等保技术白皮书

AQ-SC-040 V1.0 市场指南

目录

1. 等保背景

1.1.等保制度

网络安全等级保护制度是国家网络安全保障的基本制度、基本策略、基本方法。开展 网络安全等级保护工作是保护信息化发展、维护网络安全的根本保障， 是网络安全保障工作中国家意志的体现。最新的网络安全等级保护标准已于2019年12月1日起正式实施 (简称“等保 2.0”)。

网络安全等级保护制度体系是我国一套成体系化的信息安全政策和标准，通过开展等级保护工作，能够提升信息安全保障能力，保障信息系统安全稳定运行。《网络安全法》施行后，等级保护工作上升至法律层面，不按照等保相关要求进行安全建设将追究网络运营者及主管人员的法律责任。

• **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： • (一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任； • (二)采取防范计算机病毒和网络攻击、 网络侵入等危害网络安全行为的技术措施； • (三)采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月； • (四)采取数据分类、重要数据备份和加密等措施； • (五)法律、行政法规规定的其他义务。	• 第二百八十六条之一 拒不履行信息网络安全管理义务罪。 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，经监管部门责令采取改正措施而拒不改正， 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) 致使刑事案件证据灭失，情节严重的； • (四) 有其他严重情节的。 • 单位犯本罪的， 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， 处三年以下有期徒刑、拘役或者管制， 并处或者单处罚金。	• 拒不履行信息网络安全管 理义务，致使用户信息泄 露，具有下列情形之一的， 应当认定为刑法第二百八 十六条之一第一款第二项 规定的“造成严重后果”： • (一)致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的； • (二)致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的； • (三)致使泄露第一项、第二项规定以外的用户信息五万条以上的； • (四)数量虽未达到第一项至第三项规定标准，但是按相应比例折算合计达到有关数量标准的； • (五)造成他人死亡、重伤、 精神失常或者被绑架等严 重后果的； • (六)造成重大经济损失的； • (七)严重扰乱社会秩序的；

1.2.等保流程

定级：确定定级对象→初步确认定级对象→专家评审→主管部门审核→公安机关备案审查

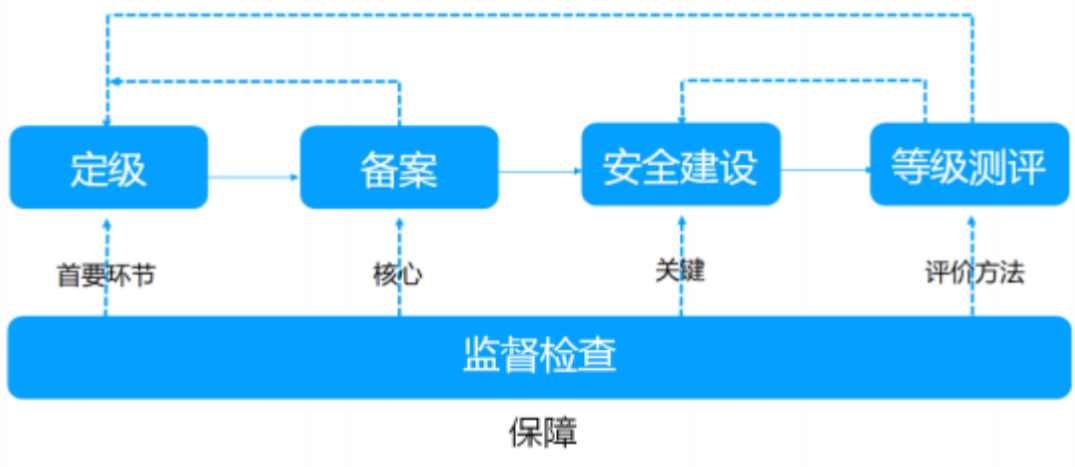
备案：持定级报告和备案表到当地公安机关网监部门进行备案

建设整改：参照信息系统当前等级要求和标准，对信息系统进行整改加固

等级测评：委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评

报告

监督检查：向当地公安机关网监部门提交测评报告，配合完成对信息安全等级保护实施情况的检查



1.3.定级依据

等级	等级定义	适用系统	测评周期
第一级	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	个人博客等	不需要测评
第二级	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严重损 害，或者对社会秩序和公共利益造成 损害，但不损害国家安全	普通网站、小门户等	每两年一次
第三级	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	用户量较大的系统，存储有较多敏感信息 的系统	每年一次
第四级	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	银行核心、电力调度 等	每半年一次
第五级	信息系统受到破坏后，会对国家安全造成特别严重损害	不能打听	依据特殊需求测评

