O poder de uma única plataforma

Desenvolvida para valor a longo prazo, segurança cibernética e integração

AXIS COMMUNICATIONS

Potencializando seus dispositivos em rede Axis

O AXIS OS é o sistema operacional baseado em Linux usado na maioria dos nossos dispositivos em rede Axis. Ele é o coração de mais de 200 produtos Axis e de dezenas de milhares de dispositivos implantados nos sites dos clientes. O Axis OS reflete um compromisso com a inovação, a confiabilidade e a integração perfeita. O software Axis é a razão de nossos dispositivos serem tão confiáveis e de fornecerem uma qualidade da imagem tão boa. E a cada versão, nós o aprimoramos mais. Na verdade, 80% de nossa pesquisa e desenvolvimento gira em torno do desenvolvimento de software.

Sempre adicionamos novos recursos e aprimoramos os recursos existentes. Reforçamos continuamente a segurança por meio da correção de vulnerabilidades dos dispositivos baseados no AXIS OS, tornando-os melhores e permitindo que mais casos de uso sejam resolvidos com mais segurança.

O AXIS OS foi desenvolvido especificamente para atender aos critérios mais importantes para dispositivos em rede: valor a longo prazo, normas de segurança cibernética e facilidade de integração.

Desenvolvido para dispositivos Axis
Criado pela organização de desenvolvimento AXIS OS e baseado na estabilidade do Linux Yocto OpenEmbedded, o AXIS OS supera configurações genéricas por ser perfeitamente otimizado para as demandas exclusivas dos dispositivos de borda Axis, como câmeras, alto-falantes e equipamento de controle de acesso.

Valor a longo prazo
O AXIS OS garante que seus dispositivos estejam sempre funcionando. Projetado para operar sem interrupções, ele oferece desempenho consistente e responsivo em alinhamento com as demandas dos seus aplicativos a longo prazo, seja de dia ou à noite.

Segurança cibernética robusta
A essência do AXIS OS é a dedicação à segurança cibernética. O AXIS OS, com arquitetura de segurança incorporada, ajuda você a proteger seus dispositivos. Por meio das práticas de desenvolvimento de software e de gerenciamento vigilante de vulnerabilidades, o AXIS OS garante que seus dados e dispositivos permaneçam resilientes contra ameaças emergentes.

Integração perfeita
O AXIS OS incorpora VAPIX e ONVIF, entre outros, que ajudam os dispositivos em rede Axis a se integrarem facilmente em vários ecossistemas. A capacidade de integração fornece uma experiência tranquila e interconectada para usuários e desenvolvedores.

O AXIS OS em números

900 desenvolvedores

24.000.000 de linhas de código escritas

4000 confirmações de código diariamente

4.000.000 de testes automatizados diariamente

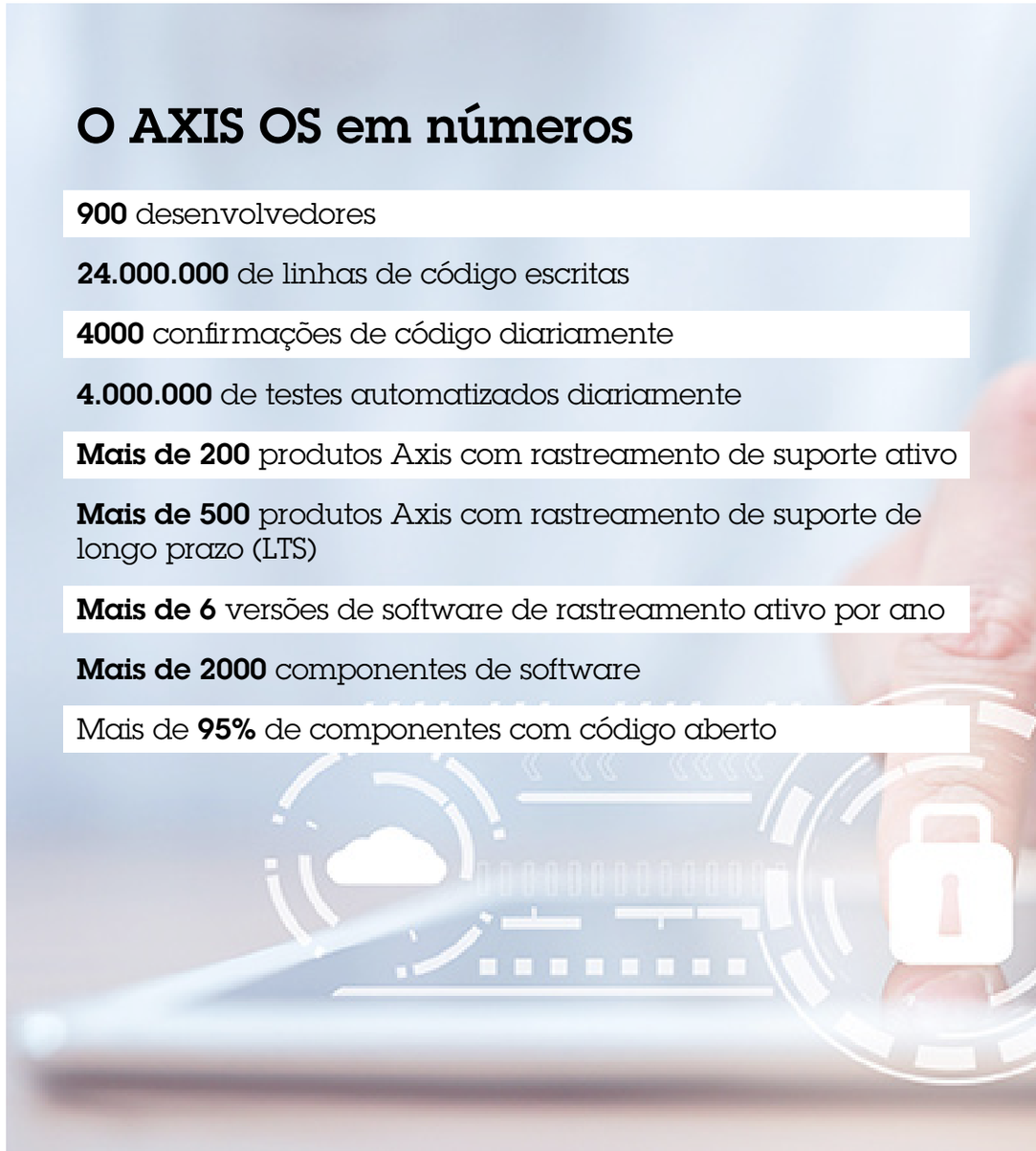
Mais de 200 produtos Axis com rastreamento de suporte ativo

