



Soluzione integrata per le **Sicurezza** e l'**Efficienza**  
di reti cablate e wireless



X



# B<sup>5</sup> Chi siamo



**Founded in 2007**  
by security professionals



**40+ patents**  
Teamed by patent-inventor engineers in Cyber Security



**20+ years experience**  
in Government security projects



**Agile company**  
for rapidly changing scenarios



**Award-winning Technologies**



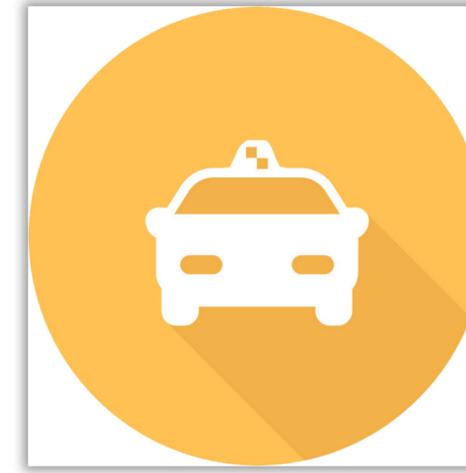
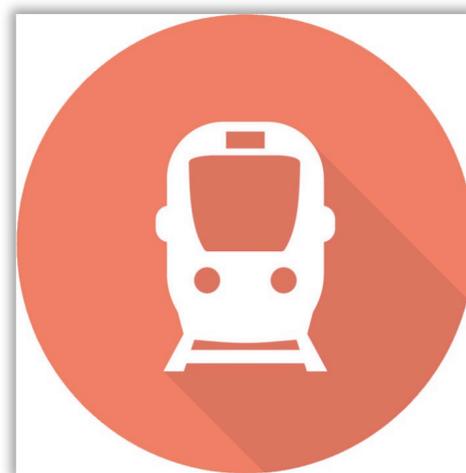
# Chi siamo

VIFRAM è una società presente da circa 23 anni sul mercato italiano, leader nelle soluzioni tecnologiche in ambito industriale, automotive e militare.

Con un organico di circa 50 collaboratori, accresce costantemente il proprio know-how nel settore dell'elettronica e delle telecomunicazioni con una continua ricerca di soluzioni tecnologiche all'avanguardia che rispondano alle esigenze dei propri clienti.

Per mantenere i livelli di qualità raggiunti, VIFRAM investe costantemente in ricerca e formazione per migliorare le prestazioni produttive ed essere adeguata agli standard di processo più evoluti.

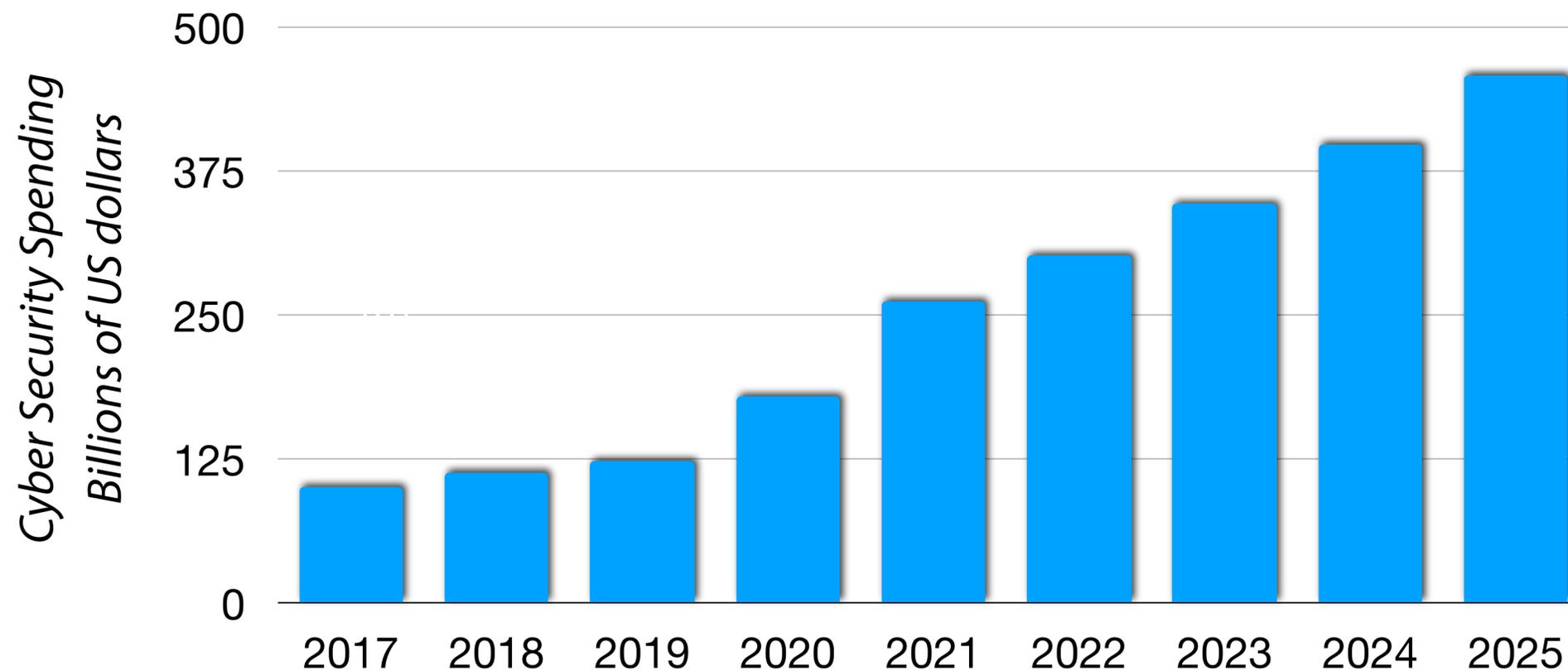
Da questo principio nasce l'esigenza di sviluppare una soluzione che offra al settore del TPL uno strumento valido, sicuro ed efficace per risolvere i problemi di sicurezza delle trasmissioni di dati sulle reti wireless e cablate, da qui nasce la collaborazione con B5, azienda leader nel settore della cyber security.