1.4.整改要求

安全管理要求：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

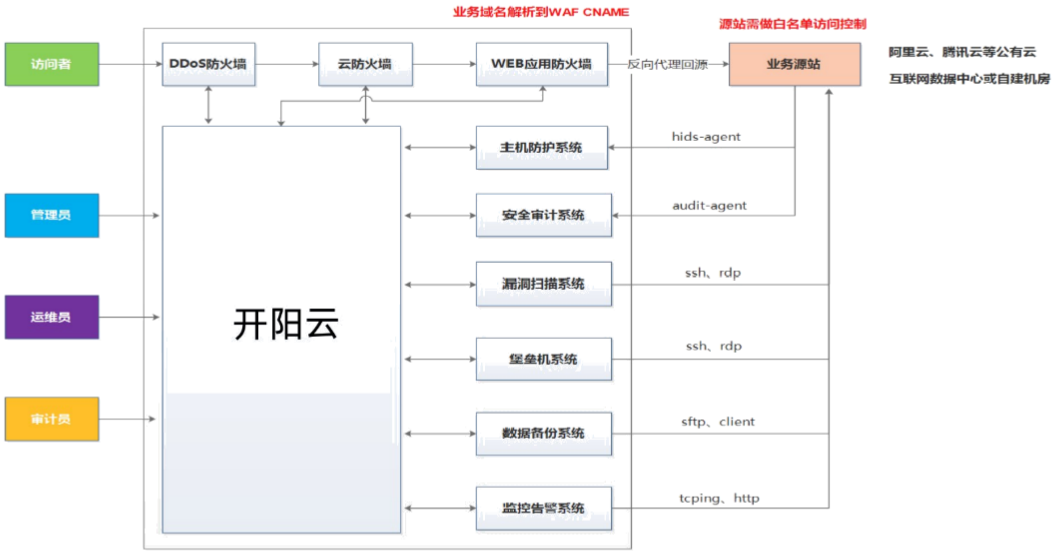
安全通用要求：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理 中心

安全扩展要求：云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工 业控制系统安全扩展要求

2. 平台介绍

2.1.平台概述

开阳云综合防御平台(等保云平台) 是一套基于开阳云计算平台构建的综合型安全运营平台， 集成了DDoS防火墙、云防火墙、WEB应用防火墙、主机防护系统、APT防御系统、漏洞扫描、数据备份、安全审计、堡垒机、态势感知等安全组件，完全满足等保2.0国家标准和企业安全运营实战需求。



2.2.安全能力

安全要求	安全组件	功能介绍
安全通信网络	云防火墙	提供统一的互联网边界、内网 VPC 边界、主机边界流 量管控防护，包括结合情报的实时入侵防护、全流量 分析可见、智能化访问控制、日志溯源分析等能力。 通过简单易用的方式交付， 全面防护各类威胁，并具备多重智能模型和智能联动手段，可持续对抗不断出现的各类新风险。支持 ACL、流控、 NAT、SSL VPN等服务。支持入侵防御和病毒防护。
安全区域边界	DDoS 防火墙	配置 DDoS 高防，将恶意攻击流量进行清洗过滤，为 用户提供的抗 DDoS 服务。 可抵御抵御 SYN Flood、 ICMP Flood 等各种常见的 DDoS 攻击，具有配置简 单、公网 IP 不用换、防护能力强、防护对象能灵活更换等特点。
	WEB 应用防火墙	通过防御 SQL 注入、 XSS 跨站脚本、常见 Web 服务器 插件漏洞、非授权核心资源访问等恶意行为攻击， 过滤海量恶意 CC 攻击，避免网站资产数据泄露，保障 网站的安全与可用性。支持 WEB 应用防护、网页防篡

