环宇数通
sotote.com

IT系统

等级保护

安全

等保一体化服务

2024年2月

前 言

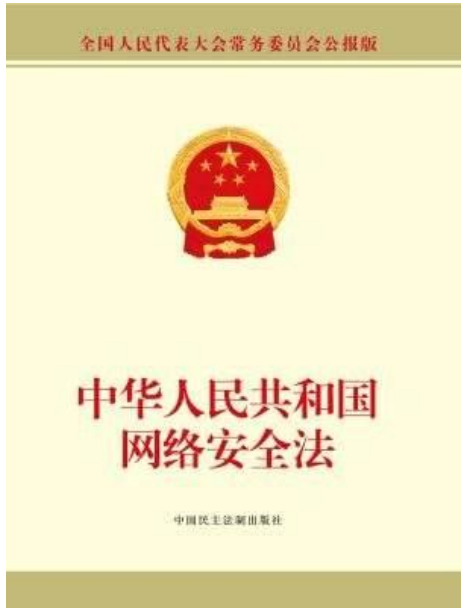
等级保护经过十多年的发展，依据《中华人民共和国网络安全法》，已经成为我国网络安全行业一项重要的制度和标准。国内企事业单位进行信息系统和网络安全建设，都会以等级保护相关标准作为重要参照依据。

目前市场上提供等级保护测评、安全建设服务的供应商众多，服务水平良莠不齐。提供一站式、低成本、高效率的一体化等保安全服务，将是企业对网络安全服务的必然要求，也是必然选择。

环宇数通
sotote.com

目 录

网络安全法



中华人民共和国主席令

第五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

中华人民共和国主席　习近平

2016年11月7日

国内首部：《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础法律。

符合趋势：《网络安全法》符合全球应对网络安全威胁挑战的大趋势，为各国之间在网络安全领域加强合作奠定了法律和能力方面的基础。

全面覆盖：中国的网络安全法立足全球视野，全面覆盖“国际法层面”、“国家安全层面”、“社会安全层面”、“企业个人安全层面”的网络安全内容。

网络安全法关键点

- 等级保护
- 关键信息基础设施
- 个人信息保护
- 敏感信息保护
- 实名制
- 法律责任

等保概念及要点

基本概念

- 基本概念
  - ✓ 《信息安全等级保护管理办法》：国家通过制定统一的信息安全等级保护**管理规范和技术标准**，组织公民、法人和其他组织对信息系统**分等级实行安全保护**，对等级保护工作的实施进行**监督、管理**。
- 法律要求
  - ✓ **《中华人民共和国网络安全法》（2017.6.1）**：“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”。
  - ✓ 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）规定：要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。
- 地位和作用
  - ✓ 国家信息安全保障工作的基本制度、基本国策；开展信息安全工作的基本方法；促进信息化、维护国家信息安全的根本保障。

关注要点

- 网络安全等级保护的**适用范围**：**中华人民共和国境内**的计算机信息系统
- 网络安全等级保护的**主管单位**：**公安机关**负责网络安全等级保护工作的监督、检查、指导
- **监管力度**：**二级及以上**系统均纳入公安机关监管范围，**其中二级系统至少两年测评一次，三级系统至少每年测评一次，四级系统至少半年测评一次，五级系统由国家专门部门随时保护检查。**
- **三级系统对安全产品主要要求**：**境内独立法人、自主知识产权、信息安全产品认证证书**
- **严重性**：发现不符合网络安全等级保护有关管理规范和技术标准要求，公安机关应当通知其运营使用单位限期整改，并发送**《网络安全等级保护限期整改通知书》**，逾期不改正的，给予警告并向其上级主管部门通报；在限期内拒不改进的，由公安机关处以警告或者**停机整顿**

等保系统分级

信息系统的安全保护等级分为以下五级，一至五级等级逐级增高：

第一级为用户自主保护级，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。在损坏后能恢复部分功能。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。
第二级为系统审计保护级，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。在损坏后能够在一段时间内恢复部分功能。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。
第三级为安全标记保护级，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损害。在损坏后能够较快恢复绝大部分功能。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。
第四级为结构化保护级，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。在损坏后能够迅速恢复所有功能。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。
第五级为访问验证保护级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查和保护。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

安全等级	损害后恢复能力
第一级	恢复部分功能
第二级	一段时间后恢复部分功能
第三级	较快恢复绝大部分功能
第四级	迅速恢复所有功能
第五级	略

相关法律及标准规范

《中华人民共和国网络安全法》

《信息安全技术网络安全等级保护实施指南》GB/T25058-2019

《信息安全技术网络安全等级保护基本要求》 GB/T22239-2019

《信息安全技术 网络安全事件应急演练指南》GB/T 38645-2020

《信息安全技术网络安全等级保护安全设计技术要求》GBT25070-2019

《信息系统安全等级保护测评要求》GB/T28448-2019

《计算机信息系统安全保护等级划分准则》（GB/T17859-1999）

《信息安全技术_信息系统安全等级保护定级指南》（GBT22240-2008）

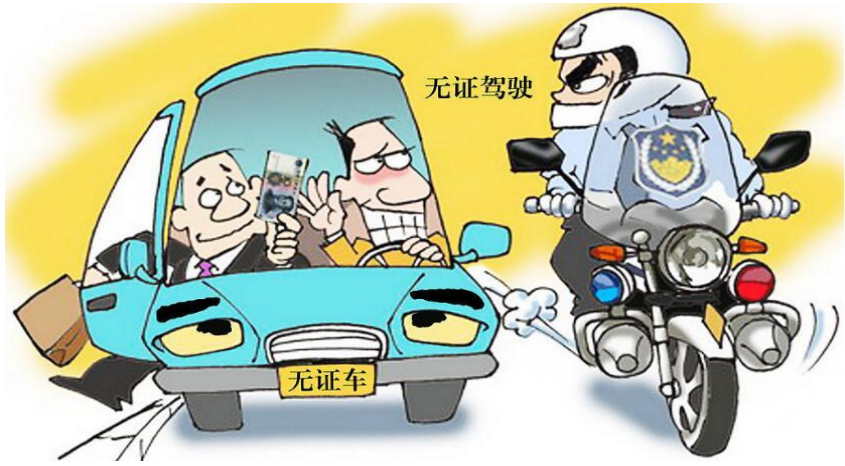
《信息技术安全技术信息安全管理体系要求》（GB/T22080-2008）

《信息技术安全技术信息安全管理实用规则》（GB/T22081-2008）

《信息技术安全技术信息技术安全性评估准则》（GB/T18336-2001）

《信息安全等级保护整改指南》

等保必要性



“等级保护定级备案”--就好比驾驶员开车要先考取驾照！

答：《中华人民共和国网络安全法》明确规定境内信息系统运营者、使用单位应当按照网络安全等级保护制度的要求，履行网络安全保护义务，如果拒不履行，视为违法。

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并给予警告；拒不改正或者危害网络安全的，处一万元以上十万元以下罚款，直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施经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并给予警告；拒不改正或者危害网络安全的，处十万元以上一百万元以下罚款，直接负责的主管人员处一万元以上十万元以下罚款。

等级保护2. 0

- 2019年5月份发布，12月强制执行
- 相对于等保1.0：范围更广（新增加了云计算、大数据、物联网相关扩展要求）；要求更严格（1.0中三级要求60分基本符合达标，2.0为70分）

等保全流程阶段

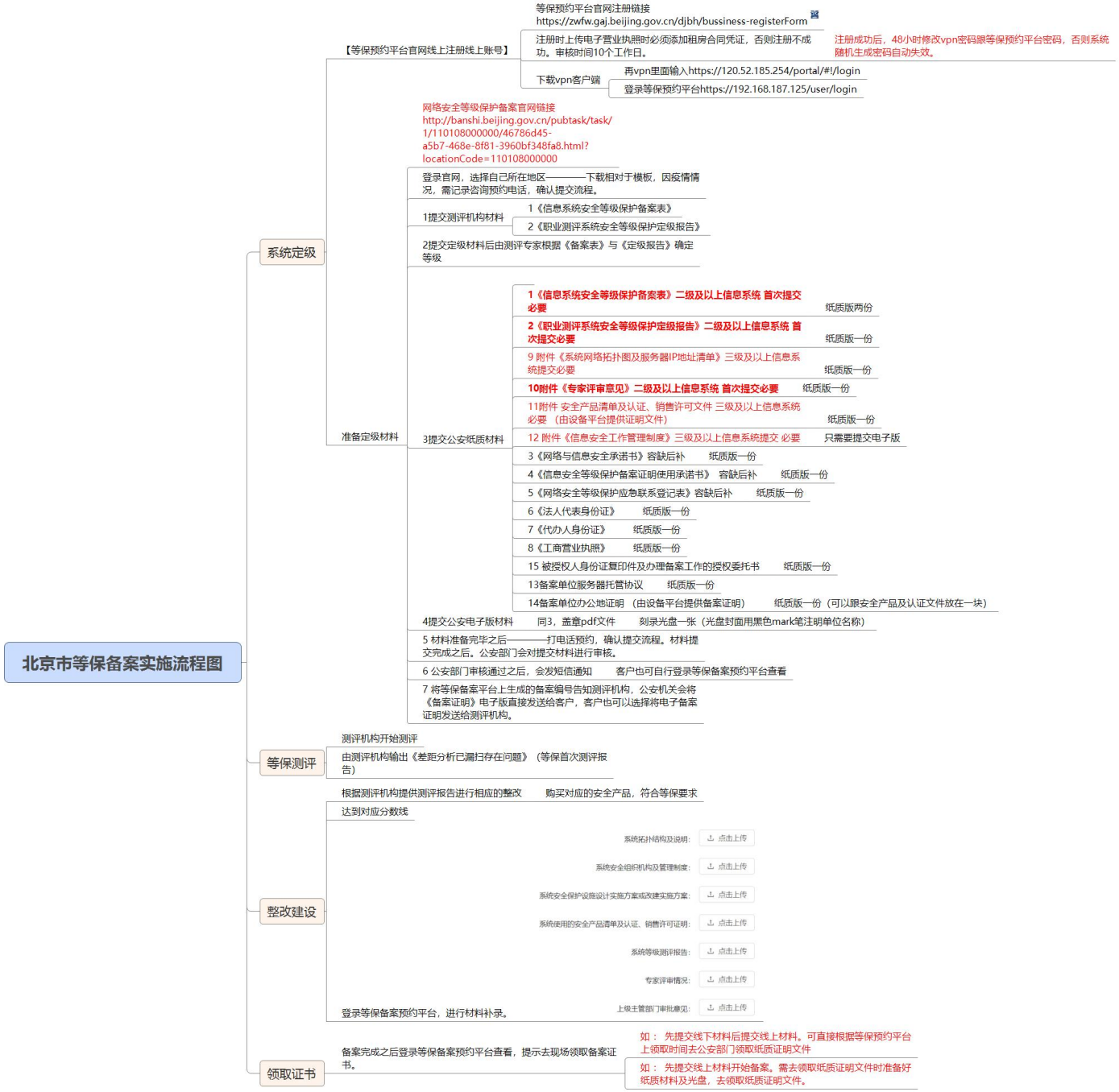
环宇数通
sotote.com

目 录

等保一体化服务

定级备案	安全建设	差距分析	整改实施	等级测评	安全运维
确立定级对象，准备备案材料；定级材料需要经过专家评审；将专家评审后的定级备案材料递交给属地公安网络监察部门进行审核、备案，并获取电子备案证明。	根据系统所定级别，进行必要的安全方案建设包括：安全架构设计、安全产品选型、漏洞修复、制定安全管理制度等。	结合分析结果与定级结果，从技术与管理两个方面基于信息系统等级标准对信息系统进行设计，给出合理的整改建。	根据整改方案进行符合信息安全认证标准的安全产品配置优化，以及优化安全管理制度规则。	测评机构完成等级保护测评，出具系统等级保护测评报告；将测评报告递交给属地公安网络监察部门，取得纸介质等保备案证明。	根据系统定级标准定期进行测评工作；保持系统网络等级保护的安全能力；接受公安网络监察部门的不定期安全检查。

