青莲云
qinglianyun.com

青莲云

公司及物联网安全解决方案介绍

青莲云
qinglianyun.com

公司介绍

公司介绍

- 青莲云是**业界领先的物联网安全解决方案提供商**，成立于**2016**年，专注于物联网安全研究、物联网安全产品及云平台
- 公司总部位于**北京中关村**，在**广州**设有全资子公司，在**深圳**设有华南区办事处
- 成立以来获国内顶级投资机构千万级投资，也是**ARM**中国加速器第一期重点企业
- 核心技术团队来自**奇虎360**，具有**10**年以上企业级安全产品和物联网云平台研发及服务经验
- 围绕物联网业务安全，打造**2**大核心业务板块：**物联网安全私有云平台和物联网安全运营中心**
- 服务过**数百家**国内外企业客户，包括**中国电信、国家电网、中软集团、融创集团、拓邦股份**等
- 联合中国信息通信研究院发布国内首份**《2017中国智能硬件安全白皮书》**
- 拥有工信部颁发的**“智能硬件（IoT）开放平台一致性可信认证”**资质证书
- 入选IDC年度行业报告**《IDC创新者：中国物联网安全，2017》**
- 荣获中国物联网产业应用联盟：**《中国最有影响力物联网安全企业奖》**
- 入选安全牛：**中国网络安全《最具发展潜力初创企业20强》**
- 入选《互联网周刊》&eNet研究院：**《2018物联网企业100强榜单》**
- 入选Gartner评选的**《2019 Gartner Cool Vendors》**

Gartner Cool Vendor唯一物联网安全厂商

- 2019年青莲云成功入选Gartner数字业务创新**Cool Vendor**厂商，为该领域唯一一家物联网安全企业。
- 同年，青莲云再次入选**Gartner China Cybersecurity**代表厂商，同期入选的包括华为、360、深信服等安全行业领军者。
- 青莲云端到端物联网安全整体解决方案覆盖物联网设备终端系统安全、可信计算安全、通信链路安全、身份认证安全、自动化安全检测、安全威胁情报以及安全态势感知等维度。通过私有化部署的方式，可以为企业建立专属的物联网安全大脑，实现物联网安全防护和安全运营的闭环统一。

荣誉资质

- 2017中国最具影响力物联网安全企业奖
- 2018物联网企业100强
- 中国网络安全最具发展潜力初创企业20强
- IOTE2018“金奖”创新产品奖
- 2018年度智能终端“墨提斯奖”
- 2018第五届中国IoT大会技术创新奖
- 中国网络安全全景图酷厂商
- CSA云安全联盟物联网安全工作组专家单位
- 2018中国最具影响力物联网安全企业奖
- AWE2019艾普兰智能创新奖
- 2019 Gartner Cool Vendors
- 微软IP Co-Sell Ready Partner企业认证
- 2019年度工业互联网优秀解决方案奖
- 广东省工业互联网产业生态供给资源池
- IOTE2019“金奖”创新产品奖
- 中国网络安全100强（2019）
- 2016中国IoT产业新锐CEO奖
- 2017年度物联网技术创新奖
- AWE2017艾普兰奖 智能创新奖
- 2017年度智能终端“墨提斯奖”
- IDC创新者：中国物联网安全，2017
- 中关村国际前沿技术创新大赛智慧城市与物联网TOP10
- 中国智能家居产业联盟理事单位
- 中国云安全与新兴技术安全创新联盟专家委员会研究贡献奖
- 广州市黄埔区广州开发区 2019 年创业英才
- 董方荣获广东省物联网协会专家委员会专家

自主知识产权

- 青莲智能硬件控制端软件V1.0
- 青莲智能硬件控制端软件(IOS版)V1.0.0
- 青莲智家硬件控制端软件V1.0.0
- 青莲智家硬件控制端软件（安卓）V1.0
- 青莲云故事机解决方案内容运营平台V1.0
- 青莲物联网云平台软件V1.0
- 青莲云物联网平台安全态势感知系统V1.0
- 青莲云物联网安全接入网关系统V1.0
- 青莲云物联网设备安全管理系统V1.0
- 青莲云物联网SDK软件（Android版）
- 青莲云物联网管理运维平台
- 青莲云物联网安全接入网关运维平台
- 青莲云设备安全管理运维平台
- 青莲云物联网私有云管理运维平台
- 青莲云物联网设备安全Agent软件
- 青莲云安全网关嵌入式SDK软件
- 青莲云模组调试助手软件
- 青莲云物联网嵌入式硬件SDK软件

- 一种可扩展的应用分发系统
- 一种用于智能设备的安全联网动态认证方法
- 一种基于HTTP API的智能硬件联动方法
- 一种基于云端规则的智能硬件联动方法
- 一种基于状态机的OTA固件升级方法
- 一种基于OTA组件的热补丁智能升级方法及系统
- 物联网终端安全会话的管理方法、网关和系统
- 一种基于安全芯片的物联网终端安全认证方法
- 一种用于物联网智能终端的基线安全检测方法及装置
- 一种基于块内存的内存总量动态控制方法及系统
- 基于物联网的数据驱动场景的方法和装置
- 一种基于蓝牙设备端的OTA固件升级方法及系统
- 用于OTA升级的服务端及嵌入式设备升级方法及装置
- 用于物联网设备的本地蓝牙动态认证方法和系统

企业资质

- 中国高新技术企业
- 中关村高新技术企业
- 工信部IoT云平台可信认证资质
- ISO/IEC 27001 信息安全管理体系认证
- ISO/IEC 27017 云信息安全管理体系认证
- ISO/IEC 27018 云隐私保护体系认证
- ISO9001质量管理体系认证

业务模式

软件定义物联网业务安全

基于云+安全的产品模式，通过私有化部署，实现企业物联网安全赋能

竞争优势

国内唯一的物联网安全端到端整体解决方案，安全自主可控

物联网云平台及安全领域：21项软件著作权，15项技术发明专利


产品研发


云安全


系统安全


嵌入式安全


移动安全


通信安全


业务安全


攻防对抗

行业分析

电力物联网发展现状介绍

2019年1月17日,国家电网公司三届四次职代会暨2019年工作会议提出,聚焦建设世界一流能源互联网企业,守正创新、担当作为,打造“枢纽型、平台型、共享型”企业,建设运营好“坚强智能电网、泛在电力物联网”,即为“三型两网”发展战略。

建设“三型两网，世界一流“能源互联网企业的战略目标,是主动适应能源革命和数字革命融合发展的必由之路,也是主动适应电力改革和国企改革纵深推进的根本要求。建设运营好“两网”一坚强智能电网、泛在电力物联网是建设世界一流能源互联网企业的重要物质基础。

电力物联网整体建设框架

泛在电力物联网建设在对内业务、对外业务、数据共享、基础支撑、安全防护和技术攻关6大领域的11个方向具有重大意义。

提高**技术公关**能力与核心产品竞争力

对内业务

- 提升客户服务水平
- 提升企业经营绩效
- 提升电网安全经济运行水平
- 促进清洁能源消纳

对外业务

- 打造智慧能源综合服务平台
- 培育发展新型业务
- 构建能源生态体系

打造**数据共享**服务

夯实**基础支撑**能力

构建全场景的**安全防护**体系

电力物联网安全建设框架

构建与“三型两网”企业相适应的全场景网络安全体系，推广“安全+业务”的防护理念，从物防、事防、人防三防切入，开展可信互联、安全互动、智能防御相关技术的研究及应用，针对物联网特性提出12个体系化的重点防护方向，结合全生命周期的安全服务，保障物联网内数据从采集、传输、整合到应用的全过程安全。