Mais de 500 produtos Axis com rastreamento de suporte de longo prazo (LTS)

Mais de 6 versões de software de rastreamento ativo por ano

Mais de 2000 componentes de software

Mais de **95%** de componentes com código aberto



Desenvolvido para dispositivos Axis

Quando projetamos o AXIS OS, nos concentramos especificamente em desempenho, integração, segurança e qualidade de software para dispositivos de borda.

Baseado na estabilidade do Linux Yocto OpenEmbedded, o AXIS OS fornece uma plataforma unificada para todos os seus dispositivos em rede Axis, oferecendo uma experiência consistente em uma variedade de produtos.

Nas páginas a seguir, você poderá ler mais sobre o valor de um sistema operacional criado especificamente para dispositivos de borda e sobre o poder de uma plataforma.

Criada para excelência na borda

Em um cenário dominado por soluções polivalentes, o AXIS OS não é apenas mais um sistema operacional Linux. Ele transcende as convenções das configurações genéricas do Linux para fornecer uma solução ajustada às necessidades específicas dos dispositivos de borda. Essa especialização oferece suporte ao desempenho, a confiabilidade e a segurança exclusivos dos produtos Axis.

Base Linux Yocto
A base robusta do Linux Yocto OpenEmbedded garante estabilidade e eficiência. O Linux Yocto OpenEmbedded também fornece um ambiente familiar para desenvolvedores. Ele fornece a base para o bom funcionamento dos dispositivos em rede Axis.

Flexibilidade do chipset
Versatilidade define o AXIS OS. Ele fornece suporte dedicado ao chipset Axis ARTPEC na maioria dos dispositivos Axis, além de também ser compatível com chips de terceiros. Por isso, uma variedade de dispositivos em rede são beneficiados pelo poder do AXIS OS.

Projetado para valor a longo prazo
Esperamos que nossos dispositivos sejam resistentes e funcionem por anos. Por isso, o AXIS OS é feito para ser robusto e sustentável. Também somos transparentes sobre a expectativa de vida de nossos dispositivos. Essas informações estão em axis.com.

Testes rigorosos para a finalidade
O AXIS OS é submetido a rigorosos testes para garantir que ele se supere na finalidade a que se destina. Nós o testamos cuidadosamente, porque queremos que ele supere as expectativas de desempenho, segurança cibernética e integração.

Qualidade do software
O AXIS OS é um testemunho de qualidade de software rigorosa. O sistema operacional é projetado mantendo o compromisso com altos padrões para uma experiência de usuário familiar, confiável e segura por toda a vida útil prolongada dos dispositivos Axis.

O poder de uma única plataforma

Nosso compromisso com a excelência transcende as categorias de produtos e está incorporado ao que chamamos o poder de uma única plataforma. Com suporte para mais de 200 produtos, de câmeras de uso corporal a soluções à prova de explosão, de câmeras PTZ a sirenes e de alto-falantes a interfones, nossa plataforma unificada foi projetada para atender nossos parceiros e clientes.

Consistência em ação
O AXIS OS atende a uma variedade de produtos. Todos os nossos produtos compartilham as mesmas APIs e comportamentos. Uma plataforma garante que integradores e desenvolvedores possam incorporar novos dispositivos Axis em seus sistemas sem drivers complexos e específicos do dispositivo. Isso não só agiliza a integração bem como prepara as soluções para o futuro, permitindo a adoção rápida de novos produtos em um ecossistema Axis em constante expansão. Dessa forma, garantimos uma experiência uniforme para o cliente final. Além da economia de tempo e dinheiro para os desenvolvedores, pois toda a solução de integração opera em todos os dispositivos AXIS OS.

Versatilidade sem complexidade
Falar sobre o poder de uma plataforma é também falar sobre uma única plataforma que permite diversificar sem trazer complexidade. Se estiver integrando uma câmera PTZ em um sistema de monitoramento ou incorporando um alto-falante a uma solução de áudio inteligente, o processo é consistente. Essa versatilidade vai além da compatibilidade para fornecer uma experiência harmoniosa e muitas possibilidades para criar soluções integradas sob medida para necessidades específicas.

Segurança unificada
Em um mundo onde segurança cibernética é primordial, o poder de uma plataforma também está no suporte oferecido a uma solução unificada para todo o espectro de produtos. Manter a segurança não é um problema enfrentado a cada produto. Quando uma vulnerabilidade é identificada e corrigida, a correção é propagada por todos os produtos com suporte. Isso não só simplifica o gerenciamento de segurança, bem como facilita uma resposta rápida e coletiva às ameaças emergentes. Além de economizar tempo e recursos, ainda reforça a resiliência em todo o ecossistema Axis.

Valor a longo prazo

O AXIS OS fornece suporte ao valor previsível durante toda a vida útil dos seus dispositivos. A arquitetura robusta e estável mantém o tempo de inatividade no mínimo.

Fornecemos atualizações de software, incluindo recursos totalmente novos, por muitos anos. Com extensa documentação, ferramentas úteis e interface intuitiva, os dispositivos Axis são fáceis de usar e de manter. Além disso, oferecemos cronogramas de lançamento transparentes e confiáveis, para que você possa planejar a manutenção de acordo com as necessidades da sua organização.

Nas páginas a seguir, você pode ler mais sobre a qualidade do software Axis, o gerenciamento da vida útil e o suporte de software do AXIS OS.

