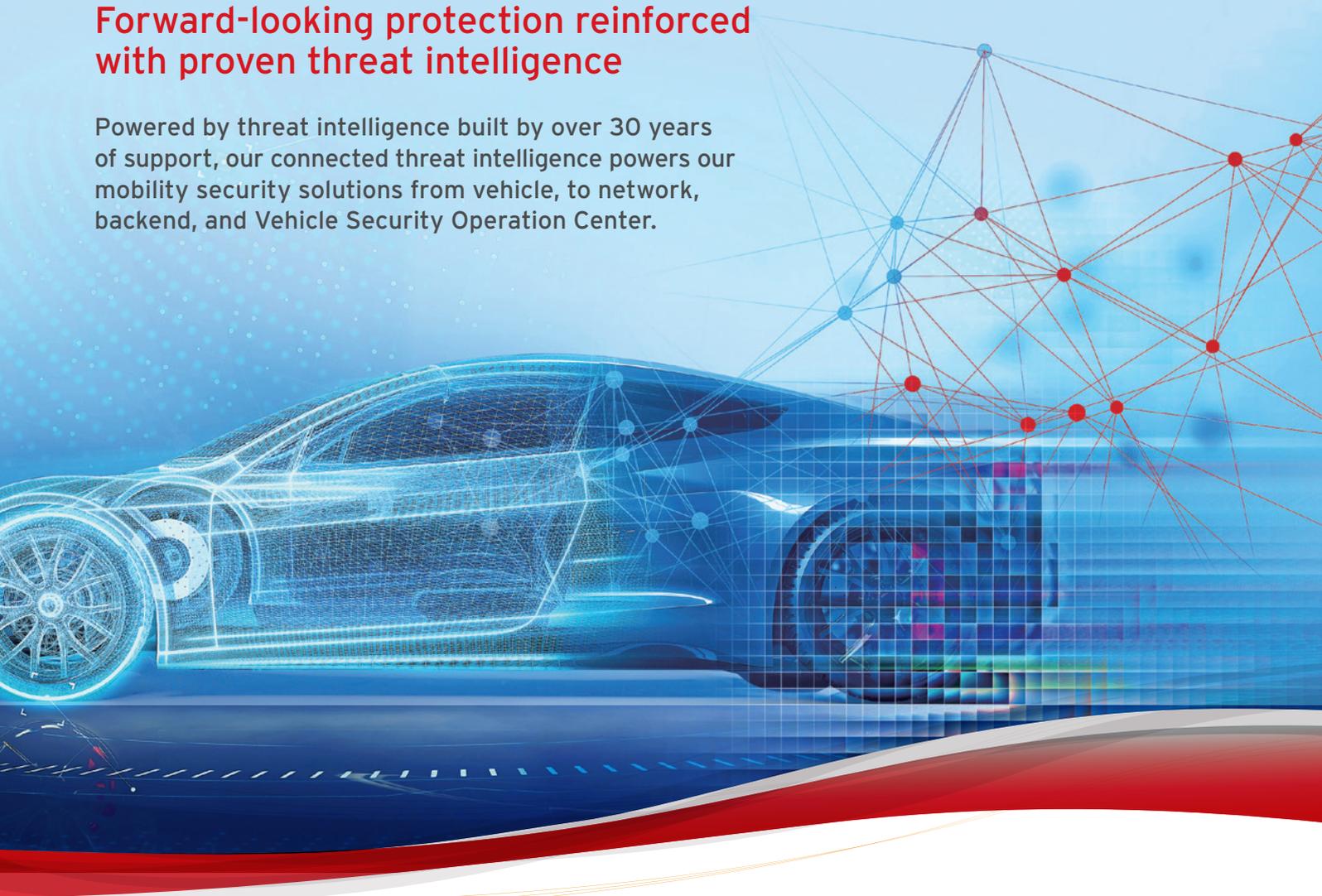**TREND MICRO**™

Securing the Ever-Changing World of Mobility

Forward-looking protection reinforced with proven threat intelligence

Powered by threat intelligence built by over 30 years of support, our connected threat intelligence powers our mobility security solutions from vehicle, to network, backend, and Vehicle Security Operation Center.
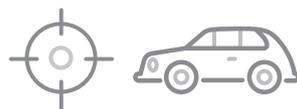
Growing Threats to Connected Cars

As the number of entrances increases, security risks grow

As cars become more connected, they become more vulnerable to outside threats. This creates greater opportunity for an attacker to steal data, disrupt operations, or take over a vehicle's control.

