WHITE PAPER

Axis 신체 착용 솔루션의 보안

10월 2026

요약

개방형 플랫폼에 기반하고 있음에도 불구하고 Axis 신체 착용 시스템은 매우 높은 수준의 시스템 보안을 자랑합니다.

카메라 분실 시 보안을 보장하기 위해 카메라는 불필요한 소프트웨어 구성 요소가 없는 최소화된 플랫폼에 기반을 두고 있습니다. 대신 물리적 위협에 덜 노출되는 시스템 컨트롤러에 더 많은 기능이 배치되어 있습니다. 또한 카메라의 내부 스토리지는 데이터에 대한 무단 액세스를 금지하기 위해 AES-256 암호화되어 있습니다. IPv6 및 인증서에 기반한 통신은 카메라가 특정 시스템 컨트롤러 또는 카메라가 속한 시스템으로만 데이터를 오프로드하도록 보장합니다.

카메라에서 시스템 컨트롤러로 데이터가 오프로드될 때 HTTPS 암호화된 네트워크 연결이 사용됩니다. 데이터는 시스템 컨트롤러의 AES-256 암호화 저장 장치에 잠시만 저장된 후, 다른 HTTPS 암호화 연결을 통해 콘텐츠 대상으로 전송됩니다.

시스템 컨트롤러의 보안과 무결성은 FIPS 140-2를 준수하는 TPM(Trusted Platform Module)을 통해 더욱 강화됩니다. 신체 착용 시스템이 다른 여러 Axis 장치와 공유하는 기타 기능으로는 Signed OS, Secure boot, Signed video가 있습니다.

AXIS Body Worn Live를 통해 영상을 라이브 스트리밍할 때, 조직은 Axis에서 호스팅하는 배포(클라우드)와 자체 호스팅 배포(온프레미스) 중에서 선택할 수 있습니다. 두 경우 모두 데이터는 저장 시와 전송 시에 암호화되며, 뷰어의 클라이언트까지 완전한 엔드 투 엔드 암호화가 적용됩니다. 또한 관리자는 특정 컴퓨터, 클라이언트, 사용자 자격 증명 수준까지 라이브 스트림을 볼 수 있는 대상을 엄격하게 제어합니다.

목차

1 약어 및 용어 4
2 서론 4
3 카메라 분실 시 보안 4
4 데이터 전송 보안 4
5 기타 보안 특성 5
6 AXIS Body Worn Live의 보안 5
6.1 Axis에서 호스팅하는 배포 6
6.2 자체 호스팅 배포 6

1 약어 및 용어

BWC. 신체 착용 카메라

VMS. 영상 관리 시스템

EMS. 증거 관리 시스템

콘텐츠 대상**. 예를 들어 신체 착용 카메라의 녹화 및 데이터를 저장하는 위치입니다. 콘텐츠 대상의 예로는 영상 관리 시스템, 증거 관리 시스템, 미디어 서버 등이 있습니다.**

2 서론

Axis 신체 착용 시스템은 개방형 플랫폼을 기반으로 하므로 영상 관리 및 증거 관리를 위해 외부 시스템과 쉽게 통합할 수 있습니다. 그럼에도 불구하고 시스템 구현의 모든 단계에서 보안에 중점을 두었기 때문에 매우 높은 수준의 시스템 보안을 자랑합니다.

이 백서에서는 Axis 신체 착용 시스템의 구성 요소 간의 데이터 흐름을 설명합니다. 특히 BWC 녹화에서 콘텐츠 대상에 이르기까지 시스템과 데이터를 보호하기 위해 취한 조치에 대해 설명합니다. 또한 AXIS Body Worn Live의 두 가지 배포 모델에서 라이브 스트림이 어떻게 암호화되는지도 설명합니다.

3 카메라 분실 시 보안

신체 착용 카메라(BWC)는 일상적인 사용 과정에서 도난 및 파손의 위험에 물리적으로 노출됩니다. 이러한 위협의 영향을 완화하기 위해 카메라가 분실되더라도 시스템 및 데이터 보안이 유지될 수 있도록 몇 가지 시스템 설계 기능이 적용되었습니다.

