Alibaba Cloud Security



Auto Industry Security Solutions

汽车行业场景化安全解决方案

阿里云

前言

随着我国车联网产业的逐步发展，传统汽车产业竞争格局发生了变化。部分ICT企业开始在汽车产业布局，网络运营商、芯片与模组厂商、终端设备商等加速了汽车网联化的进程。

智能化、网联化发展带动车联网架构更新，软件定义汽车驱动产业链重构，量产变现成为重要话题，行泊一体成为主要的实现路径并有望迎来爆发，车联网出海成为重要趋势，OEM与数据集成商合作推动车联网数据变现，安全是最基本的要求，数据安全则是重中之重。

车联网技术架构也从集中式到分布式演进：

· 早期以资产管理为特征的1.0时代，主要代表是响应式TSP服务；

· 后续发展到以交互式服务为特征的1.5时代，主要代表是服务智能座舱、车载操作系统和车云服务；

· 当前已经进入到以主动服务为特征的2.0时代，主要代表是分布式车联网，采用5&6G蜂窝通信，边缘-区域-中心，分布式云等。

阿里云通过全球领先的云基础设施、齐全的安全合规资质以及高效的分布式组网为分布式车联网提供智能网联底座，打造面向高阶智能网联车的新一代分布式车联网。一如既往，我们也会持续响应汽车行业客户不断变化的业务需求和随之升级的安全需求，以新技术方案、新行业实践，持续助力汽车行业安全发展与加速创新。

孙勇

阿里云汽车行业架构与解决方案负责人



2022年11月，阿里云正式发布“汽车云”。耗时三年，阿里云与汽车行业客户、伙伴共同打磨出面向云上车企、自动驾驶公司和上下游企业的行业解决方案。
目前，阿里云已经服务了70%的车企客户，400多家汽车产业链上下游的公司。



目录

01 阿里云汽车行业安全洞察 01

行业背景 01

新一代汽车产业数字化蓝图 02

法规与政策驱动汽车行业信息安全 03

车企信息安全挑战与机遇 05

02 为什么选择阿里云安全 06

车联网行业安全需求矩阵 06

阿里云汽车行业“云-网-端一体”安全全景 07

阿里云的技术与服务优势 08

03 阿里云汽车行业场景化安全解决方案 09

智能网联汽车上云基础安全方案 09

混合多云架构车联网统一安全管控方案 11

车企系统安全运营方案 13

车企云上数据安全治理平台方案 15

汽车行业企业风控决策方案 20

大型汽车集团办公安全方案 22

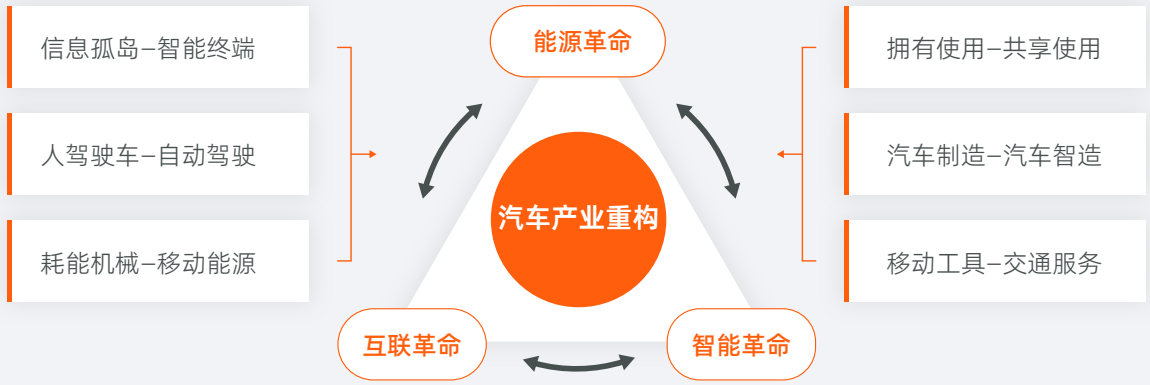
04 汽车行业云安全展望 24

一.阿里云汽车行业安全洞察

01 行业背景

汽车产业是我国国民经济支柱产业，制造业产值约占经济总量的2%，汽车产业相关增加值占GDP的10%。新一轮科技革命，使得作为传统制造集大成的汽车产业，成为继家庭和办公场所之外的“第三空间”和“新型智能终端”，正步入前所未有的变革期。

