新形式下移动安全治理之道

魏超　*爱加密*

目录

车联网生态发展

物联金融

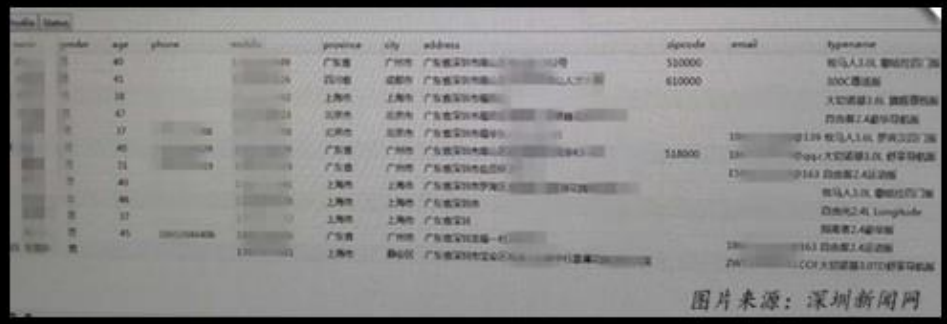
智能出行

智慧交通

◆ 车联网安全事件频发

特斯拉系统遭到破解
比亚迪云服务遭到破解
克莱斯勒Jeep被破解

◆ 车主信息泄露金融欺诈



国家政策要求

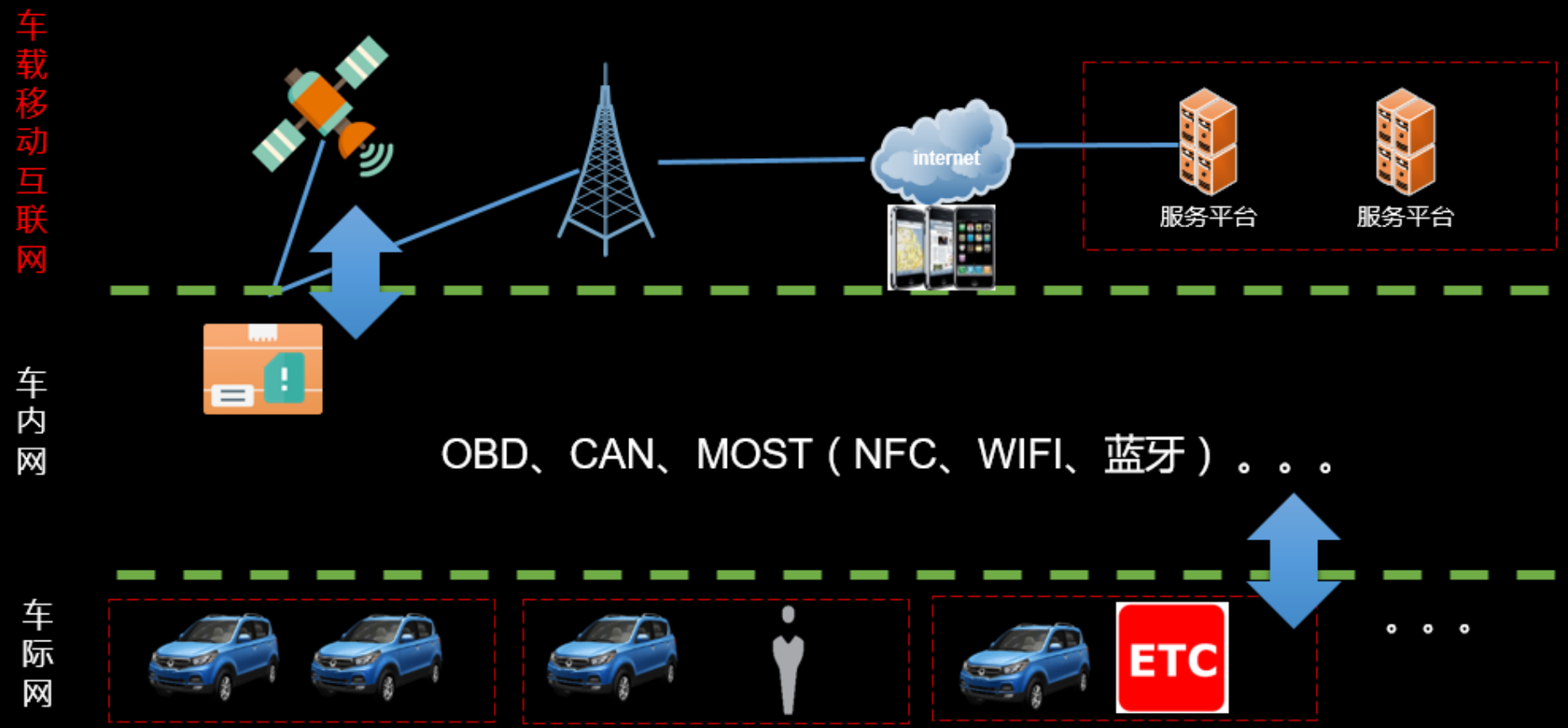
国家高度重视车联网产业安全发展，政府也推出一系列的政策、措施，推动车联网安全发展。

