WHITE PAPER

Segurança na solução de uso corporal da Axis

Outubro 2026

Resumo

Apesar de ser baseado em uma plataforma aberta, o sistema de uso corporal da Axis possui um nível muito alto de segurança.

Para garantir a segurança em caso de perda da câmera, ela é baseada em uma plataforma mínima, sem componentes de software desnecessários. Em vez disso, mais recursos foram adicionados no controlador do sistema, que geralmente fica menos exposto a ameaças físicas. Além disso, o armazenamento interno da câmera é criptografado usando AES-256 para proibir o acesso não autorizado aos dados. A comunicação baseada em IPv6 e os certificados garantem que a câmera descarregará dados apenas no controlador de sistema específico ou no sistema ao qual pertence.

Quando os dados são descarregados da câmera para o controlador do sistema, é usada uma conexão HTTPS de rede criptografada. Os dados são armazenados por um breve período no dispositivo de armazenamento criptografado (com AES-256) do controlador do sistema, antes de serem transferidos usando outra conexão criptografada HTTPS para o destino do conteúdo.

A segurança e a integridade do controlador do sistema são reforçadas por um TPM (Módulo de plataforma confiável) compatível com FIPS 140-2. Outros recursos, que o sistema corporal compartilha com muitos outros dispositivos da Axis, são o SO assinado, a inicialização segura e o vídeo assinado.

Quando as imagens são transmitidas ao vivo por meio do AXIS Body Worn Live, as organizações podem escolher entre uma implantação hospedada pela Axis (na nuvem) ou auto-hospedada (no local). Em ambos os casos, os dados são criptografados em repouso, em trânsito e totalmente criptografados de ponta a ponta diretamente para o cliente do visualizador. Além disso, o administrador controla rigorosamente quem pode assistir à transmissão ao vivo, chegando a especificar o computador, o cliente e as credenciais do usuário.

Índice

1 Siglas e terminologia 4
2 Introdução 4
3 Segurança em caso de perda da câmera 4
4 Segurança na transferência de dados 4
5 Outros recursos de segurança 5
6 Segurança com AXIS Body Worn Live 5
6.1 Implantação hospedada pela Axis 6
6.2 Implantação em servidor auto-hospedado 6

1 Siglas e terminologia

BWC. Câmera de uso corporal

VMS. Sistema de gerenciamento de vídeo

EMS. Sistema de gerenciamento de evidências

Destino do conteúdo. Local que armazena gravações e dados de, por exemplo, câmeras corporais. Exemplos de destinos de conteúdo incluem sistemas de gerenciamento de vídeo, sistemas de gerenciamento de evidências e servidores de mídia.

2 Introdução

O sistema de uso corporal da Axis é baseado em uma plataforma aberta, o que facilita a integração com sistemas externos para gerenciamento de vídeo e gerenciamento de evidências. No entanto, possui um nível muito alto de segurança de sistema, pois esse foi o foco principal em todas as etapas da implementação do sistema.

Este white paper descreve o fluxo de dados entre os componentes do sistema corporal da Axis. Descrevemos especialmente as medidas tomadas para proteger o sistema e os dados, desde uma gravação da BWC até o destino do conteúdo. Também mostramos como as transmissões ao vivo são criptografadas com o AXIS Body Worn Live em ambos os seus modelos de implantação.

3 Segurança em caso de perda da câmera

Por causa do uso diário, a câmera corporal (BWC) está fisicamente exposta a riscos de roubo e vandalismo. Vários recursos de design do sistema foram empregados para mitigar os efeitos de tais ameaças para que a segurança do sistema e dos dados seja mantida mesmo quando uma câmera é perdida.

Exemplo: a BWC baseia-se em uma plataforma de software mínima em comparação com outras câmeras Axis, e todos os componentes de software desnecessários foram removidos. A câmera e o controlador do sistema não suporta VAPIX nem protocolos como FTP, SSH ou SNMP. Além disso, a câmera não possui funcionalidade de servidor. A integração com outros sistemas, como VMS e EMS, é realizada pelo controlador do sistema, que geralmente é menos exposto a ameaças físicas do que as câmeras.

