

MAKE THE  
WORLD SEE

# Milestone e Bosch contro gli attacchi Cybersecurity

Stefano Riboli  
Bosch Security Systems S.p.A.  
Marketing Video Systems

Marco Bonfà  
Milestone Systems Italia  
Distribution Channel Manager

# TENDENZE DI MERCATO

# Non solo immagini di qualità

## Tendenze di mercato



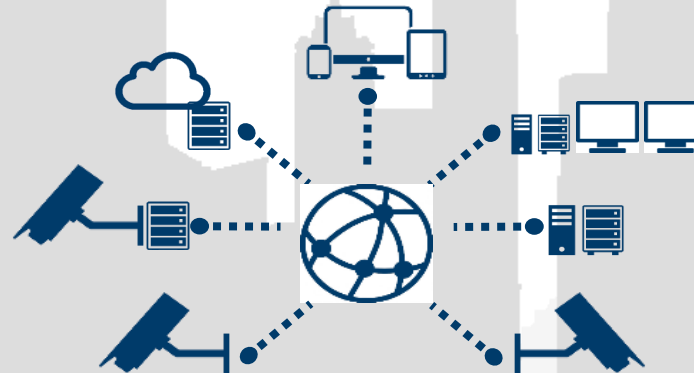
**Maggiori dettagli**



**Incremento del n. di telecamere**  
(CAGR 20% Global market for IP cameras )



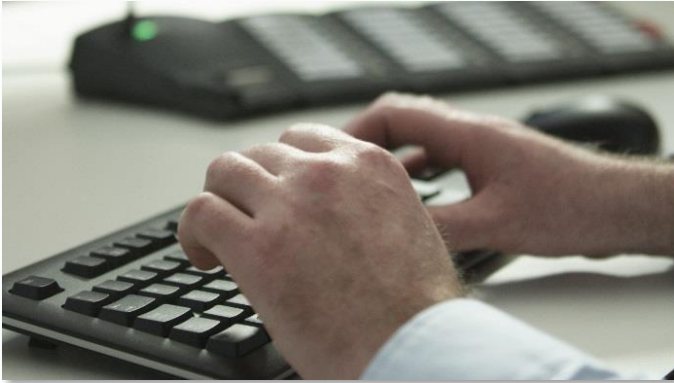
**Evidenze a prova di reato**



**Sempre più dati interconnessi tra loro**

# Non solo immagini di qualità

## Conseguenze



### Tonnellate di dati da elaborare

Cyber security market (2020):  
USD 170.21 billion, CAGR ~10%



### Tonnellate di dati video

Storage market (2020):  
USD 18.28 billion, CAGR 22%

Inoltre ...

# Questo rende la videosorveglianza vulnerabile al cyber crime!

# Salvaguardare i dati della videosorveglianza

## La necessità di sicurezza

**EXTREME TECH** Search Extremetech

Computing Mobile Internet Gaming Electronics

HOME > EXTREME > **FIRMWARE EXPLOIT GAINS CONTROL OF 18 BRANDS OF SECURITY CAMERAS**

### Firmware exploit gains control of 18 brands of security cameras

By Grant Brunner on January 29, 2013 at 3:40 pm | 4 Comments

0 shares



Networked security cameras offer a lot of convenience and peace of mind. Watching your store, keeping an eye on your pets at home, spying on the nanny are much easier now that we can check the security footage over the net. Unfortunately, 18 brands of security cameras with recording functionality are susceptible to an incredibly easy hack thanks to flawed firmware from Chinese company Ray Sharp.

**NETWORKWORLD** FROM IDG

Home > Security

**PRIVACY AND SECURITY FANATIC**  
By Ms. Smith | Follow

### IoT security camera infect seconds of plugging it in

It took a mere minute and a half for an internet-connected camera with malware

Network World | Nov 20, 2016 9:06 AM PT

**VIDEO SURVEILLANCE**

### Why surveillance botnets

BY OFER GAYER ON NOV 14, 2016

NETWORK > **L'Espresso** **LE INCHIESTE** LAVORO ANNUNCI ASTE Accedi

**R.it** Sicurezza

Home News Speciali Mobile Social Network Sicurezza Prodotti Interattivi Video

f t g+ in e

## "Attenti, i cybercriminali stanno colpendo la rete italiana"



Due hacker italiani lanciano l'allarme: "Anche l'Italia è sotto attacco" di una variante della botnet Mirai. L'obiettivo è rubare i dati alle grandi imprese di telecomunicazioni del nostro paese e alle sue banche. Ma non se ne parla

