Eine Plattform – unendliche Möglichkeiten

Speziell entwickelt für langfristige Wertschöpfung, Cybersicherheit und reibungslose Integration

AXIS COMMUNICATIONS

Das Herzstück Ihrer Axis Netzwerkgeräte

Die meisten Axis Netzwerkgeräte nutzen das Linux-basierte Betriebssystem AXIS OS. Es bildet das Herzstück von mehr als 200 Axis Produkten und Millionen Geräten, die bei unseren Kunden im Einsatz sind. AXIS OS verkörpert unseren Anspruch an Innovation, Verlässlichkeit und nahtlose Integration. Die Axis Software macht unsere Geräte bei ausgezeichneter Bildqualität so betriebssicher – und wird mit jedem Release noch ein bisschen besser. Tatsächlich gelten 80 % unserer Forschungs- und Entwicklungsaktivitäten der Software.

Wir fügen ständig neue Funktionen hinzu und optimieren bestehende. Darüber hinaus werden alle Geräte, die auf AXIS OS basieren, durch das Patchen von Sicherheitslücken immer sicherer und leistungsfähiger.

AXIS OS ist speziell auf die wichtigsten Erwartungen an Netzwerkgeräte ausgelegt: langfristige Wertschöpfung, hohe Cybersicherheit und reibungslose Integration.

Maßgeschneidert für Axis Geräte
AXIS OS, das sich bei der Stabilität an Linux Yocto OpenEmbedded orientiert, ist perfekt auf die speziellen Anforderungen von Edge-basierten Axis Geräten wie Kameras, IP-Türcontrollern und Zutrittskontrollsystemen abgestimmt - und damit generischen Betriebssystemen weit überlegen.

Langfristige Wertschöpfung
Mit AXIS OS sind Ihre Geräte immer einsatzbereit. Das Betriebssystem gewährleistet eine gleichbleibend reaktionsschnelle Leistung, die sich bei Tag und Nacht den Anforderungen Ihrer Anwendung anpasst – dauerhaft und rund um die Uhr.

Verlässliche Cybersicherheit
Cybersicherheit ist die DNA des AXIS OS. Mit seiner integrierten Sicherheitsarchitektur trägt AXIS OS zum Schutz Ihrer Geräte bei. Sichere Praktiken bei der Software-Entwicklung und ein wachsames Schwachstellen-Management schirmen Ihre Daten und Geräte dauerhaft auch vor neuartigen Bedrohungen ab.

Nahtlose Integration
AXIS OS ist unter anderem mit VAPIX und ONVIF ausgestattet, wodurch sich Ihre Axis Netzwerkgeräte reibungslos in unterschiedliche Ökosysteme einbinden lassen. Diese Integrationsfähigkeit ermöglicht eine nahtlose und vernetzte Nutzung und Entwicklung.

AXIS OS in Zahlen

900 Entwickler

24.000.000 Programmzeilen

4.000 Code-Commits pro Tag

4.000.000 automatisierte Tests pro Tag

200+ Axis Produkte mit aktivem Track-Support

500+ Axis Produkte auf langfristigen Support-Tracks (LTS)

6+ Software-Releases pro aktivem Track und Jahr

2.000+ Software-Komponenten

Über **95 %** Open-Source-Komponenten

Maßgeschneidert für Axis Geräte

Bei der Entwicklung von AXIS OS standen insbesondere Leistung, Integrationsfähigkeit, Sicherheit und Software-Qualität für Edge-Geräte im Vordergrund.

Mit der Stabilität von Linux Yocto OpenEmbedded als Vorbild bildet AXIS OS eine einheitliche Plattform für all Ihre Axis Netzwerkgeräte.

Auf den folgenden Seiten erfahren Sie mehr darüber, welche Vorteile Ihnen ein Betriebssystem bietet, das extra für Axis Geräte mit integrierten Analysefunktionen entwickelt wurde und diesen als gemeinsame Plattform dient.

Spitzenleistung inklusive

AXIS OS ist nicht einfach ein weiteres Linux-Betriebssystem in einer von Allzwecklösungen dominierten Softwarelandschaft. Stattdessen ist es genau auf die Anforderungen von Geräten mit integrierten Videoanalysefunktionen zugeschnitten und setzt sich damit über die Konventionen generischer Linux-Builds hinweg. Diese Spezialisierung macht die Produkte von Axis konkurrenzlos leistungsfähig, zuverlässig und sicher.

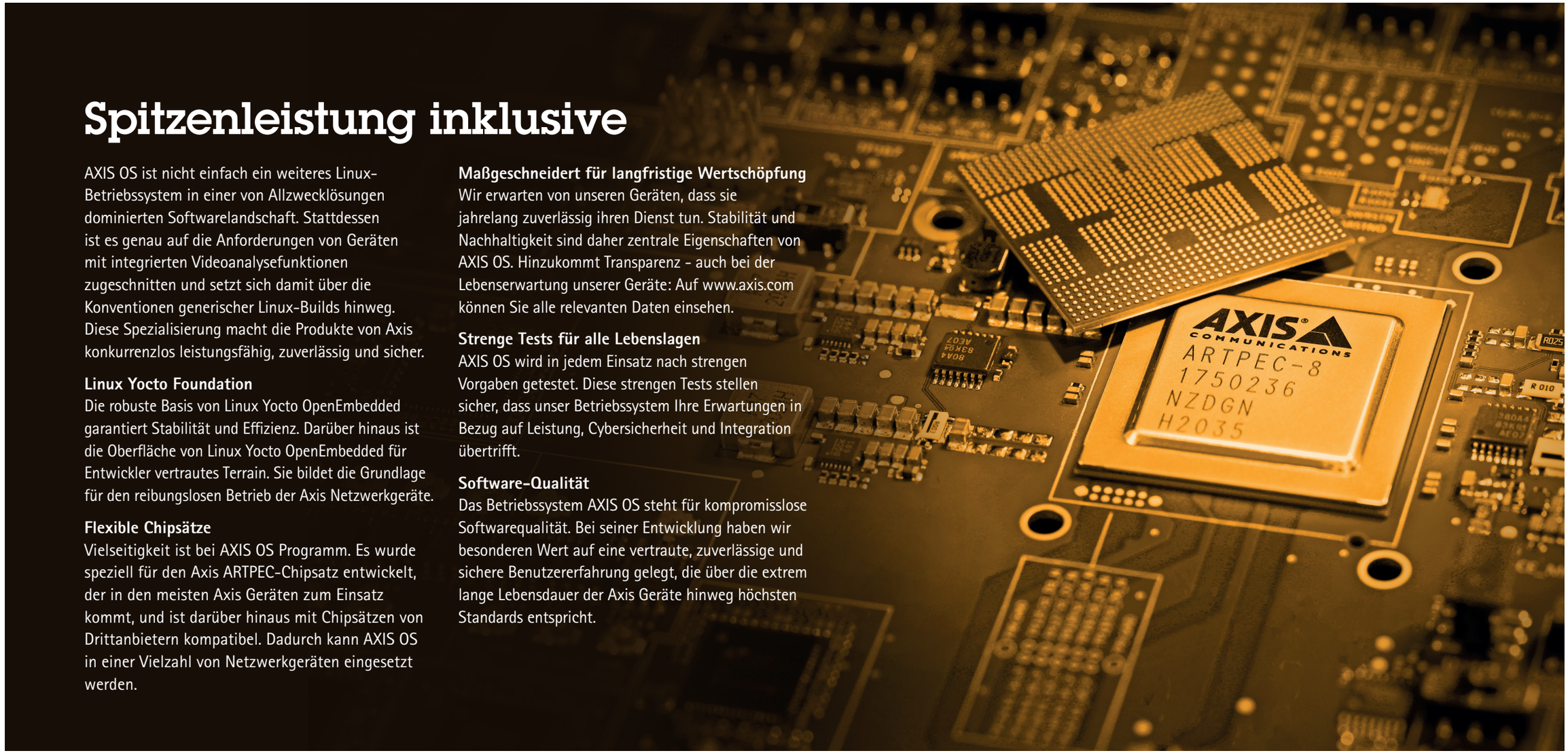
Linux Yocto Foundation
Die robuste Basis von Linux Yocto OpenEmbedded garantiert Stabilität und Effizienz. Darüber hinaus ist die Oberfläche von Linux Yocto OpenEmbedded für Entwickler vertrautes Terrain. Sie bildet die Grundlage für den reibungslosen Betrieb der Axis Netzwerkgeräte.

