La puissance d'une plateforme unique

Spécialement axée sur la valeur de long terme,
la cybersécurité et l'intégration

AXIS COMMUNICATIONS

Au cœur de vos dispositifs réseau Axis

AXIS OS est le système d'exploitation dérivé de Linux qui fait fonctionner la plupart de vos dispositifs réseau Axis. Il pilote plus de 200 produits Axis et des dizaines de millions de dispositifs déployés sur les sites des clients. AXIS OS traduit un engagement en faveur de l'innovation, de la fiabilité et de la transparence d'intégration. Le logiciel Axis est au cœur de l'extrême fiabilité de nos dispositifs et de leur excellente qualité d'image. À chaque nouvelle version, nous le perfectionnons. En chiffres, 80 % de nos activités de R&D sont liées au développement logiciel.

Nous ajoutons de nouvelles fonctionnalités et perfectionnons les autres en permanence. De plus, nous ne cessons de renforcer la sécurité des dispositifs pilotés par AXIS OS au travers de correctifs contre les vulnérabilités. Ainsi améliorés, ils peuvent prendre en charge davantage de scénarios d'application de manière plus sûre.

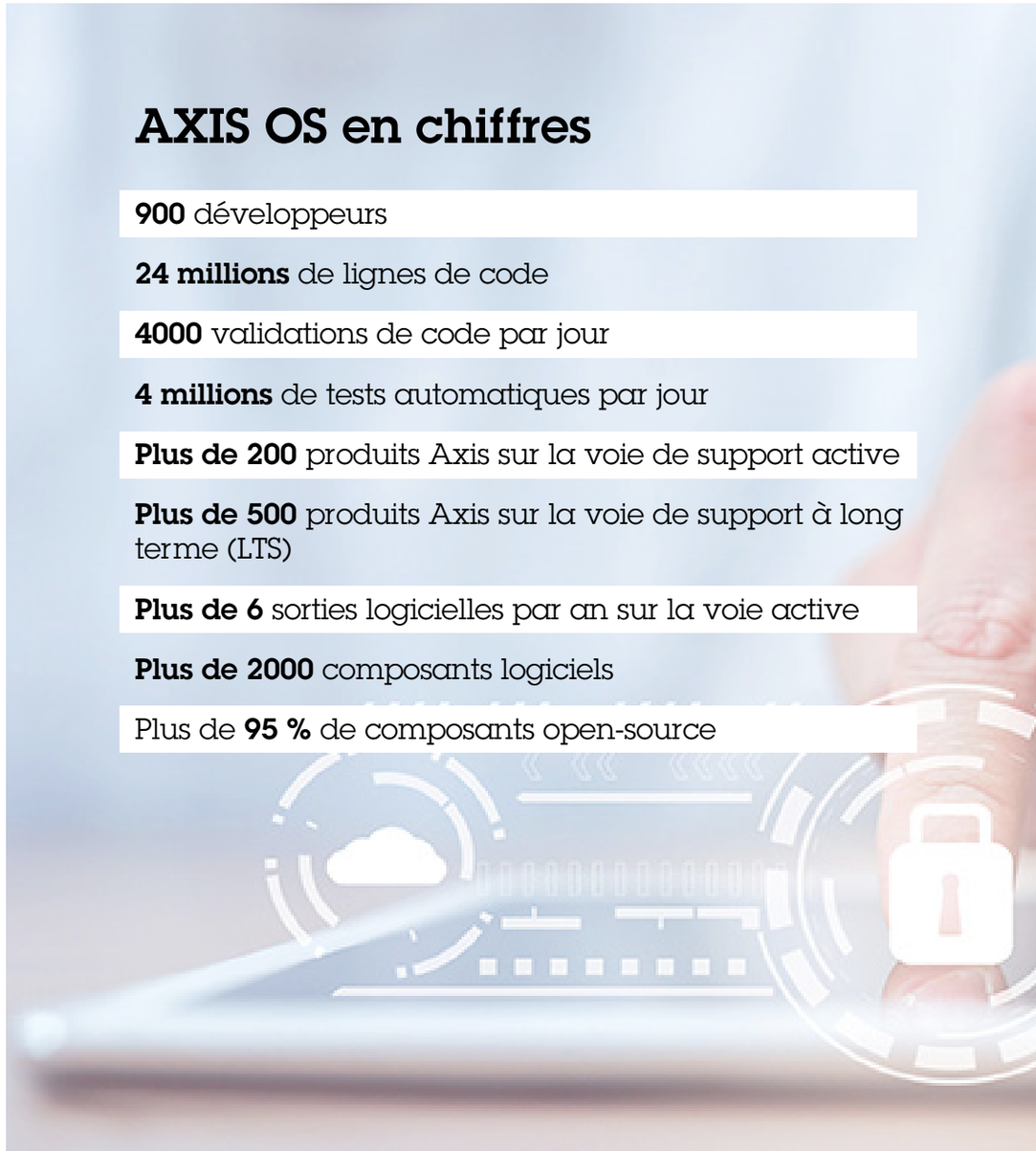
AXIS OS est conçu spécialement pour incorporer les qualités essentielles d'un dispositif réseau : valeur à long terme, mesures de cybersécurité rigoureuses et simplicité d'intégration.

Spécialement créé pour les dispositifs Axis
Créé par l'équipe de développement d'AXIS OS et profitant de la stabilité de Linux Yocto OpenEmbedded, AXIS OS surpasse les logiciels génériques, car il est parfaitement optimisé pour les spécificités uniques des dispositifs en périphérie de réseau d'Axis tels que caméras, haut-parleurs et équipements de contrôle d'accès.

Valeur à long terme
Avec AXIS OS, vos dispositifs sont toujours opérationnels. Conçu pour fonctionner 24 h/24 et 7 j/7, il offre des performances homogènes et réactives, dimensionnées aux exigences de vos applications sur la durée, de jour comme de nuit.

Cybersécurité solide
Le cœur d'AXIS OS est articulé autour de la cybersécurité. Avec son architecture de sécurité intégrée, AXIS OS vous aide à protéger vos dispositifs. Soutenu par des pratiques sécurisées de développement logiciel et une gestion vigilante des vulnérabilités, AXIS OS s'assure que vos données et vos dispositifs restent résilients face aux menaces émergentes.

Intégration transparente
Comme AXIS OS incorpore VAPIX, ONVIF et d'autres outils, vos dispositifs réseau Axis s'intègrent facilement à une diversité d'écosystèmes. Cette capacité d'intégration offre aux utilisateurs et aux développeurs une expérience d'interconnexion fluide.



AXIS OS en chiffres

900 développeurs

24 millions de lignes de code

4000 validations de code par jour

4 millions de tests automatiques par jour

Plus de 200 produits Axis sur la voie de support active

Plus de 500 produits Axis sur la voie de support à long terme (LTS)