防护思路	
应用层 数据的应用安全	数据安全基础上，重点实现应用的智能防御和快速处理。
平台层 数据的整合安全	云安全基础上，重点实现物联网态势感知和安全互动。
网络层 数据的传输安全	流量监测基础上重点实现公网、内网融合的隔离防护。
感知层 数据的采集安全	物—物互信的基础上，重点实现终端行为监控。

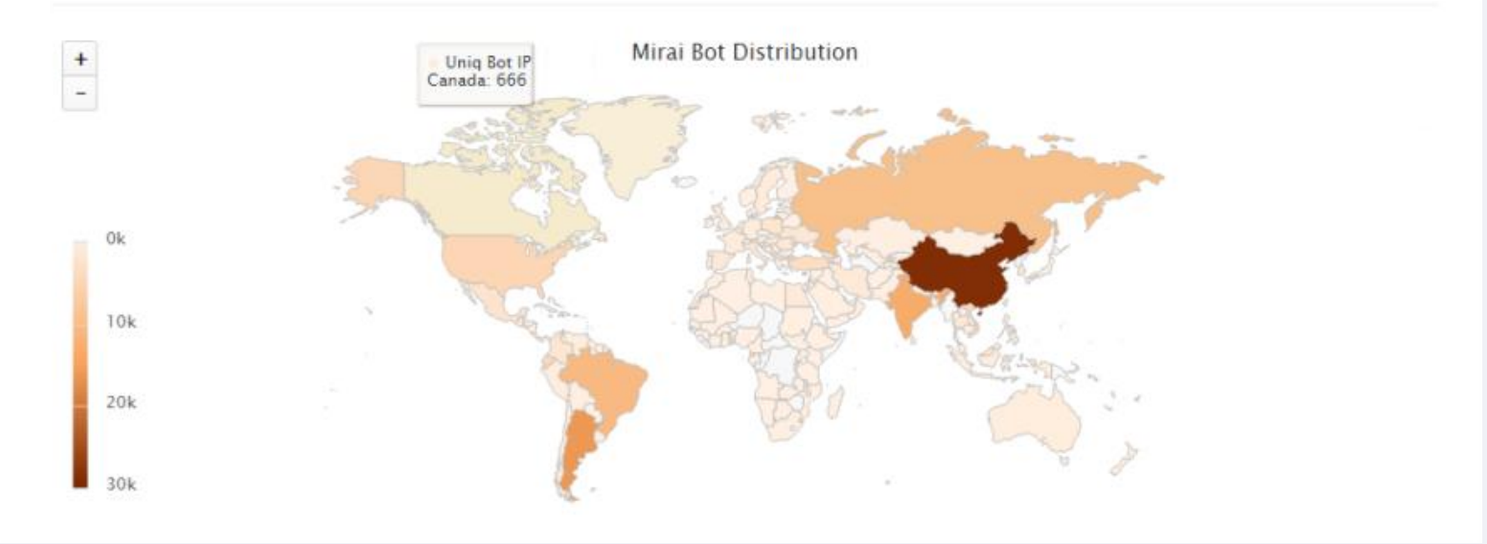
重点防护方向

数据安全		智能防御
安全态势感知		应急指挥预警
身份认证		工控专用情报库、漏洞库、病毒库
云平台安全		
全流量监测	内外网融合防护	无线安全防护
物—物互信 （设备的加固、认证、加密、可信度量）		终端行为监测

全生命周期安全服务

视频安防领域物联网安全事件分析

2016年10月21日美国东海岸地区大规模DDoS网络攻击事件，攻击目标主要是Dynamic Network Services（dyn）公司。发起期此次攻击的Mirai僵尸网络当时规模已经有70W+，主要感染的都是中国境内IoT设备（摄像头为主），事件发生26天后，美国国土安全部发布《物联网安全指导原则》。



视频安防领域物联网安全事件分析

2020年2月，青莲云IOTVD平台安全监测系统发现，有境外黑客组织发文宣称将于2020年2月13日对我国境内视频监控系统实施网络攻击活动。该黑客组织声称已掌握我境内大量摄像头控制权限，并在Pastebin网站上公布了73个网络视频监控系统管理后台信息（部分已失效，但不排除有更多未公布的攻击目标），相关攻击信息推文如下：

关于近期境外黑客组织拟对我国视频监控系统发起攻击的预警通报

原创 CNCERT 国家互联网应急中心CNCERT

前天

近期，境外黑客组织声称将于2月中旬对我国发起网络攻击，以我国多家视频监控系统作为攻击目标，并公布了其掌握的一批相关视频监控系统在用境内IP地址。经分析，我国视频监控系统存在一定的漏洞安全隐患和数据泄露风险，可能成为境外黑客发起攻击的薄弱环节。

智慧城市物联网建设现状

- **建设概况**

基于底层高精度地图和海量物联设备，通过深度融合物联网、云计算、大数据、人工智能等新技术，建设以城市数据中台为核心，以“万物互联、广泛连接、存算一体、数据安全”四大体系为支撑的智慧产业园。项目建设内容包括城市数据中台、智慧交通、智慧市政、智慧园区和数据安全防护等。

- **建设内容**

初步建成打造“411”新型数字产业园基础设施建设体系，支撑政府现代化治理能力大幅提升、民生服务更加高效、产业转型深入推进，助力将经开区打造成为全国一流的新型数字基础设施建设示范区。

“4”指“4 大支撑体系”即“万物感知、广泛连接、存算一体、数字安全”的新型数字产业园基础设施建设（一期）支撑体系，第一个“1”指“1 平台”即平台服务，第二个“1”指“1 中心”即数字经开区展示体验中心。

智慧城市物联网设备分析

数字孪生城市场景设备走查

- 智慧社区
  - 警戒摄像机
  - 智慧门禁
  - 电梯卫士
  - 数字管理机
  - 智能消防
  - 4G路由器
- 智慧园区
  - 监控摄像机
  - 水位监测仪
  - 物联网网关
  - 消防监控主机
  - 4G网关
  - 液位计
- 社会生态
  - 摄像机
  - 环保数采仪
  - DTU
  - 边缘网关
  - 数据遥传设备
- 智慧市政
  - 消防控制主机
  - 监控摄像机
  - 人脸抓拍
  - 智慧路灯控制仪
  - LORA网关
- 智慧交通
  - 道口边缘网关
  - 车载终端
  - 信号控制器
  - 数据采集仪
  - 智能公交站主机

根据对各项目的调研，目前数字孪生建设各场景中应用的物联网设备情况如下

1. 类型：近百种
2. 数量：两万左右
3. 厂商：数十家

需接入物联网防护的设备呈现出以下特点：

- **弱边界**
- **碎片化**
- **应用复杂**
- **安全能力不齐**
- **缺乏统一管理**

智慧城市安全风险分析

智慧城市中，物联网设备负责数据采集、指令执行、业务监控，其正常运行对智慧社区业务监管和调控至关重要，物联网遭受网络攻击，将不仅造成信息安全事故，更将直接导致业务受损甚至治安事故。

