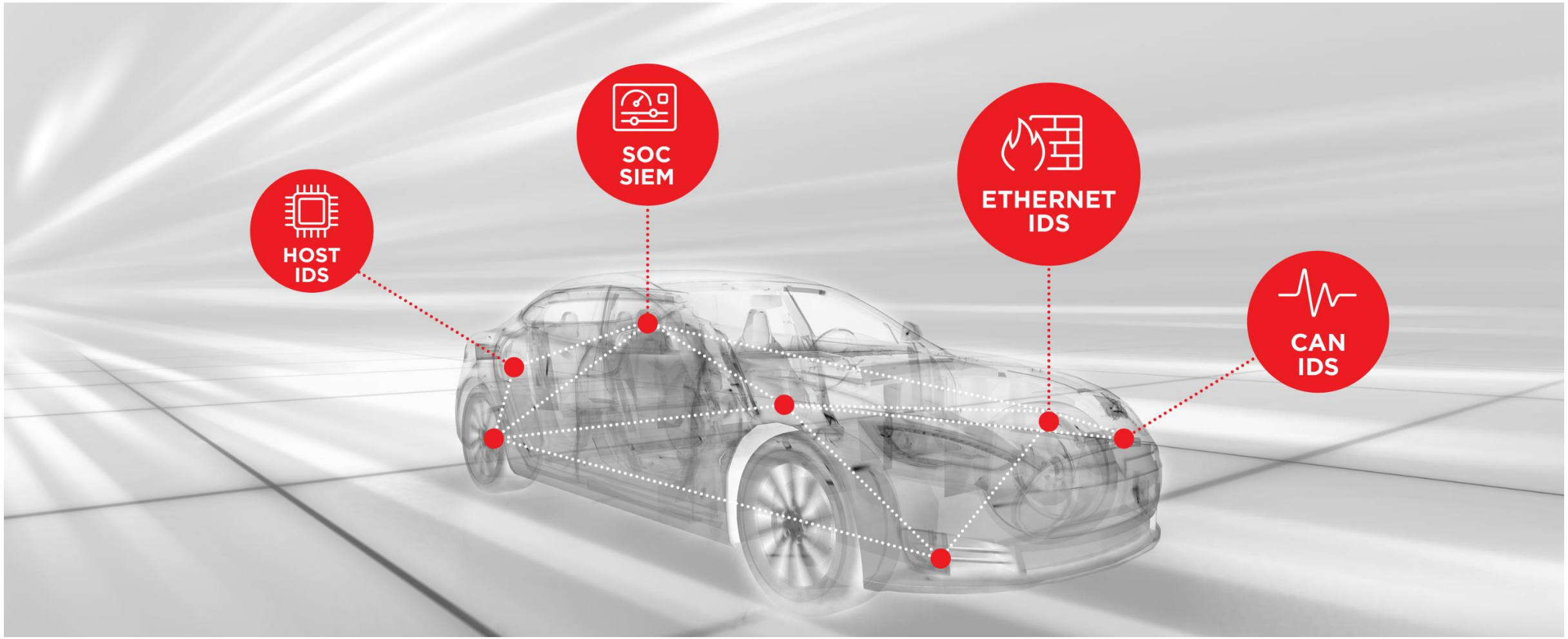


智慧护航：量产落地的盖瑞特入侵检测系统，确保智能网联汽车安全

打造领先于攻击的全面、高效、灵活的盖瑞特智能网联汽车入侵检测系统

Garrett
ADVANCING MOTION

我们的使命

盖瑞特提供尖端科技，让车辆更清洁、更高效、更互联。

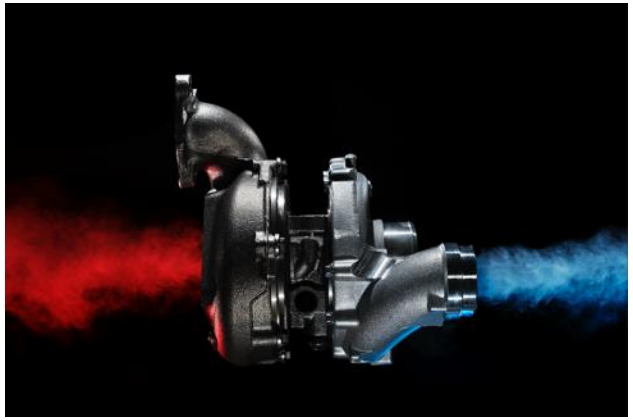
我们开发创新与差异化的解决方案，赋能全球交通产业，定义未来智行科技。

领先的技术解决方案提供商

Garrett
ADVANCING MOTION

涡轮增压技术

- 减少燃油消耗
- 减少废气排放
- 提高发动机性能



氢燃料及混动应用

- 优化燃油经济性
- 迈进零排放的未来
- 更好的驾驶响应

智能网联汽车软件

- 保护汽车免受网络攻击
- 精确诊断和预测性诊断
- 避免大规模停工或宕机

为行业提供差异化的技术，让汽车更安全，更节能，更环保

领先的技术解决方案提供商

量产验证的汽车专业技术能力

- 行业领先的入侵检测算法
- 多年来作为世界主流OEM的全球供应商
- 深度了解各种汽车开发流程与技术演进

可靠的网络技术基础

- 产品基于可靠的工业应用
- 25+年的航空航天及汽车工业的网络安全经验

坚定的生态系统承诺

- SAE、Auto-ISAC、CLEPA成员
- 与Tire-1/芯片供应商合作
- 专业的解决方案与产品供应商

盖瑞特网络安全解决方案

获奖产品

