



以“一网三体系”构建天地一体智联出行生态，让世界充满吉利

汽车企业信息安全 挑战与应对策略

张开亿



2023年09月16日

目 录

CONTENTS

一、汽车产业新格局

二、信息安全的挑战

三、汽车企业信息安全面临的威胁

四、汽车企业信息安全应对的策略

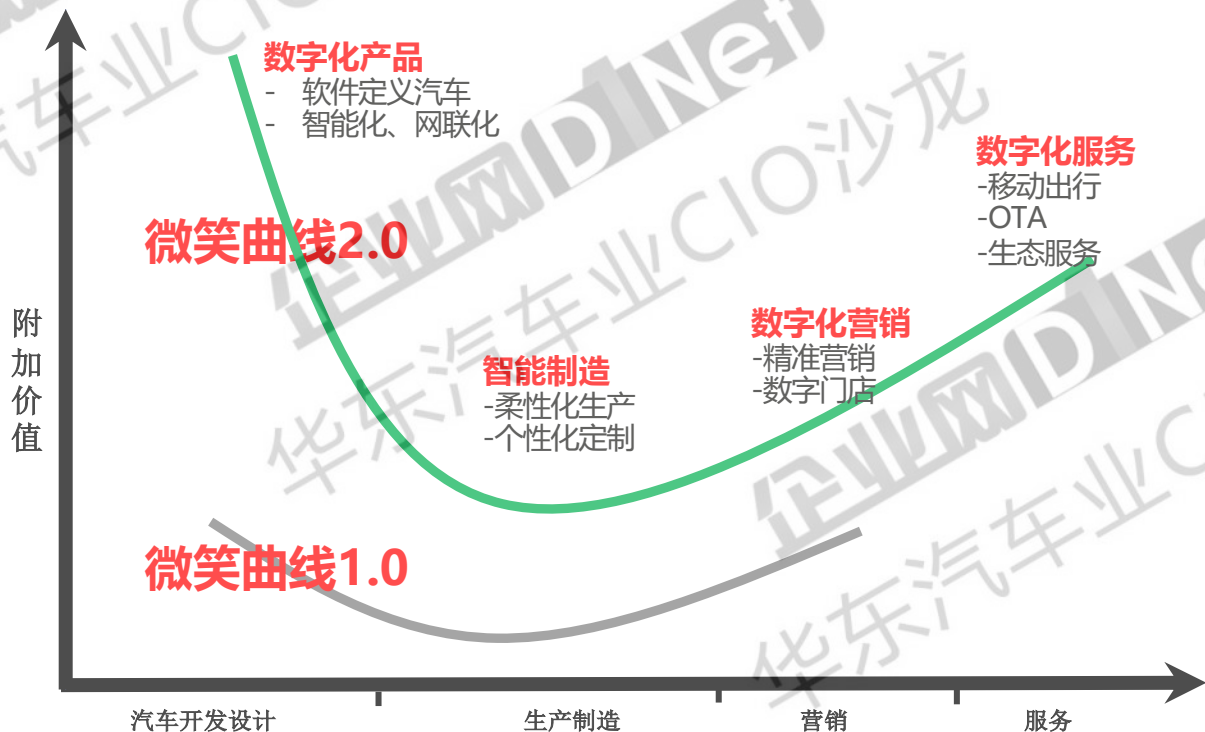
五、结束语

汽车产业新格局

- 汽车企业的新特征
- 汽车产品的智能化
- 汽车服务的全球化

汽车企业的新特征

数字化赋能价值链各环节，附加值在研发端得到大大提升并延伸到服务环节



汽车产品的智能化

未来，智能汽车、智能手机两个行业将不再各行其道，而是共同面向用户的多终端、全场景、沉浸式体验的一体融合关系。

车载应用

- VI新功能规划
- 新的交互模式
- 智能座舱体验

TSP服务

- 加油服务
- 道路救援
- 交通信息
- 停产服务

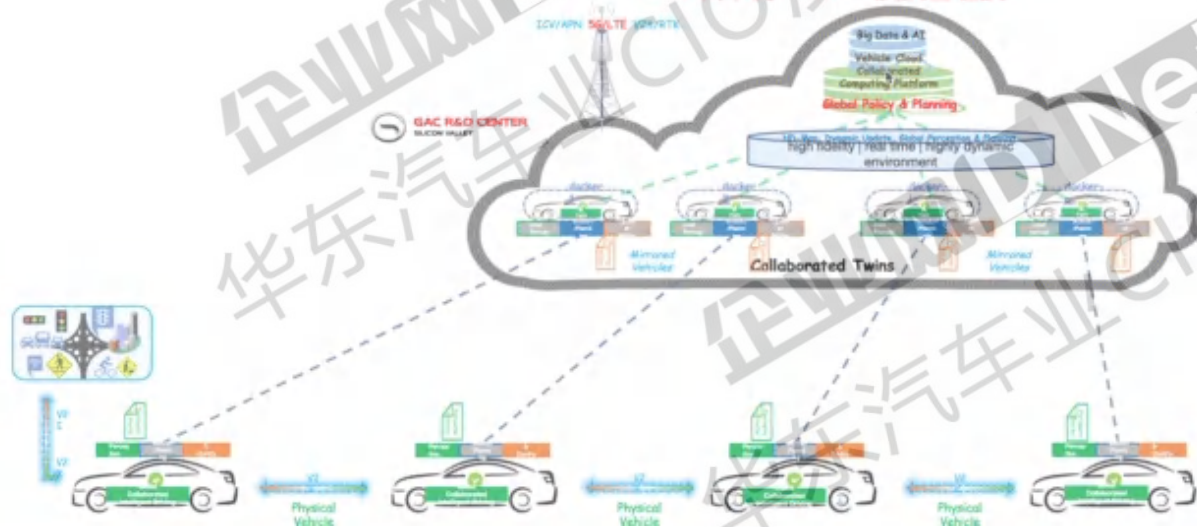
- 协同局部和全局规划