di ARTURO DI CORINTO

**WFTV 9 abc** NEWS WEATHER TRAFFIC SPORTS VIDEO 9 FAMILY HOME EXPERTS ICFLOIDA ABOUT WFTV

Google Custom Search

SIGN IN REGISTER

### 9 Investigates hacked surveillance cameras across Central Florida

Updated: Nov 3, 2016 - 6:05 PM

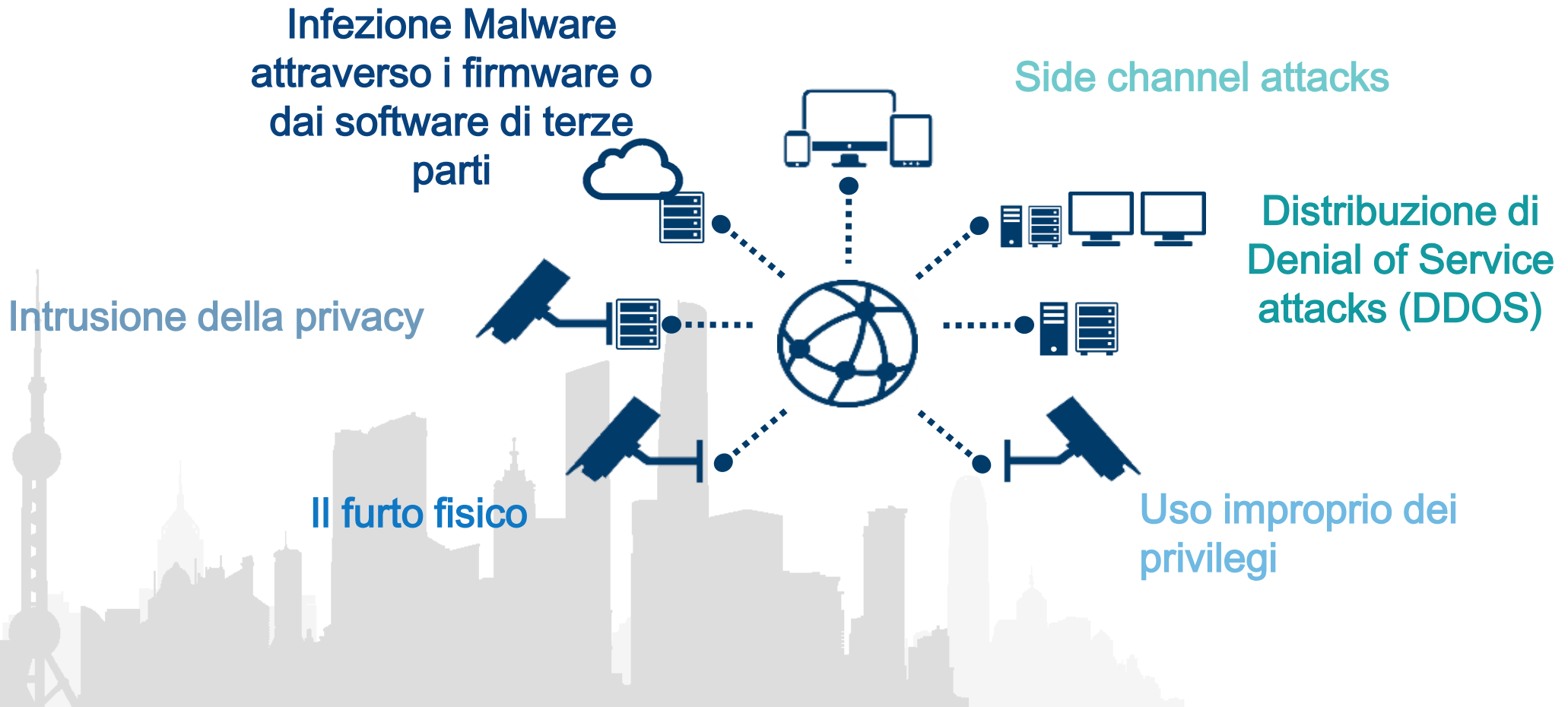
Orange County might buy much-needed





# Salvaguardare i dati della videosorveglianza

## Cosa aspettarsi



# Salvaguardare i dati della videosorveglianza

## Cos'è la data security

- ▶ “*Data security*” significa proteggere i dati, come per esempio i database, dalla distruzione e/o dall'accesso non autorizzato.”
- ▶ Proteggere i dati significa impedire l'accesso non autorizzato ai fini di prevenire la cancellazione volontaria o accidentale, virus o informazioni corrotte.