Flexible Chipsätze
Vielseitigkeit ist bei AXIS OS Programm. Es wurde speziell für den Axis ARTPEC-Chipsatz entwickelt, der in den meisten Axis Geräten zum Einsatz kommt, und ist darüber hinaus mit Chipsätzen von Drittanbietern kompatibel. Dadurch kann AXIS OS in einer Vielzahl von Netzwerkgeräten eingesetzt werden.

Maßgeschneidert für langfristige Wertschöpfung
Wir erwarten von unseren Geräten, dass sie jahrelang zuverlässig ihren Dienst tun. Stabilität und Nachhaltigkeit sind daher zentrale Eigenschaften von AXIS OS. Hinzukommt Transparenz - auch bei der Lebenserwartung unserer Geräte: Auf www.axis.com können Sie alle relevanten Daten einsehen.

Strenge Tests für alle Lebenslagen
AXIS OS wird in jedem Einsatz nach strengen Vorgaben getestet. Diese strengen Tests stellen sicher, dass unser Betriebssystem Ihre Erwartungen in Bezug auf Leistung, Cybersicherheit und Integration übertrifft.

Software-Qualität
Das Betriebssystem AXIS OS steht für kompromisslose Softwarequalität. Bei seiner Entwicklung haben wir besonderen Wert auf eine vertraute, zuverlässige und sichere Benutzererfahrung gelegt, die über die extrem lange Lebensdauer der Axis Geräte hinweg höchsten Standards entspricht.



Eine Plattform – unendliche Möglichkeiten

Für uns ist Spitzenleistung gerade gut genug: Dies gilt für alle Produktkategorien und ließ unsere gemeinsame Plattform für die verschiedensten Geräte entstehen. Im Dienst unserer Partner und Kunden unterstützt diese über 200 Produkte – von Bodycams bis hin zu explosionssicheren Lösungen, von PTZ-Kameras bis zu Sirenen, von Lautsprechern bis hin zu IP-Türsprechanlagen.

Produktvielfalt mit konstanter Leistung
AXIS OS kommt in den unterschiedlichsten Axis Produkten zum Einsatz. Was sie verbindet, sind die gleichen APIs und Eigenschaften. Dank einer gemeinsamen Plattform können Integratoren und Entwickler neue Axis Geräte reibungslos in ihre Systeme integrieren – ohne dass dafür komplexe gerätespezifische Treiber erforderlich wären. Dies beschleunigt nicht nur die Integration, sondern macht Ihre Lösungen zudem fit für die Zukunft – denn neue Produkte lassen sich im Handumdrehen in das stetig wachsende Axis Ökosystem einbinden. So profitieren die Endkunden von einem einheitlichen Nutzungserlebnis. Entwickler wiederum sparen mit dem Betriebssystem Zeit und Geld, da jede Integrationslösung auch auf jedem Gerät mit AXIS OS läuft.

Enorme Vielfalt, bestechend einfach
Die geballte Kraft einer einzigen Plattform liegt auch in der Vielzahl möglicher Anwendungen, ohne die Abläufe unnötig kompliziert zu machen. Ganz gleich, ob Sie eine PTZ-Kamera in ein Sicherheitssystem integrieren oder eine intelligente Audiolösung um einen Lautsprecher ergänzen möchten – der Prozess ist immer gleich. Dabei gewährleisten wir nicht nur die Kompatibilität, sondern ermöglichen ein einheitliches Nutzungserlebnis und unzählige Optionen zur Gestaltung integrierter und maßgeschneiderter Lösungen.

Einheitliche Sicherheit
Auch in Sachen Cybersicherheit, deren Bedeutung keinesfalls unterschätzt werden darf, erlaubt die gemeinsame Plattform eine einheitliche Lösung für das gesamte Produktspektrum. So braucht nicht jedes Produkt eine eigene Sicherheitsstrategie. Bei Erkennung und Behebung einer Schwachstelle wird die entsprechende Fehlerkorrektur automatisch auf alle unterstützten Produkte übertragen. Dies optimiert nicht nur das Sicherheitsmanagement, sondern ermöglicht auch eine zeitnahe, gemeinsame Reaktion auf neu aufkommende Bedrohungen. Darüber hinaus spart die Plattform Zeit und Ressourcen und stärkt damit die Resilienz des gesamten Axis Ökosystems.

Langfristige Wertschöpfung

AXIS OS steigert die planbare Wertschöpfung über den gesamten Lebenszyklus Ihrer Geräte. Die stabile und robuste Architektur begrenzt Ausfallzeiten auf ein Mindestmaß.

Wir versorgen Sie laufend mit Software-Updates und brandneuen Funktionen – und das über viele Jahre hinweg. Ausführliche Dokumentation, nützliche Tools und intuitive Oberflächen: Axis Geräte sind benutzerfreundlich und einfach zu warten. Darüber hinaus geben wir transparente und verlässliche Release-Termine bekannt, damit Sie Ihre Wartungsmaßnahmen an den Bedarf Ihres Unternehmens anpassen können.

Auf den folgenden Seiten erfahren Sie mehr über die Qualität der Axis Software, das Lebenszyklus-Management für AXIS OS und den Software-Support.

Auf diese Software ist Verlass

Die Qualität von AXIS OS steht für uns ganz oben auf der Tagesordnung. 900 Entwickler sind damit beschäftigt, unser Betriebssystem laufend an die aktuellen Marktbedürfnisse anzupassen, und Tag für Tag fließen 4.000 Code-Commits in den AXIS OS Hauptzweig ein. Mit zwei Builds pro Tag für jedes unserer über 200 Produkte bringen wir es auf beeindruckende 182.500 Builds pro Jahr, was wiederum iteratives Testen und einen größeren Mehrwert ermöglicht.

Strenge Tests
Für stabile Software sind sorgfältige Tests erforderlich. Tatsächlich durchlaufen unsere Systeme bemerkenswerte 4 Millionen verschiedenste Testfälle – Tag für Tag. Diese werden durch über 4.000 Code-Commits pro Tag ergänzt, die Sicherheitslücken schließen und die Qualität verbessern. Damit kommen wir auf mehr als 1 Milliarde Tests und über 1.000.000 Code-Commits pro Jahr. Außerdem haben unsere Kunden und Partner die Möglichkeit, uns mittels Datenaustausch ein direktes Feedback zu AXIS OS zu geben.

Fortlaufende Verbesserung
AXIS OS ist kein statisches System. Es wird laufend verbessert und ist damit hochdynamisch. Dank regelmäßiger Updates und Erweiterungen sind die Axis Geräte des aktiven AXIS OS Tracks immer auf dem neuesten Stand der Technik. Das bedeutet für Sie: Ein heute gekauftes Produkt wird mit der Zeit um immer neue Funktionen erweitert und gewinnt damit über seine Lebenszeit hinweg an Wert.