O software em que você pode confiar

A qualidade do AXIS OS é importante para nós. Com aproximadamente 900 desenvolvedores e 4000 confirmações de código na principal ramificação do AXIS OS todos os dias, nosso sistema operacional está em constante transformação para se adaptar às necessidades do mercado. Ajustar duas configurações por dia para cada um de nossos mais de 200 produtos significa que enfrentamos um número impressionante de 182.500 configurações anualmente, permitindo testes iterativos e adição de valor.

Testes rigorosos
Manter a estabilidade do software também requer testes rigorosos. Na verdade, nossos sistemas executam impressionantes 4 milhões de casos de teste variados diariamente. Esses testes são complementados por mais de 4000 confirmações de código para correção de vulnerabilidades e melhora da qualidade. Isso soma mais de 1 bilhão de testes e mais de 1.000.000 de confirmações de código por ano. Também permitimos que clientes e parceiros deem feedback direto sobre o AXIS OS por meio do compartilhamento de dados.

Aprimoramento contínuo
O AXIS OS não é estático. Ele é dinâmico, pois estamos sempre o aprimorando. Por meio de atualizações e aprimoramentos regulares, os dispositivos Axis no rastreamento ativo do AXIS OS evoluem acompanhando os avanços tecnológicos. Isso significa que o produto que você compra hoje ganhará novos recursos e se tornará mais valioso ao longo da vida útil dele.

Oferecer suporte a vida útil do dispositivo

Um dos benefícios de usar o AXIS OS é que ele oferece suporte a vida útil do dispositivo, desde a instalação até a manutenção e substituição. O AXIS OS fornece ferramentas e recursos para ajudar você a gerenciar e otimizar seus dispositivos Axis durante toda a vida útil deles.

Fácil instalação e configuração
O AXIS OS simplifica a instalação e a configuração dos dispositivos Axis ao fornecer assistentes, modelos e perfis para guiar você durante o processo. Você também pode usar o AXIS Device Manager (ADM) e o AXIS Device Manager Extend (ADMX) para instalar e configurar vários dispositivos de uma vez, economizando tempo e esforço.

Monitoramento contínuo e diagnósticos
Com o seu consentimento o AXIS OS monitora e analisa o desempenho e o status dos dispositivos Axis, coletando dados de monitoramento de integridade na forma de registros, relatórios e alertas. Isso o ajuda a identificar e resolver qualquer problema. E permite que aprimoremos nosso software a cada versão.

Suporte de longo prazo e compatibilidade
O AXIS OS fornece suporte de longo prazo para os dispositivos Axis com patches de segurança e correções de bugs. Nosso suporte de longo prazo rastreia a compatibilidade dos dispositivos e aplicativos Axis, minimizando alterações e interrupções. Em geral, os dispositivos que executam o AXIS OS tem uma vida útil de cerca de 10 anos ou mais. Em alguns casos, fornecemos suporte para eles por até 13 anos.

Confiabilidade e compromisso
O AXIS OS é projetado para atender às expectativas e necessidades dos clientes que valorizam a confiança e a qualidade. O AXIS OS define uma expectativa de vida clara e transparente para cada produto e os mantêm sob controle tanto quanto possível. A Axis também mantém relações duradouras por fornecer aos clientes serviços e suporte com a máxima qualidade possível.

AXIS OS beta

O AXIS OS beta é um benefício para os desenvolvedores e integradores que desejam testar e avaliar os recursos e as funcionalidades mais recentes do AXIS OS antes que eles sejam oficialmente lançados. O AXIS OS beta pode ser usado para executar testes iniciais de compatibilidade em dispositivos selecionados, verificar as próximas atualizações de segurança e acessar os próximos recursos.

Alguns dos benefícios de usar o AXIS OS beta é que você:

> Obtém uma pré-visualização dos novos e aprimorados recursos e funcionalidades que o AXIS OS oferecerá, como analíticos de borda, conectividade IoT e modularização de plataforma.

> Pode fornecer feedback e sugestões à Axis que ajudem a moldar o desenvolvimento e o aprimoramento do AXIS OS.

> Pode preparar e adaptar seus aplicativos e sistemas para as próximas alterações e atualizações no AXIS OS, evitando possíveis problemas.

Você pode ler mais sobre o AXIS OS beta aqui.

Suporte de software de vida útil do AXIS OS

O suporte de vida útil do AXIS OS é constituído por vários rastreamentos. O suporte ativo e de longo prazo são os principais rastreamentos. Também temos os rastreamentos de suporte de produtos específicos (PSS) para atender a vida útil de um único produto.

A vida útil mínima de um dispositivo Axis supera os padrões do setor. Uma robusta garantia de hardware de 5 anos é complementada pelo suporte de software AXIS OS por muitos anos. A maioria dos dispositivos tem uma impressionante vida útil do AXIS OS de 8 a 12 anos.

Funciona assim:

1. Quando a Axis lança um novo dispositivo, somente o rastreamento ativo do AXIS OS está disponível. Durante o período pós-lançamento inicial, você se beneficia das melhorias e atualizações contínuas, incluindo novos recursos.
2. Um rastreamento de suporte de longo prazo (LTS) é disponibilizado como alternativa para o rastreamento ativo em até dois anos após o lançamento do produto. Nesse momento, você pode optar entre o rastreamento ativo e o rastreamento de suporte de longo prazo. Produtos com rastreamento de suporte de longo prazo têm suporte apenas para patches e correções de bugs.
3. De dois a quatro anos após o lançamento, quando um dispositivo é descontinuado, o rastreamento ativo para aquele dispositivo também é descontinuado. Nesse momento, todos os dispositivos são automaticamente movidos para o rastreamento de suporte de longo prazo (LTS), onde recebem suporte de patches e correção de bugs por pelo menos 5 anos.

