BOSCH
Invented for life

# CYBER SECURITY from BOSCH systems


## Gábor Szűcs

Solution Consultant – Adriatic region

BOSCH
Invented for life

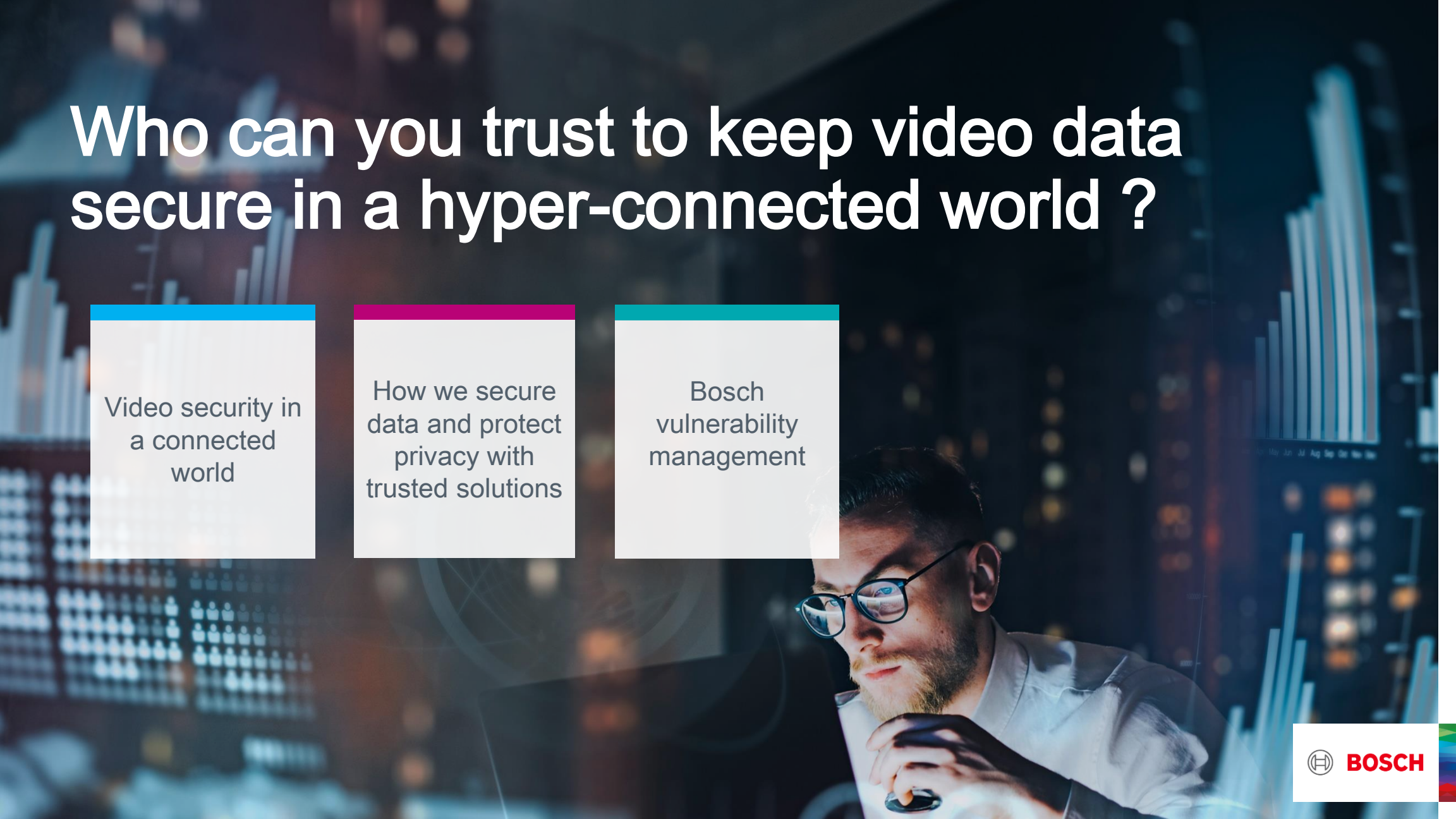
# Who can you trust to keep video data secure in a hyper-connected world ?

