Cybersecurity in focus

AXIS OS adheres to security-by-design approach. Our Axis Security Development Model (ASDM) defines processes and tools that reduce the risk of vulnerabilities during software development and beyond.

Our hardware-based cybersecurity platform, Axis Edge Vault, ensures secure boot and a tamper-protected environment for the storage of customer-loaded cryptographic keys. The AXIS OS core software consists of well-tested open-source components. And every release is complemented by a software bill of materials (SBOM) showing that AXIS OS is up to date and patched for known vulnerabilities.

AXIS OS also complies with and is certified to ETSI EN 303 645, which focuses specifically on edge-device security. FIPS 140 compliance ensures AXIS OS adheres to the latest cryptographic standards defined by the National Institutes of Technologies (NIST). And finally, as an approved CVE Numbering Authority, we follow best practices for identifying, managing, and disclosing vulnerabilities.

On the following pages, you can read more about our Axis Security Development Model, Axis Edge Vault, vulnerability management, and the concept of unified security.

Developed and maintained with cybersecurity in mind

The Axis Security Development Model (ASDM) effectively integrates cybersecurity into the software development lifecycle. It describes security activities to consider during the phases of software development. The purpose is to reduce vulnerabilities – as well as development costs – by establishing a baseline for cybersecurity and by providing guidance.

ASDM: made by Axis
The Axis Security Development Model is not a standard "off-the-shelf" framework. Instead, we reviewed many cybersecurity standards and frameworks – such as ISO 27001, IEC 62443, NIST, BSIMM, and CMMC. The common thread between them is that security is incorporated into all the development phases. With that as our starting point, we adapted our model to fit our company culture, development practices, and the type of products we provide.

The ASDM toolbox
The ASDM toolbox prescribes a range of activities that address a variety of security problems. Some examples are risk assessment, threat modeling, threat model testing, static code analysis, vulnerability scanning, and vendor assessment. Development teams choose which activities to engage in depending on the kind of software to be developed. The goal is better cybersecurity rather than just compliance with a process.

The added benefit of outside expertise
Most of the heavy lifting of secure software development is carried out within Axis, but we also recognize that we can benefit from the knowledge and expertise of others. So, we hire specialized companies for penetration testing. And we have the public AXIS OS bug bounty program, where we offer financial rewards to security researchers for helping us identify vulnerabilities.

Governance	Training	ASDM line meeting	ASDM assessment	Security compliance and standards

Requirements	Design	Implementation	Verification	Deployment
Risk assessment	Threat modeling	Static code analysis	Threat model test	Vulnerability management
Vendor assessment		Software composition analysis	External penetration test	Incident management
Data privacy			Vulnerability scanning	Product/solution security status
Open source security assessment			Internal security assessment	Bug bounty program

Visit Axis Trust Center | *Find out how Axis and its products support cybersecurity and security compliance with various regulations and standards. Access a wide range of information, from cybersecurity practices and measures, to certificates, guides and reports.*

Built-in cybersecurity

Protection from the inside out
Axis Edge Vault is our hardware-based cybersecurity platform. It provides a solid foundation for ensuring your Axis devices are a trusted and reliable part of your network. But this strong hardware-based foundation would be useless without an operating system that supports its full potential. AXIS OS uses the Edge Vault platform to provide enhanced security on the edge for every use case.

Edge Vault includes features such as:

Secure key storage
Secure keystore involves cryptographic computing modules for the secure storage and computing of cryptographic keys. They safeguard device identity and other sensitive information from unauthorized access – even if the device is compromised. The cryptographic computing modules used are the Trusted Execution Environment (TEE) built into the system-on-chip (SoC) as well as a dedicated secure element or a Trusted Platform Module (TPM 2.0), which are separate chips on the printed circuit board (PCB).

Signed OS and secure boot
Signed OS means we code-sign the device software image. Together, signed OS and secure boot mean devices can download and run only the genuine AXIS OS operating system. This adds an extra layer of protection against tampering in the software and hardware supply chains.

Axis device ID
Axis device ID is IEEE 802.1AR-compliant and enables secure device identification and onboarding on a network. It acts as a genuine passport for every Axis device manufactured.

