La potenza di un'unica piattaforma

Progettata appositamente per offrire valore a lungo termine, cybersecurity e integrazione

AXIS COMMUNICATIONS

Il centro propulsore dei dispositivi di rete Axis

AXIS OS è il sistema operativo basato su Linux utilizzato con la maggior parte dei dispositivi di rete Axis. È il cuore pulsante di oltre 200 prodotti Axis e di decine di milioni di dispositivi installati presso clienti. AXIS OS testimonia l'impegno verso l'innovazione, l'affidabilità e la perfetta integrazione. Il software Axis, migliorato versione dopo versione, è il motivo per cui i nostri dispositivi sono così affidabili e offrono una qualità d'immagine straordinaria. In effetti, l'80% delle nostre attività di ricerca e sviluppo ruota intorno allo sviluppo software.

Aggiungiamo continuamente nuove funzionalità e miglioriamo quelle esistenti. Inoltre incrementiamo costantemente la sicurezza applicando patch alle vulnerabilità dei dispositivi basati su AXIS OS, migliorandoli e consentendo di svolgere più applicazioni in modo più sicuro.

AXIS OS è progettato specificamente per soddisfare i criteri più importanti nei dispositivi di rete: valore a lungo termine, elevati standard di cybersecurity e facilità di integrazione.

Progettato specificamente per i dispositivi Axis
Realizzato dalla divisione sviluppo e basato sulla stabilità di Linux Yocto OpenEmbedded, AXIS OS supera le build generiche perché è perfettamente ottimizzato per le specifiche esigenze dei dispositivi edge Axis, come telecamere, altoparlanti e sistemi di controllo accessi.

Valore a lungo termine
AXIS OS garantisce che i dispositivi siano sempre attivi. Progettato per funzionare 24 ore su 24 e 7 giorni su 7, offre prestazioni costanti e reattive in linea con le esigenze delle tue applicazioni, di giorno e di notte.

Cybersecurity solida
Al centro di AXIS OS c'è l'impegno verso la cybersecurity. AXIS OS, con la sua architettura di sicurezza integrata, aiuta a proteggere i tuoi dispositivi. Grazie a uno sviluppo software sicuro e a un'attenta gestione delle vulnerabilità, AXIS OS garantisce che i dati e i dispositivi resistano puntualmente alle minacce emergenti.

Facile integrazione
AXIS OS incorpora VAPIX, ONVIF e altre piattaforme, aiutando i dispositivi di rete Axis a integrarsi facilmente in diversi ecosistemi. Questa integrabilità offre un'esperienza ottimale e interconnessa a utenti e sviluppatori.

I numeri di AXIS OS

900 sviluppatori

24.000.000 di righe di codice scritte

4000 commit di codice al giorno

4.000.000 di test automatici al giorno

200+ prodotti Axis con percorso di supporto Active

500+ prodotti Axis con percorso LTS (Long-Term Support)

6+ versioni software nel percorso Active all'anno

2000+ componenti software

Oltre il **95%** di componenti open source

Progettato appositamente per i dispositivi Axis

Quando abbiamo progettato AXIS OS, ci siamo concentrati specificamente su prestazioni, integrazione, sicurezza e qualità del software per i dispositivi edge.

Basato sulla stabilità di Linux Yocto OpenEmbedded, AXIS OS costituisce una piattaforma unificata per tutti i dispositivi di rete Axis, offrendo la massima coerenza in una vasta gamma di prodotti.

Le seguenti pagine illustrano in modo più approfondito il valore di un sistema operativo realizzato appositamente per i dispositivi edge e la potenza di un'unica piattaforma.

Progettato per l'eccellenza in modalità edge

In un panorama dominato da soluzioni generiche, AXIS OS non è semplicemente l'ennesimo sistema operativo Linux. Il sistema trascende le convenzioni delle build Linux generiche per offrire una soluzione perfettamente ottimizzata per le specifiche esigenze dei dispositivi edge. Questa specializzazione offre ai prodotti Axis prestazioni, affidabilità e sicurezza esclusive.

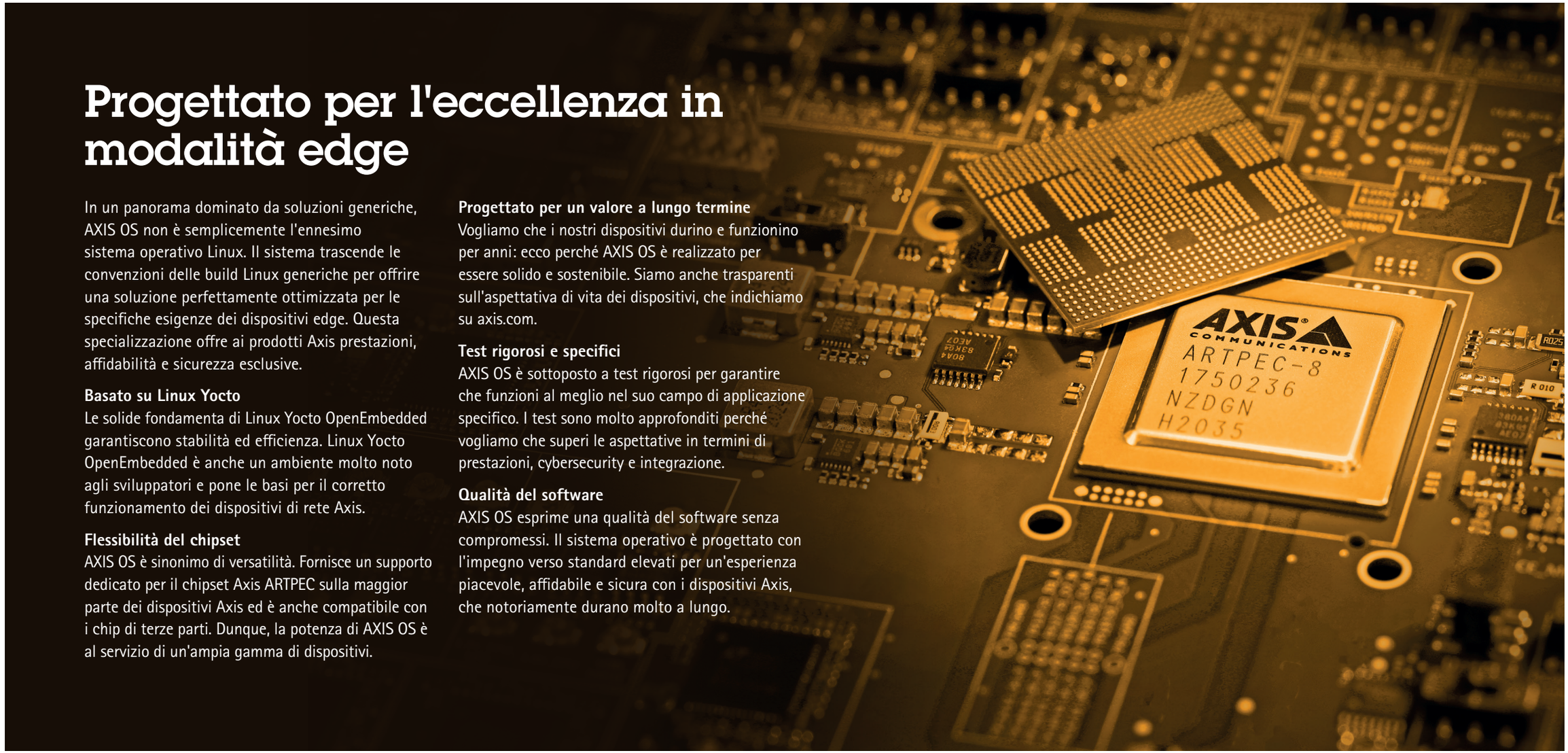
Basato su Linux Yocto
Le solide fondamenta di Linux Yocto OpenEmbedded garantiscono stabilità ed efficienza. Linux Yocto OpenEmbedded è anche un ambiente molto noto agli sviluppatori e pone le basi per il corretto funzionamento dei dispositivi di rete Axis.

