青莲网络
QINGLIAN NETWORK

一站式等保
安全合规服务

目录

青莲网络
QINGLIAN NETWORK

01 青莲网络公司介绍

1 企业简介

青莲网络 QINGLIAN NETWORK

青莲网络 | 国内领先的全栈运维及管理服务提供商

青莲网络是国内领先的全栈运维及管理服务提供商，为用户提供全流程的IT服务。作为国内首批云管理服务伙伴，凭借近20年的服务经验与专业技能，已累计为全国1万多家企业提供云+服务，业务涵盖200+城市和30+行业领域。依托ValueOps云服务管理平台，致力于打造敏捷高效和安全合规的全栈运维服务体系，以“上好云 · 用好云 · 管好云” 为服务理念，助力企业加速数字化转型。

200+
云技术专家

10000+
多领域客户案例

100%
覆盖系统
全生命周期

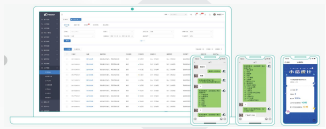
10+
云平台

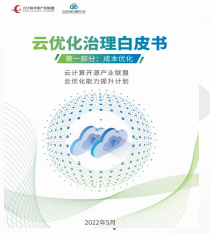
30+
服务认证

国家级
实验室

2 发展历程

青莲网络 QINGLIAN NETWORK





2009年-2015年

集团成立，提供网络安全、虚拟化、超融合、私有云等集成业务。

2015年开始布局云计算。

2016年

成为阿里云华南区授权服务中心。组建云技术团队，加入阿里云共享服务团队。

2017年

自研联客易智能工单平台1.0正式上线，全面构建标准化的云运维服务流程。

2018年

成为华南首批阿里云生态技术先锋联盟（ITP）成员。

成立云MSP产品中心，云MSP服务产品化 1.0发布。

成立青永数据子公司，提供基于混合云的IT基础架构及专业安全服务。

2019年

成为阿里云**首批战略级合作伙伴**，服务团队扩大10倍，拥有**100+云技术专家。**

成为广东电信天翼云唯一云服务战略合作伙伴。

与绿盟、360、奇安信深度合作，提供渗透、安全风评等服务。

2020年

成立上海、北京分公司，**形成全国一体化的云MSP技术服务网络。**

成为阿里云SAP能力中心，以一站式云服务携手共建城市数智化生态。

2021年

云MSP服务体系全新升级，助力超一万家大型企业实现数字化转型。

ValueOps云服务管理平台正式上线，实现云IT智能化运维管理。

与西安电子科技大学成立边缘智能技术联合实验室，并成立**专注于人工智能领域的子公司——灵图数据（杭州）。**

与VMware、英特尔等知名合作企业达成重要合作，共筑云生态。

2022年

奇墨科技成立，并打造全新子品牌——**奇墨图治**，专注于IT质量管理。

成为中国信通院“云优化提升计划”成员单位，参编《云优化治理实践指南 第1部分：成本优化》白皮书和可信云《能力评估标准》。

3 企业资质

青莲网络 QINGLIAN NETWORK

100+国家级权威认证
拥有全面完善服务创新能力

国家高新技术企业、信息系统建设和服务能力CS2 、大数据人工智能企业库、ISO9000\ISO27001\ISO2000、CMMI ML3级认证及五星级售后服务认证等

200+技术专家认证
覆盖云、信息安全、AI等多领域

CCRC安全可靠服务体系、ACE高级认证、阿里云ACP架构师认证、ASC安全架构师认证、阿里云Aliware认证、CISP、Oracle、Linux、CCNP、VMWare等行业认证

4 生态优势

阿里云

旗舰级合作伙伴
生态技术先锋
中间件核心授牌伙伴
云原生核心授牌伙伴
云MSP合作 计划核心伙伴

中国信通院

成为中国信通院“云优化能力提升计划成员”

西安电子科技大学

共建边缘智能技术联合实验室

英特尔

咨询合作伙伴

VMware

技术合作伙伴，共同推出“以云定义高敏态的云数据中心”概念

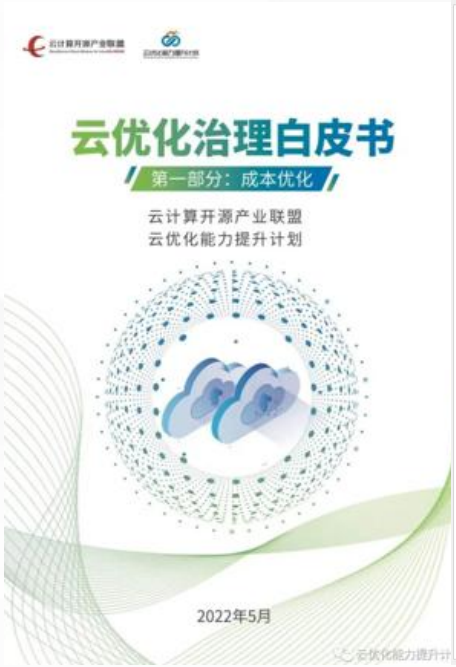
5 中国云计算标准编写单位

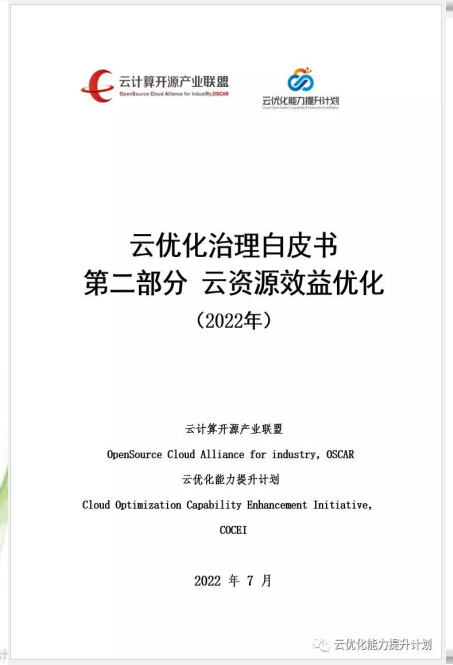
青莲网络 QINGLIAN NETWORK

国内首批云优化能力提升计划成员

由中国信息通信研究院、中国通信标准化协会、云计算开源产业联盟共同牵头成立的国家级云计算研究和标准组织

参与可信云等行业云技术标准编写
覆盖云安全、云优化、云治理、云工具





6 能力中心

青莲网络 QINGLIAN NETWORK

拥有从“私有云-公有云-混合云”的全栈云技术能力，为企业提供全方位云+服务

云咨询能力中心

云迁移能力中心

云运维能力中心

云优化能力中心

SAP上云能力中心

VMware云能力中心

数据库能力中心

云原生能力中心

云安全能力中心

云合规能力中心

7 服务网络

北京

营销、技术服务中心

广州

云、AI“产研服”综合基地

云+MSP技术研发、服务AI算法/方案研发-设计-部署

深圳

营销、技术服务中心

上海

营销、技术服务中心

杭州

科研创新中心

高阶AI算法和多模态AI算法研发

北京 杭州 上海 广州 深圳

全国一体化的云MSP服务网络、五大产研服基地

8 标杆客户

青莲网络 QINGLIAN NETWORK

助力1万+大型企业数字化转型，覆盖30+行业

青莲网络
QINGLIAN NETWORK

02

等保2.0背景概述

为企业提供一站式的安全咨询、安全建设、合规性测评整改服务

9 网络安全：新时代、新风险、新挑战

近年来，数字化转型提速，但安全形势更为复杂，针对政府、医疗、教育、金融、电力、通信等关键信息基础设施的网络攻击日渐常态化、专业化，针对性极强，造成了严重的经济损失。

勒索病毒

勒索病毒攻击更加频繁、破坏性更强

APT攻击

APT组织也在不断使用供应链攻击等新手段

有组织有目的攻击

西北工业大学遭到的有组织有目的的网络攻击

网络安全相关法律

含草案说明

中华人民共和国国家安全法

第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、**关键基础设施和重要领域信息系统及数据的安全可控**；加强网络管理，防范、制止和依法惩治**网络攻击、网络入侵、网络窃密、散布违法有害信息**等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

中华人民共和国网络安全法

含草案说明

第二十一条国家实行**网络安全等级保护制度**。**网络运营者**应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

11 刑法修正案（九）信息网络安全管理义务

中华人民共和国刑法修正案（九）——
（2015年8月29日第十二届全国人民代表大会常务委员会第十六次会议通过）

刑法修正案（九）第二百八十六条之一（新增）

第二百八十六条之一：“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门通知采取改正措施而拒绝执行，有下列情形之一的，**处三年以下有期徒刑、拘役或者管制**，并处或者单处罚金”：

（一）致使违法信息大量传播的；

（二）致使用户信息泄露，造成严重后果的；

（三）致使刑事犯罪证据灭失，严重妨害司法机关依法追究犯罪的；

（四）有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其**直接负责的主管人员和其他直接责任人员**，依照前款的规定处罚。

等级保护发展历程

1994

国务院147号令

第一次提出等级保护概念，要求对信息系统分等级进行保护

1999

等级保护强制性国家标准发布

《计算机信息系统安全保护等级划分准则》GB17859-1999

2007

公通字[2007]43号

《信息安全等级保护管理办法》（公通字[2007]43号）文件的正式发布，标志着等级保护1.0的正式启动

2008-2012

等保1.0体系

等级保护1.0的国家标准体系陆续出台

2017

网络安全法

2016年发布《中华人民共和国网络安全法》，2017年6月1日正式实施；标志着等级保护2.0的正式启动。网络安全法第二十一条明确“国家实行网络安全等级保护制度。”

2019

等保2.0体系

等保2.0国家标准对比等保1.0，在保护范围、法律效力、技术标准、安全体系、定级流程、定级指导等方面均发生变化

13 网络安全法律法规背景

青莲网络 QINGLIAN NETWORK

《中华人民共和国网络安全法》自2017年施行以来，为适应新形势，做好《中华人民共和国网络安全法》与新实施的法律（行政处罚法、数据安全法、个人信息保护法等）之间衔接协调，完善法律责任制度，进一步保障网络安全，**拟对《中华人民共和国网络安全法》作以下修改**（2022年迎来首修，拟对多处加大处罚力度）：

一、完善违反网络运行安全一般规定的法律责任制度

结合当前网络运行安全法律制度实施情况，拟调整违反网络运行安全保护义务或者导致危害网络运行安全等后果的行为的行政处罚种类和幅度。

二、修改关键信息基础设施安全保护的法律责任制度

关键信息基础设施是经济社会运行的神经中枢，为强化关键信息基础设施安全保护责任，进一步完善关键信息基础设施运营者有关违法行为行政处罚规定。

三、调整网络信息安全法律责任制度

适应网络信息安全工作实际，对违反网络信息安全义务行为的法律责任进行整合，调整了行政处罚幅度和从业禁止措施，新增对法律、行政法规没有规定的有关违法行为的法律责任规定。

四、修改个人信息保护法律责任制度

鉴于《中华人民共和国个人信息保护法》规定了全面的个人信息保护法律责任制度，拟将原有关个人信息保护的法律责任修改为转致性规定。

《中华人民共和国网络安全法》由全国人民代表大会常务委员会于2016年11月7日发布，**自2017年6月1日起施行。**

网络运营者(是指网络的所有者、管理者和网络服务提供者)**主要义务有：**

- 落实等级保护制度（**第二十一条**）
- 实施风险评估、安全测评（**第三十八条**）
- 制订安全应急预案（**第二十五条**）
- 加强安全教育 （**第三十四条**）
- 安全技术措施同步规划、同步建设、同步使用（**第三十三条**）

《网安法》原条款	**【第五十九条】**网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。 **【第六十条】**违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款： （一）设置恶意程序的； （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的； （三）擅自终止为其产品、服务提供安全维护的。 **【第六十一条】**网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 **【第六十二条】**违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。
拟修改内容	**《网安法》第五十九条、第六十条、第六十一条、第六十二条，统一拟修改为：** 违反本法第二十一条、第二十二条第一款和第二款、第二十三条、第二十四条第一款、第二十五条、第二十六条、第二十八条、第三十三条、第三十四条、第三十六条、第三十八条规定的网络运行安全保护义务或者导致危害网络运行安全等后果的，由有关主管部门责令改正，给予警告、通报批评；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节特别严重的，由省级以上有关主管部门责令改正，处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