伪造设备接入

- 通过伪造大量设备接入平台，耗尽平台资源，导致业务终端
- 伪造设备接入平台，获取平台控制指令，破解进一步非法控制其它设备

系统病毒感染

- DTU、消防主机等感染物联网僵尸病毒形成僵尸网络，向业务平台或其它网络实体发起DDoS攻击
- 路灯控制模组等设备感染病毒，导致正常业务运行性能不足，设备失控，攻击者可发起批量攻击造成治安事故

数据通信劫持

- 社区管道水压中敏感数据传输被篡改，导致监控数据无效
- 通过嗅探抓取DTU设备控制指令，实现批量化非法设备控制与劫持
- 通过录制设备控制指令，以重放方式破坏设备正常运行

设备非法入侵

- 入侵人脸门禁等设备中，篡改配置文件导致设备无法正常运行
- 消防主机等设备中业务程序文件被破坏，导致设备失灵，无法实现火灾监控与灭火功能

物联网安全国家标准和建设指南

参照多个“新基建”安全建设标准及要求，遵循网络安全等级保护基本要求（等保2.0）、关键信息基础设施网络安全保护基本要求等标准相关进行整体防护体系设计。

GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南
GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南
GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求
GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求
GB/T 37971-2019	信息安全技术 智慧城市安全体系框架
GB/T 36621-2018	智慧城市 信息技术运营指南
GB/T 37971-2019	信息安全技术 智慧城市安全体系框架
GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求
GB/T 37093-2018	信息安全技术 物联网感知层接入通信网的安全要求
GB/T 37025-2018	信息安全技术 物联网数据传输安全技术要求
GB/T 37024-2018	信息安全技术 物联网感知层平台安全技术要求
GB/T 36951-2018	信息安全技术 物联网感知终端应用安全技术要求
GB/T 35317-2017	公安物联网系统信息安全等级保护要求
GB/T 35318-2017	公安物联网感知终端安全防护技术要求

等保2.0物联网安全扩展要求

安全物理环境

物理位置选择	物理访问控制	防盗窃和防破坏	防雷击
防火	防水和防潮	防静电	温湿度控制
电力供应	电磁防护	感知节点设备设备物理防护	

安全通信网络

网络架构	通信传输	可信验证

安全区域边界

边界防护	访问控制	入侵防范	可信验证
恶意代码和垃圾邮件防范	安全审计	拨号使用控制	接入控制

安全计算环境

身份鉴别	访问控制	安全审计	入侵防范
恶意代码防范	可信验证	数据完整性	数据保密性
数据备份恢复	剩余信息保护	个人信息保护	抗数据重放
感知节点设备安全	网关节点设备安全	数据融合处理	

安全管理中心

系统管理	审计管理	安全管理	集中管控

安全管理制度

安全策略	管理制度	制定和发布	评审和修订

安全管理机构

岗位设置	人员配备	授权和审批	沟通和合作	审查和检查

安全管理人员

人员录用	人员离岗	安全意识教育和培训	外部人员访问管理

安全建设管理

定级和备案	安全方案设计	产品采购和使用	自行软件开发
外包软件开发	工程实施	测试验收	系统交付
等级测评	服务供应商选择	产品采购和使用	

安全运维管理

环境管理	资产管理	介质管理	设备维护管理
漏洞和风险管理	网络和系统安全管理		恶意代码防范管理
配置管理	密码管理	备份与恢复管理	变更管理
安全事件处置	应急预案管理	外包运维管理	感知节点管理

通用要求　通用要求+扩展要求　扩展要求

物联网安全和传统网络安全区别

传输协议不同

传输协议 4G、NB-IoT、5G CoAP、LoRA、485..

物联网设备通讯协议更复杂多变，且经常出现双信道或多信道传输，传统网络安全边界防护难以覆盖

系统架构不同

操作系统 RTOS、Linux、FreeBSD OpenWRT..

硬件架构 ARM、MIPS、ST200 Nios-32、X86.....

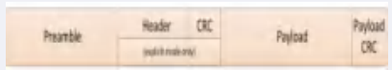
通信模组 高通、移远、乐鑫 恩智浦、新唐.....