中华人民共和国网络安全法

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

- 网络运行安全
- 网络信息安全
- 监测预警
  应急处置

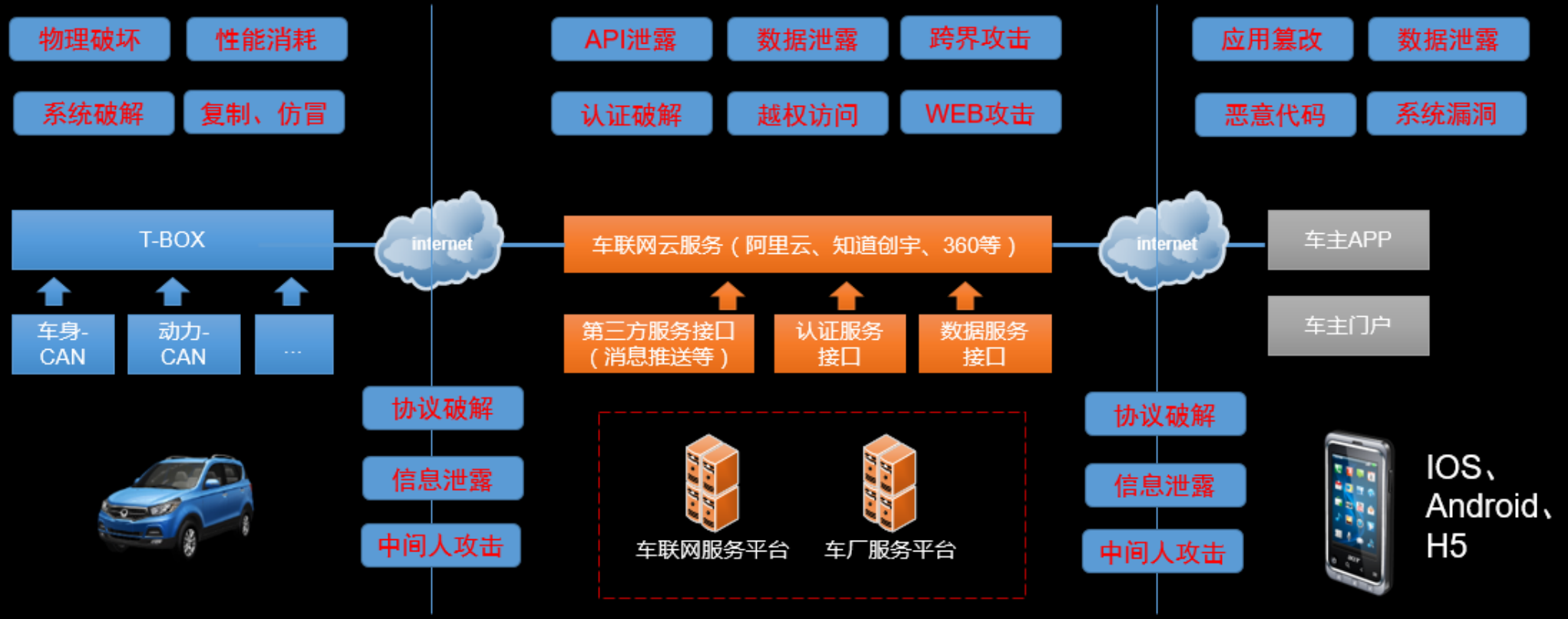
车联网应用网络架构



车联网核心，以智能网联汽车、移动智能终端、信息服务云平台为主

车联网移动网络安全风险

基于“云”、“管”、“端”架构，车联网核心对象及安全威胁。



车联网移动网络安全风险趋势

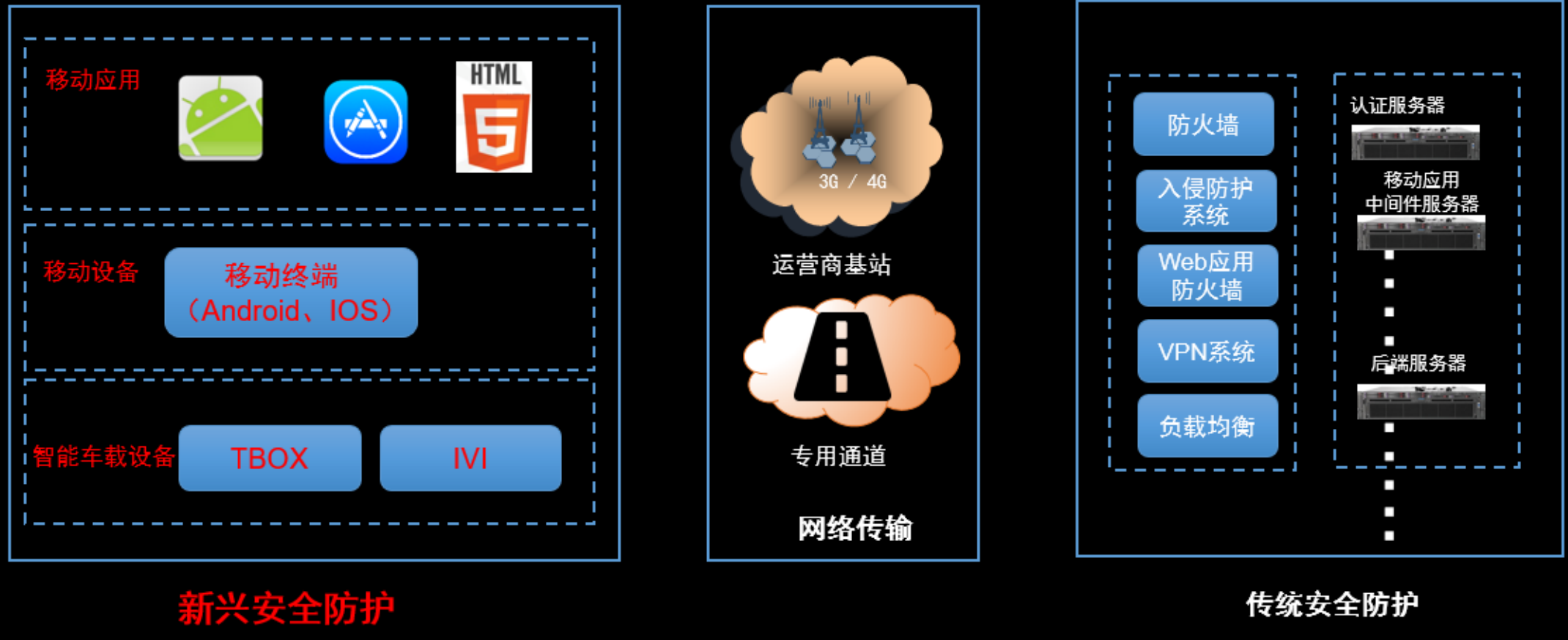
移动互联网技术更迭形成风险常态化

云技术大数据集中带来系统性复杂风险

智能设备联网跨界带来风险传导无边界

目录

车联网移动网络安全需求分析



车联网移动网络安全需求分析

企业必须在**业务安全，企业安全，安全能力**这三块共同投入建设，才能实现车联网的体系化安全。

1.业务安全包括汽车APP、终端系统、接口、数据、服务器、网络、云管理平台等.

2.企业安全是企业必须建立完善的安全管理体系，规范系统操作、数据接触、操作权限、应急处置等

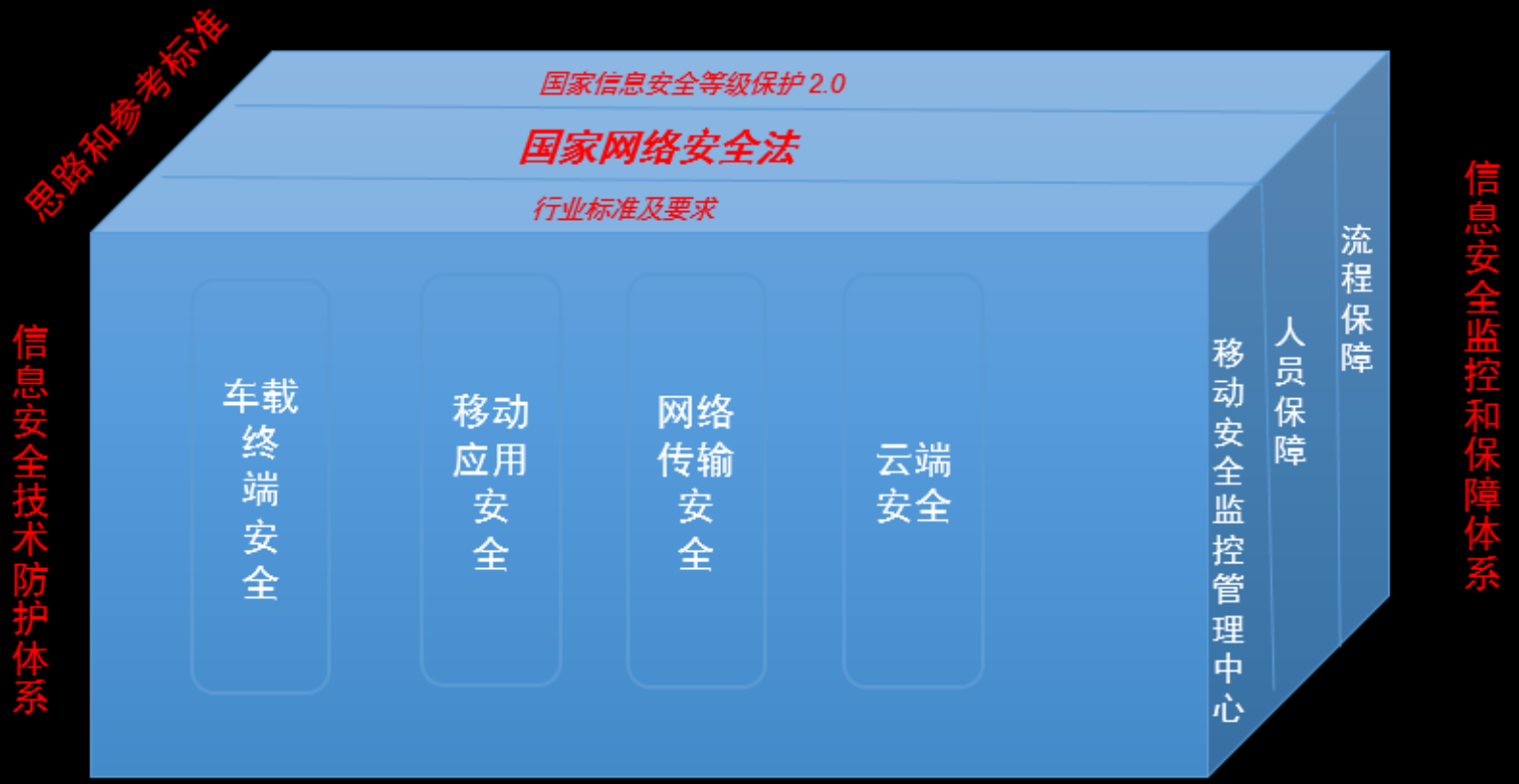
3.安全能力则是提高技术人员的专业安全能力，提高普通员工的安全意识，拉升企业的整体安全能力。