Flessibilità del chipset
AXIS OS è sinonimo di versatilità. Fornisce un supporto dedicato per il chipset Axis ARTPEC sulla maggior parte dei dispositivi Axis ed è anche compatibile con i chip di terze parti. Dunque, la potenza di AXIS OS è al servizio di un'ampia gamma di dispositivi.

Progettato per un valore a lungo termine
Vogliamo che i nostri dispositivi durino e funzionino per anni: ecco perché AXIS OS è realizzato per essere solido e sostenibile. Siamo anche trasparenti sull'aspettativa di vita dei dispositivi, che indichiamo su axis.com.

Test rigorosi e specifici
AXIS OS è sottoposto a test rigorosi per garantire che funzioni al meglio nel suo campo di applicazione specifico. I test sono molto approfonditi perché vogliamo che superi le aspettative in termini di prestazioni, cybersecurity e integrazione.

Qualità del software
AXIS OS esprime una qualità del software senza compromessi. Il sistema operativo è progettato con l'impegno verso standard elevati per un'esperienza piacevole, affidabile e sicura con i dispositivi Axis, che notoriamente durano molto a lungo.



La potenza di un'unica piattaforma

Il nostro impegno verso l'eccellenza trascende le categorie dei prodotti e si concretizza in quella che chiamiamo "la potenza di un'unica piattaforma". Con il supporto di oltre 200 prodotti, dalle Body Cam alle soluzioni antideflagranti, dalle telecamere PTZ alle sirene fino agli altoparlanti e agli interfoni, la nostra piattaforma unificata è pensata per offrire a partner e clienti prestazioni impeccabili.

Coerenza in azione
AXIS OS è utilizzato su una gamma variegata di prodotti, con API e comportamenti comuni a tutti i dispositivi. La piattaforma unificata garantisce che integratori e sviluppatori possano incorporare nuovi dispositivi Axis nei loro sistemi senza driver complessi e specifici per ogni dispositivo. Questo non solo accelera l'integrazione, ma predispone anche le soluzioni al futuro, consentendo di adottare rapidamente nuovi prodotti nell'ecosistema Axis in continua espansione. Il sistema operativo garantisce ai clienti finali un'esperienza uniforme. Inoltre, consente agli sviluppatori di risparmiare tempo e denaro perché con AXIS OS tutte le soluzioni di integrazione funzionano su tutti i dispositivi.

Versatilità senza complessità
La potenza del sistema operativo risiede anche nella sua piattaforma unificata che consente di adottare soluzioni diversificate senza immettere complessità. Che tu stia integrando una telecamera PTZ in un sistema di sorveglianza o incorporando un altoparlante in una soluzione audio intelligente, il processo è coerente. Questa versatilità si spinge oltre la compatibilità per offrire un'esperienza armoniosa, con numerose possibilità di creare soluzioni integrate su misura per esigenze specifiche.

Sicurezza unificata
In un mondo in cui la cybersecurity è fondamentale la potenza di una piattaforma si manifesta anche nella capacità di supportare gamma di prodotti tramite una soluzione unificata. Mantenere la sicurezza prodotto per prodotto è pressoché impossibile: quando una vulnerabilità viene identificata e risolta, la correzione viene distribuita a tutti i prodotti supportati. Questo non solo semplifica la gestione della sicurezza, ma facilita anche una risposta rapida e collettiva alle minacce emergenti. Inoltre fa risparmiare tempo e risorse e aumenta la resilienza dell'intero ecosistema Axis.

QUALITÀ DEL SOFTWARE
CICLO DI VITA DEL DISPOSITIVO
SUPPORTO PER IL CICLO DI VITA
QUALE PERCORSO?

Valore a lungo termine

AXIS OS mantiene un valore prevedibile durante l'intero ciclo di vita dei dispositivi. Un'architettura stabile e solida riduce al minimo i tempi di inattività.

Forniamo aggiornamenti software, comprensivi di nuove funzionalità, per molti anni. Grazie a un'ampia documentazione, strumenti utili e interfacce intuitive, i dispositivi Axis sono facili da usare e mantenere. Inoltre offriamo piani di aggiornamento trasparenti e affidabili per consentirti di programmare la manutenzione in base alle esigenze della tua azienda.

Le seguenti pagine offrono maggiori informazioni sulla qualità del software Axis, sulla gestione del ciclo di vita di AXIS OS e sul supporto software.

Un software sempre affidabile

Per noi la qualità di AXIS OS è importante. Con circa 900 sviluppatori e 4000 commit di codice al giorno nel branch principale di AXIS OS, il nostro sistema operativo è in continua trasformazione per adattarsi alle esigenze del mercato. Gestire due build al giorno per ciascuno degli oltre 200 prodotti significa occuparsi di ben 182.500 build all'anno, consentendo test iterativi e offrendo un valore aggiunto.

Test rigorosi
Anche mantenere la stabilità del software richiede test rigorosi. Ogni giorno, infatti, i nostri sistemi eseguono ben 4 milioni di casi di test diversi. A questi si aggiungono oltre 4000 commit di codice al giorno per correggere le vulnerabilità e migliorare la qualità. Il totale è oltre un miliardo di test e più di un milione di commit di codice all'anno. Inoltre consentiamo a clienti e partner di dare un feedback diretto su AXIS OS tramite la condivisione dei dati.

Miglioramento continuo
AXIS OS non è statico. È dinamico perché viene ottimizzato costantemente. Con aggiornamenti e miglioramenti regolari, i dispositivi Axis che seguono il percorso Active di AXIS OS si evolvono di pari passo con i progressi tecnologici. In altre parole, il prodotto acquistato oggi acquisirà nuove funzionalità e diventerà ancora più utile nel corso della sua vita.