# Tenere i dati video al sicuro

## L'approccio Bosch sull'infrastruttura



1: Creare attendibilità



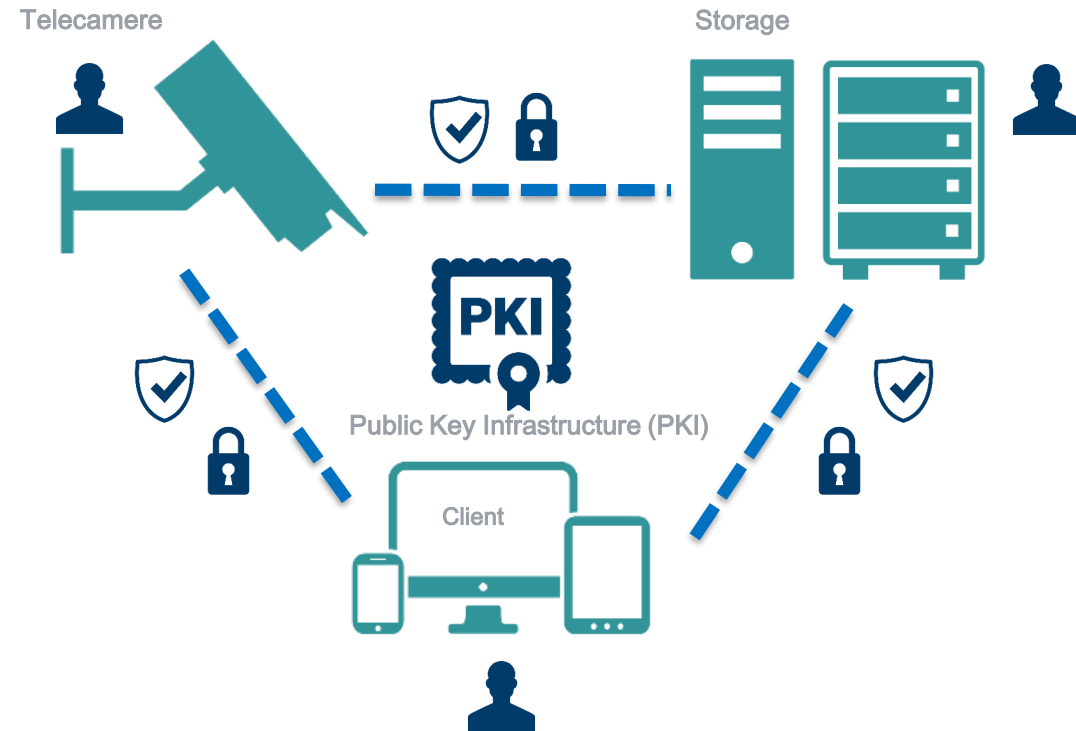
2: Proteggere i dati



3: Definire le credenziali



4: Rispettare gli standard industriali IT



**Un solo anello debole mette a rischio l'intero sistema**

# Tenere i dati video al sicuro

## Come proteggere le telecamere

### ► Misure software:

1. Solo connessioni sicure (HTTPS)
2. Password forzata
3. Porte «Non» sicure disabilitate
4. Comunicazioni remote «Non» sicure disabilitate
5. Caricamento di 3rd party software non possibile
6. Aggiornamenti sono con firmware certificato Bosch «signed firmware»