车联网移动网络安全建设目标

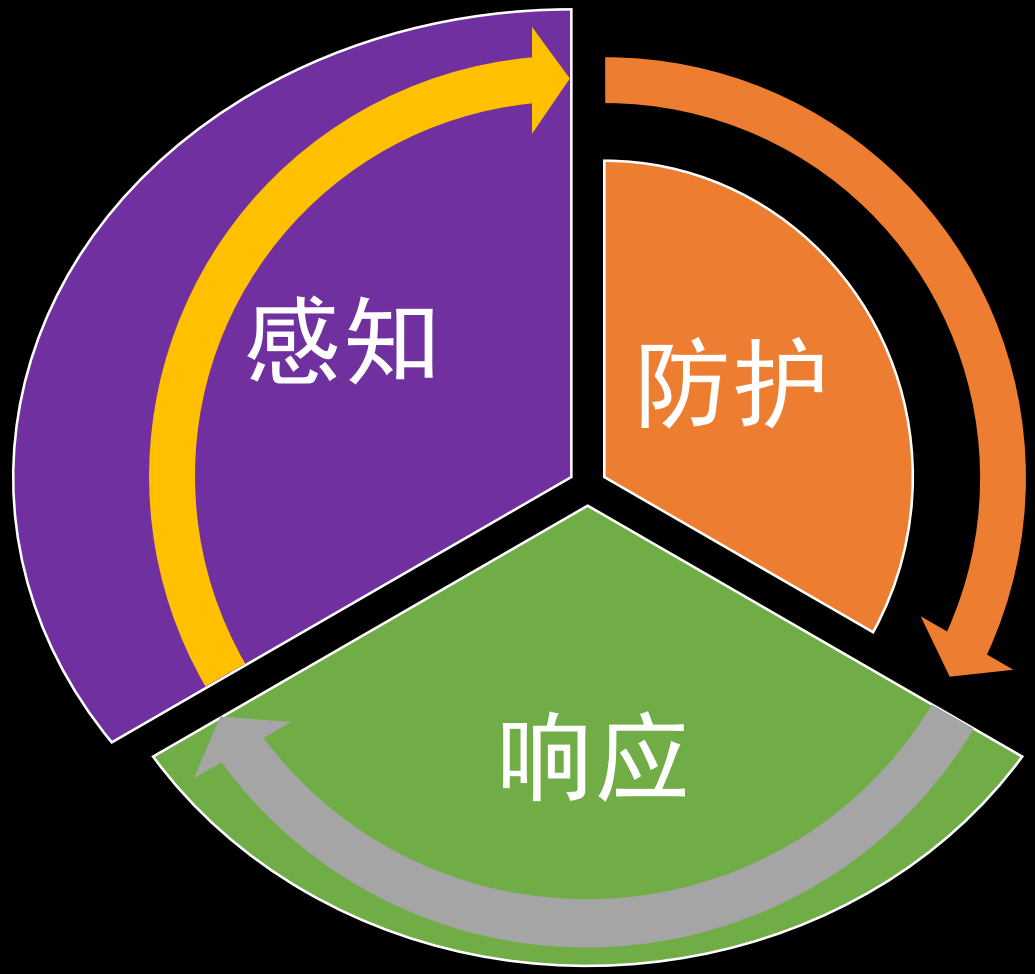
构建车联网移动全链条综合立体防御体系形成完整防御链

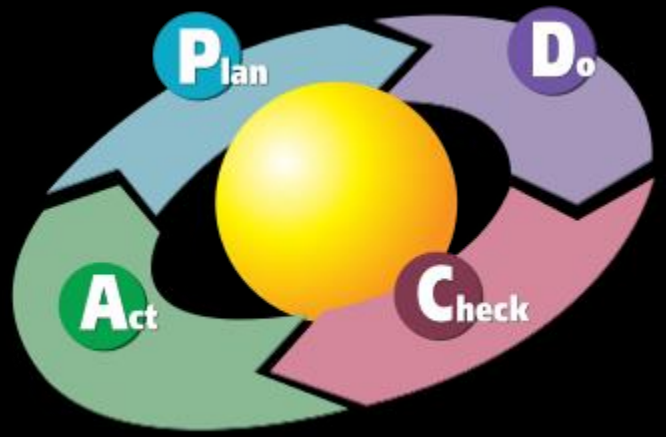
提高整车厂商和服务提供商的安全管理水平和安全防护能力

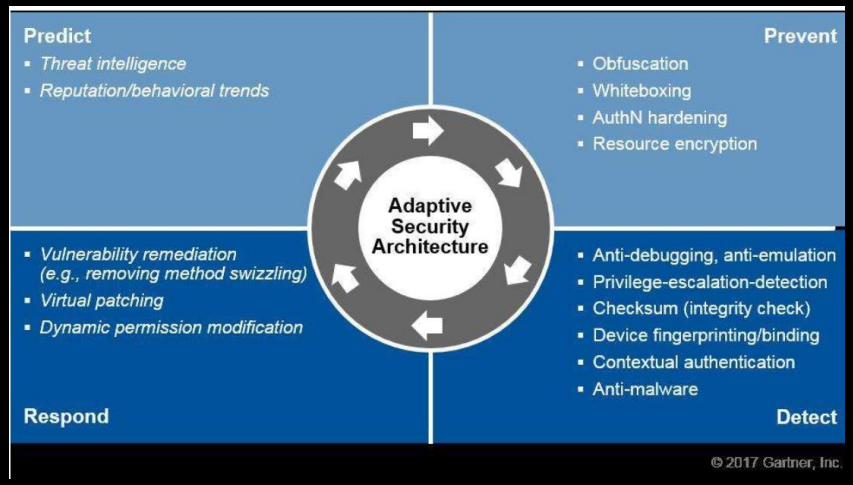
车联网移动网络核心安全体系设计原则



车联网移动网络安全特征

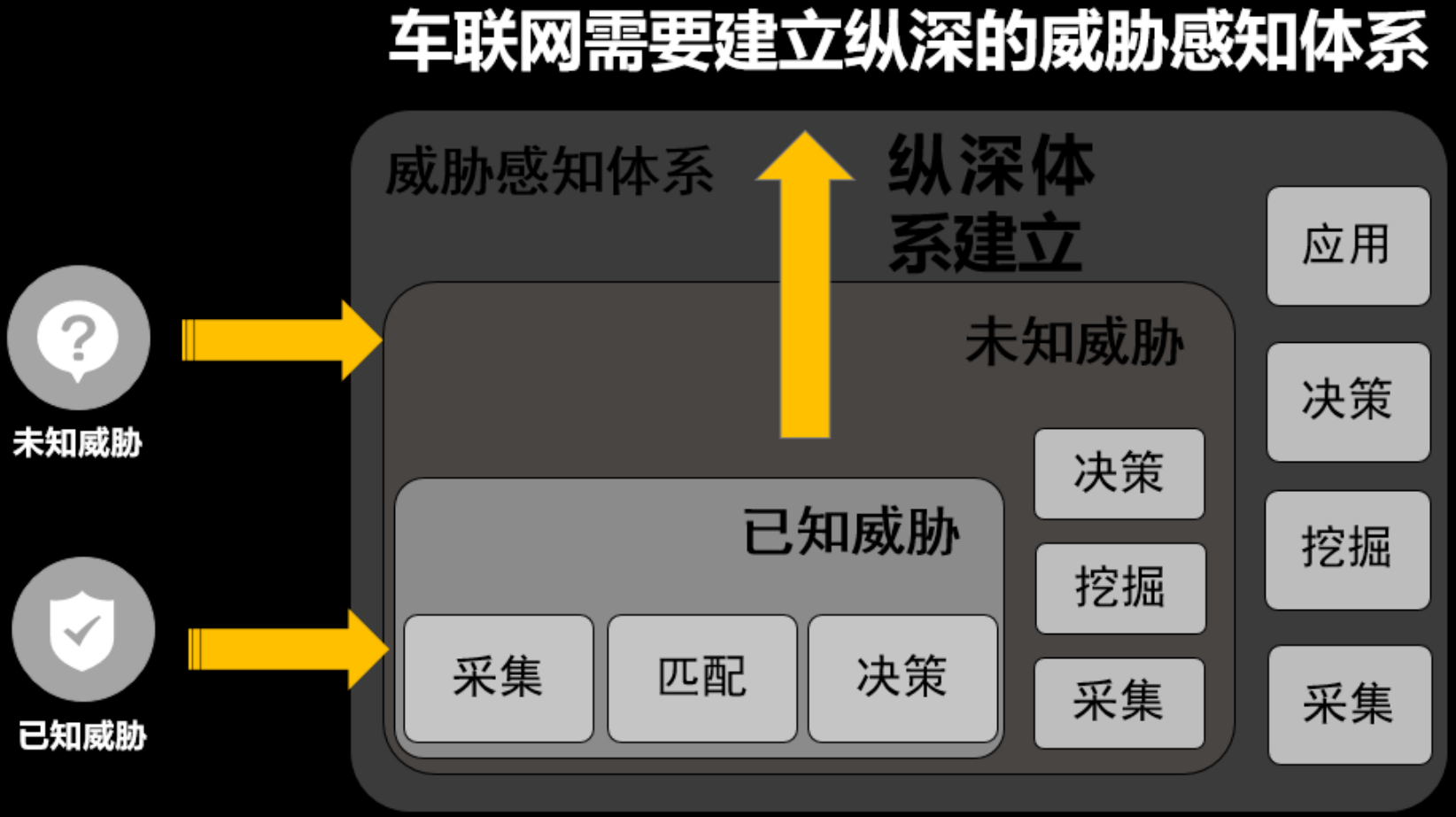