- 云车共享“OS”及安全切换

手机APP

- 新功能规划
- 新的交互模式
- 增值运营服务

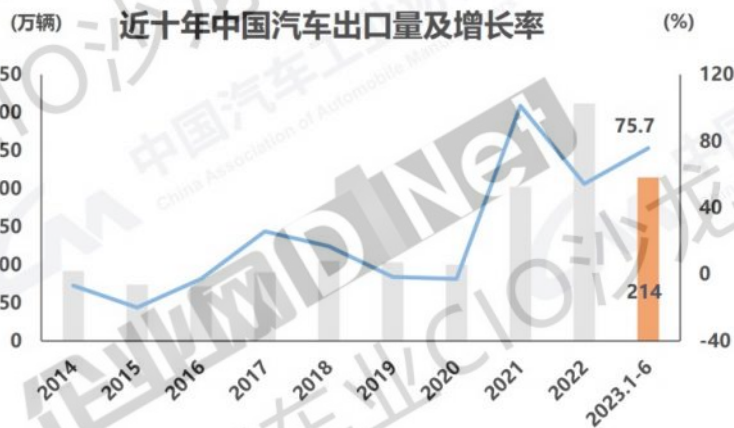
互联网生态

- 社交网络
- 移动支付
- 吃喝玩乐
- 服务预订



汽车服务的全球化

2023半年度国产汽车出口量首次超过日本，跃居全球第一



吉利集团产业布局和生态构建

以“一网三体系”构建天地一体智联出行生态，让世界充满吉利



沃飞长空



VOLOCOPTER

一网：智能科技生态网

- 以芯片、软件、数据、卫星网为核心，在智能架构、智能驾驶、智能座舱不断创新突破。
- 汽车操作系统、高精地图和导航、卫星通讯和定位等全栈自研。

三体系：智能能源体系、智能制造体系、智能服务体系

- 智能能源：智擎混动、纯电动、换电技术、甲醇科技
- 智能制造：工业互联网平台，黑灯工厂、数字化工厂
- 智能服务：100%用户直联，APP用户超1000万。



吉利、领克、极氪、银河、沃尔沃、路特斯、smart、伦敦电动汽车、宝腾、雷达、睿蓝....