物联网设备硬件架构碎片化严重，计算资源有限，传统EDR难以满足防护需求

应用协议不同

HTTP协议

私有协议



物联网应用协议缺乏统一标准，多为厂商自定义私有协议，难以通过协议解析直接提取攻击样本

设备部署分散

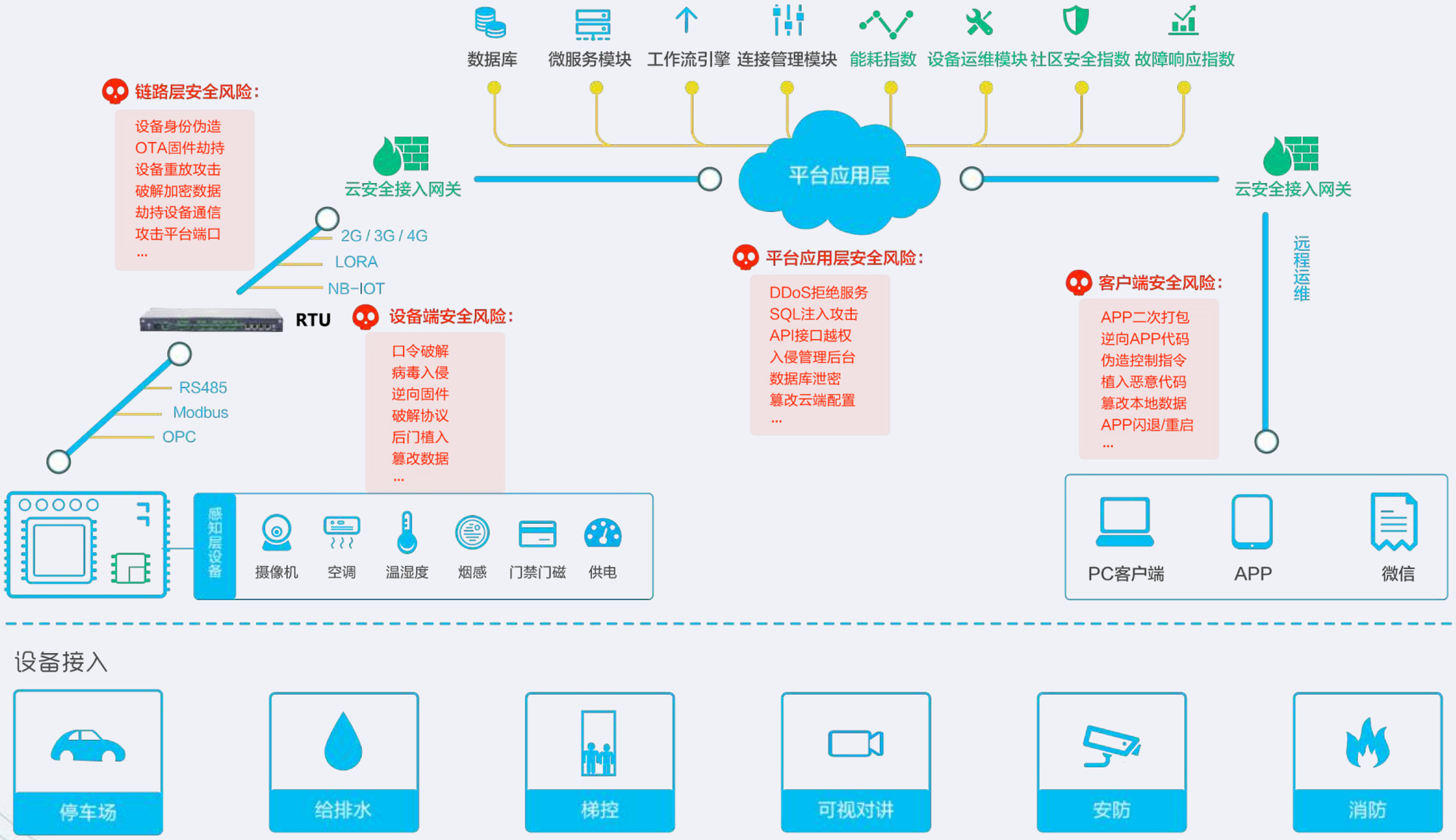
智能门禁系统

安防系统

充电桩管理系统

物联网设备部署于企业IT资产网络之外，物理位置分散难以通过网络边界防护设备统一接入

物联网端到端应用架构及安全风险识别



设备接入

解决方案

青莲云
qinglianyun.com

业务方向：物联网（业务）安全

产品理念：围绕安全开发生命周期（SDL）提供全链路安全产品和服务

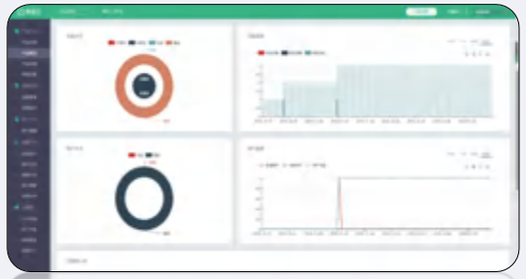
物联网云平台	物联网安全接入网关	物联网设备安全管理	物联网设备可信执行环境	物联网安全检测	物联网威胁情报库
• 全品类通信模组支持 • 实时消息 • 安全OTA • 私有化部署 • ……	• 三重身份验证 • 动态设备密钥 • 一机一密 • 通信隔离 • ……	• 安全基线检测 • 流量分析 • 异常行为分析 • 实时告警 • ……	• 数据加密 • 安全启动 • 签名验签 • 安全引导 • ……	• CVE漏洞检测 • CWE漏洞检测 • 软件漏洞检测 • 敏感信息检测 • ……	• 漏洞列表 • 漏洞补丁 • 事件分析 • 漏洞扫描 • ……
解决痛点	解决痛点	解决痛点	解决痛点	解决痛点	解决痛点
安全研发和架构设计	链路安全和身份管理	行为监控和基线管理	安全引导、安全存储	动/静态双引擎自动化扫描	最全面的物联安全漏洞库

安全培训+安全测试（体检）

使用产品和服务（治病）

物联网安全云平台

青莲云拥有自主创新的物联网安全整体解决方案，支持独立部署(青莲云物联网安全套件+企业自有物联网云平台)和集成部署(青莲云物联网安全套件+青莲云物联网云平台)两种方式，同时拥有多项物联网安全相关技术发明专利，企业客户可以根据自身需求灵活选择合作方式，青莲云会提供一对一的专业技术支持。



资质&认证

- 青莲智能硬件控制端软件V1.0
- 青莲智能硬件控制端软件(IOS版)V1.0.0
- 青莲智家硬件控制端软件V1.0.0
- 青莲智家硬件控制端软件（安卓）V1.0
- 青莲物联网云平台软件V1.0
- 青莲云物联网SDK软件（Android版）
- 青莲云物联网私有云管理运维平台
- 青莲云模组调试助手软件
- 青莲云物联网嵌入式硬件SDK软件
- 工信部IoT云平台可信认证资质
- ……

产品架构

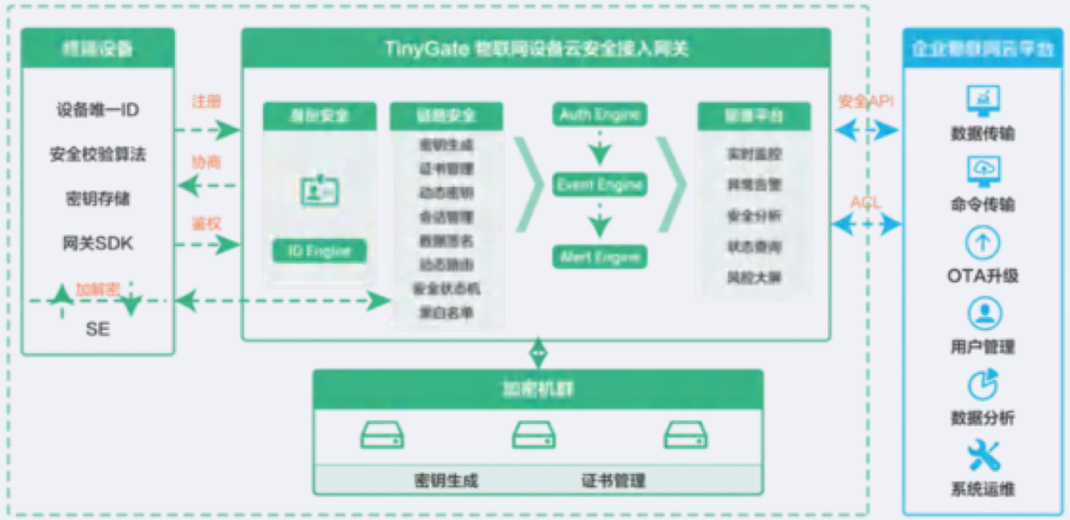
客户案例

中软 CS&S 中国软件　Midea　TCL 创意感动生活 The Creative Life　qinglia　长征电气

物联网云安全网关（TinyGate）

本系统提供出色智能的设备安全入网能力,覆盖设备授权、身份鉴权、密钥管理、加密传输、会话管理、数据签名等多种功能,保护物联网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击,并通过安全API和RPC系统调用与企业后端业务平台无缝集成,保障整个通信链路的安全和数据完整性。

