단일 플랫폼의 힘

장기적인 가치, 사이버 보안 및 통합을 위해 특별히 설계된 솔루션

AXIS COMMUNICATIONS

Axis 네트워크 장치의 핵심 기반

AXIS OS는 대부분의 Axis 네트워크 장치에서 사용되는 Linux 기반 운영 체제입니다. 이는 고객 사이트에 배포된 200종 이상의 Axis 제품과 수천만 대 장치의 핵심입니다. Axis OS는 혁신, 안정성 및 원활한 통합을 위한 노력이 반영되어 있습니다. 당사의 장치를 믿을 수 있는 이유와 뛰어난 이미지 품질을 얻을 수 있는 이유가 바로 Axis 소프트웨어 덕분이며, 저희는 매 릴리스마다 Axis 소프트웨어를 개선하고 있습니다. 실제로 저희 연구 개발의 80%는 소프트웨어 개발을 중심으로 이루어지고 있습니다.

저희는 항상 새로운 기능을 추가하고 기존 기능을 개선하기 위해 노력하고 있습니다. 또한 AXIS OS 기반 장치에 대한 취약점 패치를 통해 지속적으로 보안을 강화하고, 더 많은 사용 사례를 더 안전하게 해결할 수 있도록 개선하고 있습니다.

AXIS OS는 네트워크 장치에서 가장 중요한 기준인 장기적인 가치, 높은 사이버 보안 표준, 통합 용이성을 충족하도록 특별히 설계되었습니다.

Axis 장치 전용으로 설계
AXIS OS 개발 조직에서 구축하고 Linux Yocto OpenEmbedded의 안정성에 기반을 둔 AXIS OS는 일반적인 빌드를 능가하여 카메라, 스피커 및 접근 제어 장비와 같은 Axis 에지 장치의 고유한 요구 사항에 완벽하게 최적화되어 있습니다.

장기적인 가치
AXIS OS는 장치가 항상 켜져 있도록 보장합니다. 연중무휴 작동하도록 설계되어 있어 낮과 밤을 가리지 않고 애플리케이션의 요구사항에 맞춰 일관되고 빠른 응답 성능을 제공합니다.

견고한 사이버 보안
AXIS OS의 핵심은 사이버 보안에 대한 전념입니다. 보안 아키텍처가 내장된 AXIS OS를 사용하면 장치를 안전하게 보호할 수 있습니다. 안전한 소프트웨어 개발 관행과 철저한 취약성 관리를 통해 AXIS OS는 데이터와 장치가 새로운 위협에 맞서 복원력을 유지하도록 보장합니다.

원활한 통합
AXIS OS는 VAPIX, ONVIF 등을 통합하여 Axis 네트워크 장치를 다양한 에코시스템에 쉽게 통합할 수 있도록 지원합니다. 이러한 통합성은 사용자와 개발자에게 원활하고 상호 연결된 경험을 제공합니다.

수치로 보는 AXIS OS

900명의 개발자

24,000,000줄의 코드 작성

매일 **4,000개의** 코드 커밋

매일 **4,000,000**건의 자동 테스트

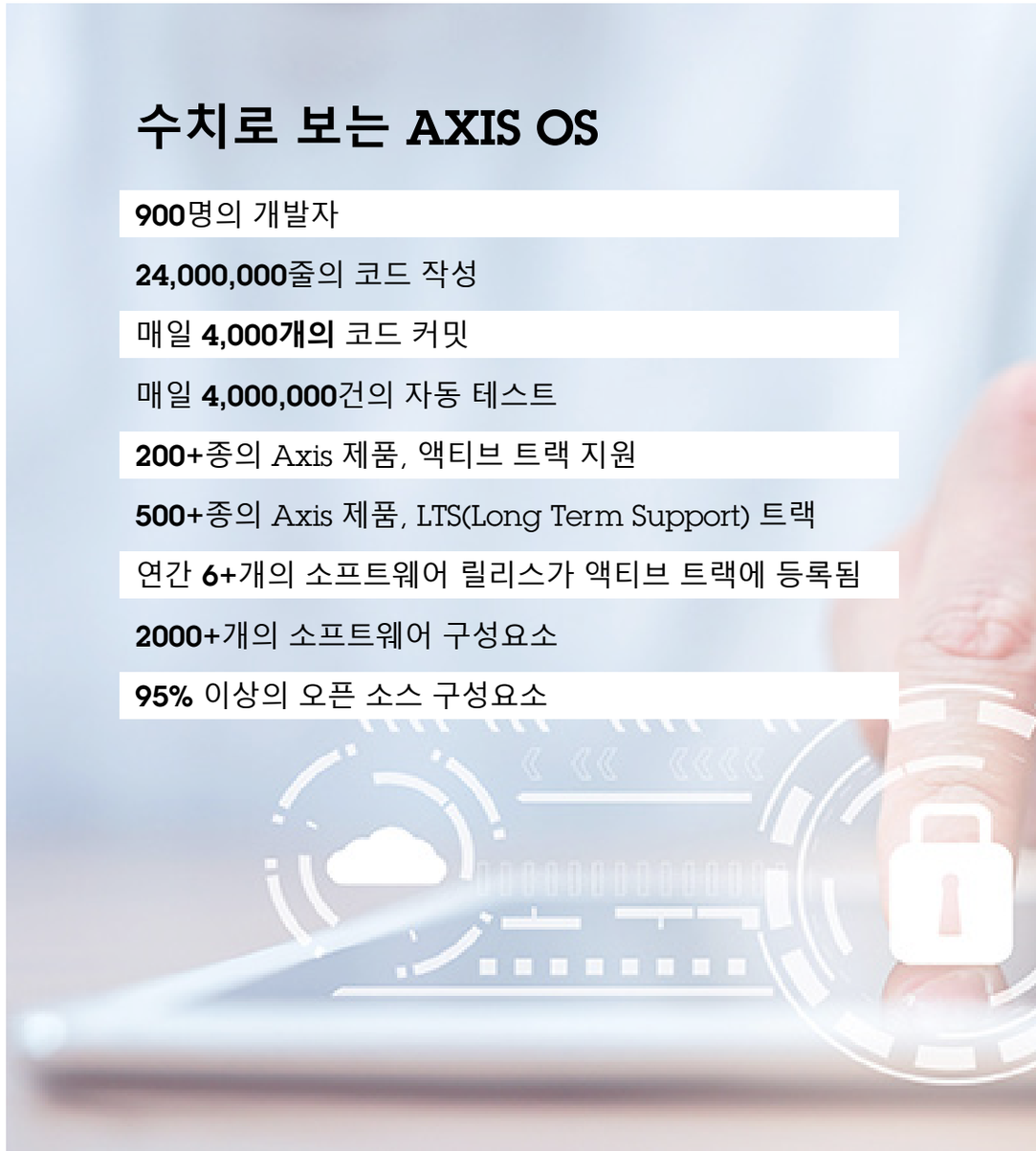
200+종의 Axis 제품, 액티브 트랙 지원

500+종의 Axis 제품, LTS(Long Term Support) 트랙

연간 **6+**개의 소프트웨어 릴리스가 액티브 트랙에 등록됨

2000+개의 소프트웨어 구성요소

95% 이상의 오픈 소스 구성요소



Axis 장치 전용으로 설계

당사는 AXIS OS를 설계할 때 특히 에지 장치의 성능, 통합, 보안 및 소프트웨어 품질에 중점을 두었습니다.

Linux Yocto OpenEmbedded의 안정성에 뿌리를 둔 AXIS OS는 모든 Axis 네트워크 장치를 위한 단일 통합 플랫폼을 제공하여 다양한 제품군에서 일관된 경험을 제공합니다.