汽车企业向数字化企业转型的过程中，安全复杂度陡增

无边界企业 – 消失的网络边界



解码无界，创造数字化转型的无限可能：中国银行业企业架构实施现状与未来

混合多态云

阿里云正式发布汽车云

行业服务	基础设施	应用层
<ul style="list-style-type: none"> 提供超A级性能10倍 在降本增效 最新7代芯片50% 最新上市车型40% 	<ul style="list-style-type: none"> 国产自主芯片 数字金融应用 智能金融风控 智能风控应用 	<ul style="list-style-type: none"> 业务管理 风险控制 核心运营 引擎运营
达摩院 平头哥 阿里云 钉钉 智能车联网 领克		

汽车金融云 地图云

数据作为新的生产要素



车联网安全建设迫在眉睫，但安全体系尚未成熟

安全组织不完善，安全管理不成熟

- 安全组织定位及职责分工
- 专业且稳定的安全团队
- 安全人才培养

安全开发过程实践经验还不成熟

- 整个行业处于经验积累中
- ISO21434明确安全流程，但是大部分安全团队缺乏实践经验



安全架构还不成熟

面对庞大生态系统、众多攻击面，整车安全架构的设计和部署还不成熟

安全技术还不成熟

- 受成本、性能影响，安全技术应用基于硬件进行辅助，较为轻量化
- 特定安全技术不成熟（AI、隐私保护）

国产汽车出海，面临更加严苛合规挑战

中美欧 - 数据安全重要立法与监管体系

国家/地区	立法名称	实施时间	监管机构	部门规章/规范性文件		立法名称	实施时间	监管机构
				实施时间	监管机构			
中国	网络安全法	2017	国家网信办	《个人信息安全规范》	2018	《网络安全法》	2017	国家网信办
	个人信息保护法	2021	国家网信办	《个人信息安全规范》	2018	《个人信息保护法》	2021	国家网信办
	数据安全法	2021	国家网信办	《个人信息安全规范》	2018	《数据安全法》	2021	国家网信办
	网络安全审查办法	2021	国家网信办	《个人信息安全规范》	2018	《网络安全审查办法》	2021	国家网信办
	车联网数据安全管理办法	2024	工信部	《个人信息安全规范》	2018	《车联网数据安全管理办法》	2024	工信部
美国	加州消费者隐私法案 (CCPA)	2018	加州信息隐私保护局 (CPIA)	《加州消费者隐私法案》	2018	《加州消费者隐私法案》	2018	加州信息隐私保护局 (CPIA)
	加州隐私权法案 (CPRA)	2023	加州信息隐私保护局 (CPIA)	《加州隐私权法案》	2023	《加州隐私权法案》	2023	加州信息隐私保护局 (CPIA)
	联邦信息隐私法案 (FOIA)	1974	美国联邦政府	《联邦信息隐私法案》	1974	《联邦信息隐私法案》	1974	美国联邦政府
	通用数据保护条例 (GDPR)	2018	欧盟委员会	《通用数据保护条例》	2018	《通用数据保护条例》	2018	欧盟委员会
	网络安全审查办法	2021	国家网信办	《网络安全审查办法》	2021	《网络安全审查办法》	2021	国家网信办
欧盟	通用数据保护条例 (GDPR)	2018	欧盟委员会	《通用数据保护条例》	2018	《通用数据保护条例》	2018	欧盟委员会
	网络安全审查办法	2021	国家网信办	《网络安全审查办法》	2021	《网络安全审查办法》	2021	国家网信办
	加州消费者隐私法案 (CCPA)	2018	加州信息隐私保护局 (CPIA)	《加州消费者隐私法案》	2018	《加州消费者隐私法案》	2018	加州信息隐私保护局 (CPIA)
	加州隐私权法案 (CPRA)	2023	加州信息隐私保护局 (CPIA)	《加州隐私权法案》	2023	《加州隐私权法案》	2023	加州信息隐私保护局 (CPIA)
	联邦信息隐私法案 (FOIA)	1974	美国联邦政府	《联邦信息隐私法案》	1974	《联邦信息隐私法案》	1974	美国联邦政府