한 가지 예로, BWC는 다른 Axis 카메라에 비해 최소화된 소프트웨어 플랫폼을 기반으로 하며 불필요한 소프트웨어 구성 요소가 모두 제거되어 있습니다. 카메라와 시스템 컨트롤러는 VAPIX를 지원하지 않으며 FTP, SSH, SNMP와 같은 프로토콜도 지원하지 않습니다. 또한 카메라에는 서버 기능이 없습니다. 대신에 카메라에 비해 물리적 위협에 덜 노출되는 시스템 컨트롤러가 VMS 및 EMS와 같은 다른 시스템과의 통합을 처리합니다.

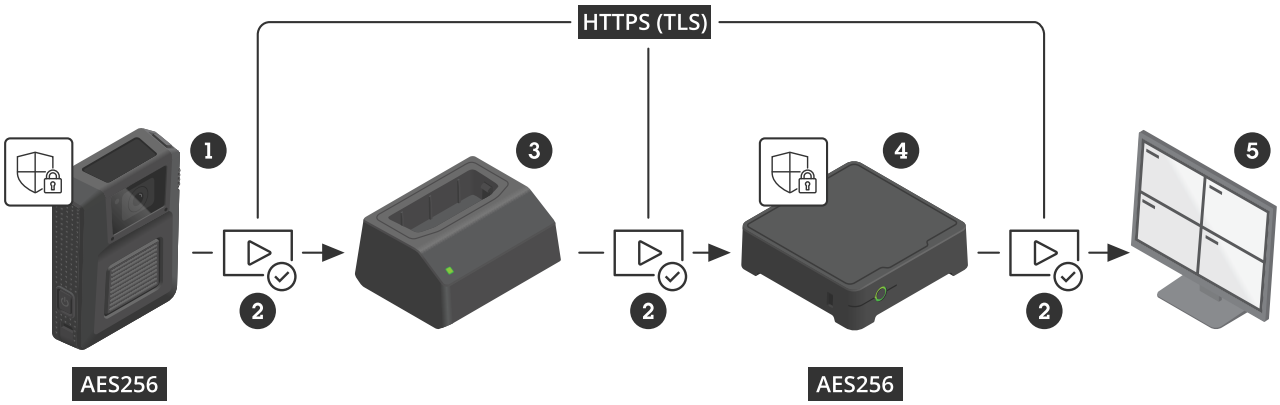
카메라 분실 시 데이터에 대한 무단 액세스를 방지하기 위해 BWC의 내부 스토리지는 AES-256을 사용하여 암호화됩니다.

카메라는 카메라가 속한 특정 시스템 컨트롤러 또는 시스템으로만 데이터를 오프로드합니다. BWC와 시스템 컨트롤러가 IPv6로 통신하고 인증서를 사용하기 때문입니다. 인증서는 카메라가 도킹될 때마다 시스템 컨트롤러의 최신 인증서에 맞게 자동으로 갱신됩니다.

카메라가 도킹 해제된 상태로 8주 동안 시스템에서 떨어져 있으면 보안상의 이유로 안전 모드로 전환되어 연결을 잠급니다. 시스템에 다시 등록되려면 마스터 키 암호를 사용한 수동 확인이 필요합니다. 이이는 분실되었거나 오랫동안 시스템에서 떨어져 있던 카메라가 눈에 띄지 않게 다시 추가되는 것을 방지하기 위한 것으로, 그러한 상황은 보안 위험을 초래할 수 있기 때문입니다.

4 데이터 전송 보안

일반적인 사용 시, 비디오와 메타데이터가 포함된 BWC를 교대 근무가 끝난 후 도킹합니다. 모든 데이터는 도킹 스테이션을 통해 HTTPS(TLS가 포함된 HTTP)로 암호화된 네트워크 연결을 사용하여 시스템 컨트롤러로 오프로드됩니다. 데이터는 시스템 컨트롤러의 AES-256 암호화 SSD 저장 장치에 잠시만 저장됩니다. 그런 다음 시스템 컨트롤러는 HTTPS를 사용하여 데이터를 콘텐츠 대상으로 전송합니다.



