Erleben Sie die Vorteile einer einzigen Plattform

Langfristige Wertschöpfung, Cybersicherheit und eine 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, Zuverlässigkeit 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 laufend neue Funktionen hinzu und optimieren die bereits vorhandenen. Dank Schwachstellen-Patching werden außerdem alle auf AXIS OS basierenden Geräte immer sicherer und besser, was zusätzliche Anwendungsfälle mit mehr Sicherheit ermöglicht.

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 die AXIS OS Entwicklungsabteilung in Sachen Stabilität nach dem Vorbild von Linux Yocto OpenEmbedded programmierte, ist perfekt auf die speziellen Anforderungen von Axis Edge-Geräten wie Kameras, Lautsprechern und Zutrittskontrollsystemen abgestimmt – und generischen Betriebssystemen damit 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

4000 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

2000+ 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, in der die verschiedensten Gerätetypen konsistent verlässliche Leistung liefern.

Auf den folgenden Seiten erfahren Sie mehr darüber, welche Vorteile Ihnen ein eigens für Edge-Geräte entwickeltes Betriebssystem bietet, das als gemeinsame Plattform für alle Produkte dient.

Exzellenz „on the edge“

AXIS OS ist nicht einfach nur ein weiteres Linux-Betriebssystem in einer von Allzwecklösungen dominierten Software-Landschaft. Stattdessen ist es präzise auf die Anforderungen der jeweiligen Edge-Geräte abgestimmt und setzt sich damit über die Konventionen der generischen Linux-Builds hinweg. Diese Spezialisierung macht Axis Produkte so konkurrenzlos leistungsstark, zuverlässig und sicher.

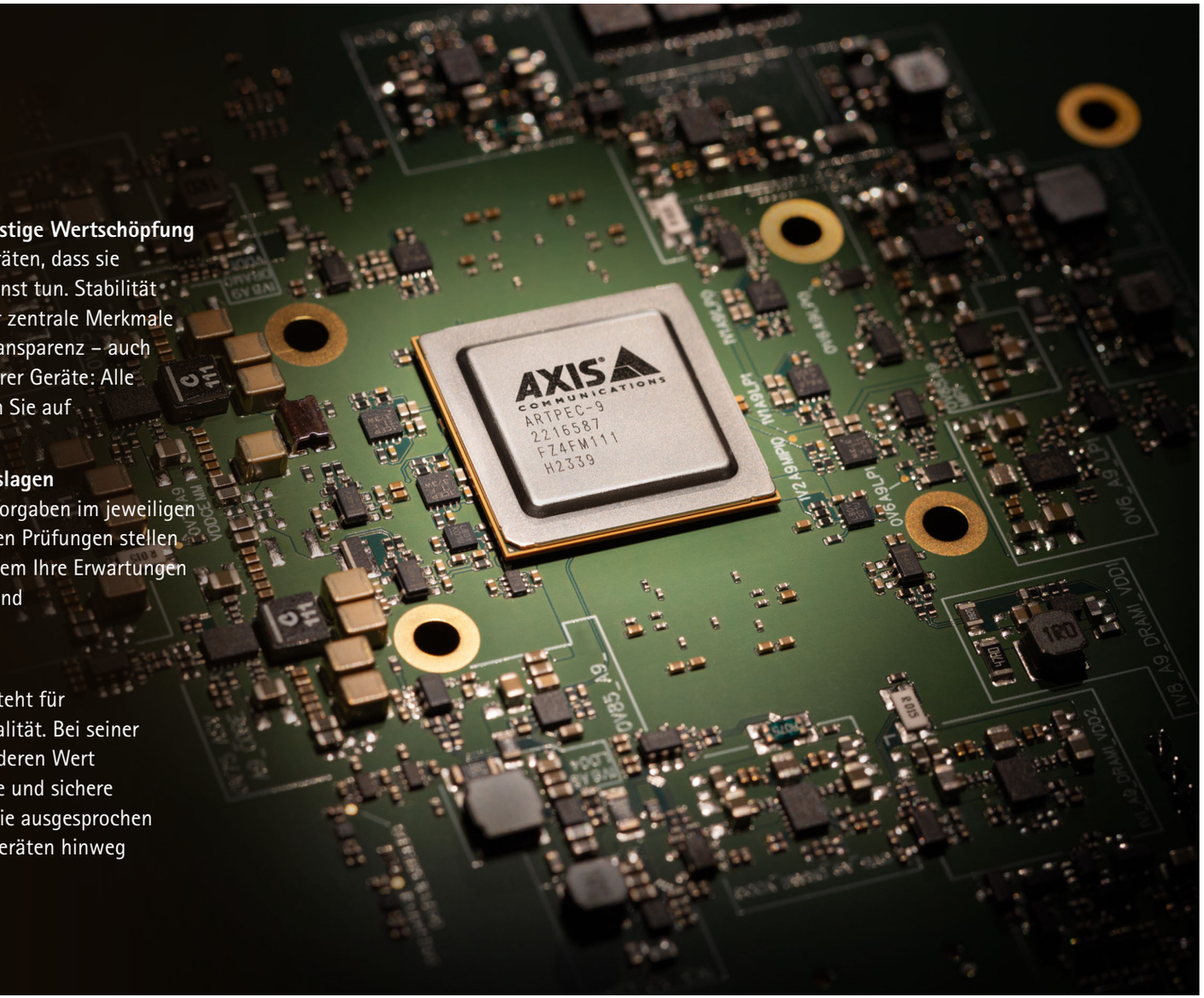
Linux Yocto Foundation
Die robuste Basis von Linux Yocto OpenEmbedded gewährleistet Stabilität und Effizienz. Außerdem ist die Oberfläche von Linux Yocto OpenEmbedded für Entwickler vertrautes Terrain. Sie bildet die Grundlage für den reibungslosen Betrieb der Axis Netzwerkgeräte.