产品架构



资质&认证

- 青莲云安全网关嵌入式SDK软件
- 青莲云物联网安全接入网关系统V1.0

产品优势

强身份鉴权

- 双向可信验证
- 动态安全协商因子
- 三重验证逻辑

传输安全

- QingLink私有协议
- AES加密
- TLS/SSL加密
- 数据包签名

会话安全

- 一机一密
- 一连一密
- 动态密钥
- 有效期管理

管理安全

- 安全状态监控
- 安全数据分析
- 设备行为分析
- 异常实时告警

客户案例

青莲云 qinglianyun.com 物联网云安全网关--硬件兼容，支持主流物联网通信模组

NO.	网络类型	芯片品牌	型号	操作系统	NO.	网络类型	芯片品牌	型号	操作系统
1	WIFI	乐鑫	ESP8266EX	NONOS	15	GSM/GPRS	移远	M26	Nucleus
			ESP8266EX	NONOS	16		移柯	L206	Nucleus
			ESP8266EX	FreeRTOS	17		移柯	L218	Nucleus
2			ESP32	FreeRTOS	18	NB-IOT	华为	BC95	
3		德州仪器	CC3200	FreeRTOS	19		华为	LSD4NBN-LB05000001	
4		庆科	EMW3165	MICO	20		锐迪科	BC60	
			EMW3031		21	NB-IOT GSM/GPRS	高通	ME3612	
			EMW1062		22		高通	SIM7000C	
			EMW3080B		23	WIFI GPRS LTE	ARM/MTK/高通……		Android
5		高通	QCA4004	ThreadX	24	SE	华大	CIU98320B	
6		联盛德微电子	W500	FreeRTOS	25		万协通	WI32U320	
7		汉枫	LPB120	CONTIKI	26		宏思	HSC08K1	
			LPB125	CONTIKI	27	蓝牙MESH	乐鑫	ESP33	FreeRTOS
			LPB200U	Mbed	28	TrustZone	新唐	M2351	FreeRTOS
			LPT230	FreeRTOS	29		NXP	LPC55S69	FreeRTOS
8		REALTEK	8711AM	FreeRTOS	30	有线	英特尔	X86	Linux C
9		锐迪科	RDA5981	Mbed					Linux java
10		全志	XR871	FreeRTOS				X64	Windows C#
11		MTK	MT7628	OpenWRT					Windows java
12		博通	BK7231	RT-Thread	31		三星	ARMA9	Linux
			BK7231u	RT-Thread	32		博通	ARMA8	Raspbian
13		锐迪科	BC30	Mbed	33		瑞萨	RenesasS7	ThreadX
14	蓝牙	乐鑫	ESP32	FreeRTOS	34		NXP	NXPLPC1778	UCOS

物联网云安全网关（TinyGate）

本平台针对设备通信安全提供出色智能的设备安全入网能力，覆盖设备授权、身份鉴权、密钥管理、加密传输、会话管理、数据签名等多种能力，保护物联网设备及数据免受重放攻击、伪造攻击、数据篡改、会话劫持等网络攻击，保障整个通信链路的安全和数据完整性。

身份管理认证

平台统一管理下发身份凭证，双向强可信身份、四重逻辑身份验证确保终端设备身份安全

安全会话管理

终端设备通信采用安全会话机制，会话具备安全有效期

密钥管理分发

加密密钥由平台统一管理下发，一机一密、一连一密、动态密钥机制确保密钥安全性

多种加密算法

支持AES/SSL/TLS等常见商密算法

支持SM4国密算法

安全OTA升级

终端设备统一安全升级管理，内置OTA状态机保证升级100%成功

重放攻击防御

防御终端设备面临的多种重放攻击

常见协议接入

支持MQTT、CoAP、UDP、HTTP等多协议接入支持

全面兼容支持

兼容终端设备常用芯片、通信模组及嵌入式操作系统

物联网终端安全管理系统（TinyEye）

本系统针对设备系统安全能够提供跨平台的终端安全管理能力，覆盖系统基线安全、文件安全、登录安全、流量安全、行为安全等全方位的终端设备深度监控体系，将处于企业IT系统边界防护之外的终端设备统一集中管理，通过与安全管理平台的联动，可以针对异常攻击行为进行主动防御，实现精确到每台设备的实时安全管控。

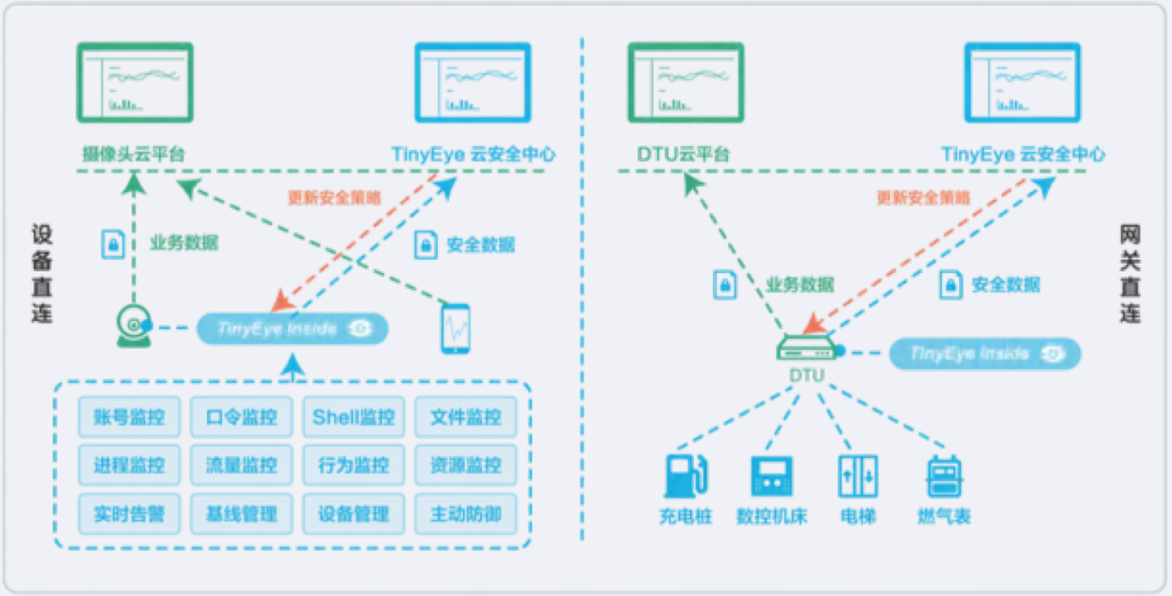
- **Agent支持ARM、MIPS、x86架构、多种基于Linux内核的定制化嵌入式操作系统**

支持操作系统	版本	硬盘占用（均值）	内存占用（均值）
OpenWRT	Chaos Calmer	295 KB	3 MB
	LEDE	297 KB	4 MB
Ubuntu	16.04 LTS 32bit	306 KB	4 MB
	16.04 LTS 64bit	320 KB	5 MB
	18.04 LTS 64bit	327 KB	6 MB
CentOS	6/7 64bit	312 KB	7 MB
Raspbian	2017 October	298 KB	5 MB
其他(Linux内核)	客户定制		

资质&认证

- 青莲云物联网设备安全Agent软件
- 青莲云物联网设备安全管理系统V1.0

产品架构



客户案例

宇视 uniview　云从科技 CLOUDWALK　TERMINUS 特斯联　qinglia　SA E-CODE

物联网终端安全管理系统（TinyEye）

本平台针对设备系统安全能够提供跨平台的终端安全管理能力，覆盖系统基线安全、文件安全、登录安全、流量安全、行为安全等全方位的终端设备深度监控体系。通过与安全管理平台的联动，可以针对异常攻击行为进行主动防御，实现精确到每台设备的实时安全管控。