다음 페이지에서 에지 장치를 위해 특별히 제작된 운영 체제의 가치와 하나의 플랫폼이 가진 힘에 대해 자세히 알아볼 수 있습니다.

탁월한 에지 환경을 위한 제작

범용 솔루션이 지배하는 환경에서 AXIS OS는 단순한 Linux 운영 체제가 아닙니다. 일반적인 Linux 빌드의 관습을 뛰어넘어 에지 장치의 특정 요구 사항에 맞게 세밀하게 조정된 솔루션을 제공합니다. 이러한 전문화는 Axis 제품 고유의 성능, 안정성 및 보안을 지원합니다.

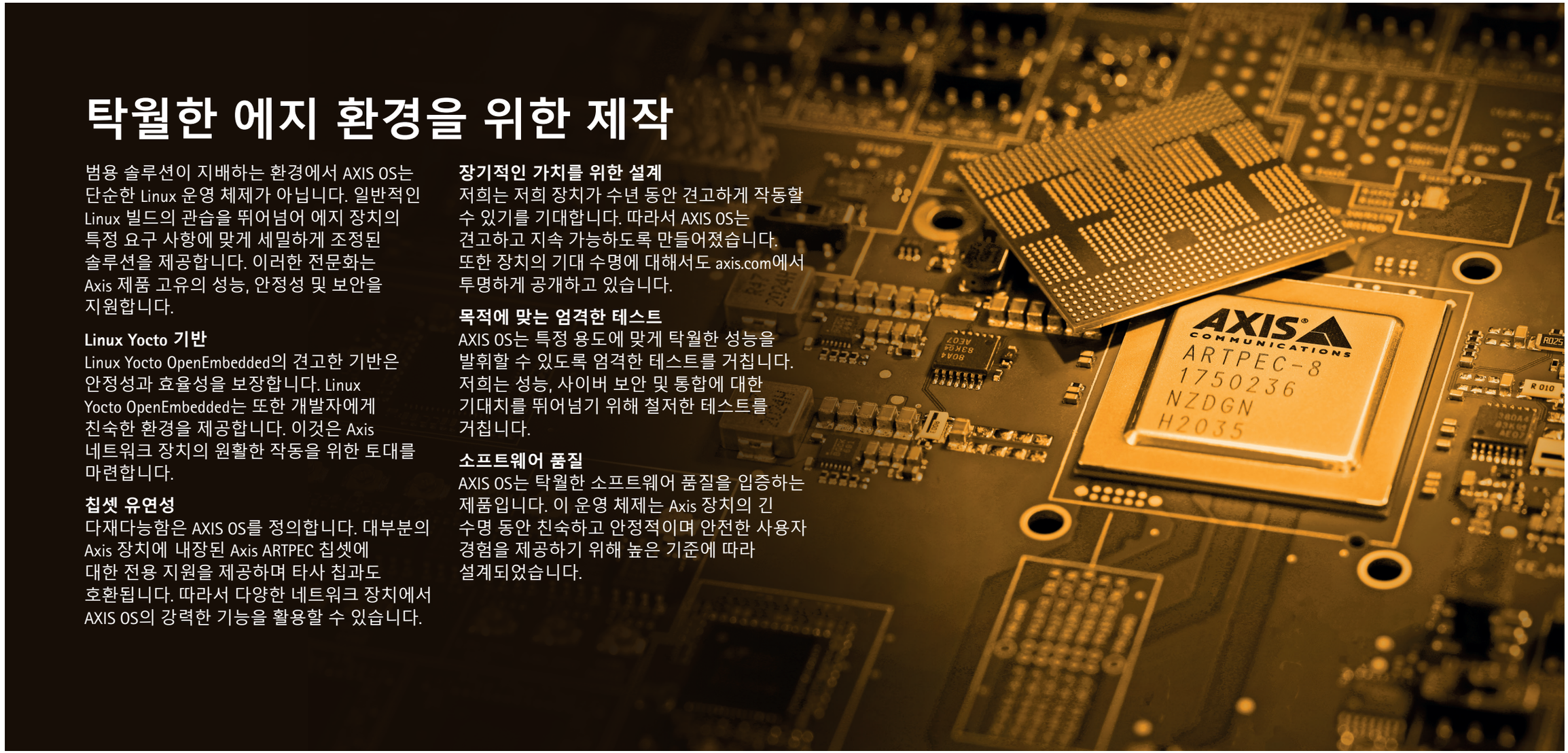
Linux Yocto 기반
Linux Yocto OpenEmbedded의 견고한 기반은 안정성과 효율성을 보장합니다. Linux Yocto OpenEmbedded는 또한 개발자에게 친숙한 환경을 제공합니다. 이것은 Axis 네트워크 장치의 원활한 작동을 위한 토대를 마련합니다.

칩셋 유연성
다재다능함은 AXIS OS를 정의합니다. 대부분의 Axis 장치에 내장된 Axis ARTPEC 칩셋에 대한 전용 지원을 제공하며 타사 칩과도 호환됩니다. 따라서 다양한 네트워크 장치에서 AXIS OS의 강력한 기능을 활용할 수 있습니다.

장기적인 가치를 위한 설계
저희는 저희 장치가 수년 동안 견고하게 작동할 수 있기를 기대합니다. 따라서 AXIS OS는 견고하고 지속 가능하도록 만들어졌습니다. 또한 장치의 기대 수명에 대해서도 axis.com에서 투명하게 공개하고 있습니다.

목적에 맞는 엄격한 테스트
AXIS OS는 특정 용도에 맞게 탁월한 성능을 발휘할 수 있도록 엄격한 테스트를 거칩니다. 저희는 성능, 사이버 보안 및 통합에 대한 기대치를 뛰어넘기 위해 철저한 테스트를 거칩니다.

소프트웨어 품질
AXIS OS는 탁월한 소프트웨어 품질을 입증하는 제품입니다. 이 운영 체제는 Axis 장치의 긴 수명 동안 친숙하고 안정적이며 안전한 사용자 경험을 제공하기 위해 높은 기준에 따라 설계되었습니다.



단일 플랫폼의 힘

우수성을 향한 Axis의 노력은 제품 카테고리를 뛰어넘어 단일 플랫폼의 힘으로 구체화됩니다. 신체 착용 카메라부터 방폭 솔루션, PTZ 카메라부터 사이렌, 스피커부터 인터콤까지 200종 이상의 제품을 지원하는 당사의 통합 플랫폼은 파트너와 고객의 만족을 염두에 두고 설계되었습니다.

작업의 일관성
AXIS OS는 다양한 제품군에 걸쳐 제공됩니다. 당사의 모든 제품에서 동일한 API와 동작이 공유됩니다. 통합업체와 개발자는 하나의 플랫폼으로 복잡한 장치별 드라이버 없이도 새로운 Axis 장치를 시스템에 통합할 수 있습니다. 이를 통해 통합을 가속화할 뿐만 아니라 미래 보장형 솔루션을 제공하여 끊임없이 확장하는 Axis 생태계 내에서 새로운 제품을 신속하게 채택할 수 있습니다. 최종 고객에게 일관된 경험을 보장합니다. 또한 모든 통합 솔루션이 모든 AXIS OS 장치에서 작동하므로 개발자의 시간과 비용을 절약할 수 있습니다.

복잡하지 않은 다재다능함
단일 플랫폼의 힘은 복잡성 없이 다양성이 제공되는 단일 플랫폼이라는 점에서도 찾을 수 있습니다. PTZ 카메라를 감시 시스템에 통합하든, 스피커를 지능형 오디오 솔루션에 통합하든, 프로세스는 일관적입니다. 이러한 다양성은 호환성을 넘어 조화로운 경험과 고유한 요구사항에 맞춘 통합 솔루션을 만들 수 있는 다양한 가능성을 제공합니다.

