NIS2 | CRA | NDAA

Video Systems and Solutions

# Cybersecure, resilient, and compliant

Your guide to future-proof your video security systems and ensure regulatory compliance

BOSCH

# Table of Contents

# Cybersecurity in the digital age

Artificial intelligence (AI) is changing all areas of our lives. As more video security cameras connect to the Internet of Things (IoT), the role of video security is changing. Cameras are no longer part of a “closed” system, solely focused on gathering, recording, and viewing images. They are transitioning into intelligent sensors that collect significantly more data than video security images alone. And since video data is often highly critical and sensitive, every component of the video security infrastructure, including cameras, storage devices, network communication, Public Key Infrastructure (PKI), and video management software, needs to be addressed. The surge in data collection also increases the risk of cybercriminals looking to steal sensitive data.

By 2030, it is expected that over **29 billion** devices will be connected to the Internet.

Statista Research 2022

# Getting to future-proof and compliant solutions

For over a decade, our unwavering commitment to data security and regulatory compliance has been a guiding focus. Cybersecurity has consistently remained a top priority in the face of escalating digital threats and interconnectedness. Our approach aims to establish trust, safeguard data, manage user access, and enhance data security to uphold the most stringent reliability benchmarks. We understand that as connectivity and data collection evolve, so do the regulations surrounding their protection. These include, but are not limited to, the European Union's Network and Information Security Directive (NIS2), the Cyber Resilience Act (CRA), and the National Defense Authorization Act (NDAA) in the United States.

Our commitment to continuous improvement is a cornerstone of our operations. We are committed to staying ahead of the curve and continually working to meet both current and future government compliance requirements in the video security industry. We are actively engaged with testing and validation agencies to ensure our products perform at or above the quality standards defined by each government organization. As a result, we consider the entire infrastructure to minimize the risk of hacking, ensure privacy, and continuously check for new legal and regulatory changes.

**Our solutions** focus on creating trust, securing data, managing user access rights, and maximizing data security to meet the highest reliability standards – in line with NIS2 Directives, CRA, and NDAA.

# Certifications

We provide comprehensive tools, documentation, and training to mitigate risks and safeguard our products and services. Our robust policies, processes, and third-party certifications ensure our security measures are always up-to-date.

As a result of our sustained efforts, we have achieved critical cybersecurity certifications, indicating that we are doing the right things beyond the competition.

## UL 2900 2-3 Level 2 Certified

### Standard for Safety and Software Cyber-security for Network-Connectable Products

- Includes penetration testing on our products to probe for vulnerabilities
- Our certification is device specific up to level 3

Underwriters Laboratories

## IEC 62443-4-1 Certified

### Security for industrial automation and control systems

- Focuses on the processes and definitions around developing and creating secure products
- It proves that Bosch can ensure a secure development process

IEC

## NDAA 2019, section 889(a)(1)(A) and (FAR) 52.225-5

### US government regulations on purchasing and trade agreements

- Compliant with United States NDAA 2019, section 889(a)(1)(A)
- Adherence to the United States Federal Acquisition Regulation (FAR) 52.225-5 on Trade Agreements

# 10 leading measures to help you build a reliable and compliant system

We embrace the highest standards when developing and manufacturing products, ensuring optimum data security and cyber resilience in every network-connected device. Since 2004, we have integrated crypto co-processors, certificates, closed operating systems, and signed firmware into all our products, including cameras, storage devices, and network communications.

### 1 Embedded login firewall

- Focus on blocking threats, not functionality
- An intelligent login firewall you can count on

### 2 Secure Element

- We set the standard with the most future-proof Secure Element with Trusted Platform Module (TPM) functionality
- Supports 4096-bit keys

### 3 Password enforcement

- Security first: set a password, then connect

### 4 Minimum TLS 1.2

- Transport Layer Security (TLS): a cryptographic protocol that provides secure communication
- A minimum version of TLS provides maximum security

### 5 Simple Certificate Enrollment Protocol (SCEP)

- Simplifies cybersecurity at scale
- An easy way to deploy and manage certificates on cameras

### 6 Software sealing

- Changes to a sealed camera configuration will trigger an alarm
- Protects against unintentional or unauthorized changes

### 7 Encrypted firmware

- Verifies firmware authenticity and prevents malware insertion

### 8 Cloud firmware check

- Stay up-to-date at all times
- Checks Download store for new firmware automatically

### 9 Session timeout

- Manage how long a configuration session can be left unattended

### 10 Secure by default

- Security by default, closed until you say it is open

### Maximum resilience

Users can rely on BVMS for maximum resilience with continuous live video and playback, no matter the interruption. The video management system keeps operations running even if both management and recording servers fail. BVMS uses Advanced Encryption Standard (AES), preventing unauthorized access to sensitive data. It also offers extensive user management to ensure only authorized users can access video data.