终端设备管理

设备统一安全管理，包含安全威胁告警及各类监控策略配置

系统风险识别

弱密码、异常端口，异常进程，异常行为，已知漏洞利用等

可疑文件监控

针对需要监控的文件或目录，对改动、新建、删除等动作进行审计

异常流量监控

知识库和机器学习算法结合，利用多个数据分析向量如协议分布、数据MTU、流量带宽等判断流量安全

安全基线监控

系统资源（CPU、内存、存储）、异常端口、异常进程等操作系统基线相关的参数进行监控

异常行为监控

实时监测恶意登录行为，审计操作历史记录，进而阻断非法IP或对设备进行相应操作

异常登陆监控

针对暴击破解、非法用户、非法IP进行实时监控

防火墙策略

更改防火墙配置。如屏蔽IP，开放关闭指定端口，数据包过滤等

物联网设备可信执行环境（TinyTEE）

青莲云推出的TinyTEE是基于ARMv8-M指令集及TrustZone技术搭建的嵌入式设备可信执行环境，充分利用硬件手段对RAM、Flash进行了隔离，有效阻止非法访问敏感数据，以保障设备运行时的安全,适用于资源受限的IoT设备。

技术优势

底层分区隔离

存储区硬件级别隔离，最高等级保障设备运行时安全。

安全存储

支持数据持久化存储，可保护本地隐私及敏感数据不被窃取，如指纹数据、关键算法、数字版权、应用密钥等。

通用密码算法

对称密码算法、非对称密码算法、散列算法、数字签名、真随机数发生器等通用算法支持。

支持定制化TA

现有通用TA可覆盖大部分应用场景，也可提供特殊功能定制化TA开发，贴合业务细节，完善方案功能。

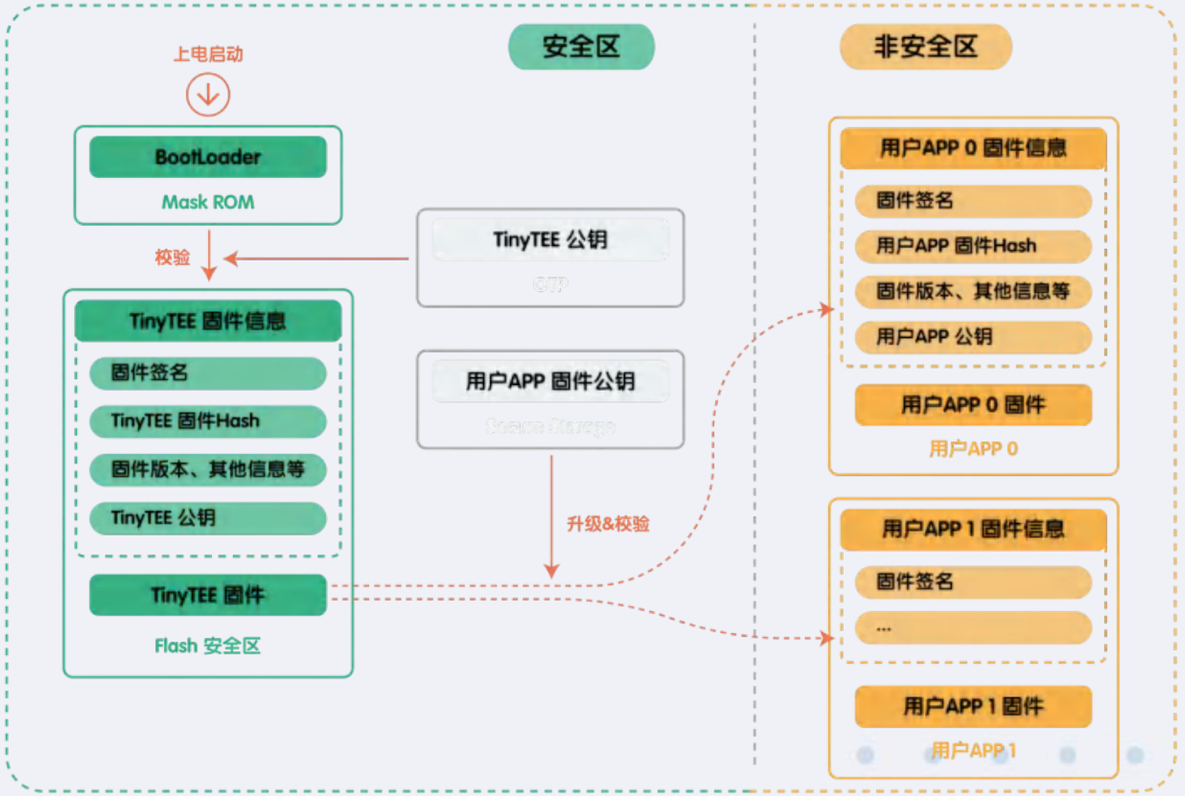
安全应用支持

支持安全启动、设备认证、安全OTA、实时消息推送等服务，实现全链路安全技术支持。

灵活flash支持

支持片外flash，如对固件存储区域的容量要求较大，可支持外接加密flash，保护产品固件。已对接 Winbond 的 W77Q 等型号。

产品架构



物联网安全检测平台（TinyScan）

青莲云推出的物联网安全检测平台以SaaS服务的形式，提供覆盖设备固件、云平台/API、客户端APP的远醒自动化安全检测服务,并出具可下载、可复测的企业专属安全检测报告，帮助企业建立属于自己的安全测试流程，定期监测产品安全漏洞。

1个小时深度分析，**3份**专业检测报告，**全面发现**设备固件、物联网云平台、APP的安全漏洞

提供**企业API**实现定期检测，助力企业建立专属安全测试流程

安全检测报告

设备固件安全检测报告

云平台/API安全检测报告

APP安全检测报告

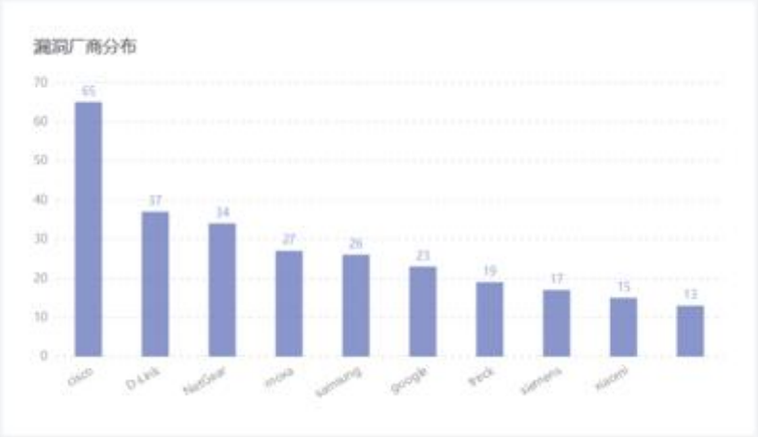
产品架构

客户案例

公安部第三研究所　OPLS Lab　盾信科技 PONSHINE　中国电信 CHINA TELECOM

物联网安全漏洞库（IoTVD）

IOTVD（IoT Vulnerability Database）是青莲云收集、整理、建立的物联网行业安全漏洞共享知识库。IOTVD平台为物联网企业提供可参考、学习、自查的漏洞信息共享和漏洞情报通知服务。建立IOTVD的目的是希望全面的收集整理物联网行业相关漏洞，覆盖云服务、硬件设备、系统架构、供应链、底层技术等众多维度，与企业客户一起持续关注物联网安全态势发展。