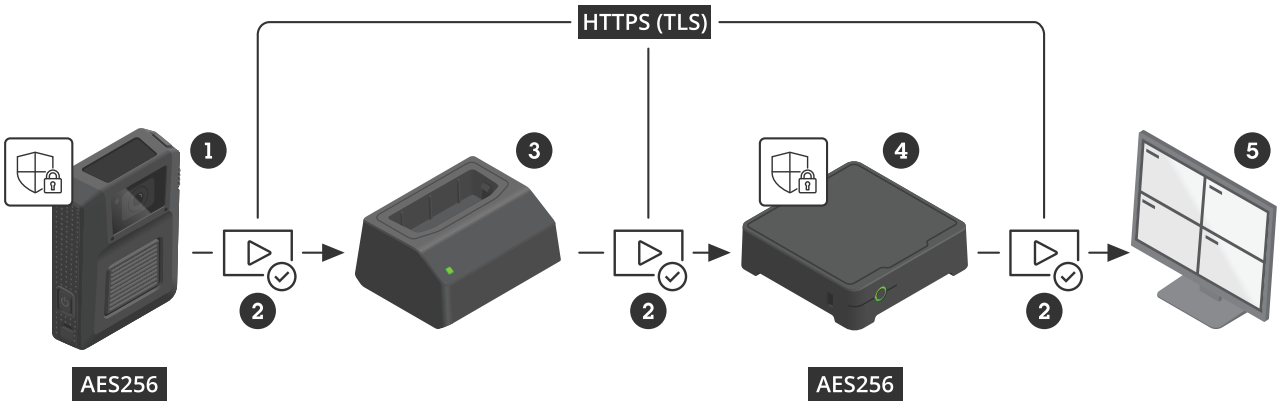
O armazenamento interno da BWC é criptografado usando AES-256 para proibir o acesso não autorizado aos dados em caso de perda da câmera.

A câmera descarregará os dados apenas para o controlador de sistema específico ou o sistema ao qual ela pertence. Isso ocorre porque a BWC e o controlador do sistema se comunicam com IPv6 e usam certificados. Os certificados são renovados automaticamente para corresponder ao mais recente do controlador do sistema toda vez que a câmera é acoplada na dock.

Caso uma câmera seja desconectada e fique fora do sistema por oito semanas, ela entrará no modo de segurança e bloqueará a conexão por motivos de segurança. Para ser aceita no sistema novamente, é necessária uma verificação manual com a senha-chave mestra. Isso é feito para garantir que uma câmera perdida ou inativa por um longo período não seja adicionada novamente sem que seja notada, pois poderia representar um risco de segurança.

4 Segurança na transferência de dados

Geralmente, após o turno, a BWC (contendo vídeos e metadados) é acoplada à dock station. Todos os dados são descarregados através da dock station para o controlador do sistema usando uma conexão de rede criptografada com HTTPS (HTTP com TLS). Os dados ficam armazenados no controlador do sistema apenas por um breve período, em seu dispositivo de armazenamento SSD, que é criptografado usando AES-256. O controlador do sistema então transfere os dados, por meio do protocolo HTTPS, para o destino do conteúdo.



Armazenamento e transferência de dados com segurança da BWC (1) para o destino do conteúdo (5).

1 *BWC com Axis Edge Vault*
2 *Vídeo assinado (recurso de segurança cibernética)*
3 *Estação de carregamento*
4 *Controlador de sistema com o Axis Edge Vault*
5 *Destino do conteúdo*

Também há suporte para usar uma chave de criptografia do destino do conteúdo para criptografar os dados na BWC e no controlador do sistema caso o destino do conteúdo forneça uma chave de criptografia pública. Nesse caso, os dados terão uma camada extra de criptografia ao serem enviados para o destino do conteúdo.

5 Outros recursos de segurança

A segurança e a integridade do controlador do sistema são reforçadas por um TPM (Módulo de plataforma confiável) compatível com FIPS 140-2.

Tanto o BWC quanto o controlador do sistema são equipados com o Axis Edge Vault, uma plataforma de segurança cibernética baseada em hardware que protege todos os dados nos dispositivos e ativa diversos recursos de segurança. Por exemplo, o sistema de arquivos é criptografado e a chave é protegida pelo Axis Edge Vault. *A inicialização segura* garante que os dispositivos possam inicializar apenas com software de dispositivo autorizado. O *SO assinado* faz com que eles rejeitem atualizações de se a integridade do software estiver comprometida. O *vídeo assinado* cria uma camada extra de proteção ao adicionar uma soma de verificação criptográfica ao stream de vídeo. Isso permite que o vídeo seja rastreado de forma confiável até a câmera exclusiva da Axis em que foi produzido, verificando se a filmagem não foi violada.