架构技术核心-全端感知采集

架构技术核心-纵深威胁感知体系

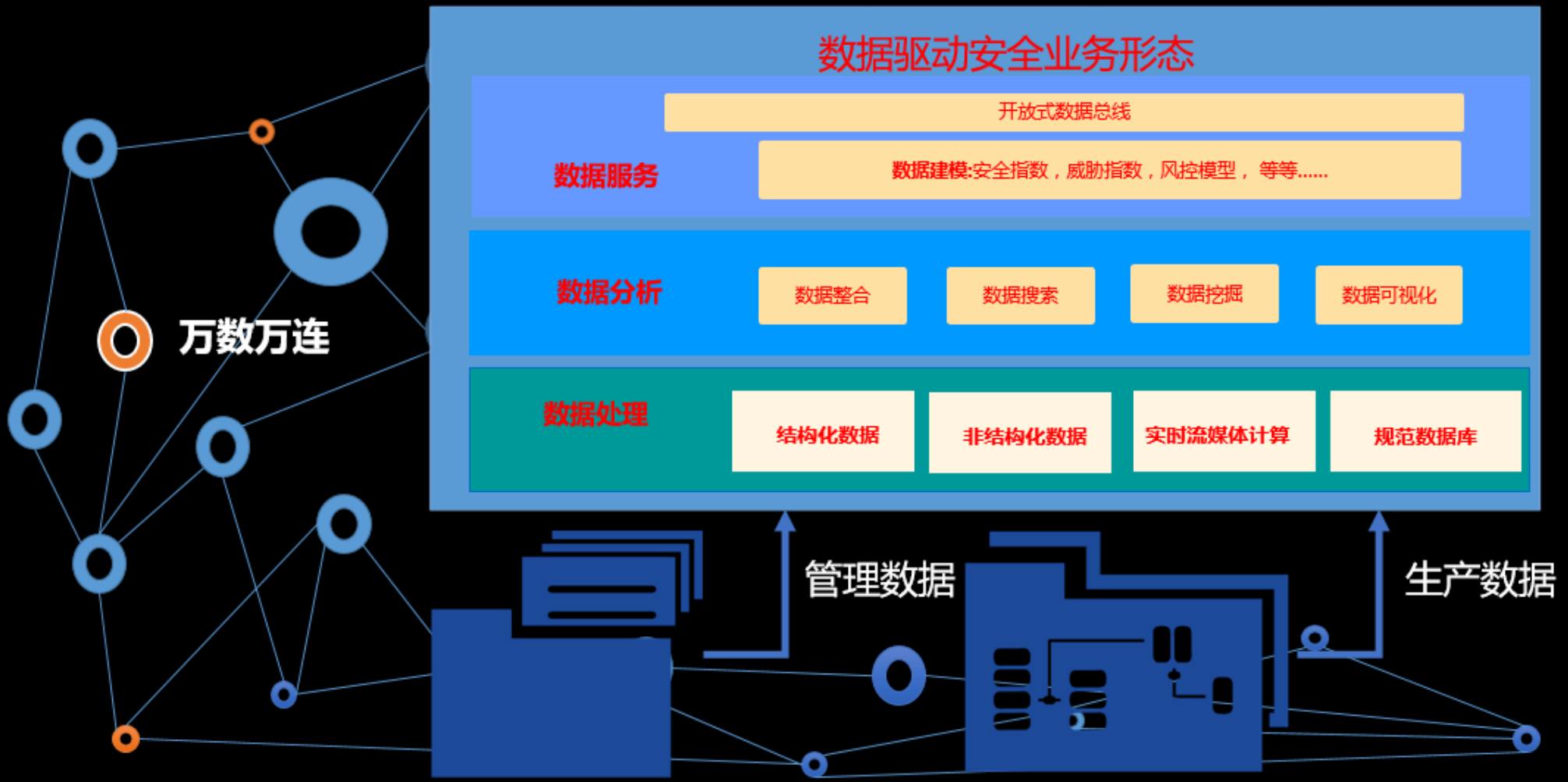


第一步：面对已知威胁，通过现有威胁模型与成熟防御工具精确匹配，快速决策。

第二步：面对未知威胁，针对不可预测的未知威胁场景，感知体系通过无监督聚类算法，将海量数据元分类，挖掘出数据之间的关联性，通过人工干预标签化并训练入库，从而预测出可能出现的未知威胁，随着企业数据的不断积累与业务的壮大，威胁感知体系自身会随着企业业务体系的壮大一起成长，不断探索出更多未知威胁服务于企业本身。