能源、互联与智能三大革命驱动下，汽车行业的产业格局变得复杂，汽车产品的核心竞争力与价值属性也在发生颠覆性改变：



汽车产业的三大革命与六大革命性变化

汽车价值链发生颠覆性改变

从“制造”到“制造+服务”的集成

汽车产业边界模糊格局复杂

从垂直网状的产业链到交叉网状的出行生态圈

汽车产品属性改变核心竞争力

从“硬件”到“重硬更重软”的平衡

产业内涵与外延不断扩展

智能汽车与汽车社会形成紧密关系，以出行、互联、共享、服务为全新特征，催生多维创新机遇

在当前的技术趋势下，国家将新能源和车联网（智能网联）作为制造业核心竞争力进行布局。

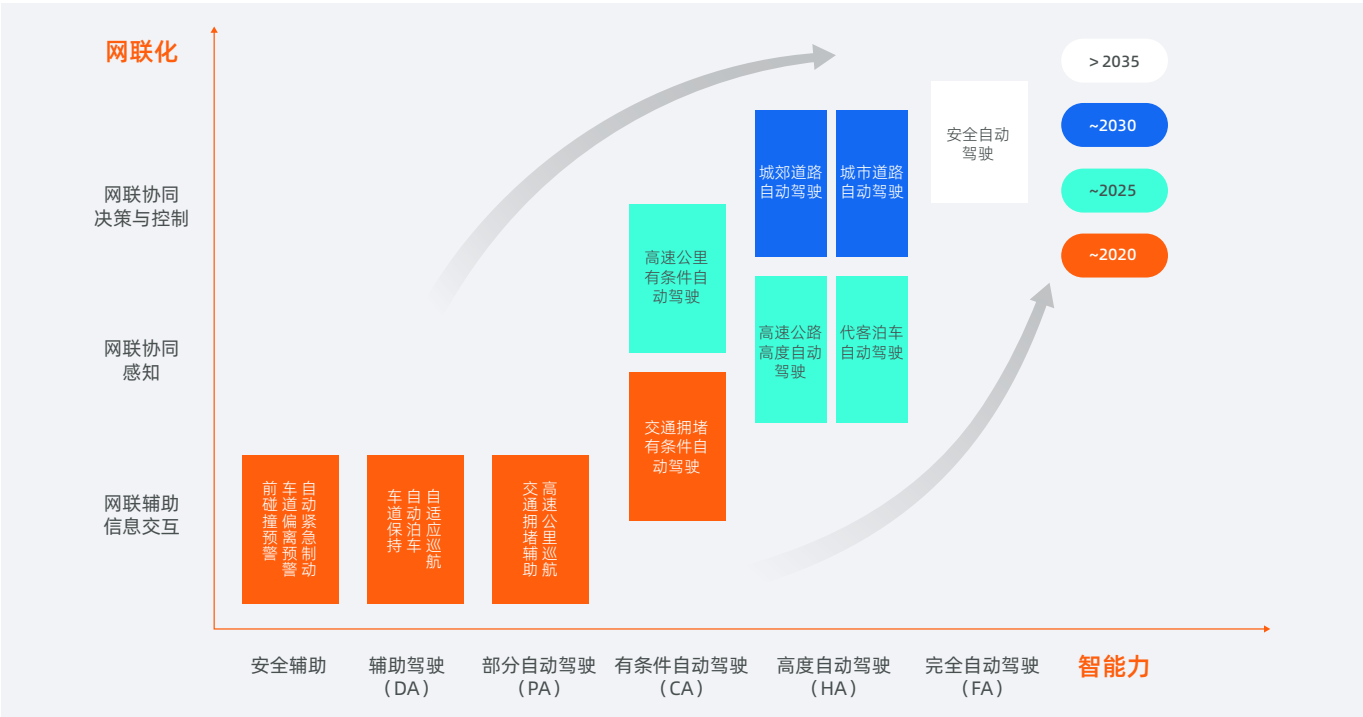
02 新一代汽车产业数字化蓝图

智能化、网联化

车联网技术由人车交互智能化技术与车辆行驶自动化技术构成，数据、通信技术与汽车深度融合，实现汽车与社会和谐发展，是汽车产业数字化转型的重点方向。



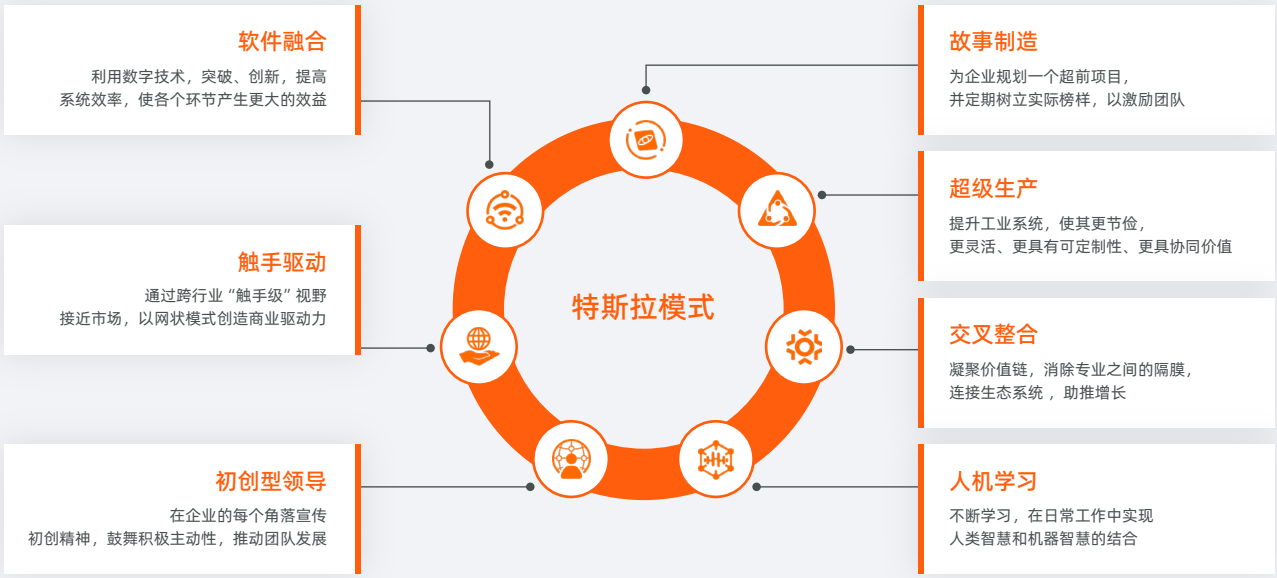
在中国，预计到2035年以后，以完全自动驾驶（FA级技术）和“网联协同决策控制”的高度网联化即将投入应用。车联网将成为未来经济发展的重中之重。



产业演进：人与车的超级连接

技术革命驱动下，汽车行业的上下游产业链都开始重新思考经营方式。同时，客户对个性化和品牌体验的需求持续上升，为全新的数字化商业模式创造了机会。

“利用人、机器和产品的超级连接，助推系统升级，实现系统连接，以满足消费者日益增长的需求”的特斯拉模式正在成为行业主流。智能制造、数字化营销和智慧出行服务等其他产业方向与智能网联汽车进一步形成合力。



03 法规与政策驱动汽车行业信息安全

新一代的汽车产业数字化蓝图，使得车联网市场的发展获得极大的利好，但同时，我们也看到，汽车安全的概念早已从传统的机械性安全外溢。随着国际强制性信息安全法规——UN/WP.29 R155的实施，信息、数据与网络的安全性成为汽车行业的关注重点。

法规驱动是比用户驱动、产品驱动更直接有效的汽车行业网络安全、数据安全的核心驱动力。近年来，国内监管部门也在加强对汽车行业信息安全监管和规范的力度，以出台法律法规、行业标准等方式落地，范围涵盖整车、车机系统、充电系统、诊断接口、远程服务系统、信息服务平台等构成要件。



2019.7

- 《电动汽车充电系统信息安全技术要求及试验方法20192313-T-339 》

2020.4

- 《汽车电子系统网络安全指南》(GB/T 38628-2020)

2020.8

- 《车联网信息服务平台安全防护技术要求YD/T 3752-2020 》

《数据安全法》

2021.4

- 《汽车诊断接口网络安全技术要求 20211169-T-339 》

2021.8

网信办

- 《汽车数据安全管理若干规定》

《网络安全法》

2021.9

工信部

- 《关于加强车联网网络安全和数据安全工作的通知》
- 《车联网信息服务平台安全防护检测要求 2021-0192T-YD 》

2021.9

全国信安标委

- 《信息安全技术汽车采集数据的安全要求》
  明确汽车出车数据进行匿名化处理
- 《汽车信息安全通用技术要求 》(GB/T 40861-2021)
- 《电动汽车远程服务与管理系统信息安全技术要求及试验方法 GB/T 40855-2021 》

《个人信息保护法》

2022.3

工信部

- 《车联网网络安全和数据安全标准体系建设指南》

2022.5

网信办

- 《数据出境安全评估办法》

明确数据处理者向境外提供数据应当通过网信部门向国家网信部门申报数据出境安全评估，加快车企对数据安全的规范化和安全建设

2022.8

自然资源部

- 《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》

明确测绘地理信息数据采集和管理等相关法律法规政策在智能网联汽车（包括智能汽车、网约车、智能公交以及移动智能配送装置等）相关活动中的适用问题

2022.10

- 《信息安全技术网络预约汽车服务数据安全要求 》(GB/T42017-2022)
- 《汽车软件升级通用技术要求 20214423-Q-339 》
- 《汽车整车信息安全技术要求 20214422-Q-339 》
- 《汽车网络安全应急响应管理指南 20213611-T-339 》

《信息系统安全等级保护制度》

04 车企信息安全挑战与机遇

针对目前越来越丰富的车联网应用场景以及V2X相关技术场景的不断扩大应用，车辆及其相关业务系统的风险面正在逐步扩大，云、管（车云网络通信及V2X等）、端三个方面的安全风险，都将成为车联网产业快速发展的阻碍。



汽车安全概念从功能安全向数据安全迁移

从端到管到云，智能网联重新定义汽车。相比于传统燃油车，网联汽车搭载大量的传感器、摄像头和强大的处理器，随着自动驾驶技术的发展，未来将会有更多用户信息与车辆信息上传至新能源车企管理后端。

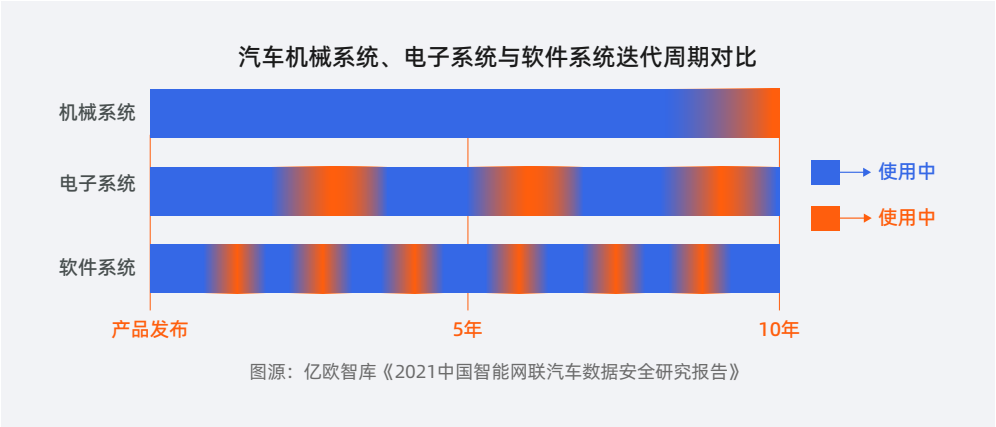
随着汽车越来越像一台大号的“手机”，汽车安全概念开始向数据安全迁移。

智能网联汽车数据数据类别繁复，除汽车自身数据外，承载大量的城市交通数据和用户个人数据，包括用户日常行为轨迹、消费“路线图”等。**其中，城市交通数据与用户个人数据的应用价值更大、泄漏后果也更严重。**