The automotive industry is becoming a more attractive target

Connected cars collect enormous amount of valuable data, such as personal information, vehicle numbers, location data, and driving history. This data can be stolen and used for cyberattacks that could endanger vehicle and driver safety.
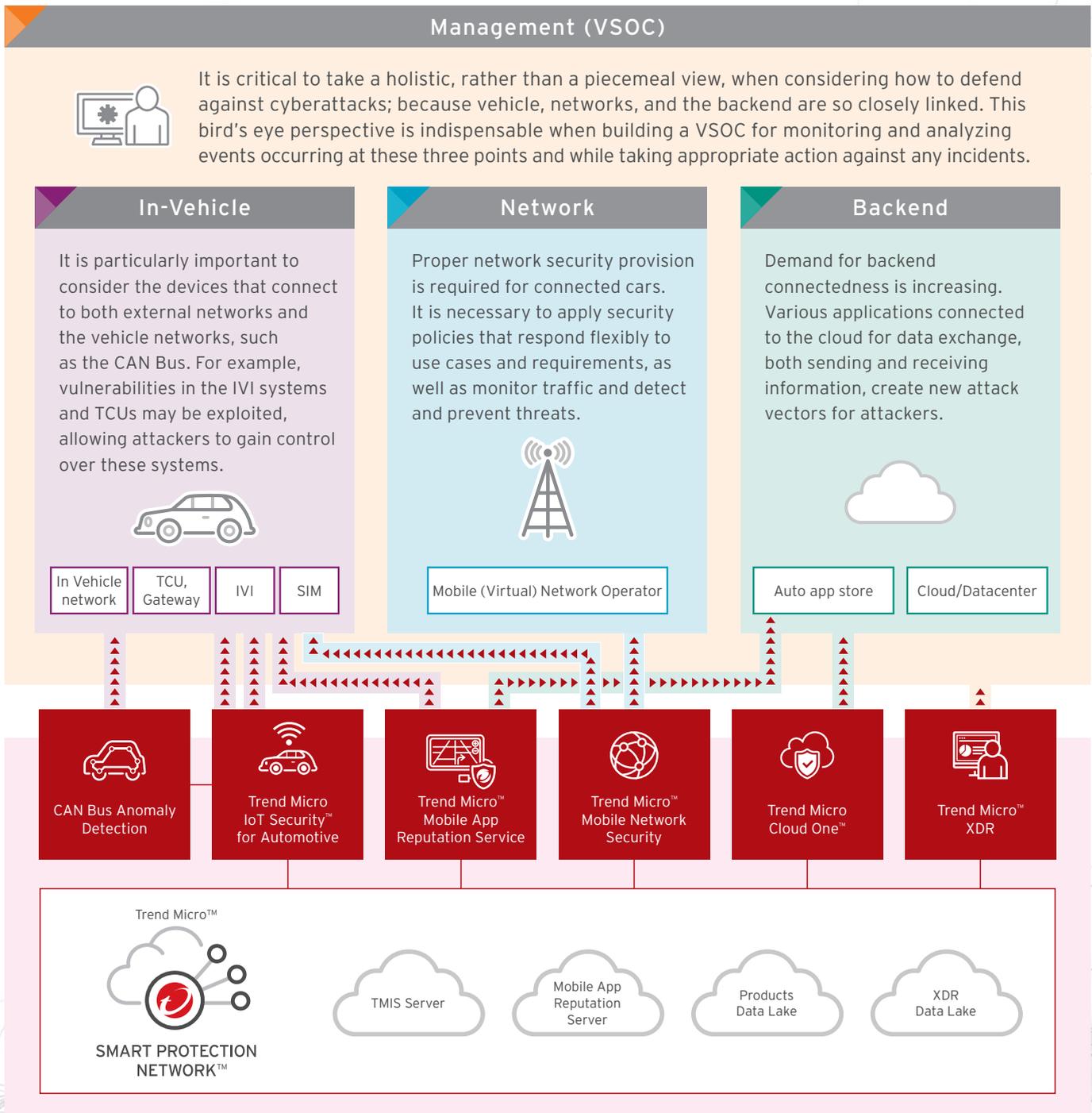
The number of cyberattacks are growing rapidly

