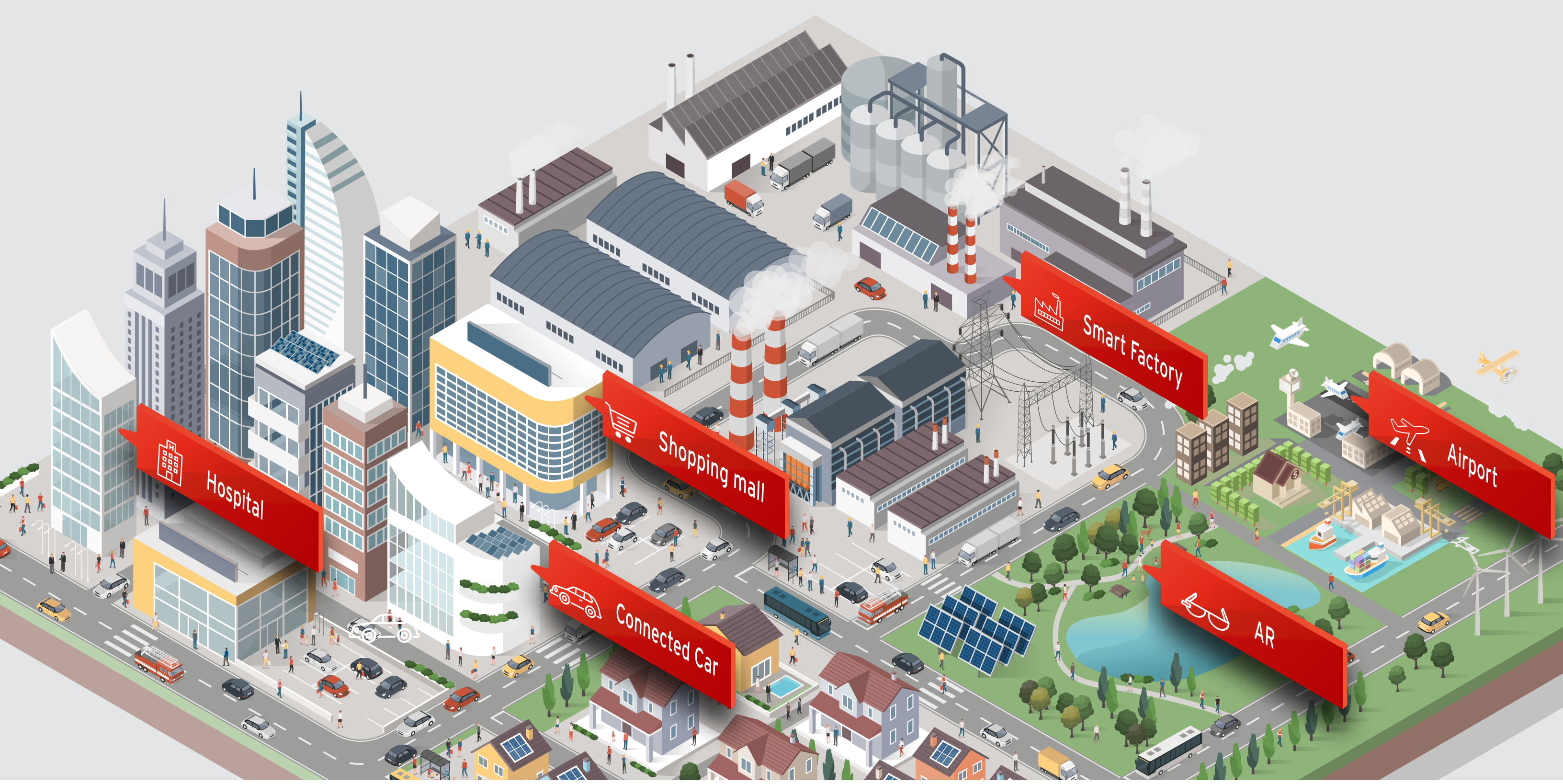
A HYBRID CYBERSECURITY SOLUTION
FOR ENTERPRISE PRIVATE MOBILE NETWORKS



Trend Micro™

Mobile Network Security

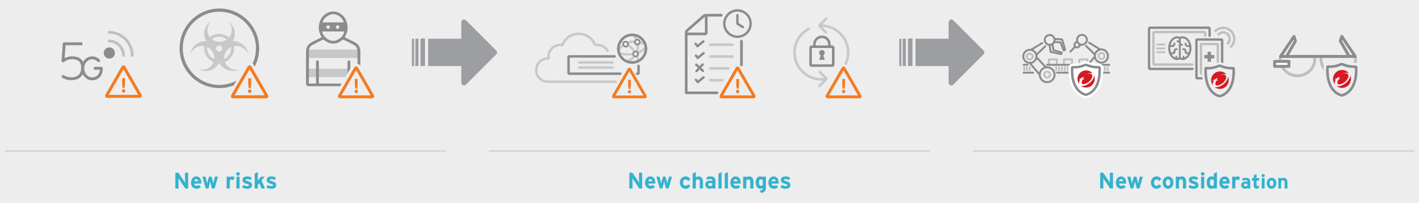
Securing Enterprise Private Mobile Networks

Advancements in connectivity bring new possibilities. It is essential to prepare for cyber threats that stem from utilizing connected mission-critical applications in a borderless internet of things (IoT) network environment.