等保实施流程

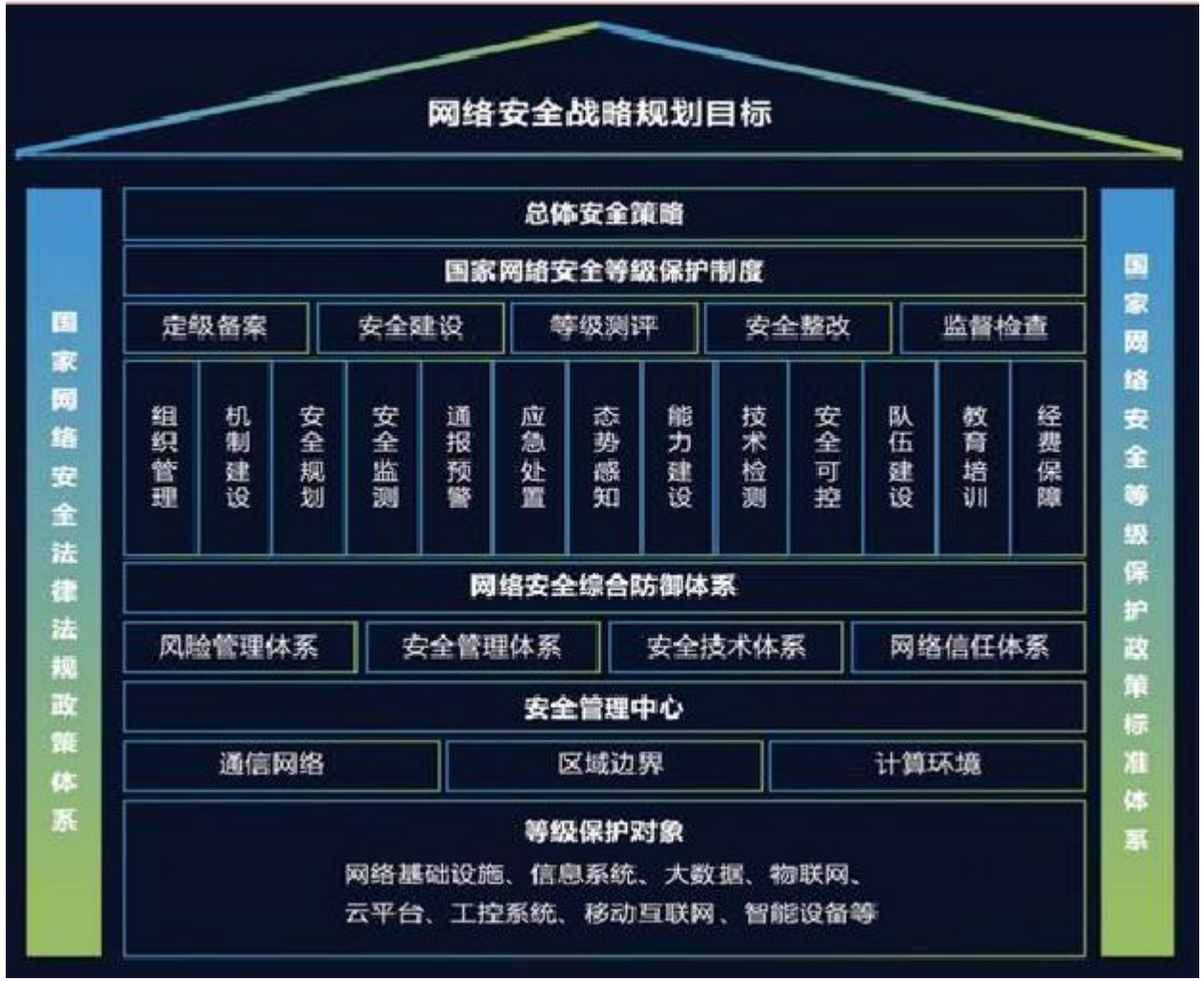

北京市等保备案实施流程图
系统定级
【等保预约平台官网线上注册线上账号】
等保预约平台官网注册链接
https://zwfw.gaj.beijing.gov.cn/djbh/bussiness-registerForm
注册时上传电子营业执照时必须添加租房合同凭证，否则注册不成功。审核时间10个工作日。
注册成功后，48小时修改vpn密码跟等保预约平台密码，否则系统随机生成密码自动失效。
下载vpn客户端
再vpn里面输入https://120.52.185.254/portal/#!/login
登录等保预约平台https://192.168.187.125/user/login
准备定级材料
网络安全等级保护备案官网链接
http://banshi.beijing.gov.cn/pubtask/task/1/110108000000/46786d45-a5b7-468e-8f81-3960bf348fa8.html?locationCode=110108000000
登录官网，选择自己所在地区————下载相对于模板，因疫情情况，需记录咨询预约电话，确认提交流程。
1提交测评机构材料
1《信息系统安全等级保护备案表》
2《职业测评系统安全等级保护定级报告》
2提交定级材料后由测评专家根据《备案表》与《定级报告》确定等级
3提交公安纸质材料
1《信息系统安全等级保护备案表》二级及以上信息系统 首次提交必要 纸质版两份
2《职业测评系统安全等级保护定级报告》二级及以上信息系统 首次提交必要 纸质版一份
9 附件《系统网络拓扑图及服务器IP地址清单》三级及以上信息系统提交必要 纸质版一份
10附件《专家评审意见》二级及以上信息系统 首次提交必要 纸质版一份
11附件 安全产品清单及认证、销售许可文件 三级及以上信息系统必要 （由设备平台提供证明文件） 纸质版一份
12 附件《信息安全工作管理制度》三级及以上信息系统提交 必要 只需要提交电子版
3《网络与信息安全承诺书》容缺后补 纸质版一份
4《信息安全等级保护备案证明使用承诺书》 容缺后补 纸质版一份
5《网络安全等级保护应急联系登记表》容缺后补 纸质版一份
6《法人代表身份证》 纸质版一份
7《代办人身份证》 纸质版一份
8《工商营业执照》 纸质版一份
15 被授权人身份证复印件及办理备案工作的授权委托书 纸质版一份
13备案单位服务器托管协议 纸质版一份
14备案单位办公地证明 （由设备平台提供备案证明） 纸质版一份（可以跟安全产品及认证文件放在一块）
4提交公安电子版材料 同3，盖章pdf文件 刻录光盘一张（光盘封面用黑色mark笔注明单位名称）
5 材料准备完毕之后————打电话预约，确认提交流程。材料提交完成之后。公安部门会对提交材料进行审核。
6 公安部门审核通过之后，会发短信通知 客户也可自行登录等保备案预约平台查看
7 将等保备案平台上生成的备案编号告知测评机构，公安机关会将《备案证明》电子版直接发送给客户，客户也可以选择将电子备案证明发送给测评机构。
等保测评
测评机构开始测评
由测评机构输出《差距分析已漏扫存在问题》（等保首次测评报告）
整改建设
根据测评机构提供测评报告进行相应的整改 购买对应的安全产品，符合等保要求达到对应分数线
系统拓扑结构及说明：
系统安全组织机构及管理制度：
系统安全保护设施设计实施方案或改建实施方案：
系统使用的安全产品清单及认证、销售许可证明：
系统等级测评报告：
专家评审情况：
上级主管部门审批意见：
点击上传
登录等保备案预约平台，进行材料补录。
领取证书
备案完成之后登录等保备案预约平台查看，提示去现场领取备案证书。
如： 先提交线下材料后提交线上材料。可直接根据等保预约平台上领取时间去公安部门领取纸质证明文件
如： 先提交线上材料开始备案。需去领取纸质证明文件时准备好纸质材料及光盘，去领取纸质证明文件。

等保定级备案

等保阶段	服务内容	服务方式
定级备案	备案材料准备及撰写：提供备案材料编写技术支持，包括答疑、建议、符合性评审等	按需（现场或远程）
	定级专家评审：协助客户开展定级专家评审工作。	按需（现场或远程）
	等保备案：备案材料提交网安，完成备案工作。	按需（现场或远程）
	电子备案证明：跟进网安备案审批工作进展，领取电子备案证明。	按需（现场或远程）

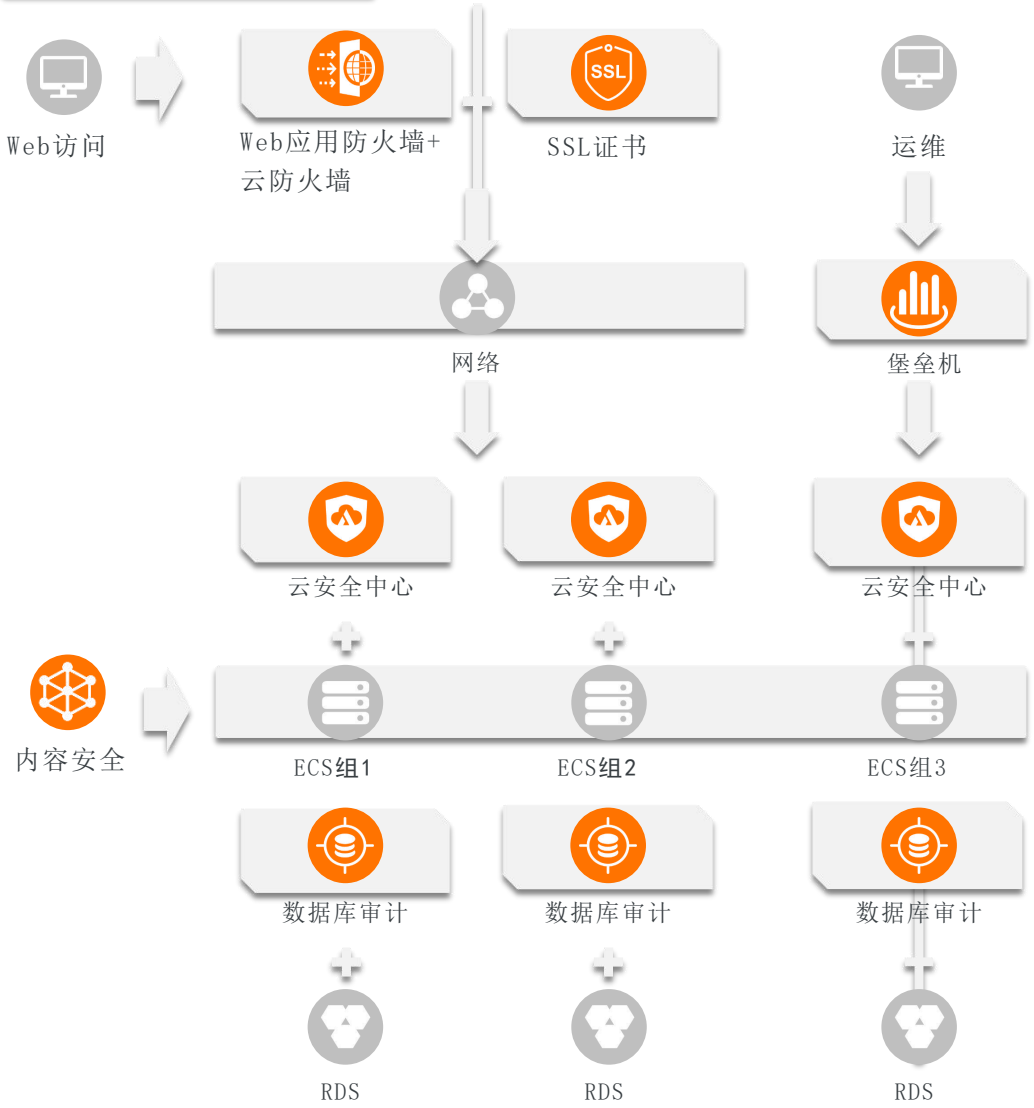
等保安全建设

等保安全建设，建立的主要手段包括使用安全产品、加固系统配置和开发安全控制。其中通过使用成熟的安全产品，可以快速满足合规要求，环宇可以提供完整的安全解决方案。



公有云等保安全架构

方案架构



核心产品功能

Web应用防火墙	• 防Web攻击、防CC、防刷、保业务安全
SSL证书	• 通过加密使网站可信，防窃听、防劫持、防篡改
云防火墙	• 访问控制、微隔离、威胁入侵检测
云安全中心	• 主机安全软件，漏洞修复检测，恶意程序检测
堡垒机	• 对IT运维人员、运维行为进行管理和控制
数据库审计	• 监控数据库安全
内容安全	• 对图片、视频、文本、语音等对象进行安全检测