BWC(1)에서 콘텐츠 목적지(5)로 안전한 데이터 전송 및 저장.

1 *Axis Edge Vault* 탑재 *BWC*
2 *Signed video(*사이버 보안 기능*)*
3 도킹 스테이션
4 *Axis Edge Vault* 탑재 시스템 컨트롤러
5 콘텐츠 대상

콘텐츠 목적지가 공개 암호화 키를 제공하는 경우 콘텐츠 목적지의 암호화 키를 사용하여 BWC 및 시스템 컨트롤러의 데이터를 암호화하는 기능도 지원됩니다. 이 경우 데이터는 콘텐츠 대상에 전송될 때 추가 암호화 계층을 갖게 됩니다.

5 기타 보안 특성

시스템 컨트롤러의 보안과 무결성은 FIPS 140-2를 준수하는 TPM(Trusted Platform Module)을 통해 더욱 강화됩니다.

BWC와 시스템 컨트롤러 모두에는 장치의 모든 데이터를 보호하고 여러 보안 기능을 활성화하는 하드웨어 기반 사이버 보안 플랫폼 Axis Edge Vault가 탑재되어 있습니다. 예를 들어, 파일 시스템은 암호화되고 키는 Axis Edge Vault로 보호됩니다. *Secure boot*는 장치가 승인된 장치 소프트웨어로만 부팅되도록 보장합니다. *Signed OS*는 소프트웨어 무결성이 손상된 경우 업그레이드를 거부하도록 합니다. *Signed video*는 비디오 스트림에 암호화 체크섬을 추가하여 추가적인 보호 계층을 생성합니다. 이를 통해 영상이 생성된 고유 Axis 카메라를 신뢰성 있게 추적할 수 있어 영상이 변조되지 않았는지 확인할 수 있습니다.

Signed video 및 Axis Edge Vault에 대한 자세한 내용은 *developer.axis.com/video-streaming-and-recording/signed-video/* 및 *axis.com/solutions/edge-vault*에서 확인할 수 있습니다

카메라 사용자가 사이트에서 녹화된 비디오를 볼 수 있는 유일한 방법은 AXIS Body Worn Assistant 애플리케이션을 사용하는 것입니다. 애플리케이션이 활성화된 경우, BWC는 애플리케이션으로 직접 비디오를 스트리밍하지만, 애플리케이션을 실행하는 장치의 캐시나 메모리에 비디오 자료가 나중에 액세스할 수 있도록 저장되지 않습니다. 비디오 스트림에는 비디오 캡처를 위한 보조 녹화 장치의 사용을 막기 위한 오버레이도 있습니다. 설화 녹화가 되어도, 비디오 클립에 대해 오버레이를 통해 BWC 사용자를 추적할 수 있습니다. BWC의 USB-C 호환 커넥터는 어떤 방식으로도 비디오를 보거나 삭제하거나 오프로드하는 데 사용할 수 없습니다.