Support über die gesamte Einsatzdauer

Von der Installation über die Wartung bis hin zum Austausch: AXIS OS unterstützt das Gerät in jeder Phase seines Lebenszyklus. AXIS OS versorgt Sie mit geeigneten Tools und Ressourcen, um Ihre Axis Geräte über deren gesamte Lebensdauer hinweg zu verwalten und zu optimieren.

Einfache Installation und Konfiguration
AXIS OS erleichtert Ihnen die Installation und Konfiguration von Axis Geräten mithilfe von Assistenten, Vorlagen und Profilen, die Sie durch den Prozess führen. Mithilfe von AXIS Device Manager (ADM) und AXIS Device Manager Extend (ADMX) können Sie außerdem mehrere Geräte gleichzeitig konfigurieren und damit Zeit und Aufwand sparen.

Fortlaufende Überwachung und Diagnose
Mit Ihrer Zustimmung erfasst AXIS OS Health-Monitoring-Daten in Form von Protokollen, Berichten und Alarmen, um Leistung und Zustand der jeweiligen Axis Geräte zu überwachen und zu analysieren. So erkennen und beheben Sie mögliche Probleme im Handumdrehen. Und wir haben die Möglichkeit, unsere Software mit jedem Release weiter zu verbessern.

Support und Kompatibilität auf lange Sicht
Dank regelmäßiger Sicherheitspatches und Bugfixes gewährleistet AXIS OS langfristigen Support für Axis Geräte. Bei unserem langfristigen Support erfassen wir die Kompatibilität der Axis Geräte und Anwendungen und beschränken Änderungen und Unterbrechungen dadurch auf ein Minimum. Geräte mit AXIS OS haben in der Regel eine Lebensdauer von mindestens 10 Jahren. Manche Geräte unterstützen wir auch bis zu 13 Jahre lang.

Vertrauen und Engagement
AXIS OS ist auf die Erwartungen und Anforderungen all jener Kunden ausgelegt, die besonderen Wert auf Qualität und Vertrauenswürdigkeit legen. Das Betriebssystem definiert für jedes Produkt eine eindeutige und transparente Lebenserwartung und hält dieses so weit wie möglich auf dem neuesten Stand. Darüber setzt sich Axis mit bestmöglichem Service und Support für langfristige Kundenbeziehungen ein.

AXIS OS beta

AXIS OS beta richtet sich vor allem an Entwickler und Integratoren, die die neuesten Funktionen und Merkmale von AXIS OS testen möchten, bevor sie offiziell herausgegeben werden. AXIS OS beta kann zur Durchführung frühzeitiger Kompatibilitätstests an ausgewählten Geräten, zur Verifizierung bevorstehender Updates und zum Zugriff auf künftige Funktionen herangezogen werden.

Einige Vorzüge der Nutzung von AXIS OS beta:

> Sie erhalten eine Vorschau der neuen und verbesserten Funktionen und Merkmale, die AXIS OS künftig haben wird, wie z. B. integrierte Analysefunktionen, IoT-Konnektivität sowie die Plattform-Modularisierung.

> Sie können Axis Feedback geben und Vorschläge zur Entwicklung und Verbesserung von AXIS OS machen.

> Sie können Ihre Anwendungen und Systeme auf bevorstehende Änderungen und Updates bei AXIS OS vorbereiten und möglichen Problemen vorbeugen.

Hier erfahren Sie mehr über AXIS OS beta.

Lebenszyklus-Support für AXIS OS

Der Lebenszyklus-Support von AXIS OS besteht aus mehreren Tracks. Die Haupt-Tracks sind der aktive und der langfristige Support. Daneben gibt es auch produktspezifische Tracks (PSS) für individuelle Produkt-Lebenszyklen.

Die Mindestlebensdauer von Axis Geräten übertrifft die branchenüblichen Standards. Die umfangreiche 5-Jahres-Gewährleistung auf die Hardware wird durch den langjährigen AXIS OS Software-Support ergänzt.

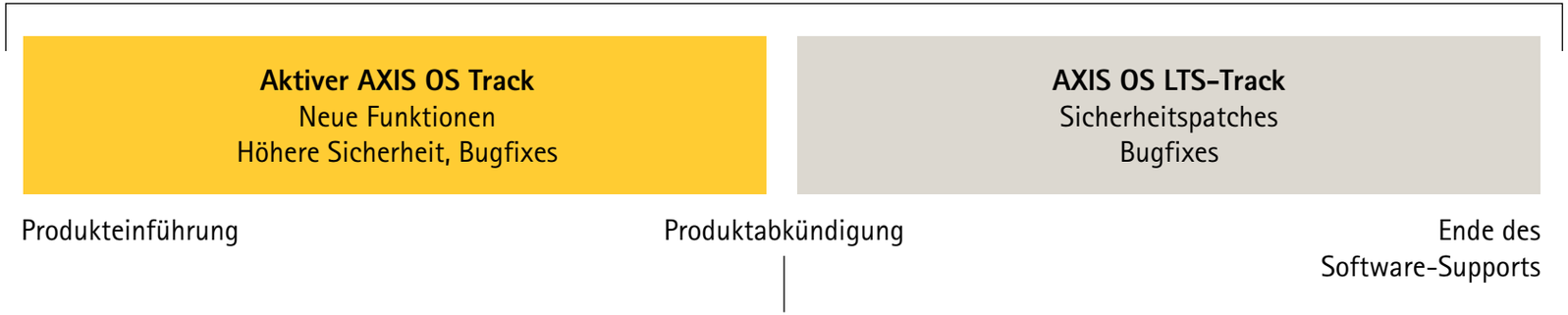
Die meisten Geräte erreichen mit AXIS OS eine Lebensdauer von sage und schreibe 8–12 Jahren.

So funktioniert es:

1. Wenn Axis ein neues Gerät auf den Markt bringt, ist in diesem Fall nur der aktive AXIS OS Track erhältlich. In der ersten Phase nach der Veröffentlichung profitieren Sie von fortlaufenden Verbesserungen und Updates, die auch neue Funktionen umfassen.
2. Innerhalb der ersten beiden Jahre nach Produktfreigabe ist auch der langfristige Support-Track (LTS) als Alternative zum aktiven Track erhältlich. Zu diesem Zeitpunkt können Sie sich zwischen dem aktiven und dem langfristigen Support-Track entscheiden. Im Rahmen des langfristigen Support-Tracks werden die Produkte ausschließlich in Form von Patches und Bugfixes unterstützt.
3. Zwei bis vier Jahre nach der Veröffentlichung läuft das Gerät aus, und auch der aktive Track für das betroffene Gerät wird eingestellt. Daraufhin werden alle Geräte automatisch in den langfristigen Support-Track (LTS) verschoben, wo sie für mindestens 5 Jahre Support in Form von Patches und Bugfixes erhalten.

Lebenszyklus-Support für AXIS OS

Software-Support (8–12 Jahre)



Ab dem Datum der Produktabkündigung setzt Axis den Software-Support für **mindestens 5 weitere Jahre** fort.