# Regulation overview

## NIS2 directive

In response to growing threats due to digitalization and interconnectedness, the Network and Information Security Directive (NIS2) seeks to strengthen the resilience of network and information systems in the European Union (EU) against cybersecurity risks. It will become an enforceable law **by October 17, 2024, requiring** critical infrastructure and essential service operators to adopt suitable security measures and promptly report any incidents to the appropriate authorities. Organizations must address risk factors and manage corporate accountability, reporting obligations, and business continuity to ensure compliance with the Directive. Non-compliance will result in heavy fines and penalties, negatively impacting cyber resilience.

## Cyber Resilience Act

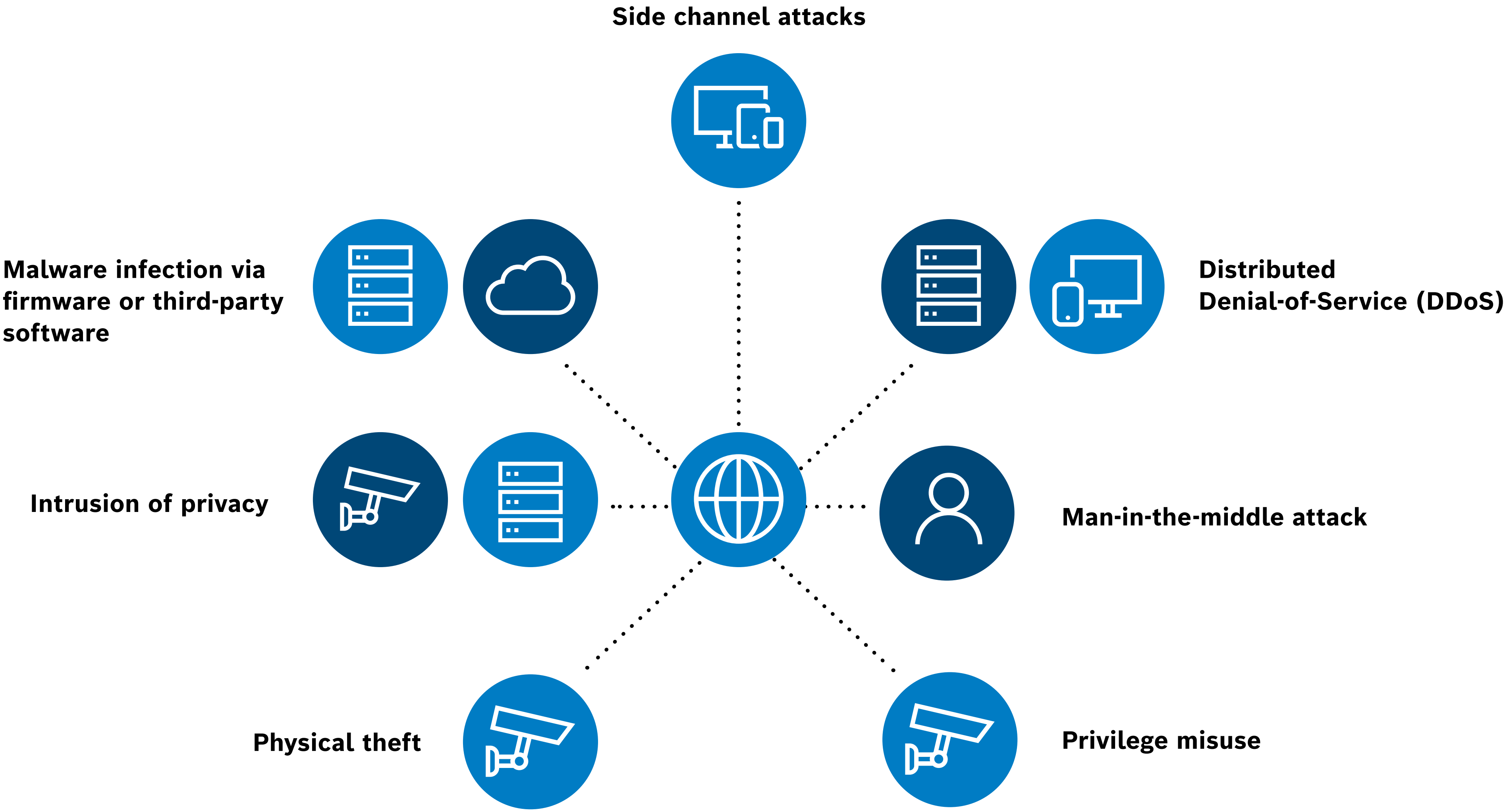
To help prevent escalating cyberattacks, the EU's Cyber Resilience Act aims to regulate cybersecurity requirements for digital products, ensuring more secure hardware and software. Manufacturers must provide complete transparency in assessing how they design products and software to enhance security and facilitate compliance.