Supportare il ciclo di vita del dispositivo

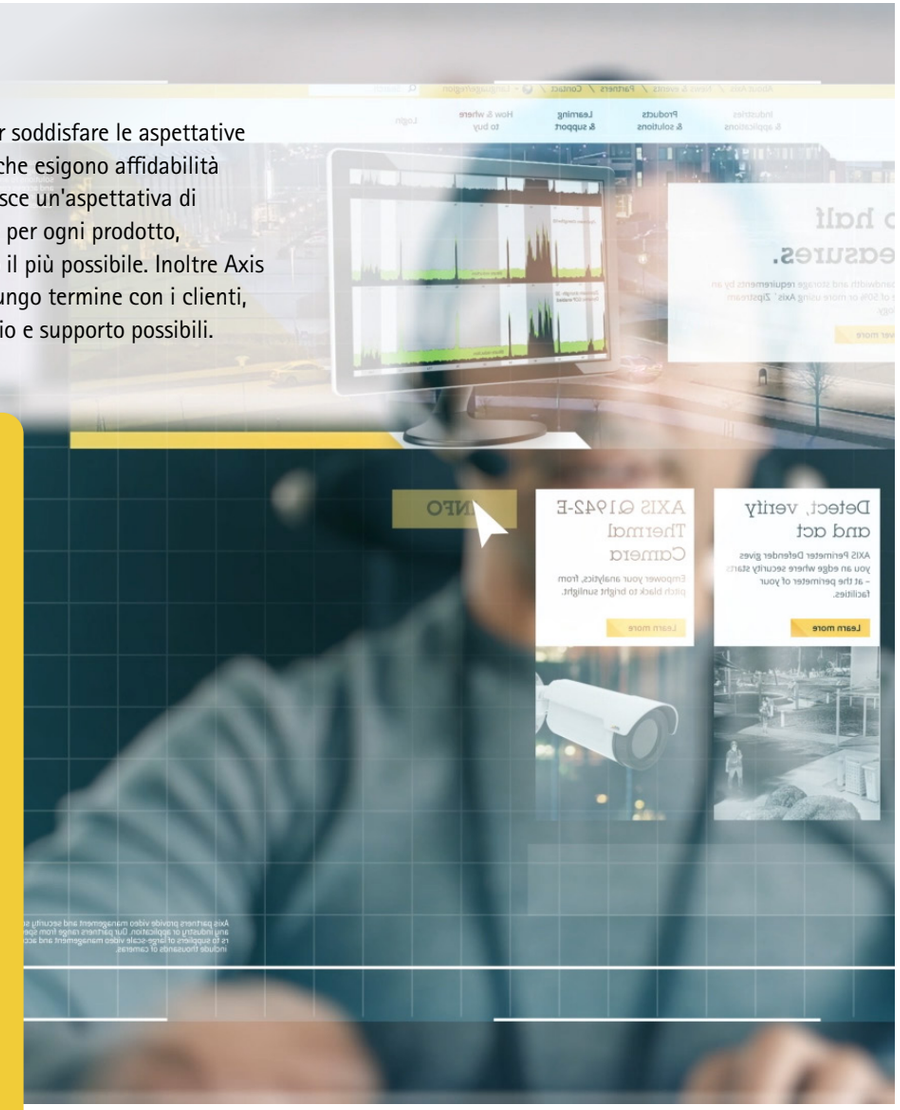
Uno dei vantaggi di AXIS OS è che supporta il ciclo di vita dei dispositivi, dall'installazione alla manutenzione fino alla sostituzione. AXIS OS offre strumenti e risorse che aiutano a gestire e ottimizzare i dispositivi Axis per tutta la loro durata.

Installazione e configurazione semplici
AXIS OS semplifica l'installazione e la configurazione dei dispositivi fornendo procedure guidate, modelli e profili che guidano l'utente in ogni processo. Puoi anche utilizzare AXIS Device Manager (ADM) e AXIS Device Manager Extend (ADMX) per installare e configurare più dispositivi contemporaneamente, risparmiando tempo e fatica.

Monitoraggio e diagnostica continui
Con il tuo consenso, AXIS OS monitora e analizza le prestazioni e lo stato dei dispositivi Axis raccogliendo dati sotto forma di registri, report e avvisi. In questo modo è più facile identificare e risolvere qualsiasi problema e il software può essere migliorato versione dopo versione.

Supporto e compatibilità a lungo termine
AXIS OS offre un supporto a lungo termine per i dispositivi Axis con periodici patch di sicurezza e correzioni di bug. Non perdiamo mai di vista la compatibilità dei dispositivi e delle applicazioni Axis, riducendo al minimo modifiche e interruzioni. In genere, i dispositivi basati su AXIS OS hanno una durata di circa 10 anni o più e in alcuni casi sono supportati fino a 13 anni.

Affidabilità e impegno
AXIS OS è progettato per soddisfare le aspettative e le esigenze dei clienti che esigono affidabilità e qualità. AXIS OS definisce un'aspettativa di vita chiara e trasparente per ogni prodotto, mantenendolo operativo il più possibile. Inoltre Axis instaura un rapporto a lungo termine con i clienti, offrendo il miglior servizio e supporto possibili.



Versione beta di AXIS OS

La versione beta di AXIS OS è vantaggiosa per gli sviluppatori e gli integratori che desiderano testarne e valutarne le funzionalità prima che vengano distribuite ufficialmente. È possibile utilizzare AXIS OS beta per eseguire test di compatibilità preventivi su dispositivi selezionati, verificare i futuri aggiornamenti di sicurezza e accedere alle prossime funzionalità.

Ecco alcuni dei vantaggi della versione beta di AXIS OS. Come utente potrai:

> Avere un'anteprima delle caratteristiche e delle funzionalità ottimizzate che AXIS OS offrirà in futuro, come analitiche edge, connettività IoT e modularizzazione della piattaforma.

> Dare feedback e suggerimenti e suggerimenti che aiutano Axis a definire lo sviluppo e i miglioramenti di AXIS OS.

> Preparare e adattare le applicazioni e i sistemi alle modifiche e ai prossimi aggiornamenti di AXIS OS per evitare potenziali problemi.

Per saperne di più sulla versione beta di AXIS OS, clicca qui.

Supporto software per il ciclo di vita di AXIS OS

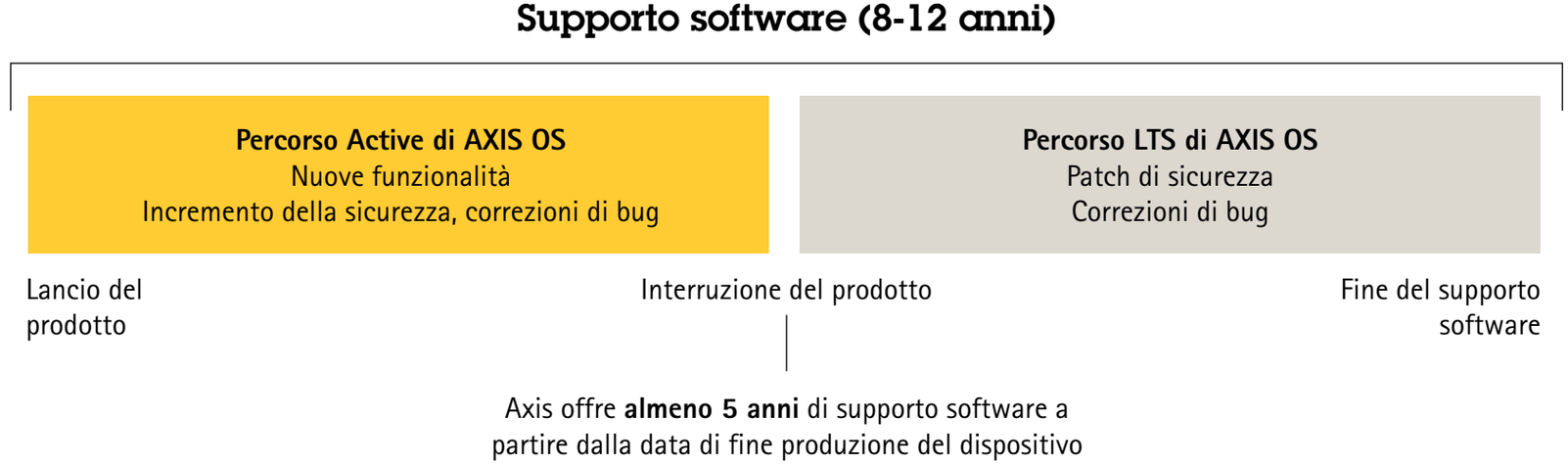
Durante il ciclo di vita di AXIS OS, il supporto segue percorsi diversi: i principali sono i percorsi Active e LTS (Long-Term Support). Esistono anche percorsi di supporto specifici per prodotto (PSS) basati sul ciclo di vita dei singoli dispositivi.