		改、防扫描、黑链、漏洞分析服务等
安全计算环境	堡垒机	实现对云上服务器的集中管控和运维审计等安全能力
	安全审计	提供虚拟化审计能力， 提供数据库审计、主机审计、 应用审计、设备审计。保障云上数据及资产的安全
	数据备份	提升主机整体安全性的服务，提供威胁情报、资产采集、合规基线、漏洞风险、安全监控、入侵威胁等服务,帮助企业降低主机安全风险
	漏洞扫描	漏洞扫描服务支持对企业外部网络、主机、系统、WEB 服务、中间件、应用等进行专业漏洞扫描；针对 扫描结果形成专业漏洞扫描报告；支持对漏洞进行归 类，并提供专家级修复建议，帮助客户更加精细化管 理业务。精准的漏洞扫描及安全风险检测，漏洞扫描 结合情报大数据、透测试实战经验和深度机器学习， 提供全面资产威胁检测，
安全管理中心	云综合防御平台	安全管理中心统一管理云平台安全组件上的能力，通 过数据分析提供合理的资源调配，控制运维成本开支提升管理效率。

3. 平台功能

3.1.DDoS 防火墙

DDoS 防火墙以开阳云覆盖全球的DDoS防护网络为基础，结合开阳云AI智能 DDoS防护体系， 提供T级别的DDOS攻击防护， 打破了传统集中式高防架构的局限性，以布局全球的高防集群和数据中心资源为基础结合智能调度算法，实现全网分布式联动防御，有效抵御超大流量DDoS、CC攻击，保证业务的安全、快速、可持续交付；

策略配置：随支持根据流量触发阈值和防御阈值来选择宽松、适中、严格、超级严格等防护策略；支持一键开启或关闭 DDoS 防护。

屏蔽列表：支持对入侵IP进行自动屏蔽；支持对已屏蔽IP进行解除屏蔽；支持一键释放全部屏蔽IP。

黑白名单：支持对入侵IP进行自动加黑处理；支持手动添加黑名单和白名单数据；支持删除已有的黑名单或白名单。

流量分析：支持查看每分、每时、每月、每年的流量数据；支持查看最大输入流量、最大输出流量、平均输入流量、平均输出流量。

连接分析：支持查看每分、每时、每月、每年的连接数据；支持查看最大TCP连接次数、最大UDP连接次数、平均TCP连接次数、平均 UDP连接次数。

攻击分析：支持按攻击时间、攻击类型、攻击状态、攻击目标进行多条件查询；支持查看攻击的目的地址、目的端口、开始日期、开始日期、结束日期、攻击类型、高层协议、攻击状态、最大流量、攻击源地址。

3.2.云防火墙

平台基于“一个中心三重防护”的合规理念进行设计，结合控制转发与管理审计分离 的设计思路， 由云防火墙实现安全通信网络和安全区域边界的防护。云防火墙组件构成一 体化全方位的防御体系能够基于传统防火墙的五元组进行安全策略配置，还可以基于应用、用户、时间等条件进行安全策略配置。提供一体化的策略，对于所有策略条件进行融合， 提供统一配置界面。此外，云防火墙由于采用商用高性能大规模防火墙，能有效抵御DDOS攻击外， 基于开阳云网络全球范围内的有效应用进行识别，可对全球URL分类过滤，基于云 端推送的威胁进行防御， 结合第三方入侵防护，病毒过滤技术进行有效防护。

访问控制策略： 随着WEB2.0技术的蓬勃发展和动态端口的新应用层出不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，而云防火墙基于7元组以及时间的访问控制策略， 能有效的控制自然人、应用的访问控制；

入侵防御： 在蠕虫、后门、木马、间谍软件、 Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，并随时关注业界最 新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提 供更新，实时完善攻击特征库， 提供最及时、最全面的入侵防御。

病毒防护：实时病毒连接阻断，病毒事件日志记录，提供超过 800W 条病毒特征数据。

APT威胁检测：支持对可疑域、可疑IP、可疑文件、可疑HTTP、恶意端口扫描、DNS消耗等威胁进行实时监测与防护。

3.3.Web应用防火墙

Web应用防火墙，是一款集静态资源、缓存、代理、安全防护、日志、统计、监控于 一体的智能WEB应用防火墙。可以对内部的业务访问进行访问控制和业务审计，防范来自内部的威胁。相比于传统的硬件WAF，等保云的虚拟WAF更专注于WEB应用自身的漏洞，并基于开阳云网络全球海量防御节点和资深的安全技术能力，结合开阳云网络态势感知平台、全球智能调度系统，提供无上限防护DDoS攻击服务，WEB攻击防御，并且提供了SSL 加速， 应用负载均衡等WEB应用安全模块，为业务安全保驾护航。

常见Web应用攻击防护：

1) 防御OWASP常见威胁：支持防御以下常见威胁：SQL注入、 XSS跨站、 Webshell上传、后门隔离保护、命令注入、非法HTTP协议请求、常见Web服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