- 一流性能 | 产品屡获奖项
- 与各地客户保持密切关系
- 独一无二的端到端车辆网络安全问题分析能力

汽车网络安全的防护机制

如何选择和应用IDS入侵检测系统

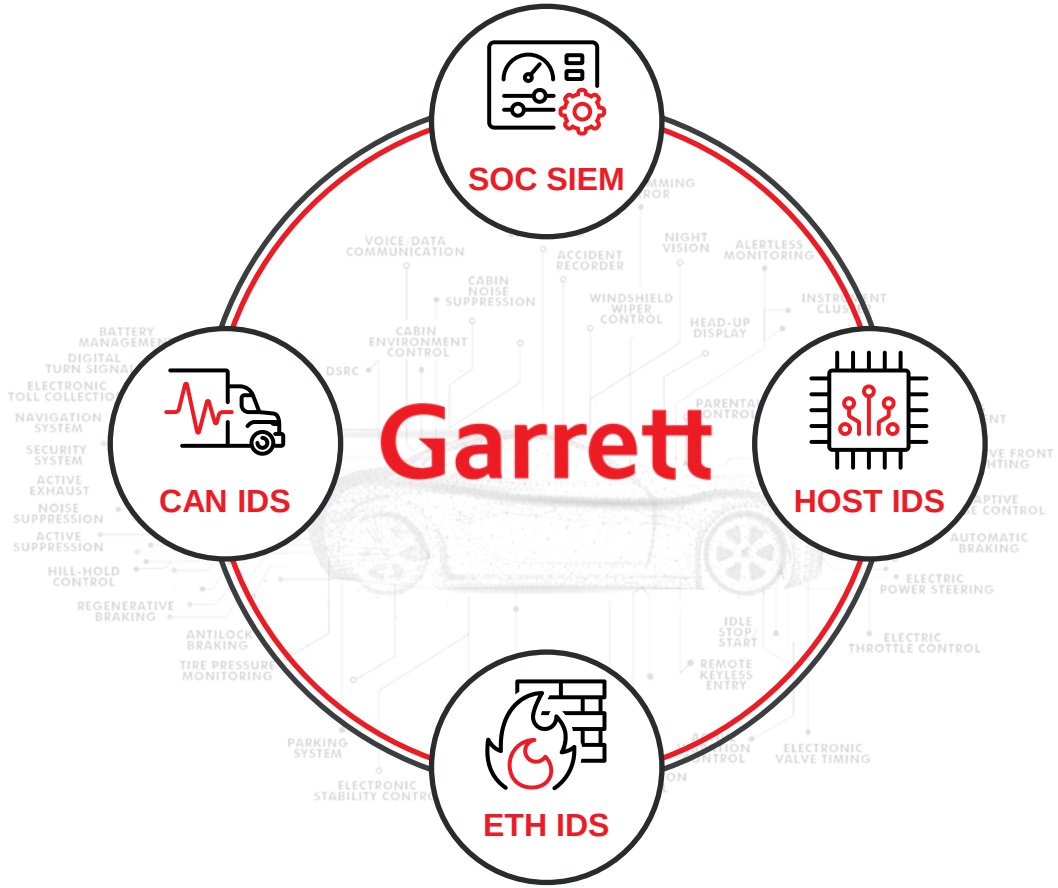
车辆需要哪种IDS入侵检测系统，需要配置在哪里?

如何使IDS入侵检测系统具有最佳性能、最佳检测精度和最小的误报?

IDS入侵检测系统是否能够覆盖全部或大部分针对车辆的网络攻击?

IDS入侵检测系统是否能够轻松地从一种车型或一种类型的控制器移植到另一种车型或控制器上?

盖瑞特入侵检测系统解决方案



- 全面（Entire）入侵检测系统解决方案
- 高效（Efficient）入侵检测系统解决方案
- 灵活（Extensible）入侵检测系统解决方案

盖瑞特入侵检测系统解决方案

- **全面（Entire）入侵检测系统解决方案**
- 高效（Efficient）入侵检测系统解决方案
- 灵活（Extensible）入侵检测系统解决方案

盖瑞特网络安全产品

Garrett
ADVANCING MOTION

1 盖瑞特车端IDS

网络攻击响应

攻击报告

检测通信和执行异常
入侵检测

实车或远程网络攻击

车载网络或主机入侵

行业领先的跨总线检测算法

独立于系统硬件和操作系统，灵活集成

配套的车辆全生命周期安全管理和相关配置工具

覆盖 CAN、CAN FD、车载以太网和高性能车载控制器

2 盖瑞特云端 SOC (安全运营中心)