La durata minima di un dispositivo Axis supera gli standard del settore. Una garanzia hardware di ben 5 anni è affiancata dal supporto software di AXIS OS per molti anni. La maggior parte dei dispositivi ha una durata di AXIS OS di ben 8-12 anni.

Ecco come funziona:

1. Quando Axis lancia un nuovo dispositivo è disponibile solo il percorso Active di AXIS OS. Nel periodo iniziale successivo ricevi aggiornamenti e miglioramenti continui, comprese le nuove funzionalità.
2. Il percorso LTS (Long-Term Support) diventa disponibile in alternativa al percorso Active entro due anni dal lancio del dispositivo. A questo punto puoi scegliere il percorso Active o il percorso LTS. I dispositivi che seguono il percorso LTS sono supportati solo con patch e correzioni di bug.
3. Quando un dispositivo esce dalla produzione, da due a quattro anni dopo viene interrotto anche il percorso Active. A questo punto, tutti i dispositivi passano automaticamente al percorso LTS e sono supportati con patch e correzioni di bug per almeno 5 anni.

Supporto software per il ciclo di vita di AXIS OS



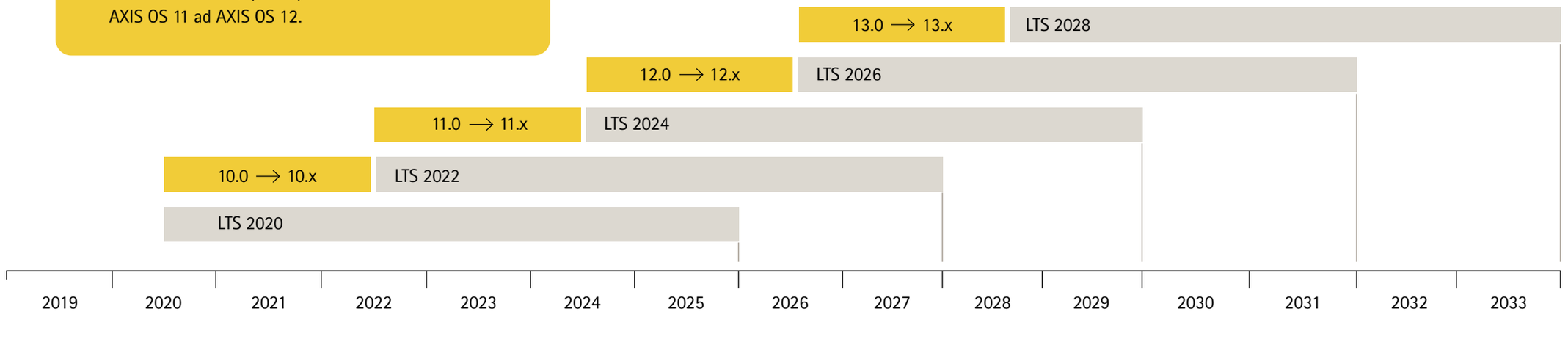
Quale percorso di supporto è più adatto a te?

Una volta disponibili sia il percorso Active che il percorso LTS, i clienti possono scegliere quello più adatto alle loro esigenze con l'assistenza di Axis.

Percorso Active
Il percorso Active offre il numero massimo di aggiornamenti e nuove funzionalità per AXIS OS. Pensato su misura per i clienti che vogliono accedere subito alle funzionalità e ai miglioramenti più recenti, è l'unico percorso disponibile per i dispositivi appena immessi in commercio. Aiuta gli utenti a rimanere al passo con l'evoluzione dei dispositivi: vengono aggiunte nuove funzionalità di cybersecurity per un uso ancora più sicuro, mentre le funzionalità esistenti ricevono miglioramenti continui. Seguendo il percorso Active di AXIS OS, ottieni di più dai dispositivi senza costi supplementari anche diversi anni dopo l'acquisto. Se non hai problemi di compatibilità, questo è il percorso che fa per te fin quando è disponibile.

Percorso LTS (Long-Term Support)
Se cerchi coerenza e compatibilità per le API ti consigliamo di scegliere il percorso LTS (Long-Term Support) appena è disponibile. Il percorso LTS è incentrato sulla compatibilità con le versioni precedenti e fornisce regolarmente patch di sicurezza e correzioni di bug. Anziché offrire nuove funzionalità di sicurezza, mantiene la cybersecurity. Allo stesso modo, per quanto riguarda le funzionalità dei dispositivi, non ne aggiunge di nuove ma riduce al minimo le modifiche per evitare interruzioni. Il percorso LTS è adatto ai clienti che privilegiano l'affidabilità e la qualità e desiderano un sistema di terze parti ben integrato. Ogni percorso LTS è supportato per 5 anni e distribuito ogni 24 mesi, in base alla distribuzione regolare di un percorso Active. Tutti i dispositivi passano automaticamente al percorso LTS quando escono di produzione.

La figura mostra il percorso Active di AXIS OS accanto ai percorsi LTS introdotti nel corso degli anni. Ogni 24 mesi circa viene creato un nuovo percorso LTS e la versione principale di AXIS OS viene incrementata. Ad esempio, nel 2024 creeremo il nuovo percorso AXIS OS LTS 2024, quindi passeremo dall'attuale AXIS OS 11 ad AXIS OS 12.



ASDM
CYBER SECURITY INTRINSECA
GESTIONE DELLE VULNERABILITÀ
ALL-IN-ONE

Focus sulla cybersecurity

AXIS OS aderisce all'approccio Security by Design. Il nostro ASDM (Axis Security Development Model) definisce processi e strumenti che riducono il rischio di vulnerabilità durante lo sviluppo del software e non solo.

Axis Edge Vault, la nostra piattaforma di cybersecurity basata su hardware, garantisce un avvio sicuro e un ambiente protetto da manomissioni per l'archiviazione delle chiavi crittografiche caricate dal cliente. Il software principale di AXIS OS è costituito da componenti open source testati accuratamente. Inoltre, ogni versione è accompagnata da una distinta base del software (SBOM) per attestare che AXIS OS è aggiornato e protetto da patch per le vulnerabilità note.

AXIS OS è anche conforme e certificato secondo la norma ETSI EN 303 645, dedicata specificamente alla sicurezza dei dispositivi edge. La conformità FIPS 140 garantisce che AXIS OS rispetti i più recenti standard crittografici definiti dal National Institute of Standards and Technologies (NIST). Infine, in qualità di CVE Numbering Authority approvata, seguiamo le best practice per identificare, gestire e divulgare le vulnerabilità.