Flexible Chipsätze
Vielseitigkeit ist für AXIS OS Programm. Es ist speziell für den Chipsatz Axis ARTPEC entwickelt, der in den meisten Axis Geräten verbaut ist, und darüber hinaus auch mit Drittanbieter-Chips kompatibel. Damit kann AXIS OS von den verschiedensten Netzwerkgeräten genutzt werden.

Maßgeschneidert für langfristige Wertschöpfung
Wir erwarten von unseren Geräten, dass sie jahrelang verlässlich ihren Dienst tun. Stabilität und Nachhaltigkeit sind daher zentrale Merkmale von AXIS OS. Hinzu kommt Transparenz – auch bei der Lebenserwartung unserer Geräte: Alle entsprechenden Daten können Sie auf axis.com einsehen.

Strenge Tests für alle Lebenslagen
AXIS OS wird nach strengen Vorgaben im jeweiligen Einsatz getestet. Diese strengen Prüfungen stellen sicher, dass unser Betriebssystem Ihre Erwartungen an Leistung, Cybersicherheit und Integration übertrifft.

Software-Qualität
Das Betriebssystem AXIS OS steht für kompromisslose Software-Qualität. Bei seiner Entwicklung legten wir besonderen Wert auf eine vertraute, verlässliche und sichere Benutzererfahrung, die über die ausgesprochen lange Lebensdauer von Axis Geräten hinweg höchsten Standards genügt.



Erleben Sie die Vorteile einer einzigen Plattform

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

Produktvielfalt mit konstanter Leistung
AXIS OS kommt in den unterschiedlichsten Produkten von Axis zum Einsatz. Was sie alle verbindet, sind die gleichen APIs und Eigenschaften. Dank der 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 auch zukunftssicher, da sich neue Produkte im Handumdrehen in das stetig wachsende Axis Ökosystem einbinden lassen. 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 Überwachungssystem integrieren oder eine intelligente Audiolösung um einen Lautsprecher ergänzen möchten – der Prozess ist immer derselbe. Dabei gewährleisten wir nicht nur die Kompatibilität, sondern ermöglichen auch ein einheitliches Nutzungserlebnis und unzählige Optionen zur Gestaltung integrierter und maßgeschneiderter Lösungen.