第三步：构建完整的数据应用生态体系，打通从数据采集，挖掘，到数据决策，数据应用的所有环节，为车联网安全精准赋能。

架构技术核心-大数据驱动业务



综合移动安全运营平台

1000+市场渠道
50万行业客户
8亿终端用户
智能网联车
和APP的感知

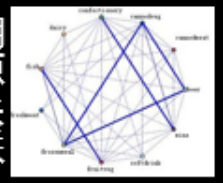
感知系统

300种感知引擎

量化展示层

统计度量

溯源关联



基线探寻

态势预测

数据分析层

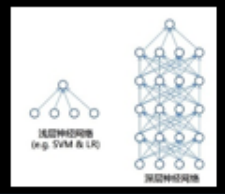
数据挖掘

- SVM
- FP-Tree
- Naive Bayes
- EM等

区块链

机器学习

神经网络



业务实现层

- 资产评估
- 威胁评估
- 脆弱性评估

- 源代码检测
- 应用检测
- TSP检测

- 整车检测
- 网络检测
- 终端检测

- 应用加固
- 服务器加固
- 设备加固
- 网络加固

- 应用实时保护
- 应用动态防护

评估 检测 加固 防御

合规管理层

资产管理 | 人员管理 | 权限管理 | 流程管理 | 应急管理 | 遵从管理

ITIL、

功能API接口
数据API接口

车联网展示门户

第三方风险数据

业务层防护

爱加密汽车安全运营平台（MSOC）

目录

安全运营中心展示

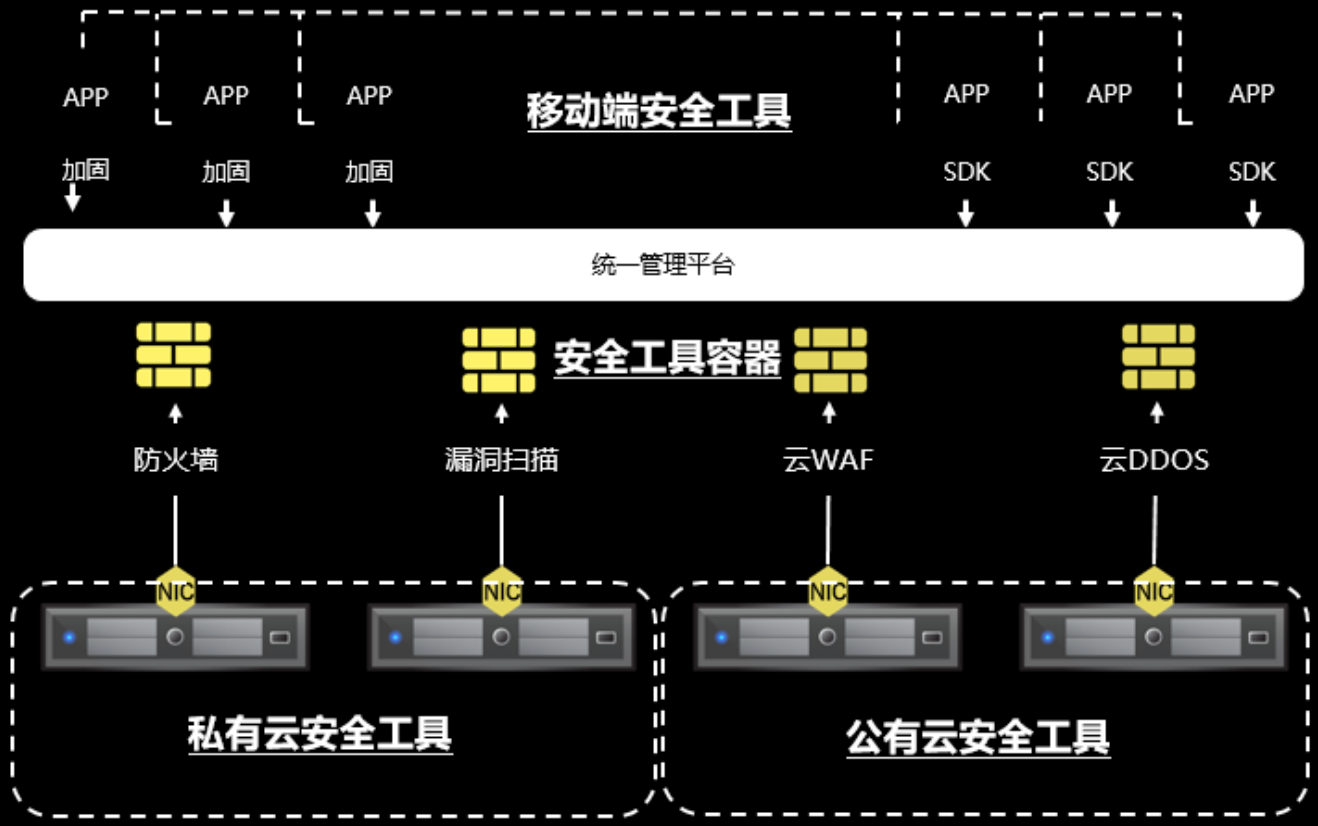
零日威胁播报

工具集中配置

业务安全态势

漏洞自处理

安全运营中心架构

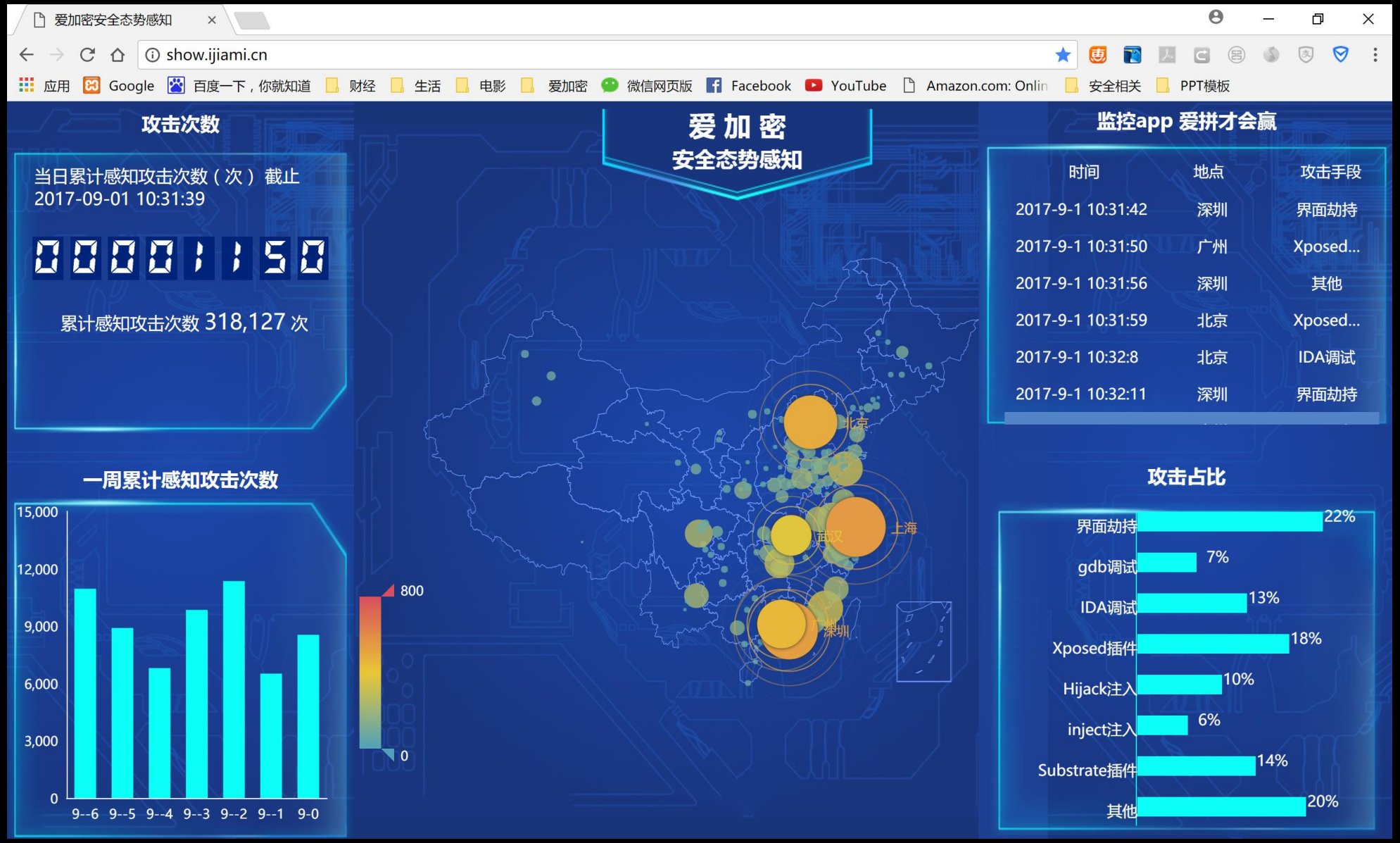


车联网安全运营中心

云安全运营中心为云上安全工具及服务提供基础统一的运行环境。

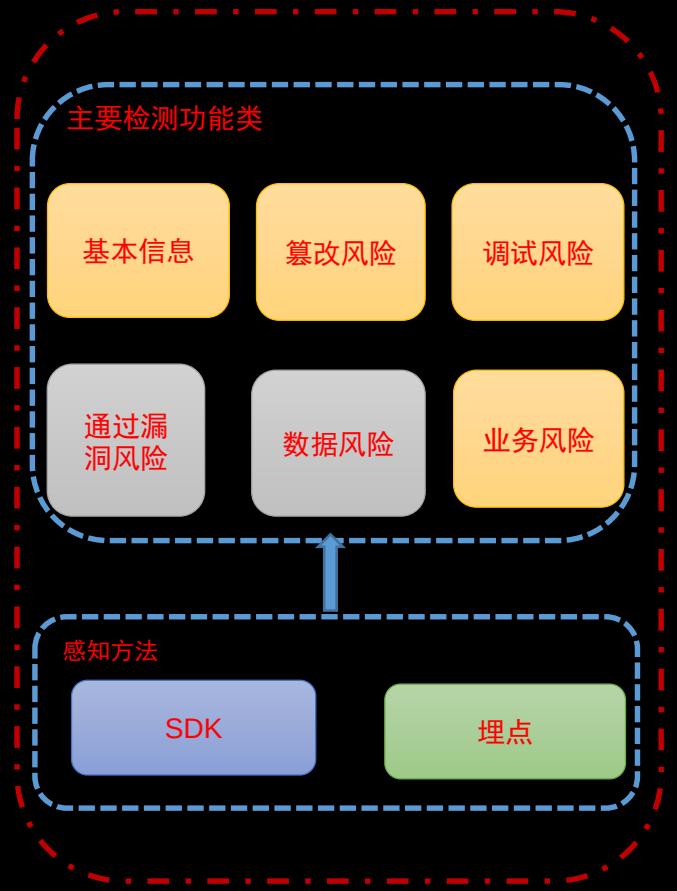
- 通过容器化技术可以将现有云上安全工具集成到同一平台进行管理运行
- 支持快速集成扩展第三方安全工具
- 支持底层数据打通与安全数据采集
- 支持上层安全工具联动进行协同防御
- 支持统一安全管理与系统管理

应用威胁感知中心展示


爱加密安全态势感知
show.ijiami.cn
应用 Google 百度一下，你就知道 财经 生活 电影 爱加密 微信网页版 Facebook YouTube Amazon.com: Onlin 安全相关 PPT模板
攻击次数
当日累计感知攻击次数（次）截止
2017-09-01 10:31:39
00001150
累计感知攻击次数 318,127 次
爱加密
安全态势感知
监控app 爱拼才会赢
时间 地点 攻击手段
2017-9-1 10:31:42 深圳 界面劫持
2017-9-1 10:31:50 广州 Xposed...
2017-9-1 10:31:56 深圳 其他
2017-9-1 10:31:59 北京 Xposed...
2017-9-1 10:32:8 北京 IDA调试
2017-9-1 10:32:11 深圳 界面劫持
北京
武汉
上海
深圳
800
0
一周累计感知攻击次数
15,000
12,000
9,000
6,000
3,000
0
9--6 9--5 9--4 9--3 9--2 9--1 9-0
攻击占比
界面劫持 22%
gdb调试 7%
IDA调试 13%
Xposed插件 18%
Hijack注入 10%
inject注入 6%
Substrate插件 14%
其他 20%

威胁感知中心核心技术

详细感知项说明



基本信息	基本信息	调试风险	Java层代码动态调试风险	数据风险	日志数据泄露风险
	应用权限检测		C层代码动态调试风险		SD卡数据泄露风险
	应用行为检测		动态注入攻击风险		Content Provider数据泄露风险
篡改风险	Java代码加壳检测	通用风险	联网环境检测		数据文件全局可读写风险
	Java代码混淆检测		WebView组件忽略SSL证书验证错误漏洞		资源文件泄露风险
	Java代码加花检测		Webview明文存储密码漏洞		数据越权备份风险
	SO文件加固检测		WebView远程代码执行漏洞		内存dump风险
	H5文件加固检测		WebView file域同源策略绕过漏洞	业务风险	业务测试信息泄露风险
	Activity最小化特权检测		Intent Scheme URL攻击漏洞		系统键盘使用风险
	Service最小化特权检测		Fragment注入攻击漏洞		应用超时连接风险
	Content Provider最小化特权检测		数据库注入漏洞		HTTP传输通道风险
	Broadcast Receiver最小化特权检测		下载任意APK漏洞		SSL证书有效性风险
	拒绝服务攻击风险		优化建议		证书文件明文存储风险
	Intent隐式调用风险				随机数不安全使用风险
	单元测试配置风险				关键界面劫持风险
	硬编码风险				加密算法不安全使用风险
	Java层关键函数风险				终端ROOT状态检测
	私有函数调用风险				
	应用完整性检测				
	程序签名保护检测				
	应用二次打包风险				