智能网联汽车软件系统迭代频繁，安全隐患多

以往，从0完成一辆传统汽车的开发需要42个月，考虑到发动机则需要48个月，是一场马拉松式的“拉锯战”。

但在“软件定义汽车”时代，汽车软件系统的迭代速度又远超机械系统与电子系统，这对车企的“软实力”提出了巨大要求。如何在快速迭代下保证汽车软件开发速度与功能体验的同时，减少软件系统漏洞、保障汽车数据安全？这已成为车企发展智能网联汽车的一大难点。



图源：亿欧智库《2021中国智能网联汽车数据安全研究报告》

云管端安全隐患不胜枚举

对车企而言，智能网联汽车云管端的安全隐患不胜枚举，并且具备以下三个特点：

1. 终端种类多，车载终端安全存在漏洞；
2. 网络协议多，通讯数据安全受到威胁；
3. 使用场景多，云、管、端各个板块安全保护方案与安全衔接较弱。

在合规与企业刚需的双重推动下，车联网安全未来可期。

二.为什么选择阿里云安全

01 车联网行业安全需求矩阵

汽车行业信息安全需求随着客户需求和网络威胁等级变化而呈现动态变动。
从当前的车联网业务来看，数据安全和网络安全需求处于极高水位，随着数字化转型进程的加速，车企对于跨环境安全运营、安全开发和出海合规认证的需求也呈现明显的上升态势。



01

数据安全：

车联网伴随自动驾驶能力的提升，对数据　采集和处理的量成几何级数增长，远程平台进行数据脱敏降密处理，满足合规要求已经成为车联网的重要安全任务。

> 一辆智能网联汽车所产生的数据类型复杂，除了驾乘人员的面部表情、声音数据，还包括高精度地图信息、高清晰度的道路环境数据、乃至汽车充电网络点数据等等。
> 一辆2020款的网联智能电动车每8小时可产生4TB的数据量，每台车对存储的需求量在32GB左右；L2级车辆预计每天产生32G数据，L4级车辆每天产生超过1.5T数据。

02

云网络安全：

云端是整个车联网生态系统中的用户服务核心，需要在保证及时响应车辆请求相关服务、支撑行业服务商完成数据交换和对接的的同时，检测并阻断因漏洞、网络攻击、系统性威胁带来的影响业务运行，造成隐私泄露和财产损失，甚至危及人身安全的问题。

03

跨环境安全运营：

现代混合数据中心架构下，跨环境的安全运营尤其复杂。传统安全产品各自为战、饱和式堆砌造成的问题是部署慢、检测运行卡、资源占用高和费用开销大，权限管理、信息与事件管理、配置管理等运营动作难以多平台高效协同，更易造成情报滞后、新漏洞无告警等系列问题。

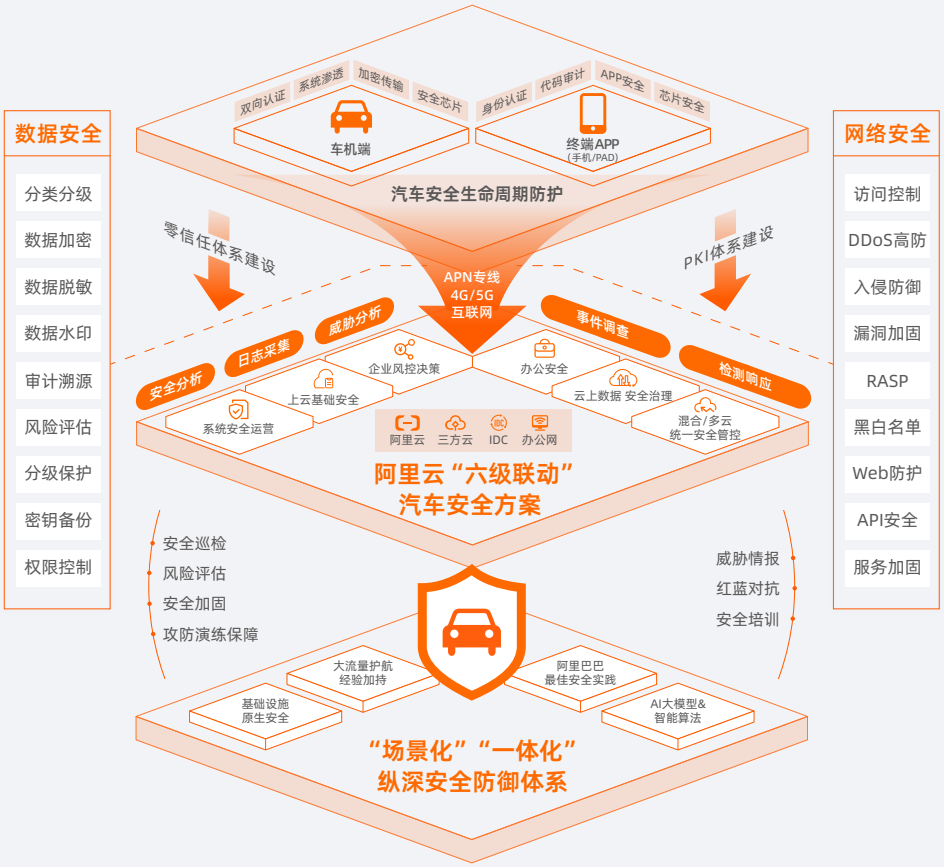
02 阿里云汽车行业“云-网-端一体”安全全景

阿里云安全为车联网用户构建 “从云到端”的纵深安全防御三道防线：

第一道防线关注混合云、多云架构边界防护，实现云与云、云与线下IDC的南北向和东西向流量安全和权限控制；

第二道防线保护云主机、容器以及办公终端的计算环境安全，并建立基于零信任的可信访问；

第三道防线关注信息与数据安全流转，实现重要地理数据、行驶数据和个人敏感数据的识别与分类分级管理，对重要数据进行加密或脱敏保护，同时设立数据行为全量审计及溯源机制。



利用三道防线的防御纵深和智能协同，最大程度帮助车联网用户抵御各类安全威胁：

自动化威胁分析模型联动MDR，快速建立一个主动的、集中化的安全事件分析及响应中心，协助分析研判，并基于事件应急响应策略或SOAR策略实现处置闭环；

为汽车各项业务开展环节注入欺诈识别、智能核身、风险内容识别等的风险管控原子化能力，帮助用户降低业务合规风险；

日常安全巡检与重保场景实战攻防有机协同，有效提升团队安全人员攻防对抗能力；

为车企提供各类专业安全咨询及认证服务，帮助用户进一步实现国家及行业的安全合规要求。

03 阿里云的技术与服务优势

为什么阿里云提供的场景化安全方案更适合汽车行业？

基础设施原生安全 打造车企“云上绿洲”：

阿里云通过强大算力，全球覆盖度高，良好的云资源接入能力和强大的边缘云网络支撑汽车企业数字化转型升级。与此同时，创新的云原生安全，拥有从硬件层透穿的最高等级安全能力，打造全环境、全生命周期的可信环境。安全能力和威胁模型，早在产品设计阶段，就已经被融入到云平台和产品设计中，以“内生、原生”安全力为汽车用户打造“云上绿洲”。