### Misure hardware:

1. Trusted Platform Module inside



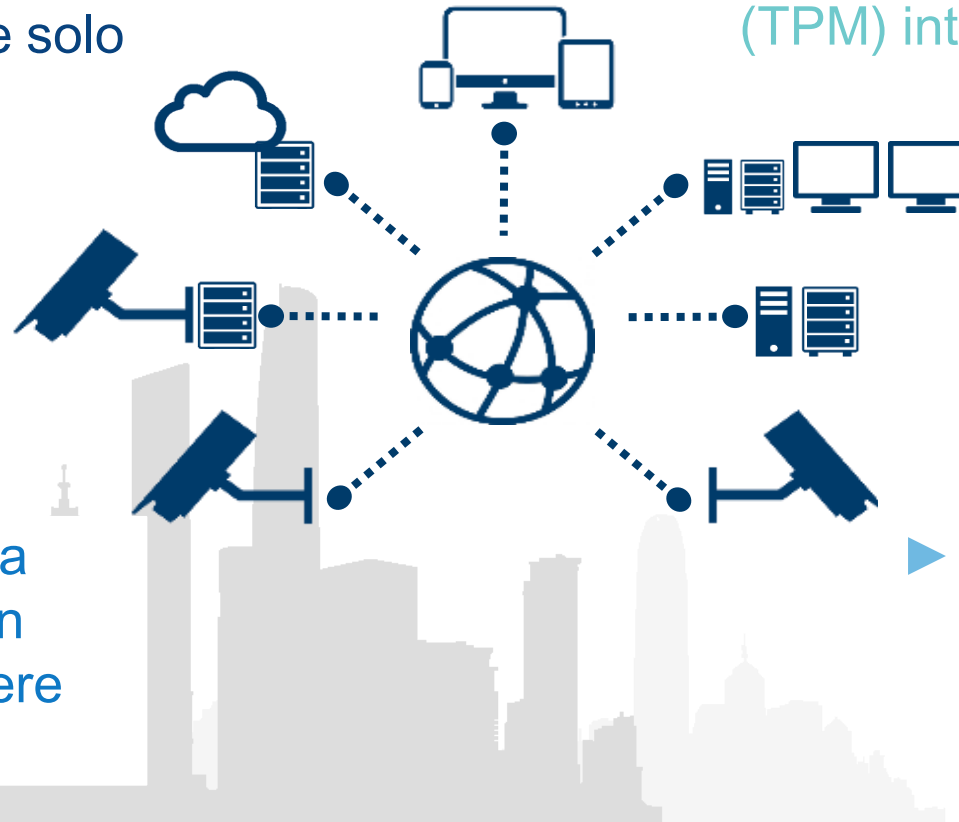
# Tenere i dati video al sicuro

## Cosa aspettarsi da Bosch

- ▶ Caricamento di software di 3rd party non possibile
- ▶ Aggiornamento firmware solo con file certificati Bosch
- ▶ Diritti di accesso nelle telecamere, nelle unità di registrazione e nel software
- ▶ Rilevazione della manomissione in tutte le telecamere Bosch

▶ Trusted Platform Module (TPM) integrato

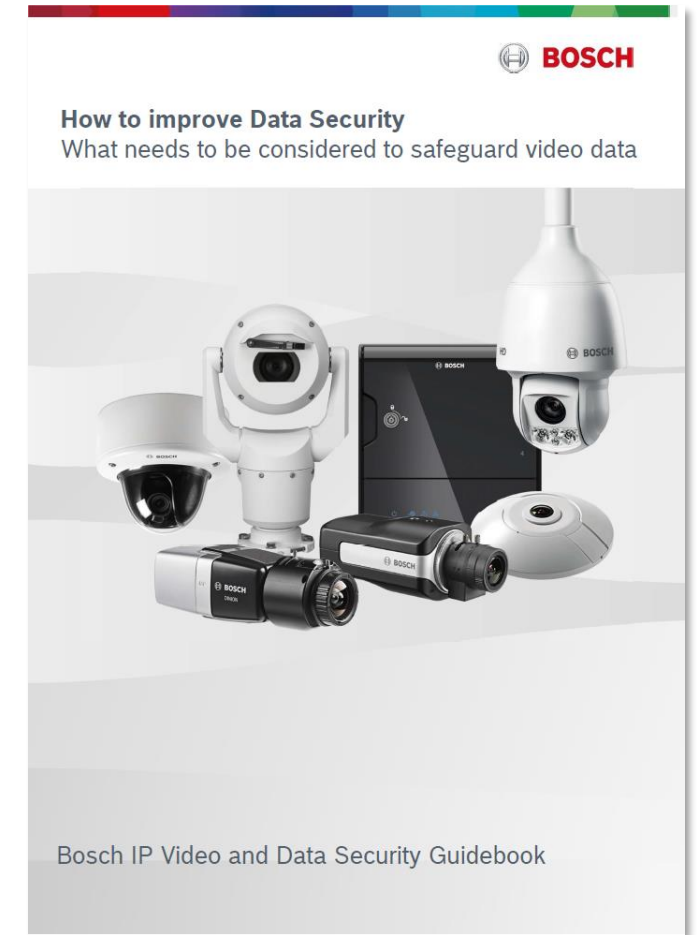
▶ Supporto di Microsoft Active Directory