Einheitliche Sicherheit
Auch im Bereich der Cybersicherheit, dessen Bedeutung keinesfalls unterschätzt werden darf, ermöglicht die gemeinsame Plattform eine einheitliche Lösung für das gesamte Produktspektrum. So muss nicht für jedes Produkt eine eigene Sicherheitsstrategie entwickelt werden. 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 Minimum.

Wir versorgen Sie laufend mit Software-Updates und brandneuen Funktionen – und das über viele Jahre hinweg. Ausführliche Dokumentation, nützliche Tools und intuitive Oberflächen erleichtern die Nutzung. 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 des Lebenszyklusmanagements und des Software-Supports für AXIS OS.

Auf diese Software ist Verlass

Die Qualität von AXIS OS hat für uns höchste Priorität. 900 Entwickler sind damit beschäftigt, unser Betriebssystem laufend an die aktuellen Marktbedürfnisse anzupassen. Tag für Tag fließen 4.000 Code-Commits in den Hauptzweig von AXIS OS ein. Mit zwei Builds pro Tag für jedes unserer über 200 Produkte kommen wir auf beeindruckende 182.500 Builds pro Jahr. Das ermöglicht iteratives Testen und einen größeren Mehrwert.

Strenge Tests
Für stabile Software sind strenge Tests erforderlich. Tatsächlich durchlaufen unsere Systeme 4 Millionen verschiedene 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 eine Milliarde Tests und über eine Million Code-Commits pro Jahr. Außerdem haben unsere Kunden und Partner die Möglichkeit, uns mittels Datenaustausch direktes Feedback zu AXIS OS zu geben.

Fortlaufende Verbesserung
Stellen Sie sich vor, Ihre Kamera wird mit der Zeit immer intelligenter, schneller und stromsparender. AXIS OS ist kein statisches, sondern ein dynamisches Betriebssystem, das laufend optimiert wird. 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.

Klar definierte Support-Lebenszyklen
Bereits vor dem Kauf eines Axis Geräts werden Kunden transparent über das Datum des Support-Endes informiert. Wir verpflichten uns, Ihr Gerät bis zu diesem Datum zu schützen und zu warten. Damit sorgen wir für Stabilität, Sicherheit und langfristige Sorgenfreiheit.



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. Mit der Axis Software für das Gerätemanagement können Sie zudem mehrere Geräte gleichzeitig installieren und konfigurieren, was Zeit und Aufwand spart.

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. Der Software-Support für Geräte mit AXIS OS erstreckt sich in der Regel über 8 bis 12 Jahre.

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. Edge-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.