Encrypted file system
File system encryption protects data in the file system from being extracted or tampered with while the device is not in use, such as during transit from a system integrator to the end customer.

Signed video
Signed video lets users verify the authenticity of captured video and that it hasn't been tampered with.

Axis Edge Vault cybersecurity platform

Cryptographic computing modules	Features	Use cases
Secure element TPM 2.0 SoC security (TEE)	Secure boot Signed OS Axis device ID Secure keystore Signed video Encrypted file system	Trusted device identity Secure key storage Video tampering detection Supply-chain protection

*Note: Not all device models support all the Axis Edge Vault features. Check the datasheet or the Axis product selector for confirmation of the features supported by specific products.

Vulnerability management

To minimize our customers' risk of exposure, we implement industry best practices in managing and responding transparently to vulnerabilities.

Best-in-class vulnerability management
There's no way to guarantee that products and services delivered by Axis are entirely free from vulnerabilities. This is not unique for us, but rather a shared condition for all software and services. But we make a concerted effort to identify and mitigate potential vulnerabilities at every stage, reducing the risk of deploying Axis products and services in customer environments.

A CVE Numbering Authority,
Axis is a CVE Numbering Authority (CNA). We joined the CVE Program to work with like-minded companies on improving vulnerability management. We align the way we handle, disclose, and patch vulnerabilities with the international framework provided by this non-profit organization and with our public vulnerability management policy.

Transparent management you can rely on
Axis uses the well-known CVSS rating system (Common Vulnerability Scoring System) to rate vulnerabilities related to either code developed by Axis or third-party open-source code. We assess vulnerabilities in open-source code according to how relevant they are for our products when best practice recommendations are applied. In our Security Advisories we transparently disclose all CVE related to AXIS OS. You can LSO subscribe to the Axis Security Notification Service to receive information about vulnerabilities and other security-related matters for Axis products.

Partnerships with security researchers and organizations
We embrace and appreciate the work of individual security researchers and security research organizations who contact us to report vulnerability findings. We don't hesitate to disclose and patch them. Handling vulnerabilities correctly and transparently with an ethical, responsible disclosure process is what's important – no matter how the vulnerability is discovered.

An all-in-one security experience

In network devices powered by AXIS OS, hardware and software components work together to enable customers to securely operate the devices, their services, and the systems they are connected to. Layer upon layer of comprehensive protection starts with a security foundation and a hardware-based security platform and continues up to the software. Devices powered by AXIS OS are guarded by this layered, defense-in-depth approach to cybersecurity. It increases the cumulative security of data, applications, and processes.

So, you can rest assured that no matter what an Axis device is used for, protection and secure communication is available, allowing for proper and secure integration into third-party systems.

Access control

Access control management
Local user device management with password complexity indicator
Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality

Privacy
Use of diagnostics data
Minimalistic approach to how much customer-specific data should be stored

Application

Application security
TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC)
Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog

Operating system

Encryption and data protection
OpenSSL 1.1.1 and 3.0
X.509 certificate PKI and cryptography
Transport layer security (TLS 1.2/TLS 1.3)
SD card encryption (AES-XTS-Plain64 256bit)
Encrypted file system (AES-XTS-Plain64 256bit),
Signed video

Default security
HTTPS enabled by default
Brute-Force Delay Protection
Host-based Firewall
Network time security (NTS)
Insecure TLS versions disabled
UART/Debug port disabled

Enterprise network security
IEEE 802.1X (network access control)
IEEE 802.1AR (secure device identity)
IEEE 802.1AE (MAC security, MACsec)

AXIS OS Operating System
Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others.
Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.

Silicon assisted security (chip)

Hardware root-of-trust
ARM-based system-on-chip (SoC) security
Trusted Execution Environment (TEE/OP-TEE)
Trusted platform module (TPM 2.0), Secure element

Secure key storage
Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.

Security foundation

Axis Security Development Model
Axis security development model (ASDM)
3rd party penetration tests
Bug bounty program with Bugcrowd
Software Bill of Material (SBOM)

Compliance
Common Criterial EAL
FIPS 140
ETSI EN 303 645

Trusted device identity
Axis Edge Vault cybersecurity platform
Secure boot with Signed OS (code-signing)
Axis Device ID (IEEE 802.1AR)