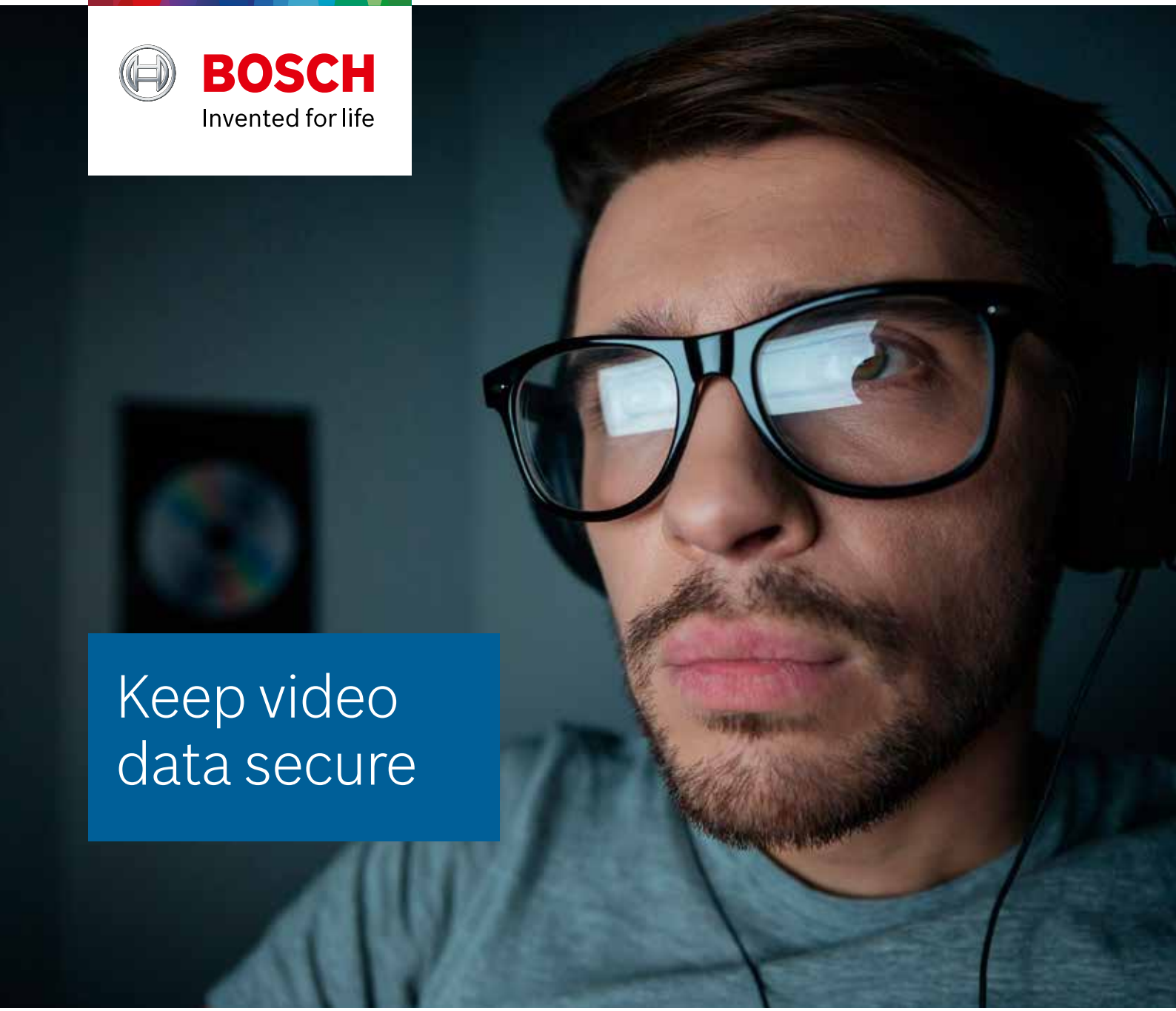
BOSCH
Invented for life



Keep video data secure

Video security data is increasingly connected across local and global networks. A growing number of edge components (cameras) send their data to core components (servers) over the Internet, where digital intruders and hackers loom.

The risks

Even a single weak link in a video security set-up can jeopardize an entire system. For example, skilled hackers can stage so-called man-in-the-middle attacks, hijacking communications between a camera and video management system (VMS). Once hackers have access, they can inject an alternate video feed to conceal illicit activity, or manipulate live camera footage to selectively remove certain details or persons from the scene.

Covering all angles

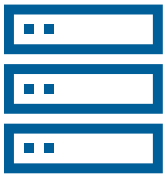
We achieve the highest standards with a four-step approach that considers the entire video security infrastructure. We create trust by assigning every component in the network an authentication key. We secure data from hackers by encrypting it at the hardware level, using a cryptographic key that is safely stored in a unique built-in Trusted Platform Module (TPM). We offer easy ways to manage user access rights ensuring that only authorized people have access to your data. And finally, we can support the set-up of a Public Key Infrastructure. So with Bosch, you couldn't be more secure.

Because video data is often highly critical and sensitive, Bosch is driving a systematic approach to maximize data security by considering physical safety and cybersecurity simultaneously. Bosch's system approach is the key to achieving the highest standards in end-to-end data security.

Bosch covers all major elements of the video security infrastructure:

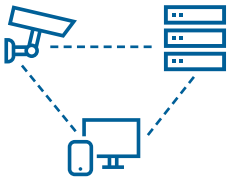
How we secure our cameras

- Secured connections supported (HTTPS)
- Password enforcement at initial set up
- Execution of 3rd party software "disabled"
- Firmware updates via manufacturer signed files only
- Cryptographic operations, for authentication and encryption, are only executed inside the unique built-in Trusted Platform Module (TPM)



How we secure our core devices

- Cryptographic operations, for authentication and encryption, are only executed inside the unique built-in Trusted Platform Module (TPM)
- Support of Microsoft Active Directory for safe management of user access rights
- Digest access authentication only
- Regular updates via security patches



How we secure network communication

- Unsecure ports are disabled by default
- Password enforcement at initial set up
- Network authentication using the 802.1x protocol
- Support of the Advance Encryption Standard (up to 256 bit keys for encryption)

How we support Public Key Infrastructures (PKI)

- Factory-loaded unique Bosch signed certificates on all cameras
- Unique built-in Trusted Platform Module (TPM) for highly secure cryptographic operations
- In-house Certificate Authority (Escrypt)
- Support of customer specific certificates
- Support of 3rd party PKI solutions

For more information download our:
Data security guidebook
Network authentication technote
VS-EH-en-06_F01U521132_03