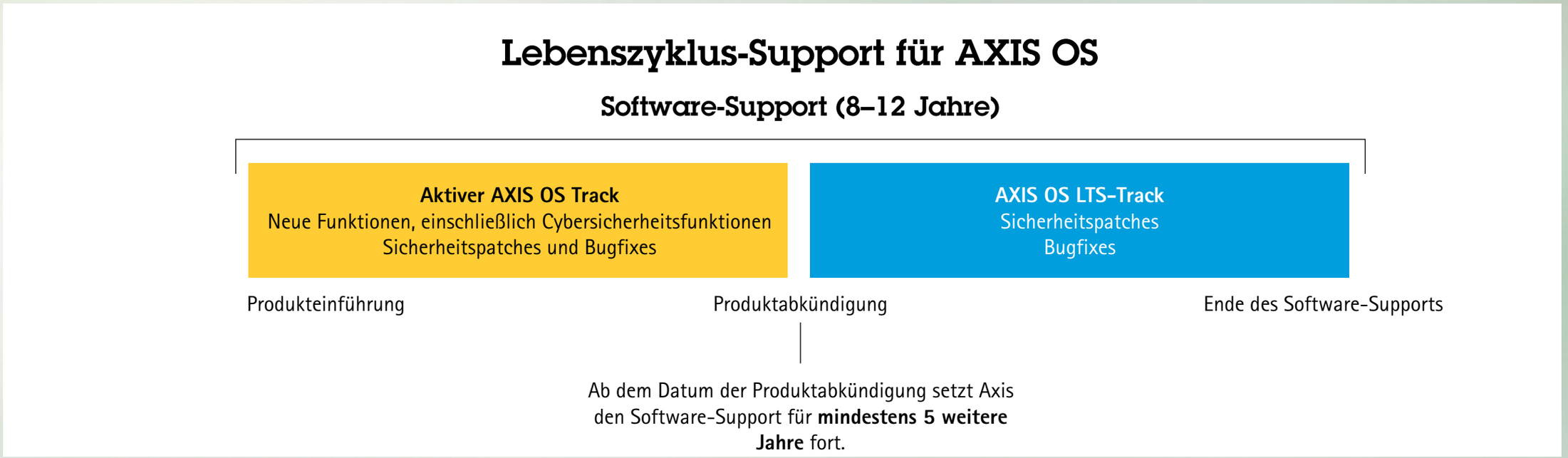
Lebenszyklus-Support für AXIS OS*

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 Support-Tracks (PSS) für individuelle Produktlebenszyklen.

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 (Long-term 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 für die entsprechenden Produkte Patches und Bugfixes bereitgestellt.
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.



** E-Mail-Benachrichtigungsdienst zu AXIS OS – Abonnieren Sie den E-Mail-Benachrichtigungsdienst zu AXIS OS, um regelmäßige Updates zu Releases und andere wichtige Informationen zu erhalten.*

Welcher Support-Track für wen?

Sobald sowohl der aktive als auch der langfristige Support-Track verfügbar sind, können Sie die für Ihre Anforderungen am besten geeignete Version auswählen und sich dabei von Axis beraten lassen.

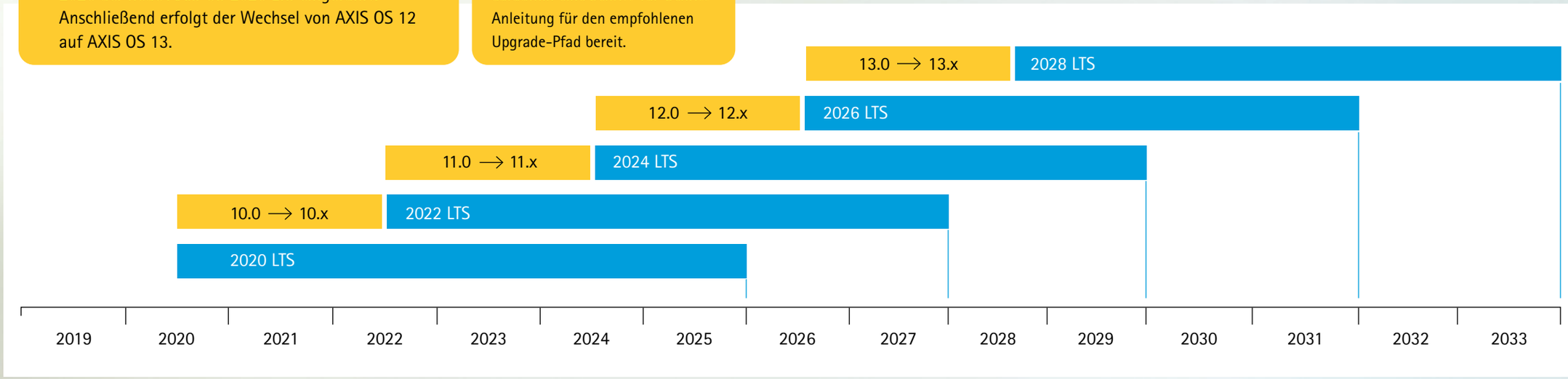
Aktiver Track
Der aktive Track von AXIS OS liefert Ihnen die aktuellste Version des Betriebssystems AXIS OS mit den meisten Funktionen. Dieser Track richtet sich gezielt an Kunden, die sich sofortigen Zugriff auf die neuesten Funktionen und Erweiterungen wünschen – daher steht für neu veröffentlichte 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 Cybersicherheitsfunktionen 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 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. Beispielsweise wird 2026 der neue AXIS OS 2026 LTS eingeführt. Anschließend erfolgt der Wechsel von AXIS OS 12 auf AXIS OS 13.