国家级攻防演习与大流量护航经验加持：

基于云上安全能力连续多年护航天猫、淘宝双十一，以及保护阿里集团核心业务100%深度用云的经验积累，长于应对大流量、高并发场景的强大产品力，形成智能网联汽车行业可复制、可落地的重保护航与日常安全运营最佳实践；

电商业务安全经验平移至汽车行业营销：

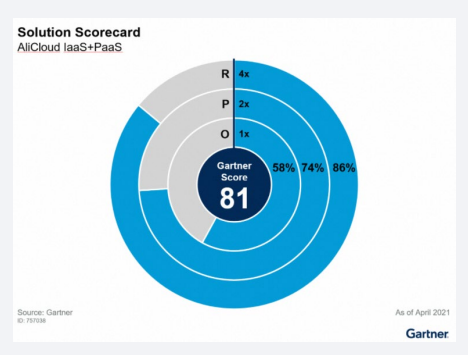
基于集团电商业务为上亿用户和上千万商家的安全保驾护航的运营经验，阿里云将业务安全反欺诈、营销交易环节风险识别、黑灰产对抗、bot管理、内容安全与智能核身等能力平移至新消费范式下的汽车行业营销场景，助力汽车行业营销能力安全升级；

AI大模型与智能算法前沿研究：

大模型对海量数据的处理能力以及多维度分析能力，为车联网尤其是自动驾驶提供了更精准、更全面的分析、预测和模型优化基础。随着阿里云「通义大模型」陆续接入阿里巴巴的各项业务中以提升用戶体验，阿里云还将为客戶和开发人员开放该大模型，令他们能以更低成本建构专属 AI 功能。进一步缩小安全能力与高速发展的智能车联网业务间的“代差”。

Gartner认证全球云厂商安全单项最高分

在Gartner发布的2021年阿里云国际IaaS+PaaS解决方案记分卡中，阿里云获得81分（满分100分），且在计算、存储、网络、安全的评估中获得最高分。 这是阿里云连续第三年入选本报告，而阿里云也是迄今为止唯一入围这份报告的中国云厂商。



三.阿里云汽车行业场景化安全解决方案

01 智能网联汽车上云基础安全方案

方案概述

新的技术趋势演进以及汽车产业数字化进程的加持下，车企IT基础设施开始全面上云，云上业务快速增长的同时，网络环境和海量数字资产更加开放，行业监管机构和消费者对汽车产品和服务的网络安全风险和数据合规风险的担忧也与日俱增。

阿里云提出的上云基础安全原生方案，针对网联汽车业务上云后的基础安全体系建设框架，参照等保2.0三级安全合规要求设计，从安全通信网络、全区域边界安全、安全计算环境和安全管理中心四个维度入手，让汽车上云后的IT基础设施快速部署接入原生安全能力，保护上云业务的安全稳定运行。

三级等保要求		对标产品
安全通信网络	应流免将重要网格区域部署在边界处。重要网络区域与其他网格区域之间应采取可靠的技术隔离手段	云防火墙
全区域边界	应在关键网格节点处检测、防止或限制从外部发起的网络攻击行为	DDoS高防
	应具有提供访问控制、边界防护、入侵防范等安全机制	Web应用防火墙
	应能对各类安全事件和新型攻击进行分析、识别、报警	云安全中心
安全计算环境	应对用户进行身份鉴别、访问控制、运维审计	壁垒机
	应启用安全审计功能，数据进行安全审计	数据库审计
	应满足数据完整性和数据保密性的要求	SSL证书
	应能发现已知漏洞，并在经过充分测试评估后，及时修补漏洞	漏洞扫描
	应仅采集和保存业务必需的用户个人信息，并对数据安全审计范围进行扩展	敏感数据保护
安全管理中心	应对系统资源和运行进行配置、控制和管理。包括用户身份、系统资源配置、系统加载和启动、异常处理、数据和设备的备份与恢复等。	安全管家



服务模式

采用阿里云安全产品企业级版本，通过包年包月方式实现按需购买。投资灵活，部署便捷。
采用阿里云安全管家企业级服务，协助开展云上安全运营。

适合客户群体

新上云的汽车企业

方案优势

智能深度防护

“自研规则+AI深度学习+主动防御”的多重安全，多年护航数据与实战经验，结合阿里真实业务场景累积的全网威胁情报，精准应对未知威胁；

快速部署接入

多数云安全产品采用原生化设计，并支持与云产品联动，一键开启即可部署，对业务“零”打扰；

稳定弹性防护

产品具备可靠的容灾能力，实现毫秒级响应，性能支持弹性扩容，贴合业务发展需要。

专业安全服务

阿里云安全专家累积的云上最佳安全运营实践，为车企上云提供深度安全检测及响应服务，快速构建基础安全运营体系。

用户价值

· 帮助业务新上云的汽车企业用户体系化搭建云上安全防护架构；
· 帮助车企业务实现一键接入，免版本更新，大幅度降低运维工作复杂度并提升工作效率；
· 按需购买安全资源，节约IT资金成本；
· 威胁情报快速协同防护，带来智能安全管理体验。

行业客户信任之选

智己汽车　斑马智行　哪吒汽车　星星充电



02 混合多云架构车联网统一安全管控方案

方案概述

汽车主机厂自身数字化底座建设和升级过程中，大量采用多云、混合云架构，这在客观上给网络安全防护与集中监控带来诸多挑战，云上云下统一安全防护无法打通、传统安全设备难以覆盖云上业务系统等问题，成为主机厂数字化升级的主要障碍。

混合云/多云架构下，阿里云的车联网统一安全管控方案，提供跨IDC和多种云环境的原生一体化安全防护，安全能力在边界、网络、主机与运维侧全面打通线下机房与其他三方云平台环境集中管理，保障数字化主机厂享受与阿里云上安全同等级的防护。