Plus de 6 sorties logicielles par an sur la voie active

Plus de 2000 composants logiciels

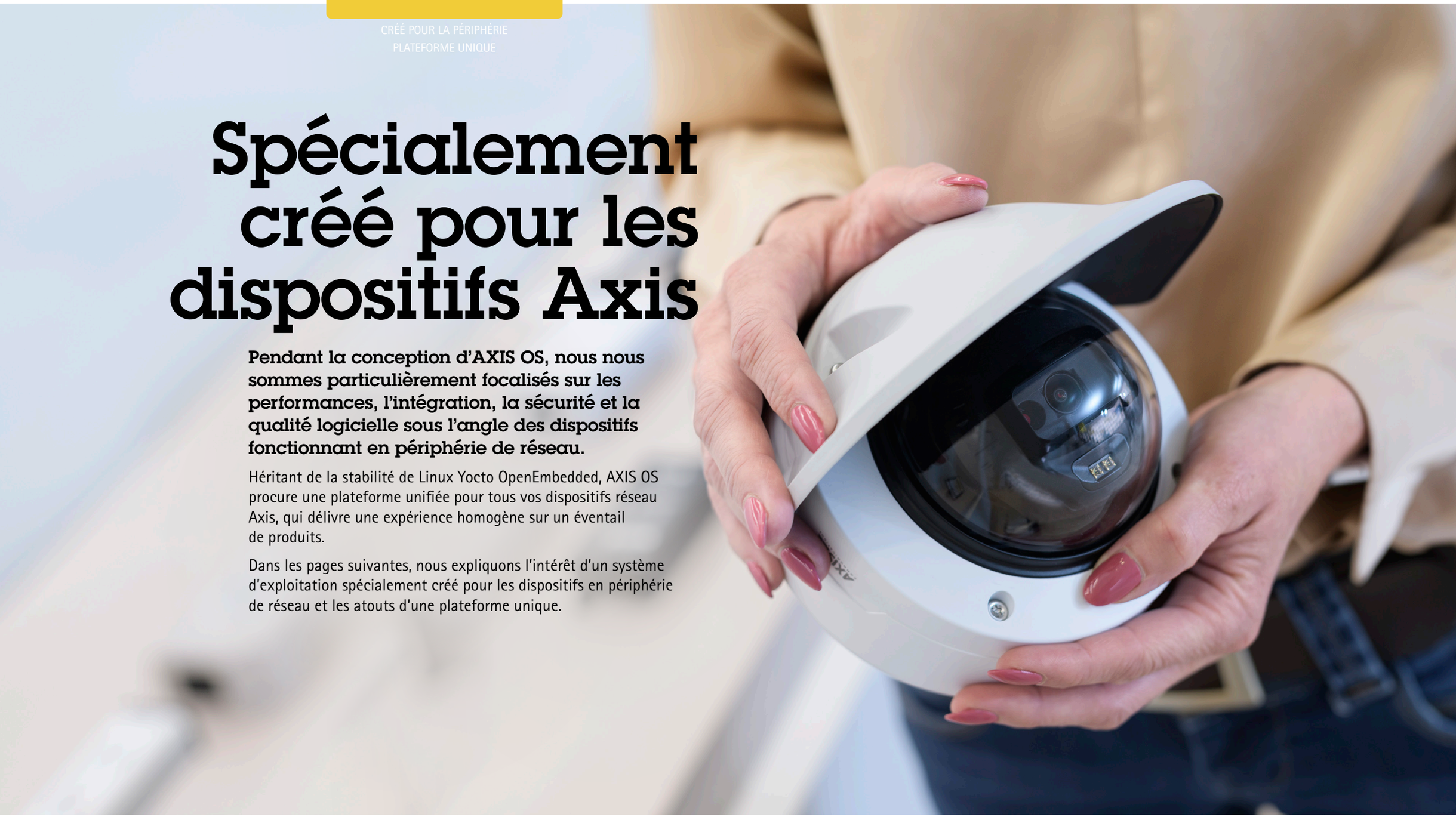
Plus de **95 %** de composants open-source

Spécialement créé pour les dispositifs Axis

Pendant la conception d'AXIS OS, nous nous sommes particulièrement focalisés sur les performances, l'intégration, la sécurité et la qualité logicielle sous l'angle des dispositifs fonctionnant en périphérie de réseau.

Héritant de la stabilité de Linux Yocto OpenEmbedded, AXIS OS procure une plateforme unifiée pour tous vos dispositifs réseau Axis, qui délivre une expérience homogène sur un éventail de produits.

Dans les pages suivantes, nous expliquons l'intérêt d'un système d'exploitation spécialement créé pour les dispositifs en périphérie de réseau et les atouts d'une plateforme unique.



Conçu pour exceller en périphérie de réseau

Sur un marché dominé par les solutions généralistes, AXIS OS n'est pas qu'un système d'exploitation de plus basé sur Linux. Il transcende les conventions des systèmes Linux génériques pour aboutir à une solution précisément taillée pour les besoins spécifiques des dispositifs en périphérie de réseau. Cette spécialisation confère aux produits Axis des propriétés uniques en termes de performances, fiabilité et sécurité.

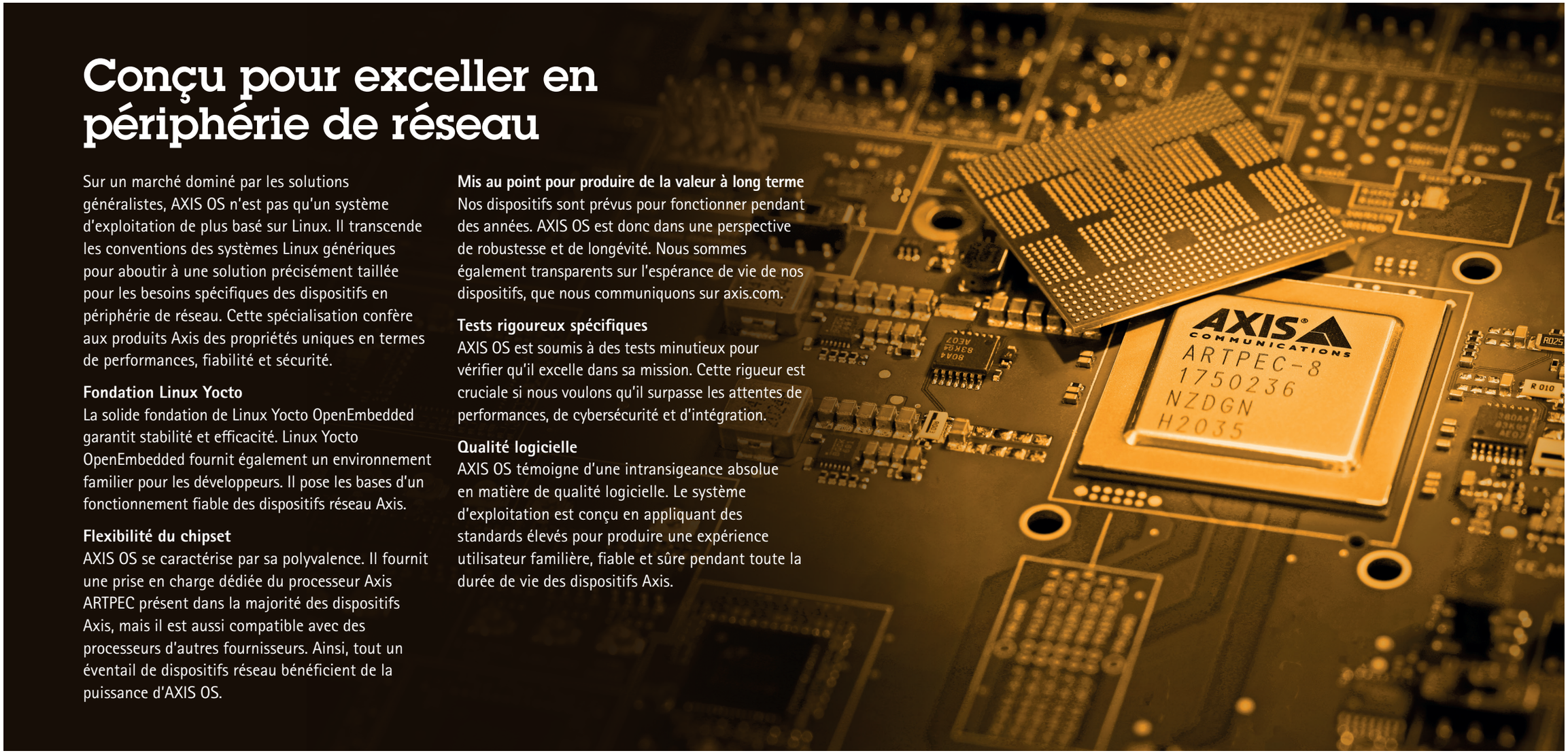
Fondation Linux Yocto
La solide fondation de Linux Yocto OpenEmbedded garantit stabilité et efficacité. Linux Yocto OpenEmbedded fournit également un environnement familier pour les développeurs. Il pose les bases d'un fonctionnement fiable des dispositifs réseau Axis.