# Tenere i dati video al sicuro

## Dispense

- ▶ [Linee guida Bosch IP Video Data Security](#)
- ▶ [Technical White Paper per Network Authentication 802.1x](#)
- ▶ [Technical White Paper per Trusted Platform Module \(TPM\)](#)

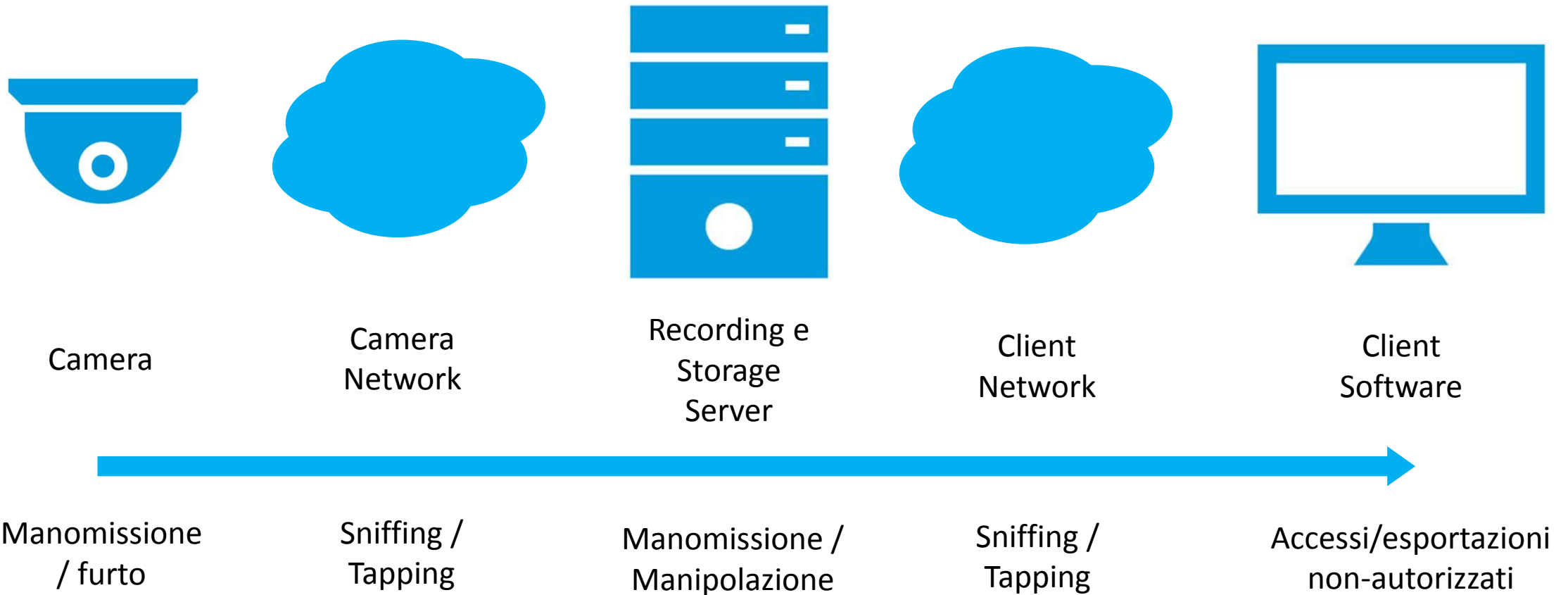


# GRAZIE

Stefano Riboli  
**Bosch Security Systems S.p.A.**  
Marketing Video Systems

Tel. +39 02 3696 3931  
[stefano.riboli@it.bosch.com](mailto:stefano.riboli@it.bosch.com)

# Security e Cybersecurity





# Camera

- **Rischio:** Camera disconnessa, rubata o danneggiata.
  - XProtect identifica e genera un evento “communication error”
  - Innesco di allarmi o regole per notificare l’evento
- **Rischio:** Camera manomessa
  - XProtect riceve eventi di manomissione e può innescare allarmi o regole per notificare l’evento.