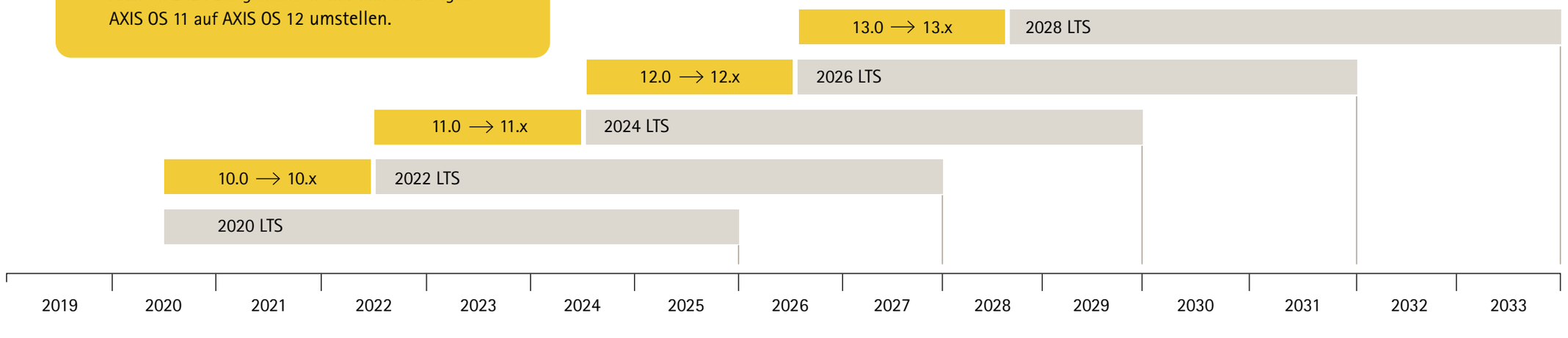
Welcher Support-Track für wen?

Sobald sowohl der aktive als auch der langfristige Track verfügbar sind, können Sie die für Ihre Anforderungen am besten geeignete Version auswählen – Axis berät Sie gern.

Aktiver Track
Der aktive Track von AXIS OS liefert Ihnen die aktuellste Version des Betriebssystems AXIS OS mit den meisten Funktionen. Dieser Track richtet sich gezielt an Kunden, die sich sofortigen Zugriff auf die neuesten Funktionen und Erweiterungen wünschen – daher steht für neu veröffentlichte Geräte auch nur dieser Track zur Verfügung. So profitieren Sie als Benutzer stets auch von neu hinzukommenden Features: Der bestehende Funktionsumfang Ihrer Geräte wird laufend erweitert und die Cybersicherheit mit Neuentwicklungen kontinuierlich erhöht. Mit dem aktiven Track von AXIS OS können Sie auch Jahre nach dem Kauf immer noch mehr aus Ihren Produkten herausholen – ganz ohne Zusatzkosten. Wenn Sie keinen bestimmten Kompatibilitätsvorgaben unterliegen, ist das genau der richtige Track für Sie.

Langfristiger Support-Track (LTS)
Wenn Sie auf API-Konsistenz und -Kompatibilität Wert legen, sollten Sie sich für den langfristigen Support-Track (LTS) entscheiden, sobald er für Sie erhältlich ist. Der Schwerpunkt des LTS-Tracks liegt auf der Abwärtskompatibilität und der regelmäßigen Bereitstellung von Sicherheitspatches und Bugfixes. Daher konzentriert sich dieser Track eher auf die Aufrechterhaltung der Cybersicherheit, anstatt neue Sicherheitsfunktionen zu implementieren. In diesem Sinne werden auch keine neuen Funktionen oder Merkmale aufgenommen, sondern Änderungen und damit Unterbrechungen auf ein Mindestmaß reduziert. Der LTS-Track richtet sich gezielt an Kunden, die hohen Wert auf Qualität und Vertrauenswürdigkeit legen und sich ein optimal integriertes Drittanbieter-System wünschen. Jeder LTS-Track wird 5 Jahre lang unterstützt. LTS-Tracks werden basierend auf einem regelmäßigen aktiven Track-Release alle 24 Monate veröffentlicht. Wenn Geräte auslaufen, werden sie automatisch in den LTS-Track verschoben.

In der Abbildung ist der aktive AXIS OS Track den LTS-Tracks gegenübergestellt, die im Lauf der Jahre eingeführt wurden. Etwa alle 24 Monate wird ein neuer LTS-Track erstellt und die AXIS OS Hauptversion erweitert. So werden wir 2024 z. B. den neuen AXIS OS 2024 LTS generieren und vom derzeitigen AXIS OS 11 auf AXIS OS 12 umstellen.



ASDM
INTEGRIERTE CYBERSICHERHEIT
SCHWACHSTELLEN-MANAGEMENT
ALL-IN-ONE

Cybersicherheit im Fokus

AXIS OS basiert auf Security by Design – die Sicherheit wurde also von Anfang an mitgedacht. Unser Axis Security Development Model (ASDM) sieht Prozesse und Tools vor, die das Risiko von Schwachstellen während und nach der Software-Entwicklung senken.

Unsere hardwarebasierte Cybersicherheitsplattform Axis Edge Vault garantiert ein sicheres Hochfahren und eine manipulationssichere Umgebung zur Speicherung der vom Kunden geladenen kryptografischen Schlüssel. Die Basissoftware AXIS OS besteht aus bewährten Open-Source-Komponenten. Zusätzlich enthält jedes Release eine Software Bill of Materials (SBOM), die belegt, dass AXIS OS auf dem neuesten Stand ist und hinsichtlich bekannter Schwachstellen gepatcht wurde.

Darüber hinaus ist AXIS OS nach der Norm ETSI EN 303 645 zertifiziert, deren besonderer Schwerpunkt auf der Sicherheit von Geräten mit integrierter Analytik liegt. Mit der Einhaltung von FIPS 140 ist dafür gesorgt, dass AXIS OS den neuesten kryptografischen Standards entspricht, die von den National Institutes of Technologies (NIST) festgelegt werden. Und schließlich haben wir uns als CVE-Nummerierungsbehörde zur Einhaltung der bewährten Verfahren zur Erkennung, Behebung und Offenlegung von Schwachstellen verpflichtet.

Auf den folgenden Seiten erfahren Sie mehr über unser Axis Security Development Model, Axis Edge Vault, unser Schwachstellen-Management und das einheitliche Sicherheitskonzept.

Für höchste Sicherheit entwickelt

Das Axis Security Development Model (ASDM) bettet die Cybersicherheit effektiv in den Software-Entwicklungsprozess ein. Es legt die Sicherheitsmaßnahmen für die einzelnen Phasen der Software-Entwicklung fest.
Das Ziel ist eine Minimierung der Schwachstellen (und Entwicklungskosten) mithilfe eines einheitlichen Fundaments und klarer Vorgaben in Sachen Cybersicherheit.

ASDM: made by Axis
Das Axis Security Development Model ist kein serienmäßig produziertes Standard-Framework. Für seine Entwicklung haben wir zahlreiche Standards und Frameworks zur Cybersicherheit herangezogen – darunter ISO 27001, IEC 62443, NIST, BSIMM und CMMC. Als roter Faden zieht sich durch diese Regelwerke, dass die Sicherheit ein wesentlicher Bestandteil aller Entwicklungsphasen ist. Davon ausgehend haben wir ein eigenes Modell entwickelt, das auf unsere Unternehmenskultur, unsere Entwicklungspraktiken und die von uns angebotenen Produkte zugeschnitten ist.

Die ASDM-Toolbox
Die ASDM-Toolbox umfasst eine Reihe von Aktivitäten, die unterschiedliche Sicherheitsprobleme angehen. Dazu gehören Risikobewertung, Bedrohungsmodellierung, Bedrohungsmodell-Tests, statische Codeanalyse, Schwachstellen-Scanning und Lieferantenbewertung. Je nach Art der zur Entwicklung vorgesehenen Software entscheiden die Entwicklungsteams über die auszuführenden Aktivitäten. Das Ziel hierbei ist keineswegs die bloße Einhaltung bestimmter Abläufe, sondern vielmehr eine höhere Cybersicherheit.