# Who can you trust to keep video data secure in a hyper-connected world ?

Video security in a connected world

How we secure data and protect privacy with trusted solutions

Bosch vulnerability management



# Video security in a connected world

## Enjoying limitless possibilities

## Worrying about the consequences

VIDEO SURVEILLANCE

Why surveillance cameras are a favorite of IoT botnets

BY OFER GAYER ON NOV 14, 2016

THEY'RE WATCHING

**Thousands of security cameras in the US can easily be hacked**

NETWORKWORLD FROM IDG

**IoT security camera infected within 98 seconds of plugging it in**

WFTV 9 abc

**9 Investigates hacked surveillance cameras across Central Florida**



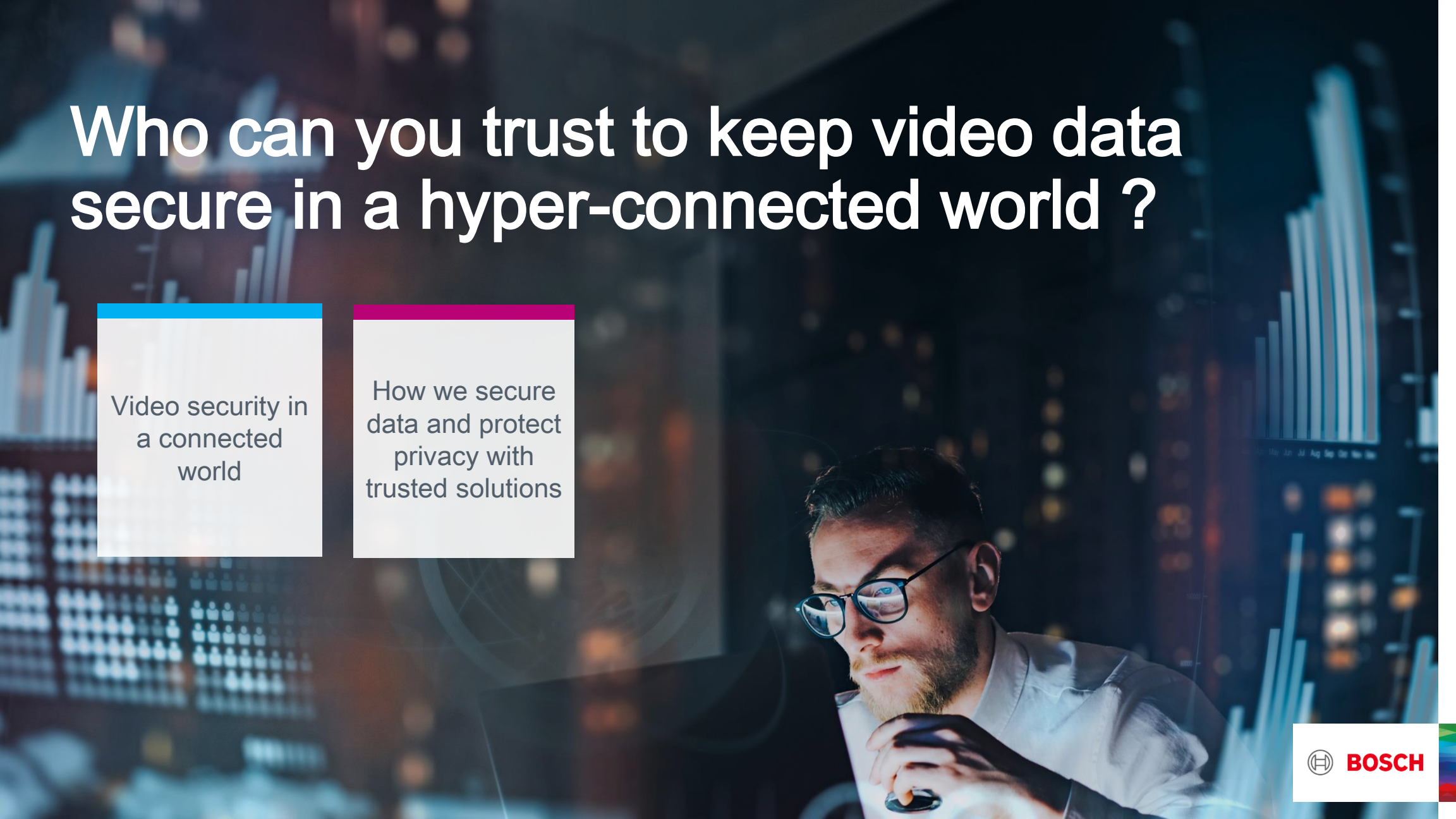


BOSCH

# Who can you trust to keep video data secure in a hyper-connected world ?

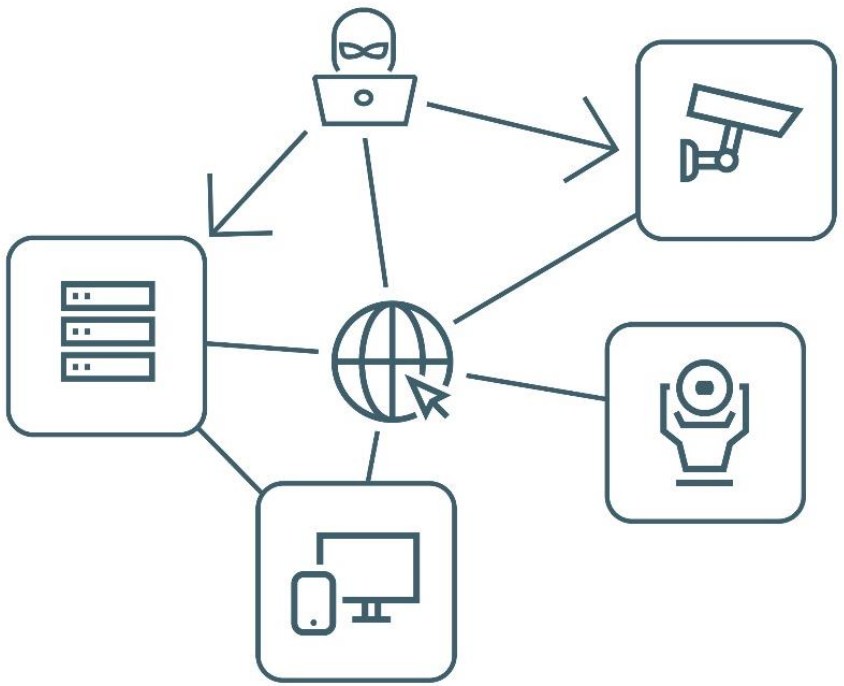
Video security in a connected world

How we secure data and protect privacy with trusted solutions



BOSCH

# How we secure data and protect privacy with trusted solutions
# Bosch four-step approach considering complete infrastructure



1. Create trust
2. Secure data
3. Manage user access rights
4. Meet IT industry standards

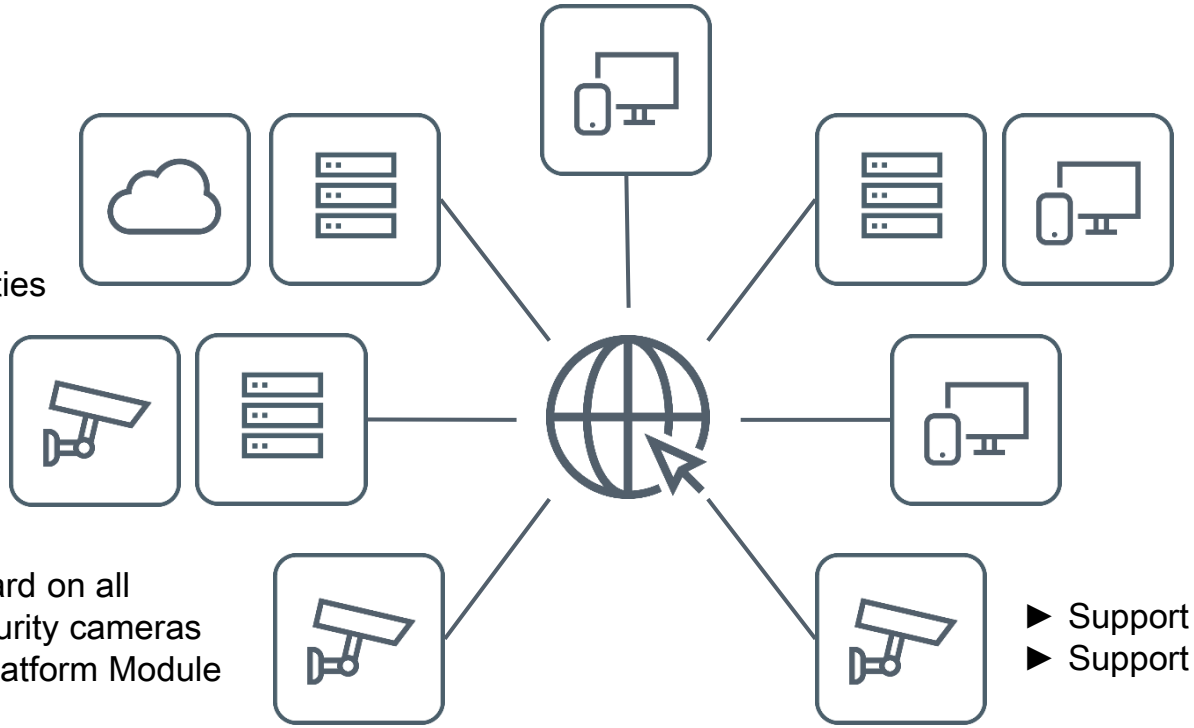
# Secure data and protect privacy
## Potential threats and our solutions