主要解决的问题

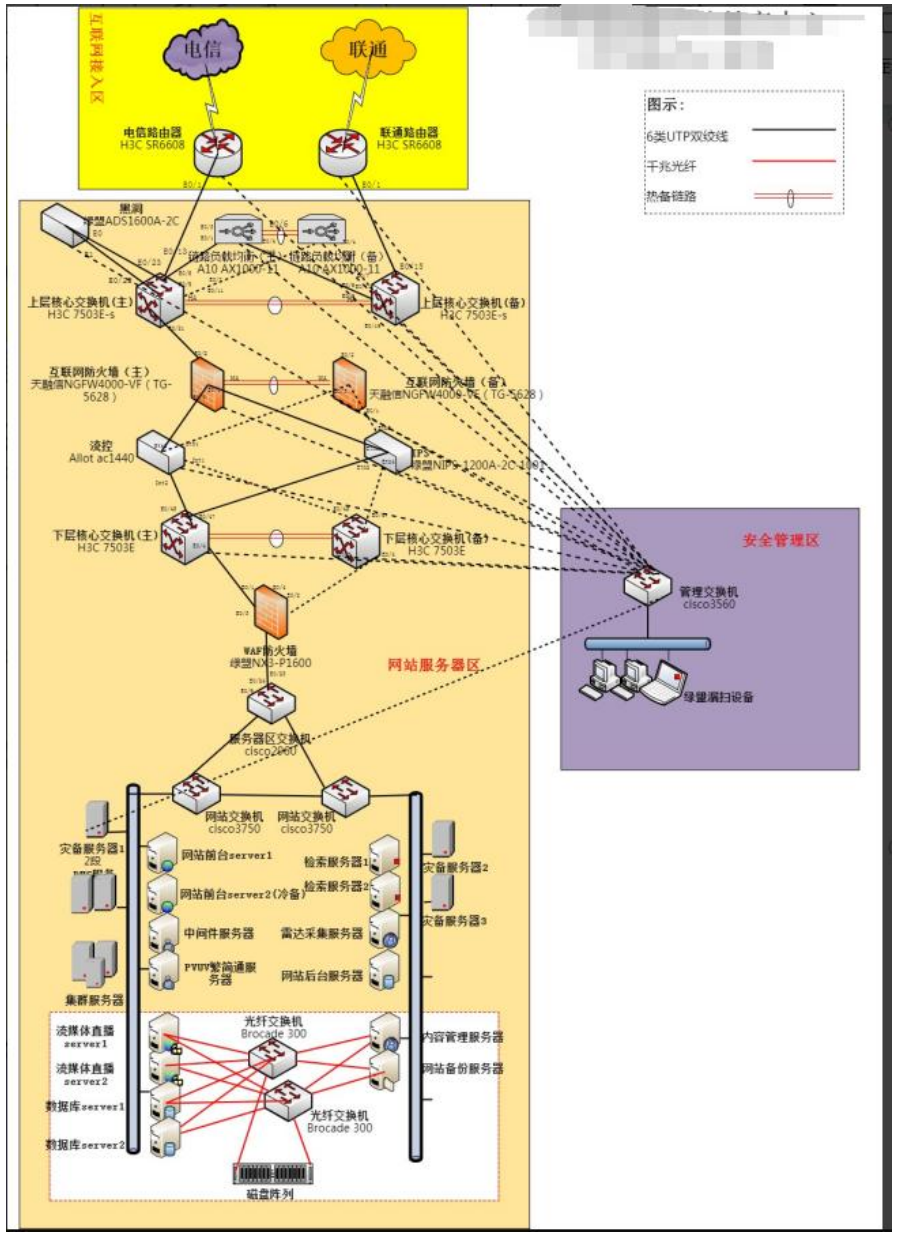
解决云上业务等保合规需求：

- 三级等保

场景方案的优势

- 一站式服务，周期短，投入低
- 高分通过等保（80分+）

物理机房等保安全架构



核心产品功能

Web应用防火墙	• 防Web攻击、屏蔽用户敏感信息，过滤状态码
CA证书	• 通过加密使网站可信，防窃听、防劫持、防篡改
互联网边界防火墙	• 访问控制、微隔离、威胁入侵检测
NIPS网络入侵防护系统	• 主动拦截黑客攻击、蠕虫、网络病毒、 • 后门木马、D.o.S等恶意流量
盟黑洞DDOS防护	• 对DDOS攻击进行抵御
服漏洞扫描	• 全面检测客户现有资产，提供相应漏洞修复和加固建议，提高网络系统整体优势

传统线下安全厂商

- **部分合作安全厂商：深信服、绿盟科技、启明星辰、三六零、奇安信、天融信等等**

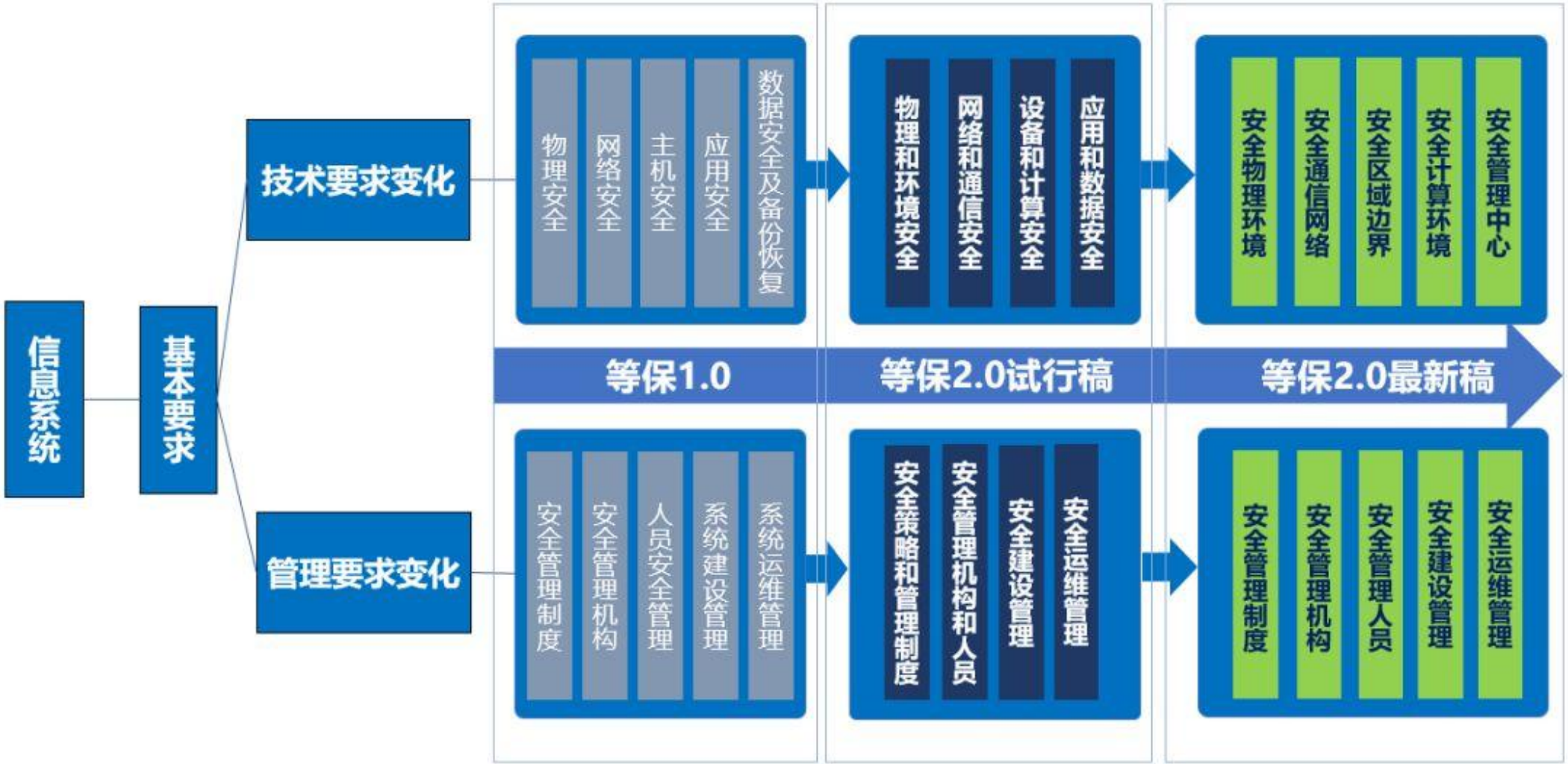
等保差距分析

等保阶段	服务内容	服务方式
差距分析	依据《信息安全技术 网络安全等级保护测评过程实施指南》GB/T 22239-2019进行调研差距分析，结合分析结果与定级结果，从技术与管理两个方面基于信息系统等级标准对信息系统进行设计，给出合理的整改建议，以达到预期的整改结果。	按需（现场或远程）

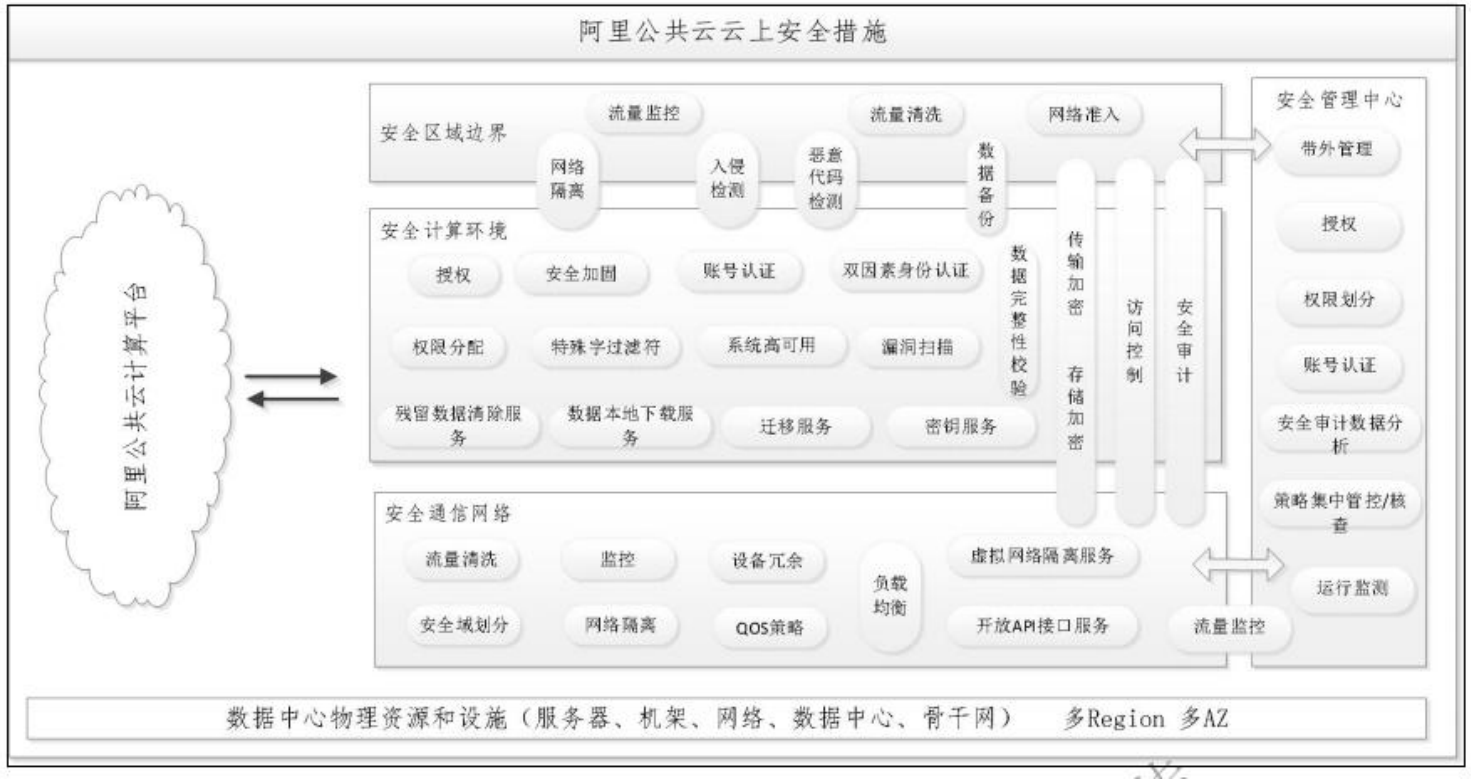
等保整改实施

等保阶段	服务内容	服务方式
整改实施	安全技术整改加固：协助给予整改支持、技术答疑等，提升整改效率和效果	按需（现场或远程）
	安全管理整改、优化：对整改后的问题和风险点进行复核确认，为测评报告输出提供协助。	按需（现场或远程）
等保测评 (测评机构)	报告输出：测评机构等保测评报告编写、盖章、输出、网安报备。 纸介质备案证明：登录等保备案预约平台查看，领取证书。	按需（现场或远程）

等保整改标准


信息系统
基本要求
技术要求变化
管理要求变化
物理安全
网络安全
主机安全
应用安全
数据安全及备份恢复
安全管理制度
安全管理机构
人员安全管理
系统建设管理
系统运维管理
物理和环境安全
网络和通信安全
设备和计算安全
应用和数据安全
安全策略和管理制度
安全管理机构和人员
安全建设管理
安全运维管理
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
等保1.0
等保2.0试行稿
等保2.0最新稿

等保安全整改：物理环境等



大部分公有云厂商机房基本获得等级保护三级标准认证，另外金融云及政务云达到等级保护四级标准认证。基于公有云的用户过等保无需关心机房等保问题，只需关注自身业务安全和管理制度。

安全分类	安全控制点	安全控制点描述
安全物理环境	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	应将设备或主要部件进行固定，并设置明显的不易除去的标识。
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	机房应设置专业灭火设备。
	防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
	温湿度控制	应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	应在机房供电线路上配置稳压器和过电压防护设备。
通信网络安全	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。
区域边界安全	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
	访问控制	a)应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

等保安全整改：安全计算环境

安全计算环境主要针对安全计算环境（网络）、安全计算环境（主机）、安全计算环境（应用和软件）来做管理或者防护的一些要求，是等级保护中安全控制点最多的部分，也是丢失分数比较多的一部分。