Gewinn durch externes Fachwissen
Die Entwicklung sicherer Software ist ein kompliziertes Unterfangen: Den größten Teil davon übernehmen die F&E-Abteilung und die Softwareentwickler von Axis. Aber natürlich wissen wir auch das Know-how und die Expertise von außen zu schätzen. Daher beauftragen wir spezialisierte Unternehmen mit der Durchführung von Penetrationstests. Darüber hinaus haben wir das Bug-Bounty-Programm für AXIS OS ins Leben gerufen: Hierbei erhalten Sicherheitsforscher eine finanzielle Belohnung, die uns beim Aufspüren von Sicherheitslücken helfen.

Governance | **Schulungen** | **ASDM-Produktlinien-Meeting** | **ASDM-Beurteilung** | **Sicherheits-Compliance und Standards**

Anforderungen	Design	Implementierung	Überprüfung	Bereitstellung
Risikobeurteilung Lieferantenbeurteilung Datenschutz Open-Source-Risikobewertung	Bedrohungsmodellierung	Statische Codeanalyse Analyse der Softwarezusammensetzung	Bedrohungsmodell-Test Externer Penetrationstest Schwachstellenscan Interne Sicherheitsbewertung	Schwachstellen-Management Ereignismanagement Sicherheitsstatus der Produkte/Lösungen Bug-Bounty-Programm

Integrierte Cybersicherheit

Schutz von innen nach außen
Bei Axis Edge Vault handelt es sich um unsere hardwarebasierte Cybersicherheitsplattform. Sie ist die Grundlage dafür, dass Ihre Axis Geräte einen verlässlichen und vertrauenswürdigen Bestandteil Ihres Netzwerks bilden. Dieses starke hardwarebasierte Fundament wäre allerdings nutzlos ohne ein Betriebssystem, das sein volles Potenzial unterstützt. Mithilfe der Edge-Vault-Plattform sorgt AXIS OS in allen Anwendungsfällen für mehr Sicherheit am Netzwerkrand.

Edge Vault bietet unter anderem folgende Funktionen:

Sichere Speicherung der Schlüssel
Der sichere Schlüsselspeicher arbeitet mit kryptografischen Rechenmodulen, die eine sichere Speicherung und Berechnung der kryptografischen Schlüssel gewährleisten. Sie schützen die Geräteidentität und andere sensible Informationen vor unbefugtem Zugriff – auch dann, wenn das Gerät bereits kompromittiert ist. Bei den eingesetzten kryptografischen Rechenmodulen handelt es sich um das in das System-on-Chip (SoC) integrierte Trusted Execution Environment sowie ein dezidiertes sicheres Element oder ein Trusted Platform Module (TPM 2.0) – allesamt separate Chips auf der Leiterplatte.

Signiertes OS und sicheres Hochfahren
Ein signiertes OS bedeutet, dass das Softwarebild des Geräts mit einer Codesignatur versehen ist. Gemeinsam sorgen das signierte OS und das sichere Hochfahren dafür, dass die Geräte ausschließlich das AXIS OS Original-Betriebssystem herunterladen und nutzen können. Damit erhalten die Geräte eine zusätzliche Schutzschicht, die sie besser vor einer Manipulation der Software- und Hardware-Lieferketten schützt.

Axis Geräte-ID
Die Axis Geräte-ID lautet IEEE 802. Sie entspricht 1AR und ermöglicht die sichere Identifikation und das sichere Onboarding von Geräten in einem Netzwerk. Außerdem weist sie jedes hergestellte Axis Gerät eindeutig aus.

Verschlüsseltes Dateisystem
Die im Dateisystem enthaltenen Daten sind durch Dateisystem-Verschlüsselung vor unbefugtem Zugriff oder Manipulation geschützt, wenn das Gerät nicht verwendet wird – z. B. beim Transport von einem Systemintegrator zum Endkunden.

Signiertes Video
Mit signiertem Video lässt sich die Echtheit eines Videos überprüfen und sicherstellen, dass es nicht manipuliert wurde.

Axis Edge Vault Cybersicherheitsplattform

Kryptografische Berechnungsmodule	Merkmale	Anwendungsbeispiele
Secure-Element TPM 2.0 SoC-Sicherheit (TEE)	Sicheres Booten Signiertes Betriebssystem Axis Geräte-ID Sicherer Schlüsselspeicher Signiertes Video Verschlüsseltes Dateisystem	Vertrauenswürdige Geräteidentität Sichere Speicherung der Schlüssel Videomanipulations-erkennung Schutz der Lieferkette

*Hinweis: Nicht alle Gerätemodelle unterstützen alle Funktionen von Axis Edge Vault. Die von den jeweiligen Produkten unterstützten Merkmale entnehmen Sie bitte dem Datenblatt oder dem Axis Product Selector.

Schwachstellen-Management

Um die Gefahr von Sicherheitslücken für unsere Kunden so gering wie möglich zu halten, befolgen wir beim transparenten Management und der Behebung dieser Schwachstellen die in der Branche bewährten Praktiken.

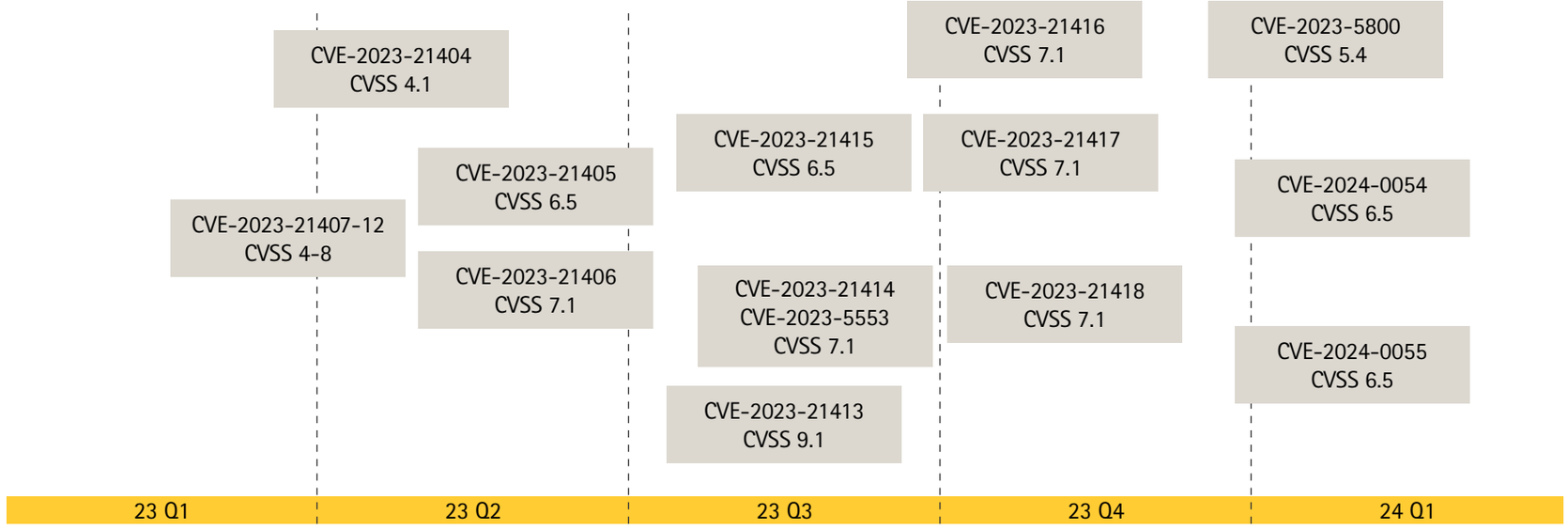
Branchenführendes Schwachstellen-Management
Es gibt keine Garantie dafür, dass die von Axis gelieferten Produkte und Dienste vollkommen frei von Sicherheitslücken sind. Damit sind wir allerdings nicht allein: Diese Problematik ist allen Softwares und Diensten gemein. Dennoch tun wir alles in unserer Macht Stehende, um potenzielle Schwachstellen in jeder Prozessphase zu erkennen und auszumerzen – und so das Risiko bei der Bereitstellung von Axis Produkten und Dienstleistungen in der Kundenumgebung auf ein Mindestmaß zu reduzieren.