### Video security example

- ► Unique built-in Trusted Platform Module

- ► No uploading of 3rd party SW
- ► Firmware updates by Bosch signed files only
- ► Fuzz testing to protect against memory corruption vulnerabilities

- ► User access management for cameras, recording solutions and video management software



- ► Embedded Login Firewall

- ► Tamper protection standard on all Bosch network video security cameras
- ► Unique built-in Trusted Platform Module
- ► Software sealing

- ► Support of Microsoft Active Directory
- ► Support of token based authentication

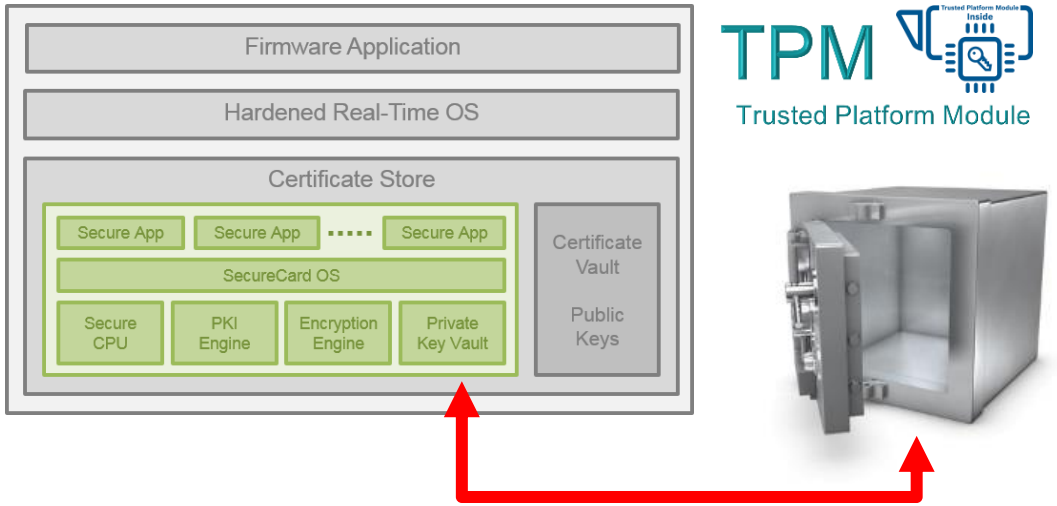
# How we secure data and protect privacy with trusted solutions
# 4. How we secure our cameras

► **Software measures:**

1. Secured connections supported
2. Password enforcement at setup
3. Unsecure ports disabled
4. Unsecure remote communication disabled
5. Uploading of 3rd party software not possible
6. Firmware updates only possible via Bosch signed firmware files
7. Embedded Login Firewall improves robustness against DoS attacks
8. **New: software sealing can detect changes in a configuration**

► **Hardware measure:**

1. Trusted Platform Module inside



# Keep video data secure with Software Sealing

Intruders can temporarily disable certain areas by:

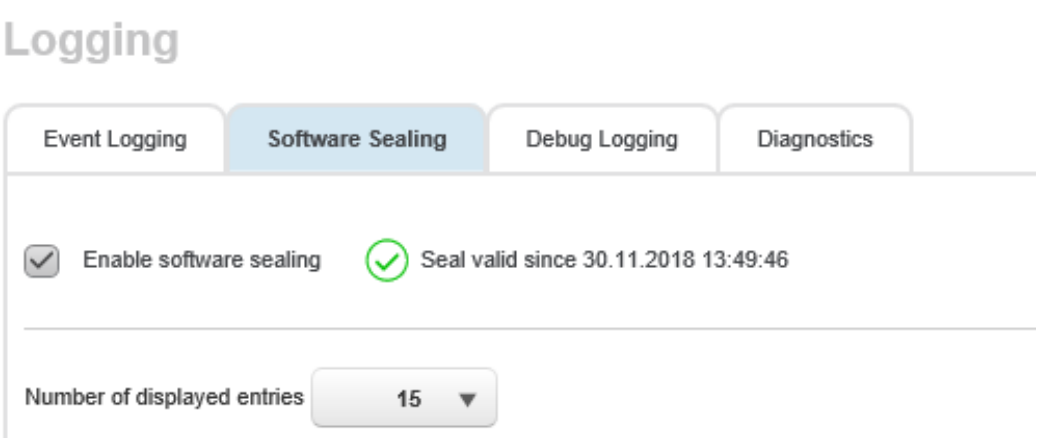
- Influencing the image processing
- Deactivating video analytics

Prevent the potential threat of the manipulation of a video management system!