Flexibilité du chipset
AXIS OS se caractérise par sa polyvalence. Il fournit une prise en charge dédiée du processeur Axis ARTPEC présent dans la majorité des dispositifs Axis, mais il est aussi compatible avec des processeurs d'autres fournisseurs. Ainsi, tout un éventail de dispositifs réseau bénéficient de la puissance d'AXIS OS.

Mis au point pour produire de la valeur à long terme
Nos dispositifs sont prévus pour fonctionner pendant des années. AXIS OS est donc dans une perspective de robustesse et de longévité. Nous sommes également transparents sur l'espérance de vie de nos dispositifs, que nous communiquons sur axis.com.

Tests rigoureux spécifiques
AXIS OS est soumis à des tests minutieux pour vérifier qu'il excelle dans sa mission. Cette rigueur est cruciale si nous voulons qu'il surpasse les attentes de performances, de cybersécurité et d'intégration.

Qualité logicielle
AXIS OS témoigne d'une intransigeance absolue en matière de qualité logicielle. Le système d'exploitation est conçu en appliquant des standards élevés pour produire une expérience utilisateur familière, fiable et sûre pendant toute la durée de vie des dispositifs Axis.



La puissance d'une plateforme unique

Notre exigence d'excellence transcende les catégories de produits et prend corps dans la puissance d'une plateforme unique. Pilotant plus de 200 produits, des caméras-piétons aux solutions antidéflagrantes, en passant par les caméras PTZ, les sirènes, les haut-parleurs et les visiophones, notre plateforme unifiée est à la hauteur des enjeux de nos partenaires et clients.

Uniformité à l'œuvre
AXIS OS est au cœur d'une diversité de produits, qui partagent tous des API et des comportements identiques. Du fait que ces produits partagent une même plateforme, les intégrateurs et développeurs peuvent incorporer de nouveaux dispositifs Axis dans leurs systèmes sans pilotes complexes ou exclusifs. Non seulement l'intégration s'en trouve accélérée, mais les solutions sont plus pérennes en facilitant l'intégration des nouveautés de l'écosystème toujours plus riche d'Axis. Ainsi, les clients finaux bénéficient d'une expérience homogène. De plus, avec une seule plateforme, les développeurs gagnent du temps et réduisent les coûts, car chaque solution d'intégration s'applique à tous les dispositifs AXIS OS.

Polyvalence sans complexité
La puissance d'une plateforme unique réside également dans son potentiel de diversification sans introduire de complexité. Pour intégrer une caméra PTZ à un système de surveillance ou un haut-parleur à une solution audio intelligente, la procédure est comparable. Cette polyvalence s'étend au-delà de la compatibilité pour produire une expérience harmonieuse et de nombreuses possibilités pour créer des solutions intégrées et personnalisées à des besoins uniques.

Sécurité unifiée
Dans un monde où la cybersécurité est primordiale, la puissance d'une seule plateforme se matérialise aussi par une solution unifiée pour toutes les gammes de produits. Dès lors, le maintien de la sécurité n'est plus une épreuve fastidieuse à répéter pour chaque produit. Après la découverte et la correction d'une vulnérabilité, le correctif est simplement distribué sur tous les produits concernés. Cet avantage rationalise la gestion de la sécurité, tout en ouvrant la voie à une réponse collective rapide face aux menaces émergentes. En plus des gains de temps et de ressources, la résilience de l'écosystème Axis tout entier s'en trouve renforcée.

QUALITÉ LOGICIELLE
CYCLE DE VIE DES DISPOSITIFS
SUPPORT SUR LE CYCLE DE VIE
VOIE DE SUPPORT

Valeur à long terme

AXIS OS confère une valeur prévisible à vos dispositifs tout au long de leur cycle de vie. Son architecture stable et robuste limite les indisponibilités au minimum.

Nous publions des mises à jour logicielles et de nouvelles fonctionnalités pendant de nombreuses années. Complétés par une documentation pléthorique, des outils pratiques et des interfaces intuitives, les dispositifs Axis sont simples à utiliser et leur maintenance ne pose aucune difficulté. De plus, nous publions des plannings transparents et fiables de sortie des mises à jour pour que vous puissiez anticiper la maintenance selon les besoins de votre entreprise.

Dans les pages suivantes, nous abordons plus en détail la qualité des logiciels Axis, la gestion du cycle de vie d'AXIS OS et le support logiciel.

Un logiciel sur lequel vous pouvez compter

La qualité d'AXIS OS représente pour nous un élément essentiel. Avec environ 900 développeurs et 4000 validations de code par jour dans la branche principale d'AXIS OS, notre système d'exploitation évolue en permanence pour s'adapter aux besoins du marché. En créant deux builds logiciels par jour pour chacun de nos 200 et quelques produits, nous atteignons le chiffre stupéfiant de 182 500 builds par an, propices aux tests itératifs et à l'ajout de valeur.

Tests rigoureux

Le maintien de la stabilité du logiciel exige des tests rigoureux. De fait, nos systèmes exécutent un nombre colossal de 4 millions de tests divers par jour. Ils sont complétés par plus de 4000 validations de code par jour pour corriger les vulnérabilités et améliorer la qualité. En cumulé, ce sont plus de 1 milliard de tests et plus de 1 million de validations de code par an. De plus, nos clients et partenaires peuvent nous envoyer directement leurs commentaires sur AXIS OS par partage de données.

Amélioration continue

AXIS OS n'est pas un produit statique, mais dynamique car nous l'améliorons en permanence. Régulièrement mis à jour et enrichis, les dispositifs Axis de la voie de support active d'AXIS OS évoluent avec les progrès technologiques. Concrètement, le produit que vous achetez aujourd'hui gagnera en fonctionnalités et en valeur tout au long de son cycle de vie.

Prise en charge des dispositifs sur leur cycle de vie

L'avantage d'utiliser AXIS OS tient en particulier à sa prise en charge des dispositifs sur tout leur cycle de vie, de l'installation au replacement, en passant par la maintenance. AXIS OS fournit des outils et des ressources pour vous aider à gérer et à optimiser vos dispositifs Axis tout au long de leur durée de vie.

Simplicité d'installation et de configuration
AXIS OS simplifie l'installation et la configuration des dispositifs Axis en proposant des assistants, des modèles et des profils qui vous guident tout au long du processus. Vous pouvez également utiliser AXIS Device Manager (ADM) et AXIS Device Manager Extend (ADMX) pour installer et configurer simultanément plusieurs dispositifs, source de gain de temps et d'économies.

Suivi et diagnostics en continu
Avec votre accord, AXIS OS surveille et analyse les performances et le statut des dispositifs Axis par la collecte de données de contrôle d'intégrité sous forme de journaux, de rapports et d'alertes. Ces éléments vous assistent dans l'identification et la résolution des anomalies, tout en nous aidant à améliorer notre logiciel avec chaque nouvelle version.

Compatibilité et support sur le long terme
AXIS OS offre une assistance sur la durée pour les dispositifs Axis grâce à la publication régulière de correctifs de sécurité et de corrections de bugs. Notre support à long terme (LTS) veille à la compatibilité des dispositifs et applications Axis en minimisant les changements et les perturbations. Les dispositifs exécutant AXIS OS ont généralement une durée de vie d'au moins 10 ans. Dans certains cas, nous les prenons en charge jusqu'à 13 ans.