OEM 深度攻击分析和处理
安全事件管理

监测入侵告警 读取、解析、关联

识别网络攻击，包括严重级别、优先级排序、事件升级

Rule based为主，深度包检测为辅

盖瑞特网络安全软件解决方案

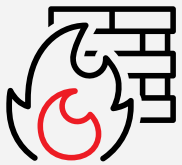
5大核心产品

CAN IDS

盖瑞特车载CAN网络IDS监测CAN流量，检测和/或阻止异常

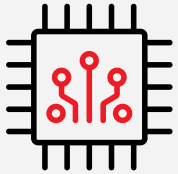
ETH IDS

盖瑞特以太网防火墙和IDS解决方案检查以太网流量并阻止车载恶意消息



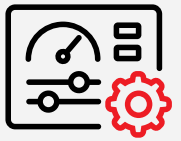
HOST IDS

盖瑞特主机IDS解决方案监控和检测汽车高性能计算机上的异常网络攻击



SOC SIEM

盖瑞特SOC SIEM 深度分析来自数百万辆汽车的网络警报



Ruleset Tool

盖瑞特图形化调参工具 降低算法参数开发维护人力

盖瑞特网络安全解决方案为网联汽车提供一流保护

盖瑞特CAN网络入侵检测系统

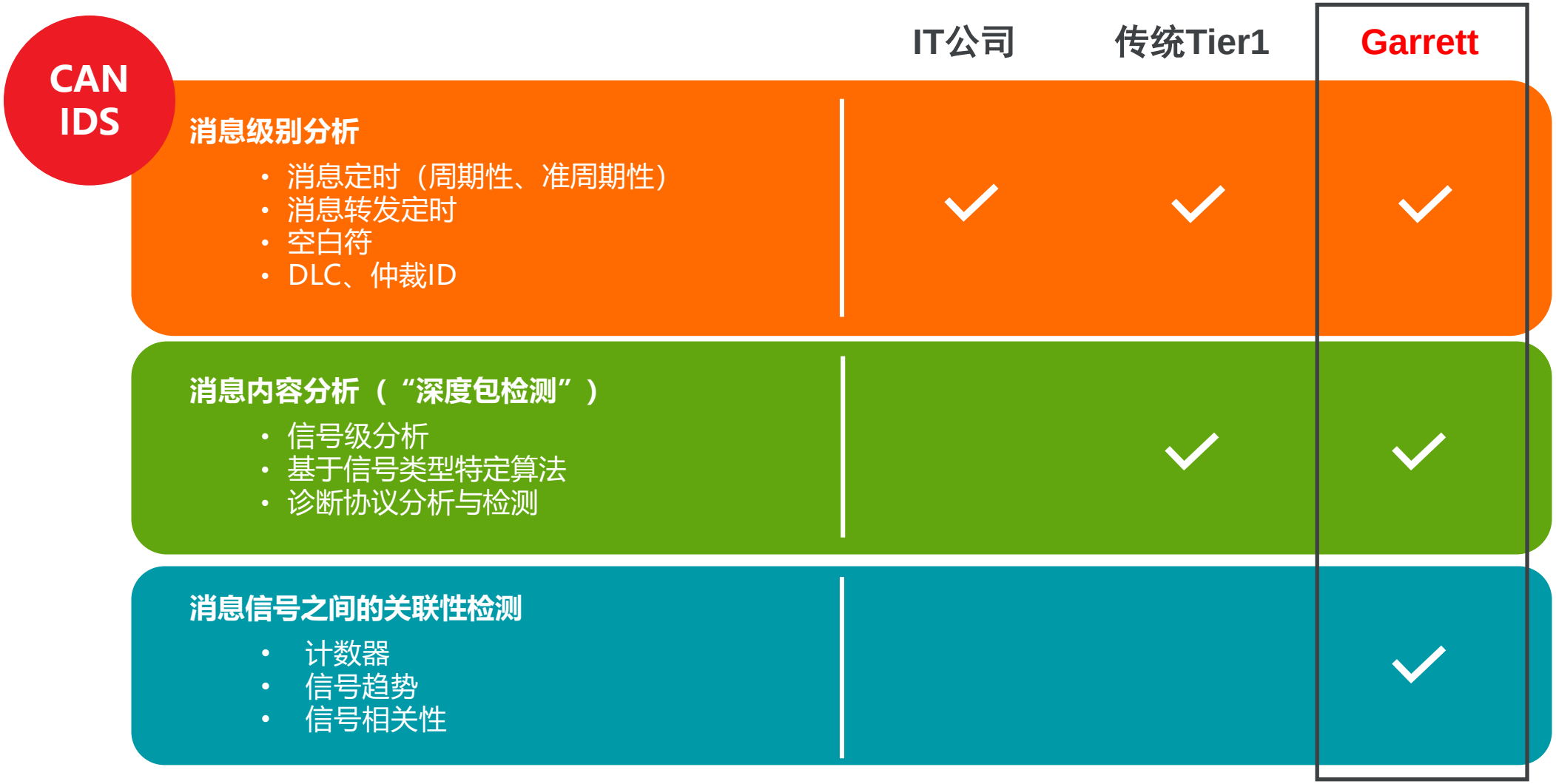
CAN IDS

盖瑞特车载CAN网络入侵检测系统能够监测流量，检测网络异常，从而及时发现和处理对车辆CAN网络的攻击。

主要功能	技术规格亮点	主要优点
• Rules based 检测 • 行业领先的异常检测算法 • 规则创建自动化 • 分布式入侵检测系统 • 生命周期入侵检测系统管理 • 模块化警报管理	• 极优的处理性能和延迟 • 灵活的警报日志设计 • 兼容领先的芯片组方案	• 一流的检测速率和误报水平 • 适应传统ECU的占用空间和模块化，便于改造 • 控制了生命周期的工程成本 • 与SOC工具配套，实现快速根本原因分析和补救

盖瑞特CAN网络入侵检测系统

Garrett
ADVANCING MOTION



50+的行业算法实现最大覆盖

盖瑞特以太网入侵检测系统

ETH IDS

盖瑞特车载以太网防火墙和入侵检测系统解决方案检查以太网消息，发现并处理针对以太网的网络攻击。

主要功能	技术规格亮点	主要优点
• Rules based检测 • 以太网多协议层检测 • 提供攻击预防功能 • 模块化警报管理 • 分布式入侵检测系统 • 生命周期入侵检测系统管理工具	• 极优的处理性能和延迟 • 灵活的警报日志设计 • 兼容领先的芯片组方案	• 异常行为检测与特定攻击标签检测方法相结合 • 一流的检测速率和误报水平 • 模块化灵活适配，升级 • 与SOC工具配套，实现快速攻击识别预处理