Você pode ler mais sobre vídeo assinado e o Axis Edge Vault em *developer.axis.com/video-transmission-and-recording/signed-video/* e *axis.com/solutions/edge-vault*

A única maneira de o usuário da câmera visualizar o vídeo gravado em campo é por meio do aplicativo AXIS Body Worn Assistant. Se o aplicativo estiver habilitado, a BWC transmitirá o vídeo diretamente para o aplicativo, mas nenhum material do vídeo será armazenado para acesso posterior no cache ou na memória do dispositivo que executa o aplicativo. Também haverá uma sobreposição no fluxo de vídeo para impedir o uso de dispositivos de gravação secundários para capturar o vídeo. Se ainda assim, isso for feito, o videoclipe poderá ser rastreado até o usuário da BWC por meio da sobreposição. O conector compatível com USB-C da BWC não pode ser usado de forma alguma para visualizar, excluir ou descarregar o vídeo.

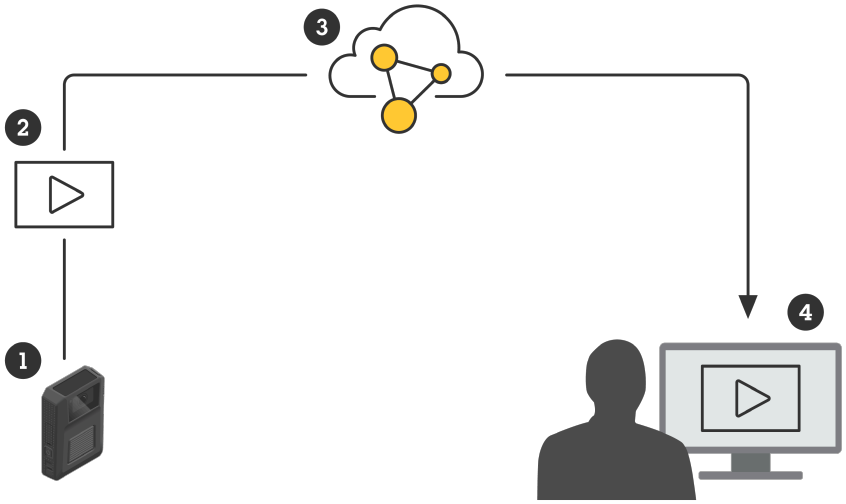
6 Segurança com AXIS Body Worn Live

O AXIS Body Worn Live é um aplicativo que permite o acesso em tempo real aos dados das câmeras corporais da Axis. Ao fornecer aos usuários uma transmissão ao vivo de vídeo, áudio e outros dados, como coordenadas de localização, o AXIS Body Worn Live permite uma percepção situacional incomparável de um incidente em andamento. Para atender às diferentes necessidades organizacionais em relação à infraestrutura e à soberania de dados, o produto está disponível em dois modelos de implantação: hospedado pela Axis e auto-hospedado.

Independentemente do modelo de implantação, o administrador do sistema da câmera corporal tem controle total sobre quem pode visualizar a transmissão em tempo real. Os dados são criptografados de forma que apenas os visualizadores explicitamente aprovados pelo administrador possam descriptografar e visualizar o vídeo. O administrador também pode revogar o acesso com base em funções para proteger a integridade dos dados. Para implantações hospedadas pela Axis, o visualizador deve ter acesso ao navegador da web autorizado, ao VMS e às credenciais de usuário corretas. Para implantações auto-hospedadas, o visualizador deve ter acesso à rede local e às credenciais de usuário corretas. Ninguém mais, nem mesmo a Axis, pode acessar a transmissão ao vivo, e a Axis não tem acesso às chaves de criptografia de ponta a ponta criadas pelos usuários.

6.1 Implantação hospedada pela Axis

Quando utilizado como serviço baseado em nuvem, todos os dados e arquivos hospedados no AXIS Body Worn Live são criptografados com AES-256 enquanto estão em repouso. Todos os canais de comunicação são protegidos usando HTTPS com TLS, empregando certificados assinados por autoridades de certificação confiáveis. Além da criptografia de transmissão, o AXIS Body Worn Live adiciona uma camada de criptografia verdadeira de ponta a ponta com o conjunto de algoritmos XChaCha20-Poly1305.