Suporte de software de vida útil do AXIS OS

Suporte de software (8 a 12 anos)

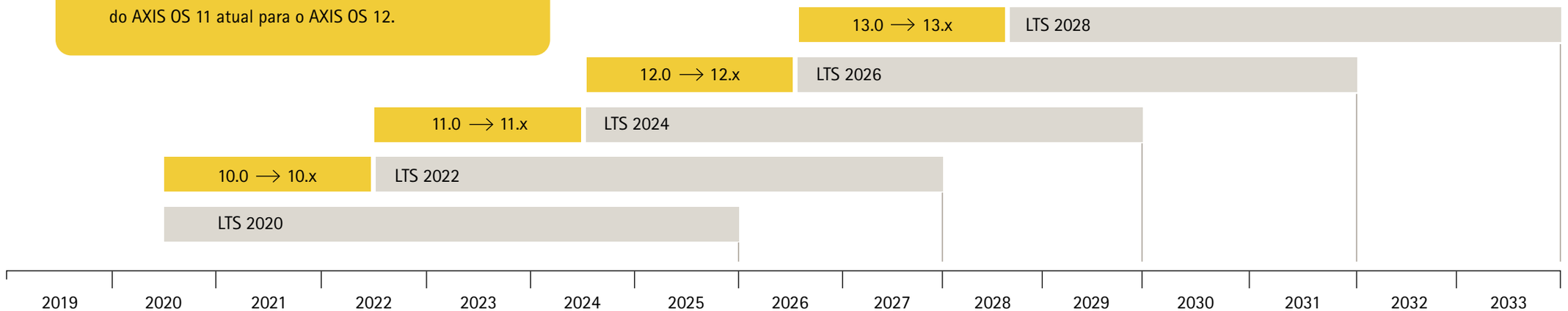
Qual rastreamento de suporte de software é o certo para você?

Assim que os rastreamentos ativo e de longo prazo estiverem disponíveis, os clientes podem optar pelo rastreamento que melhor atende às suas necessidades com orientação da Axis.

Rastreamento ativo
O rastreamento ativo do AXIS OS fornece a experiência mais atualizada e rica em recursos para o sistema operacional AXIS OS. Feito sob medida para clientes que querem se beneficiar do acesso imediato aos recursos e aprimoramentos mais recentes, esse é o único rastreamento disponível para dispositivos recém-lançados. Ele ajuda os usuários a ficarem atualizados sobre a evolução dos recursos do dispositivo: novos recursos de segurança cibernética são adicionados para operações ainda mais seguras, além disso os recursos existentes sofrem melhorias contínuas. Com dispositivos no rastreamento ativo do AXIS OS, você obtém mais dos seus produtos sem custo extra, mesmo anos depois de comprá-los. Se você não tem dependência de compatibilidade, este é o seu rastreamento pelo tempo em que estiver disponível.

Suporte de longo prazo (LTS)
Se estiver procurando por compatibilidade e consistência de API, você deve escolher o rastreamento de suporte de longo prazo (LTS) assim que estiver disponível. O rastreamento LTS se concentra na compatibilidade com versões anteriores e fornece patches de segurança e correções de bugs regulares. Ele mantém a segurança cibernética em vez de fornecer novos recursos de segurança. Da mesma forma, não adiciona novos recursos ou funcionalidades, porém minimiza as alterações para reduzir interrupções. O rastreamento LTS é ideal para clientes que valorizam a confiabilidade e a qualidade, além de desejarem um sistema de terceiros bem integrado. Cada rastreamento LTS têm suporte por 5 anos, e os rastreamentos LTS são distribuídos a cada 24 meses, tendo por base um lançamento regular de rastreamento ativo. Todos os dispositivos são automaticamente movidos para o rastreamento LTS ao serem descontinuados.

A ilustração mostra o rastreamento ativo do AXIS OS lado a lado com os rastreamentos LTS implantados ao longo dos anos. Aproximadamente a cada 24 meses, um novo rastreamento LTS é criado e a versão principal do AXIS OS é aprimorada. Por exemplo, em 2024 criaremos o novo AXIS OS 2024 LTS, então mudaremos do AXIS OS 11 atual para o AXIS OS 12.



Segurança cibernética em foco

O AXIS OS segue a abordagem segurança por desenho. Nosso Axis Security Development Model (ASDM) define processos e ferramentas que reduzem o risco de vulnerabilidades durante e depois do desenvolvimento de software.

Nossa plataforma de segurança cibernética com base em hardware, o Axis Edge Vault, garante inicialização segura e um ambiente protegido contra violações para o armazenamento de chaves criptográficas enviadas pelo cliente. O núcleo do software AXIS OS consiste em componentes de código aberto bem testados. E cada versão é complementada por um software de lista de materiais (SBOM) mostrando que o AXIS OS está atualizado e corrigido para vulnerabilidades conhecidas.

O AXIS OS também está em conformidade e é certificado pela ETSI EN 303 645, que se concentra especificamente em segurança de dispositivo de borda. A conformidade com a FIPS 140 garante que o AXIS OS segue os padrões de criptografia mais atuais definidos pelo Instituto Nacional de Padrões e Tecnologia (NIST). E por fim, como uma Autoridade de numeração CVE reconhecida, seguimos as melhores práticas para identificação, gerenciamento e divulgação de vulnerabilidades.

Nas páginas a seguir, você pode ler mais sobre nossos Axis Security Development Model, Axis Edge Vault, gerenciamento de vulnerabilidades e o conceito de segurança unificada.

Desenvolvido com a segurança em mente

O Axis Security Development Model (ASDM) integra com eficiência a segurança cibernética ao ciclo do desenvolvimento de software. Ele descreve atividades de segurança a serem consideradas durante as fases do desenvolvimento de software. A finalidade é reduzir as vulnerabilidades, bem como os custos de desenvolvimento, pelo estabelecimento de uma linha de base para segurança cibernética e o fornecimento de orientação.

ASDM: feito pela Axis
O Axis Security Development Model não é uma estrutura de normas "prontas para uso". Em vez disso, revisamos várias normas e estruturas de segurança cibernética, como as ISO 27001, ICE 62443, NIST, BSIMM e CMMC. O fator comum entre elas é que a segurança é incorporada em todas as fases do desenvolvimento. Partindo desse ponto, adaptamos nosso modelo para se adequar à cultura da nossa empresa, às práticas de desenvolvimento e ao tipo de produto que fornecemos.