平台统一

多类型主机统一管理，安全防护无死角

能力统一

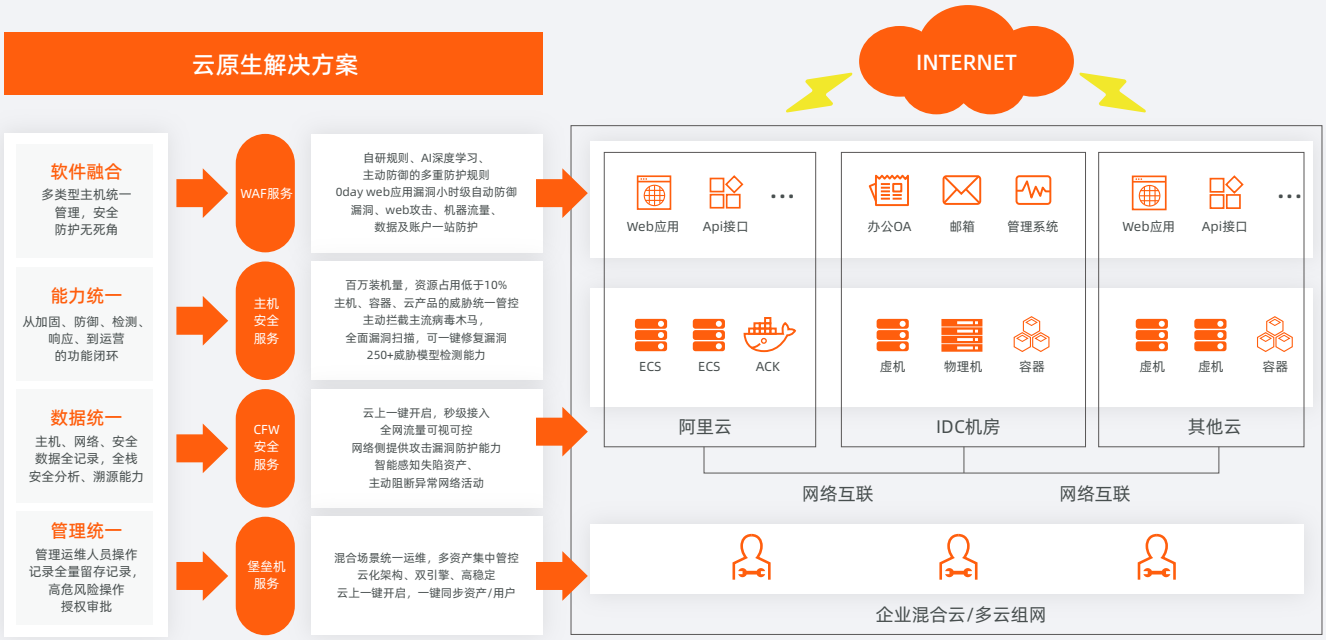
从加固、防御、检测、响应到运营的功能闭环

数据统一

主机、网络、安全数据全记录，全栈安全分析溯源能力

管理统一

管理运维人员操作记录全量留存记录，高位风险操作授权审批。



服务模式

采用阿里云安全产品混合云版本，通过包年包月方式实现按需购买。投资灵活，部署便捷。

适用客户群

多云场景下的汽车上下游企业



方案优势与用户价值

阿里云的多云，混合云场景整体安全防护方案，在日益复杂的IT环境下帮助主机厂用户实现安全方案一体化，整体防护，集中运营，全面提升云安全情报处理能力与处置效率。

统一监控、集中管理

提供多云、混合云场景的集中监控，无需多平台跳转，安全事件集中管理；

安全策略统一部署

通过网络边界、主机以及安全运维多维度安全策略统一下发，保障整体策略一致性，杜绝安全死角；

安全防护水位提升

在重保、攻防演练中，阿里云安全实时策略保障跨环境防护策略的实时同步，确保攻击事件及时发现与多方协同。

行业客户信任之选

多云场景成为IT建设的大势所趋，但是对于安全管理，多平台安全管理给日常安全运营造成极大的负担。借助阿里云混合云方案，我们实现了对公有云、专有云以及它云的安全统一管；实现边界防护策略统一部署，安全事件集中监控，安全日志集中分析。借助阿里云强大的检测引擎，实现了对复杂资产场景下的安全集中管控。

——某世界知名跑车和赛车生产商

03 车企系统安全运营方案

方案概述

伴随监管部门针对汽车主机厂信息安全监管力度增强，安全攻防演练日益成为常态化安全防护要求，主机厂的工作重心步入**「日常安全服务与重保护航并重」的安全运营新阶段。**

阿里云提供的车企常态化安全运营方案，一方面为云上汽车企业提供日常安全的MDR服务，结合阿里云专家累积的云上最佳安全运营实践的深度安全检测及响应服务，覆盖安全评估、安全检测、风险管理、云产品风险管控、资产安全加固等，为客户快速构建基础安全运营体系，保障客户云上业务安全。

另一方面基于阿里云丰富的护航经验，为客户提供量身定制的重大活动保障期间护航服务，保障客户从业务目标制定到护航方案落地全过程，在护航期间提供7x24小时应急响应，帮助客户平稳地度过业务高峰的同时提升主机厂自身攻防对抗水平。



随着智能网联汽车发展日盛，汽车行业各类对客工具与日常办公、营销工具平台均呈现应用开发密度大、迭代频率高的现状，不同应用工具的上线紧急程度不同，安全控制手段和流程也需要因情况制宜。

阿里云引入DevSecOps技术方案，通过“望闻问切”的方法，对关键业务进行识别和梳理，并对当前安全组织架构、安全管理制度和各类数字化工具的应用架构和安全防护措施进行调研。结合应用工具安全开发全生命周期流程和客户业务管理实际需求，从源头把控安全风险。以“生命周期记录表”的形式，记录业务系统“安全档案”，风险可查，责任可追。



服务模式

提供订阅方式或者按需（工作量）方式提供售卖服务

方案优势与用户价值

该方案辅助客户做好云上安全防护，全面提升安全运营、应急、保障能力，确保客户安全运营高枕无忧。

01

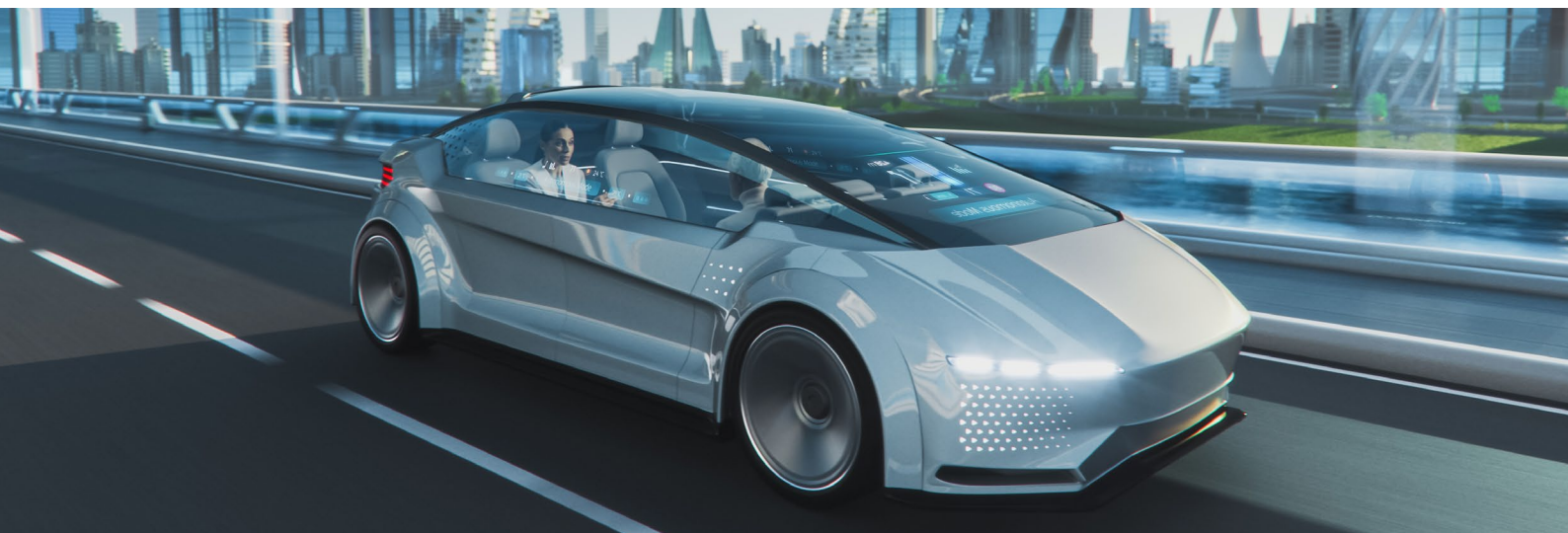
安全防护运营全覆盖

阿里云作为安全服务伙伴，提供从产品到服务，从日常安全运营到重保护航、再到攻防演练服务的全方位安全运营体系；

02

云上安全最佳实践落地

阿里云安全最佳实践以运营方案的形式落地汽车行业，为客户提供从计算、网络、数据等多方面安全评估、安全配置与风险管理最佳实践，提升整体安全水位；



行业客户信任之选

长安汽车

“长安汽车始终把用户隐私和数据保护放在第一位。阿里云提供的"研运一体"安全方案，切实可行地帮助我们将基于混合云的业务安全与数据安全融入到CDP建设和运营中，提升本质安全，实现降本提效。”