14 网络安全新法律责任对比

青莲网络 QINGLIAN NETWORK

关键对比项		网络安全法修订稿	数据安全法	个人信息保护法
	法律责任主体	网络运营者	数据处理者	个人信息处理者
法律责任形式	约谈并要求整改	有	有	/
	责令改正	有	有	有
	予以警告	有	有	有
	通报批评	有	/	/
	没收违法所得	有	有	有
	罚款	有，对网络运营者最高5000万元以下或上一年度营业额5%以下的罚款； 对直接负责的主管和直接责任人最高可处以100万云以下罚款	有，对数据处理者最高1000万元以下的罚款； 对直接负责的主管和直接责任人最高可处以100万云以下罚款	有，对个人信息处理者最高5000万元以下或上一年度营业额5%以下的罚款； 对直接负责的主管和直接责任人最高可处以100万云以下罚款
	信用惩戒	有，依照有关法律、行政法规的规定记入信用档案，并予以公示	/	有，依照有关法律、行政法规的规定记入信用档案，并予以公示
	暂停相关业务、停业整顿、吊销相关业务许可证或营业执照	有，责令关闭网站	有	有，其中针对违法处理个人信息的应用程序，可责令暂停或终止提供服务
	治安管理处罚	有，构成违反治安管理行为的，依法给与治安管理处罚	有，构成违反治安管理行为的，依法给与治安管理处罚	有，构成违反治安管理行为的，依法给与治安管理处罚
	拘留	有，最高可处15日以下拘留	/	/
	民事和刑事责任	有，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任	有，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任	有，构成犯罪的，依法追究刑事责任
	从业限制	①禁止直接负责的主管和直接责任人在一定期限内担任董事、监事、高管或者从事网络安全管理和网络运营关键岗位的工作； ②受到治安管理处罚的人员，5年内不得从事网络安全管理和网络运营关键岗位的工作； ③受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作；	/	禁止直接负责的主管和直接责任人在一定期限内担任董事、监事、高管和个人信息保护负责人

网络安全执法检查背景

两个“全力确保”

- 全力确保不发生重大网络安全事件
- 全力确保城市网络和重要信

涵盖十类重要信息系统

网络安全执法检查涵盖党政机关、教育、卫生、国资、水电气、公交、宾旅馆、大型互联网企业，其他具有一定影响力的单位等部门行业的重要信息系统，以及户外LED大屏播控系统等。

党政机关 | 教育 | 卫生 | 国资 | 水电气

公交 | 宾旅馆 | 大型互联网企业 | 一定影响力单位 | 户外LED播控系统

三个“总体目标”

- 深入排查网络安全风险
- 堵塞网络安全漏洞
- 落实网络安全责任

网络运营者应履行的义务

- 落实等级保护措施
- 落实网络安全技术防护措施
- 落实网络安全管理制度和操作规程
- 落实数据分类、重要数据备份和加密等措施
- 履行其他法律法规规定的义务

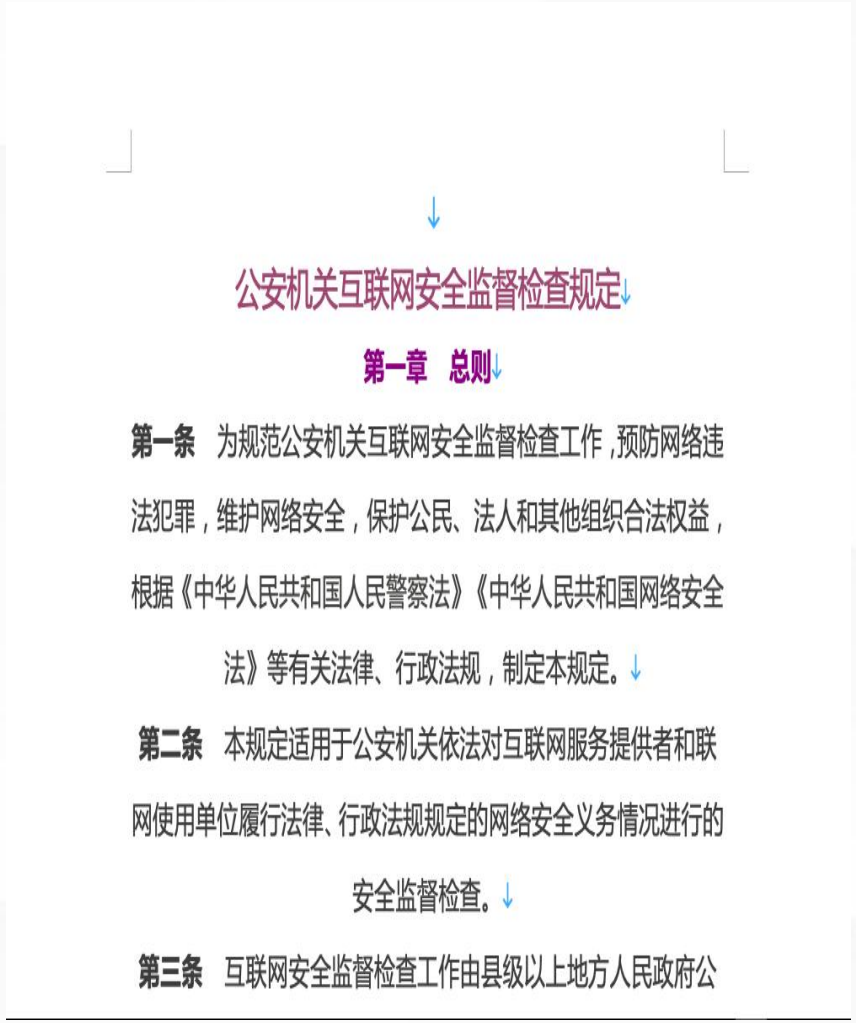
两个“重点关注”

- 提供公共服务的重要信息系统
- 存贮公民数据的重要信息系统

网络运营者应重点做好“四防”保障

- 网页防篡改
- 服务防中断
- 数据防泄漏
- 网站防病毒

公安机关监督检查



公安机关互联网安全监督检查规定

第一章 总则

第一条 为规范公安机关互联网安全监督检查工作，预防网络违法犯罪，维护网络安全，保护公民、法人和其他组织合法权益，根据《中华人民共和国人民警察法》《中华人民共和国网络安全法》等有关法律、行政法规，制定本规定。

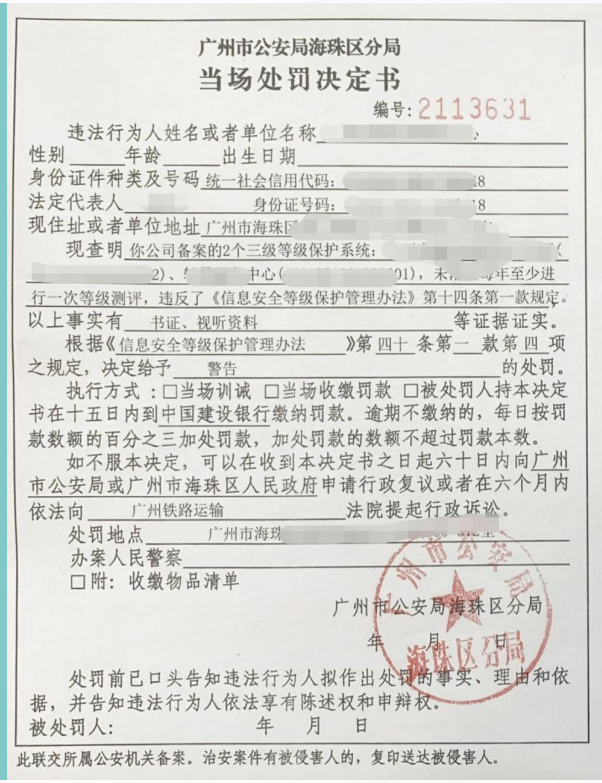
第二条 本规定适用于公安机关依法对互联网服务提供者和联网使用单位履行法律、行政法规规定的网络安全义务情况进行的安全监督检查。

第三条 互联网安全监督检查工作由县级以上地方人民政府公

- 2018年11月1日起实施《公安机关互联网安全监督检查规定》（公安部151号令）
- 第八条　互联网安全监督检查由互联网服务提供者的网络服务运营机构和联网使用单位的网络管理机构所在地公安机关实施。互联网服务提供者为个人的，可以由其经常居住地公安机关实施。
- 第十条　公安机关应当根据互联网服务提供者和联网使用单位履行法定网络安全义务的实际情况，依照国家有关规定和标准，对下列内容进行监督检查：
- （七）是否履行法律、行政法规规定的网络安全等级保护等义务。
- 第十三条　公安机关开展互联网安全监督检查，可以采取现场监督检查或者远程检测的方式进行。

17 公安监管执法形式

公安机关现场执法或下发测评整改通知书限期要求企事业单位完成等保相关工作和修复安全风险问题



广州市公安局海珠区分局

当场处罚决定书

编号:2113631

违法行为人姓名或者单位名称

性别 年龄 出生日期

身份证件种类及号码 统一社会信用代码:

法定代表人 身份证号码:

现住址或者单位地址 广州市海珠区

现查明 你公司备案的2个三级等级保护系统:

行一次等级测评，违反了《信息安全等级保护管理办法》第十四条第一款规定。

以上事实有 书证、视听资料 等证据证实。

根据《信息安全等级保护管理办法》第四十条第一款第四项之规定，决定给予 警告 的处罚。

执行方式：□当场训诫 □当场收缴罚款 □被处罚人持本决定书在十五日内到中国建设银行缴纳罚款。逾期不缴纳的，每日按罚款数额的百分之三加处罚款，加处罚款的数额不超过罚款本数。

如不服本决定，可以在收到本决定书之日起六十日内向广州市公安局或广州市海珠区人民政府申请行政复议或者在六个月内依法向 广州铁路运输 法院提起行政诉讼。

处罚地点 广州市海珠

办案人民警察

□附：收缴物品清单

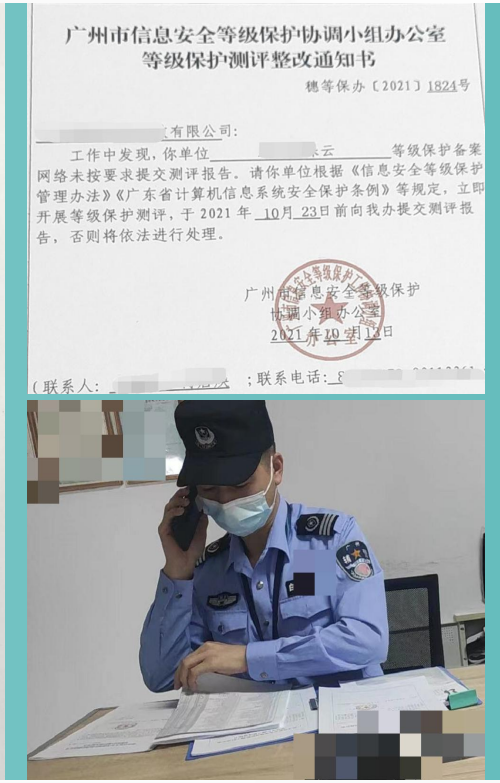
广州市公安局海珠区分局

年 月 日

处罚前已口头告知违法行为人拟作出处罚的事实、理由和依据，并告知违法行为人依法享有陈述权和申辩权。

被处罚人: 年 月 日

此联交所属公安机关备案。治安案件有被侵害人的，复印送达被侵害人。



广州市信息安全等级保护协调小组办公室

等级保护测评整改通知书

穗等保办〔2021〕1824号

有限公司:

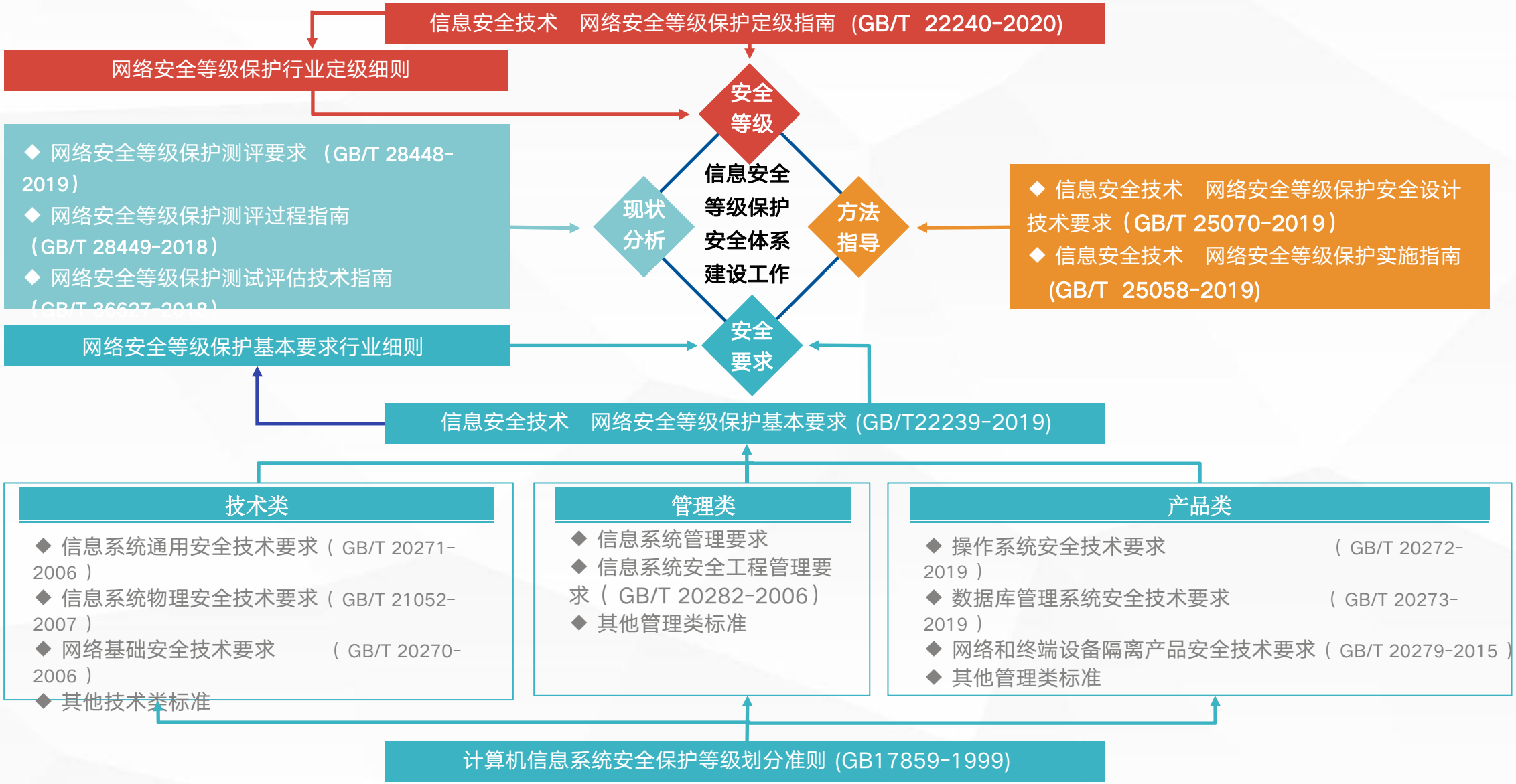
工作中发现，你单位 云 等级保护备案网络未按要求提交测评报告。请你单位根据《信息安全等级保护管理办法》《广东省计算机信息系统安全保护条例》等规定，立即开展等级保护测评，于2021年10月23日前向我办提交测评报告，否则将依法进行处理。

广州市信息安全等级保护协调小组办公室

2021年10月12日

（联系人: ；联系电话:

等级保护国家标准体系


信息安全技术　网络安全等级保护定级指南（GB/T 22240-2020）
网络安全等级保护行业定级细则
安全等级
◆ 网络安全等级保护测评要求（GB/T 28448-2019）
◆ 网络安全等级保护测评过程指南（GB/T 28449-2018）
◆ 网络安全等级保护测试评估技术指南
现状分析
信息安全等级保护安全体系建设工作
方法指导
◆ 信息安全技术　网络安全等级保护安全设计技术要求（GB/T 25070-2019）
◆ 信息安全技术　网络安全等级保护实施指南（GB/T 25058-2019）
网络安全等级保护基本要求行业细则
安全要求
信息安全技术　网络安全等级保护基本要求（GB/T22239-2019）
技术类
◆ 信息系统通用安全技术要求（GB/T 20271-2006）
◆ 信息系统物理安全技术要求（GB/T 21052-2007）
◆ 网络基础安全技术要求（GB/T 20270-2006）
◆ 其他技术类标准
管理类
◆ 信息系统管理要求
◆ 信息系统安全工程管理要求（GB/T 20282-2006）
◆ 其他管理类标准
产品类
◆ 操作系统安全技术要求（GB/T 20272-2019）
◆ 数据库管理系统安全技术要求（GB/T 20273-2019）
◆ 网络和终端设备隔离产品安全技术要求（GB/T 20279-2015）
◆ 其他管理类标准
计算机信息系统安全保护等级划分准则（GB17859-1999）

等保2.0国家标准体系

（一）基础类

1、《计算机信息系统安全保护等级划分准则》GB 17859-1999

2、《信息安全技术 网络安全等级保护实施指南》GB/T 25058-2019

（二）系统定级环节

3、《信息安全技术 网络安全保护等级定级指南》GB/T 22240-2020

（三）建设整改环节

4、《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019

5、《信息安全技术 网络安全等级保护安全设计技术要求 》GB/T25070-2019

（四）等级测评环节

6、《信息安全技术 网络安全等级保护测评要求》GB/T28448-2019

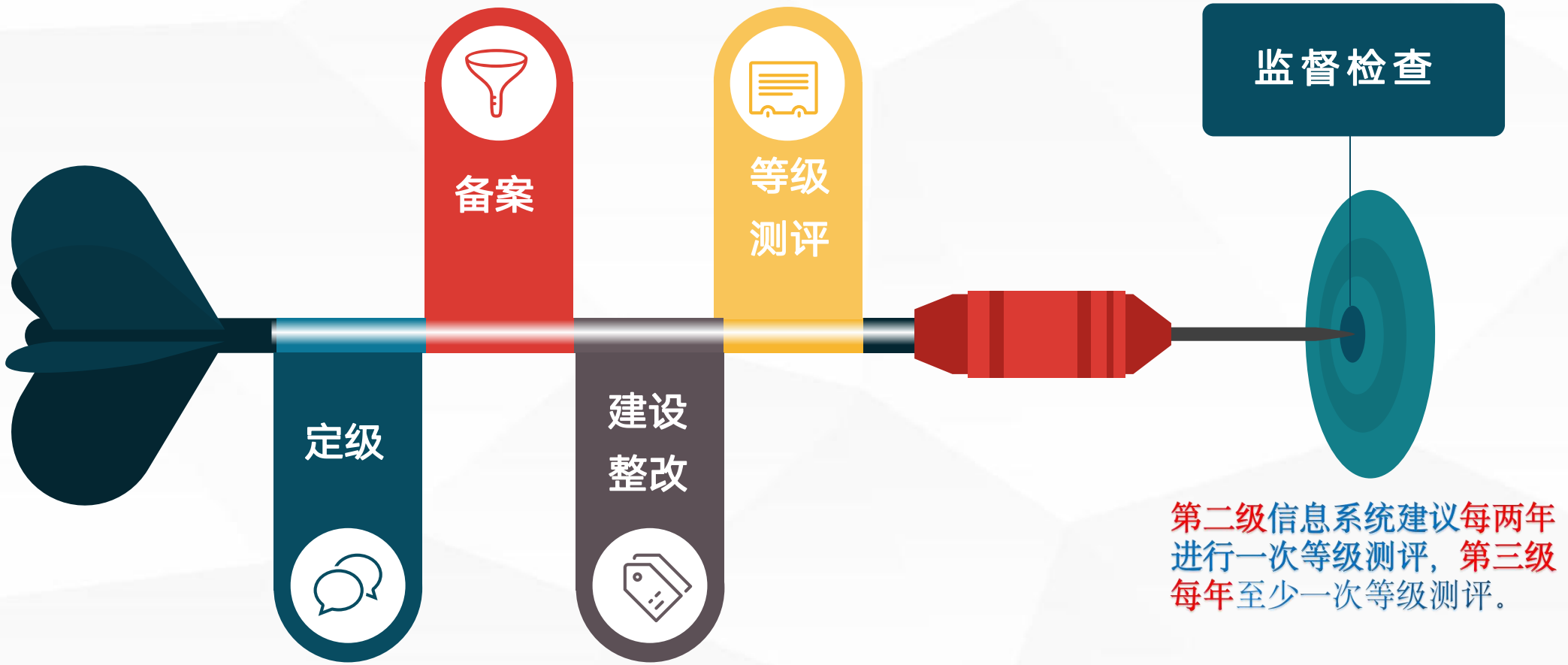
7、《信息安全技术 网络安全等级保护测评过程指南》GB/T28449-2018

等保2.0覆盖广度

覆盖范围：政府单位、金融行业、医疗行业、教育行业、公共安全行业、能源行业、企业单位以及其他有信息系统定级需求的行业与单位，均在等保2.0的监管范围，也就是覆盖**全社会**。

覆盖对象：等保2.0在1.0标准的基础上，注重全方位主动防御、安全可信、动态感知和全面审计，实现了对传统信息系统、基础信息网络、云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象的**全覆盖**。

21 等保2.0工作标准流程



第二级信息系统建议每两年进行一次等级测评，第三级每年至少一次等级测评。

青莲网络
QINGLIAN NETWORK

03

一站式等保测评服务解决方案

快至30天拿证　*通过率100%保证*　*7*24安全专家服务*

22 等级保护2.0安全框架体系

青莲网络 QINGLIAN NETWORK

等保2.0安全框架内容

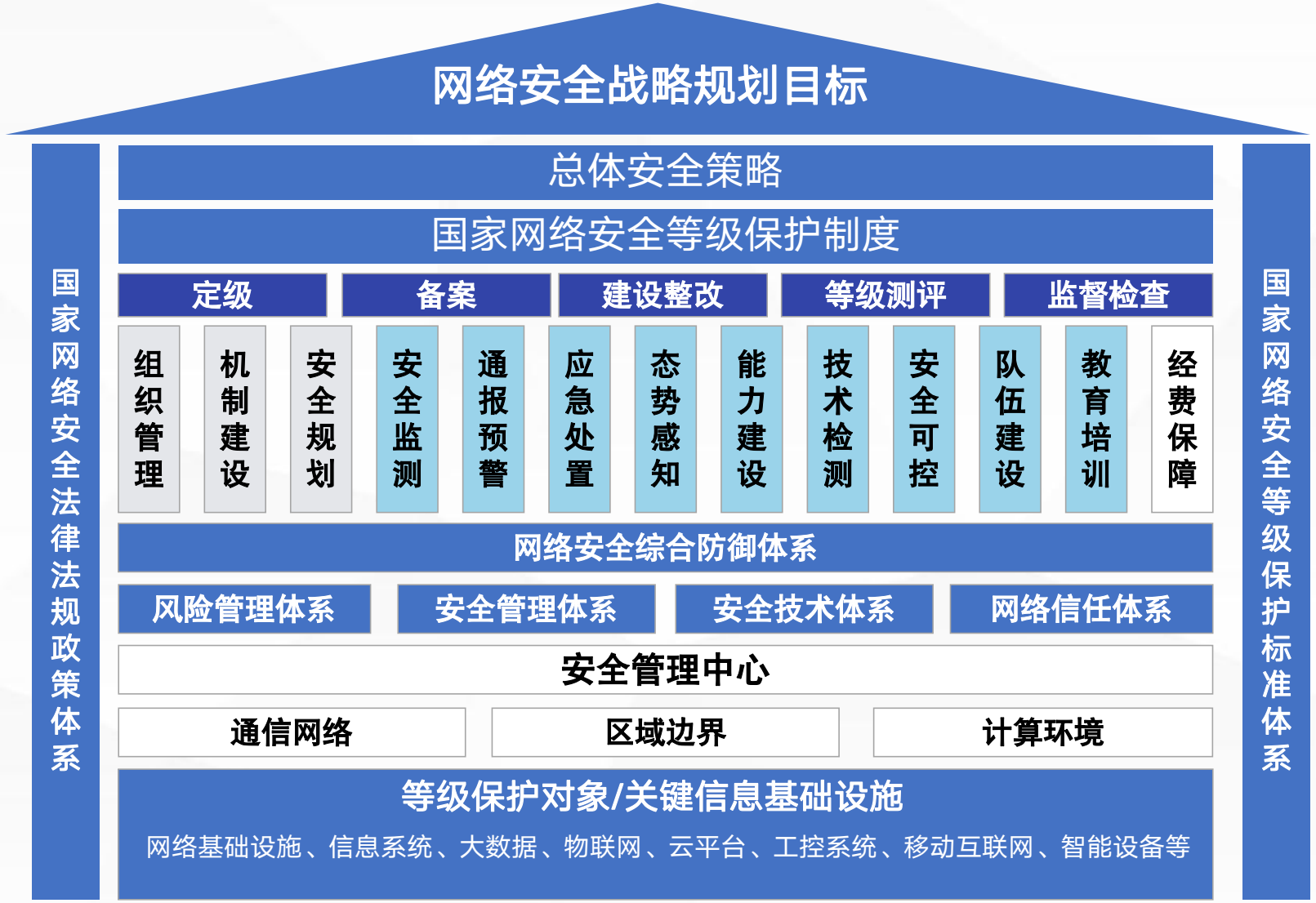
1. 依据国家网络安全法律法规和等级保护政策标准开展等级保护工作

2. 确定等级保护对象

3. 采取“一个中心、三重防护”的安全建设理念

4. 建立安全技术体系和安全管理体系，构建具备相应等级安全防护能力的网络安全综合防御体系

5. 开展组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、教育培训和经费保障等工作。



等级保护2.0安全等级划分

- 第一级（自主保护级）：一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息系统；信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- **第二级（指导保护级）**：一般适用于县级其些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等；信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成一般损害，但不损害国家安全。
- **第三级（监督保护级）**：一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成一般损害。
- 第四级（强制保护级）：一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统；信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
- 第五级（专控保护级）：一般适用于国家重要领域、重要部门中的极端重要系统；信息系统受到破坏后，会对国家安全造成特别严重损害。
- **原则上，定级为二级及以上的信息系统都是需要做等保测评**。区县的系统基本都是二级；省级单位门户网站，地级市重要行业的门户网站是三级；涉及到工作秘密、敏感信息的系统，信息泄露出去或者被非法篡改会引起民众恐慌、社会秩序混乱、破坏国家安全的系统都要定到三级；地级市及省级单位其他不涉及敏感信息、重要信息的一般系统定到二级。