The image features a 3D bar chart with several bars of varying heights, colored in shades of blue, purple, and orange. A large, thick, multi-colored arrow (red, orange, and yellow) points upwards and to the right, starting from the bottom left and passing over the top of the bars. The background is a light blue and white grid with faint, semi-transparent data points and lines, suggesting a digital or analytical environment.

***Aumentare il budget  
migliora la sicurezza delle reti?***

La spesa mondiale per prodotti e servizi di Cyber Sicurezza ha superato i 114 miliardi di dollari nel 2018, con un aumento del 12,4% rispetto al 2017\*. Gartner ha previsto un tasso di crescita annuale del 8,5% fino al 2022\*\*. Cybersecurity Ventures ha stimato un totale cumulativo di 1,75 trilioni di dollari dal 2021 al 2025\*\*\*



Sources:

\* Gartner: *Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019*

\*\* Gartner: *Forecast Analysis: Information Security, Worldwide, 2Q18 Update*

\*\*\* Cybersecurity Ventures: <https://cybersecurityventures.com/cybersecurity-spending-2021-2025>

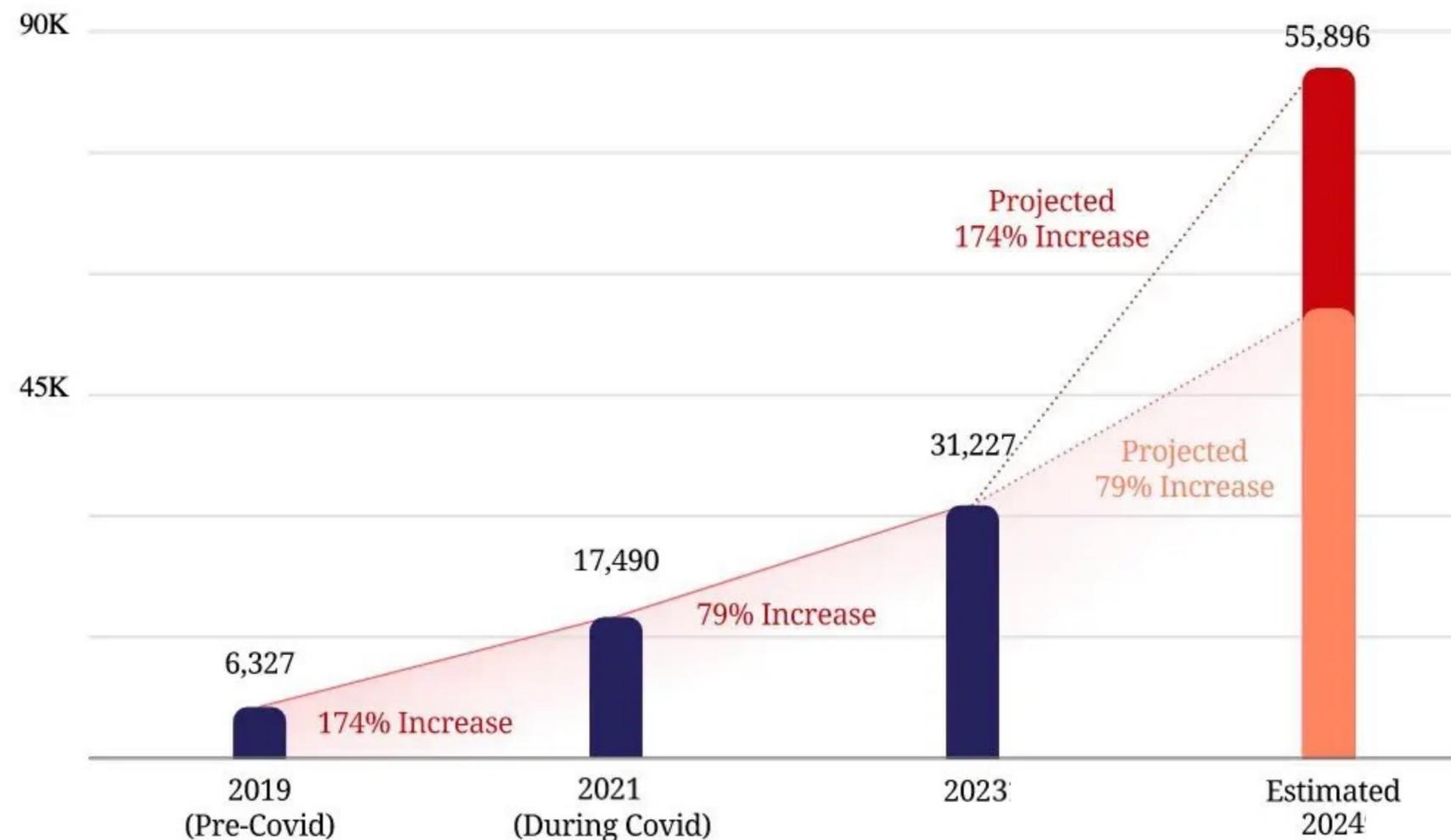
**Gli attaccanti  
diventano ogni  
giorni più forti**