——李鹏 长安汽车安全负责人

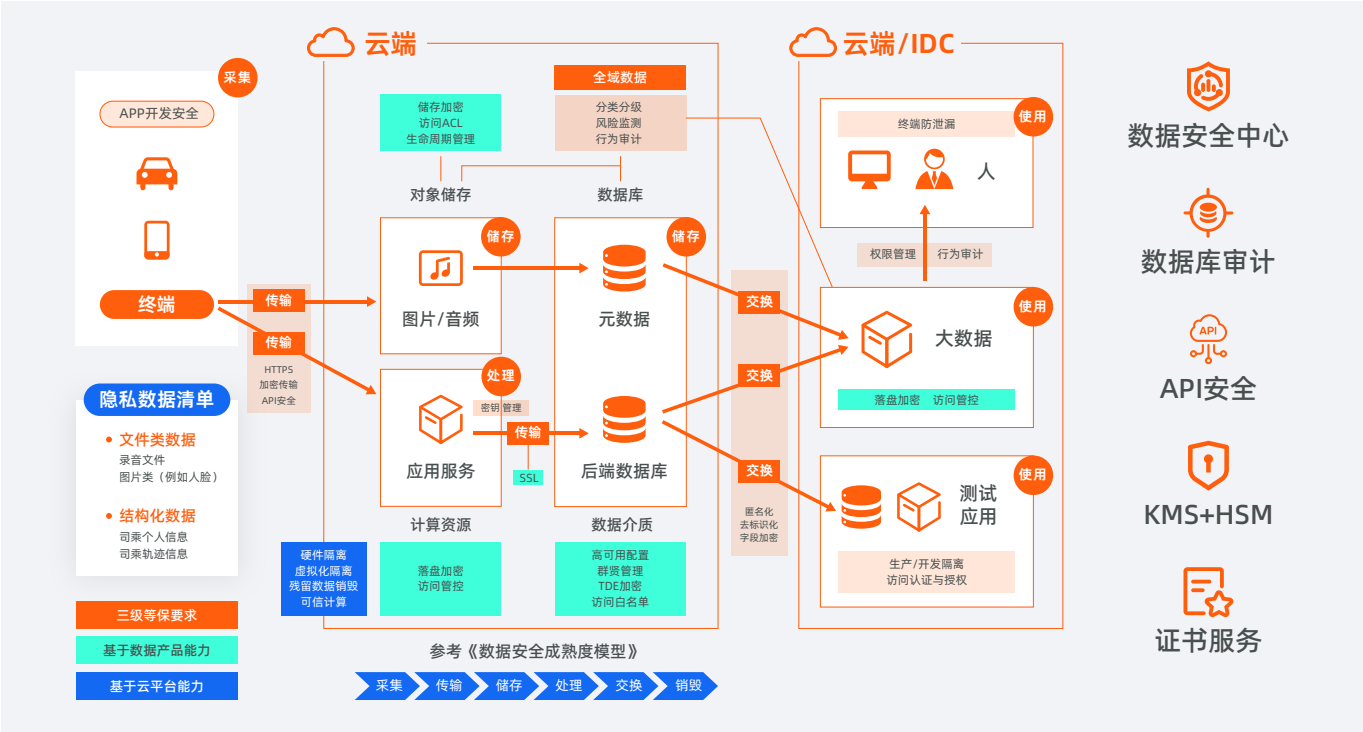


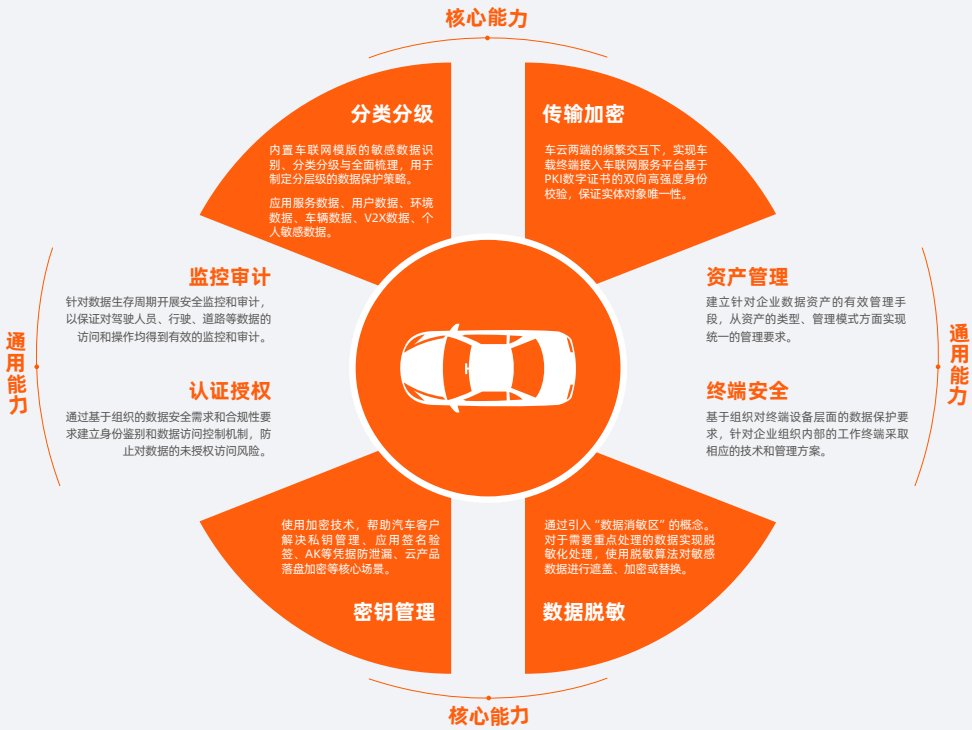
信通院“2023安全守卫者计划”优秀案例

04 车企云上数据安全治理平台方案

方案概述

汽车数据是车联网运行的关键，智能网联时代，数据中不乏大量的用户个人信息、汽车运行数据和城市道路环境数据。保障汽车数据安全，并在合规前提下促进汽车数据的充分合理利用，成为当前汽车企业面临的重大课题。
阿里云参考数据安全成熟度框架（DSMM），基于大量云上企业数据安全工作经验，提炼出云上企业需要构建的数据安全核心能力，方案覆盖数据采集、传输、存储、处理、交换、销毁的全生命周期，帮助企业提升云上数据风险防御能力，实现企业核心及敏感数据安全可控。





汽车行业重要数据（核心级）的安全保护要求：
相关单位在处理该级别数据前，应充分评估处理场景的必要性，以最小必要为原则；
在处理该级别信息时，应采取最严格的保护措施，减少数据安全风险。
——《智能网联汽车数据分类分级实践指南》（2022年）