24 等保2.0定级备案对象举例

青莲网络 QINGLIAN NETWORK

行业	关键系统	关键信息
一般企业	门户网站	发布的企业信息
国家机关、政府机关，事业单位，央企	内部重要的信息系统	涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这类系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省连接的网络系统等
云服务商/IDC	云服务平台IDC管理平台	托管客户的数据 支撑托管客户合规
游戏	游戏平台	玩家信息、资金信息、游戏状态信息
公共媒体	门户网站	发布的公共信息、广告
位置追踪	追踪定位系统、网约车系统	人员、车辆信息人员、车辆位置
金融保险类	在线交易系统	真实身份:姓名、地址、联系方式、证件类型、证件号码虚拟身份；银行账号/密码、app账号/密码资金信息、交易信息

等保2.0定级备案对象举例

行业	关键系统	关键信息
医疗机构	HIS(医院信息管理)系统 PACS(医学影像归档与通信)系统 LIS(实验室信息)系统; 电子病历(EMR)系统	病人个人信息、病人病例、缴费信息、医院管理信息
院校	招生系统/录取系统 、核心知识、技术管理系统	师生个人信息/招生、录取信息/核心技术
制造业	ERP(企业资源规划)系统 CRM(客户关系管理)系统 MES(制造过程执行)系统	生产资源信息、生产配方、生产工艺、机器程序、技术参数

- 常规民用系统定级以二级和三级为主
- 带有客户敏感信息或传播性强、承载业务核心的系统。如:带有用户身份、用户管理、交易类、报考、录取、病例等关键个人信息的系统,以及公共传媒、关键信息基础设施等系统建议定级为三级
- 四级系统一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统
- 五级系统一般适用于国家重要领域、重要部门中的极端重要系统
- 二级建议每两年进行一次测评 ， 三级系统应每年至少进行一次测评,四级系统应每半年至少进行一次测评

等保2.0定级备案详细流程

1 确定定级对象

基础信息网络、传统信息系统、云计算平台、大数据平台、物联网、移动互联和工业控制信息系统等

2 初步确定等级

等级由业务信息安全和系统服务安全两方面确定，等级的较高者决定

3 专家评审

组织信息安全专家和业务专家，评审定级结果，出具专家评审意见。

4 主管部门审核

定级对象的运营、使用单位将定级结果上报行业主管部门或上级主管部门进行审核。(备注：无主管部门可忽略这一步)

5 公安备案审查

定级资料提交公安机关，审查不通过，需重新定级；审查通过后最终确定安全保护等级

网络安全等级保护定级回执

单位名称	[redacted]委员会组织部
系统名称	[redacted]管理系统
系统级别	2
备案证号	[redacted]0006
时间	2022年07月28日

信息系统安全等级保护备案证明

依据《信息安全等级保护管理办法》的有关规定，阿里云计算有限公司 单位的：

第 三级 公共云基础服务平台 系统

予以备案。

证书编号： 330116-13016-00001

中华人民共和国公安部监制

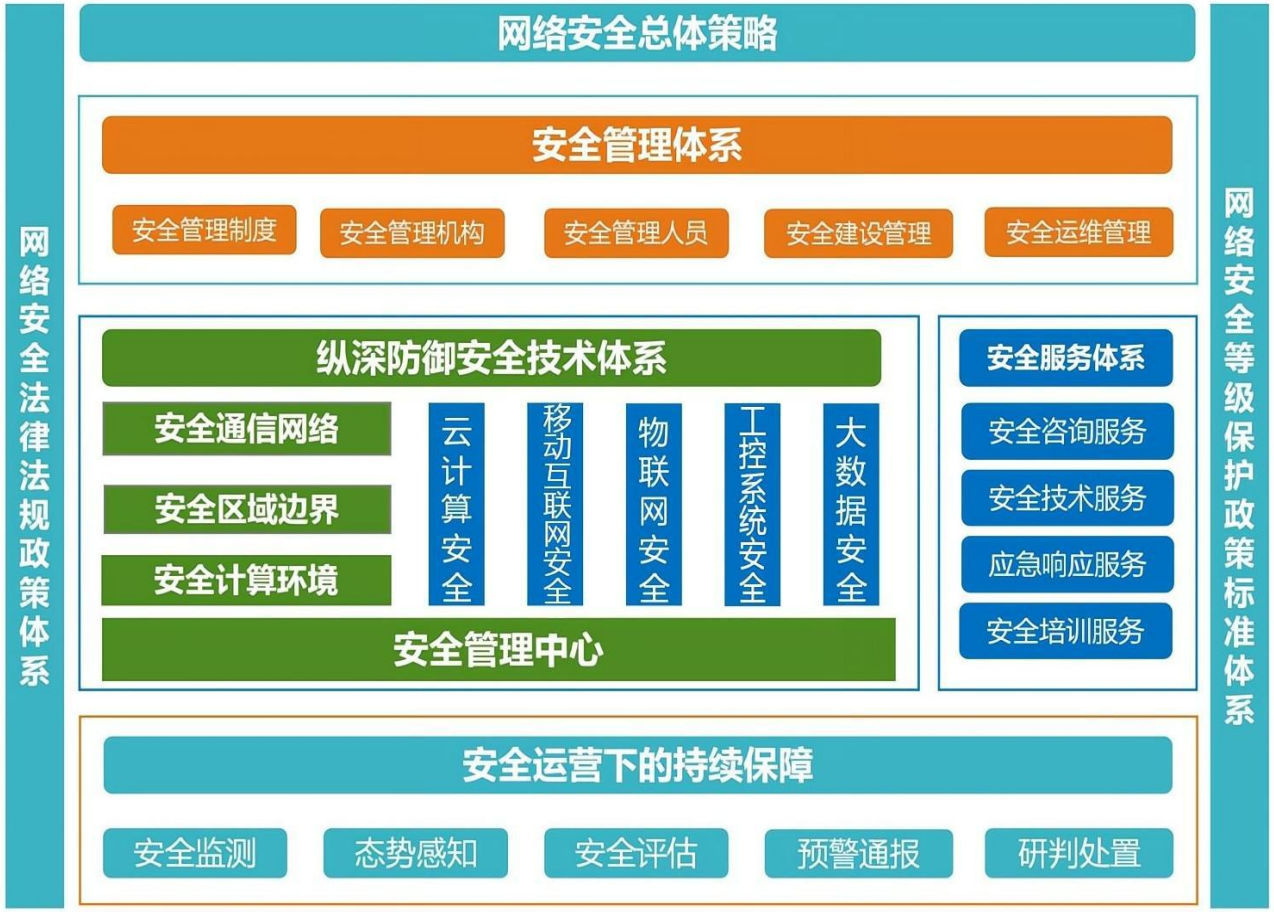
备案公安机关公章

2019年4月8日

6 确定最终等级

公安机关发放备案号或备案证明

等级保护2.0安全设计方案



安全设计方案从网络安全等级保护安全技术体系、安全管理体系两个方面提出安全建设的整体框架，建立“一个基础”（安全物理环境）、“一个中心”（安全管理中心）保障下的“三重防护体系”（安全通信网络、安全区域边界、安全计算环境）的安全架构，使得信息系统满足等保合规安全防护要求。

青莲一站式等保服务·全景图

青莲网络为企业客户提供全生命周期的等保解决方案，切实提升企业客户的安全防护能力。

青莲一站式等级保护 · 服务内容

青莲网络 QINGLIAN NETWORK

1

等保合规咨询服务

通过远程或者现场访谈的方式，为客户进行等保合规差距分析，量身定制等保解决方案。

2

等保定级备案服务

协助客户确认定级对象，并组织专家评审，准备定级报告，同时为客户准备备案材料和进行等保备案。

3

等保测评服务

协助客户进行等保差距测评工作，根据测评情况出具整改问题清单，并提供整改技术指导服务，保障整改顺利通过等保测评

4

安全产品定制服务

安全产品前期调研，根据调研情况出具安全产品采购方案，协助用户进行安全及备份产品购买和配置部署

5

等保整改服务

对系统、拓扑、软件环境、安全策略、网络架构、安全现状进行收集评估出具《整改方案》，对系统、拓扑、软件环境、安全策略、网络架构、安全现状进行收集评估出具《整改方案》，并帮助和指导用户进行系统整改，以确保满足等保合规要求。

6

安全加固建设服务

主要包括：信息系统及软件漏洞修复、操作系统安全基线配置、阿里云控制台策略配置 、安全管理制度调研和协助整改

500+客户通过等保

已为全国500+企业提供了测评及整改服务。

60+测评机构合作

已与全国60+测评机构达成服务合作，青莲直接签署测评服务

40+安全服务专家

包含测评师、渗透师、网络安全专家、备案专员

100%通过率

持续保持100%的通关率。

青莲一站式等保工作阶段·进展比重

系统定级咨询

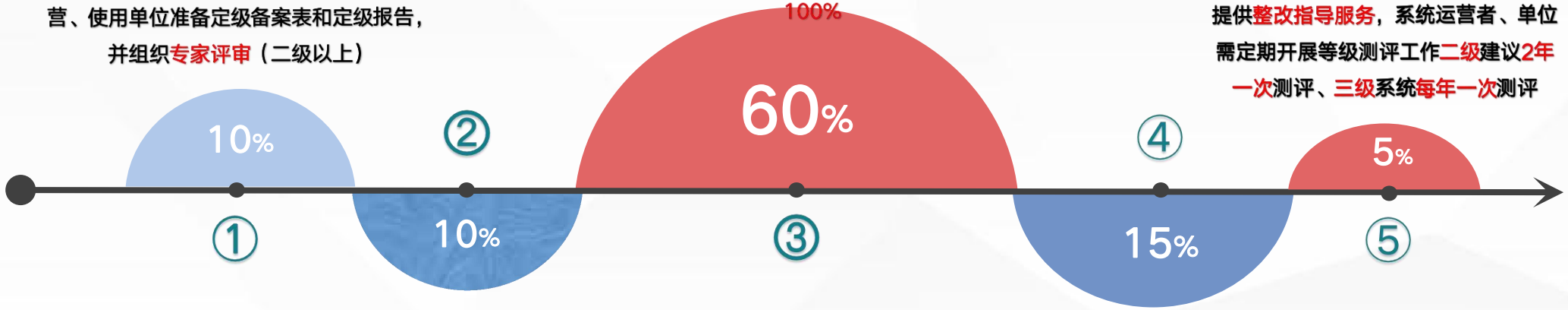
青莲协助系统运营者或企事业单位确认定级对象，为其提供等保咨询服务，辅导运营、使用单位准备定级备案表和定级报告，并组织专家评审（二级以上）