Securing the new reality of connectivity

New technological evolutions to IoT and advanced mobile networks like 5G will push mission-critical network-security management for enterprises to new levels.

As we transition to the new reality, the ideal cybersecurity solution balances harmonized networks with the emerging mobile technology.



New risks

New challenges

New consideration

Challenges faced by enterprises when deploying a private mobile network:

Risky entry points

- SIM cards can be lost or stolen, allowing attackers to access a customer's private mobile network
- Employees may violate company policy by installing a company-issued SIM card on a risky device

Lack of device and security visibility

- Traditional IT security products do not know which cellular user equipment (UE) is at risk because they are unfamiliar with International Mobile Equipment Identity (IMEI) or International Mobile Subscriber Identity (IMSI), which are used in communications technology (CT) networks
- CT solutions are generally bad at identifying threats

Hard to manage security policies

- The IP address of a UE in a private mobile network change occasionally, thus, security management can no longer be based on IP addresses

Lack of expertise in CT and IT integration

- Interconnection between CT and IT can be a challenge when managing private mobile network security across these two heterogeneous platforms

Quick response needed

- Some advanced IT security products may know which UE is risky, but security operators can still have difficulty with quickly responding to and preventing the UE from accessing its CT network. This is because UEs access to its CT network is managed by CT system, and it takes time for a security operator to respond to the threat between IT and CT networks

Critical assets need to be protected

- Edge computing application servers, such as facial recognition, mixed reality (MR), and automatic optical inspection (AOI) on your multi-access edge computing (MEC) system, are generally closed systems. This makes it hard to install any existing security products on them, thus, they can be vulnerable to threats
- UEs in a private mobile network may have difficulty maintaining the most up-to-date patches, therefore making them vulnerable to threats

Trend Micro™ Mobile Network Security (TMMNS)

TMMNS is a hybrid cybersecurity solution developed for enterprise customers to ensure the security of mobile user equipment (UE) and IoT endpoint devices, as well as critical edge computing application servers that reside inside of the enterprise's campus network. Based on the European Telecommunication Standards Institute (ETSI) Network Functions Virtualization (NFV) framework, TMMNS provides a fully virtualized solution that has the flexibility and agility to be deployed in the most popular commercial and open source virtualization platforms with high performance and low latency. Unlike most traditional cybersecurity solutions, TMMNS bridges the gap between information and communication technologies (IT/CT) to provide comprehensive protections, covering the network and endpoint layers to help customers face the new and diverse threats being seen throughout cyberattacks in 4G/LTE, NB-IoT, and the 5G network.

Joint-defense Between Network and Endpoint

As a comprehensive solution, TMMNS offers two-layers of protection for your private mobile network:

- **TMMNS Network Protection** Identifies and blocks vulnerability exploitation, malicious content, and suspicious network behaviors at the data network of a mobile network core, protecting your private mobile network at the network level
- **TMMNS Endpoint Protection** Provides cellular UE visibility, identifies illegitimate cellular UE, and denies a cellular UE access to its radio access network, protecting your private mobile network at the endpoint level

