Datasheet

Trend Micro™ Mobile Network Security (TMMNS)

Secure your enterprise mobile IoT networks

Trend Micro™ Mobile Network Security (TMMNS), powered by CTOne, is a hybrid cybersecurity solution developed for enterprises to ensure the security of mobile user equipment (UE) and internet of things (IoT) endpoint devices. In addition, it protects 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 you with a fully virtualized solution. You're given the flexibility and agility to be deployed in the most popular commercial or open-source virtualization platforms with high performance and low latency.

Unlike most traditional cybersecurity solutions, TMMNS allows you to bridge the gap between information and communication technologies (IT/CT) to provide comprehensive protection, covering the network and endpoint layer to help customers face the new and diverse threats being seen in cyberattacks across 4G/LTE and 5G networks.

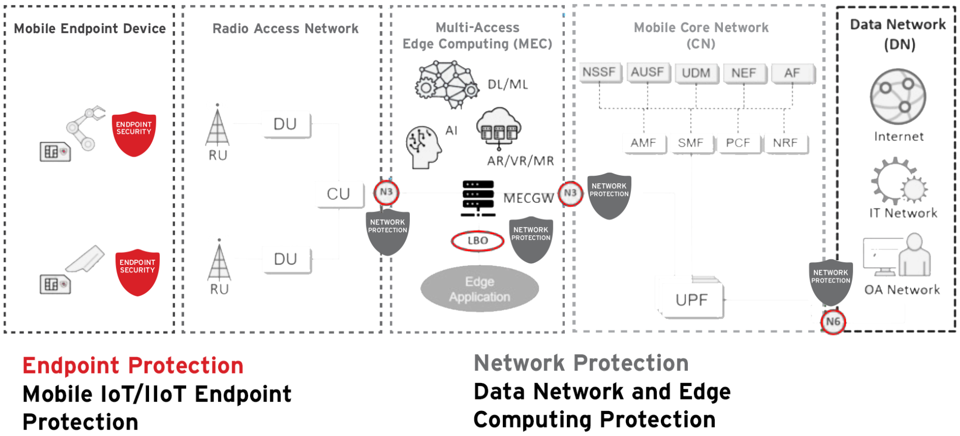

Figure 1: TMMNS, powered by CTOne, in a mobile network

Hybrid Protection for the Network and Endpoint

TMMNS includes two layers of protection, one for the network and the other for the endpoint. These two solutions can work independently, as well as interact closely to provide you with the most complete cybersecurity.

Trend Micro™ Mobile Network Security (TMMNS) Network Protection

TMMNS Network Protection is equipped with deep packet inspection (DPI) and innovative network packet acceleration technologies. This gives you the ideal balance between security and processing capability. With virtual central processing unit (vCPU) resources, a single TMMNS Network Protection instance (network traffic processing element) can achieve 10 Gbps when all features are enabled. Utilizing the ETSI NFV framework, you can deploy TMMNS Network Protection transparently on multiple network points (for example N3/N6/LBO) to detect cyber threats and access control of your endpoints. This is done through inline or mirror mode without changing the current network architecture.

By monitoring the internet protocol (IP) and General Packet Radio System (GPRS) Tunneling Protocol (GTP) traffic in a mobile network, TMMNS Network Protection identifies vulnerabilities, threats, malicious content, and suspicious network behaviors. Once identified, they are blocked in the wire to protect your mobile UE/IoT endpoint devices.

Protection Points

- Mobile IoT endpoint devices
- Edge computing application servers
- Mobile network core system

Threat Protection

- Mobile data network access control
- Mobile radio network access control
- Intrusion prevention
- Virtual patching
- Web URL categorization
- Malicious web content filtering
- IoT reputation service
- Zero-trust security

Threat Intelligence

Trend Micro and CTOne continue to evolve and improve their entire ecosystem of integrated security products. At the heart of their layered, continually evolving threat detection is Trend Micro™ Smart Protection Network™. Hundreds of millions of sensors are deployed globally to collect suspicious objects and behaviors before being sent back to a cloud-based analyzing center for heuristic machine learning and continuous big-data analysis. Trend Micro™ Zero Day Initiative™ (ZDI), the world's largest vendor-agnostic bug bounty program, has more than 18 years of proven experience securing the ecosystem of critical enterprise-class vulnerabilities.

Empowered by these powerful threat intelligence sources, TMMNS Network Protection provides you with early protection and the most efficient defense.

Trend Micro™ Mobile Network Security (TMMNS) Endpoint Protection

TMMNS Endpoint Protection is delivered by secure Java applet software that can be deployed on a variety of subscriber identity modules (SIM), including a physical SIM, eSIM, and iSIM. This allows you to harden mobile UE and IoT endpoint device security in a mobile network environment.

More enterprises are embracing cutting-edge 5G technology to connect mobile IoT endpoint devices for critical, daily operations. The IoT environment has become diverse, complex, and fragmented. By leveraging a SIM, you gain a full-standardized secure element and universal platform to enable a simple plug-and-play security service. Initially, TMMNS Endpoint Protection helps your IT and InfoSec administrators establish visibility of all cellular IoT endpoint devices—an important security management baseline.

The zero-trust security posture creates a virtual perimeter to define a network accessing boundary. Device isolation provides your administrators with the ability to control mobile radio network access to mitigate the threats spreading from suspicious mobile IoT endpoint devices. TMMNS Endpoint Protection provides you with the visibility, detection, and response capabilities required to secure customers' mobile IoT endpoint devices.

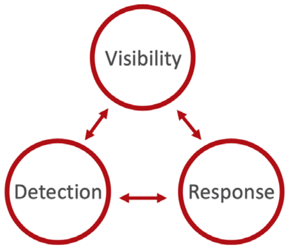

Figure 2:
Value of TMMNS

Interactions Between Network and Endpoint (Joint-Defense)

TMMNS Network Protection and TMMNS Endpoint Protection perform their functions in their respective positions while simultaneously working together to give you a joint defense against cyber threats. The multi-layered protection turns TMMNS into a comprehensive solution.

Zero-Trust Management

The principal management of TMMNS across mobile networks is based on zero-trust management. TMMNS verifies the identity and confirms the behaviors in multi-phases; from endpoints, radio ID locations and network services, to destination. This ensures every UE`s identity and behavior is trustworthy to access each phase of the 5G framework.

Specifications

TMMNS Hardware Requirements

COMPONENTS	VCPU CORE	RAM	DISK SPACE
TMMNS Management Server	4	8 GB	100 GB
TMMNS Inspector	2	12 GB	8 GB

TMMNS Endpoint Protection SIM Card Specification

ITEMS	SPECIFICATION
Java Card Platform Version	3.0 or above
RAM	8 KB
EEPROM/Flash	128 KB
USIM Application Toolkit (USAT)	Yes
Remote File Management	Yes

For details about what personal information we collect and why, please see our Privacy Notice on our website at: **www.trendmicro.com/privacy**

CTOne, A subsidiary of Trend Micro, offers enterprise cybersecurity solutions for next-generation wireless networks. **www.ctone.com**

Request for demo or proof of concept:
www.trendmicro.com/5G-IoT-contact

[DS07_Mobile_Network_Security_Datasheet_230615US]