安全合规建设

基于等保2.0的安全技术和管理要求进行建设和整改,青莲提供一体化等保合规安全产品和编制安全管理制度服务，辅导客户进行定级相关系统和组件的安全加固服务、技术全程指导整改服务，辅导通过率100%

监督检查

青莲协助客户应对公安机关定期检查和提供整改指导服务，系统运营者、单位需定期开展等级测评工作二级建议2年一次测评、三级系统每年一次测评



系统定级备案

青莲主导运营、使用单位准备定级备案相关材料、备案资料盖章扫描和提交网安进行备案，并实时跟进网安审核进度

等级测评

根据等保2.0技术要求、管理要求，青莲主导沟通专业的测评机构开展现场测评及报告编制工作，为客户提供公安部门认可的等保测评报告，降低客户沟通成本和项目周期

一站式等保测评 · 标准指标

等保2.0	控制类	二级	三级	四级
技术要求	安全物理环境	15	22	24
	安全通信网络	4	8	11
	安全区域边界	11	20	21
	安全计算环境	23	34	36
	安全管理中心	4	12	13
安全管理	安全管理制度	6	7	7
	安全管理机构	9	14	15
	安全管理人员	7	12	14
	安全建设管理	25	34	35
	安全运维管理	31	48	52
合计		135	211	228
扩展指标	云计算平台	29	46	49
	物联网	7	20	16
	移动互联	14	19	21
	工业控制	15	21	22
专业检测	漏洞扫描、渗透测试、APP安全检测			

一站式等保测评 · 检测对象

物理环境

- 机房环境、设备和设施等
- 存储重要数据的介质
- 系统的网络拓扑结构

安全设备

- 安全设备、包括不限于防火墙、入侵检测设备、堡垒机、防病毒网关等

网络设备

- 边界网络设备，包括路由器、防火墙和认证网关等
- 网络互联设备，如核心交换机、汇聚层交换机、核心路由器等

系统

- 承载业务、数据的服务器（包括其操作系统和数据库）

业务相关

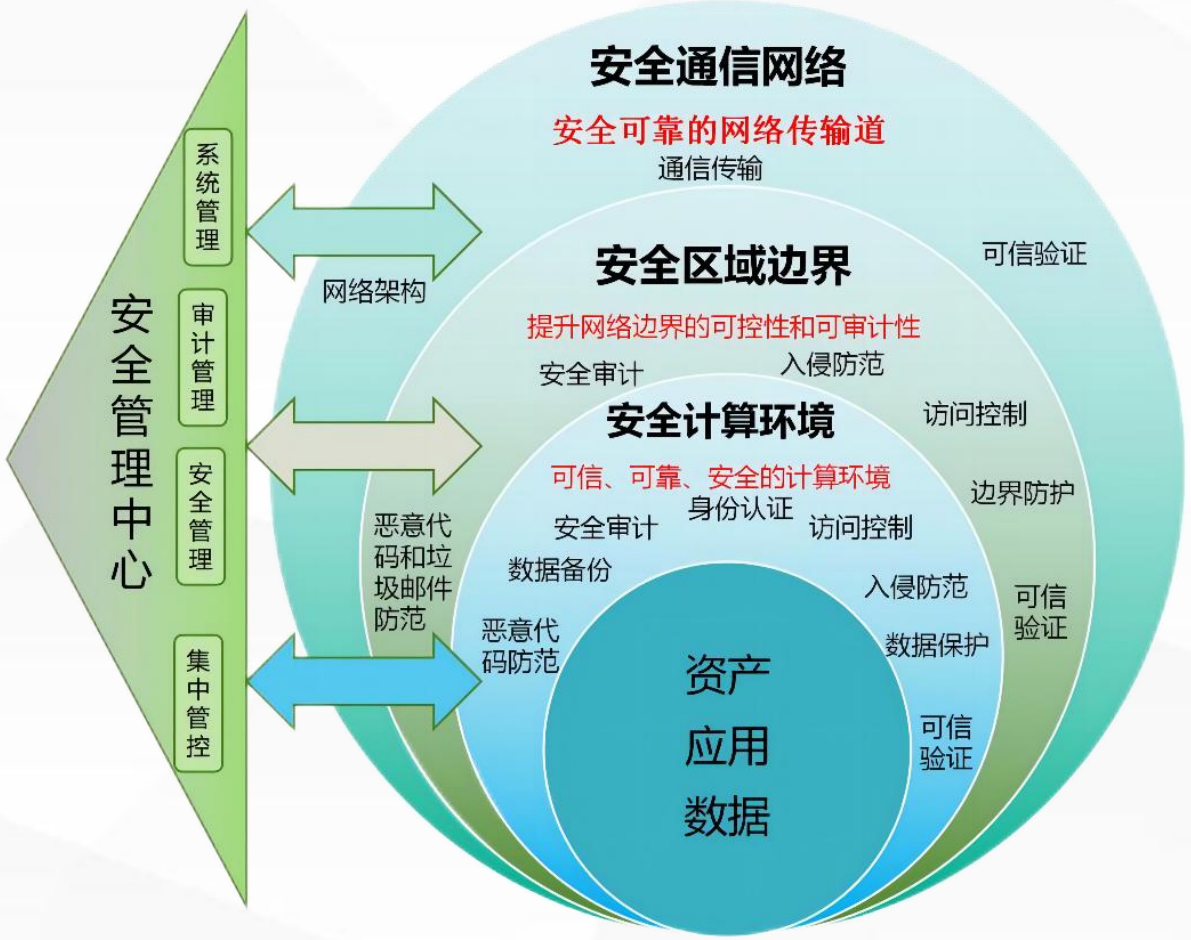
- 能够代表被测系统主要使命的业务应用
- 重要管理终端
- 客户端软件、App、小程序、公众号等

人员与管理

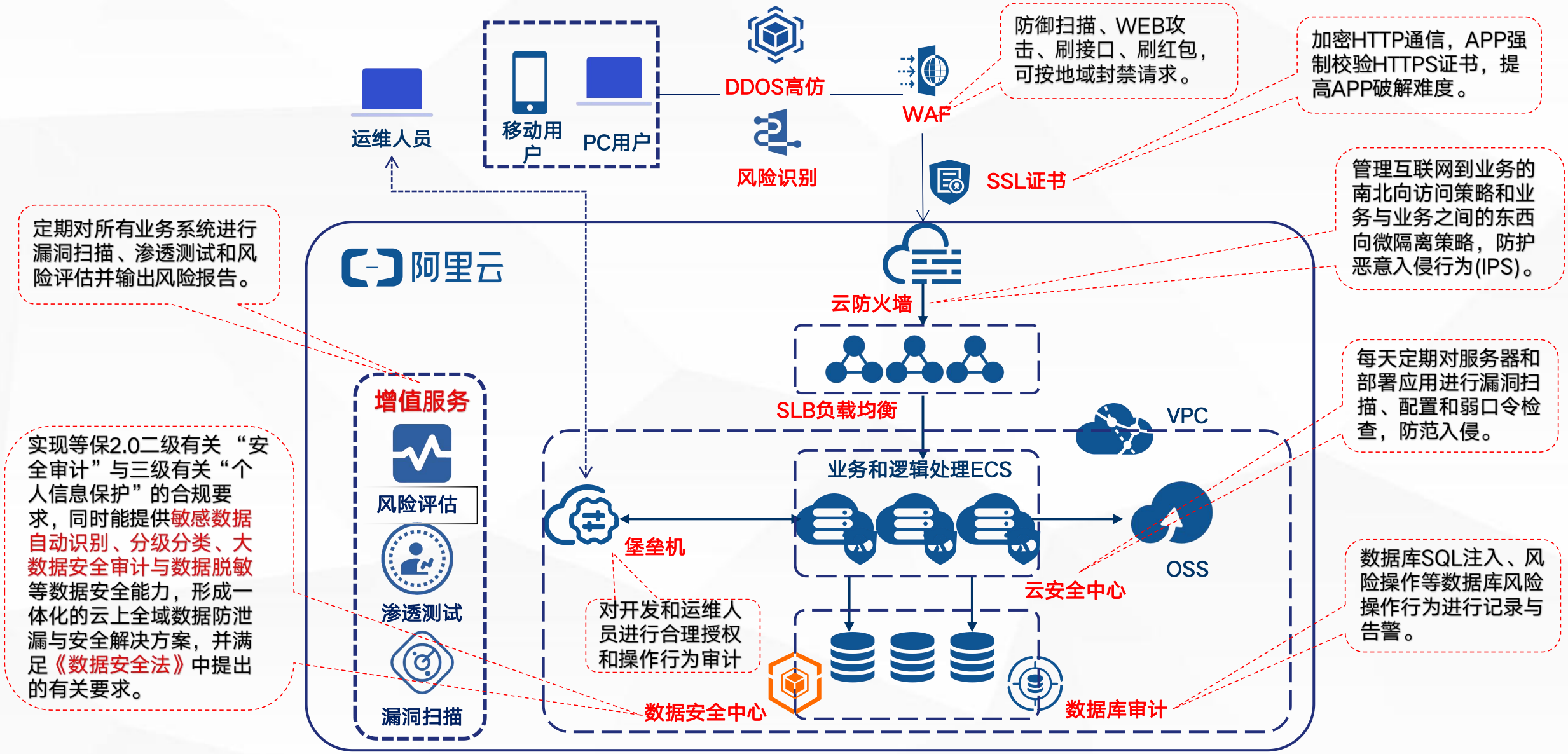
- 信息安全主管人员、各方面的负责人员
- 涉及到信息系统安全的所有管理制度和记录

等保2.0整改建设思路·纵深防御体系

通过”一个中心，三重防护”的总体建设思路，针对等级保护对象构建安全通信网络防护，安全区域边界防护、安全计算环境防护多重防护机制，在整体上保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证等级保护对象整体的安全保护能力。



一站式等保测评 · 技术安全防护（三级）



一站式等保测评·安全产品建设清单（三级）

序号	安全产品名称	服务介绍	备注	必要性
1	WEB应用防火墙	保护您的web业务免受常见WEB攻击，诸如SQL注入、XSS跨站脚本等常见应用攻击，同时也可对CC影响网站可用性的攻击进行防护。	满足等保2.0应用安全、网络安全、网页防篡改等安全要求	必选
2	云防火墙	通过流量可视化技术，为企业云上应用提供便捷、易用的网络访问控制服务。	满足等保2.0网络安全、IPS入侵防御等安全要求	必选
3	云安全中心	专为企业安全运维团队打造，结合云主机和全网的威胁情报，利用机器学习，进行安全大数据分析的威胁检测平台。可让客户全面、快速、准确地感知过去、现在、未来的安全威胁。	满足等保2.0，主机安全、恶意代码防御等安全要求	必选
4	云堡垒机	主要包括账号管理、认证管理、权限管理、审计管理、自动化运维等功能，解决系统账号复用、运维权限混乱、运维过程不透明等IT运维难题。	满足等保2.0身份鉴别、访问控制、安全审计等审计要求	必选
5	数据库审计	支持RDS云数据库、ECS自建数据库的操作行为审计，符合等级保护三级标准，帮助用户满足合规性要求。	满足等保2.0数据安全、安全审计要求	必选
6	CA证书	通过阿里云证书服务购买受信任CA认证中心颁发的数字证书，然后部署在云平台网站，将HTTP访问转换成HTTPS，提供认证加密功能。	满足等保2.0应用及通信安全、数据完整性和数据保密性的要求	必选
7	日志服务	提供系统及访问日志集中存储至少180天，并可分析日志和生产报表展示	满足等保2.0日志审计要求存储不少于180天	必选
8	数据备份服务	实现对各类数据库进行实时异地备份功能	满足等保2.0数据异地备份要求	必选
9	VPC/安全组	阿里云专有网络，可以实现VLAN级隔离，并自定义IP地址分配；状态检测防火墙，对不同的安全组进行四层访问控制。免费	满足等保2.0边界安全、VLAN隔离	必选
10	云监控	对服务器内存、CPU、磁盘、带宽等进行实时监控，并提供多样式告警	满足等保2.0对重要服务器的运行性能进行监视，并自动告警	必选

一站式等保测评·安全管理制度建设

安全管理制度

- 制定安全策略
- 建立安全管理制度
- 专人负责制定和发布管理
- 定期评审和修订管理制度

安全管理机构

- 设立相应领导、管理、审计、运维机构和岗位
- 配备系统管理、审计管理和安全管理员
- 明确授权和审批事项和制度
- 加强内部和外部安全专家沟通协作
- 定期审核和检查安全策略和安全管理制度