Le seguenti pagine offrono ulteriori informazioni su ASDM, Axis Edge Vault, la gestione delle vulnerabilità e il concetto di sicurezza unificata.

Sviluppato pensando alla sicurezza

L'Axis Security Development Model (ASDM) integra con efficacia la cybersecurity nel ciclo di sviluppo del software, descrivendo le attività di sicurezza da tenere in considerazione nelle le varie fasi. Lo scopo è ridurre le vulnerabilità – nonché i costi di sviluppo – stabilendo una base di riferimento per la cybersecurity e fornendo linee guida.

ASDM: made in Axis
L'Axis Security Development Model non è un framework standard "pronto all'uso". Al contrario, abbiamo esaminato molti standard e framework di cybersecurity come ISO 27001, IEC 62443, NIST, BSIMM e CMMC. Il filo conduttore è uno: la sicurezza deve essere incorporata in tutte le fasi di sviluppo. A partire da questo abbiamo adattato il modello alla nostra cultura aziendale, alle procedure di sviluppo e al tipo di prodotti che offriamo.

Toolbox ASDM
Il toolbox ASDM prescrive una serie di attività per contrastare diversi problemi di sicurezza. Alcuni esempi sono la valutazione del rischio, la modellizzazione delle minacce, i test del modello di minaccia, l'analisi statica del codice, la scansione delle vulnerabilità e la valutazione dei fornitori. I team di sviluppo scelgono in quali attività impegnarsi in base al tipo di software da sviluppare. L'obiettivo è una maggiore cybersecurity, più che la semplice conformità a un processo.

Un vantaggio in più: le competenze esterne
La maggior parte del pesante lavoro di sviluppo viene svolto dal reparto R&S e dagli ingegneri software Axis. Tuttavia riconosciamo che possiamo anche trarre vantaggio dalla conoscenza e dall'esperienza degli altri: ecco perché per i penetration test ci affidiamo ad aziende specializzate. Inoltre abbiamo organizzato il programma bug bounty di AXIS OS, che offre un premio in denaro ai ricercatori che ci aiutano a identificare le vulnerabilità di sicurezza.

Governance | **Formazione** | **Riunione linea ASDM** | **Valutazione ASDM** | **Conformità e standard di sicurezza**

Requisiti	Progettazione	Installazione	Verifica	Deployment
Valutazione dei rischi	Modellizzazione delle minacce	Analisi statica del codice	Test del modello di minaccia	Gestione delle vulnerabilità
Valutazione fornitori		Analisi della composizione software	Penetration test esterno	Gestione degli incidenti
Privacy dei dati			Scansione delle vulnerabilità	Stato di sicurezza prodotto/soluzione
Valutazione della sicurezza open source			Valutazione della sicurezza interna	Programma bug bounty

Cybersecurity incorporata

Protezione dall'interno all'esterno
Axis Edge Vault è la nostra piattaforma di cybersecurity basata su hardware. Costituisce una solida base per garantire che i dispositivi Axis siano un elemento affidabile della rete, ma sarebbe inutile senza un sistema operativo che ne esprima tutte le potenzialità. AXIS OS utilizza la piattaforma Edge Vault per offrire una maggiore sicurezza in modalità edge per ogni applicazione.

Edge Vault include funzionalità come:

Archiviazione sicura delle chiavi
L'archivio chiavi sicuro utilizza moduli di calcolo crittografico per l'archiviazione in sicurezza e il calcolo delle chiavi crittografiche. Protegge l'identità del dispositivo e altre informazioni sensibili dagli accessi non autorizzati, anche quando il dispositivo è compromesso. I moduli di calcolo crittografico utilizzati sono il Trusted Execution Environment integrato nel System-on-Chip (SoC) e un elemento sicuro dedicato o un Trusted Platform Module (TPM 2.0), che sono chip separati sul circuito stampato (PCB).

Sistema operativo firmato e Secure Boot
Il sistema operativo è firmato, ovvero l'immagine del software del dispositivo è firmata in codice. Insieme, il sistema operativo firmato e Secure Boot consentono ai dispositivi di scaricare ed eseguire solo versioni originali di AXIS OS. Questi accorgimenti aggiungono un ulteriore livello di protezione dalle manomissioni nelle catene di fornitura del software e dell'hardware.

ID dispositivo Axis
L'ID dispositivo Axis è conforme allo standard IEEE 802.1AR e consente l'identificazione e l'onboarding sicuri dei dispositivi in rete. Funziona come un vero e proprio passaporto per ogni dispositivo Axis prodotto.

File system criptato
La crittografia del file system protegge i dati dall'estrazione o dalla manomissione mentre il dispositivo non è in uso, ad esempio durante il transito dal system integrator al cliente finale.

Video con firma
Il video con firma consente agli utenti di verificare l'autenticità delle immagini acquisite, garantendo anche che non siano state manomesse.

Piattaforma di cybersecurity Axis Edge Vault

Moduli di calcolo crittografico	Funzionalità	Applicazioni
Secure Element TPM 2.0 Sicurezza del SoC (TEE)	Secure Boot SO firmato ID dispositivo Axis Archivio chiavi sicuro (keystore) Video con firma File system criptato	Identità del dispositivo attendibile Archiviazione sicura delle chiavi Rilevamento di manomissioni nel video Protezione della catena di fornitura

*Nota: le funzionalità di Axis Edge Vault non sono supportate da tutti i dispositivi. Consultare la scheda tecnica o il selettore prodotti Axis per verificare le funzionalità supportate da dispositivi specifici.

Gestione delle vulnerabilità

Per ridurre al minimo il rischio di esposizione dei nostri clienti seguiamo le best practice del settore per gestire e risolvere le vulnerabilità in modo trasparente.