图2 中美欧的数据安全重要立法及监管体系

汽车网络安全管理

2020年UN/WP.29发布**R155**。
 根据要求，从2022年7月起所有新车型必须满足该法规，才能在欧盟上市销售。
 2024年7月起**所有车辆**必须满足该法规要求方可出厂销售。

数据安全法规

2016年欧盟议会批准发布**GDPR**（通用数据保护条例）
 违反GDPR的行为，可处**2000万欧元**行政罚款或集团全球前一年**营业额4%**（最高）。

三、汽车企业信息安全面临的威胁

汽车企业在产品、运营、服务、生态、社会环境都面临多方面的信息安全威胁

汽车行业多方面的信息安全威胁：

- 数据泄漏和勒索
- 网络攻击
- 产品设计安全
- 国内外监管



三、汽车企业信息安全面临的威胁

汽车企业信息安全案例



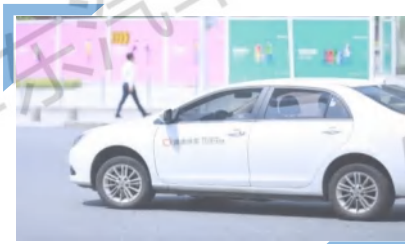
法拉利遭受黑客入侵，
客户资料被盗取



特斯拉汽车在2023黑客挑战赛被破解，可远程操控



因**供应商遭网络攻击**，丰田汽车14家工厂停产



头部出行服务公司海外上市被**网络安全审查并处罚**

应用名称 ¹	应用开发者 ²	应用来源 ³	应用版本 ⁴	所涉问题 ⁵
出行		百度手机助手 ⁶	5.1.1 ⁷	APP 强制、频繁、过度索取权限 ⁸
	深圳比亚迪车云信息技术有限公司 ⁹	百度手机助手 ⁶	5.1.7 ⁷	违规收集个人信息 ⁸ 违规使用个人信息 ⁸ APP 强制、频繁、过度索取权限 ⁸
		App Store ¹⁰	5.1.7 ⁷	APP 强制、频繁、过度索取权限 ⁸

车企APP收到公开通报批评
涉及**个人信息数据违规收集**

汽车企业信息安全关注点



「定战略」

信息安全目标

安全人才需求

安全技术路线

组织架构设计

安全技术方案

安全产品路线

「定组织」



「定框架」



一些感悟

- 哪些自研/哪些商用
- 哪些先买后造
- 安全从独立的工具建设到与业务场景的集成建设

以零信任构建企业网络安全防护 – 办公空间安全

端

全链路的信息透明

一体化的安全终端

网

全链路的信息透明

一张SASE的零信任网络

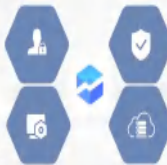
安全
一致

一致的办公安全空间

1. 统一的终端威胁全面防护 (XDR)

All In One 一站式解决办公终端的安全威胁

- 无侵入式安装部署，静默运行
- 终端-网络全链路安全防护
- 总部分支统一安全策略



2. 立体的数据保护 (DLP)

为企业构建全球数据安全与治理体系

- 数据知识识别与分类审计
- 通道 (网盘、邮箱、FTP、IM、代码仓) 检测和外发拦截
- USB、AirDrop、外发第一道门
- 敏感文件数字水印、数据脱敏本地扫描