# Camera Network

- **Rischio:** Invasa da traffico inaspettato (DDOS attack)
  - XProtect identifica e genera un evento “communication error”
  - Innesco di allarmi o regole per notificare l’evento
    - Registrazione su Edge Storage in attesa del ripristino della rete.
- **Rischio:** Accesso non-autorizzato in grado di intercettare lo stream video.
  - XProtect supporta HTTPS su alcune camera. Encryption tra camera e server (SSL).





# Recording e Storage

- **Rischio:** Windows compromesso.  
Possibilità di accesso al video database.
  - Prevenzione dell'accesso fisico e logico a Windows Server
  - Cifratura delle registrazioni
    - “Light” (solo header) o “Strong”
    - Supporto AES 256 (R2)
  - Firma digitale del database per prevenire manomissioni
    - Supporto SHA2 (Secure Hash Algorithm 2)





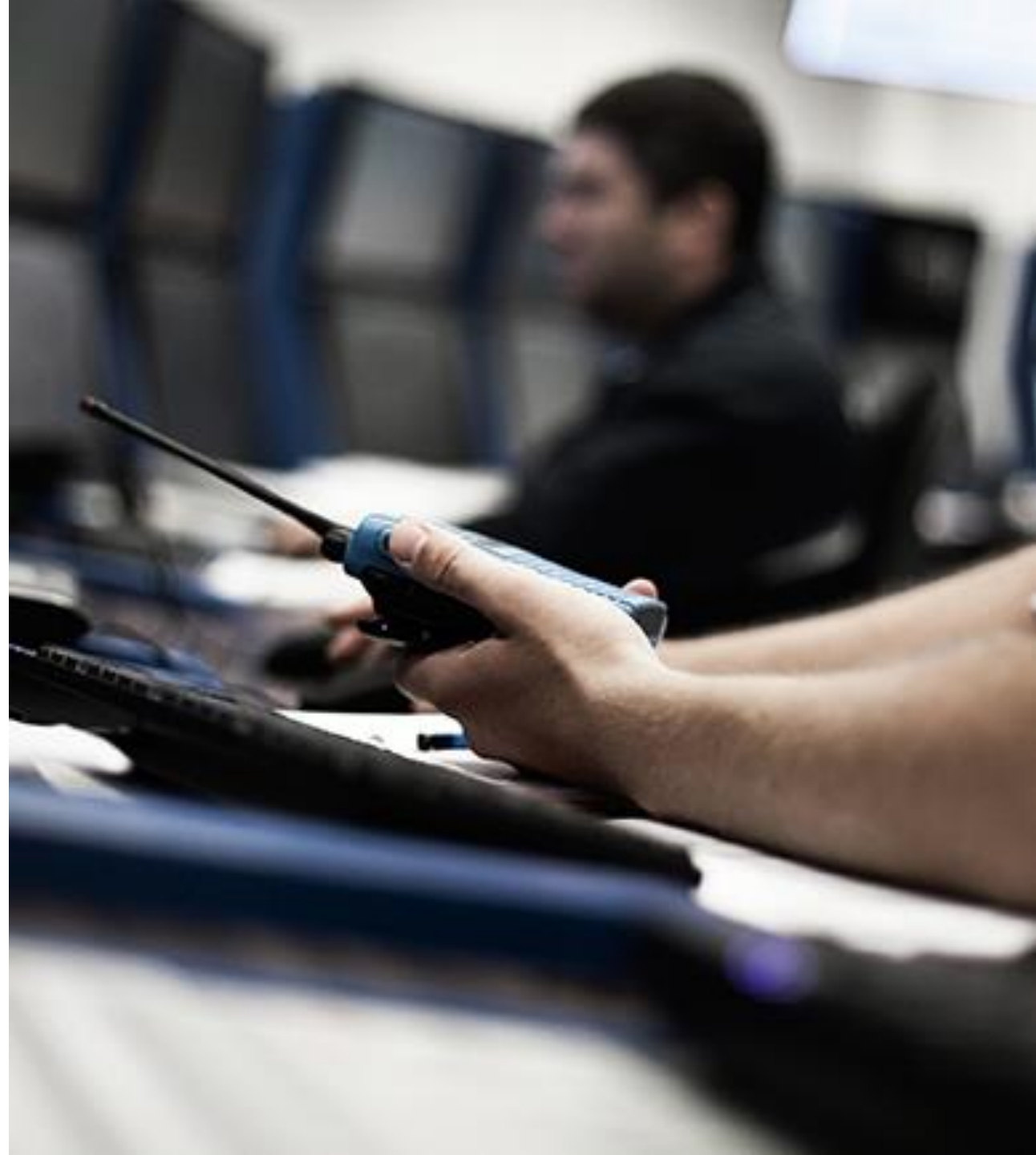
# Client Network

- **Rischio:** Invasa da traffico inaspettato (DDOS attack)
  - Perdita della visualizzazione parziale o totale
  - Registrazione garantita se implementata su rete “dedicata”
- **Rischio:** Accesso non-autorizzato in grado di intercettare lo stream video.
  - XProtect supporta HTTPS su alcune camere. Encryption tra camera e server (SSL).
  - Supporto HTTPS per Web Client e Mobile Client.



# Client Software

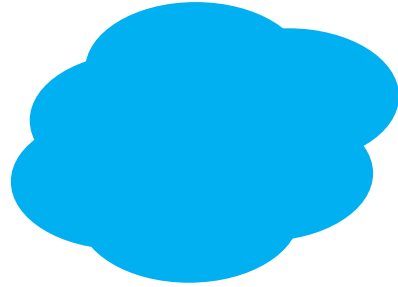
- **Rischio:** Furto o ottenimento delle credenziali di login.
  - XProtect supporta Active Directory e Kerberos
  - Accesso con userid, password di autenticazione e one-time access code
  - Abilitazione accesso per tipo di client (Smart, Web, Mobile)
  - Profilazione dell'utente client



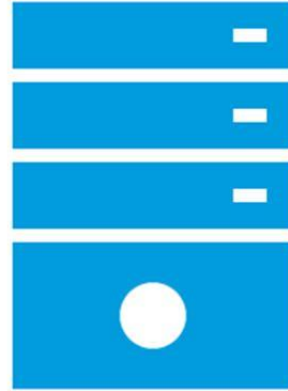
# Security e Cybersecurity



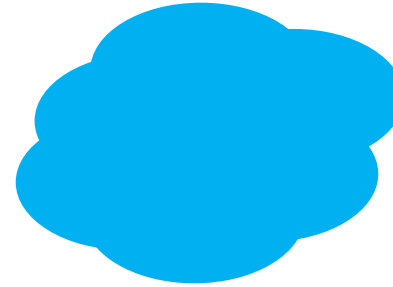