主要涵盖点包括：
身份鉴别、安全审计、入侵防范、可信验证、恶意代码防范、数据完整性、数据保密性、数据备份与恢复、个人信息保护、剩余信息保护。

在这些涵盖点下会细分许多相应的安全控制点，用户需要根据安全控制点完成安全整改。

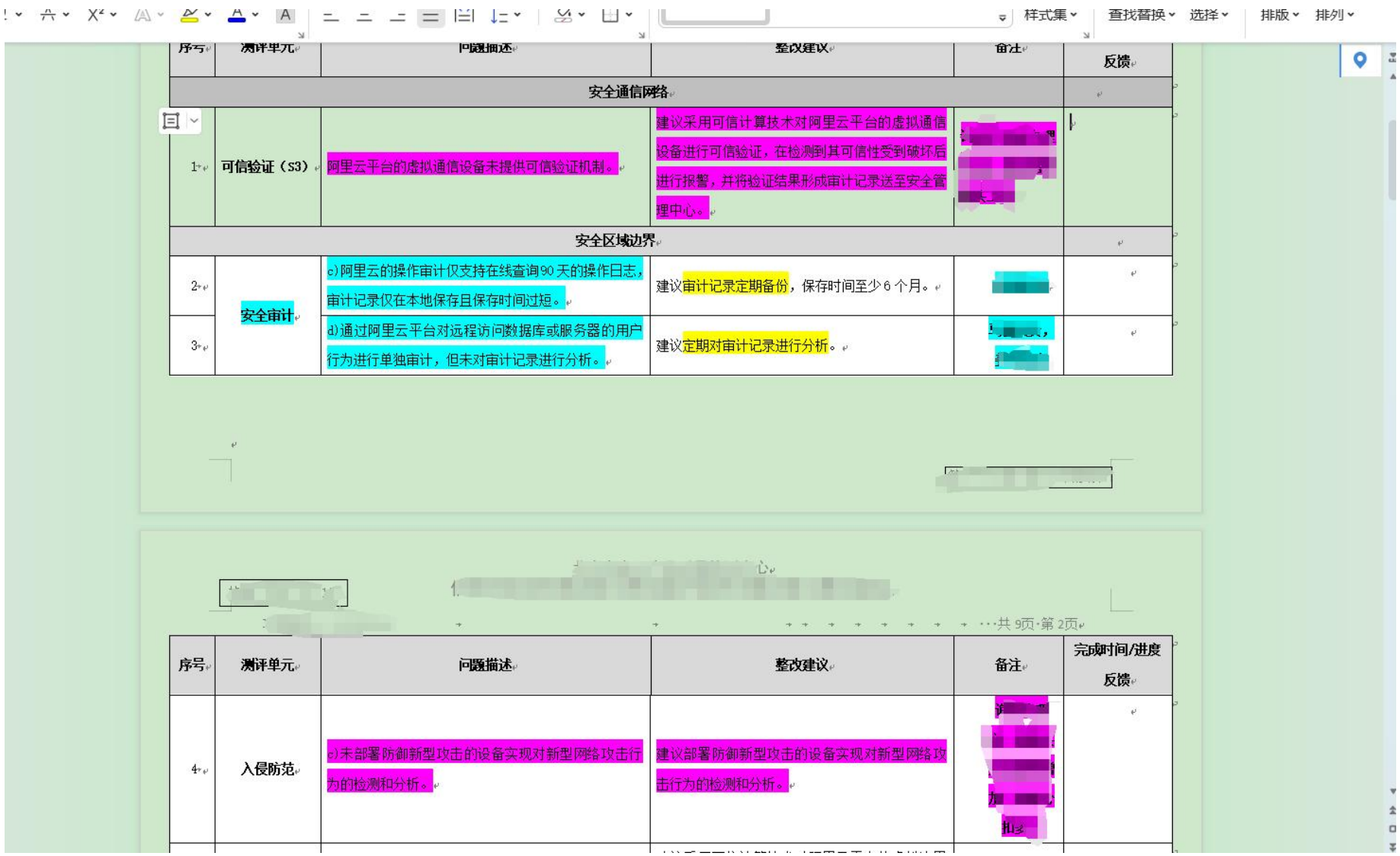
等保安全整改：安全管理

网络运营者应制定安全管理制度文档，形成安全管理体系，设置安全管理部门和管理员，定人定岗，并在日常工作期间落实安全管理制度，培养员工网络安全防护意识，定期组织网络安全应急演练。

安全管理中心	审计管理
	安全管理
	集中管控
安全策略和管理制度	安全策略
	管理制度
	制定和发布
	评审和修订
安全管理机构和人员	岗位设置
	人员配备
	授权和审批
	沟通和合作
	审核和检查
	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
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
	变更管理
	备份与恢复管理
	安全事件处置
	应急预案管理
	外包运维管理

等保安全整改实施



序号	测评单元	问题描述	整改建议	备注	反馈
	安全通信网络				
1	可信验证（S3）	阿里云平台的虚拟通信设备未提供可信验证机制。	建议采用可信计算技术对阿里云平台的虚拟通信设备进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。		
	安全区域边界				
2	安全审计	c)阿里云的操作审计仅支持在线查询90天的操作日志，审计记录仅在本地保存且保存时间过短。	建议审计记录定期备份，保存时间至少6个月。		
3		d)通过阿里云平台对远程访问数据库或服务器的用户行为进行单独审计，但未对审计记录进行分析。	建议定期对审计记录进行分析。		

序号	测评单元	问题描述	整改建议	备注	完成时间/进度反馈
4	入侵防范	c)未部署防御新型攻击的设备实现对新型网络攻击行为的检测和分析。	建议部署防御新型攻击的设备实现对新型网络攻击行为的检测和分析。		

