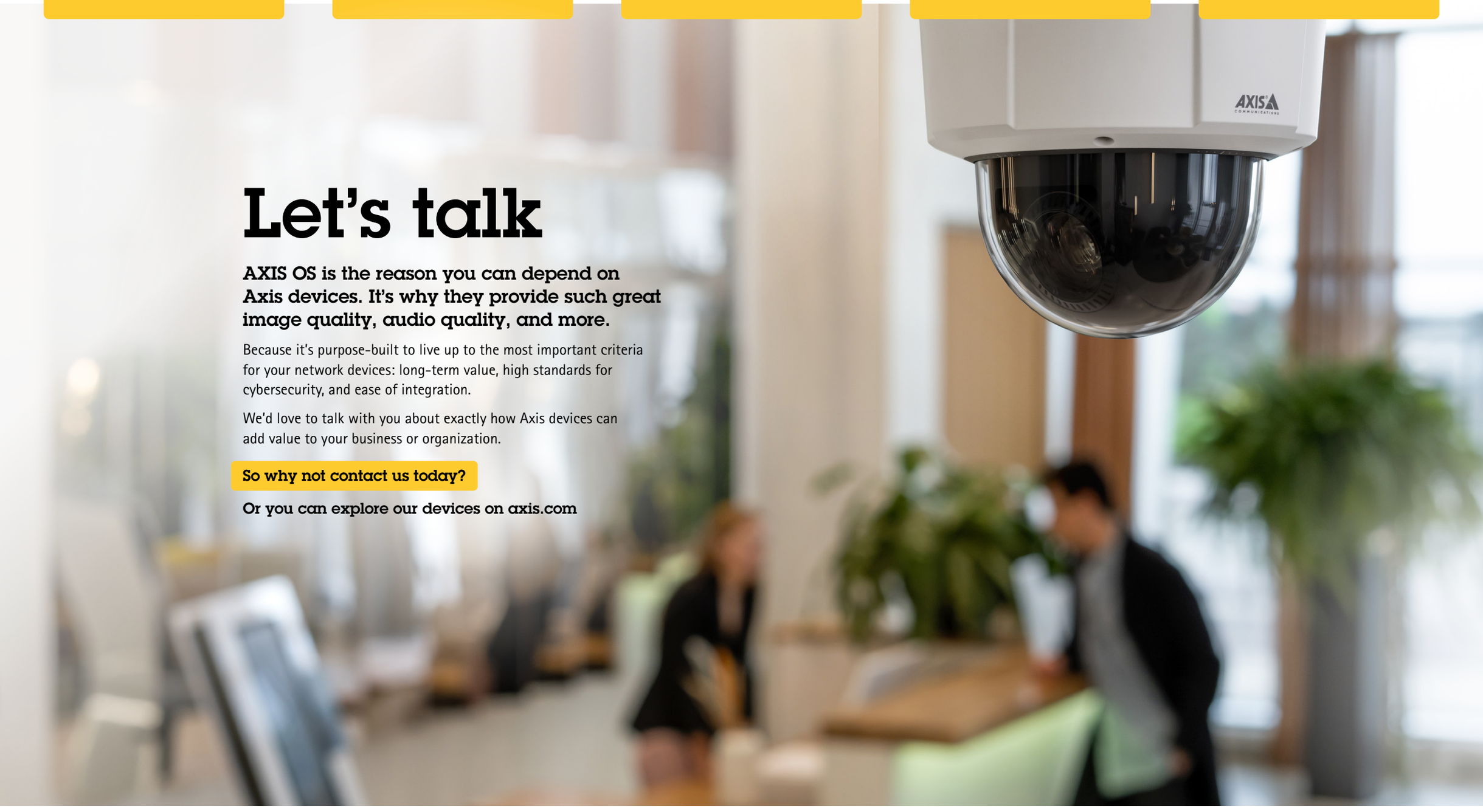
Easy implementation of zero-trust

AXIS OS supports IEEE technologies such as IEEE 802.1AR for secure device identification and authenticity, IEEE 802.1X for network authentication, and IEEE 802.1AE MACsec for fundamental network layer-2 encryption, effectively doubling network security when used in combination with HTTPS and other TLS protocols. So, your network policy engine or access control application can securely onboard and operate Axis devices automatically. Plus, Axis devices are preconfigured from factory with no vendor lock-in. For instance, they support solutions such as Extreme Networks Fabric Attach and HPE Aruba. In addition, the publicly available VAPIX API allows you to integrate Axis devices quickly and flexibly into your system, using only what you need for your specific setup. What's more, centralized identity and access management (IAM) with OAuth 2.0 integration allows you to authenticate your Axis devices using multi-factor authentication (MFA) and tailored password complexity enforcement and rotation.

Secure device lifecycle management

You can monitor all Axis devices on your network, 24/7, with a comprehensive audit log that sends end-to-end encrypted data via remote Syslog and SNMP for SIEM monitoring of configuration changes and login activities. Axis devices support vulnerability scanning using third-party tools such as Tenable Nessus, Rapid7, and others. In addition, AXIS OS Security Scanner Guide offers recommendations on how to solve certain remarks from the scanners and outlines common "false positives," enabling transparent software supply chain audits. With our device management software, it's easy to maintain compliance with your IT policies and schedule software upgrades for Axis devices. Furthermore, a built-in Layer 2/3 firewall enables micro-segmentation, improving network security and Identity and Access management (IAM). This all ensures you always have full control over what and who can access Axis devices over your network.





Let's talk

AXIS OS is the reason you can depend on Axis devices. It's why they provide such great image quality, audio quality, and more.

Because it's purpose-built to live up to the most important criteria for your network devices: long-term value, high standards for cybersecurity, and ease of integration.

We'd love to talk with you about exactly how Axis devices can add value to your business or organization.

So why not contact us today?

Or you can explore our devices on axis.com

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.

©2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.