Confiance et engagement
AXIS OS est conçu pour satisfaire les attentes et besoins des clients qui privilégient la confiance et la qualité. AXIS OS établit une espérance de vie claire et transparente pour chaque produit et la maintient dans toute la mesure du possible. Axis entretient également des relations de long terme en offrant à ses clients un service et une assistance irréprochables.

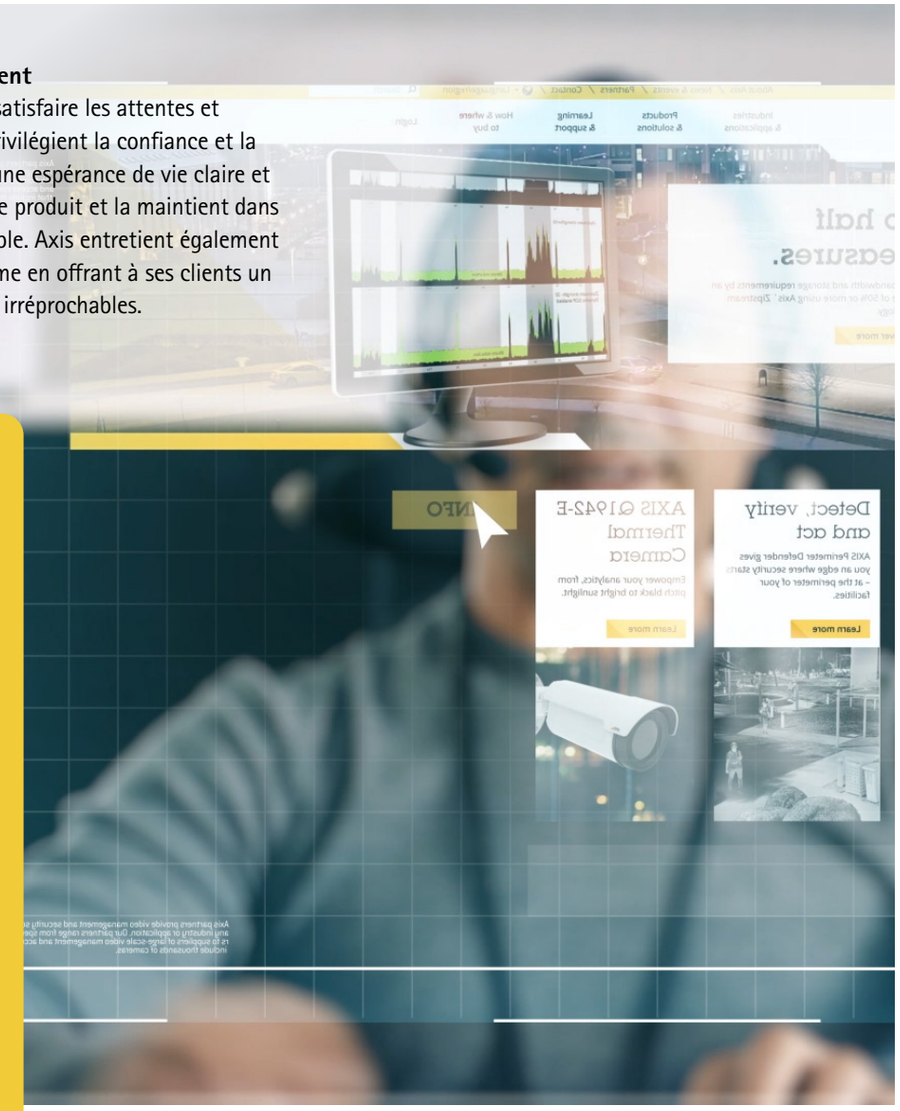
AXIS OS bêta

AXIS OS bêta est un avantage pour les développeurs les intégrateurs qui veulent évaluer et tester les nouvelles fonctionnalités d'AXIS OS avant leur publication officielle. AXIS OS bêta peut servir à tester la compatibilité sur certains dispositifs à un stade précoce, à vérifier les prochaines mises à jour de sécurité et à accéder à de nouvelles fonctions.

Parmi les avantages de l'utilisation d'AXIS OS bêta :

> Aperçu des fonctions nouvelles et améliorées d'AXIS OS en avant-première, par exemple fonctions d'analyse locales, connectivité IoT et modularisation de la plateforme.
> Opportunité de transmettre des commentaires et des suggestions à Axis pour contribuer à orienter le développement et les améliorations d'AXIS OS.
> Possibilité de préparer et d'adapter vos applications et systèmes pour les mises à jour et changements à venir dans AXIS OS pour vous prémunir de problèmes potentiels.

Pour en savoir plus sur les préversions AXIS OS bêta, cliquez ici.



Support du logiciel AXIS OS sur son cycle de vie

La prise en charge d'AXIS OS sur son cycle de vie comporte plusieurs voies. Le support actif et le support à long terme (LTS) sont les voies principales. Il existe également des voies de support spécifique au produit (PSS) pour accompagner le cycle de vie de certains produits.

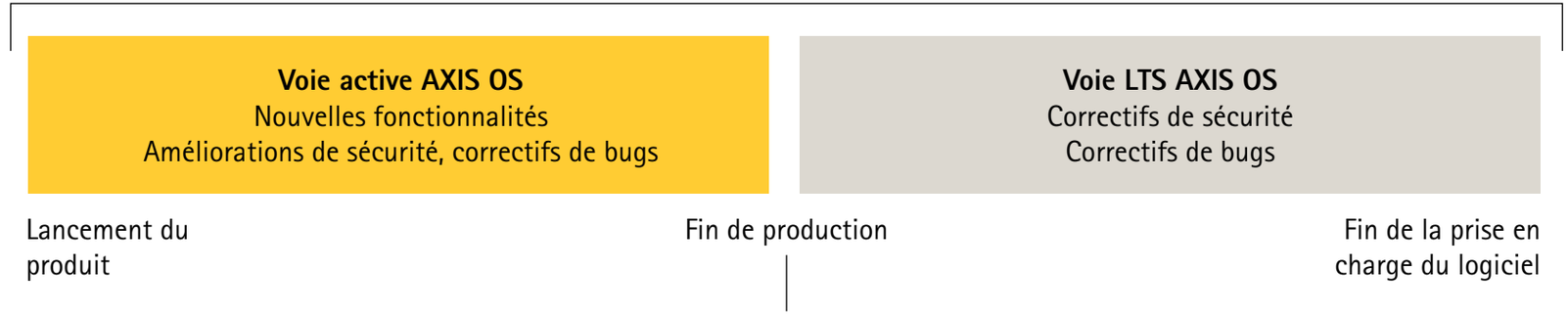
La durée de vie minimale d'un dispositif Axis dépasse la moyenne du marché. La solide garantie de 5 ans sur les matériels est complétée par la prise en charge du logiciel AXIS OS pendant de nombreuses années. La plupart des dispositifs embarquent un logiciel AXIS OS dont la durée de vie remarquable atteint 8 à 12 ans.

Voici comment :

1. Lorsqu'Axis commercialise un nouveau dispositif, seule la voie active AXIS OS est disponible. Pendant la période initiale d'exploitation, vous bénéficiez de mises à jour et d'améliorations régulières, y compris des nouvelles fonctionnalités.
2. Une voie de support à long terme (LTS) est ensuite proposée comme alternative à la voie active dans les deux ans suivant la sortie du produit. À ce stade, vous pouvez choisir l'une ou l'autre : la voie active ou la voie LTS. Les produits de la voie LTS sont actualisés avec des correctifs de vulnérabilités et de bugs uniquement.
3. Lorsqu'un dispositif n'est plus fabriqué, soit deux à quatre ans après sa sortie, la voix active correspondante est abandonnée. À ce stade, tous les dispositifs passent automatiquement à la voie de support LTS, où ils sont pris en charge avec des correctifs de vulnérabilités et de bugs pendant au moins 5 ans supplémentaires.