环宇数通
sotote.com

目 录

安全运维体系

网络安全法及等级保护系列标准

客服云平台
（用户前台）

工单服务平台
（工程师后台）

网络监测系统

统一安管系统

自动化系统

SLA管理 | 配置管理 | 容量管理 | 可用性管理 | 备份/恢复

巡检/加固 | 变更管理 | 应急预案 | 事件/问题 | 知识库管理

应用系统：网站、APP、微信小程序、OA、财务、ERP等应用

中间件：apache、tomcat、mysql、oracle、redis、mongoDB等

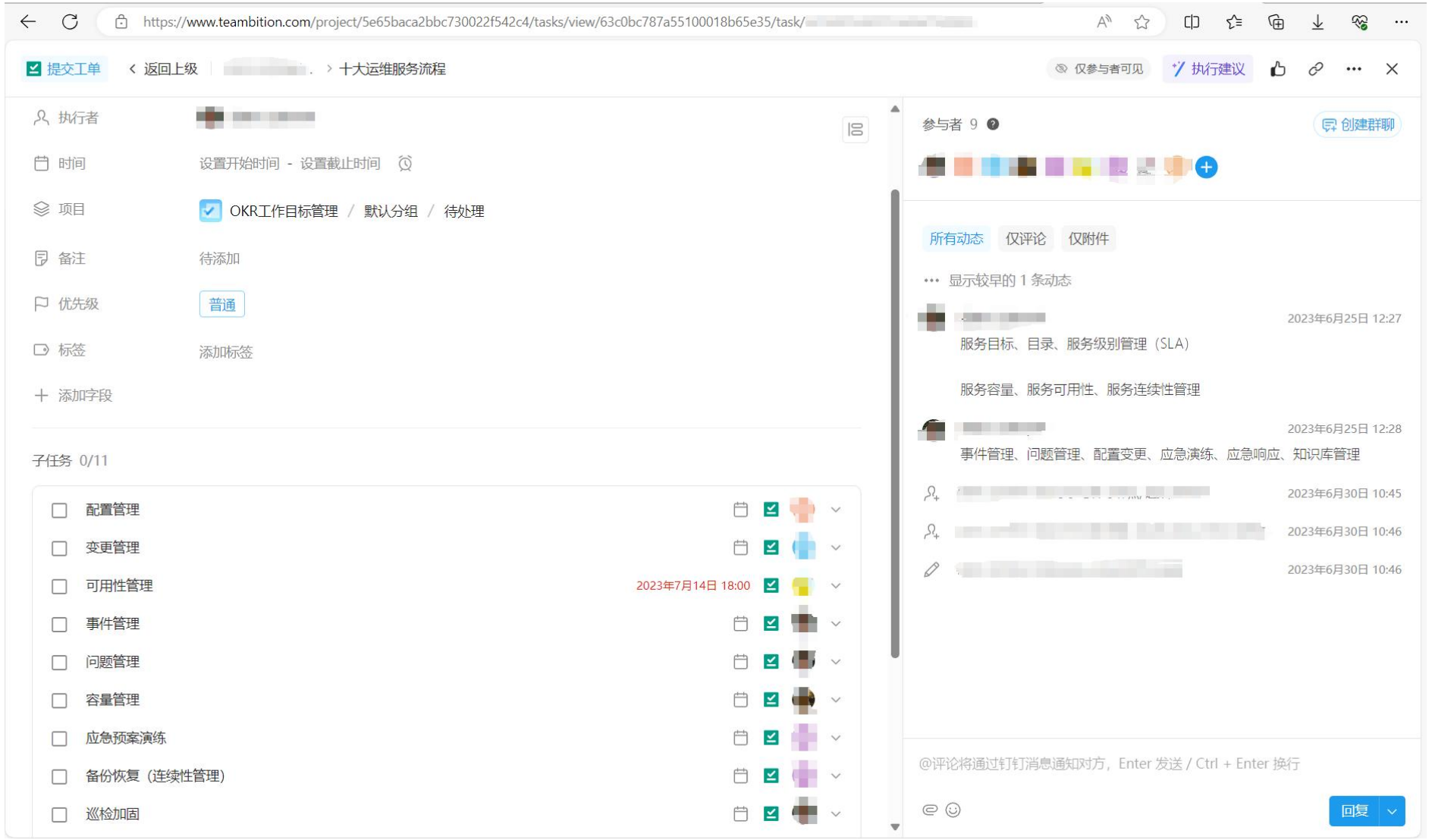
IT基础软件：操作系统、云平台、大数据平台等

IT硬件设备：网络、服务器、存储、安全设备等

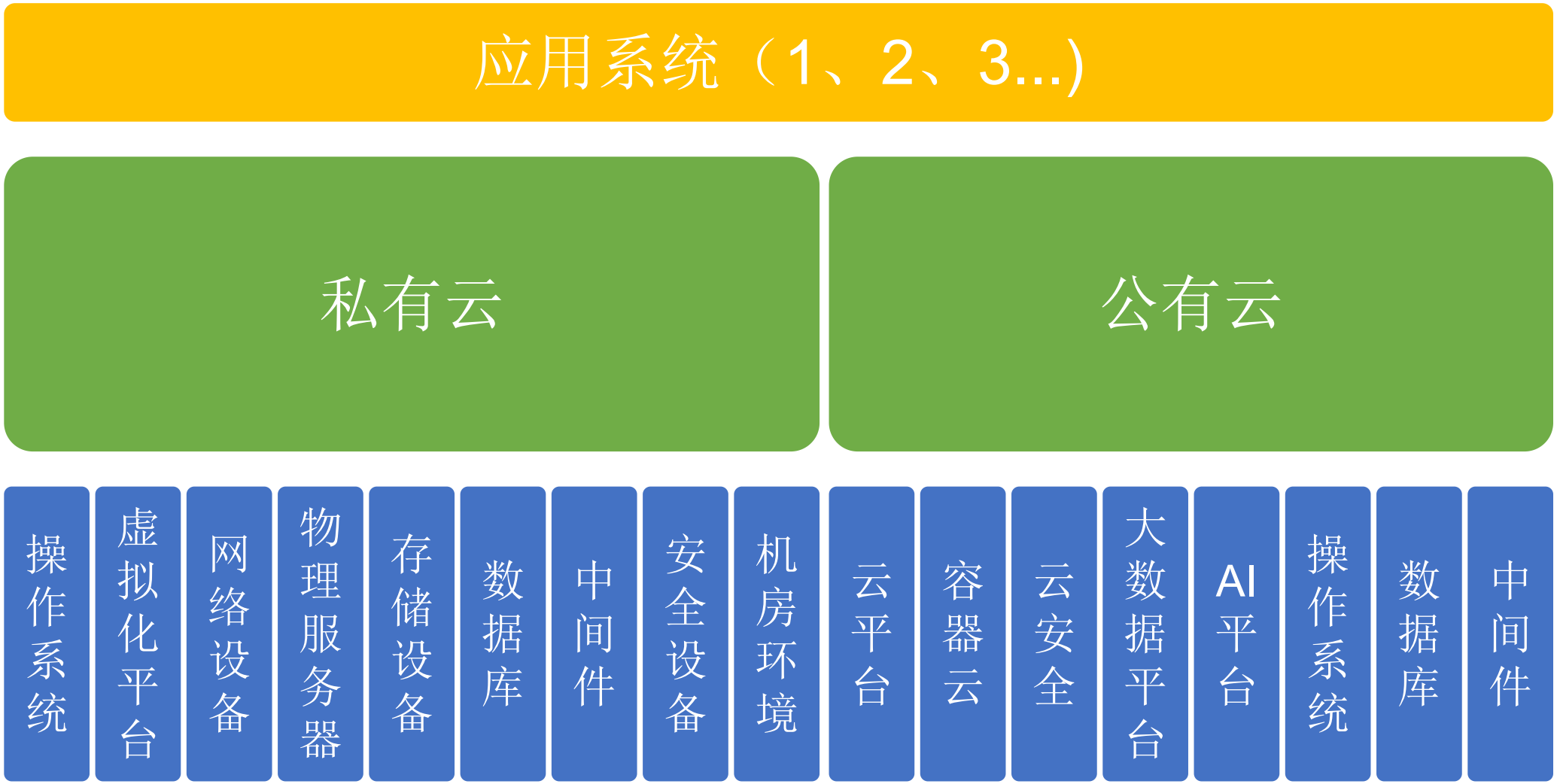
机房环境：电力系统、UPS、通风制冷、防静电防雷等

ISO20000/27001

运维工单系统


https://www.teambition.com/project/5e65baca2bbc730022f542c4/tasks/view/63c0bc787a55100018b65e35/task/
提交工单
返回上级
十大运维服务流程
仅参与者可见
执行建议
执行者
时间
设置开始时间 - 设置截止时间
项目
OKR工作目标管理 / 默认分组 / 待处理
备注
待添加
优先级
普通
标签
添加标签
添加字段
子任务 0/11
配置管理
变更管理
可用性管理
2023年7月14日 18:00
事件管理
问题管理
容量管理
应急预案演练
备份恢复（连续性管理）
巡检加固
参与者 9
创建群聊
所有动态
仅评论
仅附件
显示较早的 1 条动态
2023年6月25日 12:27
服务目标、目录、服务级别管理（SLA）
服务容量、服务可用性、服务连续性管理
2023年6月25日 12:28
事件管理、问题管理、配置变更、应急演练、应急响应、知识库管理
2023年6月30日 10:45
2023年6月30日 10:46
2023年6月30日 10:46
@评论将通过钉钉消息通知对方，Enter 发送 / Ctrl + Enter 换行
回复

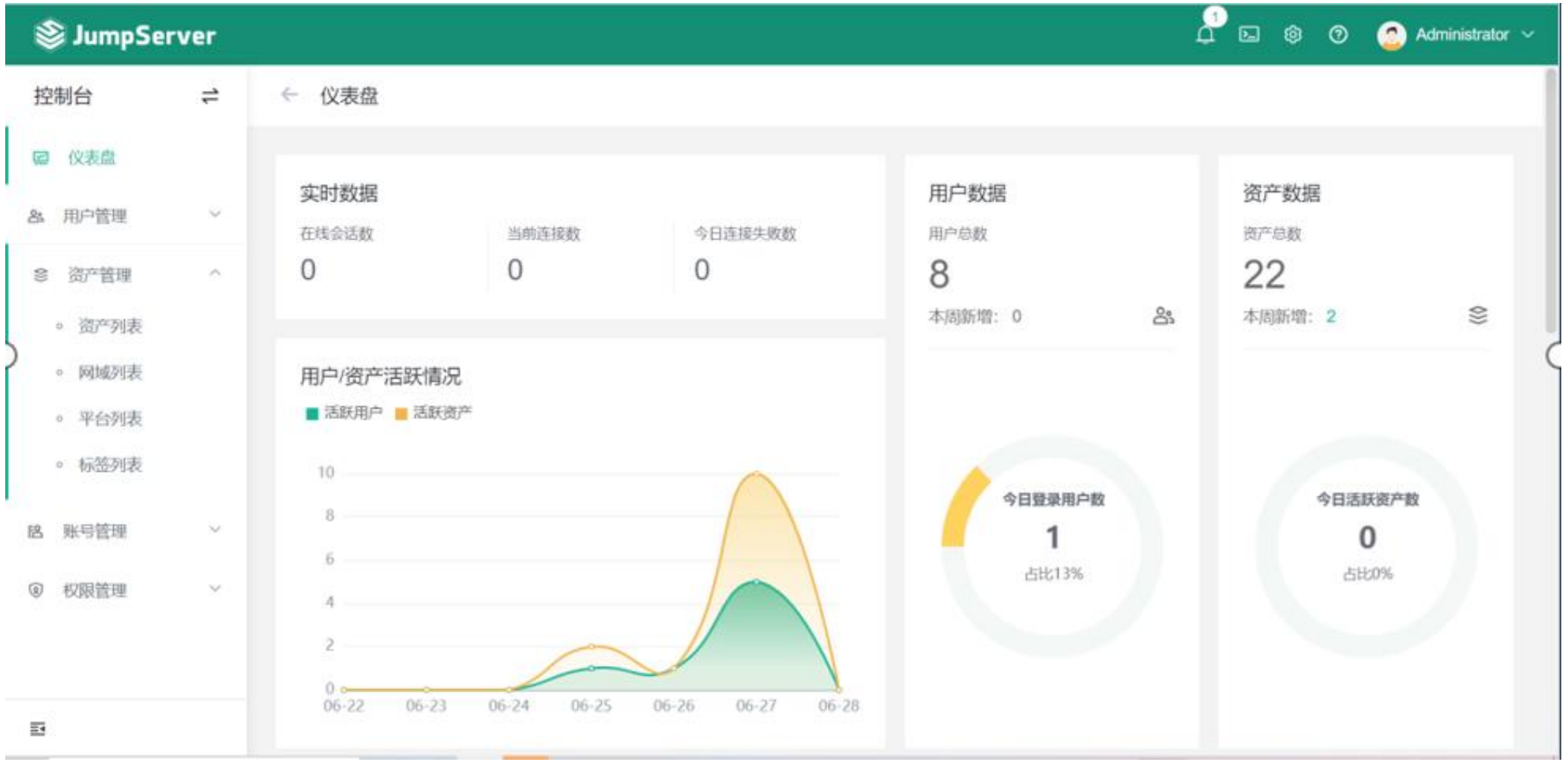
应用系统梳理


应用系统（1、2、3...）
私有云
公有云
操作系统
虚拟化平台
网络设备
物理服务器
存储设备
数据库
中间件
安全设备
机房环境
云平台
容器云
云安全
大数据平台
AI平台
操作系统
数据库
中间件

7*24云监控


安全预警
安全评分
78/100
告警
0
漏洞
5
云产品风险监测 10
SSL 证书 去配置
Web入侵检测 61
资源预警
正在报警
1
事件概览
近1天
严重 0
警告 0
待修复漏洞 1
安全分 -5
帮助文档
存在未修复的应急漏洞
存在5个未修复的应急漏洞
立即处理
云平台配置风险 2
安全分 -17
帮助文档
云产品配置存在高危风险
存在6个高风险云产品配置检查项
立即处理
云产品配置存在中低危风险
存在5个中低危风险云产品配置检查项
立即处理
报警服务 / 正在报警
正在报警
云产品
应用分组
站点监控
产品
报警数
操作
站点监控
1
展开详情
报警资源
报警规则
报警值/触发条件
发生时间
持续时间
操作
0
可用率 <90% P3 连续2次就报警
2021年12月6日 04:53:00
秒
报警历史

统一安管平台


JumpServer
Administrator
控制台
仪表盘
用户管理
资产管理
资产列表
网域列表
平台列表
标签列表
账号管理
权限管理
仪表盘
实时数据
在线会话数
0
当前连接数
0
今日连接失败数
0
用户/资产活跃情况
活跃用户
活跃资产
10
8
6
4
2
0
06-22
06-23
06-24
06-25
06-26
06-27
06-28
用户数据
用户总数
8
本周新增: 0
今日登录用户数
1
占比13%
资产数据
资产总数
22
本周新增: 2
今日活跃资产数
0
占比0%

实时监测与派单

Global view

添加仪表盘 / Global view

系统信息

参数	值	细节
Zabbix服务器端运行中	是	localhost:10051
Number of hosts (enabled/disabled)	25	25 / 0
Number of templates	326	
监控项数量（已启用/已禁用/不支持）	3239	3058 / 0 / 181
触发器数量（已启用/已禁用 [问题/正常]）	1717	1717 / 0 [38 / 1679]
用户数(线上)	4	2

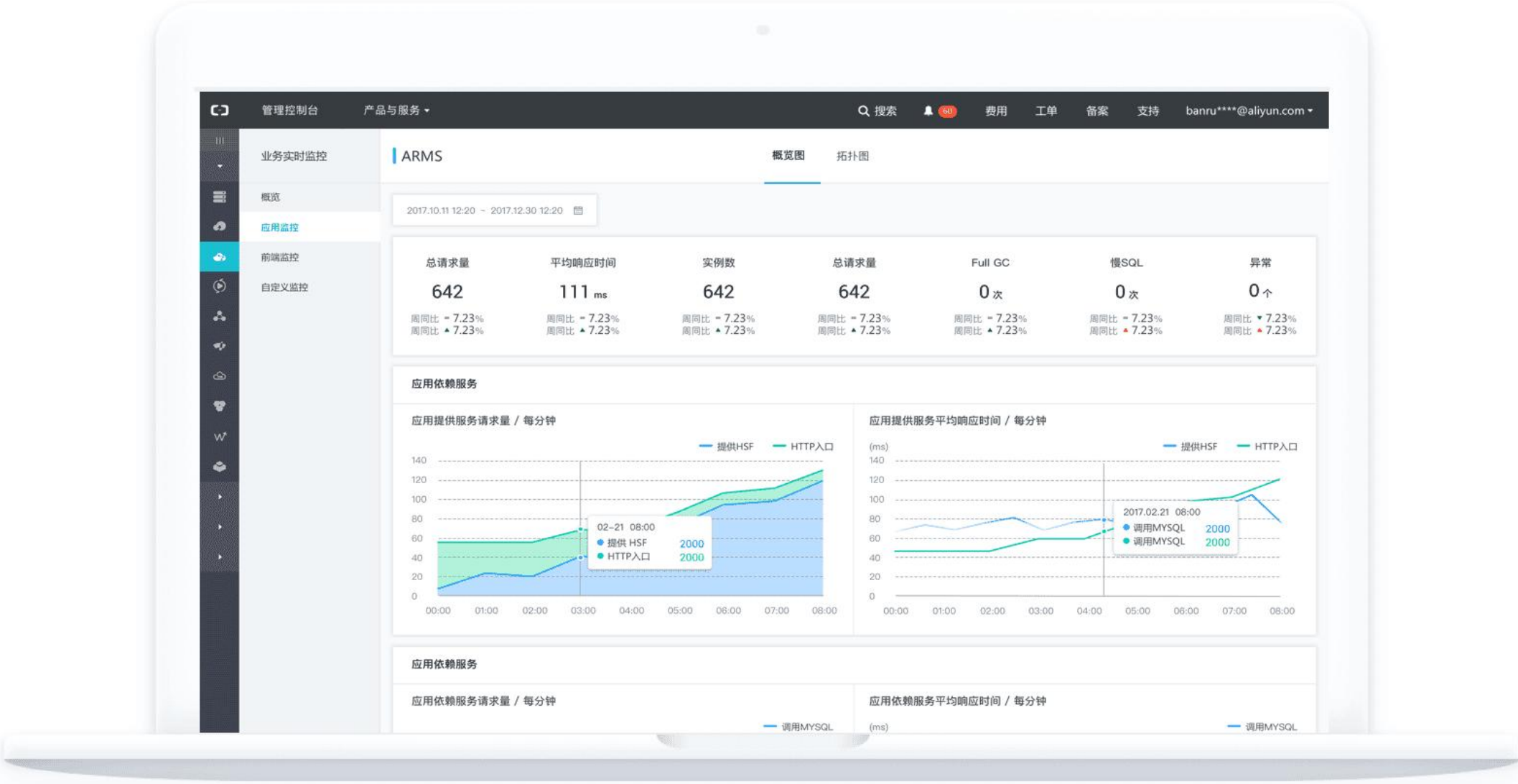
	可用	不可用	未知的	合计
Zabbix 客户端	18	0	0	18
SNMP	7	0	0	7
JMX	0	0	0	0

0 灾难	0 严重	17 一般严重	9 警告	10 信息	0 未分类

问题

时间 ▼	恢复时间	状态	信息	主机	问题 • 严重性	Operational data	持续时间	确认	动作	标记
2023-07-13 13:42:24		问题		192.168.16.233（SW3）	Interface GigabitEthernet0/0/16(): Link down	Current state: down (2)	7d 22h 12m	不	1	class: network component: network description •••
2023-07-13 13:42:24		问题		192.168.16.233（SW3）	Interface GigabitEthernet0/0/16: Link down	Current state: down (2)	7d 22h 12m	不	1	class: network component: network description •••
2023-07-07 10:51:19		问题		192.168.16.232（SW2）	Interface GigabitEthernet0/0/24(): Link	Current state: down (2)	14d 1h 3m	不	1	class: network component: network description •••