盖瑞特主机入侵检测系统

HOST IDS

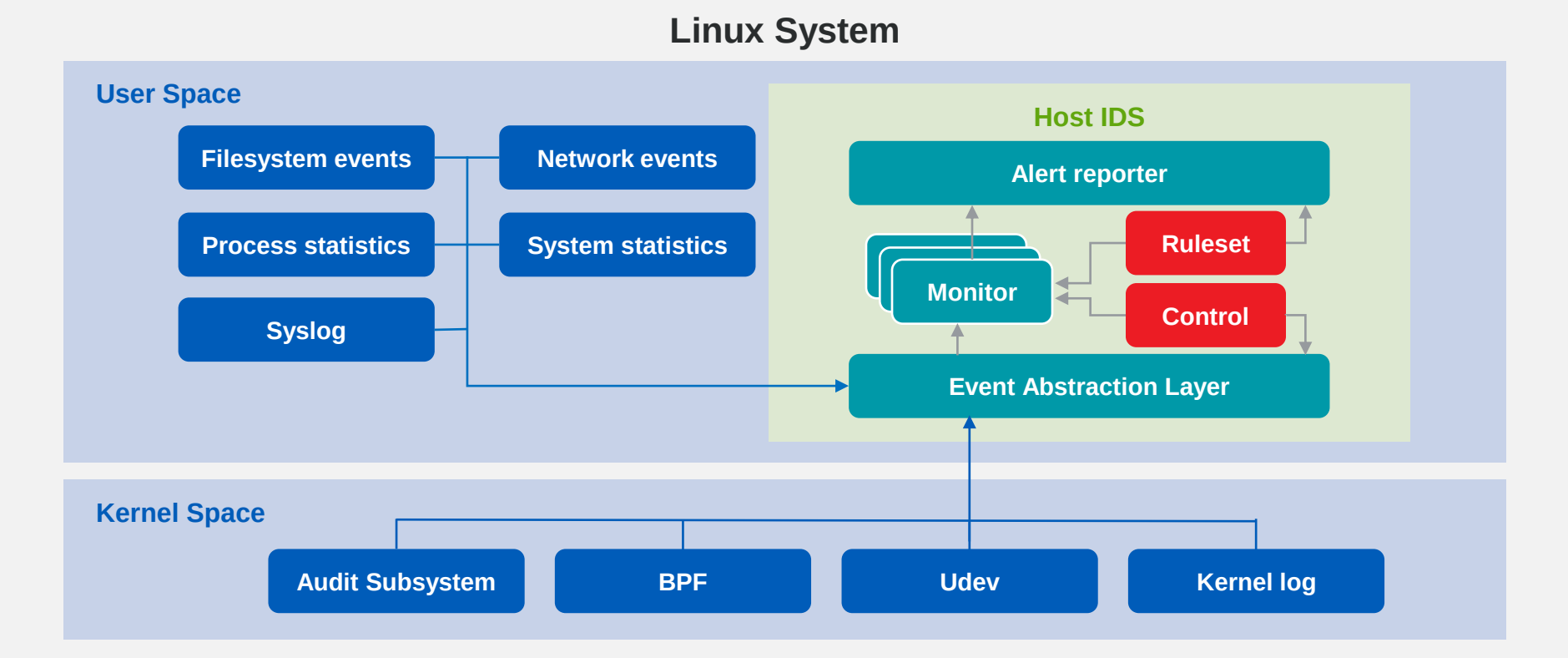
盖瑞特车载主机入侵检测系统监控和检测对汽车内高性能计算机的网络攻击

主要功能	技术规格亮点	主要优点
• 主机应用异常检测 • 主机对外对内通信异常检测 • 主机复杂操作系统异常检测 • 主机基础防御异常检测	• 本解决方案基于Linux，但可轻松移植到其他POSIX系统 • 与盖瑞特网络IDS产品共同检测针对整车系统的复杂攻击 • 在检测事件源方面高度可配置	• 轻量级的主机检测软件部署 • 一流的检测速率和误报水平 • 与SOC工具配套，实现快速攻击识别预处理

盖瑞特主机入侵检测系统

HOST IDS

- 兼容盖瑞特的网络IDS
- 文件系统监控，进程监控，系统关键接口监控，
  性能监控，外设接口监控，用户权限监控，以及网络接入点监控



盖瑞特SOC — 安全运营管理中心

SOC
SIEM

非车载软件，用于接收车队上报的网络攻击告警并分析，识别处理网络攻击

主要功能	技术规格亮点	主要优点
• 数据获取、解析、关联 • 模块化严重程度、优先级、升级规则 • 灵活处理多种车载入侵检测系统或非入侵检测系统上报信息 • 可综合盖瑞特健康管理系统	• 操作系统：Ubuntu、CentOS等 • 数据流：Kafka等 • 搜索引擎：Elastic • 容器化—Docker Swarm，以便于携带和扩展	• 以最低成本管理全球大型车队网络安全 • 未知问题、攻击故障排除 • 轻松集成和部署 • 鉴别攻击与缺陷

盖瑞特SOC — 安全运营管理中心

SOC
SIEM

- 车端警报自动化归类分析
- 全过程工单邮件系统，所有操作记录存档，责任人明确，极简化运维人力负担
- 采用容器部署，云端架构承受千万级车辆运维，且支持实时扩容，增强云端接收分析能力