통합된 보안
사이버 보안이 가장 중요한 세상에서 하나의 플랫폼의 힘은 전체 제품 스펙트럼에 걸쳐 통합 솔루션을 지원한다는 점에서도 찾을 수 있습니다. 보안을 유지하는 것은 제품별 사안이 아닙니다. 취약점이 식별되어 해결되면 지원되는 모든 제품에 수정 사항이 전파됩니다. 이를 통해 보안 관리를 간소화할 뿐만 아니라 새로운 위협에 신속하고 집단적으로 대응할 수 있습니다. 또한 시간과 리소스를 절약하고 전체 Axis 에코시스템의 복원력을 강화합니다.

장기적인 가치

AXIS OS는 장치의 수명 주기 전반에 걸쳐 예측 가능한 가치를 지원합니다. 안정적이고 견고한 아키텍처로 가동 중지 시간을 최소화합니다.

새로운 기능을 포함한 소프트웨어 업데이트를 수년에 걸쳐 제공합니다. 광범위한 문서, 유용한 도구, 직관적인 인터페이스를 갖춘 Axis 장치는 사용이 간편하고 유지 관리가 쉽습니다. 또한 투명하고 신뢰할 수 있는 릴리스 일정을 제공하므로 조직의 필요에 맞게 유지 관리를 계획할 수 있습니다.

다음 페이지에서 Axis 소프트웨어의 품질, AXIS OS 수명 주기 관리 및 소프트웨어 지원에 대해 자세히 알아볼 수 있습니다.

신뢰할 수 있는 소프트웨어

AXIS OS의 품질은 우리에게 매우 중요합니다. 매일 약 900명의 개발자와 4,000개의 코드 커밋이 AXIS OS 메인 브랜치에 투입되는 가운데, 당사의 운영 체제는 시장의 요구에 맞춰 지속적으로 변화하고 있습니다. 200종이 넘는 제품 각각에 대해 하루에 두 번의 빌드를 수용한다는 것은 연간 182,500개의 빌드를 처리한다는 의미이며, 이를 통해 반복적인 테스트와 부가가치를 창출할 수 있습니다.

엄격한 테스트

소프트웨어 안정성을 유지하려면 엄격한 테스트도 필요합니다. 실제로 저희 시스템은 매일 4백만 건에 달하는 다양한 테스트 케이스를 실행하고 있습니다. 취약점을 패치하고 품질을 개선하기 위해 매일 4,000개 이상의 코드 커밋을 통해 이를 보완하고 있습니다. 이것은 매년 10억 건 이상의 테스트와 1,000,000건 이상의 코드 커밋이 수행됨을 의미합니다. 또한 데이터 공유를 통해 고객과 파트너가 AXIS OS에 대한 직접적인 피드백을 제공할 수 있습니다.

지속적인 개선

AXIS OS는 정적이지 않습니다. 항상 개선하기 때문에 역동적입니다. AXIS OS 액티브 트랙의 Axis 장치는 정기적인 업데이트와 개선을 통해 기술 발전과 함께 진화하고 있습니다. 즉, 오늘 구입한 제품은 평생 동안 새로운 기능을 추가하고 더 가치 있는 제품이 될 수 있습니다.

장치의 수명 주기 지원

AXIS OS 사용 시 이점 중 하나는 설치부터 유지보수, 교체에 이르는 장치 수명 주기를 지원한다는 점입니다. AXIS OS는 수명이 다할 때까지 Axis 장치를 관리하고 최적화하는 데 도움이 되는 도구와 리소스를 제공합니다.

손쉬운 설치 및 구성
AXIS OS는 프로세스를 안내하는 마법사, 템플릿 및 프로파일을 제공하여 Axis 장치의 설치 및 구성을 간소화합니다. 또한, AXIS Device Manager(ADM) 및 AXIS Device Manager Extend(ADMX)를 사용하여 여러 장치를 한 번에 설치하고 구성할 수 있으므로 시간과 노력을 절약할 수 있습니다.

지속적인 모니터링과 진단
사용자의 동의가 있는 경우, AXIS OS는 로그, 보고서 및 경고의 형태로 상태 모니터링 데이터를 수집하여 Axis 장치의 성능 및 상태를 모니터링하고 분석합니다. 이를 통해 문제를 식별하고 해결할 수 있습니다. 또한 릴리스할 때마다 소프트웨어를 개선할 수 있습니다.

장기적인 지원 및 호환성
AXIS OS는 정기적인 보안 패치 및 버그 수정을 통해 Axis 장치에 대한 장기적인 지원을 제공합니다. Axis의 장기적인 지원은 변경 및 중단을 최소화하여 Axis 장치 및 애플리케이션의 호환성을 추적합니다. AXIS OS에서 실행되는 장치의 수명은 일반적으로 약 10년 이상입니다. 경우에 따라 최대 13년 동안 지원하기도 합니다.

신뢰와 약속
AXIS OS는 신뢰와 품질을 중시하는 고객의 기대와 요구를 충족하도록 설계되었습니다. AXIS OS는 각 제품에 대해 명확하고 투명한 기대 수명을 설정하고 이를 최대한 준수합니다. Axis는 또한 고객에게 최상의 서비스와 지원을 제공함으로써 장기적인 관계를 유지합니다.

AXIS OS 베타

AXIS OS 베타는 공식 출시 전에 AXIS OS의 최신 기능을 테스트하고 평가하고자 하는 개발자와 통합업체를 위한 혜택입니다. AXIS OS 베타를 사용하여 선택한 장치에서 초기 호환성 테스트를 수행하고, 예정된 보안 업데이트를 확인하고, 향후 출시될 기능에 액세스할 수 있습니다.

AXIS OS 베타를 사용하면 다음과 같은 이점이 있습니다.

> 에지 분석, IoT 연결, 플랫폼 모듈화 등 향후 AXIS OS가 제공할 새롭고 개선된 기능 미리 보기.
> AXIS OS의 개발 및 개선에 도움이 되는 피드백과 제안을 Axis에 제공할 수 있음.
> 잠재적인 문제를 방지하기 위해 애플리케이션과 시스템을 AXIS OS의 향후 변경 및 업데이트에 대비하고 적응시킬 수 있음.

AXIS OS 베타에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

AXIS OS 수명 주기 소프트웨어 지원

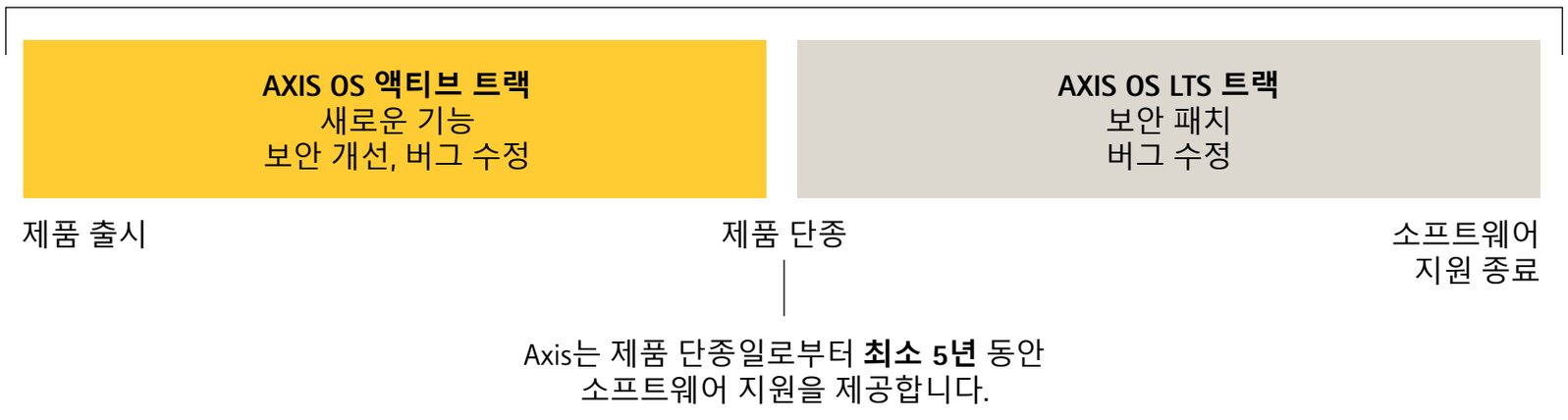
AXIS OS 수명 주기 지원은 다양한 트랙으로 구성됩니다. 액티브 트랙과 장기지원(LTS) 트랙이 주요 트랙입니다. 개별 제품 수명 주기를 지원하기 위한 제품별 지원 트랙(PSS)도 있습니다.