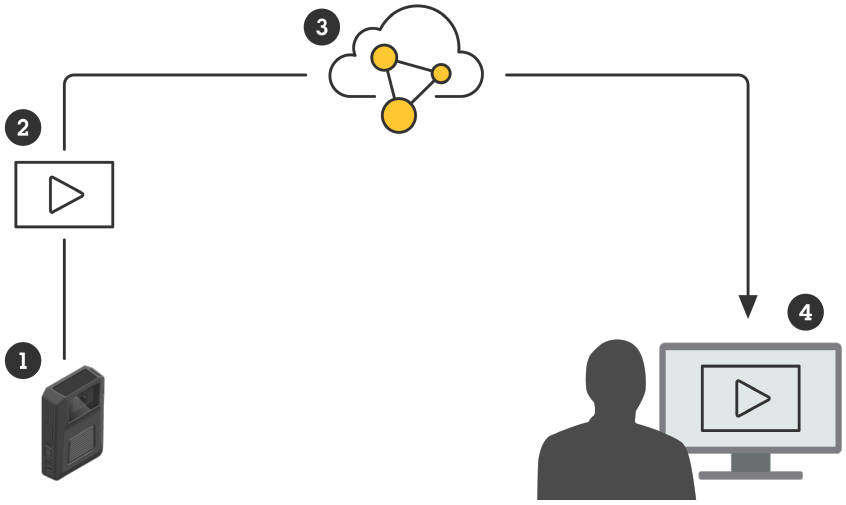
6 AXIS Body Worn Live의 보안

AXIS Body Worn Live는 Axis 신체 착용 카메라의 실시간 데이터에 액세스할 수 있도록 하는 애플리케이션입니다. AXIS Body Worn Live는 비디오, 오디오 및 위치 좌표와 같은 기타 데이터를 실시간으로 스트리밍하여 진행 중인 사건에 대한 비할 데 없는 상황 인식을 제공합니다. 인프라 및 데이터 주권에 관한 다양한 조직의 요구 사항을 충족하기 위해 두 가지 배포 모델로 제공됩니다. Axis에서 호스팅하는 방식과 자체 호스팅 방식으로 제공됩니다.

배포 모델과 관계없이 신체 착용 카메라 시스템의 관리자가 라이브 스트림을 볼 수 있는 대상을 전적으로 제어합니다. 데이터는 관리자가 명시적으로 승인한 뷰어만 비디오를 복호화하여 볼 수 있는 방식으로 암호화됩니다. 또한 관리자는 데이터 무결성을 보호하기 위해 역할에 따라 액세스 권한을 취소할 수 있습니다. Axis에서 호스팅하는 배포에서는 뷰어가 승인된 웹 브라우저와 VMS에 액세스할 수 있어야 하며 올바른 사용자 자격 증명을 갖추어야 합니다. 자체 호스팅 배포에서는 뷰어가 로컬 네트워크에 액세스할 수 있어야 하며 올바른 사용자 자격 증명을 갖추어야 합니다. Axis를 포함한 그 누구도 라이브 스트림에 액세스할 수 없으며, Axis는 사용자가 생성한 엔드 투 엔드 암호화 키에도 액세스할 수 없습니다.

6.1 Axis에서 호스팅하는 배포

클라우드 기반 서비스로 사용할 경우, AXIS Body Worn Live에 호스팅되는 모든 데이터와 파일은 저장 시 AES-256을 사용하여 암호화됩니다. 모든 통신 채널은 신뢰할 수 있는 인증 기관에서 서명한 인증서를 사용하는 TLS가 포함된 HTTPS를 사용하여 보안을 유지합니다. AXIS Body Worn Live는 전송 암호화에 더해 XChaCha20-Poly1305 암호 제품군을 사용한 진정한 엔드 투 엔드 암호화 계층을 추가합니다.



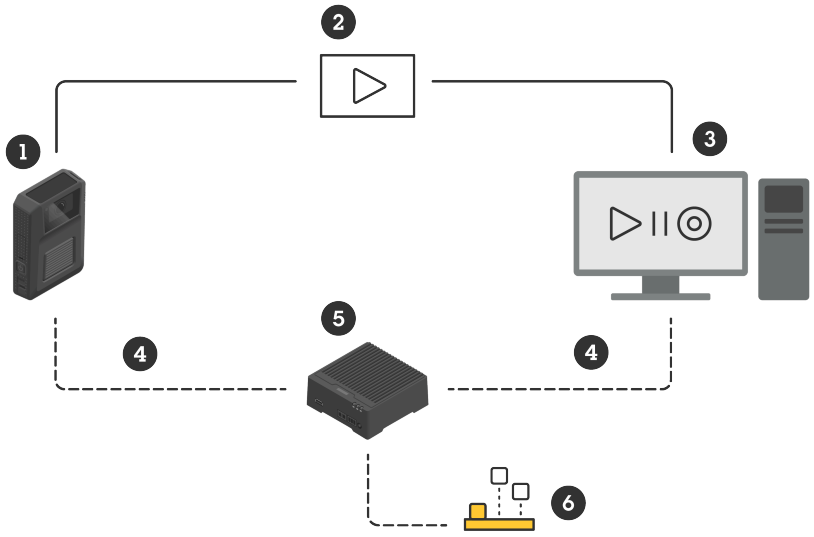
Axis에서 호스팅하는 배포에서 엔드 투 엔드 암호화를 적용한 안전한 라이브 스트리밍