**Oltre il 79% di  
violazioni dal  
2021 al 2023 e le  
proiezioni per il  
2024 sono  
disastrose**

Sources:

\* Coro: <https://go.coro.net/cyberthreats2022>

## Actual and Projected Number of Attacks per Company



Le organizzazioni iniziano a chiedersi se l'aumento dei budget riduca effettivamente gli incidenti informatici



# Le soluzioni tradizionali non sono più sufficienti!



**Gartner**<sup>®</sup>

---

Gartner Security & Risk Management Summit, Nov 2021

# Evoluzione della Sicurezza di Rete



# E se non ci fosse nulla da attaccare?

Creare un Air-Gap Reale  
attraverso Reti Virtuali



**SElink**<sup>TM</sup>

# Cyber Resilienza - Cyber Security in chiave moderna

*Zero Trust Approach*

*Assumed Breach Model*

*How effectively an  
organisation manages  
cyberattacks or breaches  
while maintaining  
business operations*

*Logic Inversion*

*Paradigm Shift*

# Ecosistemi Smart Bus

## Sfide

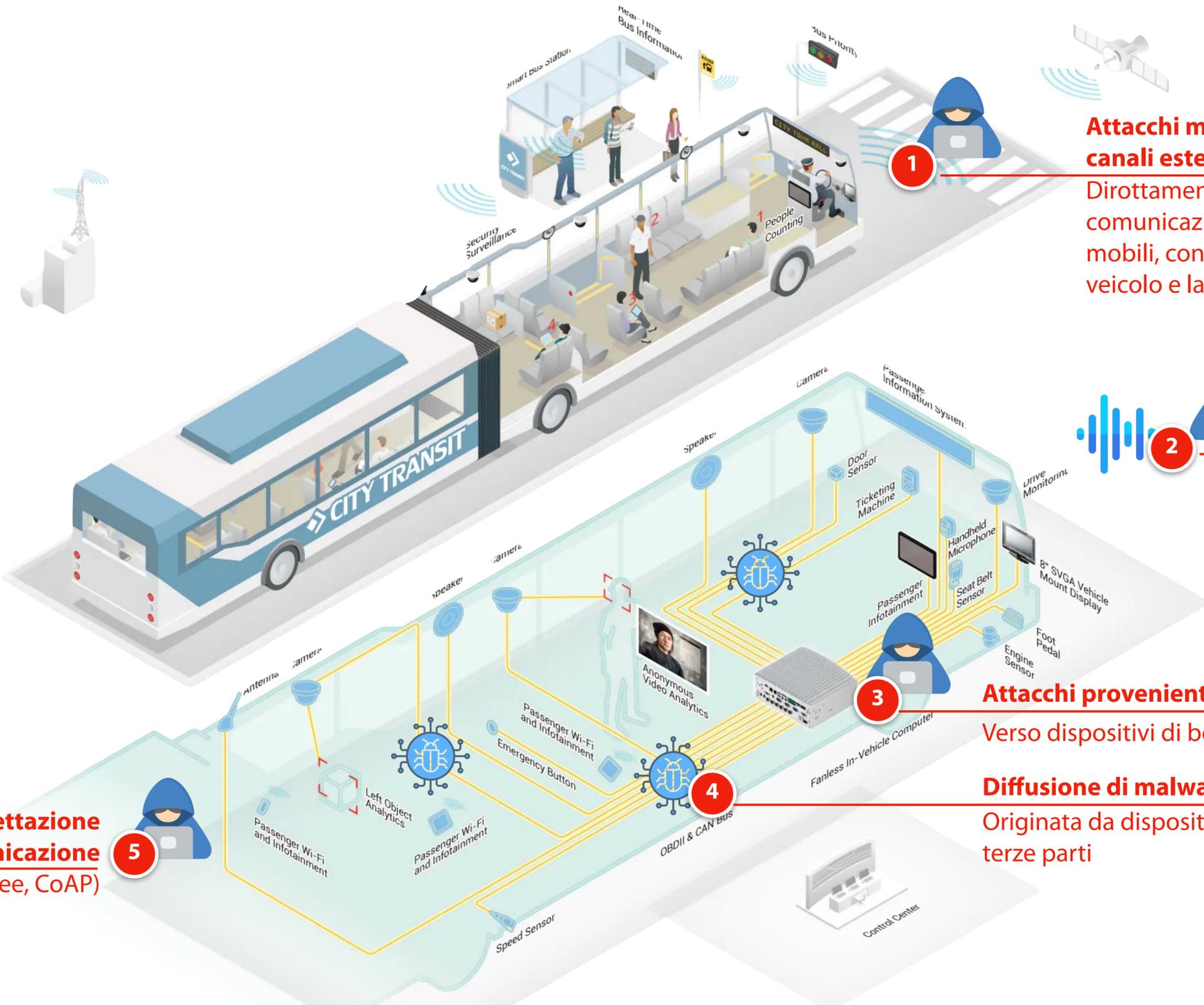
- Tracciamento in tempo reale delle condizioni dei passeggeri e degli autisti nei bus navetta
- **Connettività di rete affidabile e costante** nei veicoli in movimento
- **Larghezza di banda elevata** per supportare streaming video di alta qualità e senza interruzioni
- **Interruzione del servizio** e delle informazioni
- **Manipolazione e intercettazione dei dati**
- **Perdite finanziarie**



Soluzione di Zero Trust Networking per una migliore connettività, semplificazione della rete e resilienza da attacchi informatici.

Strategie di **Virtualizzazione Sicura** delle reti combinate con **Strategie di Accesso alla rete** basate su principi Zero Trust.