分类	感知项	平台	描述
环境感知	模拟器运行感知	Android	程序运行终端是否是模拟器
	终端Root/越狱感知	Android/iOS	终端是否运被root/越狱感知
	终端病毒APP感知	Android	终端是否存在病毒APP感知
	终端系统签名内核机制破坏感知	Android	终端系统的签名内核机制是否被破坏感知
	终端设备信息篡改感知	Android	终端系统获取设备信息的接口是否被恶意篡改感知
	终端系统LIBC内核破坏感知	Android	系统LIBC内核是否被破坏感知

终端应用漏洞检测

多项检测依据

主要检测功能类

- 移动应用漏洞检测
- 移动应用安全规范检测
- 恶意第三方SDK
- 移动应用基本信息检测
- 恶意代码检测
- 敏感内容

检测方法

- APP 静态检测
- APP 动态检测

爱加密检测平台

检测报告

应用名称	XXX 移动应用
检测分数	58
检测项总数	48 (包括 41 项风险检测、7 项基本信息检测)

表2-1 检测得分

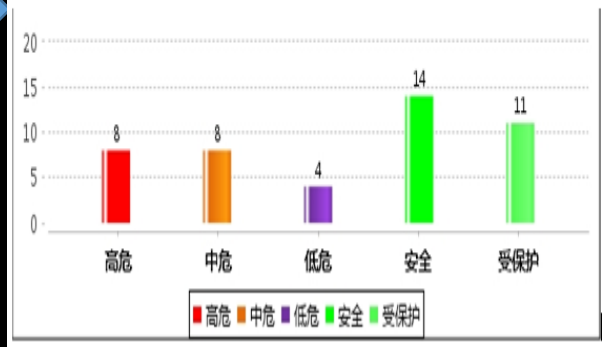


图2-2 检测结果汇总

终端应用安全（Android）

爱加密 www.ijiami.cn

防逆向

DEX文件保护

- 双重VMP技术
- DEX整体加壳
- DEX函数分离
- 多个DEX加密

SO库保护

- SO文件加壳
- SO库混淆（LLVM编译级）

防篡改

代码防篡改

- DEX代码防篡改
- SO库文件防篡改
- H5代码防篡改

资源文件防篡改

- Assets防篡改
- AndroidManifest配置文件防篡改
- Res资源防篡改

签名防篡改

防调试

- 防动态调试
- 防进程调试
- 防内存代码注入
- 防内存DUMP
- 防模拟器
- 防HOOK攻击

数据防泄漏

- 数据传输加密 SDK
- 防日志泄漏
- 本地文件加密
- 本地数据保护

页面数据保护

- 应用防截屏
- 应用防劫持
- 安全键盘 SDK

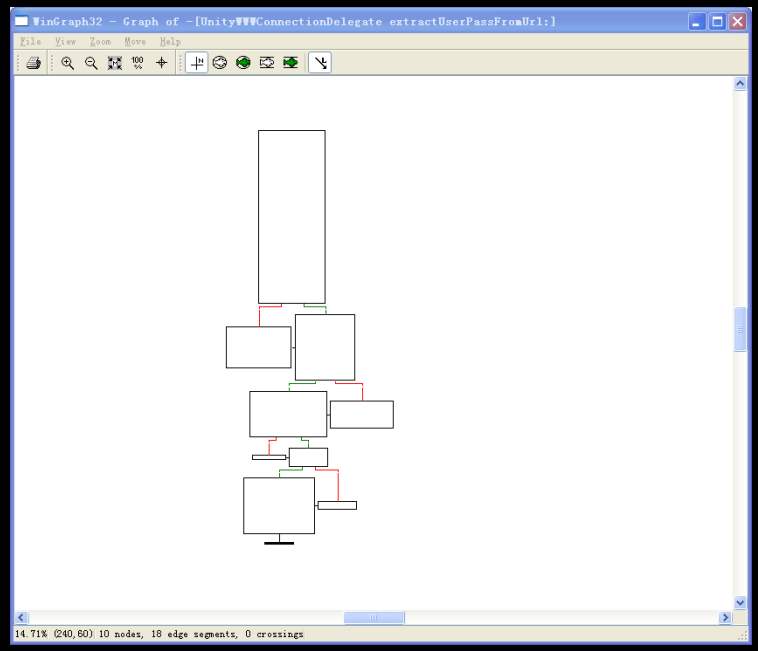
终端应用安全（IOS）

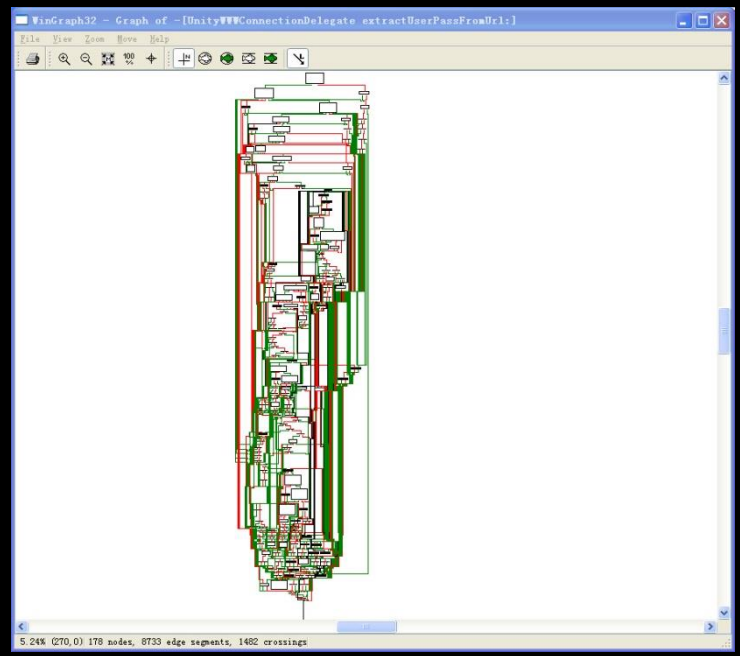
- 爱加密基于移动安全领域的先进的技术和经验，业内首家推出iOS加固方案。
- 针对黑客在分析阶段的攻击手段和行为进行分析，利用iOS混淆加密工具，可以有效的增加黑客信息搜集的难度和复杂度，防止iOS应用被破解，防止App破解后植入病毒和广告代码。