关联分析快速定位


管理控制台
产品与服务
搜索
费用
工单
备案
支持
banru****@aliyun.com
业务实时监控
ARMS
概览图
拓扑图
概览
应用监控
前端监控
自定义监控
2017.10.11 12:20 - 2017.12.30 12:20
总请求量
642
平均响应时间
111 ms
实例数
642
总请求量
642
Full GC
0 次
慢SQL
0 次
异常
0 个
应用依赖服务
应用提供服务请求量 / 每分钟
提供HSF
HTTP入口
02-21 08:00
提供 HSF 2000
HTTP入口 2000
应用提供服务平均响应时间 / 每分钟
2017.02.21 08:00
调用MYSQL 2000
调用MYSQL 2000
应用依赖服务
应用依赖服务请求量 / 每分钟
应用依赖服务平均响应时间 / 每分钟
调用MYSQL

AI自动化处置

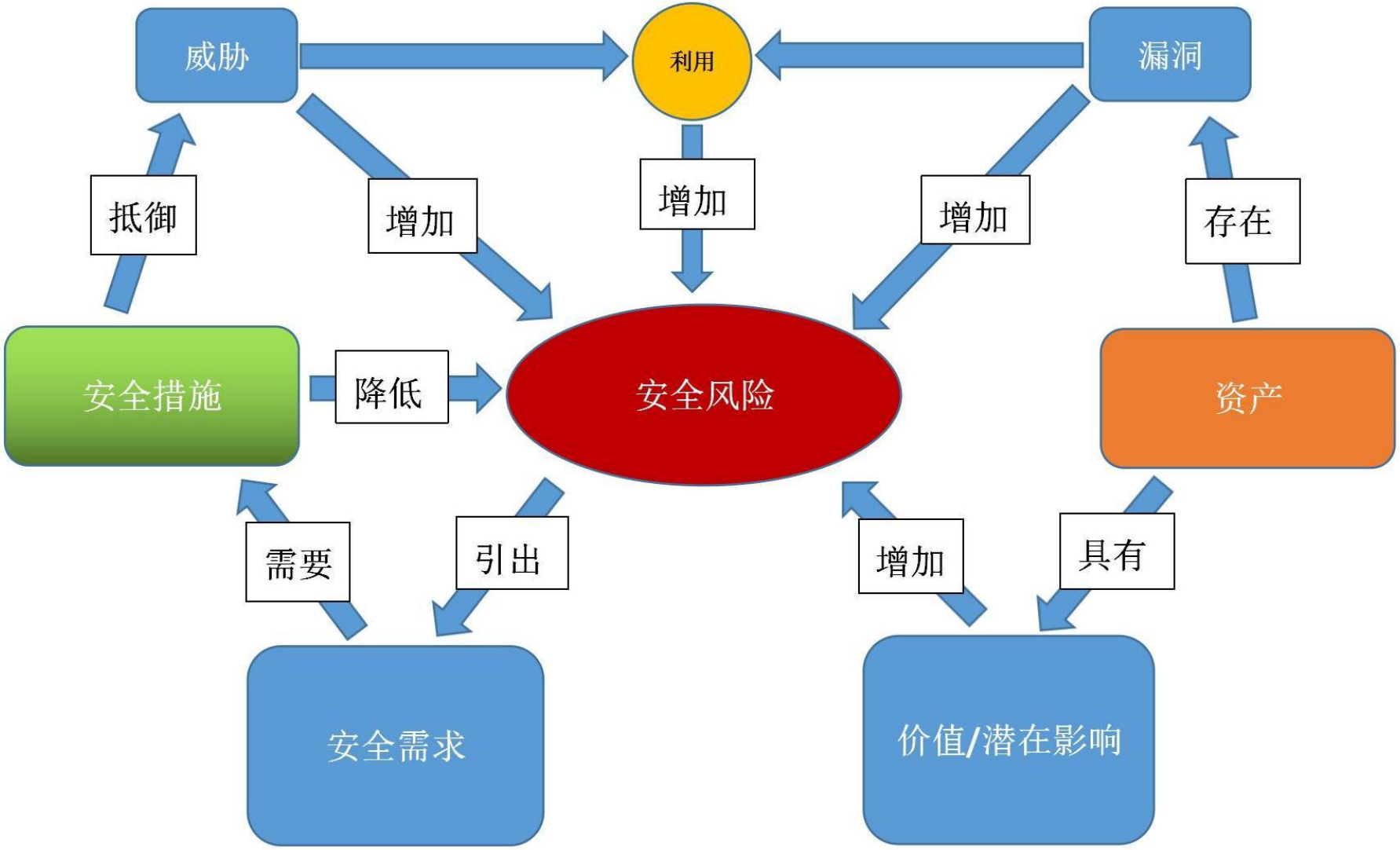
应急演练服务


应急预案
总则
编制目的
切实做好信息安全事件的防范和应急响应工作
提高预防和控制信息安全事件的能力和水平
减轻或消除信息安全事件的危害和影响
编制依据
《中华人民共和国计算机信息系统安全保护条例》
《中华人民共和国计算机信息网络国际联网安全保护管理办法》
《国家信息化工作领导小组关于加强信息安全保障工作的意见》
《关于信息安全等级保护工作的实施意见》
适用范围
攻击事件
故障事件
灾害事件
工作原则
依法管理
分级负责、责任到头
谁主管，谁负责
角色及职责
角色的划分及职责
应急响应领导小组
应急响应实施小组
应急响应日常运行小组
组织的外部协作
预防和预警机制
参照国家有关等保要求采取相应安全保障措施，不断完善安全防御系统
建立安全事件预警预报体系，严格执行网络与信息安全管理制度
做好服务器及数据中心的数据备份及等级工作，建立灾难性数据恢复机制
应急响应流程
应急响应保障措施
人力保障
物质保障
技术保障
事件通告
信息通报
信息上报
信息披露
事件分类与定级
事件分类
攻击事件
故障事件
灾害事件
事件定级
一般事件
重大事件
特别重大事件
应急启动
一般事件日常监测和维护可解决的无需启动应急
重大事件和特别重大事件的启动流程
应急处置
灾害事件处置流程
故障或攻击事件处置流程
病毒传播处置
外部如今处置
内部入侵处置
网络故障处置
其他因素灾害处置
后期处置
概述
信息系统重建
应急响应总结

环宇数通
sotote.com

目 录

IT系统风险评估



定级材料一站式协助

名称	修改日期	类型	大小
2、备案表表四附件		文件夹	
7、三级及以上网络系统"三员"材料（仅三级网络系统提交）		文件夹	
1、网络安全等级保护备案表.docx		DOCX 文档	49 KB
3、网络安全等级保护定级报告.docx		DOCX 文档	29 KB
4、等级保护备案登记表.xlsx		XLSX 工作表	10 KB
5、信息系统基本信息表.doc		DOC 文档	42 KB
6、信息系统及网络安全检查自查表.doc		DOC 文档	39 KB

01《XX单位-网络拓扑图及说明》
02《XX单位-网络安全领导小组》
02《XX单位-网络安全工作管理制度》
03《XX单位-整改实施方案》
04《网络使用的安全产品清单及认证、销售许可证明》
05《XX单位XX 网络-专家评审意见》
06《上级主管部门审批意见文件名称》
07《XX单位网络安全等级保护定级报告》（在网安部门领取备案证明后30日内原件提交网安部门）

优选测评机构

测评机构选择需要综合考虑多个方面，以确保选择到专业、合规、服务优质且价格合理的测评机构。主要看以下几点：

一、**资质和认证**：是否具备相关的等保测评资质，确认其专业性和合规性。

二、**经验和口碑**：测评机构的历史背景、行业覆盖、专家团队、客户评价、行业声誉等。

三、**综合性价比**：测评机构的测评速度，测评的专业性、服务质量、以及价格。

优选测评机构

等保测评机构

- 部分合作测试机构：GA等保评估中心、中科院信工所、北京质检所、银行卡检测中心、金源动力、国顺集团等。

安全产品优选

服务名称	产品名称	产品介绍
等保合规安全产品	web应用防火墙	Web应用防火墙是一种安全防护设备，用于保护Web应用程序免受各种攻击。功能有Web防护、网页保护、负载均衡、应用交付等，为用户提供一站式的安全解决方案。
	数据库审计	数据库审计（Database Audit）是一种安全技术，它通过对数据库操作进行跟踪、记录、分析和报告，来实时监控和分析数据库活动，从而发现潜在的安全风险、违规行为或异常行为。
	网络防火墙	保护服务、应用程序和数据免受各种网络攻击和威胁。它可以提供多种安全功能，如访问控制、流量过滤、威胁检测、日志审计等。

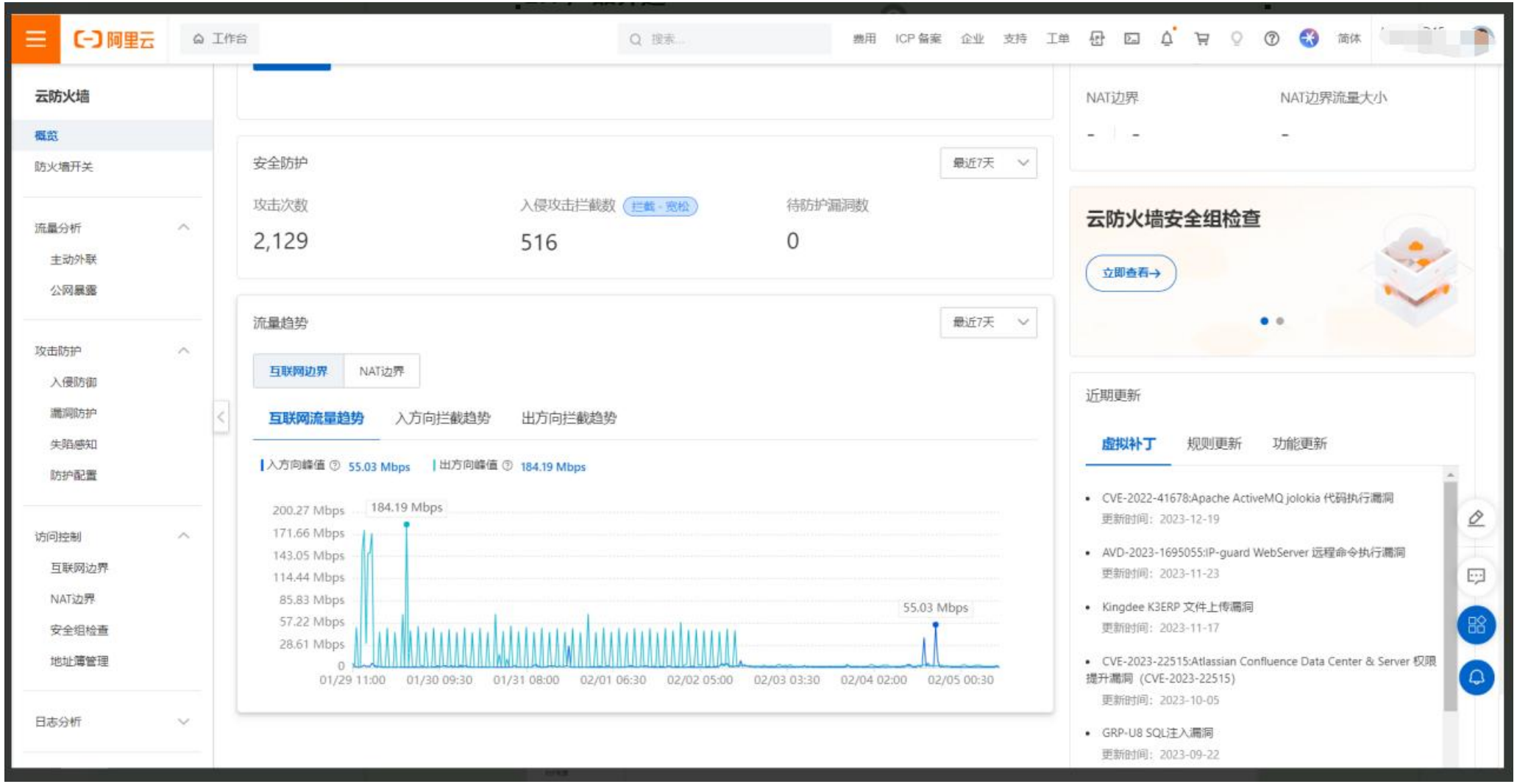
安全产品优选

服务名称	产品名称	产品介绍
等保合规安全产品	主机防护	主机防护是一个实时识别、分析、预警安全威胁的服务器主机安全管理系统，通过防勒索、漏洞扫描修复、防病毒、防篡改、合规检查等安全能力。保护云上主机、本地服务器和容器安全，并满足监管合规要求。
	DDOS基础防护	DDoS基础防护为轻量应用服务器提升DDoS攻击防御能力，当流量超出DDoS基础防护的默认清洗阈值后，自动触发流量清洗，实现DDoS攻击防护。
	RAM访问控制	访问控制是管理用户身份与资源访问权限的服务。
	操作审计	操作审计（ActionTrail）帮助您监控并记录管理员账号的活动，包括通过控制台、OpenAPI、开发者工具对产品和服务的访问和使用行为。