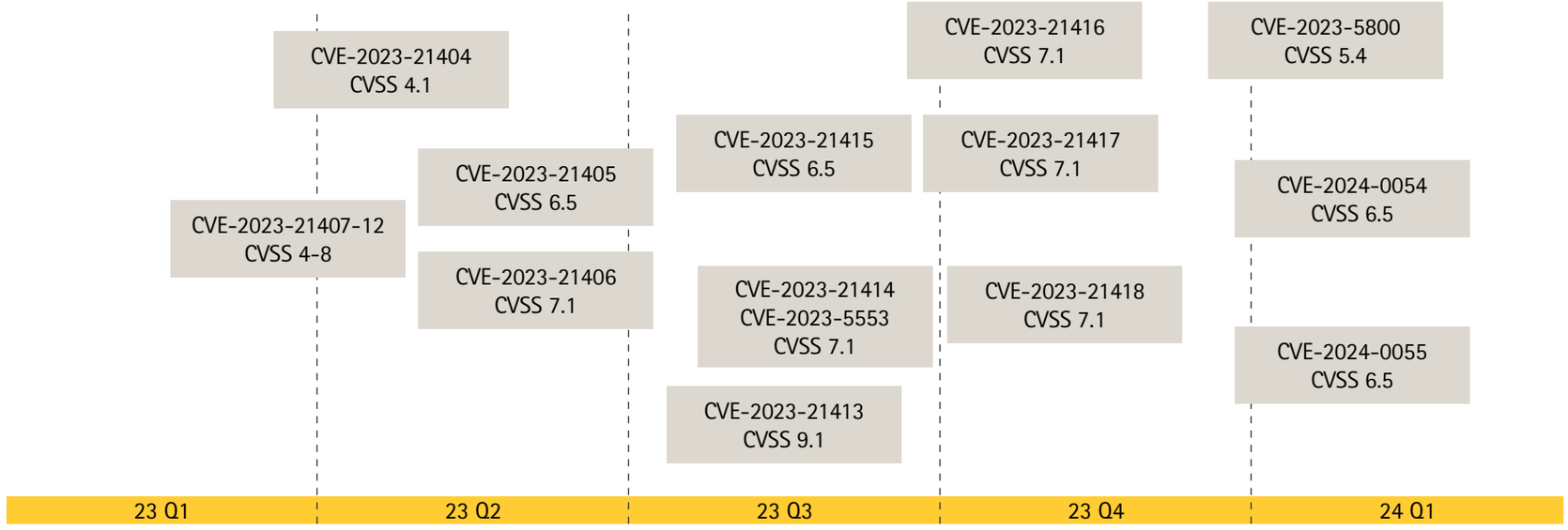
Altissimo livello di gestione delle vulnerabilità
Non esiste alcun modo per garantire che i prodotti e i servizi forniti da Axis siano totalmente esenti da vulnerabilità. Questa condizione non riguarda solo noi, ma tutti i software e i servizi. Tuttavia, ogni reparto si impegna a identificare e attenuare le potenziali vulnerabilità in ogni fase, riducendo i rischi che si corrono quando i dispositivi e i servizi Axis vengono utilizzati negli ambienti dei clienti.

CVE Numbering Authority
Axis è stata nominata CVE Numbering Authority (CNA), ovvero aderisce al programma CVE per collaborare con aziende che la pensano allo stesso modo e vogliono migliorare la gestione delle vulnerabilità. Il modo in cui gestiamo, divulghiamo e risolviamo le vulnerabilità è in linea con il framework internazionale di questa organizzazione no profit e con la nostra politica di gestione pubblica delle vulnerabilità.

Gestione trasparente e affidabile
Axis usa il noto sistema CVSS (Common Vulnerability Scoring System) per classificare le vulnerabilità relative al codice sviluppato da Axis o al codice open source di terze parti. Valutiamo le vulnerabilità del codice open source in base alla loro rilevanza per i prodotti quando si applicano le best practice raccomandate. È possibile iscriversi ad Axis Security Notification Service per ricevere informazioni sulle vulnerabilità e altre questioni relative alla sicurezza dei prodotti Axis.

Partnership con ricercatori e organizzazioni nel campo della sicurezza
Apprezziamo molto il lavoro dei ricercatori e delle organizzazioni di ricerca sulla sicurezza, che ci contattano per segnalare eventuali vulnerabilità e le loro conseguenze. Una volta a conoscenza di un problema non esitiamo a divulgarlo pubblicamente e ad applicare le patch correttive. L'importante è gestire le vulnerabilità in modo corretto e trasparente, con un processo di divulgazione etico e responsabile indipendentemente da come la vulnerabilità sia stata individuata

Vulnerabilità di AXIS OS



Vulnerabilità divulgate da Axis per AXIS OS.

Sicurezza all-in-one

Sui dispositivi di rete basati su AXIS OS i componenti hardware e software lavorano in sinergia per consentire ai clienti di utilizzare in sicurezza i dispositivi, i relativi servizi e i sistemi a cui sono connessi. Una protezione totale a livelli inizia da solide fondamenta e da una piattaforma di sicurezza basata su hardware, per proseguire fino al software. I dispositivi basati su AXIS OS sono protetti da questo approccio alla cybersecurity, che aumenta la sicurezza complessiva di dati, applicazioni e processi.

Avrai dunque la certezza che, indipendentemente da come usi un dispositivo Axis, sarà protetto e comunicherà in totale sicurezza, consentendo un'integrazione corretta nei sistemi di terze parti.

Controllo accessi

Gestione del controllo accessi
Gestione del dispositivo dell'utente locale con indicatore di complessità della password
La gestione federata dei dispositivi degli utenti tramite OpenID Connect (RFC6749, 1.3.1 Codice di autorizzazione) fornisce l'integrazione ADFS per offrire funzionalità come l'applicazione di password complesse, la rotazione delle password, il blocco automatico degli account, l'autenticazione multifattore (MFA) e la funzionalità di gestione dei diritti dell'utente tramite Microsoft AD

Privacy
Utilizzo dei dati diagnostici
Approccio minimalista alla quantità di dati specifici del cliente da archiviare

Applicazione

Sicurezza delle applicazioni
Sicurezza delle applicazioni basata su TLS (MQTT, SFTP, NTS, HTTPS, WebRTC)
Streaming video crittografato (RTSPS/SRTP, HTTPS), Remote Syslog sicuro

Sistema operativo

Crittografia e protezione dei dati
OpenSSL 1.1.1 e 3.0
PKI con certificati X.509 e crittografia
Transport Layer Security (TLS 1.2/TLS 1.3)
Crittografia delle schede SD (AES-XTS-Plain64 256 bit)
File system crittografato (AES-XTS-Plain64 256 bit), Video con firma

Sicurezza predefinita
HTTPS abilitato di default
Brute-Force Delay Protection
Firewall basato su host
Network Time Security (NTS)
Versioni TLS non sicure disabilitate
Porta UART/Debug disabilitata

Sicurezza della rete aziendale
IEEE 802.1X (controllo di accesso alla rete)
IEEE 802.1AR (identità dispositivo sicura)
IEEE 802.1AE (sicurezza MAC, MACsec)

Sistema operativo AXIS OS
Sistema operativo comune basato su Linux con oltre il 95% di componenti software open source standard nel settore, come OpenSSL, Apache, Curl e altri.
Percorso Active per l'ampliamento delle funzionalità e percorsi LTS (Long-Term Support) di 5 anni per l'integrazione con sistemi di terze parti e compatibilità con le versioni precedenti.

Silicon Assisted Security (chip)

Radice di attendibilità hardware
Sicurezza per System-on-Chip (SoC) basati su ARM
Ambiente di esecuzione affidabile (TEE/OP-TEE)
Trusted Platform Module (TPM 2.0), Secure Element

Archiviazione sicura delle chiavi
Archiviazione e funzionamento protetti dalla manomissione delle chiavi crittografiche, come chiavi private caricate dal cliente, chiavi di firma video e ID del dispositivo Axis.

Fondamenta di sicurezza

Axis Security Development Model
Axis Security Development Model (ASDM)
Penetration test esterni
Programma bug bounty con Bugcrowd
Software Bill of Material (SBOM)

Compliance
Common Criteria EAL
FIPS 140
ETSI EN 303 645

Identità del dispositivo attendibile
Piattaforma di cybersecurity Axis Edge Vault
Secure Boot con sistema operativo firmato (firma del codice)
ID dispositivo Axis (IEEE 802.1AR)

Integrazione perfetta

L'integrazione ha un ruolo fondamentale per i prodotti Axis. Ci impegniamo a creare API solide e coerenti che si integrino facilmente in un'ampia gamma di applicazioni.