Axis 장치의 최소 수명은 업계 표준을 초과합니다. 강력한 5년 하드웨어 보증은 수년에 걸친 AXIS OS 소프트웨어 지원으로 보완됩니다. 대부분의 장치는 8~12년이라는 인상적인 AXIS OS 수명을 제공합니다.

작동 방식은 다음과 같습니다.

1. Axis가 새 장치를 출시하면, AXIS OS 액티브 트랙만 사용할 수 있습니다. 출시 후 초기 기간 동안에는 새로운 기능을 포함한 지속적인 업데이트와 개선 사항의 혜택을 누릴 수 있습니다.
2. 제품 출시 후 2년 이내에 액티브 트랙의 대안으로 LTS(Long Term Support) 트랙을 사용할 수 있습니다. 이 시점에서 액티브 트랙 또는 LTS(long-term support) 중 하나를 선택할 수 있습니다. LTS(long-term support) 대상 제품은 패치 및 버그 수정으로만 지원됩니다.
3. 출시 후 2~4년이 지나 장치가 단종되면, 해당 장치의 액티브 트랙도 단종됩니다. 이 시점에서 모든 장치는 자동으로 LTS(Long Term Support) 트랙으로 이동되어 최소 5년 동안 패치 및 버그 수정이 지원됩니다.

AXIS OS 수명 주기 소프트웨어 지원



Axis는 제품 단종일로부터 **최소 5년** 동안 소프트웨어 지원을 제공합니다.

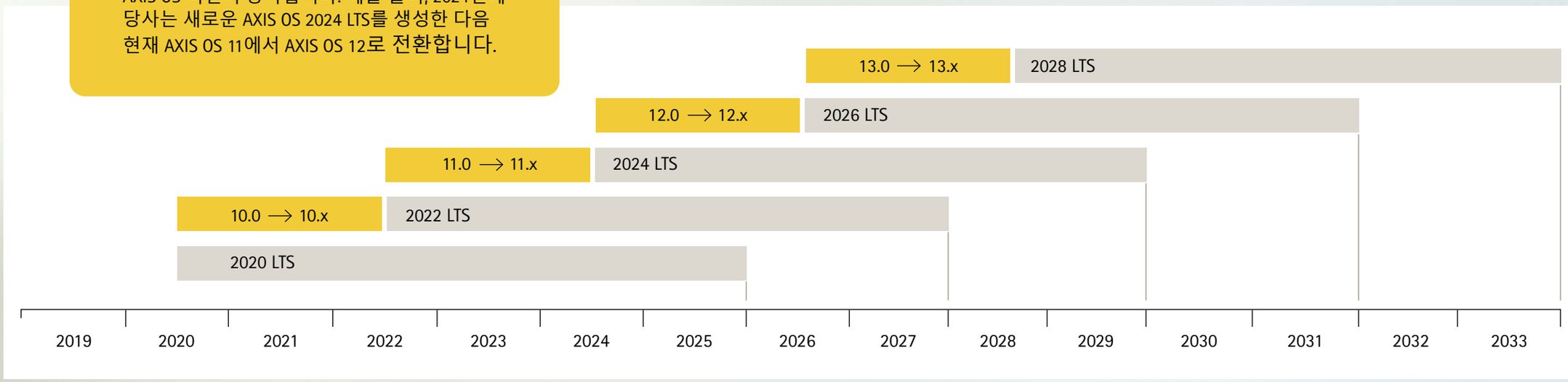
어떤 소프트웨어 지원 트랙이 나에게 적합할까요?

액티브 트랙과 LTS 트랙을 모두 사용할 수 있게 되면 고객은 Axis의 안내에 따라 자신의 필요에 가장 적합한 트랙을 선택할 수 있습니다.

액티브 트랙
AXIS OS 액티브 트랙은 AXIS OS 운영 체제를 위한 가장 최신의 풍부한 기능을 제공합니다. 최신 기능 및 개선 사항을 즉시 이용하고자 하는 고객을 위해 맞춤화된 이 트랙은 새로 출시된 장치만 이용할 수 있습니다. 사용자가 진화하는 장치의 기능을 파악할 수 있도록 도와줍니다. 보다 안전한 운영을 위해 새로운 사이버 보안 기능이 추가되고 기존 기능은 지속적으로 개선됩니다. AXIS OS 액티브 트랙의 장치를 사용하면 제품을 구입한 지 몇 년이 지난 후에도 추가 비용 없이 제품을 더 많이 활용할 수 있습니다. 호환성 종속이 없는 경우, 이 트랙이 제공되는 동안에는 당신에게 가장 적합한 트랙입니다.

LTS(Long Term Support) 트랙
API 일관성 및 호환성을 원하는 경우, LTS(Long Term Support) 트랙이 제공되면 이를 선택하는 것이 좋습니다. LTS 트랙은 이전 버전과의 호환성에 포커스를 맞추고 있으며 정기적인 보안 패치와 버그 수정을 제공합니다. 새로운 보안 기능을 제공하기보다는 사이버 보안을 유지합니다. 마찬가지로 새로운 기능이나 기능을 추가하는 것이 아니라 변경 사항을 최소화하여 혼란을 줄입니다. LTS 트랙은 신뢰와 품질을 중시하고 타사 시스템과 잘 통합되기를 원하는 고객에게 적합합니다. 각 LTS 트랙은 5년 동안 지원되며, 정기적인 액티브 트랙 릴리스를 기준으로 24개월마다 LTS 트랙이 발급됩니다. 모든 장치는 단종 시 자동으로 LTS 트랙으로 이동합니다.

아래 그림은 수년에 걸쳐 도입된 LTS 트랙과 함께 AXIS OS 액티브 트랙을 나란히 보여줍니다. 대략 24개월마다 새로운 LTS 트랙이 생성되고 주요 AXIS OS 버전이 증가합니다. 예를 들어, 2024년에 당사는 새로운 AXIS OS 2024 LTS를 생성한 다음 현재 AXIS OS 11에서 AXIS OS 12로 전환합니다.



ASDM
내장형 사이버보안
취약성 관리
올인원

사이버 보안에 대한 포커스

AXIS OS는 설계에 따른 보안 접근 방식을 준수합니다. 당사의 Axis Security Development Model(ASDM)은 소프트웨어 개발 중에, 그리고 그 이후의 취약성 위험을 줄이는 프로세스 및 도구를 정의합니다.

하드웨어 기반 사이버 보안 플랫폼인 Axis Edge Vault는 보안 부팅(Secure boot)과 고객이 로딩한 암호화 키 저장을 위한 훼손 방지 환경을 보장합니다. AXIS OS 핵심 소프트웨어는 충분한 테스트를 거친 오픈 소스 구성 요소로 이루어져 있습니다. 또한 모든 릴리스에는 AXIS OS가 최신 상태이며 알려진 취약점에 대한 패치가 적용되었음을 보여주는 소프트웨어 구성품 명세서(SBOM)가 포함되어 있습니다.