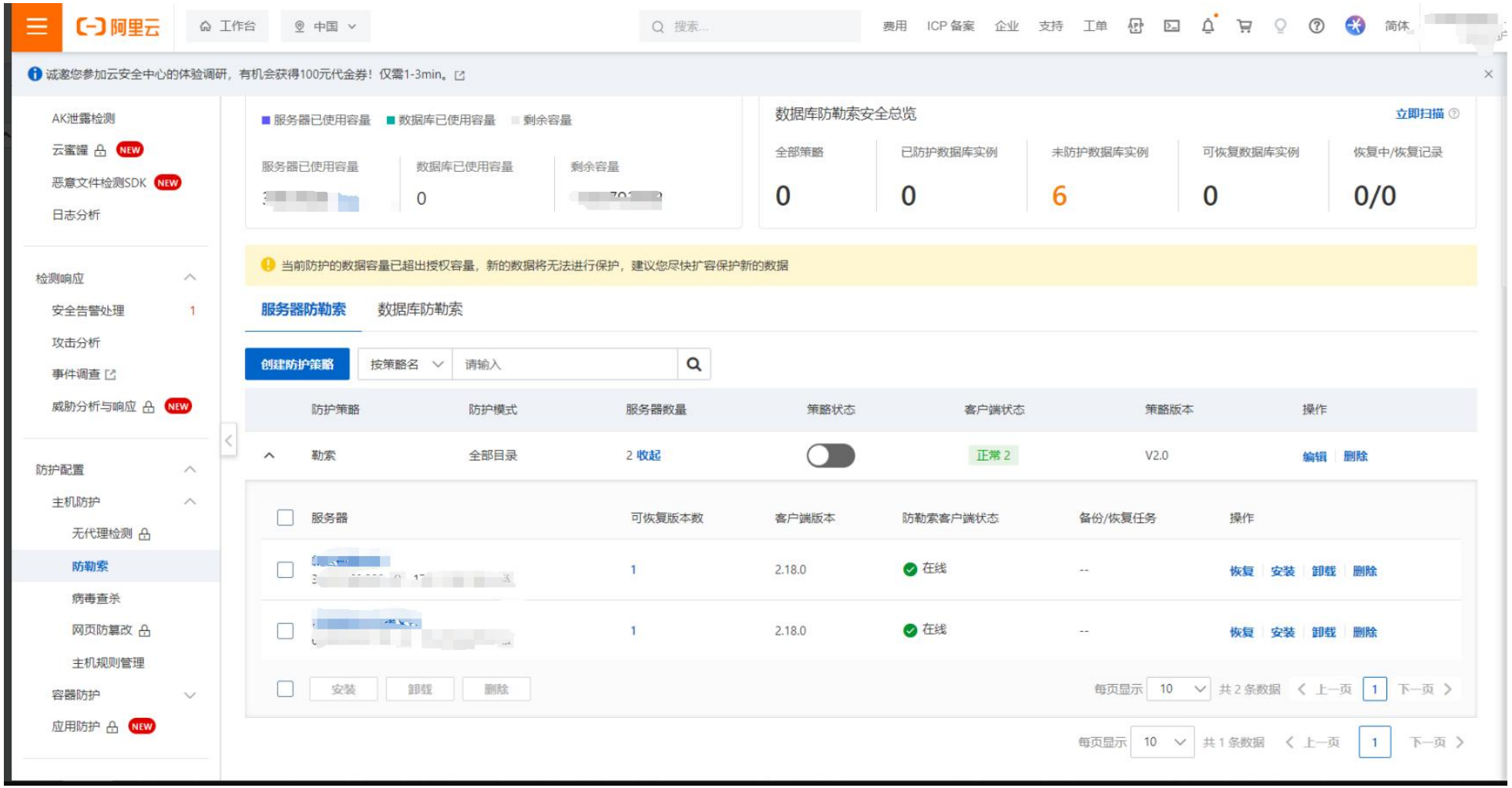
安全产品优选

服务名称	产品名称	产品介绍
等保合规安全产品	业务服务器-备	备服务器是备份服务器的主要目的是防止数据丢失，并在系统出现操作失误情况下，能够及时恢复数据，保证企业业务的连续性。
	业务数据库	业务数据库是企业中非常重要的资产，包含了大量的业务数据，如客户信息、交易记录、库存情况等。
	负载均衡	负载均衡将来自客户端的请求或数据流量分发到多个服务器上进行处理，提高系统的性能、可伸缩性和可靠性。

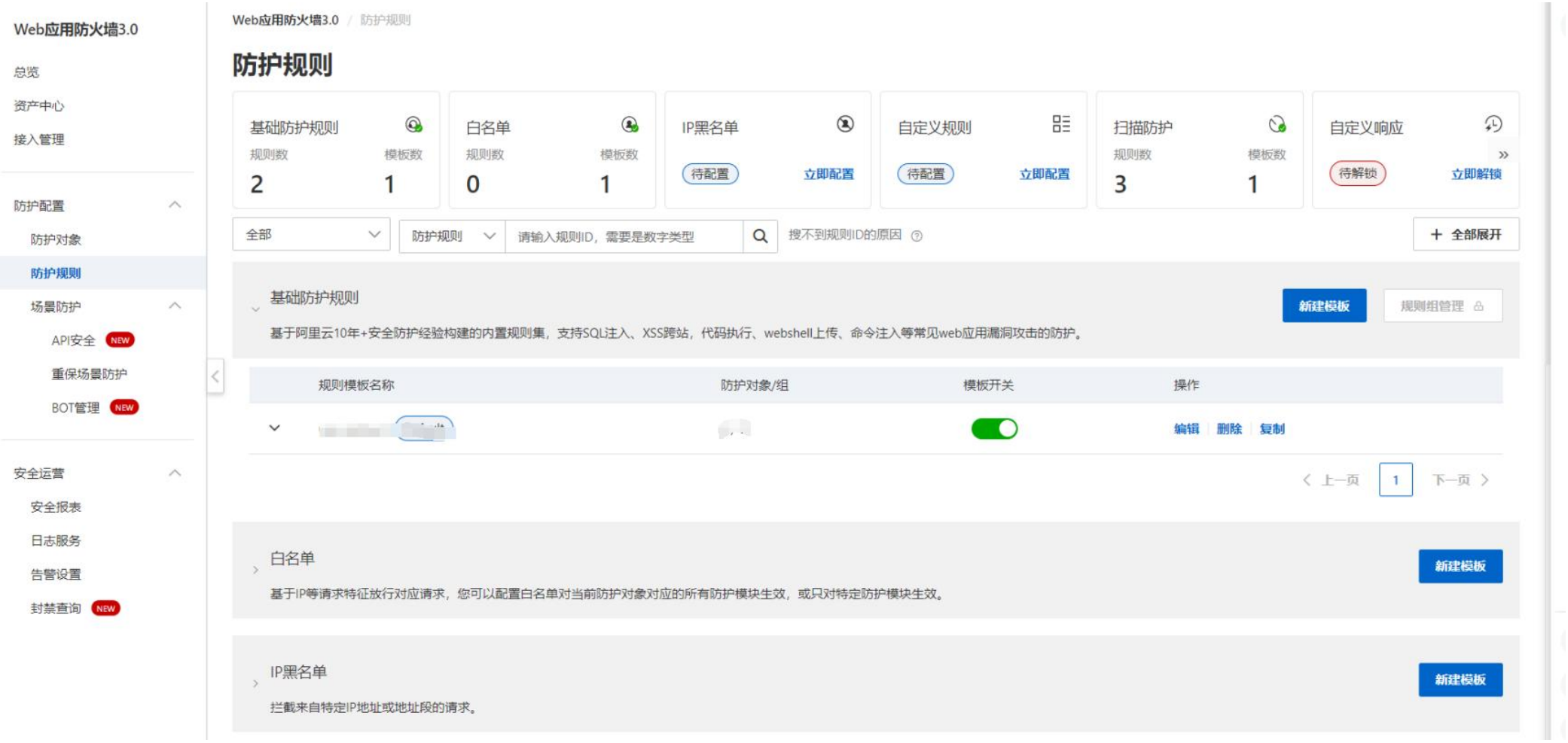
安全配置优化：云防火墙


阿里云
工作台
搜索...
费用
ICP 备案
企业
支持
工单
简体
云防火墙
概览
防火墙开关
流量分析
主动外联
公网暴露
攻击防护
入侵防御
漏洞防护
失陷感知
防护配置
访问控制
互联网边界
NAT边界
安全组检查
地址簿管理
日志分析
安全防护
最近7天
攻击次数
2,129
入侵攻击拦截数
拦截 - 宽松
516
待防护漏洞数
0
流量趋势
最近7天
互联网边界
NAT边界
互联网流量趋势
入方向拦截趋势
出方向拦截趋势
入方向峰值 55.03 Mbps
出方向峰值 184.19 Mbps
200.27 Mbps
171.66 Mbps
143.05 Mbps
114.44 Mbps
85.83 Mbps
57.22 Mbps
28.61 Mbps
0
184.19 Mbps
55.03 Mbps
01/29 11:00
01/30 09:30
01/31 08:00
02/01 06:30
02/02 05:00
02/03 03:30
02/04 02:00
02/05 00:30
NAT边界
NAT边界流量大小
云防火墙安全组检查
立即查看→
近期更新
虚拟补丁
规则更新
功能更新
CVE-2022-41678:Apache ActiveMQ jolokia 代码执行漏洞
更新时间：2023-12-19
AVD-2023-1695055:IP-guard WebServer 远程命令执行漏洞
更新时间：2023-11-23
Kingdee K3ERP 文件上传漏洞
更新时间：2023-11-17
CVE-2023-22515:Atlassian Confluence Data Center & Server 权限提升漏洞 (CVE-2023-22515)
更新时间：2023-10-05
GRP-U8 SQL注入漏洞
更新时间：2023-09-22