物联网安全企业培训体系

课程名称	内容纲要
《物联网硬件安全测试与攻防技术分享》	1.物联网软件层面攻防基本思路 2.固件的逆向 3.通信分析 4.协议分析 5.云端业务逻辑分析 6.编写漏洞POC
《物联网重大安全事件技术原理分享》	1.智能插座远程控制案例分析 2.智能洗衣机远程控制案例分析 3.智能豆浆机远程控制案例分析 4.智能手环通信链路劫持案例分析 5.某共享单车数据泄漏案例分析 6.智能路由器命令执行漏洞分析
《移动APP安全开发实践》	1.移动应用安全设计和安全开发 2.移动应用漏洞分析
《移动APP安全测试与攻防技术分享》	1.APK 的逆向 2.APK 总配置文件的解析 3.APK 的第三方库分析 4.APK 的源码分析

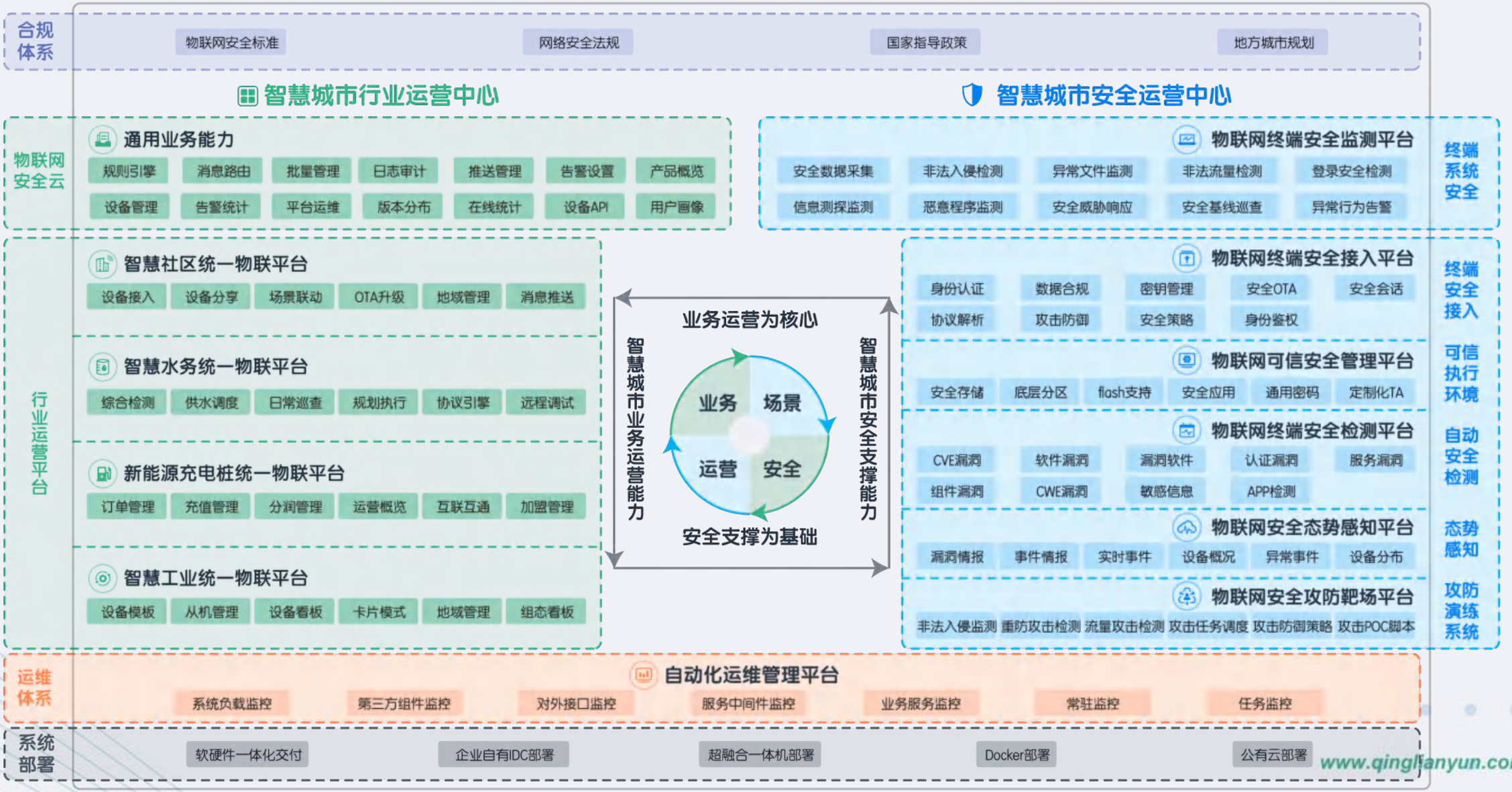
课程名称	内容纲要
《物联网终端设备通信安全技术分享》	1.安全双向身份验证机制介绍 2.加密不等于安全 3.设备重放攻击防御介绍 4.基于会话管理的安全机制技术介绍 5.安全 VS 性能 6.NB-IOT安全技术实践 7.物联网安全接入网关结构
《物联网云平台系统安全架构分享》	1.物联网云平台软件架构 2.物联网云平台安全策略 3.物联网云平台系统结构 4.设备接入SDK技术介绍 5.分层服务器技术介绍 6.安全接入网关技术介绍 7.核心服务组件技术介绍
《物联网云端安全态势感知平台技术分享》	1.适用于物联网的大数据分析系统架构介绍 2.实时计算平台和离线计算平台介绍 3.物联网大数据安全分析维度介绍 4.如何建立基于行为的大数据安全分析模型

课程名称	内容纲要
《物联网云平台引擎安全开发技术实践分享》	1.物联网云平台的安全需求 2.物联网云平台的安全模型 3.物联网云平台外部边界安全 4.物联网云平台内部边界安全 5.物联网云平台服务自身安全 6.安全开发流程 7.基本开发规范
《物联网嵌入式终端安全开发实践技术分享》	1.嵌入式设备硬件级安全开发介绍 2.基于嵌入式操作系统的安全开发介绍 3.无操作系统的安全开发介绍 4.嵌入式软件安全编码介绍
《物联网产品安全开发周期分享》	1.移动应用安全威胁及风险 2.关于SDL安全开发生命周期 3.关于SAMM模型 4.物联网应用软件架构的演变 5.物联网应用团建安全风险架构 6.实施SDL的意义 7.SDL的实施流程 8.适用于物联网应用开发的SDL

青莲云物联网安全整体解决方案建设思路

青莲云智慧城市解决方案整体架构

“一体化方案”、“两个中心”、“三大体系”、“四个场景”、“六重安全”



行业案例介绍

高铁动环监控物联网安全云平台

项目简介：

青莲云与中软合作共建高铁动环监控大数据分析可视化平台，实时采集机房动环数据并通过大数据实时分析、实时告警，联动实时处理，极大的缩减了传统依靠人力巡检的人员成本，实现铁道机房智能化、高效化、可视化集中管理运营。