3. 零信任安全访问

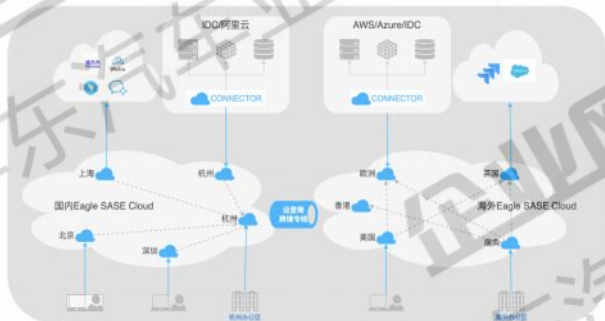
让员工享受高效、安全、稳定的办公体验

- 全场景覆盖移动办公访问
- 最小化数据权限防止横向移动
- 内网行为与流量实时监控

4. IT运营管理

全面统一管理IT资产

- 支持全属性设备类型全面管控
- 70+ 主流品牌硬件终端环境
- 支持软件自动化运维和软件一键推送、静默安装



零信任内网访问

随时随地远程办公

混合办公互联网防护

安全水位一致，统一策略

一体化办公数据安全

数据流转下的数据防泄漏

安全工程实践分享

零信任访问、漏洞修复、病毒查杀

The dashboard displays several key components:

- 企业内网 (Intranet):** A top navigation bar with a '连接中心' (Connection Center) button.
- 连接中心 (Connection Center):** A large blue circular button with a lock icon and the text '连接中心'.
- 仪表盘 (Dashboard):** A section with various charts and data points, including a circular gauge showing '20%' and a line graph.
- 系统日志 (System Logs):** A table listing system events with columns for time, user, and details.

数据防泄漏 - “重检测，轻防护”

The report details a data leakage event:

- 风险等级 (Risk Level):** 低 (Low)
- 综合风险 (Overall Risk):** 低
- 检测建议 (Detection Suggestion):** 本检测系统检测到... (This detection system detected...)

上报时间	事件名称	所属用户	分析线索	状态	审计	操作
2022-10-18 16:09:44	发送...	信利	使用钉钉沟通, 共外发1个敏感文件, 其中: 54 1个	未解除风险		解除风险

发送加密文件

- 使用终端: [redacted] X86
- 外发文件: 54
- 文件类型: 办公文档 1个
- 敏感数据: 办公文档 加密文件 1个
- 文件大小: 38.5 KB
- 发送通道: 钉钉
- 发送时间: 16:09:23-16:09:35

操作时间

- 操作时间: 2022-10-18 16:09:25
- 上传时间: 2022-10-18 16:09:35

使用通道

- 具体通道: 钉钉

附件操作

- 附件名称: 办公文档、办公文档 1个
- 附件大小: 38.5 KB
- 附件类型: 办公文档
- 附件路径: [redacted]
- MD5 Hash: 2f2570e8150d75e3031... 1651c2
- 创建时间: 2022-10-14 19:44:52
- 最后修改时间: 2022-10-18 16:09:02