安全管理人员

- 考核录用人员专业技能，签署保密协议。
- 离岗人员及时回收权限、证照等
- 加强安全意识和安全技能教育培训
- 定期进行安全技术考核
- 外部人员访问管理

安全建设管理

- 等保定级和备案
- 安全方案设计
- 安全产品采购和使用
- 自主和外包软件开发管理
- 安全保护工程实施管理
- 安全防护测试验收
- 系统验收交付
- 定期等保测评
- 监督、评审和审核安全服务提供商

安全运维管理

- 运行环境管理
- 被保护资产管理
- 信息存储介质管理
- 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
- 系统、变更配置和密码管理
- 备份与恢复管理
- 安全事件和应急预案管理
- 外包运维管理

一站式等保测评 · 合格标准

等保2.0测评结论:优、 良、中、差(四个等级)。其中测评结论"差"的判别依据是被测对象中存在安全问题,而且会导致被测对象面临高等级安全风险,或被测对象综合得分低于70分。

优	被测对象中存在安全问题,但不会导致被测对象面临中、高等级安全风险,且系统综合得分90分以上(含90分)。
良	被测对象中存在安全问题,但不会导致被测对象面临高等级安全风险,且系统综合得分80分以上 (含80分)。
中	被测对象中存在安全问题,但不会导致被测对象面临高等级安全风险,且系统综合得分70分以上 (含70分)。
差	被测对象中存在安全问题,而且会导致被测对象面临高等级安全风险,或被测对象综合得分低于70分。

一站式等保测评 · 合格交付物

网络安全等级保护定级回执

单位名称	管理咨询有限公司
系统名称	学习平台
系统级别	3
备案证号	0106 0200
时间	2022年11月15日

提交网络安全等级测评报告回执

单位名称	技股份有限公司
系统名称	学习平台
系统级别	三
备案证号	112 02000
时间	2022年11月07日

信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，科技股份有限公司单位的：

第三级学习平台系统

予以备案。

证书编号：0006

中华人民共和国公安部监制

备案公安机关公章
2022年11月08日

报告编号：11010513629-22001-22-0032-01

网络安全等级保护
系统等级测评报告

被测单位：限公司
测评单位：北京息化测评技术有限公司
报告时间：2022 年 04 月 28 日

等级测评结论

测评结论和综合得分			
被测对象名称	系统	安全保护等级	第三级（S3A3）
等级保护对象形态	☑传统 IT 系统 ☑云计算 ☑采用移动互联技术的系统 ☐物联网 ☐工业控制系统 ☐大数据 ☐其他系统		
被测对象描述	系统的业务流程制定和业务操作由有限公司负责，系统的所有设备和设施的运行、维护和管理支有限公司负责，所有限公司系统的责任部门，有限公司是该系统的安全责任单位，该系限公司的定级对象。		
测评工作描述	本次安全测评的范围主要包括的物理环境、主机、网络、业务、应用系统、安全管理制度和人员等等。安全测评通过静态评估、现场测试，综合评估等相关环节和阶段，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个方面，对该云平台系统进行综合测评。		
等级测评结论	良	综合得分	91.40

深圳市网络安全等级保护
测评结果通知书

编 号：SZCP20220617

依据《信息安全等级保护管理办法》等有关规定，技有限公司已按规定开展2022年度等级保护测评工作。

特此通知

测评系统信息：
1、平台系统，三级，良。

深圳市信息安全等级保护工作协调领导小组办公室
2022 年 07 月 08 日

测评机构：发展有限公司
测评日期：2022.01.18-2022.06.21

一站式等保测评服务 · 全国化

业务全国化

目前已经可以在16个省或直辖市开展等保一站式服务，帮助企业顺利通过等保合规要求，联手了30多个等保测评单位，提供全方位的一站式等保服务。

覆盖广&专业化

等保合规解决方案覆盖阿里云、华为云、腾讯云、京东云、平安云、政务云、金融云等公有云平台，还涉及线下系统等保；具有专业的信息安全技术团队，丰富的项目实战经验，极具行业竞争力。

服务优势

业务与资源全国化

业务覆盖16省或直辖市，联手60+测评单位提供全方位的一站式安全合规服务，缩短企业60%的整改及测评时间，大大提高通过效率。

专业技术服务团队

具备专业的信息安全技术团队，可提供1对1专家服务，实现咨询+测评+整改的端到端全流程覆盖，协助企业了解自身安全合规问题。

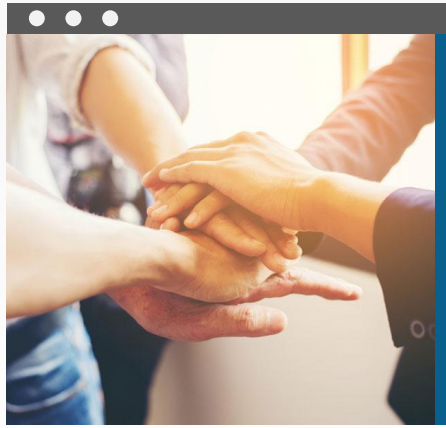
5000+安全项目经验

可提供覆盖云上云下的安全合规解决方案，包括阿里云、华为云、腾讯云、京东云、平安云、政务云、金融云等，涵盖了政府、银行、保险、房地产、医疗、教育、物流、互联网等多个领域。

行业安全支撑单位

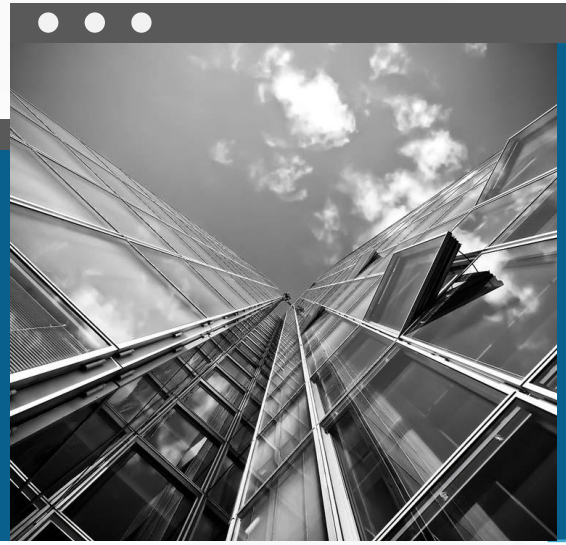
政企长期的“护网”支撑单位，通管局、信通院、网安大队常驻安全支撑单位，国家级攻防演练大赛前10%，安服团队在58同城、vivo等网站安全应急响应中心（SRC）中名列前茅。

41 客户收益



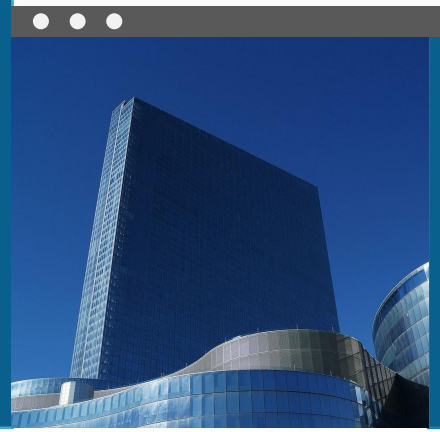
高效

履行法律法规



100%

安全合规通过率



低成本

构建安全能力

满足法规监管政策要求

降低企业运营过程中因网络系统、APP应用、业务服务等安全问题而被监管部门通报及业务下架的法律风险，避免经济/名誉损失。

保障业务稳定安全运行

提供全生命周期的安全合规解决方案，以最低成本构建企业安全体系，形成安全纵深防御，让企业合理安排资源、预算，提高安全管控效率。

全面提高企业安全意识

通过合规化报告、定级备案程序等，全面审视企业自身网络安全潜在风险，并可用作企业IT人员安全培训，提升企业安全意识。

04

典型场景和增值服务

覆盖行业范围广

支撑5000+企业安全合规

一站式等保服务·典型场景（阿里云三级）

青莲网络 QINGLIAN NETWORK

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》和《信息安全等级保护管理办法》中均明确规定金融、电力、广电、教育、医疗等行业信息系统运营、使用单位应当按照网络安全等级保护制度要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。

客户痛点

1.无专人主导：中小型客户的IT人员配备十分有限，专职的安全技术人员缺失；
2.采购成本高：等保建设涉及的安全产品种类繁多，其中设备成本、时间成本和沟通成本都是客户不能承受之重；
3. 专业涉及广：缺少了解操作系统、数据库、应用安全、网络信息安全、系统架构图等运维和执行的专业技术；

青莲解决方案

1.安全通信网络：重要网络区域与其他网络区域之间应采取可靠的技术隔离手段(云防火墙）

2.安全区域边界：（1）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）

（2）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）

（3）应对用户进行身份鉴别、访问控制、运维审计（堡垒机）

（4）应启用安全审计功能，数据进行安全审计（数据库审计）

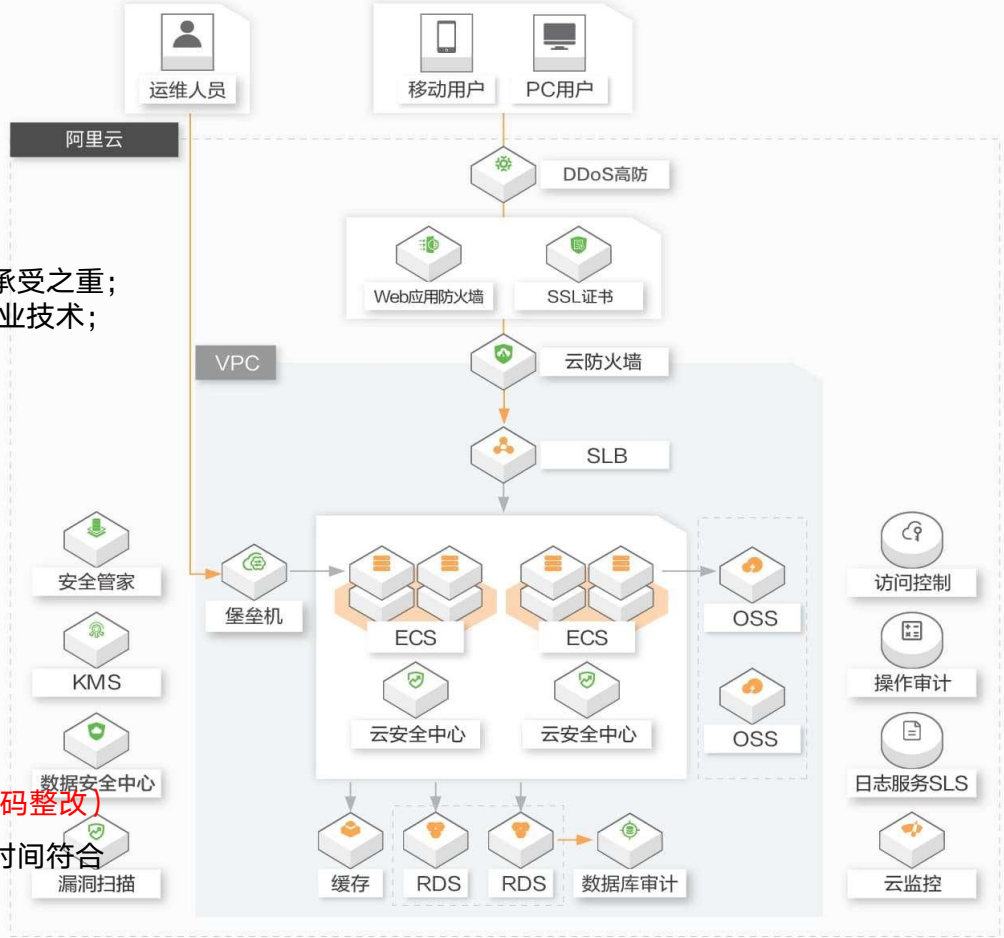
3.安全计算环境：（1）应满足数据完整性和数据保密性的要求（SSL 证书）

（2）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（渗透测试）

(3）支持双因子/双向认证，支持国密/国际算法，支持身份/权限认证（辅助应用代码整改）

4.安全管理中心：应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求（记录至少保存6个月及以上）；（日志服务）

5.安全管理建设：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理（青莲提供全套）



典型客户：

香雪制药 | 粮达网 Liangdawang.com | BIOSTIME 合生元 | 广大医院 | 省省回头车 省时 省心 省钱 | 中港通GPS 视频监控专家 | DST 地上铁 新能源运营服务平台

一站式等保服务·典型场景（华为云三级）

青莲网络 QINGLIAN NETWORK

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行相关安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