또한 AXIS OS는 에지 장치 보안에 중점을 둔 ETSI EN 303 645를 준수하고 인증을 받았습니다. FIPS 140 준수를 통해 AXIS OS는 미국 국립표준기술연구소(NIST)에서 정의한 최신 암호화 표준을 준수합니다. 마지막으로, 당사는 승인된 CVE 번호 지정 기관으로서 취약점을 식별, 관리 및 공개하는 모범 사례를 따릅니다.

다음 페이지에서 Axis 보안 개발 모델, Axis Edge Vault, 취약성 관리 및 통합 보안의 개념에 대해 자세히 알아볼 수 있습니다.

보안을 염두에 두고 개발

Axis 보안 개발 모델(ASDM)은 사이버 보안을 소프트웨어 개발 수명 주기에 효과적으로 통합합니다. 이것은 소프트웨어 개발 단계에서 고려해야 할 보안 활동에 대해 설명합니다. 그 목적은 사이버 보안을 위한 베이스 라인을 설정하고 지침을 제공하여 취약점과 개발 비용을 줄이는 것입니다.

ASDM: Axis에서 제작

Axis Security Development Model은 표준 "기성품" 프레임워크가 아닙니다. 대신 ISO 27001, IEC 62443, NIST, BSIMM, CMMC 등 다양한 사이버 보안 표준과 프레임워크를 검토했습니다. 이 둘의 공통점은 모든 개발 단계에 보안이 통합되어 있다는 점입니다. 이를 출발점으로 삼아 회사 문화, 개발 관행, 제공하는 제품 유형에 맞게 모델을 조정했습니다.

ASDM 도구 상자

ASDM 도구 상자에는 다양한 보안 문제를 해결하는 다양한 활동이 규정되어 있습니다. 위험 평가, 위협 모델링, 위협 모델 테스트, 정적 코드 분석, 취약성 스캔, 공급업체 평가 등이 그 예입니다. 개발팀은 개발할 소프트웨어의 종류에 따라 어떤 활동에 참여할지 선택합니다. 목표는 단순히 프로세스를 준수하는 것이 아니라 사이버 보안을 강화하는 것입니다.

외부 전문 지식의 추가적인 이점

보안 소프트웨어 개발의 무거운 작업은 대부분 Axis R&D와 소프트웨어 엔지니어가 수행합니다. 하지만 우리는 다른 사람의 지식과 전문성을 통해 도움을 받을 수 있다는 사실도 잘 알고 있습니다. 그래서 저희는 침투 테스트를 위해 전문 업체를 고용하고 있습니다. 또한 취약점을 식별하는 데 도움을 준 보안 연구원에게 금전적 보상을 제공하는 AXIS OS 버그 바운티 프로그램을 운영하고 있습니다.

거버넌스 | **훈련** | **ASDM 라인 미팅** | **ASDM 평가** | **보안 규정 준수 및 표준**

요구 사항	설계	구현	검증	배치
위험 평가 벤더 평가 정보 보호 오픈 소스 보안 평가	위협 모델링	정적 코드 분석 소프트웨어 구성 분석	위협 모델 테스트 외부 침투 테스트 취약점 검사 내부 보안 평가	취약성 관리 사고 관리 제품/솔루션 보안 상태 버그 바운티 프로그램

내장형 사이버보안

내부로부터 시작되는 보호
Axis Edge Vault는 당사의 하드웨어 기반 사이버 보안 플랫폼입니다. Axis 장치가 네트워크의 신뢰할 수 있고 안정적인 일부가 될 수 있도록 견고한 기반을 제공합니다. 하지만 이 강력한 하드웨어 기반은 그 잠재력을 최대한 지원하는 운영 체제가 없다면 소용이 없을 것입니다. AXIS OS는 Edge Vault 플랫폼을 사용하여 모든 사용 사례에 대해 에지에서 향상된 보안을 제공합니다.

Edge Vault에는 다음과 같은 기능이 내장되어 있습니다.

안전한 키 보관
보안 키 스토리지에는 암호화 키의 안전한 저장 및 컴퓨팅을 위한 암호화 컴퓨팅 모듈이 포함됩니다. 장치가 손상된 경우에도 장치의 신원 및 기타 민감한 정보가 무단 액세스되지 않도록 보호합니다. 사용되는 암호화 컴퓨팅 모듈은 시스템 온 칩(SoC)에 내장된 신뢰할 수 있는 실행 환경과 전용 보안 요소 또는 인쇄 회로 기판(PCB)에 있는 별도의 칩인 신뢰할 수 있는 플랫폼 모듈(TPM 2.0)입니다.

Signed OS 및 Secure boot
Signed OS(서명된 OS)는 장치 소프트웨어 이미지에 코드 서명을 한다는 의미입니다. Signed OS와 Secure boot를 함께 사용하면 장치는 정품 AXIS OS 운영 체제만 다운로드하여 실행할 수 있습니다. 이것은 소프트웨어 및 하드웨어 공급망의 훼손을 방지하기 위한 추가적인 보호 계층입니다.

Axis device ID
Axis 장치 ID는 IEEE 802.1AR을 준수하며 네트워크에서 장치를 안전하게 식별하고 온보딩할 수 있게 지원합니다. 제조된 모든 Axis 장치에 대한 여권 역할을 한다고 볼 수 있습니다.

암호화된 파일 시스템
파일 시스템 암호화는 시스템 통합업체에서 최종 고객으로 전송되는 동안과 같이 장치를 사용하지 않는 동안 파일 시스템의 데이터가 추출되거나 훼손되지 않도록 보호합니다.

Signed video(서명된 비디오)
Signed video를 통해 사용자는 캡처한 동영상의 진위 여부와 훼손되지 않았음을 확인할 수 있습니다.

Axis Edge Vault 사이버 보안 플랫폼

암호화 컴퓨팅 모듈	특징	사용 사례
보안 요소 TPM 2.0 SoC 보안(TEE)	Secure boot Signed OS Axis device ID 보안 키 저장소 Signed video 암호화된 파일 시스템	신뢰할 수 있는 장치 ID 안전한 키 보관 비디오 변조 감지 공급망 보호

*참고: 모든 장치 모델이 모든 Axis Edge Vault 기능을 지원하는 것은 아닙니다. 특정 제품에서 지원되는 기능을 확인하려면 데이터시트 또는 Axis 제품 선택기를 확인하십시오.

취약성 관리

저희는 고객의 노출 위험을 최소화하기 위해 취약점을 투명하게 관리하고 대응하는 업계 모범 사례를 따릅니다.