Support du logiciel AXIS OS sur son cycle de vie

Prise en charge du logiciel (8 à 12 ans)



Axis assure une prise en charge du logiciel **pendant au moins 5 ans** à partir de la date d'abandon du produit

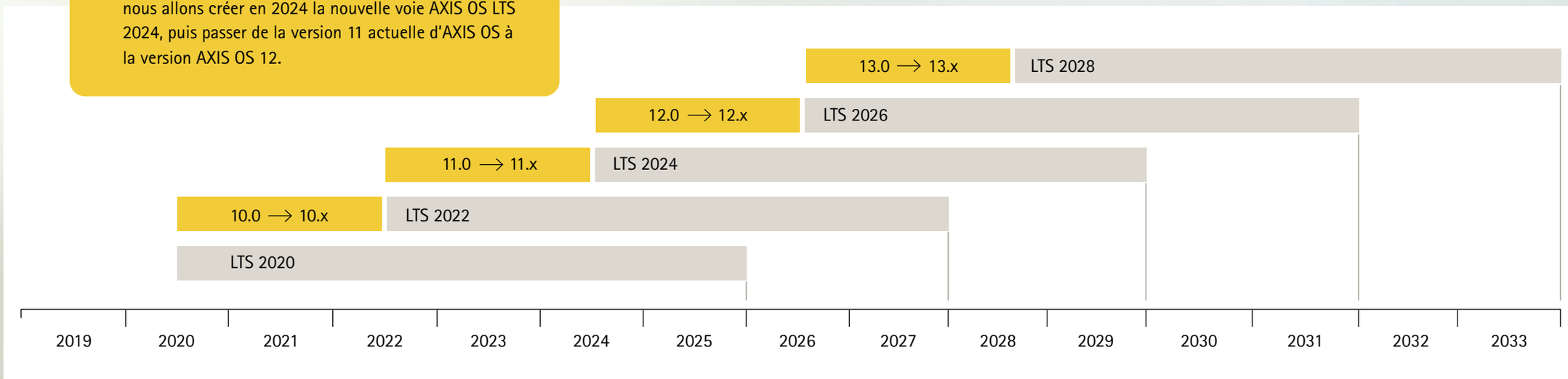
Voie de support logiciel : laquelle pour vous ?

Une fois que la voie active et la voie de support à long terme sont disponibles, les clients peuvent choisir la plus adaptée à leurs besoins sur les préconisations d'Axis.

Voie de support active
La voie active AXIS OS restitue l'expérience la plus actuelle et la plus fonctionnelle du système d'exploitation AXIS OS. Destinée aux clients qui veulent bénéficier immédiatement des améliorations et fonctions les plus récentes, cette voie est la seule disponible pour les dispositifs sortis récemment. Elle permet aux utilisateurs de profiter de toutes les évolutions des fonctionnalités du dispositif : de nouvelles fonctions de sécurité sont ajoutées pour une exploitation encore plus sûre, et les fonctionnalités existantes reçoivent des améliorations régulières. Lorsque vos dispositifs suivent la voie active AXIS OS, vous en tirez plus de valeur sans frais supplémentaires, même des années après leur achat. En l'absence de dépendance de compatibilité, la voix active est à privilégier pendant toute la période où elle est disponible.

Voie de support à long terme (LTS)
Si vous recherchez l'uniformité des API et la compatibilité, vous devriez choisir la voie de support à long terme une fois qu'elle est disponible. La voie LTS se focalise sur la rétrocompatibilité et fournit régulièrement des correctifs de sécurité et des corrections de bugs. Cette voie est axée sur la cybersécurité plutôt que sur l'ajout de nouvelles fonctions de sécurité. Au lieu d'ajouter des nouveautés, elle minimise les changements pour réduire les perturbations. La voie LTS convient aux clients qui privilégient la confiance et la qualité, et qui recherchent un système tiers bien intégré. Chaque voie LTS est prise en charge pendant 5 ans. Les voies LTS sont publiées tous les 24 mois, en phase avec une nouvelle version de la voie active normale. Tous les dispositifs passent automatiquement à la voie LTS une fois leur production abandonnée.

Ce graphique illustre la voie active AXIS OS à côté des voies LTS introduites au fil des années. Tous les 24 mois environ, une nouvelle voie LTS est créée et la version majeure d'AXIS OS augmente d'une unité. Par exemple, nous allons créer en 2024 la nouvelle voie AXIS OS LTS 2024, puis passer de la version 11 actuelle d'AXIS OS à la version AXIS OS 12.



MODÈLE ASDM
CYBERSÉCURITÉ INTÉGRÉE
GESTION DES VULNÉRABILITÉS
TOUT-EN-UN

Gros plan sur la cybersécurité

AXIS OS adopte une approche « Security by design », où la sécurité fait partie intégrante de la conception. Notre modèle de développement de sécurité ASDM (Axis Security Development Model) définit les processus et outils pour réduire le risque de vulnérabilités pendant la phase de développement logiciel et au-delà.

Axis Edge Vault, notre plateforme matérielle de cybersécurité, garantit un amorçage sécurisé et un environnement à l'épreuve des intrusions pour le stockage des clés cryptographiques chargées par le client. Le cœur du logiciel AXIS OS est formé de composants open-source soigneusement testés. Chaque version est accompagnée d'une nomenclature logicielle (SBOM) qui démontre qu'AXIS OS est à jour et que les vulnérabilités connues sont corrigées.

AXIS OS est également certifié selon la norme ETSI EN 303 645, qui concerne spécifiquement la sécurité des dispositifs en périphérie de réseau. La conformité FIPS 140 signifie qu'AXIS OS respecte les normes cryptographiques les plus récentes définies par le National Institute of Standards and Technology (NIST). Et enfin, en tant qu'autorité de numérotation CVE (Common Vulnerability and Exposures), nous appliquons les bonnes pratiques d'identification, de gestion et de publication des vulnérabilités.

Les pages suivantes détaillent le modèle ASDM, Axis Edge Vault, la gestion des vulnérabilités et le concept de sécurité unifiée.

Développement à sécurité intégrée

Le modèle Axis de développement de sécurité (ASDM, Axis Security Development Model) intègre efficacement la cybersécurité dans le cycle de développement logiciel. Il décrit les activités de sécurité à mener durant les différentes phases de développement logiciel. Son objectif est de réduire les vulnérabilités et les coûts de développement, par la définition d'un cadre de référence de cybersécurité et de consignes d'application.

Modèle ASDM créé par Axis
Le modèle Axis de développement de sécurité ne provient pas d'un cadre standard prêt à l'emploi. Nous avons examiné une multitude de normes et de cadres relevant de la cybersécurité, tels que ISO 27001, IEC 62443, NIST, BSIMM et CMMC. Le lien qui les unit est l'incorporation de la sécurité à toutes les phases de développement. Avec ce référentiel comme point de départ, nous avons adapté notre modèle à notre culture d'entreprise, à nos pratiques de développement et aux types de produits que nous commercialisons.

Boîte à outils ASDM
La boîte à outils ASDM prescrit une série d'activités pour résoudre une variété de problèmes de sécurité : analyse de risque, modélisation des menaces, tests des modèles de menace, analyse du code statique, recherche des vulnérabilités et évaluation des fournisseurs en sont des exemples. Les équipes de développement choisissent les activités à entreprendre selon le type de logiciel à développer. L'ambition consiste à renforcer la cybersécurité plutôt qu'à simplement respecter un processus.

Atouts d'une expertise extérieure
La plupart des grandes tâches de développement sécurisé des logiciels sont menées par l'équipe R&D d'Axis et nos ingénieurs en logiciels. Cependant, nous admettons que les connaissances et l'expertise des autres peuvent nous être bénéfiques. Ainsi, nous sous-traitons les tests de pénétration à des entreprises spécialisées. Par ailleurs, nous animons le programme de chasse aux bugs d'AXIS OS, qui décerne des récompenses financières aux chercheurs en sécurité qui nous aident à identifier les vulnérabilités.