In questo modo puoi creare soluzioni complete che sfruttano tutte le funzionalità dei tuoi dispositivi Axis.

Nelle seguenti pagine troverai ulteriori informazioni su VAPIX (la nostra API), sul nostro lavoro con ONVIF e l'IoT, sulla modularizzazione della piattaforma con ACAP e sull'automazione per l'integrazione in rete.

I vantaggi di Axis nell'integrazione: VAPIX, ONVIF, IoT e cloud

In un mondo dinamico come quello della sorveglianza e della connettività, Axis Communications offre una suite di soluzioni per l'integrazione che ridefiniscono gli standard del settore.

VAPIX: una tradizione di estensibilità
VAPIX, il nostro framework API aperto, sottolinea il nostro impegno verso l'innovazione. Supportando le richieste HTTP GET e POST, insieme ai formati JSON e XML, consente agli sviluppatori di creare facilmente soluzioni su misura. Con la libreria più ampia e coerente sul mercato, VAPIX è pioniera nell'integrazione aperta dei dispositivi di rete Axis ed è addirittura precedente a ONVIF.

ONVIF: standard di settore collaborativi
Axis collabora con il forum aperto ONVIF per promuovere uno spirito di collaborazione che porti avanti il settore e fornisca agli utenti soluzioni complete e interoperabili. ONVIF fornisce e promuove interfacce standardizzate per un'interoperabilità efficace dei dispositivi di sicurezza fisica basati su IP. Questo semplifica l'integrazione per i nostri partner, garantendo che i dispositivi Axis si adattino perfettamente a una vasta gamma di sistemi.

IoT: abbracciare il futuro
Mentre l'Internet of Things (IoT) ridisegna la connettività, i dispositivi Axis contribuiscono a un ecosistema in continua evoluzione. Axis supporta protocolli come MQTT che si allineano con le innovazioni dell'IoT. Con Axis, i tuoi dispositivi non sono solo connessi, ma fanno parte di un fiorente panorama come quello dell'IoT.

Integrazione cloud: innovazione oltre le nuvole
Nel campo della connettività digitale Axis sta esplorando l'integrazione cloud con API progettate per un'interazione fluida con le principali piattaforme, come Microsoft Azure e Amazon Web Services (AWS). Con l'evolversi della tecnologia supporteremo più tecnologie cloud, come MQTT per i servizi di messaggistica e WebRTC per lo streaming video e audio. L'obiettivo è consentire agli utenti di sfruttare al meglio la tecnologia cloud.

Modularizzazione della piattaforma tramite ACAP

Una delle principali caratteristiche di AXIS OS è che consente la modularizzazione della piattaforma tramite AXIS Camera Application Platform (ACAP). ACAP è un framework che permette agli sviluppatori di creare e distribuire applicazioni e servizi, come analitiche video, analitiche audio e altre estensioni personalizzate per requisiti aziendali specifici. Le applicazioni ACAP sono indipendenti dalle funzionalità principali di AXIS OS e possono essere installate, aggiornate e rimosse senza influire sul resto del sistema. Le applicazioni ACAP possono anche comunicare tra loro e con sistemi esterni utilizzando protocolli e API standard.

Scalabilità e prestazioni
ACAP utilizza l'architettura a microservizi del sistema operativo sui dispositivi Axis. Ogni servizio può essere ampliato o ridotto in modo indipendente in base alla domanda e al carico di lavoro. In questo modo migliorano le prestazioni complessive e la disponibilità del sistema, per un uso e un'allocazione efficienti delle risorse.

Adattabilità e personalizzazione
Con ACAP, i dispositivi Axis sono più versatili, adattabili e personalizzabili perché supportano diversi tipi di integrazioni, analitiche e dispositivi. Inoltre, ACAP riduce l'interdipendenza e aumenta la coesione della piattaforma perché ciascuna applicazione è accoppiata liberamente ad AXIS OS ed è altamente coesa al suo interno.

Manutenibilità e affidabilità
Ogni servizio può essere testato, monitorato e sottoposto a debug in modo indipendente e isolato. Ciò semplifica la risoluzione dei problemi e la diagnostica, migliorando la resilienza e la tolleranza del sistema ai guasti, e fa spiccare AXIS OS per la qualità del software.

AXIS OS per i team IT

Un'automazione e un'integrazione corrette nell'infrastruttura IT garantiscono controlli di sicurezza adeguati e possono far risparmiare tempo e denaro. Le complessità del sistema superflue sono ridotte al minimo. La combinazione di dispositivi e software Axis integrati nell'infrastruttura IT aziendale offre diversi vantaggi. Ad esempio puoi:

> Ridurre al minimo la complessità del sistema rimuovendo le reti di staging dedicate ai dispositivi fisici.

> Risparmiare sui costi aggiungendo processi automatici di onboarding e gestione dei dispositivi

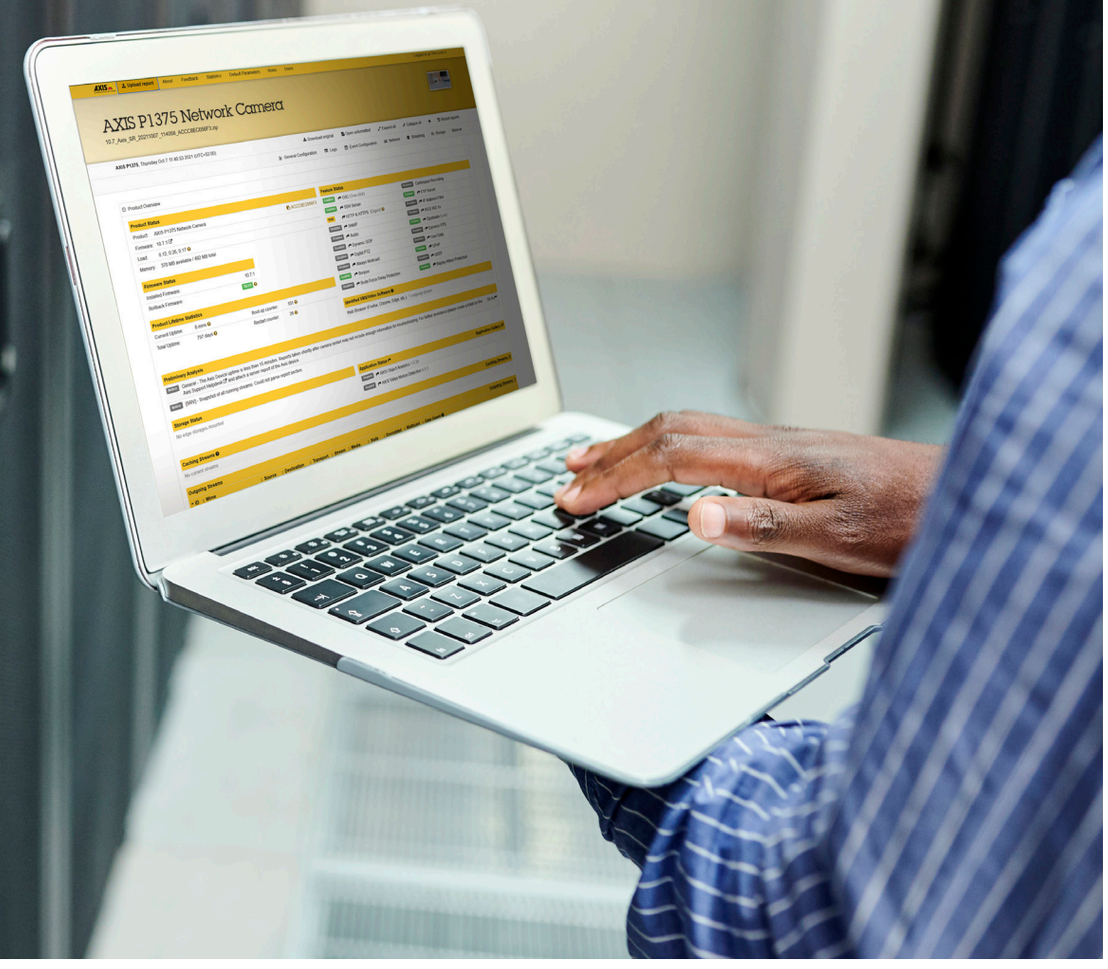
> Sfruttare i controlli di sicurezza di rete Zero Trust come IEEE 802.1X, IEEE 802.1AR