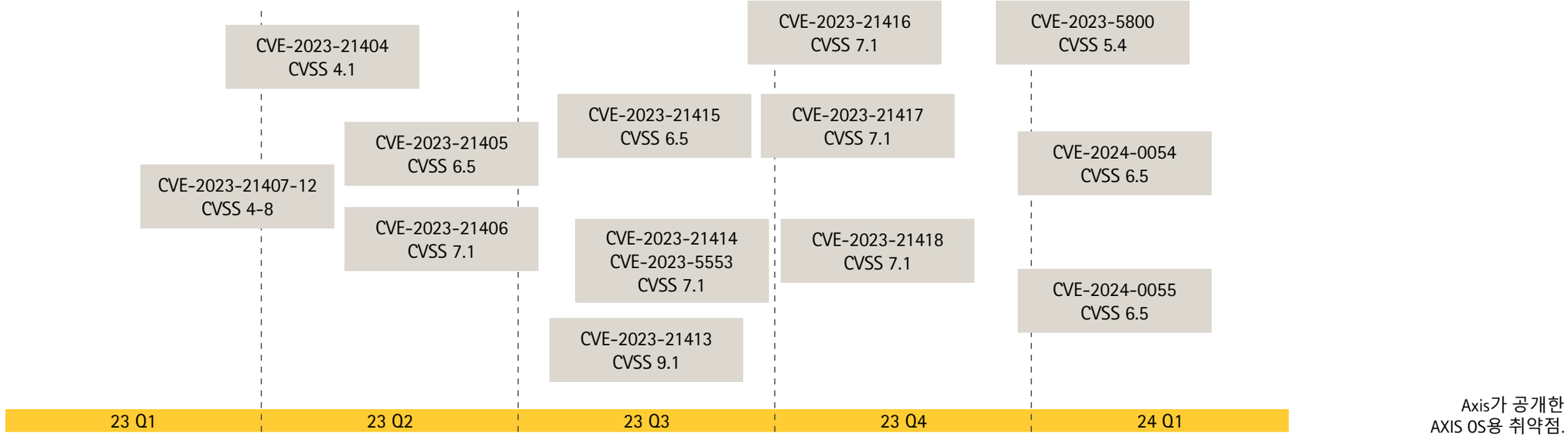
업계 최고의 취약성 관리
Axis에서 제공하는 제품 및 서비스에 취약점이 전혀 없다고 보장할 수 있는 방법은 없습니다. 이는 저희만의 문제가 아니라 모든 소프트웨어와 서비스에 공통적으로 적용되는 조건입니다. 그러나 Axis는 모든 단계에서 잠재적인 취약성을 식별하고 완화하여 고객 환경에 Axis 제품 및 서비스를 배포하는 데 따르는 위험을 줄이기 위해 공동으로 노력하고 있습니다.

CVE 번호 부여 기관,
Axis는 CVE 번호 부여 기관(CNA)입니다. 저희는 취약점 관리 개선을 위해 같은 생각을 가진 기업들과 협력하기 위해 CVE 프로그램에 가입했습니다. Dropbox는 취약점을 처리, 공개 및 패치하는 방식을 이 비영리 단체가 제공하는 국제 프레임워크 및 Dropbox의 공공 취약점 관리 정책에 부합하도록 조정합니다.

신뢰할 수 있는 투명한 관리
Axis는 잘 알려진 CVSS 평가 시스템(Common Vulnerability Scoring System)을 사용하여 Axis에서 개발한 코드 또는 타사 오픈 소스 코드와 관련된 취약점을 평가합니다. 당사는 모범 관행 권장 사항이 적용될 때 Axis 제품과 얼마나 관련이 있는가 하는 것에 따라 오픈 소스 코드의 취약점을 평가합니다. Axis 보안 알림 서비스(Axis Security Notification Service)에 가입하면 Axis 제품에 대한 취약점 및 기타 보안 관련 문제에 대한 정보를 받을 수 있습니다.

보안 연구자 및 조직과의 파트너십
Axis는 취약점 발견을 보고하기 위해 당사에 연락하는 개인 보안 연구자 및 보안 연구 단체의 노력을 수용하고 감사하게 생각합니다. 저희는 주저하지 않고 이를 공개하고 패치합니다. 취약점이 어떻게 발견되더라도 윤리적이고 책임감 있는 공개 프로세스를 통해 정확하고 투명하게 취약점을 처리하는 것이 중요합니다.

AXIS OS 취약점



Axis가 공개한 AXIS OS용 취약점.

올인원 보안 경험

AXIS OS 기반 네트워크 장치에서 하드웨어 및 소프트웨어 구성 요소는 함께 연동하여 고객이 장치, 서비스 및 연결된 시스템을 안전하게 운영할 수 있도록 지원합니다. 보안 기반과 하드웨어 기반 보안 플랫폼에서 시작하여 소프트웨어까지 포괄적인 보호 계층이 이어집니다. AXIS OS 기반 장치는 사이버 보안에 대한 이러한 계층화된 심층 방어 접근 방식을 통해 보호됩니다. 데이터, 애플리케이션, 프로세스의 누적 보안을 강화합니다.

따라서 Axis 장치를 어떤 용도로 사용하든 보호 및 보안 통신이 가능하므로 타사 시스템과 적절하고 안전하게 통합할 수 있습니다.

접근 제어

접근 제어 관리
패스워드 복잡도 표시기를 통한 로컬 사용자 장치 관리
패스워드 복잡성 적용, 순환, 자동 계정 잠금 해제, 다단계 인증(MFA), Microsoft AD 권한 부여 기능과 같은 기능을 잠금 해제하는 ADFS 통합을 제공하는 OpenID Connect(RFC6749, 1.3.1 인증 코드)를 통한 페더레이션 사용자 장치 관리

프라이버시
진단 데이터 사용
저장해야 하는 고객별 데이터의 양에 대한 최소한의 접근 방식

애플리케이션

애플리케이션 보안
TLS 기반 애플리케이션 보안(MQTT, SFTP, NTS, HTTPS, WebRTC)
암호화된 비디오 스트리밍(RTSPS/SRTP, HTTPS), 보안 원격 syslog

운영 체제

암호화 및 데이터 보호
OpenSSL 1.1.1 및 3.0
X.509 인증서 PKI 암호화
전송 계층 보안(TLS 1.2/TLS 1.3)
SD 카드 암호화(AES-XTS-Plain64 256비트)
암호화된 파일 시스템(AES-XTS-Plain64 256비트)
Signed video(서명된 비디오)

기본 보안
기본 설정으로 HTTPS 활성화
무차별 대입 지연 보호
호스트 기반 방화벽
네트워크 시간 보안(NTS)
보안되지 않은 TLS 버전 비활성화됨
UART/디버그 포트 비활성화됨

기업 네트워크 보안
IEEE 802.1X(네트워크 액세스 제어)
IEEE 802.1AR(보안 장치 ID)
IEEE 802.1AE(MAC 보안, MACsec)

AXIS OS 운영 체제
95% 이상의 업계 표준 오픈 소스 소프트웨어 구성 요소(예: OpenSSL, Apache, Curl 등)가 포함된 일반적인 Linux 기반 운영 체제입니다. 기능 성장을 위한 액티브 트랙과 타사 통합 및 이전 버전과의 호환성 사용 사례를 위한 5년의 LTS(Long Term Support) 트랙이 제공됩니다.

실리콘 지원 보안(칩)

하드웨어 신뢰 루트
ARM 기반 시스템 온 칩(SoC) 보안
신뢰할 수 있는 실행 환경(TEE/OP-TEE)
신뢰할 수 있는 플랫폼 모듈(TPM 2.0), 보안 요소

안전한 키 보관
고객이 업로드한 개인 키, 비디오 서명 키 및 Axis 장치 ID와 같은 암호화 키의 훼손 방지 저장 및 작동.

보안 기초

Axis 보안 개발 모델
Axis 보안 개발 모델(ASDM)
타사 침투 테스트
Bugcrowd와 함께하는 버그 바운티 프로그램
소프트웨어 구성품 명세서(SBOM)

규정 준수
Common Criterial EAL
FIPS 140
ETSI EN 303 645

신뢰할 수 있는 장치 ID
Axis Edge Vault 사이버 보안 플랫폼
Signed OS를 활용한 Secure boot(코드 서명)
Axis 장치 ID (IEEE 802.1AR)

세계적 수준의 통합

통합은 Axis 제품에서 중추적인 역할을 합니다. 저희는 다양한 애플리케이션에 걸쳐 손쉬운 통합을 지원하는 강력하고 일관된 API를 제공하기 위해 최선을 다하고 있습니다.

따라서 Axis 장치의 모든 기능을 활용하는 포괄적인 솔루션을 만들 수 있습니다.