客户痛点

1.无精准的解决方案：依据差距的问题单，比较难设计出精确的整改方案解决方法；
2.整改规范不清楚：整改到什么水平，完成到怎样的程度才算可以，难以掌握，欠缺具体指导；
3.管理方案定偏：在信息化安全管理方案这方面，90%以上企业是缺少的。需编上百份有关制度文档；

青莲解决方案

1.安全通信网络：重要网络区域与其他网络区域之间应采取可靠的技术隔离手段(云防火墙）

2.安全区域边界：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）

3.安全计算环境：（1）应满足数据完整性和数据保密性的要求、数据安全审计（SSL 证书和数据库审计）

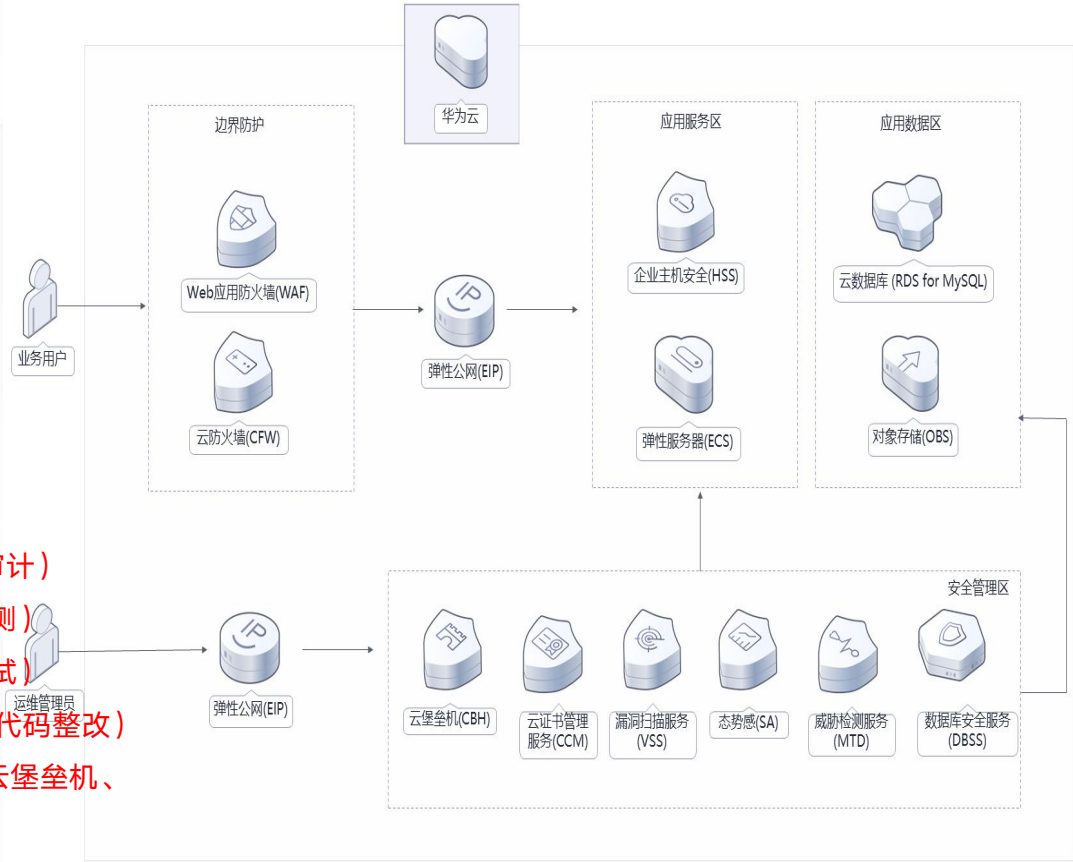
（2）应能对各类安全事件和新型攻击进行分析、识别、报警（主机安全和威胁检测）

（3）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（渗透漏扫测试）

(4）支持双因子/双向认证，支持国密/国际算法，支持身份/权限认证（辅助应用代码整改）

4.安全管理中心：集中管控（态势感知），集中监测（云监控），身份鉴别、访问控制、运维审计（云堡垒机、云审计和云日志），数据备份管理（本地备份CBR、异地备份OBS)

5.安全管理建设：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理（青莲提供全套）



典型客户：

星海音乐厅 XINGHAI CONCERT HALL

融数联智

大白互联 DABBY INTERNET TECHNOLOGY

广东省出版集团数字出版有限公司 数字创造出版未来

蜘点集团

一站式等保服务·典型场景（腾讯云三级）

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行相关安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

客户痛点

1.无精准的解决方案：依据差距的问题单，比较难设计出精确的整改方案解决方法；
2.整改规范不清楚：整改到什么水平，完成到怎样的程度才算可以，难以掌握，欠缺具体指导；
3.管理方案定偏：在信息化安全管理方案这方面，90%以上企业是缺少的。需编上百份有关制度文档；

青莲解决方案

1.安全通信网络：重要网络区域与其他网络区域之间应采取可靠的技术隔离手段(云防火墙）

2.安全区域边界：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）

3.安全计算环境：（1）应满足数据完整性和数据保密性的要求、数据安全审计（SSL 证书和数据安全审计）

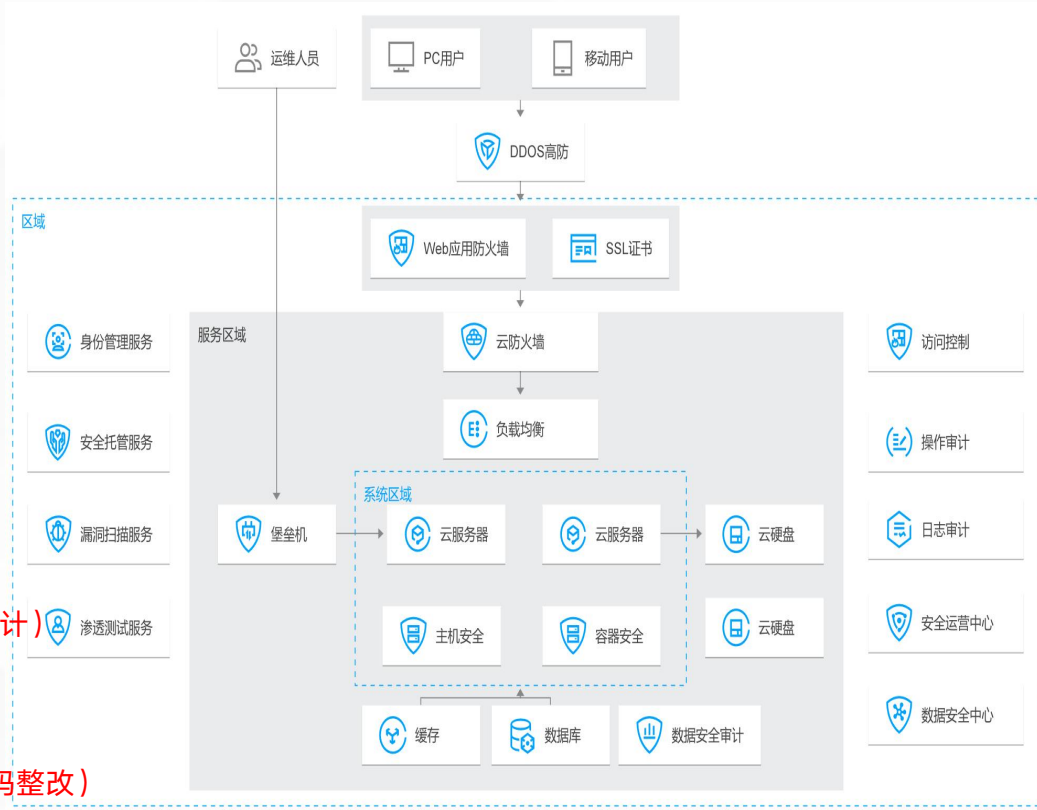
（2）应能对各类安全事件和新型攻击进行分析、识别、报警（主机安全）

（3）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（渗透漏扫测试）

(4）支持双因子/双向认证，支持国密/国际算法，支持身份/权限认证（辅助应用代码整改）

4.安全管理中心：集中管控、集中监测（安全运营中心），身份鉴别、访问控制、运维审计（堡垒机、操作审计和日志审计），数据备份管理（本地备份COS、异地备份DBS)

5.安全管理建设：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理（青莲提供全套）



典型客户：

国工智保 | 银小保 保险连接价值 | 爱的番茄 TOMATO OF LOVE | 翼卡车联网 ECAR TELEMATICS | CHC 春华健康 Chunhua Health | 虎硕教育 HUSHUO EDUCATION 让学习简单快乐

一站式等保服务 · 典型场景（政务云）

青莲网络 QINGLIAN NETWORK

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行相关安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

客户痛点

1.无精准的解决方案：依据差距的问题单，比较难设计出精确的整改方案解决方法；
2.信息安全技术缺失：无专业负责安全防护设计和落地实施的专业技术人才；
3.运维团队缺失：政府行业因自身的局限性，大都不会自建运维团队，企业的运维通常与运营商合作，传统运营商却缺少对云数据中心的运维经验；

青莲解决方案

1.安全物理环境：政务云平台本身已通过等保三级认证（默认已合规）

2.安全通信网络：重要网络区域与其他网络区域之间应采取可靠的技术隔离手段

3.安全区域边界：应具有提供访问控制、边界防护、入侵防范等安全机制（统一由政务云平台搭建的安全池提供安全防护）

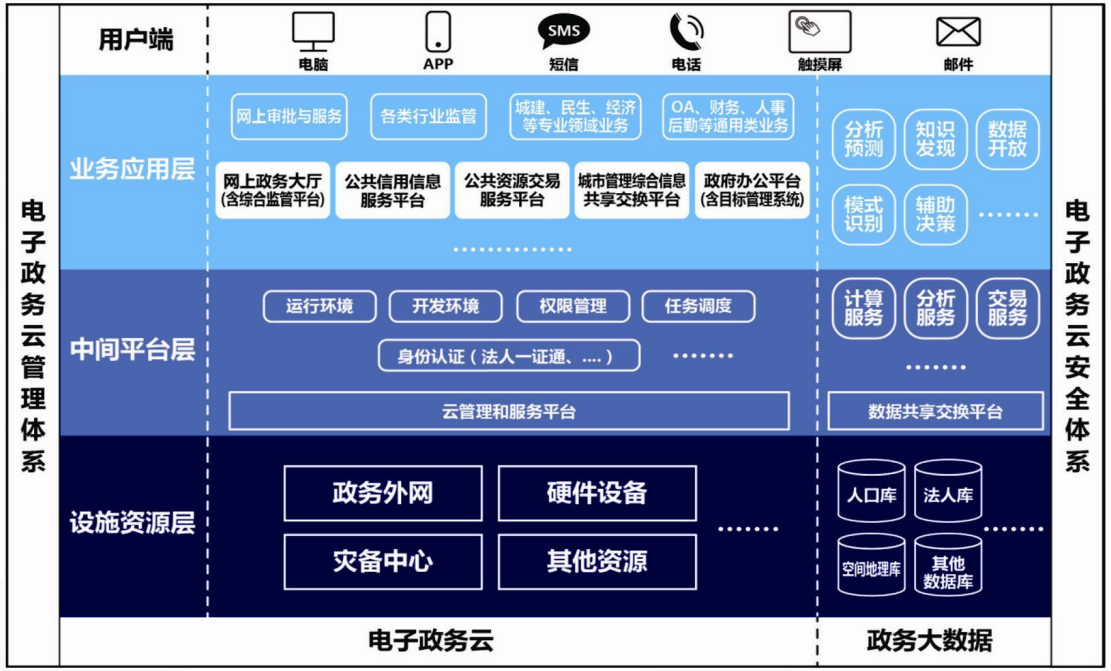
4.安全计算环境：（1）应满足数据完整性和数据保密性的要求、数据安全审计（SSL 证书和数据安全审计）

（2）应能对各类安全事件和新型攻击进行分析、识别、报警（企业版杀毒软件）

（3）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（渗透漏扫测试）

(4）支持双因子/双向认证，支持国密/国际算法，支持身份/权限认证（辅助用户应用代码整改）

5.安全管理建设：[illegible]



市级电子政务云架构图

典型客户：

佛山市禅城区民政局 FoShan Shi ChanCheng Qu Min Zheng Ju

大同市博物馆 DATONG MUSEUM

中山市博物馆

东城区静态交通智慧综合管理系统

广州市林业和园林局 Bureau of Forestry and Landscaping of Guangzhou Municipality

一站式等保服务·典型客户（混合云三级）

青莲网络 QINGLIAN NETWORK

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》第二十一条：国家实行网络安全等级保护制度；以及企业自身内部安全要求。