截屏

离职员工
自动
风险
报告

构建一致安全的企业混合多云 - 云空间安全

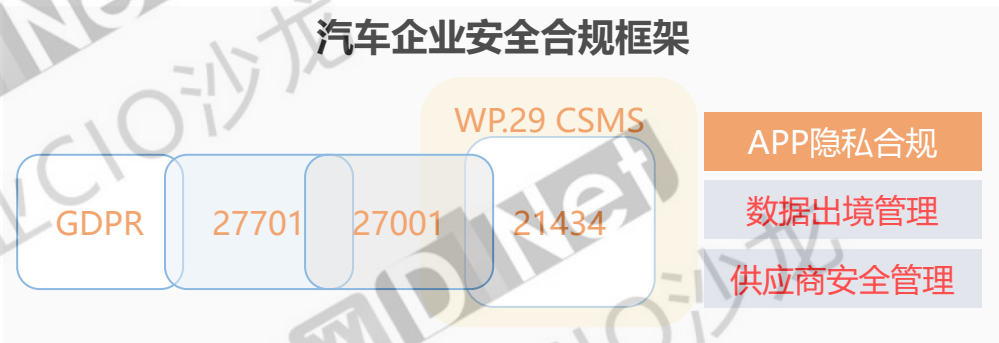
汽车行业多云安全建议：

- 云上安全是基本防护，行业提供通用的解决方案
- **云中安全需引起关注**（云账号/密钥泄漏、存储桶暴露、云服务配置错误等）
- DevOps和云安全融合是关键提升点（制品安全、代码安全等）



四、汽车企业信息安全应对的策略

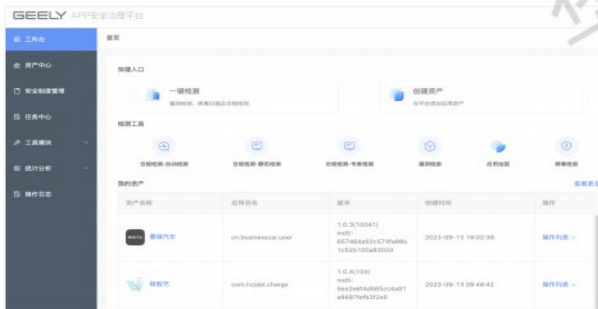
汽车企业安全合规框架



工程实践分享

APP安全治理平台：隐私合规检测、应用漏洞扫描、病毒检测、应用加固

首页



概览信息



隐私设计



跨境通信



汽车企业信息安全建设从“事件导向型”向“成熟型”发展

管控型企业		成熟型企业	
流程导向		风险导向	
<ul style="list-style-type: none"> • 强调IT 的安全管理 • 每年信息安全经费预算介于整个IT预算的1%和10%之间 • 信息资产分类 • 正式的安全组织 • 完善的安全策略、标准和流程 • 部署了基本的安全工具 		<ul style="list-style-type: none"> • 强调IT 的安全管理和安全技术的平衡 • 每年安全经费预算基于风险评估结果 • 集成且统一的安全体系管理架构、技术架构 • 基于国际标准的完善的安全策略、标准和流程 • 部署了必要的安全工具 • 应急响应机制完善且定期演练 • 预防为主、防治结合 	
事件导向		技术导向	
<ul style="list-style-type: none"> • 事件、故障发生以后再采取相应补救措施 • 不注重IT 的安全管理 • 无计划中的信息安全预算 • 使用基本的用户名密码管理 • 部署了基本的安全工具 		<ul style="list-style-type: none"> • 强调并依赖IT 的安全技术 • 部署了各种领先的安全工具 • 每年安全经费预算 > 10% • 没有正式的安全组织，安全策略、标准和流程 • 员工安全意识普遍薄弱 	
被动型企业		技术型企业	

安全流程

安全技术

汽车企业信息安全挑战与应对策略

- ★ 汽车产业正在向“微笑曲线2.0”新特征发展；
- ★ 汽车产品正在向智能化网联化共享化方向发展；
- ★ 中国汽车质量提升，出口增势明显；
- ★ 以上因素给汽车企业信息安全带来巨大挑战；
- ★ 数据、网络、隐私将成为汽车企业信息安全关注的重点；
- ★ 汽车企业信息安全应从目前的“事件导向型”向“成熟型”方向发展。



恭喜
《汽车企业数字化转型 认知与实现》
上市两周
荣登京东新书榜第1位

NO.1
《汽车企业数字化转型 认知与实现》
上市两周
荣登当当新书榜第1位

当当网 dangdang.com

汽车企业追求的
数字化转型方法论

6个颠覆性洞见
汽车企业数字化转型

JD.COM

新书榜第1位！
机械工业出版社

dangdang.com



19th Asian Games
Hangzhou 2022



吉利汽车
GEELY AUTO

杭州2022年亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

快乐人生，吉利相伴