다음 페이지에서는 VAPIX(자체 API), 당사의 ONVIF 및 IoT 작업, ACAP를 통한 플랫폼 모듈화, 네트워크 통합 자동화에 대해 자세히 알아볼 수 있습니다.

VAPIX, ONVIF, IoT 및 클라우드 통합에서 Axis의 이점

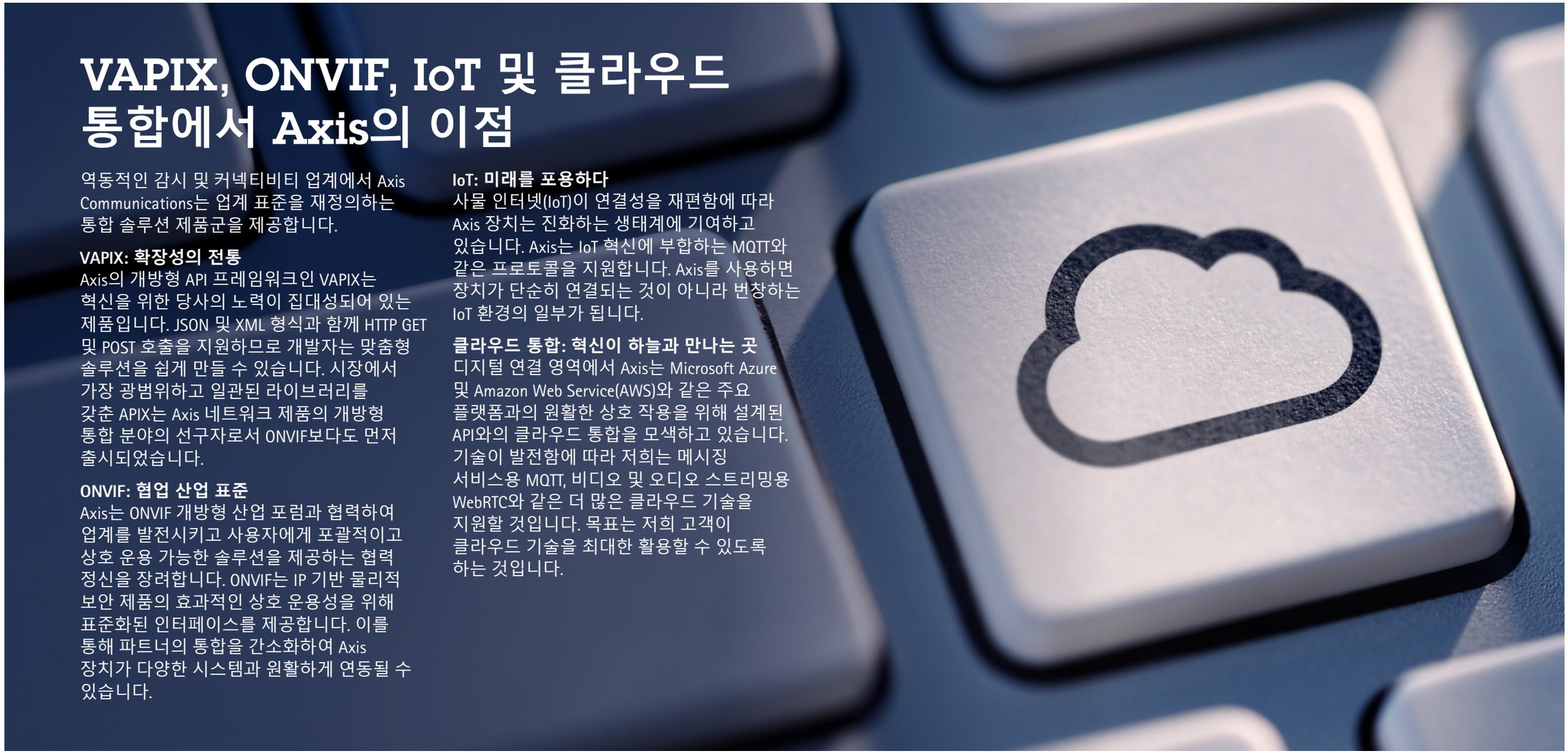
역동적인 감시 및 커넥티비티 업계에서 Axis Communications는 업계 표준을 재정의하는 통합 솔루션 제품군을 제공합니다.

VAPIX: 확장성의 전통
Axis의 개방형 API 프레임워크인 VAPIX는 혁신을 위한 당사의 노력이 집대성되어 있는 제품입니다. JSON 및 XML 형식과 함께 HTTP GET 및 POST 호출을 지원하므로 개발자는 맞춤형 솔루션을 쉽게 만들 수 있습니다. 시장에서 가장 광범위하고 일관된 라이브러리를 갖춘 APIX는 Axis 네트워크 제품의 개방형 통합 분야의 선구자로서 ONVIF보다도 먼저 출시되었습니다.

ONVIF: 협업 산업 표준
Axis는 ONVIF 개방형 산업 포럼과 협력하여 업계를 발전시키고 사용자에게 포괄적이고 상호 운용 가능한 솔루션을 제공하는 협력 정신을 장려합니다. ONVIF는 IP 기반 물리적 보안 제품의 효과적인 상호 운용성을 위해 표준화된 인터페이스를 제공합니다. 이를 통해 파트너의 통합을 간소화하여 Axis 장치가 다양한 시스템과 원활하게 연동될 수 있습니다.

IoT: 미래를 포용하다
사물 인터넷(IoT)이 연결성을 재편함에 따라 Axis 장치는 진화하는 생태계에 기여하고 있습니다. Axis는 IoT 혁신에 부합하는 MQTT와 같은 프로토콜을 지원합니다. Axis를 사용하면 장치가 단순히 연결되는 것이 아니라 번창하는 IoT 환경의 일부가 됩니다.

클라우드 통합: 혁신이 하늘과 만나는 곳
디지털 연결 영역에서 Axis는 Microsoft Azure 및 Amazon Web Service(AWS)와 같은 주요 플랫폼과의 원활한 상호 작용을 위해 설계된 API와의 클라우드 통합을 모색하고 있습니다. 기술이 발전함에 따라 저희는 메시징 서비스용 MQTT, 비디오 및 오디오 스트리밍용 WebRTC와 같은 더 많은 클라우드 기술을 지원할 것입니다. 목표는 저희 고객이 클라우드 기술을 최대한 활용할 수 있도록 하는 것입니다.



ACAP를 통한 플랫폼 모듈화

AXIS OS의 주요 기능 중 하나는 AXIS Camera Application Platform (ACAP)을 통해 플랫폼 모듈화를 활성화한다는 것입니다. ACAP는 개발자가 비즈니스 요구 사항을 충족하기 위해 비디오 분석, 오디오 분석 및 기타 맞춤형 확장과 같은 애플리케이션과 서비스를 만들고 배포할 수 있는 프레임워크입니다. ACAP 애플리케이션은 핵심 AXIS OS 기능과 독립적이며 시스템의 나머지 부분에 영향을 주지 않고 설치, 업데이트 및 제거할 수 있습니다. ACAP 애플리케이션은 표준 프로토콜 및 API를 사용하여 서로 통신하거나 외부 시스템과도 통신할 수 있습니다.

확장성 및 성능
ACAP는 Axis 장치에서 운영 체제의 마이크로 서비스 아키텍처를 사용합니다. 각 서비스는 수요와 부하에 따라 독립적으로 확장하거나 축소할 수 있습니다. 이를 통해 시스템의 전반적인 성능과 가용성이 향상되고 효율적인 리소스 사용 및 할당이 가능해집니다.