盖瑞特SOC
界面预览

强大的客户化
定制能力

全闭环解决方案

大数据分析能力

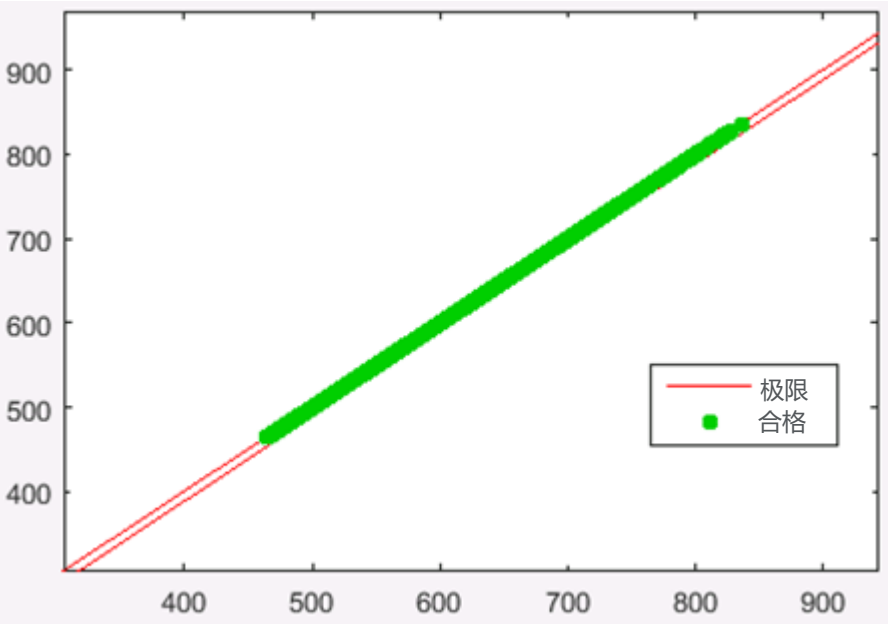
盖瑞特入侵检测系统解决方案

- 全面（Entire）入侵检测系统解决方案
- **高效（Efficient）入侵检测系统解决方案**
- 灵活（Extensible）入侵检测系统解决方案

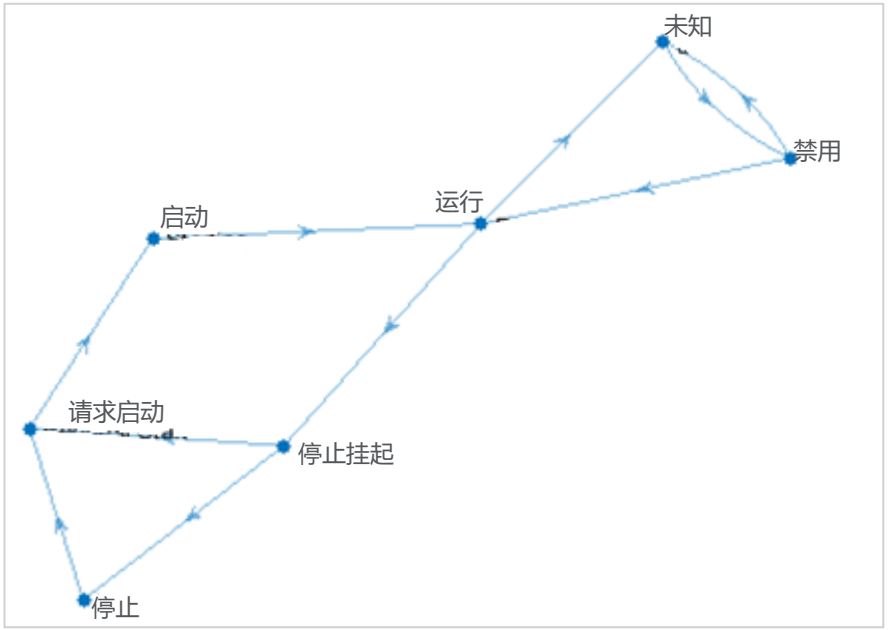
盖瑞特解决方案价值总结

		亮点和客户价值
IDS	方法和算法	• Rules based检测异常和签名，使用DBC和实车数据 • 多种行业先进的算法，包括通用算法和定制算法，确保覆盖大量异常行为
	工具链	• 规则校准和验证工具： 1）维护时，对盖瑞特的依赖度低 2）本地团队提供高效支持
	精度	• 检测率：>98% • 误报率：<1% • SOC效率更高 = 人力成本较低
	性能	• 占用空间小 • 延迟低
SOC		• 从日志获取到取证分析的完整功能 • 高级取证功能，含健康管理 • 轻松集成到OEM环境并优化部署成本

盖瑞特入侵检测系统高效关联规则构建示例



- 信号可以来自同一条消息，也可以来自不同的消息
- 如果信号超过关联极限，则发出警报
- 可推广到超过两个非线性关系的离散和/或连续信号
- 自动寻找相关性信号匹配对，无需人工介入



- 监控包含状态信息的信号值
- 检查当前值是否与前值不同（FSM中的状态转换）
- 状态发生变化时，触发“有效的值转换”检查

盖瑞特入侵检测系统解决方案

- 全面（Entire）入侵检测系统解决方案
- 高效（Efficient）入侵检测系统解决方案
- **灵活（Extensible）入侵检测系统解决方案**

挑战 -回顾

如何选择和应用IDS入侵检测系统

车辆需要哪种IDS入侵检测系统，需要配置在哪里?

如何使IDS入侵检测系统具有最佳性能、最佳检测精度和最小的误报?