# Superficie di attacco di un veicolo



**Attacchi mirati all'intercettazione di canali esterni di comunicazione**

Dirottamento e controllo delle comunicazioni esterne tramite canali radio mobili, connessioni satellitari e WiFi tra il veicolo e la stazione di controllo

**Attacchi a servizi di terze parti**

Aggiornamenti di sistema, manutenzione e troubleshooting

**Attacchi provenienti da dispositivi non autorizzati**

Verso dispositivi di bordo

**Diffusione di malware**

Originata da dispositivi locali e remoti controllati da terze parti

**Attacchi mirati all'intercettazione di canali interni di comunicazione**  
(Bluetooth, MQTT, ZigBee, CoAP)



Soluzione di **Cyber Security** per  
**Sistemi Integrati di Trasporto Pubblico**  
basata su strategie **Zero Trust** e **Resilienza**

# Sistemi di Trasporto Pubblico Sicuri ed Efficienti

## Integrazioni native in Sistemi e Dispositivi di Terze Parti



### Telecamere

Sistemi multi-vendor di Video Sorveglianza e Video Analytics



### Sistemi di bigliettazione

Per pagamenti elettronici e interoperabili

### Gateway AVM

Sistemi di bordo per comunicazioni tra dispositivi e Stazione di Controllo



### Conteggio Passeggeri

Sistemi multi-vendor per il rilevamento dei passeggeri

### Validatore e Controllo Accessi

Sistemi di controllo di accesso e validazione documento di trasporto



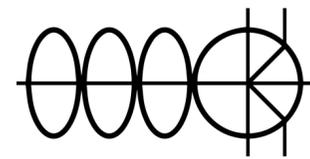
### Router

WiFi per comunicazioni con fornitori di servizi di trasporto e tra dispositivi



Blu5 Group

X



**VIFRAM**

*Manage the Change*