要点1、数据全生命周期安全治理

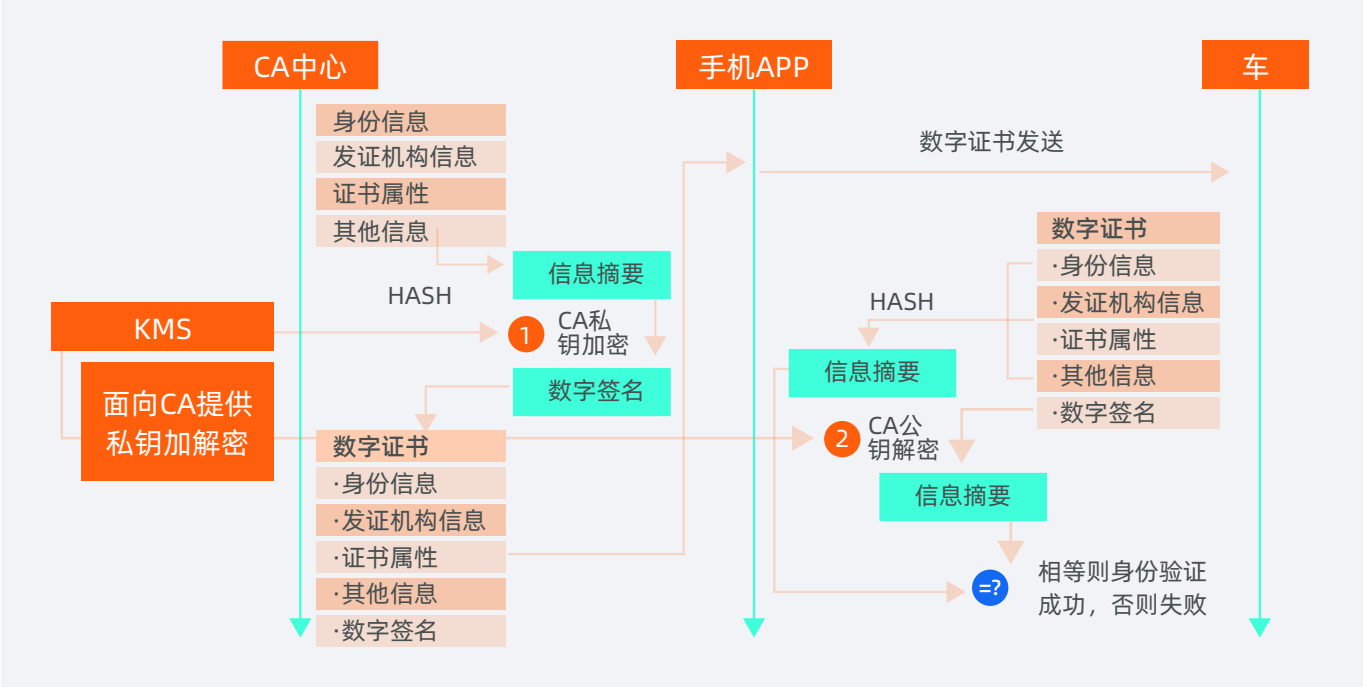


数据安全治理过程（全生命周期保护）

要点2、敏感数据脱敏与数据加密

阿里云提供的密钥管理服务（KMS）基于国密密码机，提供密钥安全托管、密码运算等基本功能，内置密钥轮转等安全实践，同时支持其他云产品通过一方集成的方式对云产品管理的用户数据进行加密保护。

· 针对核心资源ECS、RDS、OSS提供默认加密，并且对于核心数据进行整体加密，提升数据安全水位；
· 针对个人、汽车、车机等敏感数据对称加解密，加密过程中可支持企业客户10万+QPS的实时加密请求，密钥备份与恢复支持全球地域，实现业务数据高可用；
· 面向企业客户提供签名验签的能力，支持针对企业双向认证之后的证书签名、密钥验签的能力；



· 凭据管家能力针对汽车客户APP、web应用产品服务中的AK、SK、RDS账号口令进行有效托管，实现解决AK、SK的安全风险问题。

服务模式

采用阿里云安全产品企业级版本，通过包年包月方式实现按需购买。
采用阿里云数据安全咨询服务，协助开展数据安全治理。

适用客户群体

车联网上云用户

方案优势与用户价值

方案帮助车企用户体系化搭建云上数据安全防护架构，提供强大的数据保护机制，在秘钥管理等核心数据保护场景，为用户提供强大支撑平台，更加安全可靠，有效减少自建开发成本。

01

以国家标准为顶层指导框架

阿里云作为国家标准《GB/T 37988-2019 数据安全能力成熟度模型》（DSMM）的主要起草方与参与方，为客户提供的是具备“顶层视角”的数据生命周期整体解决方案。

02

可复制的阿里云数据安全最佳实践

基于阿里巴巴多年数据安全工作实践，结合阿里云在协助海量企业上云过程中累积的丰富经验，提炼出的可供广大汽车主机厂参考并实践的云上数据安全最佳实践。

03

产品能力行业化沉淀，可扩展性强

数据安全中心支持车联网分类分级模版，并支持用户自定义策略，贴合行业数据特点；提供多维度数据安全报告，满足监管要求。

04

安全可靠的原生级加密服务

支持广泛的云产品集成，提供独享的云密码机集群，拥有云密码机的完整控制权，具备更高的密钥安全保障，密钥管理服务在每个地域构建了多可用区冗余的密码计算能力，保证向密钥管理服务发起的请求可以得到低延迟处理。

行业客户信任之选

哪吒汽车

借助阿里云的数据安全中心，第一次照亮了我们在云端的数据资产，看清了敏感数据分布，通过产品提供的风险管理能力，让我们可以顺利完成数据风险治理和保护工作，从容应对数安法、个保法等合规要求。”

——朱翱宇 云平台高级总监 合众汽车



中国信通院“2022星河案例”数据安全专项优秀案例



05 汽车行业企业风控决策方案

方案概述

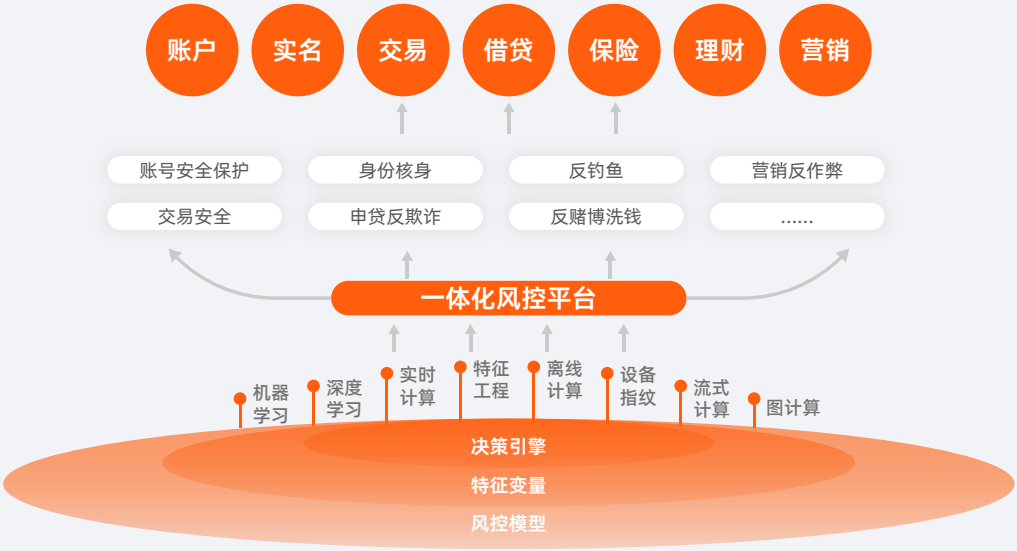
汽车行业的数字化营销已经形成普及态势，主机厂的数字化营销逐渐转向：

线上用户运营，提高用户粘住度和忠诚度；

打造高频营销活动，提升用户群体的活跃度；

推出自有金融信贷业务，实现用户群体用车需求闭环。

哪里有利益哪里就有黑灰产。车企在用户运营过程中面对到的恶意注册、刷单、羊毛党等问题，催生出了平台与黑产的高对抗需求。阿里云汽车行业企业风控决策方案，提供实时分析、精准识别、全场景覆盖的业务风险管理产品，基于海量攻防样本、机器学习算法以及流式计算等技术，帮助汽车一站式管理用户注册、营销活动以及后续金融信贷等关键业务的欺诈风险。