2) 网站隐身：不对攻击者暴露站点地址、避免其绕过Web 应用防火墙直接攻击。

3) 识别精准：内置语义分析+正则双引擎，黑白名单配置，误报率更低。支持防逃逸， 自动还原常见编码，识别变形攻击能力更强。

4) 0day 补丁定期及时更新：防护规则及时更新最新漏洞补丁，第一时间全球同步下发最新补丁，对网站进行安全防护。

CC攻击防护：

1) 对单一源 IP 的访问频率进行控制，基于重定向跳转验证， 人机识别等。

2) 针对海量慢速请求攻击， 根据统计响应码及 URL 请求分布、异常 Referer 及 User-Agent 特征识别， 结合网站精准防护规则进行综合防护。

精准访问控制

1) 支持 IP、Path、Referer、User-Agent 等 HTTP 常见字段的条件，配置强大的 精准访问控制策略。

2) 与 Web 常见攻击防护、 CC 防护等安全模块结和， 搭建多层综合保护机制； 依据需求，轻松识别可信与恶意流量。

3) 支持黑白名单、国家地区运营商封锁、 SSL 管理， TCP/HTTP/WS 协议反向代理， CDN 缓存加速。

高级 Web 应用安全防护

1) 支持多种端口： 支持除 80 和 443 以外的非标端口的防御需求。

2) 扫描器爬虫防护：自定义扫描器与爬虫规则，用于阻断非授权的网页爬取行 为，添加定制的恶意爬虫、扫描器特征， 使爬虫防护更精准。

3) 黑白名单设置： 添加始终拦截与始终放行的黑白名单 IP，增加防御准确性。

4) 网页防篡改：对网站的静态网页进行缓存配置，当用户访问时返回给用户缓 存的正常页面， 并随机检测网页是否被篡改。

5) 网站反爬虫：动态分析网站业务模型，结合人机识别技术和数据风控手段， 精准识别爬虫行为。

6) 误报屏蔽： 针对特定请求忽略某些攻击检测规则， 用于处理误报事件。

7) 隐私屏蔽： 避免在防护事件日志中， 出现用户名或者密码等敏感信息。

8) 防敏感信息泄露：防止在页面中泄露用户的敏感信息，例如：用户的身份证 号码、手机号码、电子邮箱等。

3.4.漏洞扫描

开阳云网络等保云经过多年的安全研究沉淀和全球服务实践经验的基础上，研发的一款 用于评估网络运行环境风险的产品，可以对各类服务器、网络设备、安全设备等操作系统 环境、数据库环境、 WEB 应用等进行综合漏洞扫描检测。该系统主要用于分析和指出存在 的相关安全漏洞即被测系统的薄弱环节，给出详细的检测报告， 在业务环境受到危害会签 为安全管理员提供专业、有效的安全分析和修补建议。该系统从系统扫描、 Web 扫描、数 据库扫描、安全基线扫描和弱口令扫描五大类发现信息系统、网站页面、数据库安全漏洞， 检查系统存在的弱口令， 收集系统必要开放的账号、服务、端口，检查不合规的设备配置， 形成整体安全风险报告， 帮助安全管理人员限于攻击者发现安全问题， 及时进行自我修补。

系统扫描：主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节， 给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建 议。 全方位检测信息系统存在的主机、 软件的安全漏洞，安全配置问题， 弱口令， 不必要开放的账户、服务、端口，独创的端口识别技术，结合丰富的协议指纹库， 能自动快速准确的识别出非标准开放端口和应用服务类型， 准确扫描端口对应的 服务漏洞， 避免扫描过程中的漏报和误报；

Web 扫描：全面支持 OWASP 检测， 可以帮助用户充分了解 Web 应用存在的安全隐患，建立安全可靠的 Web 应用服务， 改善并提升应用系统抗各类 Web 应用攻击的 能力(如：注入攻击、跨站脚本、文件包含、钓鱼攻击、信息泄漏、恶意编码、 表单绕过等)，协助用户满足等级保护、 PCI、内控审计等规范要求；

3.5.主机防护系统

适应公有云、私有云及混合云架构，采用自适应安全及端点检测及响应 (EDR)的解决 方案， 提供云+端的云安全管理平台为用户解决公有云、私有云和混合云环境中可能遇到的 安全及管理问题；独立的自助安装界面， 支持自动生成下载和安装命令。