贵阳经开区智慧城市物联网安全中心

项目简介：

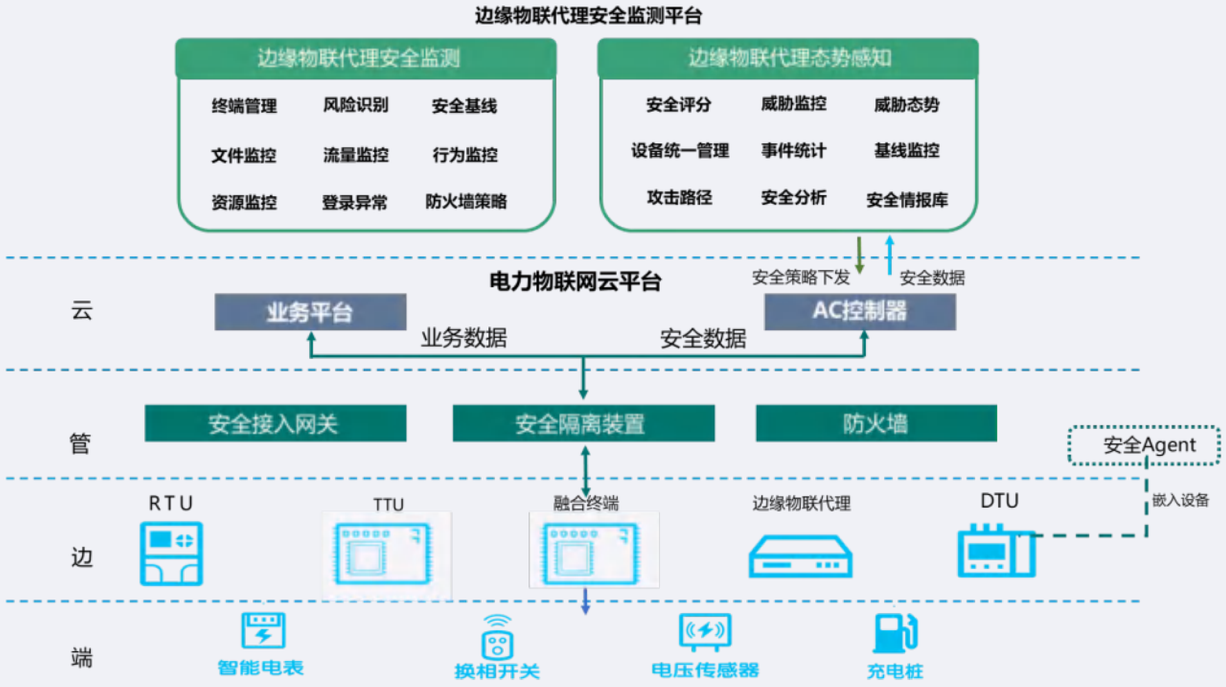
基于底层高精度地图和海量物联设备，通过深度融合物联网、云计算、大数据、人工智能等新技术，建设以城市数据中台为核心，以“万物互联、广泛连接、存算一体、数据安全”四大体系为支撑的智慧产业园。项目建设内容包括城市数据中台、智慧交通、智慧市政、智慧园区和数据安全防护等。

暖通行业工业物联网安全管理平台

项目简介：

青莲云推出“工业互联网管理平台”，帮助工业互联网厂商具备安全接入、安全管理的能力，无需企业客户二次开发，只需几步即可完成部署，贴合工业客户业务场景需求，实现工业设备迅速上云、便捷管理。

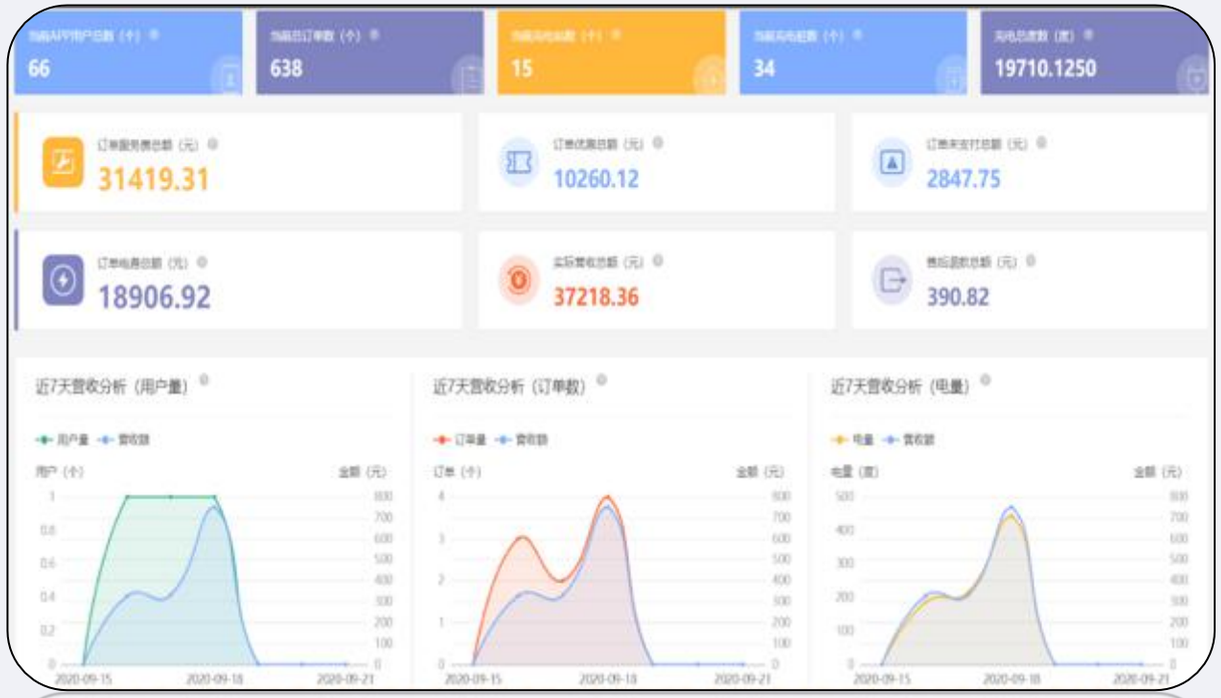
国家电网物联网终端安全运营中心



项目简介：

青莲云电力行业物联网安全平台实现对电力物联网海量边缘智能设备安全统一管理与防护，涉及系统、身份、数据、通信、行为等多维度安全保障。挖掘边缘设备安全数据内生价值，结合态势感知、安全情报等多种手段相结合建立泛在电力物联网边缘安全主动防御机制。

新能源智能充电桩设备运营管理平台



项目简介：

在基于物联网安全防护和国家安全合规要求的基础上提供充电平台的业务运营和设备管理能力，通过私有化部署帮助企业快速构建自主可控的充电桩运营管理平台，目前已经同国网电动汽车服务有限公司和联行科技展开项目合作

青莲云
qinglianyun.com

完整闭环方案，持续赋能行业

工业制造

智慧城市

运营商

安全合规

安全芯片

电力系统

消费电子

让安全成为物联网应用的基础设施