安全配置优化：云安全中心



安全配置优化：Web应用防火墙



安全配置优化：数据库审计

环宇数通
sotote.com

目 录

发展历程

2013年核心团队来自顶级IT厂商

2015年自主知识产权数通云产品

2016年阿里云全国授权服务中心

2017年建立完善的环宇云服务体系

2018年获得ISO27001安全服务资质

2019年助力企业互联网＋云转型

2020年助力企业数字化创新转型

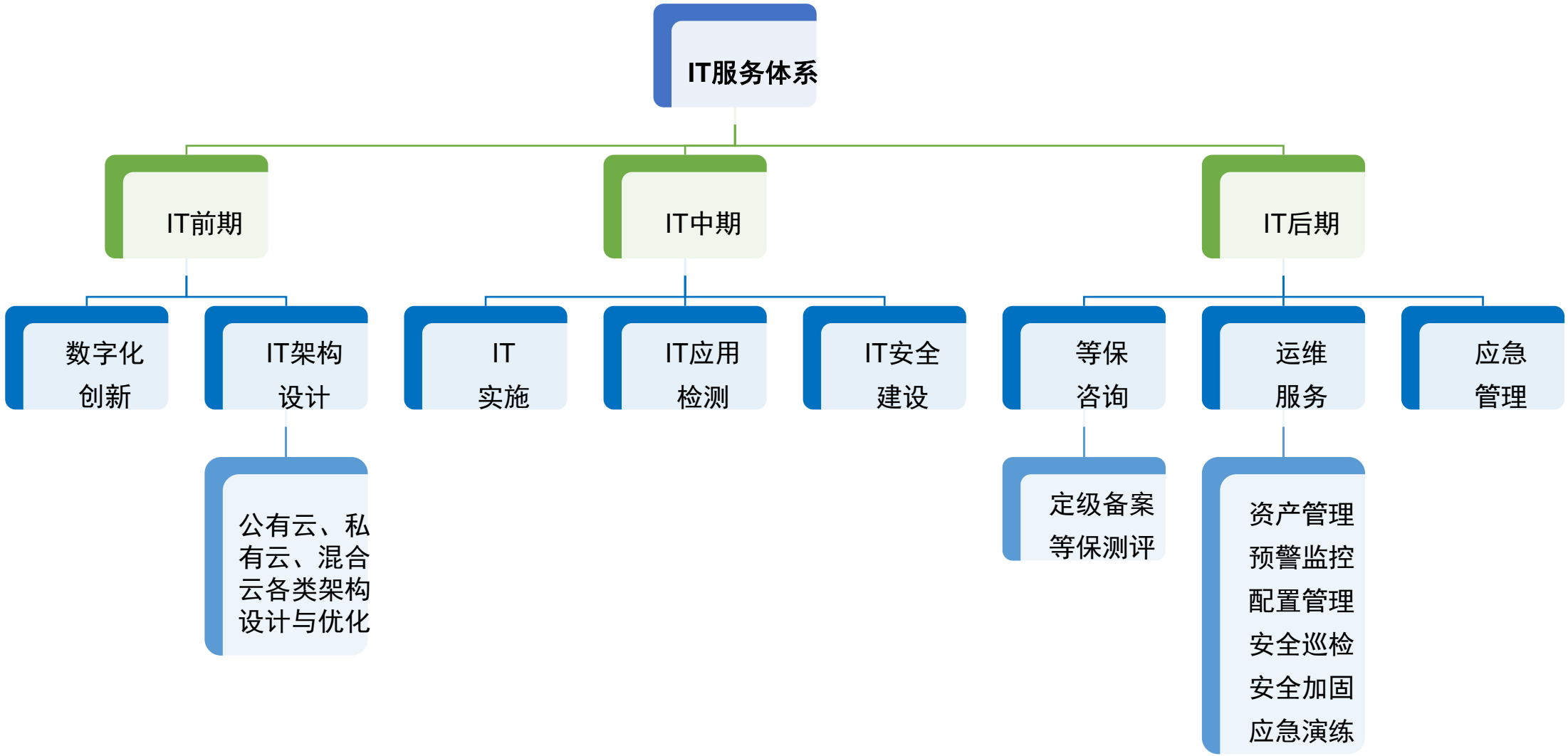
2022-2024年助力企业轻松步入AI时代

企业愿景：中国领先智能安全服务商

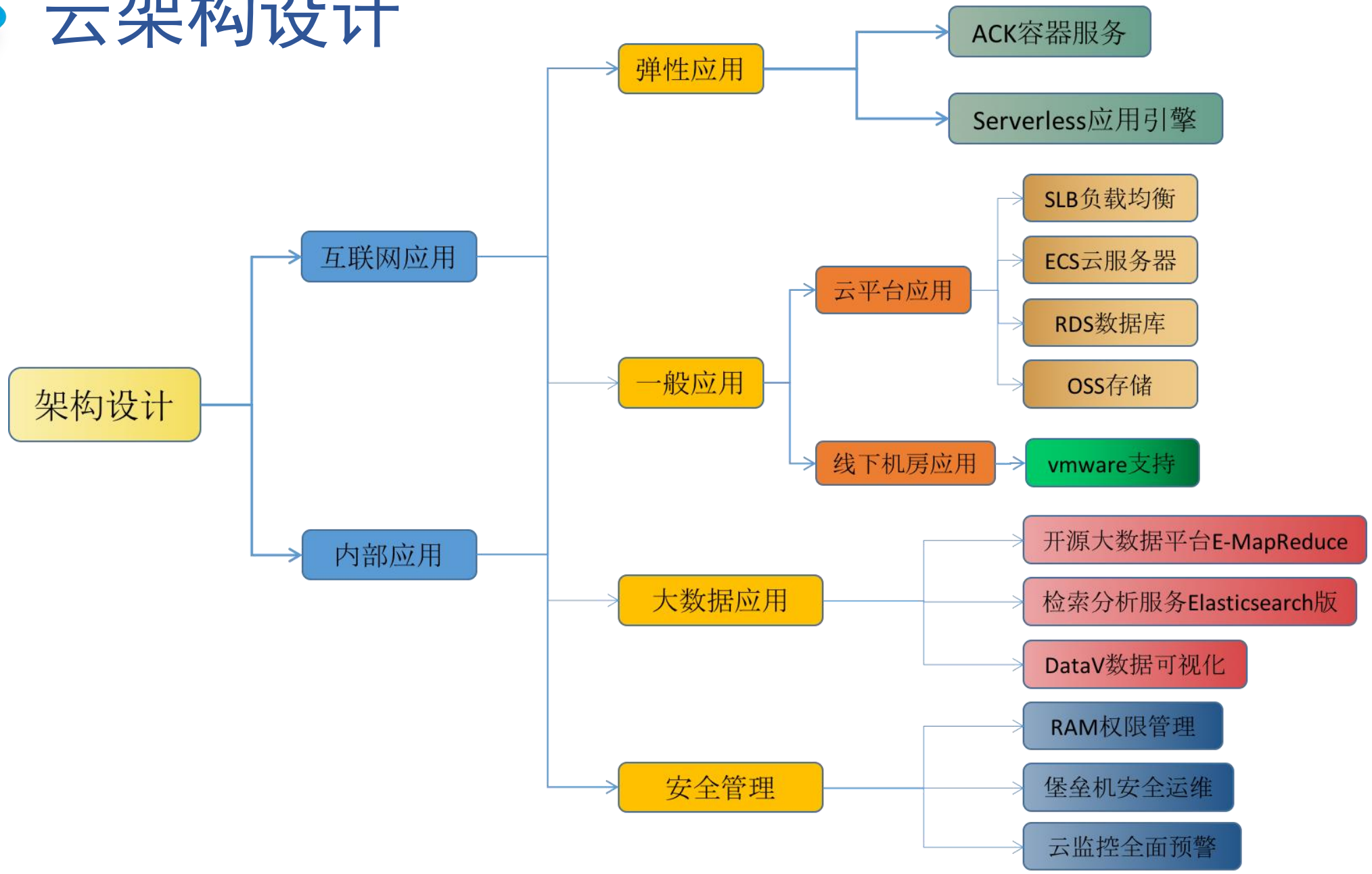
企业宗旨：助力企业轻松步入AI时代

企业文化：精益求精、真诚守信、团结一心、勇于创新

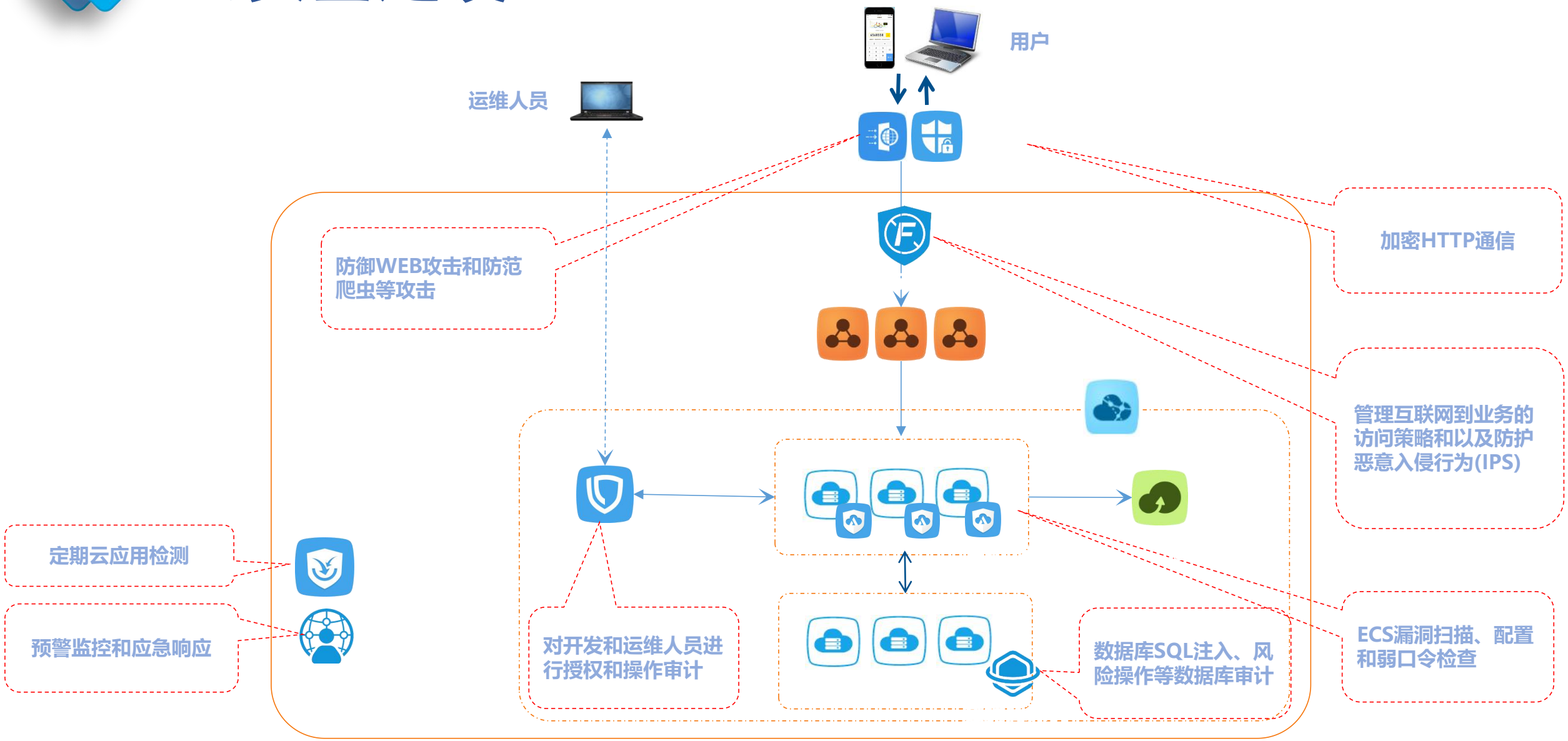
IT咨询服务


IT服务体系
IT前期
IT中期
IT后期
数字化
创新
IT架构
设计
公有云、私有云、混合云各类架构设计与优化
IT
实施
IT应用
检测
IT安全
建设
等保
咨询
定级备案
等保测评
运维
服务
资产管理
预警监控
配置管理
安全巡检
安全加固
应急演练
应急
管理

云架构设计


架构设计
互联网应用
内部应用
弹性应用
ACK容器服务
Serverless应用引擎
一般应用
云平台应用
SLB负载均衡
ECS云服务器
RDS数据库
OSS存储
线下机房应用
vmware支持
大数据应用
开源大数据平台E-MapReduce
检索分析服务Elasticsearch版
DataV数据可视化
安全管理
RAM权限管理
堡垒机安全运维
云监控全面预警

云安全建设


用户
运维人员
防御WEB攻击和防范爬虫等攻击
加密HTTP通信
管理互联网到业务的访问策略和以及防护恶意入侵行为(IPS)
定期云应用检测
预警监控和应急响应
对开发和运维人员进行授权和操作审计
数据库SQL注入、风险操作等数据库审计
ECS漏洞扫描、配置和弱口令检查

智能IT运维

网络安全法及等级保护系列标准

客户服务平台　　工单服务平台

云网监测系统　　统一安管系统　　智能处置系统

应用系统梳理　　人员职责分工　　资产统一管理

SLA管理　配置管理　容量管理　可用性管理　备份/恢复

巡检/加固　变更管理　应急预案　事件/问题　知识库管理

实时监测告警　　关联分析定位　　AI自动化处置

应用系统：网站、APP、微信小程序、互联网应用系统

中间件：apache、tomcat、mysql、oracle、redis、mongoDB等

云平台：云平台、操作系统、容器云、大数据平台等

ISO20000/27001

专业服务团队


中国信息安
China Information Technology
注册信息安全专
Certified Information
首次注册：2004年9月21日
Certified Since
发证日期：2017年4月28日
Issue Date
有效期：2017年4月28日
Valid thru
注册信息安
CERTIFIED IN
SECURITY E
阿里云
Alibab
Alibaba
Certificate ID: PSA-ACSA008-20200468
Valid Until: Jun 22, 2024
Alibab
Alibaba Cloud
Certificate ID: PSA-ACSA014-20200286
Valid Until: Apr 26, 2024
cisco
Cisco Certified N
Date Certified June 29, 2019
Valid Through June 29, 2022
Cisco ID No. CSCO13479947
Chuck Robbins
Chief Executive Officer
Cisco Systems, Inc.
Alib
Alibab
Certificate ID: ACP0
Valid Until: Nov 23, 2022
ACP
Cloud Security
D: ACP04200600170291
Jun 27, 2022
ACP
President of Alibaba Cloud
关闭
Alibaba Cloud
Alibaba Cloud Certification
Chunjie Zhang
HAS SUCCESSFULLY COMPLETED THE ALIBABA CLOUD CERTIFICATION
REQUIREMENTS AND OFFICIALLY OBTAINED THE CERTIFICATE
Alibaba Cloud Certified Partner Solutions Architect
容器服务解决方案
PSA
President of Alibaba Cloud
Certificate ID: PSA-ACSA008-20200469
Valid Until: Jun 22, 2024

环宇服务价值

更低成本

更高效率

更加安全

环宇数通
sotote.com

智能时代　未来已来

北京环宇数通科技有限公司－中国领先的智能安全服务商

企业官网：www.sotote.com
联系地址：北京市海淀区上地三街9号F座506