Minimizing cybersecurity risks with a lifecycle approach.

Cyberthreats can happen at any point in a product lifecycle – when a product is being built, delivered, or in use.

That's why we look at the full picture, and undertake measures at every lifecycle phase to proactively reduce risks to help safeguard your system.

#1

Security Foundation

Cybersecurity starts early – right from the first line of code. Our software development process works continuously to improve product security and minimize vulnerabilities, even after the products are installed by customers. AXIS OS and Axis Edge Vault also form part of our security foundation.

#2

Production

We work closely with trusted manufacturing partners, and use protective measures such as 24/7 monitoring during production – mitigating the risk of having compromised components.

#3

Distribution

Whether it's a hardware delivery or a software download, we have measures like signed OS and secure boot, as well as integrity checksums, to defend against software tampering along the way.

#4

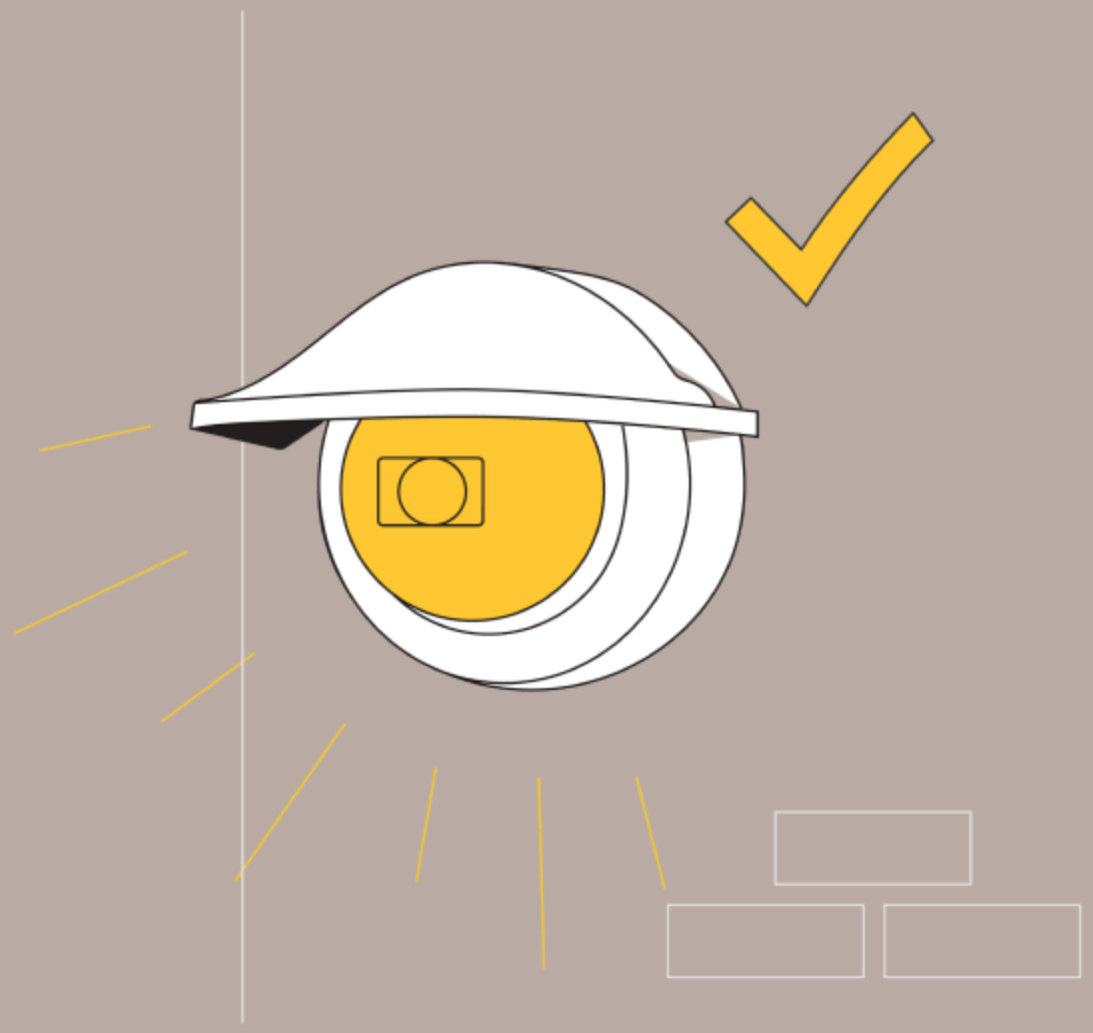
Implementation

Built-in security measures for identity and access management (IAM), secure device onboarding, and encrypted communications provide beneficial capabilities. Guides, trainings and support help you optimize security.

#5

In Service

Maintaining the security of products for the long haul includes working continuously to identify and address new vulnerabilities, being transparent about them, and encouraging customers to implement software updates that include security patches.



#6

Decommissioning

It’s important to retire products that are no longer supported to avoid risks from unpatched vulnerabilities. We help you track warranty and end-of-support dates. Before disposal, make a factory default and allow the device to reboot to ensure no data or configuration is left behind.