1. 신체 착용 카메라가 실시간 비디오와 기타 데이터를 수집합니다. 데이터는 카메라에서 이미 암호화됩니다.
2. 라이브 스트리밍(엔드 투 엔드 암호화됨).
3. Axis에서 호스팅하는 클라우드. 데이터와 파일은 AES-256을 사용하여 암호화됩니다.
4. 웹 클라이언트. 데이터는 뷰어의 웹 브라우저에서 복호화됩니다.

6.2 자체 호스팅 배포

인프라를 전적으로 자체 통제 네트워크 환경 내에 두어야 하는 엄격한 정책을 시행하는 조직은 서버 애플리케이션인 AXIS BodyWorn Live, Self Hosted를 장치에 로컬로 설치할 수 있습니다. 이 서버 장치로는 AXIS W401 Body Worn Activation Kit 또는 AXIS D3110 Mk II Connectivity Hub를 사용할 수 있습니다. 로컬 서버 장치에는 비디오나 민감한 데이터가 저장되지 않으며, 이 장치는 오로지 연결을 유지하는 역할만 수행합니다. 카메라와 통합 시스템 간에 미디어를 전송하는 통신 채널은 DTLS 1.0 이상 버전을 사용하여 보안을 유지합니다. 서버와 통합 시스템 간에 시그널링 및 이벤트를 전송하는 통신 채널은 고객이 제공한 인증서와 TLS 1.2 이상 버전을 사용하는 HTTPS로 보안을 유지합니다.

자체 호스팅 버전으로 데이터를 스트리밍할 때, 로컬 서버는 서버와 BWC 간에 인증서 기반 인증을 사용하여 WebRTC 시그널링을 안전하게 설정합니다. 연결이 설정되면 BWC와 뷰어의 WebRTC 클라이언트(예: VMS) 사이에 암호화된 피어 투 피어 연결이 직접 형성됩니다. 비디오 스트림은 중간 저장 없이 이 암호화된 연결을 통해 직접 전송되므로 무단 가로채기가 방지됩니다. 이 시스템은 인터넷 액세스 없이 폐쇄된 분할 네트워크에서 작동하도록 설계되어 외부 위협에 대한 공격 표면을 최소화합니다.



자체 호스팅 배포에서의 안전한 라이브 스트리밍

1 신체 착용 카메라가 실시간 비디오와 기타 데이터를 수집합니다. 데이터는 카메라에서 이미 암호화됩니다.
2 피어 투 피어 스트리밍(암호화됨).
3 뷰어의 *WebRTC* 클라이언트.
4 *WebRTC* 시그널링.
5 *AXIS Body Worn Live*, *Self Hosted* 서버 장치.
6 *AXIS Body Worn Live*, *Self Hosted* 서버 앱. *WebRTC* 시그널링을 설정하는 데 사용됩니다.

Axis Communications에 대하여

Axis는 보안, 안전, 운영 효율성 및 비즈니스 인텔리전스를 향상시켜 더 스마트하고 더 안전한 세상을 실현합니다. 네트워크 기술 회사이자 업계 선도 기업인 Axis는 영상 감시, 접근 제어, 인터콤 및 오디오 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 보완되고 고품질 교육을 통해 지원됩니다.

50개 이상의 국가에서 약 5,000명의 Axis 임직원이 전 세계의 기술 및 시스템 통합 파트너와 협력하여 고객에게 최적의 솔루션을 제공하고 있습니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다.

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC 및 VAPIX는 각 관할 지역에서 Axis AB의 등록상표입니다. 모든 다른 상표는 각 소유주의 재산입니다. Axis는 사전 통지 없이 수정할 권리를 갖고 있습니다.