Gestion	formation	Réunion de l'équipe ASDM	Évaluation ASDM	Conformité et normes de sécurité

Configuration requise	Conception	Mise en œuvre	Vérification	Déploiement
Analyse de risque Évaluation des fournisseurs Confidentialité des données Évaluation de la sécurité open-source	Modélisation des menaces	Analyse du code statique Analyse de composition des logiciels	Test des modèles de menace Test de pénétration externe Analyse des vulnérabilités Évaluation de la sécurité interne	Gestion des vulnérabilités Gestion des incidents Statut de sécurité des produits/ solutions Programme de chasse aux bugs

Cybersécurité intégrée

Protection de l'intérieur
Axis Edge Vault est notre plateforme matérielle de cybersécurité. Elle représente une fondation solide pour s'assurer que vos dispositifs Axis sont fiables et dignes de confiance aux yeux de votre réseau. Mais ce socle matériel perdrait tout son sens en l'absence d'un système d'exploitation capable d'en concrétiser tout le potentiel. AXIS OS utilise la plateforme Axis Edge Vault pour renforcer la sécurité en périphérie de réseau dans tous les scénarios d'application.

Axis Edge Vault comporte plusieurs fonctionnalités, notamment :

Stockage sécurisé des clés
Le magasin de clés sécurisé fait appel à des modules de calcul cryptographique pour protéger le calcul et le stockage des clés cryptographiques. Il préserve l'identifiant de dispositif et d'autres informations sensibles contre les accès non autorisés, même en cas de dispositif compromis. Les modules de calcul cryptographique utilisés sont l'environnement d'exécution de confiance (TEE) intégré au processeur SoC (System-on-Chip), ainsi qu'un élément sécurisé dédié ou un module de plateforme sécurisé (TPM 2.0), sous forme de composants distincts sur la carte électronique.

Système d'exploitation signé et amorçage sécurisé
La signature du système d'exploitation revient à signer le code de l'image logicielle du dispositif. Avec le système d'exploitation signé et l'amorçage sécurisé, les dispositifs peuvent télécharger et exécuter uniquement le système d'exploitation AXIS OS authentique. Ce niveau de protection supplémentaire empêche toute altération dans les chaînes d'approvisionnement en matériels et en logiciels.

Identifiant de dispositif Axis
L'ID de dispositif Axis est conforme à la norme IEEE 802.1AR et certifie l'identification du dispositif pour l'intégrer à un réseau. Il fait office de passeport d'authenticité pour chaque dispositif Axis fabriqué.

Système de fichiers chiffré
Le chiffrement du système de fichiers protège les données qu'il contient de toute extraction ou altération lorsque le dispositif est inutilisé, par exemple pendant son transport entre les locaux d'un intégrateur de système et le client final.

Vidéo signée
La vidéo signée permet aux utilisateurs de confirmer l'authenticité de la vidéo capturée et l'absence d'altération.

Plateforme de cybersécurité Axis Edge Vault

Modules de calcul cryptographique	Points forts	Scénarios d'utilisation
Élément de sécurité TPM 2.0 Sécurité du SoC (environnement TEE)	Démarrage sécurisé Système d'exploitation signé Identifiant du périphérique Axis Fichier de clés sécurisé Vidéo signée Système de fichiers crypté	Identité de dispositif de confiance Stockage sécurisé des clés Détection des modifications à la vidéo Protection de la chaîne d'approvisionnement

*Remarque : Certains dispositifs ne prennent pas en charge toutes les fonctionnalités d'Axis Edge Vault. Consultez la fiche technique ou le sélecteur de produits Axis pour vérifier les fonctions prises en charge par un produit donné.

Gestion des vulnérabilités

Pour minimiser le risque d'exposition de nos clients, nous respectons les bonnes pratiques de gestion et de traitement transparent des vulnérabilités.

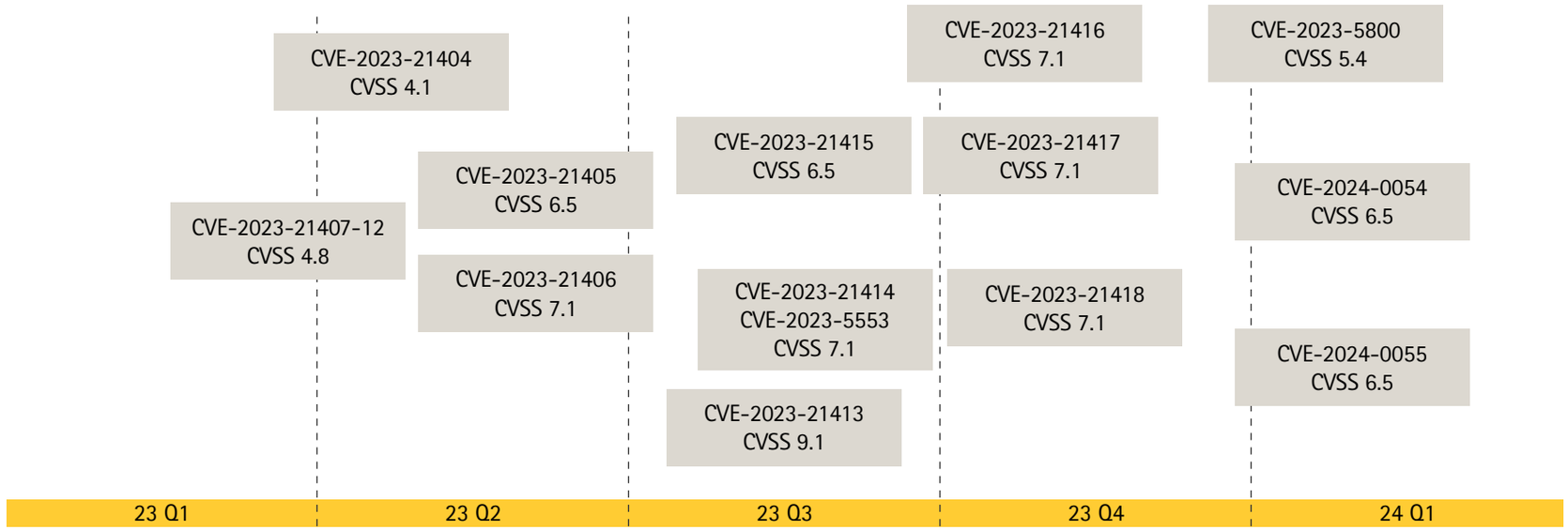
Excellente gestion des vulnérabilités
Il n'existe aucune méthode pour garantir l'absence totale de vulnérabilités dans les produits et services fournis par Axis. C'est d'ailleurs le cas pour tous les logiciels et services d'où qu'ils viennent. En revanche, nous nous efforçons d'identifier et de neutraliser les vulnérabilités potentielles à toutes les étapes pour minimiser le risque lié au déploiement de produits et services Axis dans l'environnement des clients.

Autorité de numérotation CVE
Axis est une autorité de numérotation CVE (CNA). Nous adhérons au programme CVE (Common Vulnerabilities and Exposures) pour collaborer avec des entreprises œuvrant elles aussi à l'amélioration de la gestion des vulnérabilités. Nos méthodes de traitement, publication et correction des vulnérabilités respecte le cadre international défini par cet organisme à but non lucratif et par notre politique de gestion des vulnérabilités auprès du public.