客户痛点

1.合规难：信息安全合规要求法律法规层出不穷，企业不知如何才能准确合规规避风险；
2.整改难：混合云架构体系，等保认证过程中即考量线下机房安全防护建设又涉及公有云安全防护，涉及整改范围广，专业知识强，企业团队建设很难统一兼顾；
3.运维难：系统架构复杂，维护难度大，专业技术人员短缺，对系统故障问题定位难、时效难以保证；运维中出现复杂的问题，不能及时处理，甚至无法处理。

青莲解决方案

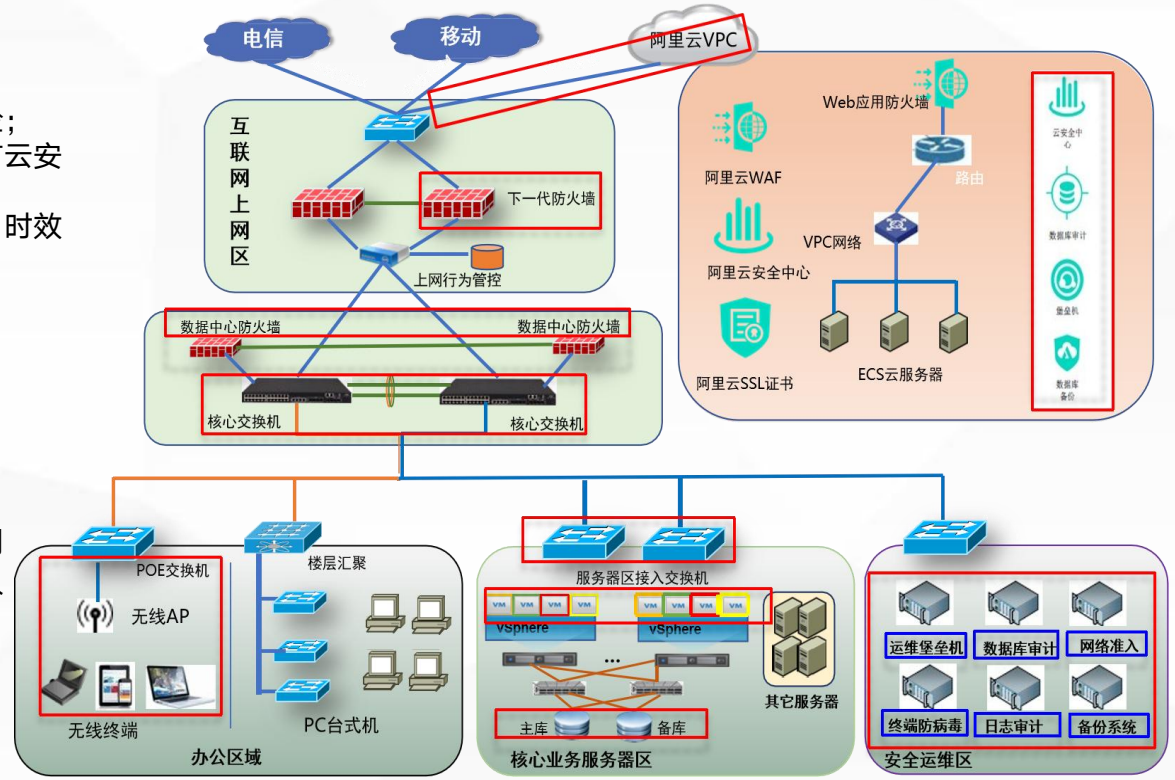
1.安全建设：针对客户云上系统安全现状，进行重新安全架构设计，部署了waf、云安全中心、SSL证书、堡垒机和数据库审计等安全设备；线下核心设备进行冗余部署（例如下一代防火墙、核心交换机及数据库备份等）

2.安全通信网络：重要网络区域与其他网络区域之间部署了下一代防火墙进行访问控制

3.安全区域边界：新建安全运维区对核心业务、办公网络、无线网络等区域进行分区分域，建立精细的访问控制、边界防护、入侵防范等防护措施；

4.安全计算环境：通过漏洞扫描和渗透测试检测应用系统本身安全现状并指导应用本身进行安全加固；

5.安全管理建设：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理（青莲提供全套）



典型客户：

花都供水　大白互联 DABBY INTERNET TECHNOLOGY　海伦堡地产 HELENBERGH ESTATE 让家重新想象　华能海门电厂

一站式等保服务·典型场景（线下机房）

青莲网络 QINGLIAN NETWORK

项目背景

国家法律法规及行业监管政策均要求企业开展等级保护工作，在《网络安全法》第二十一条：国家实行网络安全等级保护制度；以及企业自身内部安全要求。

客户痛点

1.缺少专业人员：单位未装备专业的信息安全专职人员，对网络安全等级保护一头雾水，更不知道如何开展；
2.难度大、周期长：很多层面的整改，比如主机、数据库、网络等层面的整改都需要专业的技术人员，而且整改期间会不可避免的影响业务运行，不愿整改迟迟不能验收；
3.测评机会有限：测评单位只给予一次差距测评和一次验收测评，某些测评单位会给予附加的1~2次复测待遇，但会存在二次收费的情况；

青莲解决方案

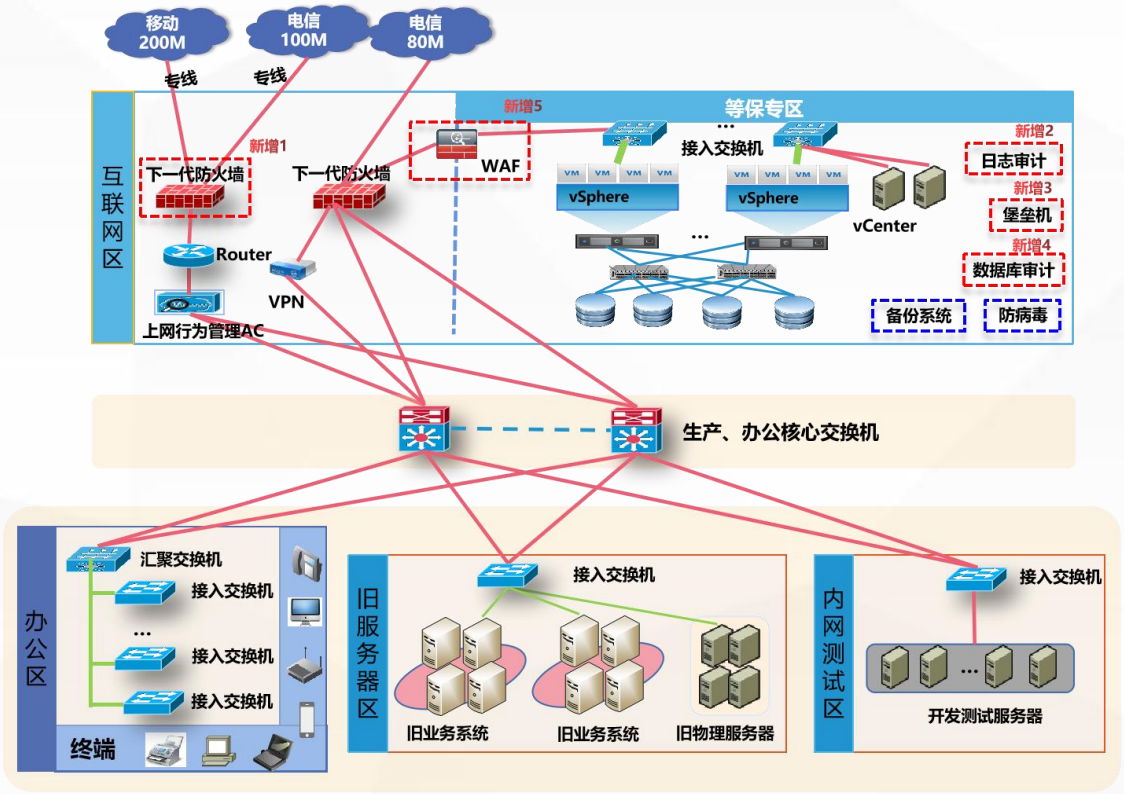
1.安全建设：针对客户云上系统安全现状，进行重新安全架构设计，核心业务区部署了waf、下一代防火墙、日志审计、堡垒机、数据库审计等防护设备

2.安全通信网络：重要网络区域与其他网络区域之间部署下一代防火墙进行隔离

3.安全区域边界：对核心业务区、办公区、内网测试区及互联网区等区域进行分区分域，建立精细的访问控制、边界防护、入侵防范等防护措施；

4.安全计算环境：通过漏洞扫描和渗透测试检测应用系统本身安全现状并指导应用本身进行安全加固；

5.安全管理建设：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理（青莲提供全套）



典型客户：

南方醫院 NANFANG HOSPITAL
广州港集团 GUANGZHOU PORT GROUP
R&F 富力地产 R&F PROPERTIES
中交第四航务工程勘察设计院有限公司 CCCC-FHDI ENGINEERING CO.,LTD.
东风 HONDA

一站式等保服务 · 典型行业客户

青莲网络 QINGLIAN NETWORK

为客户提供多场景的等保合规安全解决方案，满足多行业业务诉求，快速省心等保合规

01 政府/地产行业

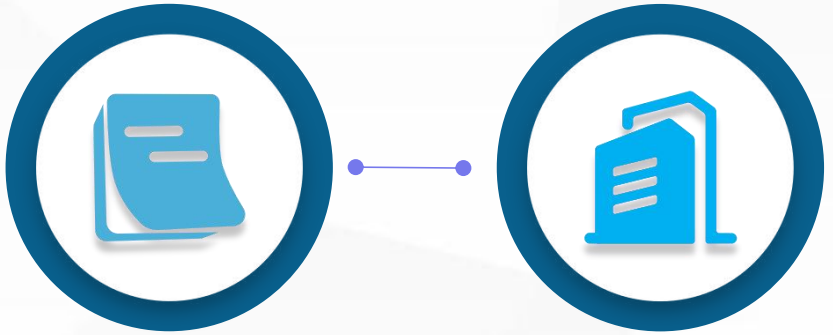
广州市林业局、佛山禅城区民政局、佛山地铁集团、广州港集团、广州市政设计工程研究院、中石化第五建设、润建股份、富力地产、海伦堡地产、越秀地产等

02 医疗行业

南方医院、广大医院、佛山第一人民医院、清远/中山第三人民医院、云康集团、华银康集团、香雪制药、大参林等

03 教育行业

合景教育集团、华文教育、中正教育、恺睿教育、华翰教育、耕子教育、十牛教育、民生教育集团、深圳三合同创、虎硕教育、智趣猴教育等



04 金融行业

广州金融发展中心、明珠数科、金控征信、广州民间金融街、国工智保、银小保、银安科技、联华国际保险等

05 新闻传媒

南方传媒、广东音像教材出版社、触电传媒、羊城晚报社、时代传媒、南方出版传媒股份等

06 交通行业

省省回头车、货多多、中港通、地上铁、翼卡车联网、湖州万鑫国际货运、赛威智能车联网、江得利智能卫星定位云平台等

青莲增值服务

青莲网络 QINGLIAN NETWORK

ITQM质量管理

满足SLA要求的云代维服务体系
咨询规划→迁移→运维的全栈运维服务
省心版：云上资产的管理员
放心版：基于ITIL的最佳管理实践
安心版：参照cobit一般控制规范

- 多地域支持
- 灵活敏捷
- 全栈技术积累
- 一站式服务
- 成本优化

云专项服务

成本优化服务
容器集群搭建
全栈应用监控
堡垒机部署
云容灾服务
日志发现服务
数据保护验证
数据库优化

- 行业内领先荣获ISO27001
- 信息系统建设和服务能力评估CS2级别
- CCRC信息安全服务资质认证

云原生服务

云原生计算部署
CI/CD流水线
应用容器化改造
跟踪和可视化
云原生监控
云原生安全合规
容器编排和管理

- 高效管理与调度
- 高拓展高兼容
- 弹性使用
- 安全自主可控

安全合规服务

等保一站式
通保一站式
安全风险评估
APP隐私合规
云安全建设
云安全架构设计
渗透漏扫测试
攻防演练

- 覆盖全国
- 专业团队
- 高通过率
- 安全保密
- 一站式服务
- 风险可控

5分钟响应　7*24服务时效性　99.5%服务可用率　降低1亿TCO服务效能

青莲网络
QINGLIAN NETWORK

谢谢观看