Year by year, cyberattacks against vehicles are increasing. Hereafter, as 5G begins to expand and vehicles become more connected, the number of attacks increase at an ever-accelerating rate.

Four Key Areas in Connected Car Security

As connected cars have become information communication hubs, it is critical to offer comprehensive protection against cyberattacks at four points: the vehicle, the network, the backend, and the Vehicle Security Operation Center (VSOC).

Management (VSOC)

It is critical to take a holistic, rather than a piecemeal view, when considering how to defend against cyberattacks; because vehicle, networks, and the backend are so closely linked. This bird's eye perspective is indispensable when building a VSOC for monitoring and analyzing events occurring at these three points and while taking appropriate action against any incidents.

In-Vehicle

It is particularly important to consider the devices that connect to both external networks and the vehicle networks, such as the CAN Bus. For example, vulnerabilities in the IVI systems and TCUs may be exploited, allowing attackers to gain control over these systems.

| In Vehicle network | TCU, Gateway | IVI | SIM |

Network

Proper network security provision is required for connected cars. It is necessary to apply security policies that respond flexibly to use cases and requirements, as well as monitor traffic and detect and prevent threats.

Mobile (Virtual) Network Operator

Backend

Demand for backend connectedness is increasing. Various applications connected to the cloud for data exchange, both sending and receiving information, create new attack vectors for attackers.

| Auto app store | Cloud/Datacenter |

CAN Bus Anomaly Detection

Trend Micro IoT Security™ for Automotive

Trend Micro™ Mobile App Reputation Service

Trend Micro™ Mobile Network Security

Trend Micro Cloud One™

Trend Micro™ XDR

Trend Micro™

SMART PROTECTION NETWORK™

TMIS Server

Mobile App Reputation Server

Products Data Lake

XDR Data Lake

The Trend Micro™ Smart Protection Network™

The Smart Protection Network uses proactive techniques like machine learning, artificial intelligence, and behavior monitoring to provide customers with advanced protection. We can accurately detect and quickly defend customers from both known and unknown threats. We block 180M+ threats and identify 18M+ new and unique threat every day, stopping threats before they reach you.