Conjunto de ferramentas do ASDM
O conjunto de ferramentas do ASDM estabelece uma série de atividades que abordam uma variedade de problemas de segurança. Alguns exemplos são avaliação de risco, modelagem de ameaças, teste de modelos de ameaças, análise de código estático, varredura de vulnerabilidades e avaliação de fornecedor. As equipes de desenvolvedores escolhem em quais atividades tomarão parte, dependendo do tipo de software a ser desenvolvido. O objetivo é melhorar a segurança cibernética e não apenas estar em conformidade com um processo.

O benefício adicional da expertise externa
A maior parte do trabalho pesado do desenvolvimento seguro de software é realizada pelo Axis R&D e por nossos engenheiros de software. Porém, também reconhecemos que podemos ser beneficiados pelo conhecimento e a expertise de terceiros. Portanto, contratamos empresas especializadas para a realização de testes de penetração. E nós temos o programa de recompensas para a identificação de bugs do AXIS OS, onde oferecemos compensação financeira a pesquisadores de segurança que nos ajudam a identificar vulnerabilidades.

Governança | **Treinamentos** | **Reunião online do ASDM** | **Avaliação do ASDM** | **Conformidade e padrões de segurança**

Requisitos	Design	Implementação	Verificação	Implantação
Avaliação de risco	Modelagem de ameaças	Análise de código estático	Teste de modelo de ameaça	Gerenciamento de vulnerabilidades
Avaliação do fornecedor		Análise de composição de software	Teste de penetração externo	Gerenciamento de incidentes
Privacidade de dados			Varredura de vulnerabilidades	Status de segurança de produto/ solução
Avaliação de segurança de código aberto			Avaliação de segurança externa	Programa de recompensas para a identificação de bugs

Segurança cibernética incorporada

Proteção de dentro para fora
O Axis Edge Vault é nossa plataforma de segurança cibernética baseada em hardware. Ele fornece uma base sólida que garante que seus dispositivos Axis são uma parte segura e confiável da sua rede. Porém, essa base sólida criada sobre hardware seria inútil sem um sistema operacional que oferecesse suporte a todo o seu potencial. O AXIS OS usa a plataforma Edge Vault para fornecer segurança aprimorada na borda para cada caso de uso.

O Edge Vault inclui recursos como:

Armazenamento de chave seguro
O armazenamento de chave seguro envolve módulos de computação criptográfica para armazenamento e computação seguros de chaves criptográficas. Eles protegem a identidade do dispositivo e outras informações confidenciais contra acesso não autorizado, mesmo se o dispositivo estiver comprometido. Os módulos de computação criptográfica usados são o Trusted Execution Environment incorporado ao sistema em um chip (SoC), bem como um elemento seguro dedicado ou um Trusted Platform Module (TPM 2.0), que são chips separados na placa de circuito impresso (PCB).

Sistema operacional assinado e inicialização segura
Sistema operacional assinado significa que assinamos com código a imagem do software do dispositivo. Juntos, o SO assinado e a inicialização segura significam que os dispositivos podem baixar e executar somente o legítimo sistema operacional AXIS OS. Isso adiciona uma camada de proteção extra que protege contra violações na cadeia de fornecimento de software e hardware.

ID de dispositivo Axis
A ID de dispositivo AXIS está em conformidade com a IEEE 802.1AR e permite a identificação e a integração do dispositivo de segurança em uma rede. Ela age como um verdadeiro passaporte para cada dispositivo fabricado pela Axis.

Sistema de arquivos criptografados
A criptografia do sistema de arquivos protege os dados do sistema de arquivos contra extração ou violação enquanto o dispositivo não estiver em uso, como durante o trajeto entre o integrador de sistemas e o cliente final.

Vídeo assinado
O vídeo assinado permite aos usuários verificar a autenticidade do vídeo capturado e se ele não foi violado.

Plataforma de segurança cibernética Axis Edge Vault

Módulos de computação criptográfica	Recursos	Casos de uso
Componente de segurança TPM 2.0 Segurança SoC (TEE)	Inicialização segura SO assinado ID de dispositivo Axis Armazenamento seguro de chaves Vídeo assinado Sistema de arquivos criptografados	Identidade de confiança de dispositivos Armazenamento de chave seguro Detecção de violação de vídeo Proteção da cadeia de fornecimento

*Observação: nem todos os modelos de dispositivos são compatíveis com todos os recursos do Axis Edge Vault. Verifique a folha de dados ou o seletor de produtos Axis para obter a confirmação dos recursos com suporte para produtos específicos.

Gerenciamento de vulnerabilidades

Para reduzir o risco de exposição dos nossos clientes, seguimos as melhores práticas do setor no gerenciamento e resposta transparentes às vulnerabilidades.