方法体、方法名高级混淆

程序结构混排

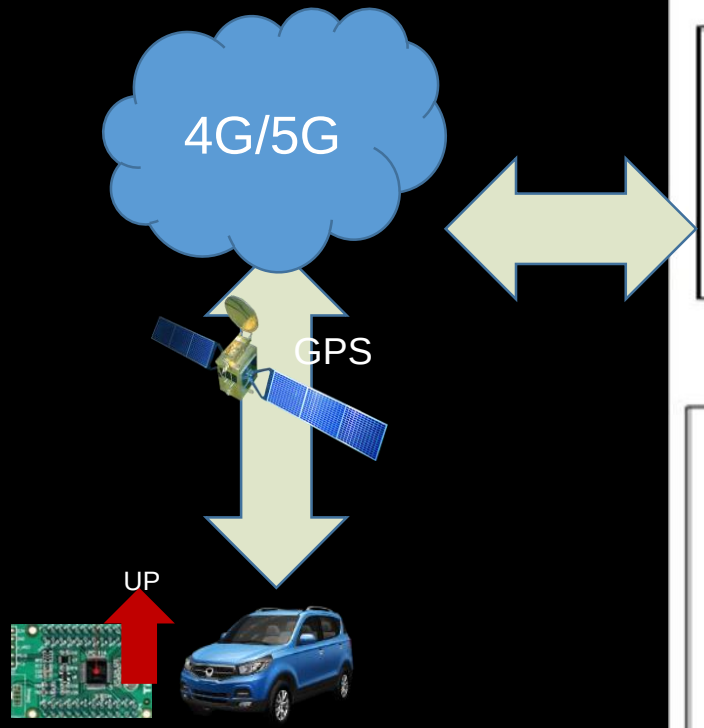
URL编码加密

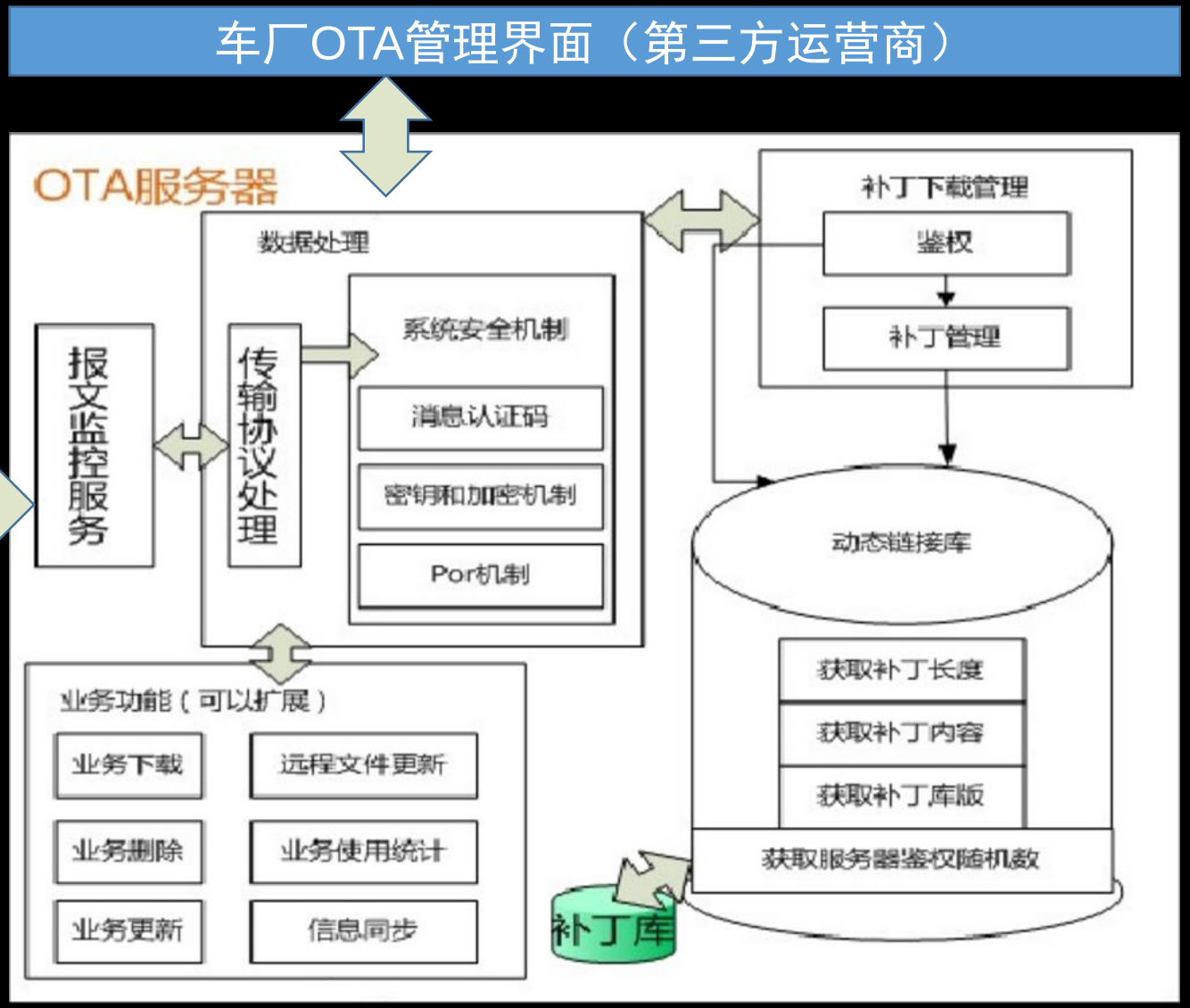




终端系统安全

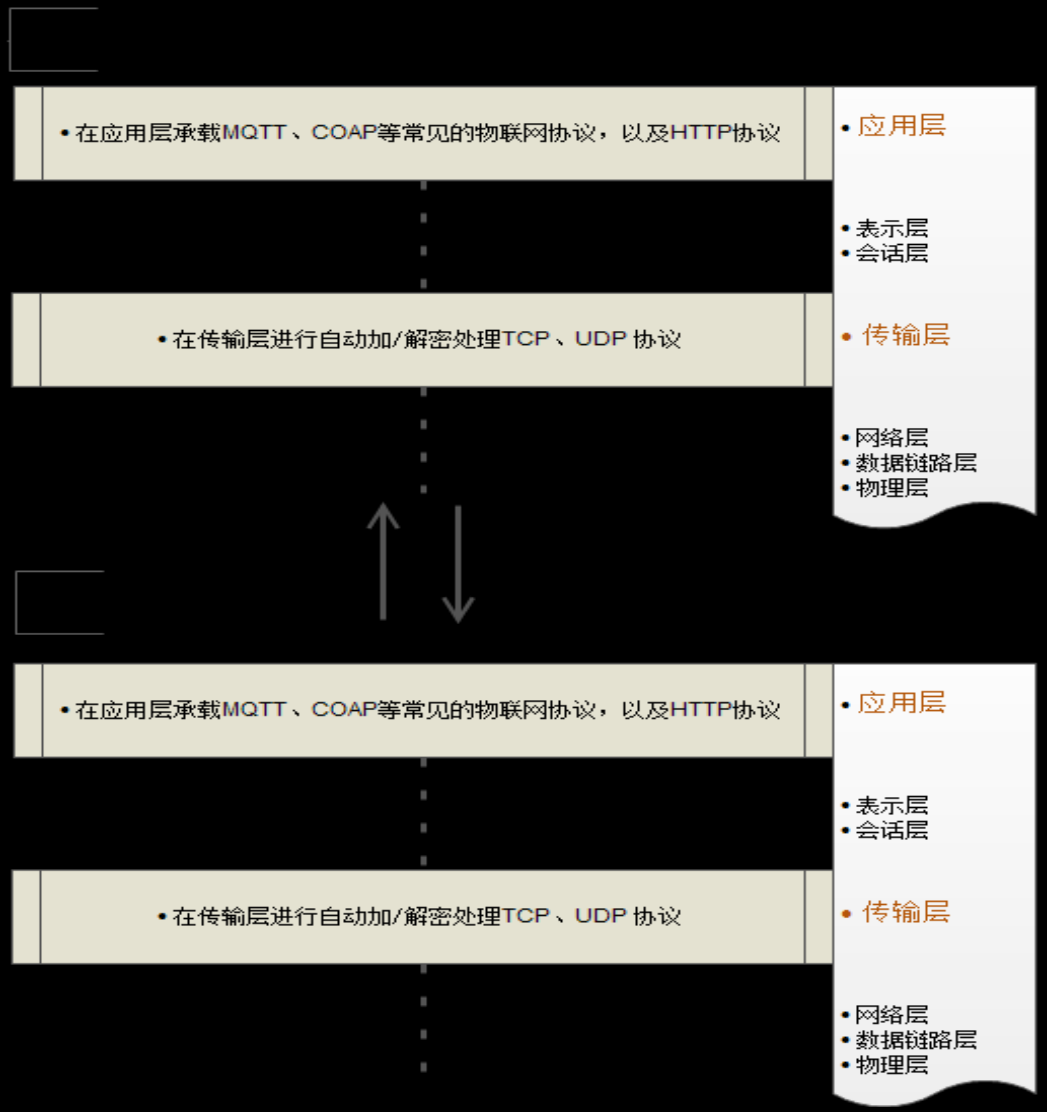
- 固件系统升级
- 车载应用升级
- 系统补丁修复



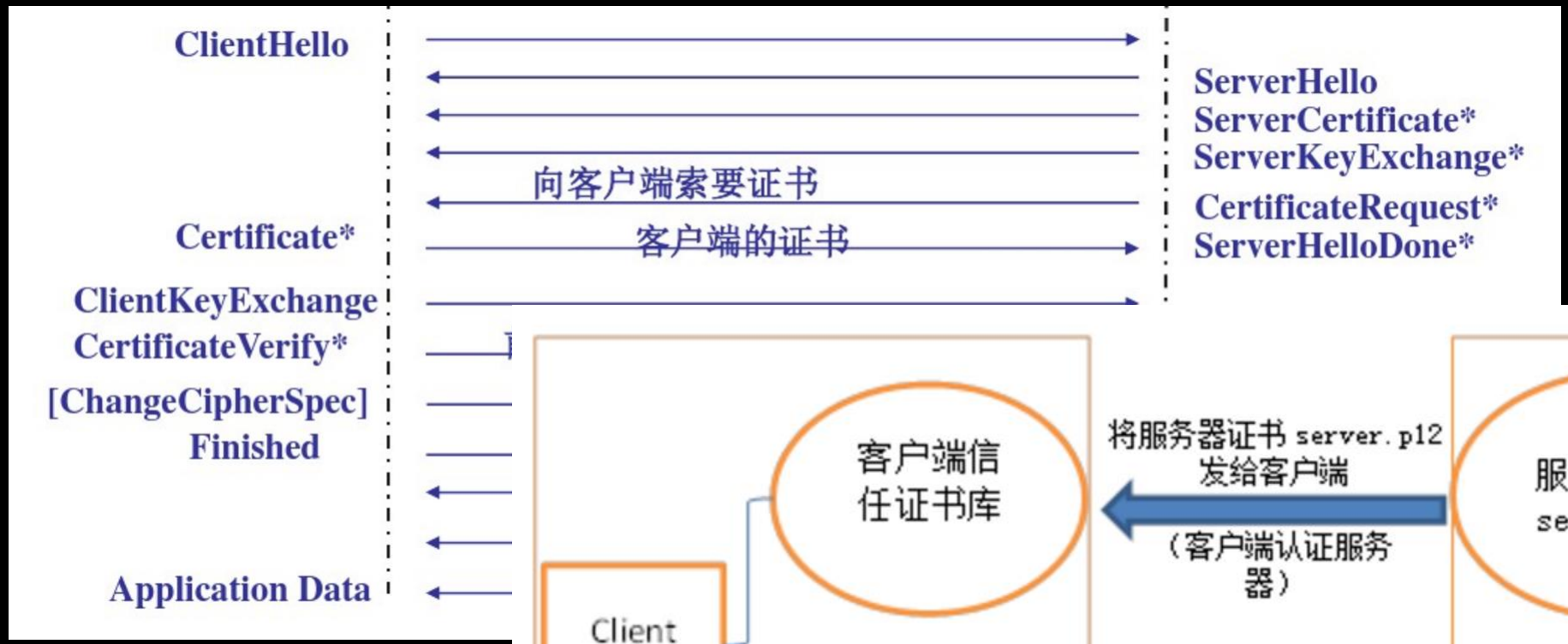


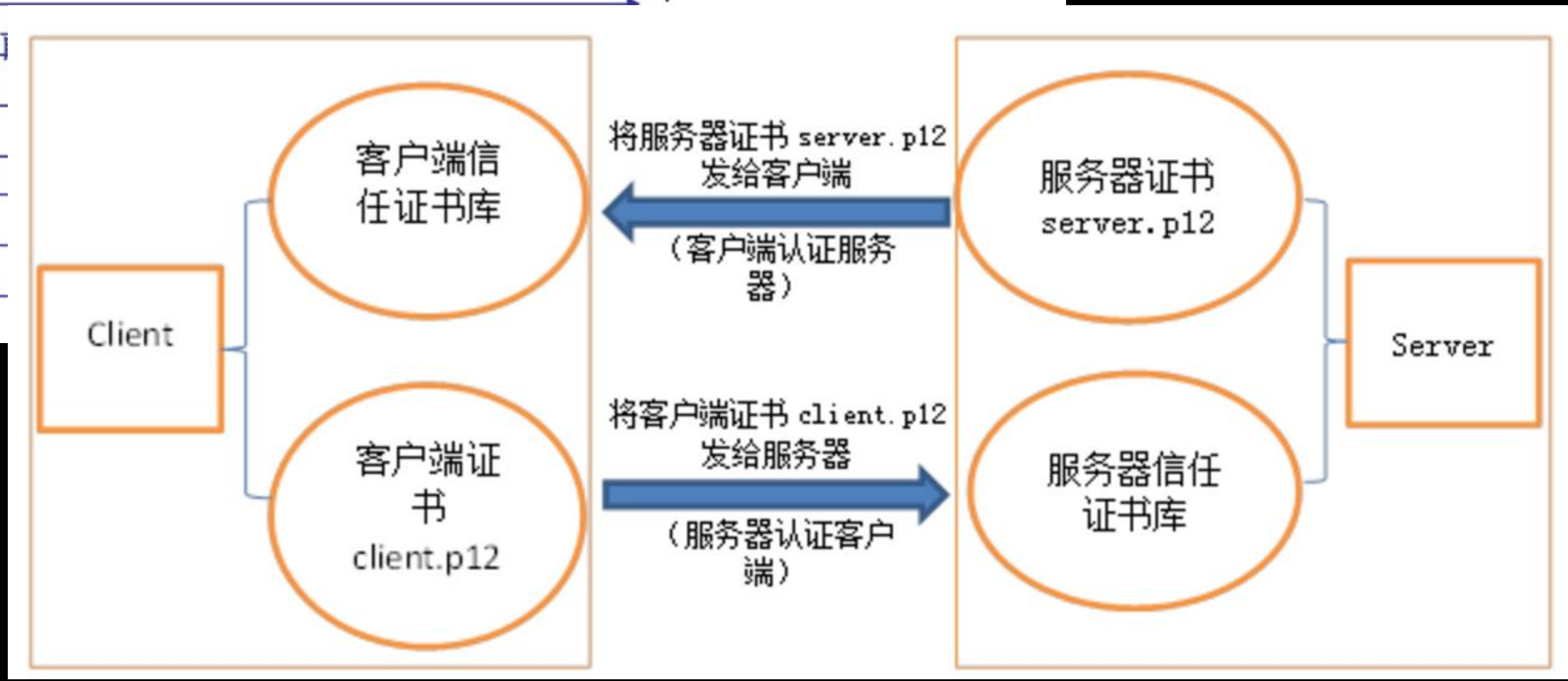
终端通讯安全-私有传输协议

- 基于SSL/TLS协议的优化
- 动态密钥参数
- 双向身份认证
- 可承载COAP和MQTT等常用物联网协议



终端通讯安全





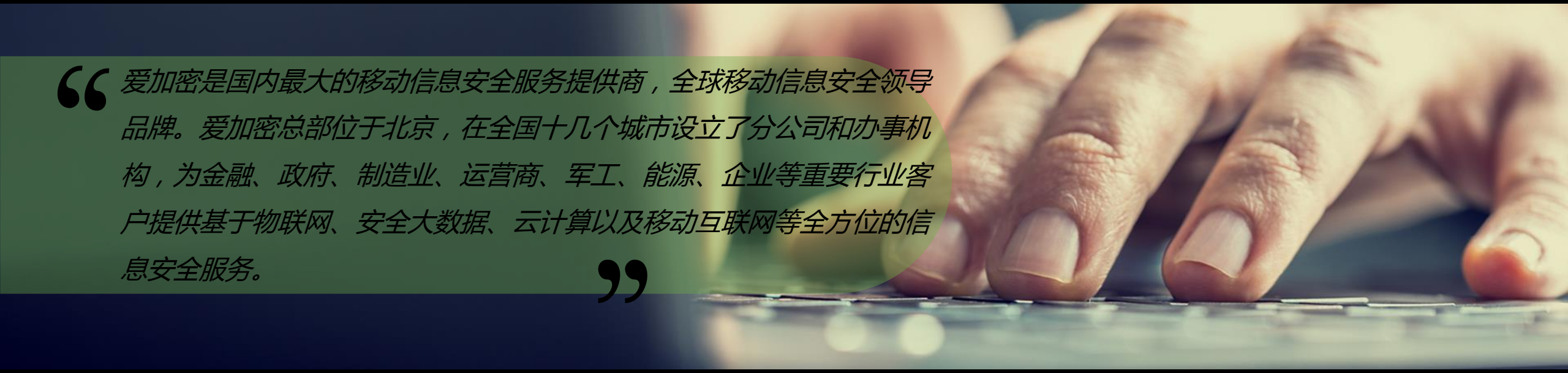
目录

车联网安全愿景


生态建设
行业标准/联盟
联合创新
智能设备漏洞库
开发者万维共管计划
专业服务
商业咨询/网络咨询
SDK集成服务
物联云托管服务
解决方案
爱加密智能车联网安全运营平台
智能设备加固
威胁感知
车联大数据
智慧城市
智能终端
故障抢修、设备管理
……

关于爱加密

爱加密
www.ijiami.cn



爱加密是国内最大的移动信息安全服务提供商，全球移动信息安全领导品牌。爱加密总部位于北京，在全国十几个城市设立了分公司和办事机构，为金融、政府、制造业、运营商、军工、能源、企业等重要行业客户提供基于物联网、安全大数据、云计算以及移动互联网等全方位的信息安全服务。

- 400+员工
- 70%+技术人员
- 超过1500+标杆行业客户
- 50+公司权威资质认证

- 覆盖Android、iOS、H5及物联网设备
- 保护80万+APP
- 覆盖8亿+个人智能终端
- 50+产品软著及专利

爱加密 让移动更安全