Mit dem Upgrade-Assistenten für Axis Gerätesoftware müssen Sie lediglich Ihre aktuelle Version und die gewünschte Zielversion angeben. Der Assistent stellt Ihnen daraufhin eine Schritt-für-Schritt-Anleitung für den empfohlenen Upgrade-Pfad bereit.



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 Edge-Geräten 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.

Entwicklung und Wartung mit Fokus auf Cybersicherheit

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. Diese Regelwerke haben gemeinsam, dass die Sicherheit ein wesentlicher Bestandteil aller Entwicklungsphasen ist. Auf dieser Grundlage 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

Der Großteil der Arbeit zur Gewährleistung einer sicheren Softwareentwicklung wird intern bei Axis geleistet. Dennoch sind wir uns bewusst, dass wir auch vom Wissen und der Fachkompetenz anderer profitieren können. Daher beauftragen wir spezialisierte Unternehmen mit der Durchführung von Penetrationstests. Darüber hinaus haben wir ein öffentliches Bug-Bounty-Programm für AXIS OS ins Leben gerufen. Hierbei erhalten Sicherheitsforscher eine finanzielle Belohnung für ihre Unterstützung beim Aufspüren von Sicherheitslücken.

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

Anforderungen	Planung	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



Besuchen Sie das Axis Trust Center | *Erfahren Sie, wie Axis und seine Produkte die Cybersicherheit und die Einhaltung verschiedener Sicherheitsvorschriften und -standards unterstützen. Greifen Sie auf eine Vielzahl von Informationen zu – von Cybersicherheitspraktiken und -maßnahmen bis hin zu Zertifikaten, Leitfäden und Berichten.*

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 (TEE) sowie um ein dediziertes sicheres Element oder ein Trusted Platform Module (TPM 2.0), die beide als separate Chips auf der Leiterplatte untergebracht sind.

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. Dies bietet eine zusätzliche Schutzebene gegen Manipulationen in den Software- und Hardware-Lieferketten.

Axis Geräte-ID
Die Axis Geräte-ID lautet IEEE 802. Sie entspricht 1AR und ermöglicht die sichere Identifizierung 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 Videomanipulationserkennung 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, wenden wir bei der transparenten Verwaltung und Behebung dieser Schwachstellen bewährte Branchenpraktiken an.

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, sofern die Best-Practice-Empfehlungen befolgt werden. In unseren Sicherheitshinweisen legen wir sämtliche CVE-Einträge im Zusammenhang mit AXIS OS transparent offen. Wenn Sie sich zum Benachrichtigungsdienst zum Thema Sicherheit von Axis 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.



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 abwärtskompatible Anwendungsfälle.

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)

DIE VORTEILE VON AXIS
GESCHÄFTSOPTIMIERUNG
IT-TEAMS



Erstklassige Integration

Die Integrationsfähigkeit ist für Axis Produkte von entscheidender Bedeutung. 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 sich schnell entwickelnden Welt der Videosicherheit und Vernetzung bietet Axis Communications eine Reihe von Integrationslösungen an, 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. Die kürzlich erfolgte Anpassung der VAPIX-APIs an den offenen API-Standard bekräftigt dieses Engagement und unterstreicht unser Bestreben nach kontinuierlichem Ausbau und langfristiger Weiterentwicklung.

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 Services (AWS) ausgelegt sind. Wir unterstützen Cloud-Technologien wie MQTT für Messaging-Dienste und WebRTC für 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.



Sichere und einfache Integration sowie Rund-um-die-Uhr-Überwachung von Axis Geräten

Axis verfügt über langjährige Erfahrung bei der Bereitstellung IT-relevanter Funktionen und setzt weiterhin auf kontinuierliche Innovation, Transparenz und bewährte Branchenpraktiken. AXIS OS ermöglicht die sichere Integration von Axis Geräten in Ihre IT-Infrastruktur, sodass Sie diese genauso wie Ihre übrigen IT-Geräte verwalten und überwachen können. Sie können Software-Upgrades ganz einfach planen und so sicherstellen, dass die Software jederzeit Ihren IT-Richtlinien entspricht. Axis Geräte sind bereits ab Werk mit robusten Cybersicherheitsfunktionen vorkonfiguriert, und es besteht keine Herstellerbindung.