CVE-Nummerierungsbehörde
Axis fungiert als CVE-Nummerierungsbehörde (CNA). Wir haben uns dem CVE-Programm angeschlossen, um gemeinsam mit gleichgesinnten Unternehmen einen Beitrag zur Verbesserung des Schwachstellen-Managements zu leisten. Bei Behebung, Offenlegung und Patching von Schwachstellen handeln wir gemäß dem internationalen Regelwerk, das diese gemeinnützige Organisation vorgibt, und entsprechend unserer öffentlichen Strategie zum Schwachstellen-Management.

Transparentes Management, auf das Verlass ist
Axis verwendet das bekannte CVSS-Bewertungssystem (Common Vulnerability Scoring System), um Schwachstellen zu bewerten, die entweder mit von Axis entwickeltem Code oder mit Open-Source-Code von Dritten zusammenhängen. Schwachstellen im Open-Source-Quelltext bewerten wir dabei im Hinblick darauf, wie relevant diese für unsere Produkte sind, wenn die Best-Practice-Empfehlungen befolgt werden. Wenn Sie sich zum Axis Benachrichtigungs-Service zur Meldung von Sicherheitslücken anmelden, werden Sie über Schwachstellen und andere sicherheitsrelevante Aspekte zu Axis Produkten informiert.

Partnerschaften mit Sicherheitsforschern und Organisationen
Wir wissen die Arbeit unabhängiger Personen und Unternehmen im Bereich der Sicherheitsforschung zu schätzen, die sich aktiv mit uns in Verbindung setzen, um uns erkannte Schwachstellen mitzuteilen. Wir zögern nicht, solche Schwachstellen offenzulegen und zu patchen. Wichtig ist, Schwachstellen im Rahmen eines ethischen und verantwortungsbewussten Offenlegungsprozesses korrekt und transparent zu beheben – ganz unabhängig davon, wie die einzelne Schwachstelle entdeckt wurde.

Sicherheitslücken bei AXIS OS



Von Axis erkannte Sicherheitslücken bei AXIS OS

Umfassendes Sicherheitskonzept

Bei den mit AXIS OS betriebenen Netzwerkgeräten wirken Hardware- und Software-Komponenten zusammen, um auf Kundenseite den sicheren Betrieb von Geräten, Diensten und den damit verbundenen Systemen zu gewährleisten. Dieses umfassende Sicherheitskonzept beginnt mit dem Sicherheitsfundament und erstreckt sich über die hardwarebasierte Sicherheitsplattform bis hin zur Software. Durch dieses vielschichtige Abwehrsystem, das auch als Defense-in-Depth-Konzept bezeichnet wird, sind mit AXIS OS betriebene Geräte in puncto Cybersicherheit zuverlässig geschützt. Dies erhöht auch die kumulative Sicherheit von Daten, Anwendungen und Prozessen.

Ganz gleich also, wofür Sie Ihr Axis Gerät verwenden: Sie können sich stets darauf verlassen, dass es optimal geschützt und eine sichere Kommunikation gewährleistet ist. Damit gelingt auch die ordnungsgemäße und sichere Integration in Drittanbieter-Systeme.

Zutrittskontrolle

Verwaltung der Zutrittskontrolle
Lokales Benutzer-Gerätemanagement mit Anzeige der Kennwortkomplexität
Gerätemanagement mit föderierten Identitäten mittels OpenID Connect (RFC6749, 1.3.1 Autorisierungscode) und ADFS-Integration, das Funktionen wie die Durchsetzung komplexer Kennwörter, Rotation, automatische Kontoabmeldung, Multi-Faktor-Authentifizierung (MFA) und die Microsoft AD-Berechtigungsverwaltung freischaltet

Datenschutz
Nutzung von Diagnosedaten
Minimalistischer Ansatz bei der Speicherung kundenspezifischer Daten

Anwendung

Anwendungssicherheit
TLS-basierte Anwendungssicherheit (MQTT, SFTP, NTS, HTTPS, WebRTC)
Verschlüsseltes Video-Streaming (RTSPS/SRTP, HTTPS), sicheres Remote Syslog

Betriebssystem

Verschlüsselung und Datenschutz
OpenSSL 1.1.1 und 3.0
X.509-Zertifikat PKI und Kryptografie
Transportschichtsicherheit (TLS 1.2/TLS 1.3)
SD-Kartenverschlüsselung (AES-XTS-Plain64 256bit)
Verschlüsseltes Dateisystem (AES-XTS-Plain64 256bit)
Signiertes Video

Sicherheit als Standard
HTTPS als Standardeinstellung
Verzögerungsschutz gegen Brute-Force-Angriffe
Hostbasierte Firewall
Network Time Security (NTS)
Unsichere TLS-Versionen deaktiviert
UART/Debug-Port deaktiviert

Unternehmensnetzwerk-Sicherheit
IEEE 802.1X (Netzwerkzugriffskontrolle)
IEEE 802.1AR (sichere Geräteidentität)
IEEE 802.1AE (MAC-Sicherheit, MACsec)

Betriebssystem AXIS OS
Linux-basiertes Standard-Betriebssystem mit über 95 % Open-Source-Software-Komponenten gemäß Branchenstandard, darunter OpenSSL, Apache und Curl. Aktiver Track zur Erweiterung des Funktionsumfangs und langfristiger Support-Track (LTS) über 5 Jahre für die Integration von Drittanbieter-Systemen und abwärtskompatiblen Anwendungsfällen.

Siliziumgestützte Sicherheit (Chip)

Zuverlässige Hardware
ARM-basierte System-on-Chip-Sicherheit (SoC)
Trusted Execution Environment (TEE/OP-TEE)
Trusted Platform Module (TPM 2.0), Secure Element

Sichere Speicherung der Schlüssel
Manipulationssicherheit bei Speicherung und Betrieb der kryptografischen Schlüssel, wie z. B. von Kunden hochgeladene private Schlüssel, Video-Signaturschlüssel und die Axis Geräte-ID.

Sicherheitsfundament

Axis Security Development Model
Axis Security Development Model (ASDM)
Externe Penetrationstests
Bug-Bounty-Programm mit Bugcrowd
Software-Materialliste (SBOM)

Compliance
Common Criterial EAL
FIPS 140
ETSI EN 303 645

Vertrauenswürdige Geräteidentität
Axis Edge Vault Cybersicherheitsplattform
Sicheres Hochfahren mit signiertem Betriebssystem (Codesignatur)
Axis Geräte-ID (IEEE 802.1AR)

Erstklassige Integration

Die Integrationsfähigkeit ist für Axis Produkte ein ganz entscheidender Faktor. Wir haben uns robuste und konsistente APIs auf die Fahnen geschrieben, die sich reibungslos in die verschiedensten Anwendungen integrieren lassen.

Damit können Sie komplexe Lösungen erstellen, die das volle Potenzial Ihrer Axis Geräte ausschöpfen.

Auf den folgenden Seiten erfahren Sie mehr über VAPIX (unsere eigene API), unsere Arbeit mit ONVIF und IoT, die Plattform-Modularisierung mit ACAP sowie die Automatisierung der Netzwerkintegration.