SMART PROTECTION NETWORK

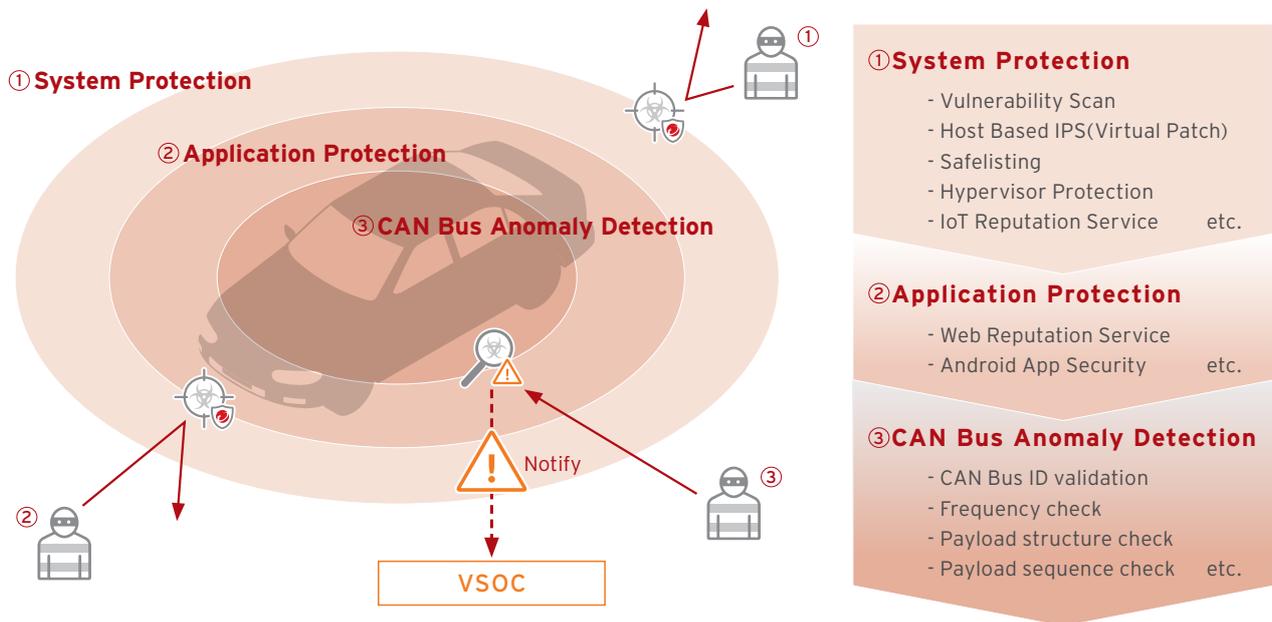# Trend Micro as Your Connected Car Security Provider

It is important to holistically enhance the security of connected cars instead of piecemeal measures at the vehicle, network, or backend level. This also enables uniform management and control.
Trend Micro offers comprehensive defense and a proven solution to support connected car management, defending against attacks that target the vehicle, network, and backend. Providing a multi-layer response to cyberattacks, Trend Micro offers protection, detection, response, and monitoring.

In-Vehicle

Trend Micro IoT Security™ for Automotive (TMIS for Auto)

TMIS for Auto is a security solution that monitors and protects critical devices (e.g, the IVI). By linking to Trend Micro's Threat Intelligence System, it can quickly detect security risks and protect connected cars—along with their systems, applications, and CAN Bus—from ever-growing threats.

① System Protection

② Application Protection

③ CAN Bus Anomaly Detection

① System Protection

Notify

VSOC

① System Protection
- Vulnerability Scan
- Host Based IPS(Virtual Patch)
- Safelisting
- Hypervisor Protection
- IoT Reputation Service   etc.

② Application Protection
- Web Reputation Service
- Android App Security   etc.

③ CAN Bus Anomaly Detection
- CAN Bus ID validation
- Frequency check
- Payload structure check
- Payload sequence check   etc.

Network

Trend Micro™ Mobile Network Security

Applies the appropriate network security protocols for connected cars to monitor traffic, detect threats, and take countermeasures.
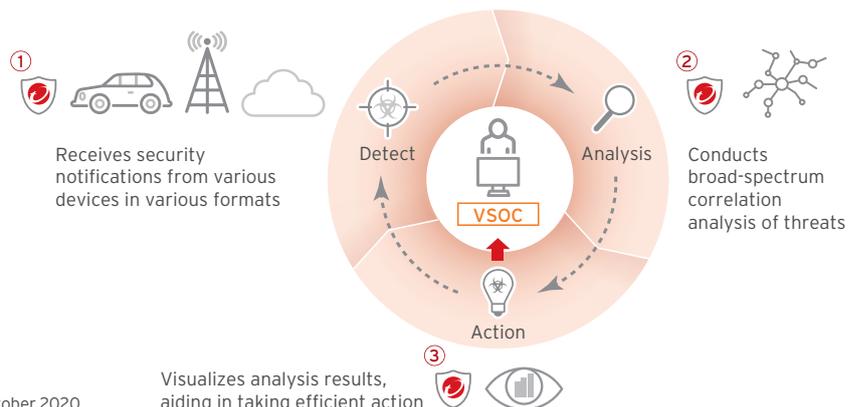
Backend

Trend Micro Cloud One™

Secure your data center, cloud, and containers without compromising performance or security.