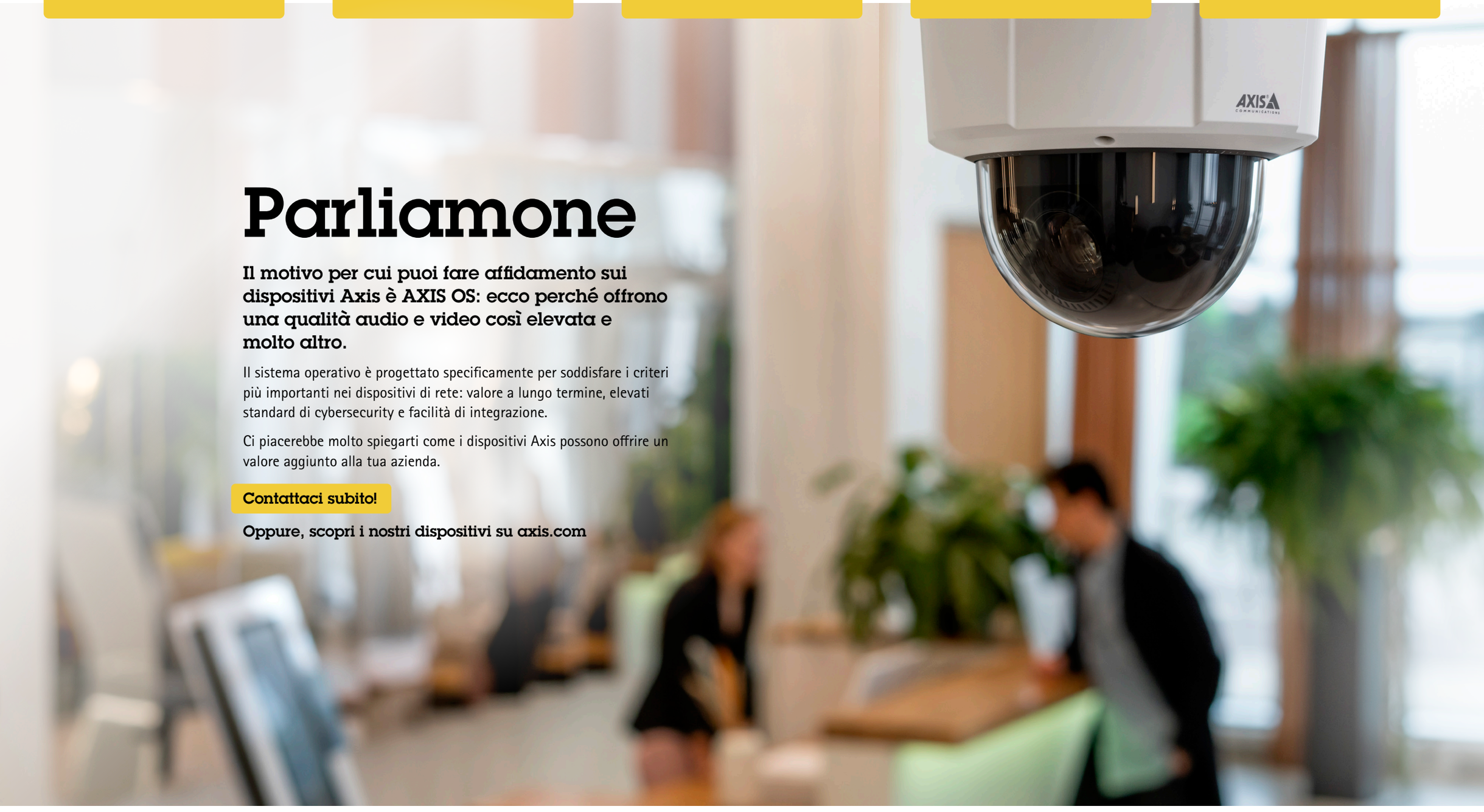
> Aumentare la sicurezza complessiva della rete introducendo la crittografia dei dati a livello fondamentale con l'aiuto di IEEE 802.1AE MACsec. Dunque, è lo stesso dispositivo Axis a contribuire alla sicurezza della rete.

> Monitorare il dispositivo Axis tramite protocolli standardizzati come Remote Syslog, per consentire ad esempio il monitoraggio dei registri e dello stato.

Reti sicure basate sui principi Zero Trust
Creare reti convergenti e sicure basate sui principi Zero Trust è fondamentale per eliminare i sistemi isolati che operano da soli. Una maggiore sicurezza, minori costi di configurazione e manutenzione e un'applicazione più orientata alle policy IT sono possibili integrando i dispositivi Axis nell'infrastruttura IT aziendale tramite protocolli e standard di rete aperti e ben definiti.

Un vantaggio per i reparti IT
I reparti IT hanno il compito di proteggere la rete ed è proprio per questo che i dispositivi Axis sono vantaggiosi. I nostri dispositivi sono più facili da integrare, mantenere e utilizzare grazie alla loro versatilità e alla somiglianza con le soluzioni IT definite da protocolli di rete IEEE e IETF aperti e standardizzati, oltre che a una progettazione condivisa. I dispositivi Axis sono come "cittadini fidati" nelle reti dei clienti, contribuendo a incrementare la sicurezza.





Parliamone

Il motivo per cui puoi fare affidamento sui dispositivi Axis è AXIS OS: ecco perché offrono una qualità audio e video così elevata e molto altro.

Il sistema operativo è progettato specificamente per soddisfare i criteri più importanti nei dispositivi di rete: valore a lungo termine, elevati standard di cybersecurity e facilità di integrazione.

Ci piacerebbe molto spiegarti come i dispositivi Axis possono offrire un valore aggiunto alla tua azienda.

Contattaci subito!

Oppure, scopri i nostri dispositivi su axis.com

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro grazie a soluzioni che migliorano la sicurezza e le prestazioni aziendali. In qualità di azienda leader nelle tecnologie di rete, Axis offre prodotti e servizi per la videosorveglianza, il controllo accessi, intercom e sistemi audio, che supporta con applicazioni analitiche intelligenti e una formazione di alta qualità.

Axis ha oltre 4000 dipendenti in più di 50 paesi e collabora con partner tecnologici e integratori di sistemi in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.