Transmissão ao vivo segura com criptografia de ponta a ponta em uma implantação hospedada pela Axis

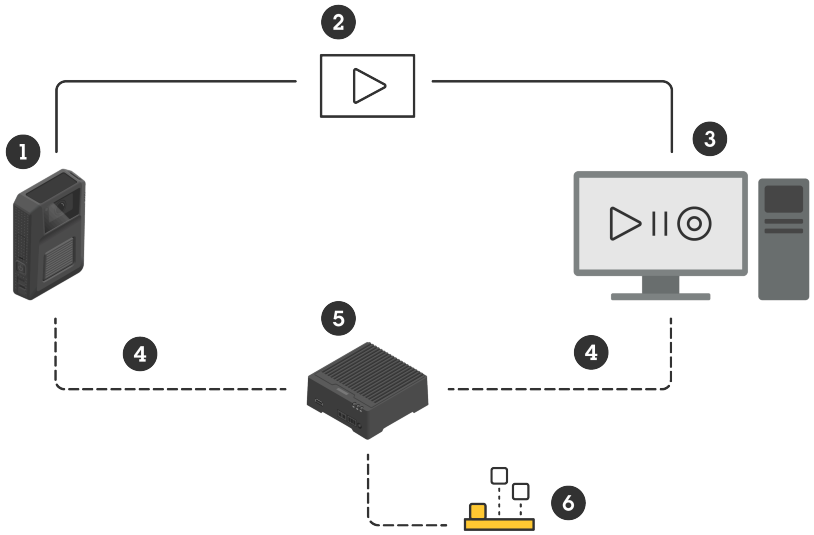
1. *A câmera corporal grava vídeo em tempo real e coleta outros dados. Os dados já vêm criptografados na câmera.*
2. *Streaming ao vivo (criptografado de ponta a ponta).*
3. *Nuvem hospedada pela Axis. Os dados e arquivos são criptografados usando AES-256.*
4. *Cliente da Web. Os dados são descriptografados no navegador do visualizador.*

6.2 Implantação em servidor auto-hospedado

Organizações com políticas rigorosas, que exigem que a infraestrutura permaneça inteiramente dentro de seus próprios ambientes de rede controlados, podem instalar a aplicação de servidor AXIS Body Worn Live, auto-hospedado localmente em um dispositivo. Este dispositivo servidor pode ser o AXIS W401 Body Worn Activation Kit ou o AXIS D3110 Mk II Connectivity Hub. Nenhum vídeo ou dado confidencial é armazenado em repouso no dispositivo local; ele funciona exclusivamente para manter a conexão. O canal de comunicação para a transmissão de mídia entre câmeras e integrações é protegido por meio do DTLS 1.0 ou versões posteriores. O canal de comunicação para a transmissão de sinalização e eventos entre o servidor e as integrações é protegido por meio do protocolo HTTPS, usando certificados fornecidos pelo cliente e o TLS 1.2 ou versão posterior.

Quando o fluxo de dados é transmitido por meio da versão auto-hospedada, o servidor local configura de forma segura a sinalização WebRTC com autenticação baseada em certificado entre o servidor e o BWC. Uma vez estabelecida, é formada uma conexão ponto a ponto criptografada diretamente entre a BWC e o cliente WebRTC do visualizador (como um VMS). Como o fluxo de vídeo é enviado diretamente por meio dessa conexão

criptografada, sem armazenamento intermediário, evita-se a interceptação não autorizada. O sistema foi projetado para operar em redes fechadas e segmentadas, sem a necessidade de acesso à internet, minimizando assim a superfície de ataque contra ameaças externas.



Transmissão ao vivo segura em implantação auto-hospedada

1 *A câmera corporal grava vídeo em tempo real e coleta outros dados. Os dados já vêm criptografados na câmera.*
2 *Transmissão ponto a ponto (criptografada).*
3 *Cliente WebRTC do visualizador.*
4 *Sinalização WebRTC.*
5 *AXIS Body Worn Live, dispositivo servidor auto-hospedado.*
6 *AXIS Body Worn Live, aplicativo de servidor auto-hospedado. Isso é usado para configurar a sinalização do WebRTC.*

Sobre a Axis Communications

A Axis possibilita um mundo mais inteligente e seguro, aprimorando a segurança, proteção, eficiência operacional e inteligência nos negócios. Como uma empresa de tecnologia em rede e líder do setor, a Axis oferece soluções de videomonitoramento, controle de acesso, intercomunicação e áudio. Essas soluções são aprimoradas por meio de aplicativos de análise inteligentes e apoiadas por treinamentos de alta qualidade.

A Axis conta com cerca de 5.000 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.

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC e VAPIX são marcas comerciais registradas da Axis AB em várias jurisdições. Todas as outras marcas comerciais pertencem aos respectivos proprietários.Reservamo-nos o direito de inserir modificações sem aviso prévio.trademarkdisclaimer