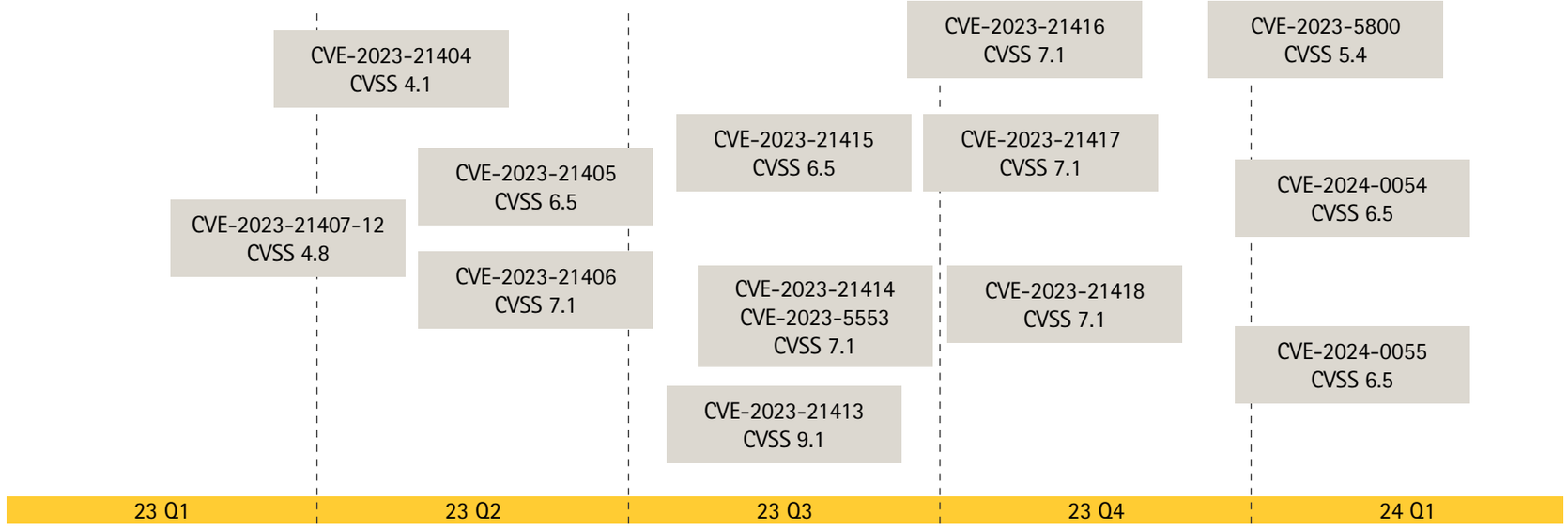
Melhor gerenciamento de vulnerabilidades da categoria
Não existe uma forma de garantir que os produtos e serviços fornecidos pela Axis sejam completamente livres de vulnerabilidades. Isto não é exclusividade nossa, mas sim uma condição compartilhada para todos os softwares e serviços. Porém nos empenhamos com seriedade para identificar e mitigar potenciais vulnerabilidades em todas as fases, reduzindo o risco da implantação dos produtos e serviços Axis nos ambientes do cliente.

Uma Autoridade de numeração CVE,
A Axis é uma Autoridade de numeração CVE (CNA). Aderimos ao Programa CVE com o objetivo de trabalhar com empresas que tenham ideias semelhantes sobre melhoria do gerenciamento de vulnerabilidades. Alinhamos a forma como lidamos, divulgamos e corrigimos vulnerabilidades com a estrutura internacional fornecida por esta organização sem fins lucrativos e com a nossa política pública de gerenciamento de vulnerabilidades.

O gerenciamento transparente no qual você pode confiar
A Axis usa o sistema de classificação CVSS (Common Vulnerability Scoring System) muito conhecido para classificar vulnerabilidades relacionadas ao código desenvolvido pela Axis ou ao código-fonte aberto de terceiros. Avaliamos vulnerabilidades em códigos abertos de acordo com a relevância delas para os nossos produtos quando as recomendações de melhores práticas são aplicadas. Você pode assinar o Axis Security Notification Service para receber informações sobre vulnerabilidades e outros assuntos relacionados à segurança dos produtos Axis.

Parcerias com pesquisadores e organizações de segurança
Adotamos e apreciamos o trabalho de pesquisadores de segurança privados e de organizações de pesquisa de segurança que entram em contato conosco para relatar descobertas de vulnerabilidades. Não hesitamos em divulgá-los e corrigi-los. O importante é lidar com as vulnerabilidades de forma correta e transparente com um processo de divulgação ético e responsável, não importa como a vulnerabilidade é descoberta.

Vulnerabilidades do AXIS OS



Vulnerabilidades divulgadas pela Axis para o AXIS OS.

Uma experiência completa de segurança

Em dispositivos em rede alimentados pelo AXIS OS, os componentes de software e hardware trabalham em conjunto permitindo que os clientes operem seus dispositivos, serviços e sistemas aos quais estão conectados com segurança. Várias camadas de proteção abrangente começam com uma base de segurança e uma plataforma de segurança baseada em hardware, que se estende até o software. Os dispositivos alimentados pelo AXIS OS são protegidos por essa abordagem em camadas e de defesa profunda para a segurança cibernética. Isso aumenta a segurança cumulativa de dados, aplicativos e processos.

Por isso, você pode ter certeza de que não importa qual a utilização de um dispositivo Axis, proteção, segurança e comunicação segura estão disponíveis, permitindo a integração perfeita e segura em sistemas de terceiros.

Controle o acesso

Gerenciamento de controle de acesso
Gerenciamento de dispositivo de usuário local com indicador de complexidade de senha
Gerenciamento de dispositivos de usuário federado pelo OpenID Connect (Código de autorização RFC6749, 1.3.1), fornecendo integração com ADFS que desbloqueia recursos como aplicação de complexidade de senha, rotação, bloqueio automático de conta, autenticação multifator (MFA) e a funcionalidade direitos do Microsoft AD.

Privacidade
Uso de dados de diagnóstico
Abordagem minimalista sobre a quantidade dados específicos do cliente que deve ser armazenada.

Aplicação

Aplicativo de segurança
Aplicativo de segurança com base em TLS (MQTT, SFTP, NTS, HTTPS, WebRTC)
Streaming de vídeo criptografado (RTSPS/SRTP, HTTPS), syslog remoto seguro

Sistema operacional

Criptografia e proteção de dados
OpenSSL 1.1.1 e 3.0
Certificado X.509 PKI e criptografia
Segurança da camada de transporte (TLS 1.2/TLS 1.3)
Criptografia de cartões SD (AES-XTS-Plain64 256 bits)
Sistema de arquivos criptografado (AES-XTS-Plain64 256bit).
Vídeo assinado

Segurança padrão
HTTPS ativado por padrão
Proteção contra atraso de força bruta
Firewall baseado em host
Network time security (NTS)
Versões inseguras do TLS desativadas
Porta de depuração/UART desativada

Segurança em rede para empresas
IEEE 802.1X (controle de acesso à rede)
IEEE 802.1AR (identidade de dispositivo seguro)
IEEE 802.1AE (MAC security, MACsec)

Sistema operacional AXIS OS
Sistema operacional comum baseado em Linux com mais de 95% de componentes de software de código aberto padrão do setor, como OpenSSL, Apache, Curl e outros.
Rastreamento ativo para ampliação de recursos e rastreamento de suporte de longo prazo (LTS) de 5 anos para integração de terceiros e casos de uso de compatibilidade com versões anteriores.