Einfache Zero-Trust-Implementierung
AXIS OS unterstützt IEEE-Standards wie IEEE 802.1AR zur sicheren Identifizierung und Authentifizierung von Geräten, IEEE 802.1X zur Netzwerkauthentifizierung sowie IEEE 802.1AE MACsec zur grundlegenden Layer-2-Verschlüsselung. In Kombination mit HTTPS und anderen TLS-Protokollen wird so die Netzwerksicherheit deutlich erhöht. Damit können Sie Axis Geräte automatisch und sicher über Ihr Netzwerksicherheits- oder Zugriffskontrollsystem einbinden und betreiben. Axis Geräte sind außerdem werkseitig vorkonfiguriert, und es besteht keine Herstellerbindung. Beispielsweise unterstützen sie Lösungen wie Fabric Attach von Extreme Networks und HPE Aruba. Mithilfe der öffentlich verfügbaren VAPIX-API können Sie Axis Geräte zudem schnell und flexibel in Ihr System integrieren und dabei nur die Funktionen nutzen, die Sie für Ihre spezifische Konfiguration benötigen. Darüber hinaus ermöglicht Ihnen das zentrale Identitäts- und Zugriffsmanagementsystem (IAM) mit OAuth 2.0-Integration die Authentifizierung Ihrer Axis Geräte mittels Multi-Faktor-Authentifizierung (MFA) sowie die Festlegung individueller Anforderungen an die Komplexität von Kennwörtern und deren regelmäßigen Wechsel.

Sichere Verwaltung des Gerätelebenszyklus
Sie können sämtliche Axis Geräte in Ihrem Netzwerk rund um die Uhr überwachen. Dazu steht Ihnen ein umfassendes Audit-Protokoll zur Verfügung, das über Remote-Syslog und SNMP Ende-zu-Ende-verschlüsselte Daten zur SIEM-Überwachung von Konfigurationsänderungen und Anmeldeaktivitäten übermittelt. Axis Geräte unterstützen Schwachstellenscans mithilfe von Drittanbieter-Tools wie Tenable Nessus, Lösungen von Rapid7 und anderen. Der AXIS OS Security Scanner Guide bietet Empfehlungen zur Behebung bestimmter von den Scannern gemeldeter Probleme und beschreibt häufige „Fehlalarme“. Dies ermöglicht transparente Audits der Software-Lieferkette. Mit unserer Software für das Gerätemanagement können Sie die Einhaltung Ihrer IT-Richtlinien einfach sicherstellen und Software-Upgrades für Axis Geräte planen. Zudem ermöglicht eine integrierte Layer-2/3-Firewall die Mikrosegmentierung und verbessert so die Netzwerksicherheit sowie das Identitäts- und Zugriffsmanagement (IAM). So haben Sie jederzeit die volle Kontrolle darüber, welche Benutzer und Systeme über Ihr Netzwerk auf Axis Geräte zugreifen dürfen.





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, betrieblicher Effizienz und Geschäftsperformance. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte für die Videosicherheit und Zutrittskontrolle sowie Intercoms und Audiosysteme. Diese werden durch intelligente Analyseanwendungen erweitert und durch hochwertige Schulungen unterstützt.

Axis hat rund 5.000 engagierte Mitarbeiter in über 50 Ländern und arbeitet weltweit mit Technologie- und Systemintegrationspartnern zusammen, um kundenspezifische Lösungen zu liefern. Axis wurde 1984 gegründet, der Hauptsitz befindet sich in Lund, Schweden.

Weitere Informationen über Axis finden Sie unter www.axis.com

©2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC und VAPIX sind in verschiedenen Jurisdiktionen eingetragene Marken von Axis AB. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.