Gestion transparente et fiable
Axis utilise le système bien connu de notation CVSS (Common Vulnerability Scoring System) pour classer les vulnérabilités liées au code développé par Axis ou au code open-source d'autres fournisseurs. Nous analysons les vulnérabilités dans le code open-source en fonction de leur pertinence pour nos produits lorsque les recommandations des bonnes pratiques sont appliquées. Vous pouvez vous abonner au Service de notifications de sécurité Axis pour recevoir des informations concernant les vulnérabilités et d'autres sujets liés à la sécurité des produits Axis.

Partenariats avec le monde de la recherche en sécurité
Nous accueillons favorablement le travail des chercheurs en sécurité et des organismes d'étude sur la sécurité qui nous contactent pour signaler des vulnérabilités. Nous n'hésitons pas à les publier et à les corriger. L'important, c'est une gestion correcte et transparente des vulnérabilités, complétée par une procédure de publication éthique et responsable. Les circonstances de leur découverte sont secondaires.

Vulnérabilités d'AXIS OS



Vulnérabilités d'AXIS OS publiées par Axis.

Expérience de sécurité tout-en-un

Dans les dispositifs réseau exécutant par AXIS OS, les composants matériels et logiciels interagissent pour permettre aux clients d'exploiter en toute sécurité les dispositifs, leurs services et les systèmes auxquels ils sont connectés. Une protection complète en couches superposées commence par une fondation de sécurité et une plateforme matérielle de sécurité et s'achève par le logiciel. Les dispositifs pilotés par AXIS OS sont protégés par une approche de la cybersécurité en profondeur et multicouches. Ce principe accroît la sécurité cumulée des données, des applications et des processus.

Ainsi, quelle que soit la finalité d'un dispositif Axis, la protection et la sécurité de communication sont immanquablement incluses pour l'intégrer correctement et en toute sécurité aux systèmes d'autres fournisseurs.

Contrôle d'accès	**Gestion du contrôle d'accès** Gestion locale des dispositifs utilisateurs avec indicateur de complexité du mot de passe Gestion fédérée des dispositifs utilisateur par OpenID Connect (RFC6749, section 1.3.1, Authorization Code) pour intégration aux services AD FS et application de fonctions comme l'obligation de mots de passe complexes, la rotation des mots de passe, l'authentification multifacteur (MFA), le blocage automatique de compte ou la fonctionnalité d'habilitation Microsoft AD		**Confidentialité** Usage des données de diagnostic Approche minimaliste du volume de données spécifiques au client à stocker
Application	**Sécurité applicative** Sécurité applicative basée sur TLS (MQTT, SFTP, NTS, HTTPS, WebRTC) Flux vidéo chiffré (RTSPS/SRTP, HTTPS), Remote Syslog sécurisé		
Système d'exploitation	**Chiffrement et protection des données** OpenSSL 1.1.1 et 3.0 Cryptographie et infrastructure PKI à certificats X.509 Protocole de sécurité TLS 1.2/TLS 1.3 Chiffrement des cartes SD (AES-XTS-Plain64 256 bits) Système de fichiers chiffré (AES-XTS-Plain64 256 bits), Vidéo signée	**Sécurité par défaut** HTTPS actif par défaut Protection contre les attaques par force brute Pare-feu sur hôte NTS (Network Time Security) Versions TLS non sécurisées désactivées Port de débogage/UART désactivé	**Sécurité des réseaux d'entreprise** IEEE 802.1X (contrôle d'accès réseau) IEEE 802.1AR (identité de dispositif sécurisée) IEEE 802.1AE (sécurité MAC, MACsec)
	Système d'exploitation AXIS OS Système d'exploitation basé sur Linux comptant plus de 95 % de composants open-source standard, dont OpenSSL, Apache, Curl, etc. Voie active pour enrichir les fonctionnalités et voies de support à long terme (LTS) sur 5 ans pour les scénarios de rétrocompatibilité et d'intégration aux systèmes d'autres fournisseurs.		
Sécurité assistée par matériel (processeur)	**Racine de confiance matérielle** Sécurité basée sur processeur SoC (System-on-Chip) ARM Environnement d'exécution de confiance (TEE/OP-TEE) Module de plateforme sécurisé (TPM 2.0), élément sécurisé	**Stockage sécurisé des clés** Stockage et opérations des clés cryptographiques protégés des altérations : clés privées chargées par le client, clés de signature vidéo, ID de dispositif Axis, etc.	
Fondation de sécurité	**Modèle de développement de sécurité Axis** Modèle de développement de sécurité Axis (ASDM) Tests de pénétration par des prestataires Programme de chasse aux bugs avec Bugcrowd Nomenclature logicielle (SBOM)	**Conformité** Common Criteria EAL FIPS 140 ETSI EN 303 645	**Identité de dispositif de confiance** Plateforme de cybersécurité Axis Edge Vault Amorçage sécurisé avec système d'exploitation signé (signature de code) ID de dispositif Axis (IEEE 802.1AR)

Intégration de première classe

L'intégration joue un rôle central pour les produits Axis. C'est pourquoi nous favorisons des API robustes et homogènes qui simplifient l'intégration dans une diversité d'applications.

Vous pouvez ainsi créer des solutions complètes qui exploitent toutes les capacités de vos dispositifs Axis.

Les pages suivantes approfondissent VAPIX (notre API maison), notre travail avec ONVIF et l'IoT, la modularisation de la plateforme avec ACAP et l'automatisation de l'intégration aux réseaux.

Avantage Axis avec VAPIX, ONVIF, l'IoT et l'intégration cloud

Sur le marché dynamique de la surveillance et de la connectivité, Axis Communications propose une suite de solutions d'intégration qui redéfinissent l'ordre établi.

VAPIX : extensibilité historique
VAPIX, notre cadre d'API ouvert, met en lumière notre engagement en faveur de l'innovation. Prenant en charge les appels HTTP GET et POST, ainsi que les formats JSON et XML, il permet aux développeurs de créer des solutions sur mesure en toute simplicité. VAPIX dispose de la bibliothèque la plus riche et durable du marché. Il fait figure de pionnier dans l'intégration ouverte des produits réseau Axis, avant même ONVIF.

ONVIF : normes collaboratives
Axis collabore au forum ouvert ONVIF pour développer un esprit de coopération faisant progresser le marché et offrant aux utilisateurs des solutions complètes et interopérables. ONVIF propose des interfaces normalisées et encourage leur utilisation pour une interopérabilité efficace des produits de sécurité physique sur IP. Il en résulte pour nos partenaires une intégration simplifiée, où les dispositifs Axis s'imbriquent en toute transparence dans une variété étendue de systèmes

IoT : cap sur l'avenir
Alors que l'internet des objets (IoT) réinvente la connectivité, les dispositifs Axis contribuent à l'évolution de cet écosystème. Axis prend en charge des protocoles comme MQTT qui stimulent l'innovation dans le domaine IoT. Avec Axis, vos dispositifs ne sont pas seulement connectés, ils s'inscrivent dans un environnement IoT en pleine croissance.

Intégration au cloud : là où l'innovation atteint des sommets
Dans le domaine de la connectivité numérique, Axis développe l'intégration au cloud au moyen d'API conçues pour interagir sans difficulté avec les grandes plateformes comme Microsoft Azure et Amazon Web Services (AWS). Avec les avancées technologiques, vous allons prendre en charge davantage de technologies cloud, comme MQTT pour les services de messagerie et WebRTC pour la diffusion vidéo et audio. Notre ambition consiste à offrir à nos utilisateurs les moyens de capitaliser au maximum sur les technologies cloud.

Modularisation de la plateforme avec ACAP

Une des caractéristiques essentielles d'AXIS OS est la capacité de modularisation de sa plateforme au travers d'ACAP (AXIS Camera Application Platform). La plateforme d'applications ACAP est un cadre permettant aux développeurs de créer et de déployer des applications et services répondant au cahier des charges d'un projet, par exemple des fonctions d'analyse vidéo ou audio et d'autres extensions personnalisées. Comme les applications ACAP ne dépendent pas des fonctionnalités de base d'AXIS OS, elles peuvent être installées, mises à jour et éliminées sans incidence sur le reste du système. Les applications ACAP peuvent également communiquer entre elles et avec les systèmes externes par des protocoles et des API standardisés.