Segurança assistida por silício (chip)

Raiz de confiança de hardware
Segurança de sistema em um chip (SoC) baseada em ARM
Trusted Execution Environment (TEE/OP-TEE)
Trusted platform module (TPM 2.0), Elemento seguro

Armazenamento de chave seguro
Armazenamento e operação protegidos contra violação de chaves criptográficas, como chaves privadas enviadas pelo cliente, chaves de assinatura de vídeo e ID de dispositivo Axis.

Base de segurança

Axis Security Development Model
Axis Security Development Model (ASDM)
Testes de penetração terceirizados
Programa de recompensas para a identificação de bugs com a Bugcrowd
Lista de material de software (SBOM)

Conformidade
Critérios Comuns EAL
FIPS 140
ETSI EN 303 645

Identidade de confiança de dispositivos
Plataforma de segurança cibernética Axis Edge Vault
Inicialização segura com sistema operacional assinado (assinatura de código)
ID de dispostivo Axis (IEEE 802.1AR)

Integração de alto nível

A integração desempenha um papel fundamental para os produtos Axis. Nos dedicamos a APIs robustas e consistentes que oferecem suporte fácil à integração em uma grande variedade de aplicativos.

Para que você possa criar soluções abrangentes que aproveitem todos os recursos dos seus dispositivos Axis.

Nas páginas seguir, você pode ler mais sobre VAPIX (nossa própria API), nosso trabalho com ONVIF e IoT, a modularização de plataforma com ACAP e a automação para integração em rede.

A vantagem da Axis em VAPIX, ONVIF, IoT e integração na nuvem

No dinâmico mundo do monitoramento e da conectividade, a Axis Communications oferece um conjunto de soluções de integração que redefinem os padrões do setor.

VAPIX: um legado de extensibilidade
VAPIX, nossa estrutura de API aberta, reitera nosso compromisso com a inovação. Ao oferecer suporte para chamadas HTTP GET e POST, juntamente com formatos JSON e XML, permite que os desenvolvedores criem soluções personalizadas com facilidade. Com a maior e mais consistente biblioteca no mercado, a VAPIX é a pioneira na integração aberta de produtos em rede Axis que antecede até mesmo o ONVIF.

ONVIF: normas de colaboração do setor
A Axis colabora com o fórum aberto do setor industrial ONVIF em apoio a um espírito de colaboração que avança nesse setor e fornece aos usuários soluções abrangentes e interoperáveis. O ONVIF fornece e promove interfaces padronizadas para interoperabilidade eficaz de produtos de segurança física baseados em IP. Isso simplifica a integração para os nossos parceiros, garantindo que os dispositivos Axis integrem-se perfeitamente a uma grande variedade de sistemas.

IoT: abraçando o futuro
À medida que a Internet das Coisas (IoT) dá nova forma à conectividade, os dispositivos Axis contribuem para um ecossistema em evolução. A Axis oferece suporte a protocolos como o MQTT que se alinham com a inovação da IoT. Com a Axis, seus dispositivos não estão simplesmente conectados, eles fazem parte de um cenário próspero de IoT.

Integração em nuvem: onde a inovação atinge o céu
Nos domínios da conectividade digital, a Axis explora a integração em nuvem com APIs projetadas para interação simples com as principais plataformas como o Microsoft Azure e a Amazon Web Service (AWS). Acompanhando o processo evolutivo tecnológico, ofereceremos suporte a mais tecnologias em nuvem, como MQTT para serviços de mensagens e WebRTC para streaming de vídeo e de áudio. O objetivo é permitir que os usuários aproveitem ao máximo a tecnologia em nuvem.

Modularização de plataforma pela ACAP

Um dos principais recursos do AXIS OS é que ele permite a modularização da plataforma por meio da AXIS Camera Application Platform (ACAP). A ACAP é uma estrutura que permite aos desenvolvedores criar e implantar aplicativos e serviços, como analíticos de vídeo, analíticos de áudio e outras extensões personalizadas para atender aos requisitos de negócios. Os aplicativos ACAP são independentes das funcionalidades principais do AXIS OS e podem ser instalados, atualizados e removidos sem afetar o restante do sistema. Os aplicativos ACAP também podem se comunicar uns com os outros e com sistemas externos usando protocolos e APIs padrão.

Escalabilidade e desempenho
A ACAP utiliza a arquitetura de microsserviços do sistema operacional em dispositivos Axis. Cada serviço pode ser ampliado ou reduzido independentemente, de acordo com a demanda e a carga. Isso melhora o desempenho geral e a disponibilidade do sistema, permitindo o uso e a alocação eficiente de recursos.

Adaptabilidade e personalização
Com a ACAP, os dispositivos Axis são mais versáteis, adaptáveis e personalizáveis, pois oferecem suporte a diferentes tipos de integração, analíticos e dispositivos. A ACAP também reduz o acoplamento e aumenta a coesão da plataforma porque cada aplicativo é fracamente acoplado ao AXIS OS e altamente coeso em si mesmo.

Capacidade de manutenção e confiabilidade
Cada serviço pode ser testado, monitorado e depurado de forma independente e isolada. Isso simplifica a solução de problemas e o diagnóstico, além de aumentar a resiliência e a tolerância do sistema a falhas. E faz com que AXIS OS se destaque quando o assunto é qualidade de software.