服务模式

提供SaaS化服务，按场景、请求测试进行，预付费、后付费。

适用客户群体

数字化营销下主机厂、经销商等。

方案优势&用户价值

保障客户数字化营销的正常开展，提升与黑产对抗能力，提供更丰富、更智能的识别能力和智能算法。

01

极速分析

支持毫秒级分析，高并发，快速返回分析结果，更快发现风险，及时止损。

02

实战经验丰富

经历多年淘宝、支付宝、阿里云等实际业务风险管理考验，拥有海量的特征样本及丰富的数据模型分析经验。

03

人工智能

运用机器学习算法，与风险对抗过程中不断学习与进化，风险识别快人一步。

04

灵活接入

接口级服务，高易用性，快速接入。

05

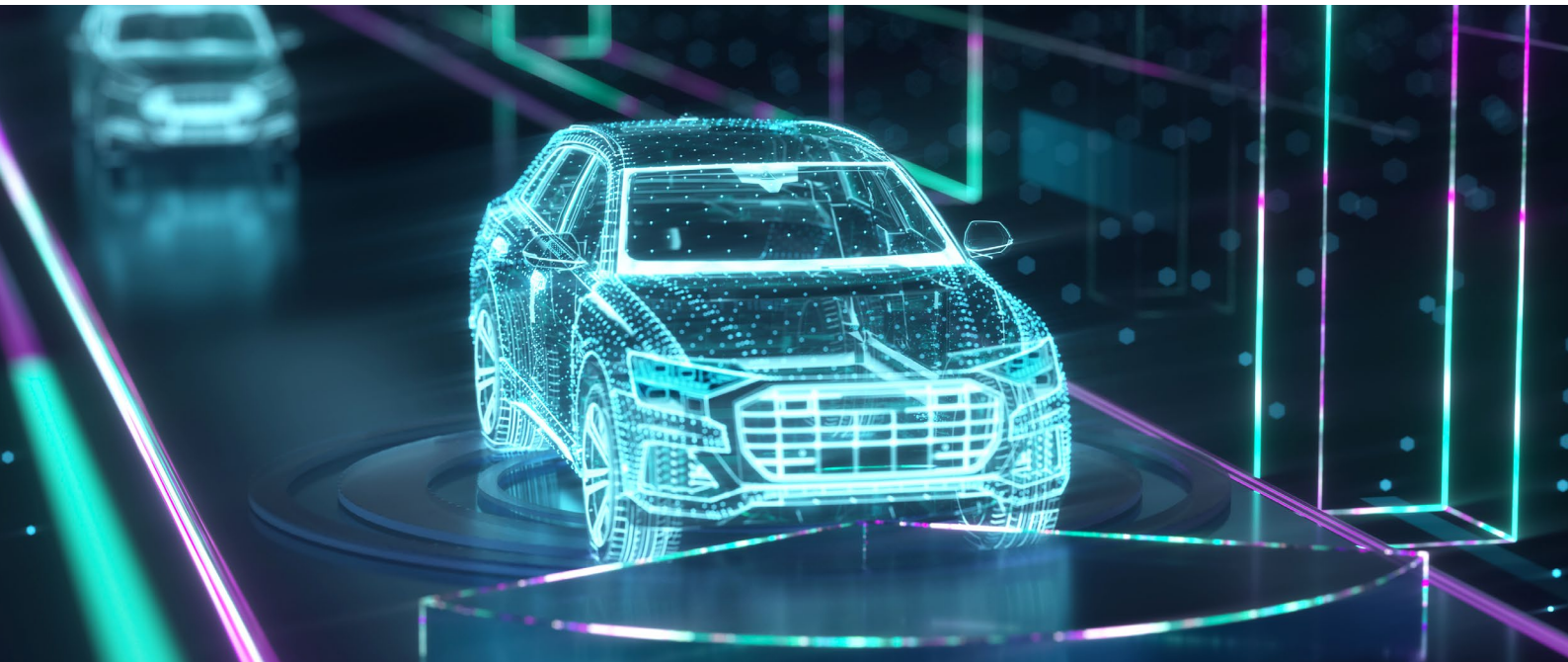
全链路防控

结合客户端边缘计算与云端大数据，全链路对抗粗暴机刷与精细化人刷等风险操作手法。

行业客户信任之选

集团数字化运营为销售业务带来巨大用户增长的同时也面临着薅羊毛、社群恶意控评等严峻挑战，借助阿里云全链路风控解决方案，让我们得以真正将黑灰产拦在用户营销的大门之外，全面保障了广大汽车用户的切身利益和集团营销资金安全。

——某大型上市车企，轨道交通与新能源领导品牌

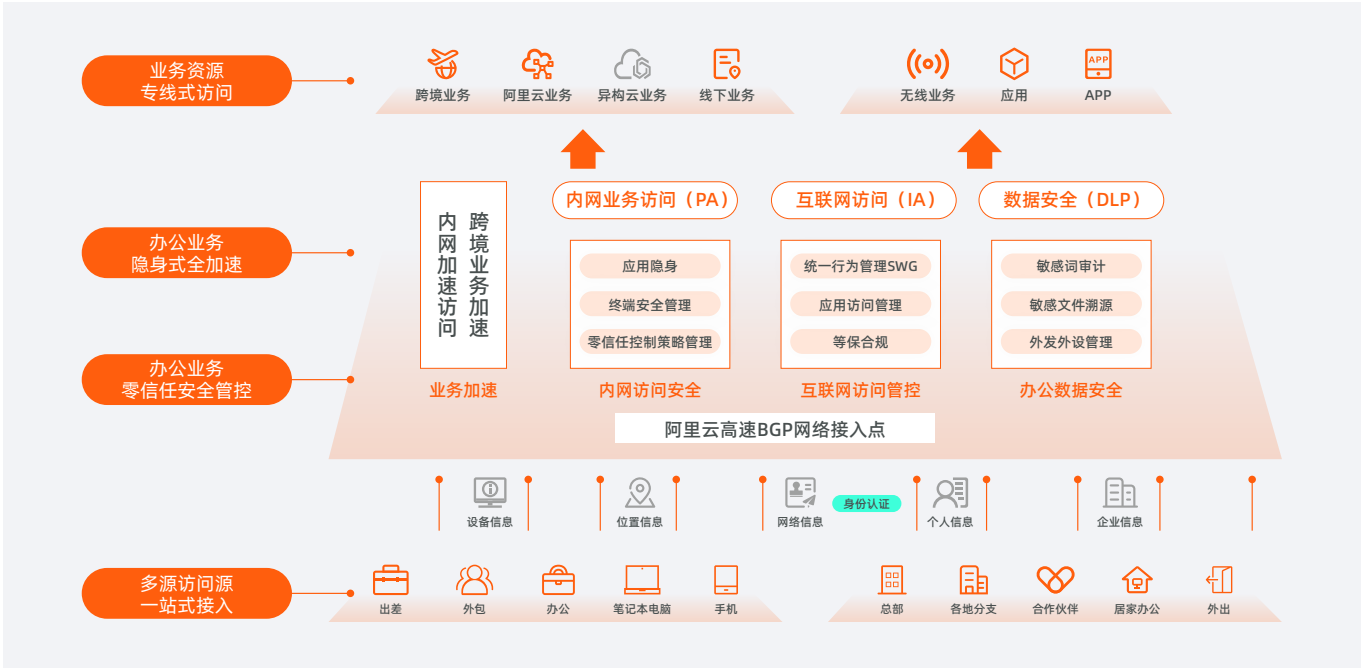


06 大型汽车集团办公安全方案

方案概述

伴随主机厂数字化转型的深入，远程办公、远程运维、多分支机构系统办公成为日常工作常态。零信任也在其中起到重要的安全作用，确保身份、行为的持续验证。

阿里云办公安全方案，提供一站式办公安全管控平台，企业无需再投资复杂且昂贵的安全硬件设备，即可快速构建零信任内网访问、办公数据防泄漏、上网行为管理与审计、办公访问加速等在内的办公安全体系。



服务模式

按照授权数进行按月、年购买服务。

适用客户群体

多分支机构集团型汽车企业、多云混合云部署的汽车企业、大量三方服务人员的汽车企业等。

方案优势&用户价值

为客户提供安全、可靠的远程办公环境，提升员工远程接入办公网的上网体验，边缘触达能力保证无论身在何处，都能享受内部网络的办公的顺畅和安全性。

01

最小访问权限&极致访问体验

兼容标准的SAML、SCIM身份协议，减少安全暴露面，提供端到端、端到应用的最小访问权限管控；内网访问加速，为分支和门店、远程移动办公访问内部服务提供极致的体验。