적응성 및 맞춤화
ACAP는 다양한 유형의 통합, 분석 및 장치를 지원하기 때문에 Axis 장치의 용도, 적응성, 맞춤화가 강화됩니다. 또한 각 애플리케이션이 AXIS OS와 느슨하게 결합되어 있고 자체적으로 응집력이 높기 때문에 ACAP가 결합을 줄이고 플랫폼의 응집력을 높일 수 있습니다.

유지보수 능력 및 신뢰성
각 서비스는 독립적으로 분리되어 테스트, 모니터링 및 디버깅될 수 있습니다. 이를 통해 문제 해결 및 진단이 단순화되고 시스템의 복원력과 오류에 대한 내성이 향상됩니다. 그리고 이는 소프트웨어 품질 측면에서 AXIS OS를 돋보이게 만듭니다.

IT 팀을 위한 AXIS OS

적절한 자동화를 구축하고 IT 인프라에 통합하면 적절한 보안 제어가 보장되고 시간과 비용을 절약할 수 있습니다. 불필요한 시스템 복잡성이 최소화됩니다. 기업 IT 인프라에 통합된 Axis 장치와 소프트웨어를 결합하면 다음과 같은 이점을 얻을 수 있습니다.

> 전용 물리적 장치 준비 네트워크를 제거하여 시스템 복잡성을 최소화.

> 자동화된 온보딩 프로세스와 장치 관리를 추가하여 비용 절감

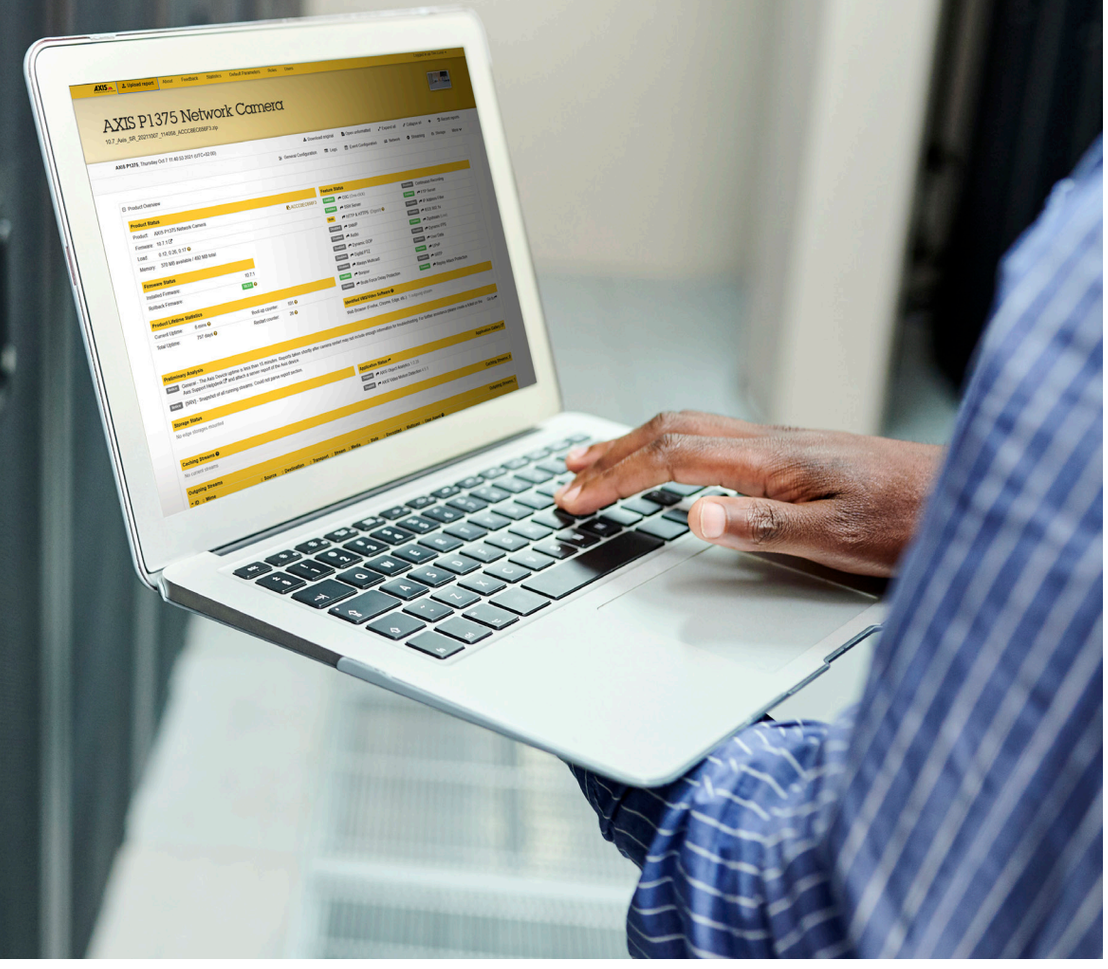
> IEEE 802.1X, IEEE 802.1AR 등 제로 트러스트 네트워크 보안 제어를 활용.

> IEEE 802.1AE MACsec의 도움으로 기본 수준에서 데이터 암호화를 도입하여 전반적인 네트워크 보안을 강화. 이와 같은 방법을 통해 Axis 장치는 네트워크 보안에 기여합니다.

> 표준화된 프로토콜을 통해 Axis 장치를 모니터링 (예: 원격 Syslog를 활용해 로그 및 상태 모니터링).

제로 트러스트 원칙에 기반한 보안 네트워크
제로 트러스트 원칙에 기반한 통합 보안 네트워크를 구축하는 것은 고립된 시스템이 자체적으로 운영되는 것을 없애는 데 핵심입니다. Axis 장치를 잘 정의된 개방형 네트워크 프로토콜 및 표준을 사용하여 기업 IT 인프라에 통합하면 보안이 강화되고 구성 및 유지보수 비용이 절감되며 IT 정책 중심의 시행이 가능해집니다.

IT 부서를 위한 장점
IT 부서는 IT 네트워크 보안을 책임지고 있으므로 Axis 장치가 이들에게 유리합니다. Axis 장치는 다양한 기능과 표준화된 개방형 IEEE 및 IETF 네트워크 프로토콜 및 공유 설계로 정의된 IT 솔루션과 유사하기 때문에 통합, 유지 관리 및 운영이 더 쉽습니다. Axis 장치는 고객 네트워크에서 보안 향상에 기여하는 "신뢰할 수 있는 시민"과 같은 존재입니다.



더 알아보시겠습니까?

AXIS OS는 Axis 장치를 신뢰할 수 있는 이유이며 Axis 장치가 뛰어난 이미지 품질, 오디오 품질, 그 외 다양한 성능을 제공하는 기반입니다.

왜냐하면 AXIS OS는 네트워크 장치에서 가장 중요한 기준인 장기적인 가치, 높은 사이버 보안 표준, 통합 용이성을 설계되었기 때문입니다.

Axis 장치가 귀하의 비즈니스나 조직에 정확히 어떻게 가치를 더할 수 있는지에 대해 알려드리고 싶습니다.

지금 바로 문의 주세요!

또는 axis.com에서 Axis 장치를 살펴볼 수 있습니다.

Axis Communications에 대하여

Axis는 보안 및 비즈니스 성과 향상을 위한 솔루션을 개발하여 더 스마트하고 더 안전한 세상을 만들 수 있도록 지원합니다. 네트워크 기술 회사이자 업계 선도 기업인 Axis는 영상 감시, 접근 제어, 인터콤 및 오디오 시스템을 위한 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 보완되고 고품질 교육을 통해 지원됩니다.

50개 이상의 국가에서 약 4,000명의 Axis 임직원이 전 세계의 기술 및 시스템 통합 파트너와 협력하여 고객에게 최적의 솔루션을 제공하고 있습니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다.