AXIS OS para equipes de TI

O estabelecimento de automação e integração adequadas à infraestrutura de TI garante controles de segurança apropriados e pode economizar tempo e dinheiro. A complexidade desnecessária do sistema é reduzida. Alguns dos benefícios da combinação entre dispositivos Axis e software integrado na infraestrutura de TI de empresas são permitir a você:

> Minimizar a complexidade do sistema removendo redes de staging de dispositivos físicos dedicados

> Economizar custos adicionando processos de integração automatizados e gerenciamento de dispositivos

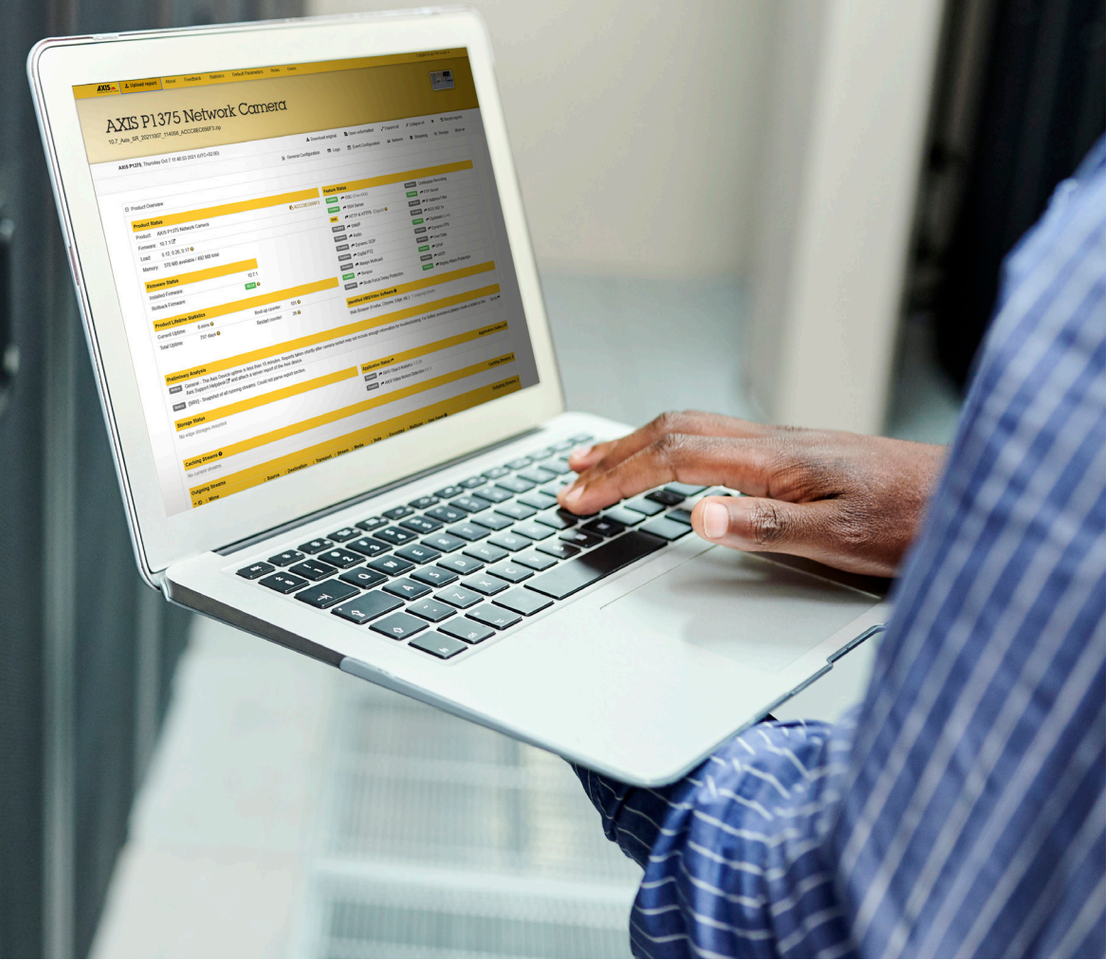
> Aproveitar os controles de segurança em rede zero-trust, como IEEE 802.1X, IEEE 802.1AR

> Aumentar a segurança geral em rede introduzindo a criptografia de dados em um nível básico com a ajuda do IEEE 802.1AE MACsec. Dessa forma, o dispositivo Axis contribui para a segurança em rede, por exemplo.

> Monitorar o dispositivo Axis por meio de protocolos padronizados como o Remote Syslog, permitindo o monitoramento de registros e integridade, por exemplo.

Redes seguras com base em princípios zero-trust
A criação de redes convergentes e seguras baseadas em princípios zero-trust é fundamental para eliminar sistemas isolados que operam por conta própria. Mais segurança, custos de configuração e manutenção mais baixos e mais aplicação das políticas de TI são possíveis quando os dispositivos Axis são integrados à infraestrutura de TI da empresa usando protocolos e padrões de rede abertos e bem definidos.

Uma vantagem para os departamentos de TI
Os departamentos de TI são responsáveis pela proteção da rede de TI, por isso os dispositivos Axis são vantajosos para eles. Os dispositivos Axis são mais fáceis de integrar, manter e operar graças à sua versatilidade e ao fato de serem semelhantes às soluções de TI definidas pelos protocolos de rede abertos e padronizados IEEE e IETF e desenho compartilhado. Os dispositivos Axis são como "cidadãos confiáveis" nas redes dos clientes contribuindo para uma melhor segurança.



Vamos conversar

O AXIS OS é o motivo de você confiar nos dispositivos Axis. Isso se deve ao fato dele oferecer excelente qualidade da imagem, qualidade de áudio e muito mais.

Por ter sido desenvolvido especificamente para atender aos critérios mais importantes para seus dispositivos em rede: valor a longo prazo, normas de segurança cibernética e facilidade de integração.

Adoraríamos conversar com você sobre como exatamente os dispositivos Axis podem agregar valor à sua empresa ou organização.

Então, por que não entra em contato conosco hoje?

Ou você pode explorar nossos dispositivos em axis.com

Sobre a Axis Communications

A Axis viabiliza um mundo mais inteligente e seguro, criando soluções que melhoram a segurança e o desempenho empresarial. Como uma empresa de tecnologia em rede e líder do setor, a Axis oferece soluções para sistemas de videomonitoramento, controle de acesso, interfone e áudio. Esses sistemas são aprimorados por meio de aplicativos de análise inteligentes e apoiados por treinamentos de alta qualidade.

A Axis conta com cerca de 4.000 funcionários dedicados, em mais de 50 países, e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para oferecer soluções aos clientes. A Axis foi fundada em 1984 e está sediada em Lund, na Suécia.