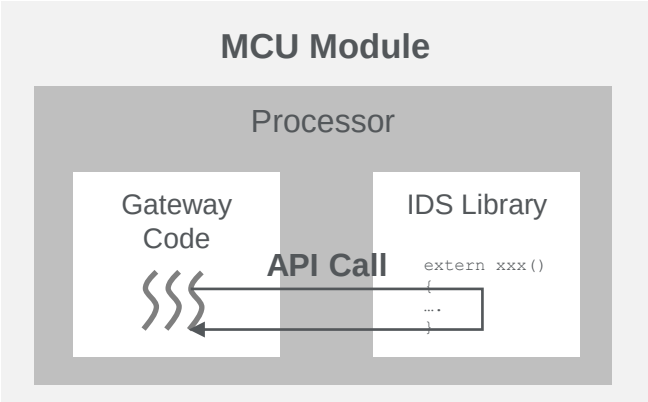
IDS入侵检测系统是否能够覆盖全部或大部分针对车辆的网络攻击?

IDS入侵检测系统是否能够轻松地从一种车型或一种类型的控制器移植到另一种车型或控制器上?

盖瑞特入侵检测系统低耦合，易集成

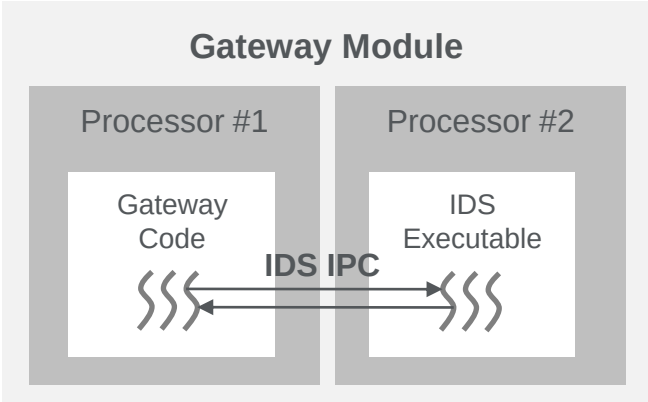
静态库集成

- 跨平台直接生成对应的静态链接库
- 最简化API接口
  - 初始化接口
  - 报文评估接口
  - 评估结果接口



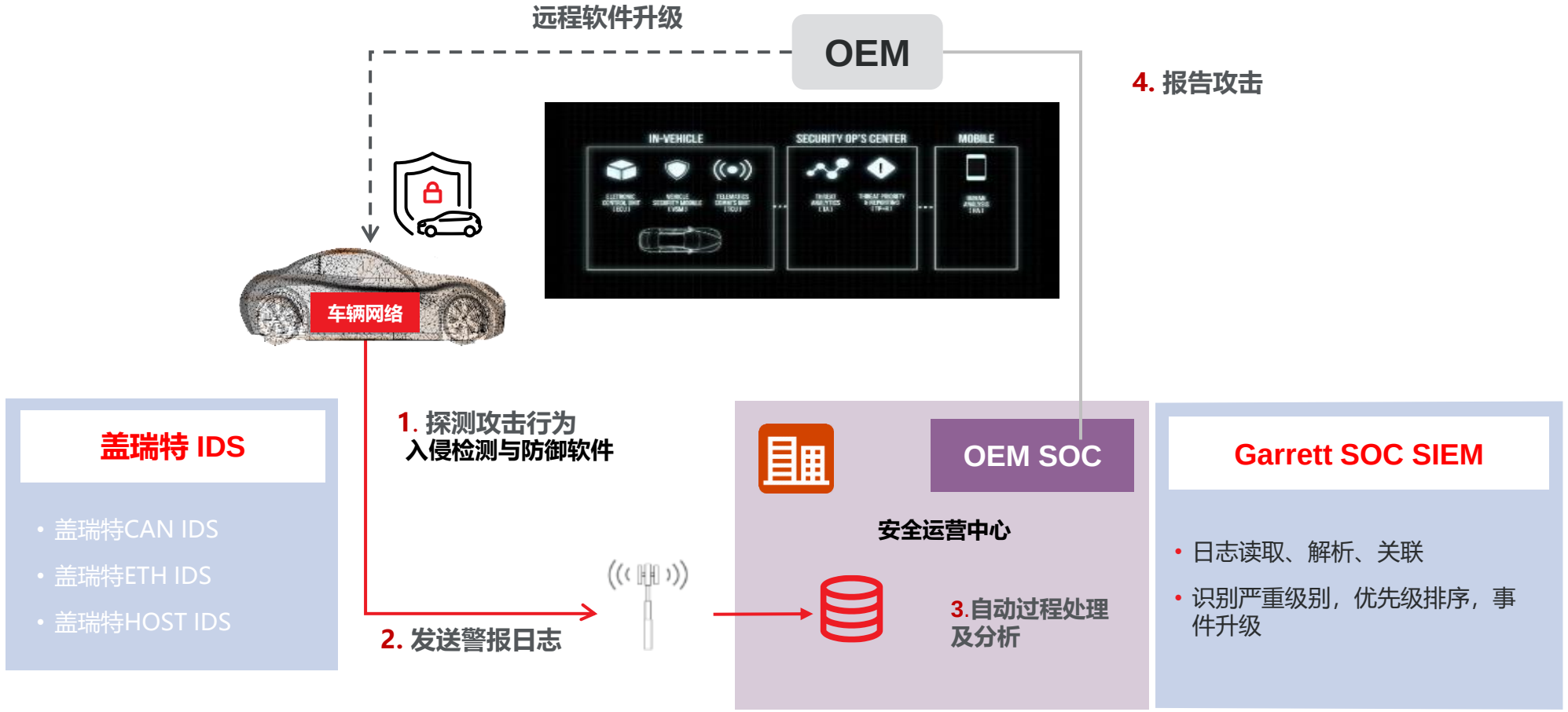
应用程序

- 应用程序形式运行IDS(Unix平台)
- IPC通讯方式交互信息
  - 报文通过消息队列或者共享内存形式交互
  - 警报通过ring buffer推送给云端