Évolutivité et performances
ACAP exploite l'architecture en microservices du système d'exploitation des dispositifs Axis. Ainsi, chaque service peut monter ou descendre en gamme en toute indépendance, en fonction de la demande et de la charge. Cette architecture améliore les performances et la disponibilité globales du système en optimisant la consommation et l'allocation des ressources.

Adaptabilité et personnalisation
Avec ACAP, les dispositifs Axis gagnent en polyvalence, en adaptabilité et en personnalisation, car ils prennent en charge plusieurs types d'intégrations, de fonctions d'analyse et de dispositifs. De plus, ACAP réduit le couplage et accroît la cohésion de la plateforme, car chaque application est en grande partie indépendante d'AXIS OS et fortement cohésive en elle-même.

Fiabilité et simplicité de maintenance
Il est possible de tester, surveiller et déboguer chaque service de manière isolée et indépendante. La recherche de panne et le diagnostic s'en trouvent simplifiés, renforçant la résilience du système et sa tolérance aux pannes. C'est là que se distingue une fois encore AXIS OS en termes de qualité logicielle.

AXIS OS pour les équipes informatiques

Une automatisation et une intégration bien pensées dans l'infrastructure informatique garantit des contrôles de sécurité appropriés et peut faire gagner du temps tout en réduisant les coûts. Toute complexité superflue du système est ainsi minimisée. Parmi les avantages de combiner les dispositifs Axis avec les logiciels intégrés à l'infrastructure informatique d'entreprise, vous pouvez :

> réduire la complexité du système en éliminant les réseaux intermédiaires dédiés aux dispositifs physiques ;

> réduire les coûts en ajoutant des processus automatiques d'intégration et de gestion des dispositifs ;

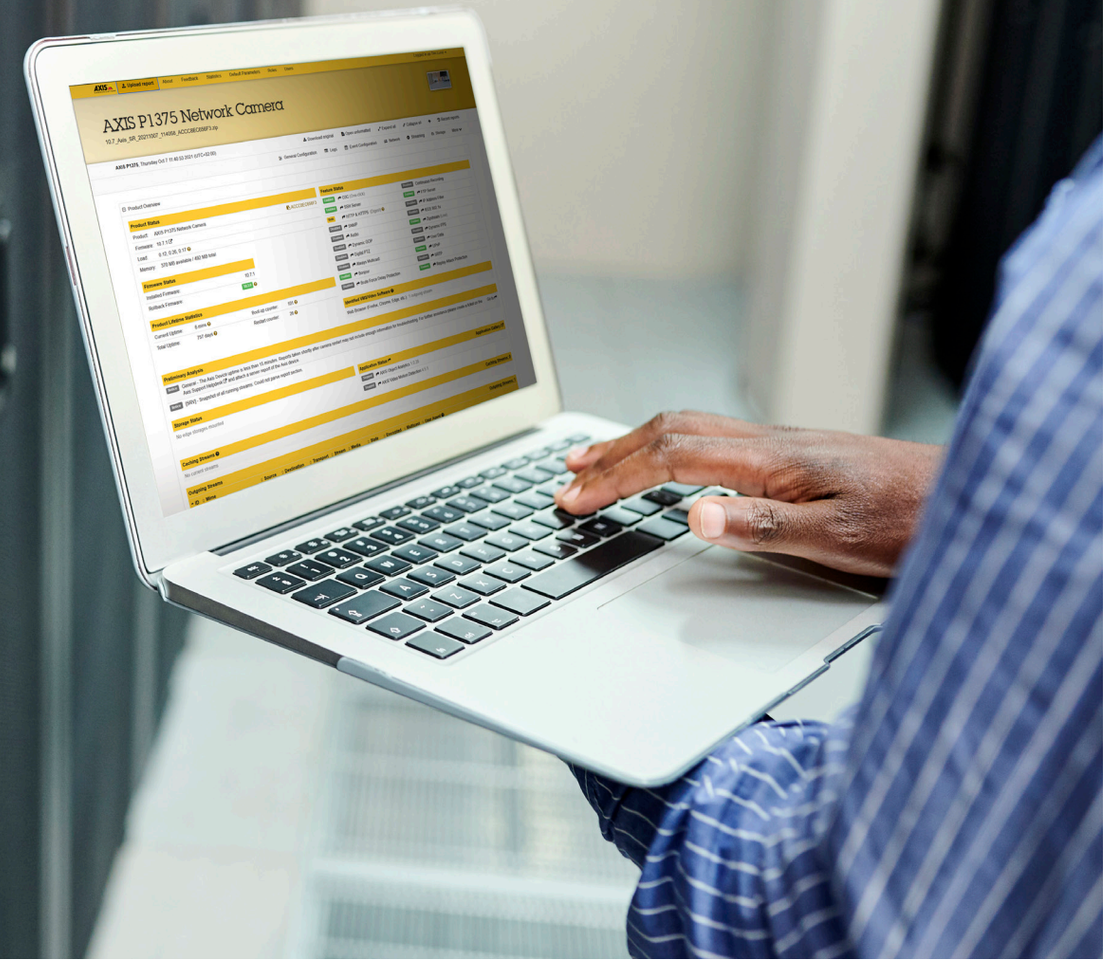
> capitaliser sur les contrôles de sécurité des réseaux Zero-Trust tels que IEEE 802.1X et IEEE 802.1AR ;

> renforcer la sécurité globale des réseaux par l'introduction du chiffrement des données à un niveau fondamental avec l'aide de IEEE 802.1AE MACsec, par exemple pour que le dispositif Axis contribue à la sécurité du réseau ;

> surveiller le dispositif Axis par des protocoles normalisés comme Remote Syslog, par exemple pour le suivi des journaux et de l'état d'intégrité.

Réseau sécurisé d'après les principes du Zero-Trust
La création de réseaux convergents sécurisés basés sur les principes du Zero-Trust est capitale pour éliminer les systèmes isolés autonomes. Le renforcement de la sécurité, la baisse des coûts de configuration et de maintenance et une application plus rigoureuse des politiques informatiques sont possibles en intégrant les dispositifs Axis à l'infrastructure informatique d'entreprise au moyen de normes et de protocoles réseau ouverts bien définis.

Avantage pour les équipes informatiques
Pour les équipes informatiques chargées de la sécurité du réseau, les dispositifs Axis constituent un avantage. L'intégration, la maintenance et l'exploitation des dispositifs Axis sont plus simples, car en plus de leur polyvalence, ils rappellent les solutions informatiques définies par des protocoles réseau normalisés IEEE et IETF et en partagent la conception. Les dispositifs Axis sont considérés comme des « citoyens de confiance » dans les réseaux des clients, favorisant une meilleure sécurité.



Parlons-en

AXIS OS est la raison pour laquelle vous pouvez compter sur les dispositifs Axis. Il est central à la qualité d'image, à la qualité audio et bien plus.

AXIS OS est écrit spécialement pour concrétiser les critères essentiels de vos dispositifs réseau, à savoir valeur à long terme, mesures de sécurité rigoureuses et simplicité d'intégration.

Nous nous ferons un plaisir d'échanger avec vous sur la valeur ajoutée que peuvent apporter les dispositifs Axis à votre activité ou votre entreprise.

Contactez-nous sans attendre !

Vous pouvez également découvrir nos dispositifs sur axis.com

À propos d'Axis Communications

En créant des solutions qui renforcent la sécurité et améliorent la performance des entreprises, Axis contribue à un monde plus intelligent et plus sûr. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 4000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.