Camera



Camera  
Network



Recording e  
Storage  
Server



Client  
Network



Client  
Software



Manomissione  
/ furto

Notifiche /  
Allarmi

Sniffing /  
Tapping

Allarmi  
/HTTPS  
/Edge  
Storage

Manomissione /  
Manipolazione

Sicurezza fisica e  
logica /  
encryption /  
Firma Digitale

Sniffing /  
Tapping

HTTPS

Accessi/esportazioni  
non-autorizzati

Autenticazione/  
Accesso /Profilatura



# <https://www.milestonesys.com/support/resources/cyber-security/>



[Where to Buy](#) | [About Us](#) | [Language](#) | [My Milestone](#) | [Log out](#) | [Search](#)

[SOLUTIONS](#) | [COMMUNITY](#) | [SUPPORT](#) | [EVENTS](#) | [NEWS](#)



CYBERSECURITY

## Resource center

Suspect your system is at risk?

If you suspect a security vulnerability with a Milestone product or service, please report the problem immediately. Milestone will reply within 48 hours.

[CONTACT US](#)

Ensuring the security and integrity of all Milestone installations will always remain a top priority to us. Use this page to learn more or to contact us if you suspect you have a cybersecurity vulnerability. We minimize customers' exposure to risk by ensuring our software and hardware is secure by design, secure by default and secure by deployment.

If a vulnerability flaw is detected, Milestone will provide mitigations and/or software updates as soon as possible with security fixes to customers and partners free of charge – provided the product is still supported.

These documents help you choose and implement the right level of security for your system:



Milestone CyberSecurity Development Policy



Milestone XProtect® VMS System Security Feature Brief



Milestone Hardening guide

# Domande ?



# Grazie !