盖瑞特入侵检测系统
使用实例

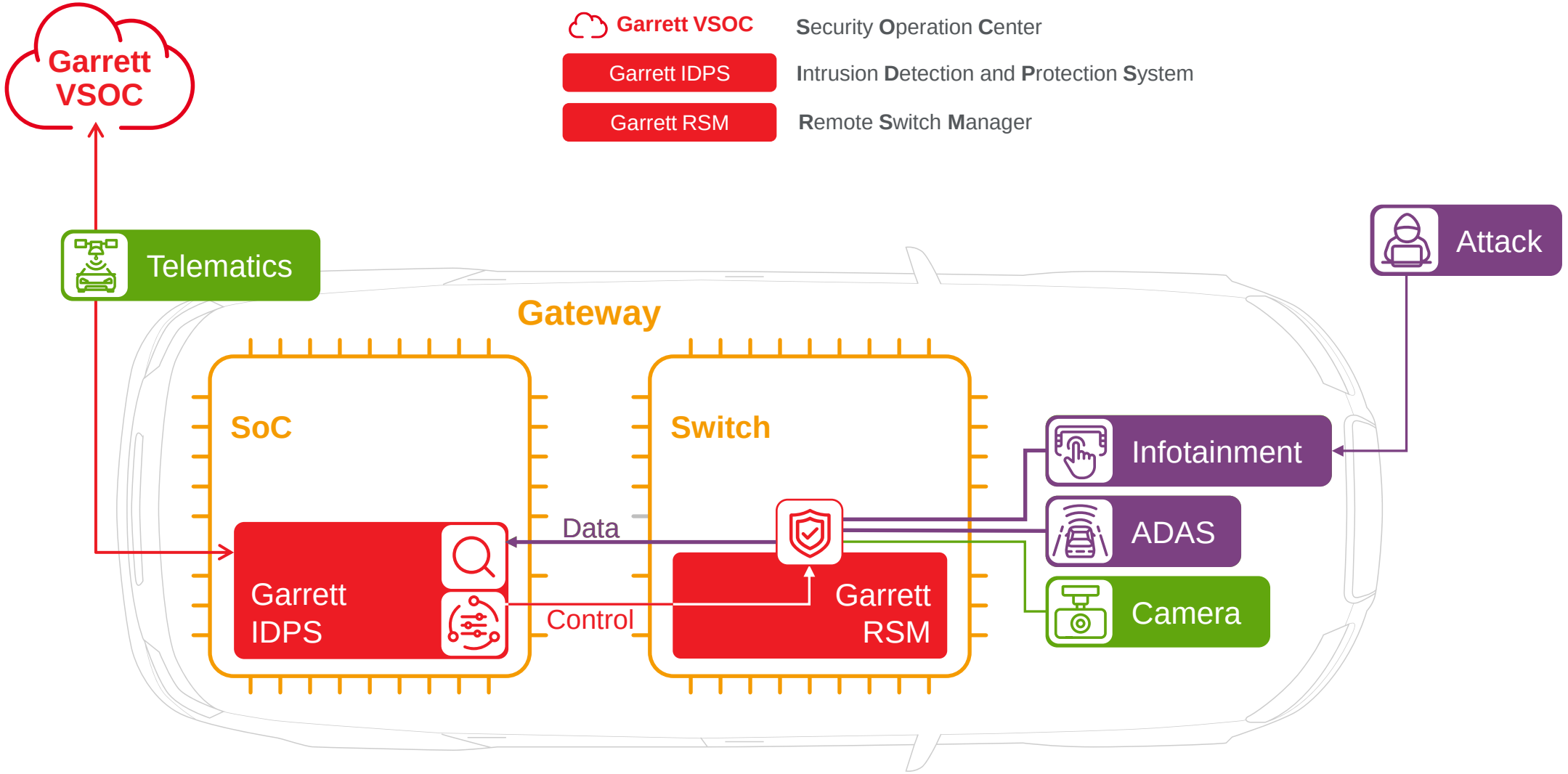
盖瑞特网络安全整体方案



盖瑞特为OEM提供从车端到云端的全面入侵检测系统解决方案

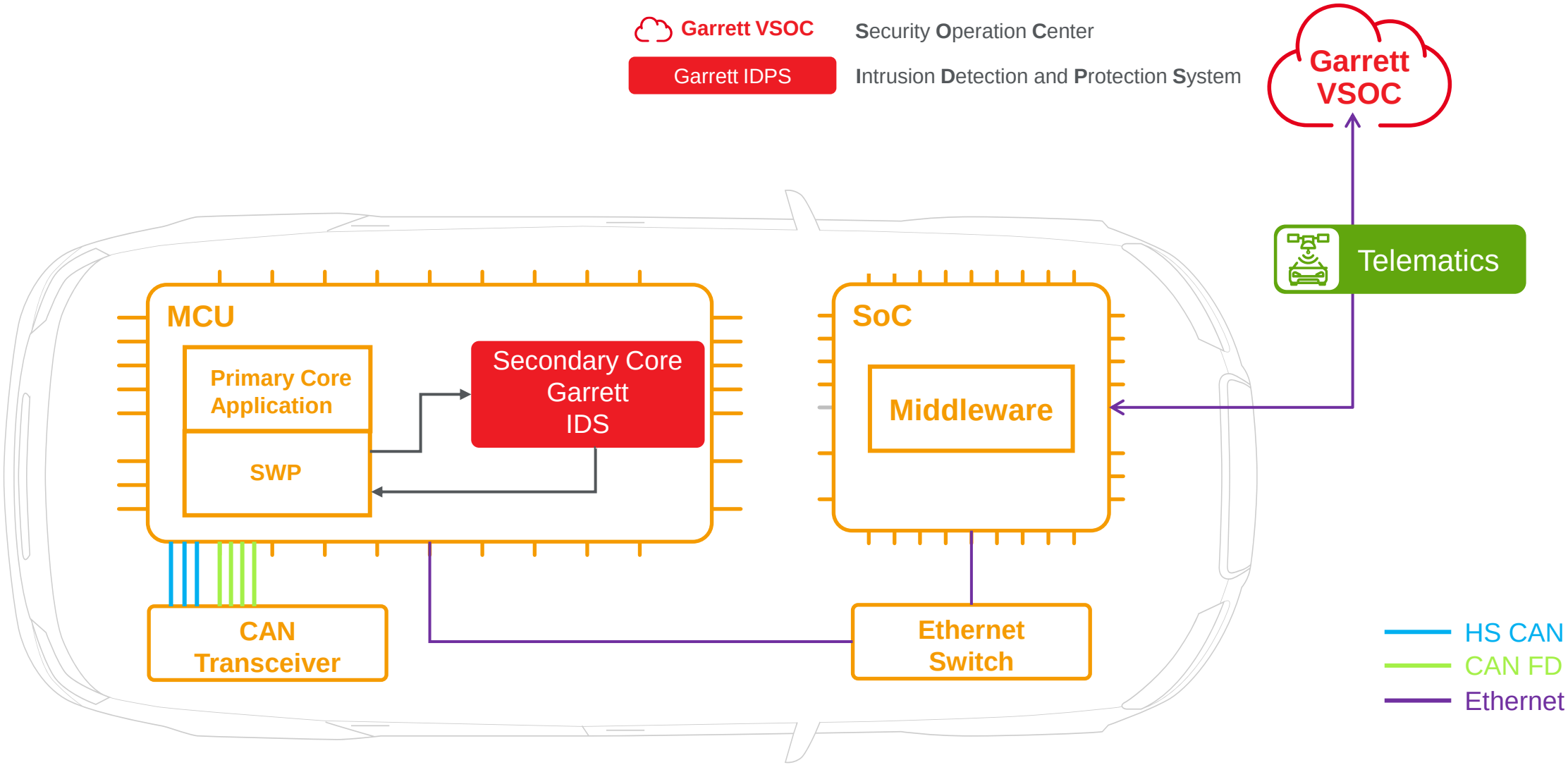
Gateway(网关)的IDPS实施方案

Garrett
ADVANCING MOTION



盖瑞特面向网关控制器的入侵检测系统解决方案

MCU(微控制器)的IDS实施方案



盖瑞特面向MCU控制器的入侵检测系统解决方案

流程合规：协助客户获得VTA证书

Garrett Cyber Security Solutions	CAN IDS	ETHERNET IDS	HOST IDS	SOC SIEM
Communications Channels Threats	✓	✓		
Unintended human actions facilitating a cyber attack	✓	✓	✓	
External connectivity and connections Threats	✓	✓		
Vehicle Data and Code			✓	
Protection and Hardness	✓	✓	✓	
Monitor, detect, respond to cyber threats	✓	✓	✓	✓
Management System for Monitored Vehicle				✓

盖瑞特协助OEM通过VTA，作为安全措施证明