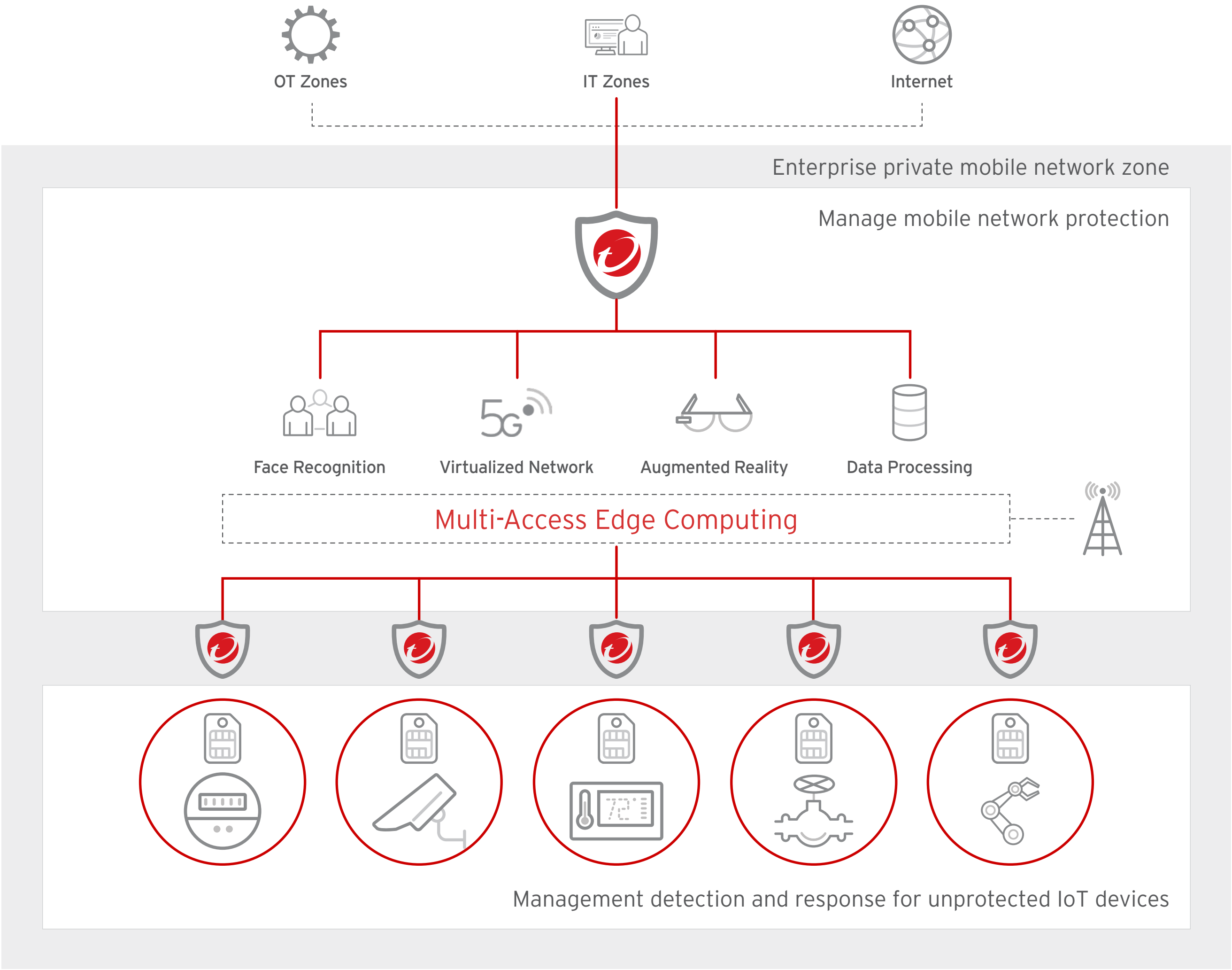
TMMNS Network Protection and TMMNS Endpoint Protection provide multi-layered protections by performing their functions in individually while simultaneously working together to provide a join defense against cyber threats.

Benefits

- **Meet end-to-end security** in mission-critical private mobile networks
  - Ensures that your mobile UE, IoT endpoint devices, and application servers on your MEC system are well protected
  - Prevents misused or illegitimate UEs from attacking your IT or OT networks
  - Offers you an additional security protection layer across CT/endpoint and IT/network
  - Blocks risky cellular UE access to its radio access network, ensuring your private mobile data network is clean
- **Reduce security management workload** of IT sec admin in enterprise ICT
  - Purpose-built for seamless CT and IT integration without third-party systems; security policy management is based on IMEI/IMSI rather than on IP address
  - Visibility of risk status for each cellular UE
  - Simple yet efficient security management in one console
- **Cost efficiency** for deployment in mission-critical private mobile networks
  - No third-party systems needed for CT and IT integration, making deployment cost-efficient
  - Agentless and no firmware integration required for each cellular UE

Trend Micro™ Mobile Network Security (TMMNS)

Comprehensive hybrid cybersecurity solutions for enterprise private mobile networks


OT Zones
IT Zones
Internet
Enterprise private mobile network zone
Manage mobile network protection
Face Recognition
Virtualized Network
Augmented Reality
Data Processing
Multi-Access Edge Computing
Management detection and response for unprotected IoT devices

Trusted Device Management

via physical SIM card or Java applet

- ✓ Unprotected IoT security
- ✓ Trusted IoT link
- ✓ Device isolation
- ✓ Data security

Comprehensive Network Protection

via virtual software solution

- ✓ East-west network protection to secure edge computing application traffic
- ✓ North-south network protection to secure UE and IoT endpoint devices

Protection throughout various vertical markets

Our solutions help system integrators leverage shared band or unlicensed band radio to help build their customer's private mobile network.

Shopping Mall

Smart Factory

Port

Airport

Mining

Enterprise

Over 30 Years of Trusted Cybersecurity Leadership

Global Threat Research

To help you better understand and address the security challenges of today and tomorrow.

450+
internal threat researchers and data scientists

10,000
registered white hat researchers from 100 different countries

100s of millions
of threats blocked daily

Customers Agree

With over 500,000 commercial customers and offices in over 65 countries, Trend Micro protects many of the largest organizations in the world.

FORTUNE
GLOBAL
500

- 10 of Top 10 Telecom
- 9 of Top 10 Petroleum
- 9 of Top 10 Healthcare
- 8 of Top 10 Banking
- 8 of Top 10 Automotive

Contact us at
https://www.trendmicro.com/5G-IoT-contact

TREND MICRO™
Securing Your Connected World

[SB02_Mobile_Network_Security_210406US]