## National Defense Authorization Act (NDAA)

NDAA 2019, section 889(a)(1)(A) limits the United States government's access to equipment or services manufactured by certain companies with ties to China to protect national security. It prohibits obtaining or extending a contract for any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component. The rule aims to prevent cyber-attacks and exfiltration of information and intellectual property by foreign adversaries, posing risks to the US government and industry. Installers should assess if equipment or services contain the non-compliant manufacturers' products.

# Rising to meet the challenges: Understanding the threat landscape

It’s important to understand the growing threats and risks associated with unauthorized access and how to address any vulnerability and achieve compliance.



Side channel attacks

Malware infection via firmware or third-party software

Distributed Denial-of-Service (DDoS)

Intrusion of privacy

Man-in-the-middle attack

Physical theft

Privilege misuse

# Challenge: Malware infection aimed at gaining control of systems

- These are program codes entering the system via the downloading of new fake software packages. Bad actors insert storage media into a device that contain things like viruses and worms.

**Solution:** All our firmware is encrypted and verifies authenticity to prevent malware insertion.

## Challenge: Privilege misuse

- Once a user has rights to access the system these privileges could become known to another person who could misuse those access rights. For example, a person leaving the company may retain their access rights for a period. Or an internal person intentionally misuses their access rights against the company.

**Solution:** Cameras and encoders are protected against unauthorized access with password requirements, user management, authentication via certificates, data encryption, and network protocols in line with industry standards.

- The NIS2 Directive emphasizes that only authorized people should have secure access to sensitive areas and critical resources, and we ensure that only authorized users have access to the system.

- Access to the premise or specific areas has to be strictly controlled. Unauthorized access might result in serious consequences, such as confidential information theft or physical harm.

# Challenge: Denial of Service (DDoS) and side channel attacks

- A DDoS attack overwhelms an online service with traffic from multiple sources, making it unavailable. It can hit various essential resources, presenting a significant challenge for publishing and accessing important information.

- A side channel attack occurs when a device is opened, or electromagnetic waves are measured to determine what the device is executing.

**Solution:** Every one of our cameras has a built-in Secure Element (SE) with Trusted Platform Module (TPM) functionality and key vault for the highest level of security.

- Our measures support secure connections (HTTPS), and the hardware securely stores all certificates and cryptographic keys required for authentication and encryption, so data will remain safe beyond 2030.

- Software sealing detects any changes in configuration settings, and updates are only possible via Bosch-signed firmware files.

- All devices with Firmware 6.3 (2015) or higher have an embedded login firewall. All defaulted devices with Firmware 6.4 (2017) and above cannot be accessed or configured without a complex password. If there are three failed login attempts within 20 seconds, the camera blocks the attempting IP address.

# Your trusted partner for peace of mind

We deliver video security solutions that are:

**Predictive-ready, supporting data-driven decision-making to enable proactive and timely responses, minimizing risks and potential damages**

**Secure, cyber-resilient, and meet reliability standards – in line with NIS2 Directives, CRA, and NDAA**

**Designed to perform, last, and be accessible no matter what, empowering you to focus on your business**

# Learn more

Check out our resources below. If you can't find what you're looking for, please contact us. Our experienced and trained technical support team can help you build and configure a secure and compliant system wherever you are.

**IP video and data security guidebook**

**Secure by default tech note**

**Network Authentication white paper**

**Camera firmware and release notes download area**

**Data security training site portal**

**Data security in-depth web page**

**Security Advisory RSS feed**

**Contact us and speak with an expert**

**Bosch Security and Safety Systems**
Protecting lives, buildings and assets is our aim. Our product portfolio includes video security, intrusion detection, fire detection and voice evacuation systems as well as access control and management systems. Professional audio and conference systems for communications of voice, sound and music complete the range.

Bosch Security and Safety Systems
To learn more about Video Systems
please visit www.boschsecurity.com

www.twitter.com/BoschSecurityUS
www.youtube.com/BoschSecurity

Invented for life

BOSCH