Management (VSOC)

Trend Micro™ XDR

XDR supports* quick and effective action by correlating threats detected from the endpoint, network, and backend with individual notifications from each, enabling a bird's eye view of comprehensive elements. Layering in global threat intelligence, it provides clarity and assistance to threat investigators.

*XDR supports only limited Trend Micro products as of October 2020

① Receives security notifications from various devices in various formats

② Conducts broad-spectrum correlation analysis of threats

③ Visualizes analysis results, aiding in taking efficient action

Detect

Analysis

Action

VSOC

Your Connected Car Security Partner Advantages

9 of Top 10
FORTUNE
GLOBAL
500

Nine of the top ten
Fortune 500 companies
worldwide are
Trend Micro clients.

8 of Top 10
Automotive Companies

Eight of the top ten
companies in the automotive
industry have adopted
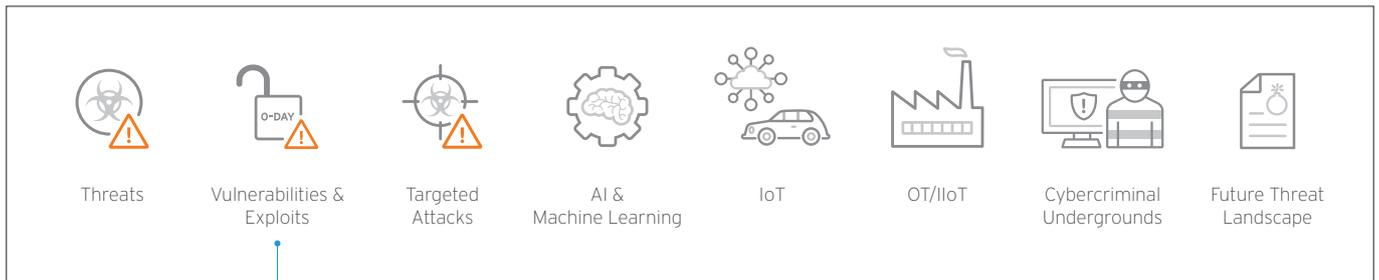Trend Micro solutions.

Partnership

Partnering with automotive
industry leaders to provide
cybersecurity expertise and
comprehensive solutions.

Threat intelligence supporting our solutions

Trend Micro Research, global research organization

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.
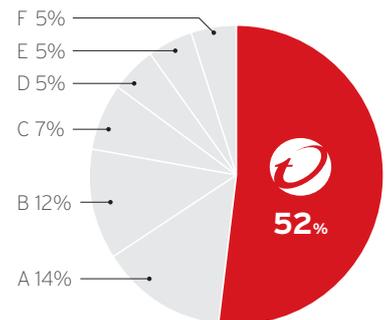
Threats	Vulnerabilities & Exploits	Targeted Attacks	AI & Machine Learning	IoT	OT/IIoT	Cybercriminal Undergrounds	Future Threat Landscape

ZERO DAY INITIATIVE (ZDI)

ZERO DAY INITIATIVE

Vulnerability report track record
The ZERO DAY INITIATIVE (ZDI), Trend Micro's bug bounty program, discovers thousands of zero-day vulnerabilities through its collaborative community of over 3,500 security researchers.
In 2018, ZDI reported over half of all disclosed vulnerabilities to public agencies and vendors.

Source: IHS Markit, 2018 Public Cybersecurity Vulnerability Market

F 5%
E 5%
D 5%
C 7%
B 12%
A 14%
52%

Insights to improve Trend Micro's core technology and products

▼ Go To WEB Site
https://www.go-tm.jp/auto/

TREND MICRO™
Securing Your Connected World