盖瑞特网络安全解决方案优点及量产项目经验

Garrett
ADVANCING MOTION

盖瑞特拥有完整的产品线 （CIDS+EIDS+HIDS+SOC）

- 源于20多年的航空航天，汽车及其他工业行业的安全经验，盖瑞特提供完整，独特以及成熟车端IDS和云端SOC的解决方案
- 车端IDS累积了行业领先的50多种网络攻击的监测算法，能够全面涵盖车联网场景攻击监测
- 车端IDS独立于系统硬件及软件，易于系统集成和系统扩展
- 云端SOC 能够做到车辆网络安全异常信息读取，解析，整合，关联，做到车辆安全全方位态势感知
- 云端SOC结合汽车信息安全漏洞库，并辅以机器学习分析算法不断提高自动化分析，识别，处理网络攻击的能力

盖瑞特丰富的国内外量产经验为客户提供可靠的项目落地及实施

- 与全球客户在网络安全预研及量产项目上保持密切合作
- 与国内主机厂网络安全量产一期项目已经于2022年11月上市，其他项目将于2023年分批上市
- 与海外主机厂主力车型网络安全量产项目已于2021年底及2022年依次上市，且支持相关主机厂获得欧盟VTA车型认证
- 主机厂SOC云端持续自动化管理车端警报，每月管理数据量超千万条，密切监控车端异常行为(控制器元器件失效，车端攻击行为等)

盖瑞特完整产品线以及丰富的项目经验

感谢聆听!

Jianfeng.zhang@garrettmotion.com

欢迎关注盖瑞特

Garrett

ADVANCING MOTION

www.garrettmotion.com.cn | 盖瑞特