Der Axis Vorteil in puncto VAPIX, ONVIF, IoT und Cloud-Integration

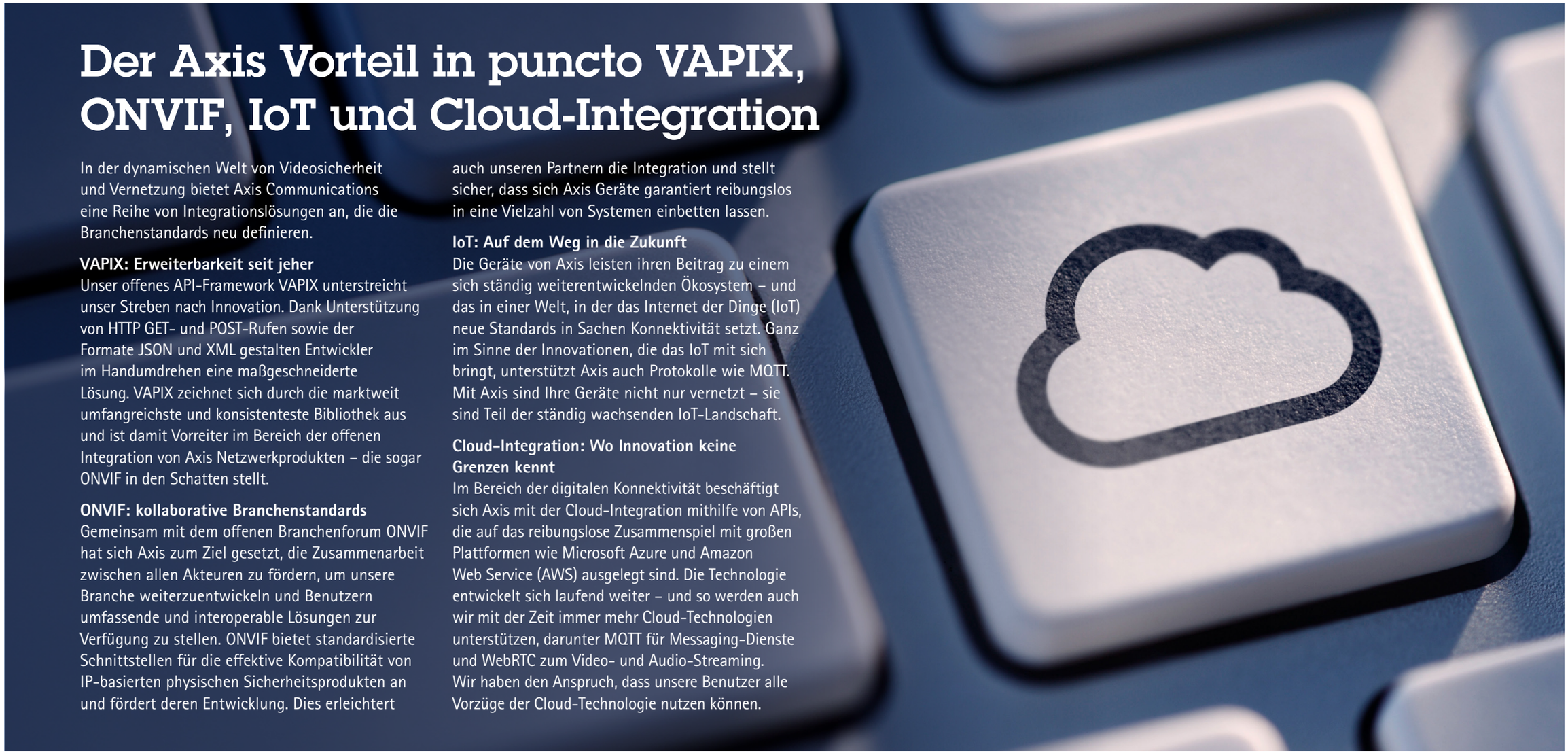
In der dynamischen Welt von Videosicherheit und Vernetzung bietet Axis Communications eine Reihe von Integrationslösungen an, die die Branchenstandards neu definieren.

VAPIX: Erweiterbarkeit seit jeher
Unser offenes API-Framework VAPIX unterstreicht unser Streben nach Innovation. Dank Unterstützung von HTTP GET- und POST-Rufen sowie der Formate JSON und XML gestalten Entwickler im Handumdrehen eine maßgeschneiderte Lösung. VAPIX zeichnet sich durch die marktweit umfangreichste und konsistenteste Bibliothek aus und ist damit Vorreiter im Bereich der offenen Integration von Axis Netzwerkprodukten – die sogar ONVIF in den Schatten stellt.

ONVIF: kollaborative Branchenstandards
Gemeinsam mit dem offenen Branchenforum ONVIF hat sich Axis zum Ziel gesetzt, die Zusammenarbeit zwischen allen Akteuren zu fördern, um unsere Branche weiterzuentwickeln und Benutzern umfassende und interoperable Lösungen zur Verfügung zu stellen. ONVIF bietet standardisierte Schnittstellen für die effektive Kompatibilität von IP-basierten physischen Sicherheitsprodukten an und fördert deren Entwicklung. Dies erleichtert auch unseren Partnern die Integration und stellt sicher, dass sich Axis Geräte garantiert reibungslos in eine Vielzahl von Systemen einbetten lassen.

IoT: Auf dem Weg in die Zukunft
Die Geräte von Axis leisten ihren Beitrag zu einem sich ständig weiterentwickelnden Ökosystem – und das in einer Welt, in der das Internet der Dinge (IoT) neue Standards in Sachen Konnektivität setzt. Ganz im Sinne der Innovationen, die das IoT mit sich bringt, unterstützt Axis auch Protokolle wie MQTT. Mit Axis sind Ihre Geräte nicht nur vernetzt – sie sind Teil der ständig wachsenden IoT-Landschaft.

Cloud-Integration: Wo Innovation keine Grenzen kennt
Im Bereich der digitalen Konnektivität beschäftigt sich Axis mit der Cloud-Integration mithilfe von APIs, die auf das reibungslose Zusammenspiel mit großen Plattformen wie Microsoft Azure und Amazon Web Service (AWS) ausgelegt sind. Die Technologie entwickelt sich laufend weiter – und so werden auch wir mit der Zeit immer mehr Cloud-Technologien unterstützen, darunter MQTT für Messaging-Dienste und WebRTC zum Video- und Audio-Streaming. Wir haben den Anspruch, dass unsere Benutzer alle Vorzüge der Cloud-Technologie nutzen können.



Plattform-Modularisierung mit ACAP

Eines der wichtigsten Merkmale von AXIS OS besteht darin, dass dieses Betriebssystem die Plattform-Modularisierung über die AXIS Camera Application Platform (ACAP) ermöglicht. Bei ACAP handelt es sich um ein Framework, in dem Entwickler ihre eigenen Anwendungen und Dienste entwickeln und bereitstellen können. Dazu gehören auch Video- und Audioanalyse sowie andere kundenspezifische Erweiterungen zur Erfüllung von Geschäftsanforderungen. Die ACAP-Anwendungen arbeiten unabhängig von den Kernfunktionen von AXIS OS und können installiert, aktualisiert und entfernt werden, ohne das verbleibende System zu beeinträchtigen. Darüber hinaus sind ACAP-Anwendungen auch in der Lage, über Standard-Protokolle und APIs untereinander und mit externen Systemen zu kommunizieren.

Skalierbarkeit und Leistung
ACAP nutzt die Microservice-Architektur des Betriebssystems der Axis Geräte. Je nach Anforderung und Auslastung kann ein Dienst entweder erweitert oder reduziert werden. Dies steigert die Gesamtleistung und Verfügbarkeit des Systems und ermöglicht eine effiziente Ressourcenzuweisung und -nutzung.