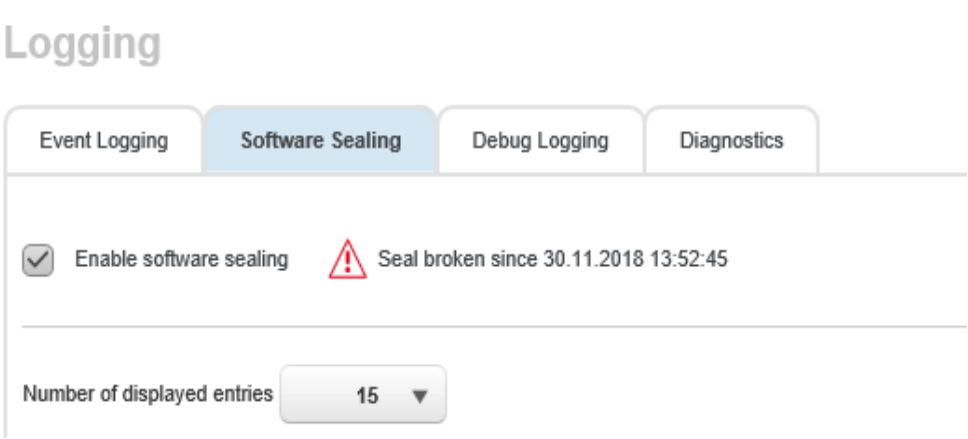
# Keep video data secure

## Software sealing, a new security enhancement feature

### Software seal enabled




### Software seal broken



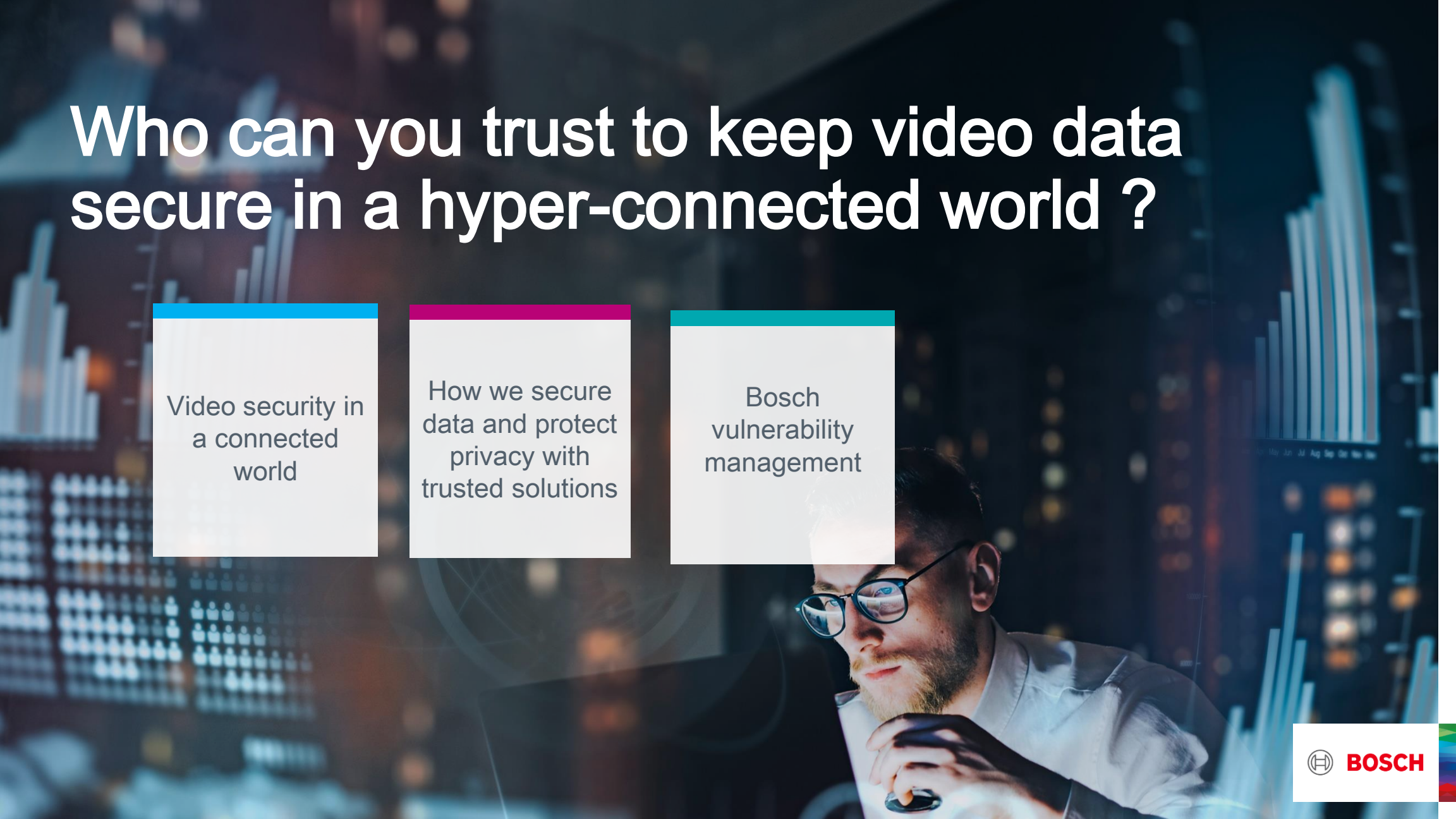

- If a change is needed, it must be authorized and the seal needs to be renewed afterwards.
- Software sealing can also be applied to an entire video system.

# Who can you trust to keep video data secure in a hyper-connected world ?

Video security in a connected world

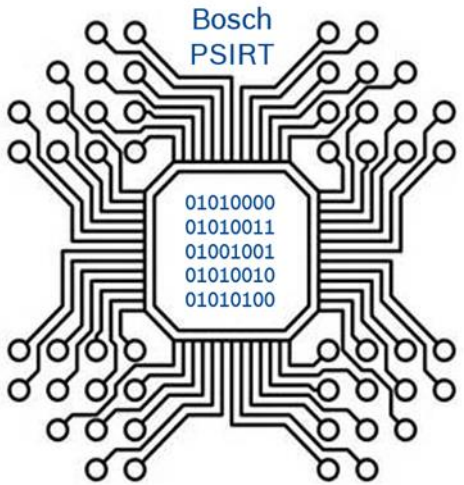
How we secure data and protect privacy with trusted solutions

Bosch vulnerability management



BOSCH

# BOSCH vulnerability management




**Bosch Product Security Incident Response Team (PSIRT) investigates all vulnerability reports.**

## Security Incident Response

- Efficient incident handling and resolution
- Communication between business units, subject matter experts, and central teams

## Vulnerability Management

- Effective vulnerability management across the Bosch Group
- This entails both vulnerabilities in Bosch products reported by Security researchers, and vulnerabilities in 3rd party product components.

## Security Community Work

- Active participation in the Incident Response community.
- Support security research
- Encourage the responsible disclosure of vulnerabilities.

https://psirt.bosch.com

# Security has to be transparent

1. Balanced approach

2. Software and Hardware layers

3. Deep diving and knowledge sharing

4. Best security experts

# THANK YOU