Anpassung und Personalisierung
Axis Geräte mit ACAP unterstützen verschiedene Integrationstypen, Analysefunktionen und Geräte – und sind damit in höherem Maße flexibel, anpassungsfähig und personalisierbar. Darüber hinaus senkt ACAP die Anzahl der erforderlichen Kopplungsvorgänge und erhöht die Kohäsion der Plattform, da jede Anwendung lose mit AXIS OS gekoppelt und in sich selbst kohäsiv ist.

Wartungsfreundlichkeit und Verlässlichkeit
Jeder Dienst kann unabhängig und isoliert getestet, überwacht und auf Fehler untersucht werden. Dies vereinfacht die Fehlerbehebung und Diagnose und sorgt für eine höhere Resilienz und Fehlertoleranz des Systems. Und in puncto Software-Qualität ist es ein Alleinstellungsmerkmal von AXIS OS.

AXIS OS für IT-Teams

Eine professionelle Automatisierung und Integration in die IT-Infrastruktur ermöglicht angemessene Sicherheitskontrollen und spart Zeit und Geld. Die Systeme sind nur so komplex, wie es unbedingt nötig ist. Axis Geräte mit Software zu kombinieren, die in die IT-Infrastruktur des Unternehmens integriert ist, hat z. B. folgende Vorteile:

> Minimierung der Systemkomplexität durch Entfernung dezidierter, physischer Netzwerke zur Bereitstellung von Geräten.

> Einsparung von Kosten durch automatisierte Einbindungsprozesse und Geräteverwaltung

> Nutzung des Potenzials von Zero-Trust-Netzwerk-Sicherheitskontrollen wie IEEE 802.1X, IEEE 802.1AR

> Steigerung der allgemeinen Netzwerksicherheit durch Datenverschlüsselung auf der ersten Ebene mithilfe von IEEE 802.1AE MACsec. Dadurch kann ein Axis Gerät beispielsweise zur Netzwerksicherheit beitragen.

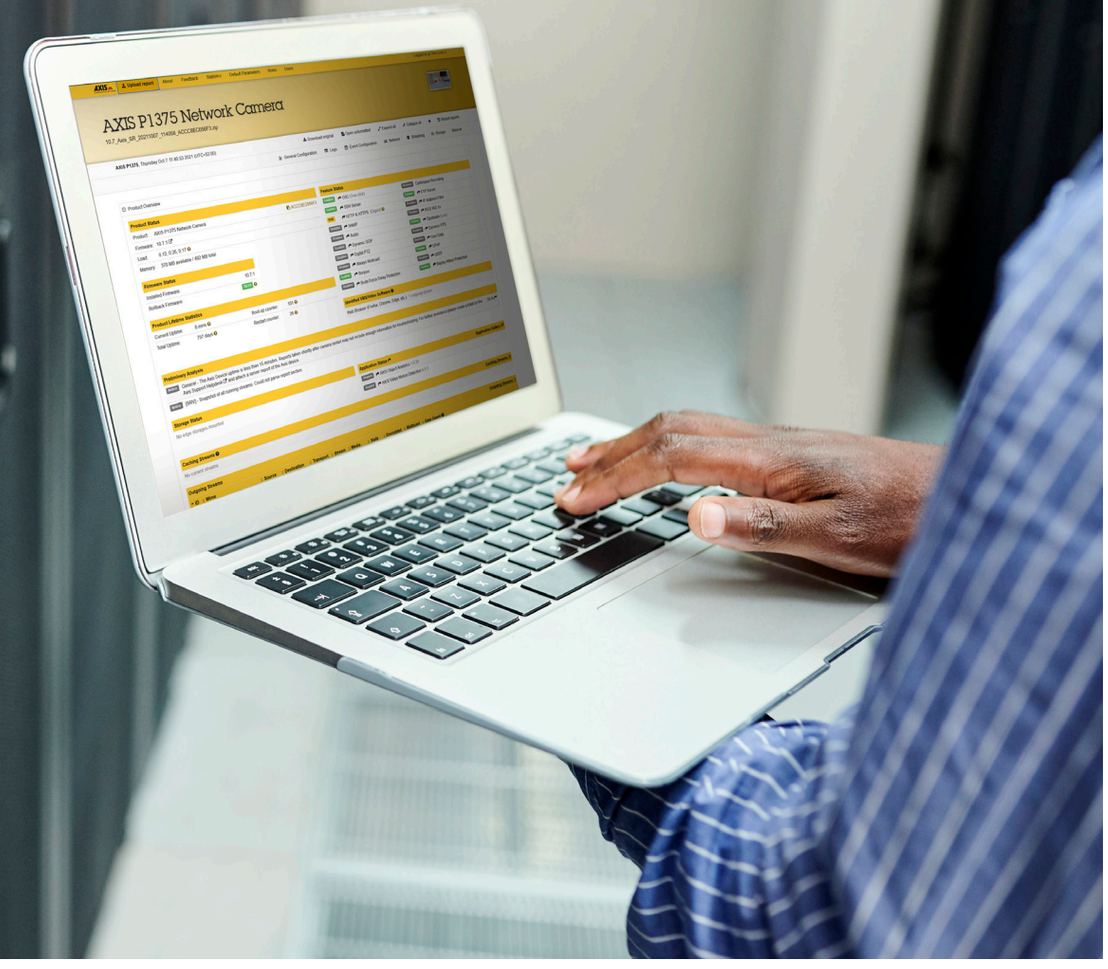
> Überwachung des Axis Geräts über standardisierte Protokolle, wie z. B. Remote Syslog zur Protokoll- und Zustandsüberwachung.

Sichere Netzwerke auf der Grundlage von Zero-Trust-Prinzipien

Der Aufbau konvergierter, sicherer Netzwerke auf der Grundlage von Zero-Trust-Prinzipien ist entscheidend für die Beseitigung isoliert betriebener Systeme. Geräte von Axis, die über klar definierte, offene Protokolle und Standards in die IT-Infrastruktur eines Unternehmens integriert werden, erhöhen die Sicherheit, senken die Kosten für Konfiguration und Wartung und ermöglichen eine einheitlichere Umsetzung von IT-Richtlinien.

Ein Gewinn für IT-Abteilungen

IT-Abteilungen sind für die Sicherheit von IT-Netzwerken verantwortlich – und genau an dieser Stelle kommen Axis Geräte ins Spiel. Dank ihrer Vielseitigkeit und der Tatsache, dass sie IT-Lösungen ähneln, die von offenen, standardisierten IEEE- und IETF-Netzwerkprotokollen definiert sind und ein gemeinsames Design haben, lassen sich Axis Geräte besonders einfach integrieren, warten und betreiben. Als vertrauenswürdige Elemente erhöhen Axis Geräte die Sicherheit kundenseitiger Netzwerke.



Sprechen wir darüber

Dank AXIS OS ist auf Axis Geräte stets Verlass. Außerdem erklärt es z. B. ihre hervorragende Bild- und Tonqualität.

Dieses Betriebssystem ist speziell auf die Erfüllung der wichtigsten Kriterien für Netzwerkgeräte ausgelegt: langfristige Wertschöpfung, hohe Standards in Sachen Cybersicherheit und reibungslose Integration.

Sie interessieren sich dafür, welchen Mehrwert Axis Geräte in Ihrem Unternehmen oder Ihrer Organisation generieren können? Wir beraten Sie gern!

Melden Sie sich noch heute bei uns!

Oder machen Sie sich auf axis.com ein Bild von unserem Produktangebot.

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Entwicklung von Lösungen zur Verbesserung von Sicherheit und Geschäftsperformance. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte für die Videosicherheit und Zutrittskontrolle sowie Intercoms, Audiosysteme und intelligente Analyseanwendungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 4.000 engagierte MitarbeiterInnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.