系统支持： 支持 Windows 2003、Windows 2008、Windows 2012、Windows 2016、Ubuntu、Centos、RedHat、Fedora、Suse、OpenSuse、Debian 等操作系统

主机体检：支持采集已安装轻代理主机中的各类信息，支持采集主机内外网 IP、主机名、操作系统、安装时间、在线状态等信息； 支持对主机进行一键体检。

文件事件：支持检测暴力破解、账号异常登录、进程异常等安全事件

病毒查杀：支持发现二进制病毒木马信息， 包含病毒的 hash、路径、发现世界，并且提供对病毒的隔离。

合规基线：提供常用的linux及windows系统基线模板，支持基线检查及异常项展示,并提出修复建议。

完整性监控：监控文件和目录的完整性情况，包括文件被修改、删除和新增。

3.6.安全审计

提供数据库安全审计、主机安全审计、应用安全审计；以高性能日志采集能力与强大 的分析功能，对大量分散数据库、主机及应用的日志进行统一管理、集中存储、统计分析、快速查询， 为用户提供真正可信赖的事件追责依据和业务运行的深度安全。

数据库审计： 支持 MySQL、Oracle、SQL Server、MongoDB 等市面上大多数的数据库日志审计。多维度分析，识别并预警风险语句。

日志审计： 支持对Windows、 Linux 等主机日志审计、支持Nginx、IIS、Tomcat 等应用中间件日志审计、支持各种网络设备的日志审计。

报告订阅： 提供丰富的报告展示，可订阅日报、周报、月报。

安全告警： 支持自定义告警规则；支持按关键词、告警周期、目标资产进行指定告警规则； 支持站内信、邮件、钉钉等方式告警。

3.7.堡垒机

提供的核心系统运维和安全审计的管控平台， 可集中管理资产权限，全程管控操作行 为，实时还原运维场景， 保障运维行为身份可鉴别、权限可管控、操作可审计，解决众多 资产难管理、运维职责权限不清晰以及运维事件难追溯等问题， 助力企业满足等保合规需求。

资源管理： 集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。支持 SSH、RDP、VNC、TELNET 等协议类型主机资源。

运维审计： 全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。

3.8.数据备份

为云内的云服务器、云硬盘进行备份，通过备份快速恢复数据，保证业务安全可靠。在数据误删除、云服务器宕机、黑客攻击或病毒入侵情况下都可以通过备份快速恢复数据，保证业务不受影响。

4. 开阳云等保合规解决方案

4.1.等保建设SaaS方案

4.1.1. 【方案描述】

智云保(等保建设 SaaS 服务)，以开阳云一站式等保云平台+安全合规专家的服务形式， 为客户提供一站式等保咨询整改服务。产品完全云化部署， 客户通过 IP 地址切换、 DNS 域名切换等方式接入，无需对现有系统的软件、硬件做任何迁移或调整。不需要客户具备专 业安全知识，安全专家全程指导操作。最快 10 分钟内可实现无缝快速接入；

4.1.1. 【适用场景】

客户待测评系统的源站是在互联网中可访问的 (公有云、私有云、VPC、IDC 等场景均满足) ，特别适用于那些没有安全运维人员、没有特殊的数据私密安全要求、想省心过等保的企业客户。只需在等保平台上开通账号并配置待测评系统相关信息后，即可满足等保测评要求。

4.1.2. 【方案优势】

功能丰富：多种安全组件满足用户在等保建设过程中所需的各类安全防护需求。
配置灵活： 安全组件能够持续更新和扩展，为用户持续提供全方位的防护。
管理统一： 安全组件通过内部网络通讯联动，出现安全事件时可快速做出响应。
部署快速： 采用 All In One 的设计理念，缩短安全服务的交付周期
一站式服务： 一站式合规检测服务，覆盖等保2.0检测、隐私合规检测、安全合规检测、等保过检加固。

4.1.3. 【接入流程】

登录开阳云一站式等保云平台，配置 WAF 回源规则，获得高防 CNAME 并更换业务域名解 析为高防 CNAME，完成业务流接入。
登录测评系统关联的服务器，安装和配置主机防护 agent、安全审计 agent，然后登录开阳云一站式等保云平台配置堡垒机和数据备份，完成管理流接入。

4.1.4. 【计费方式】

计费方式： 半年、包年计费；
根据客户实际等保评级(二级或三级)情况， 按测评系统套数收费。

4.1.5. 【产品套餐】

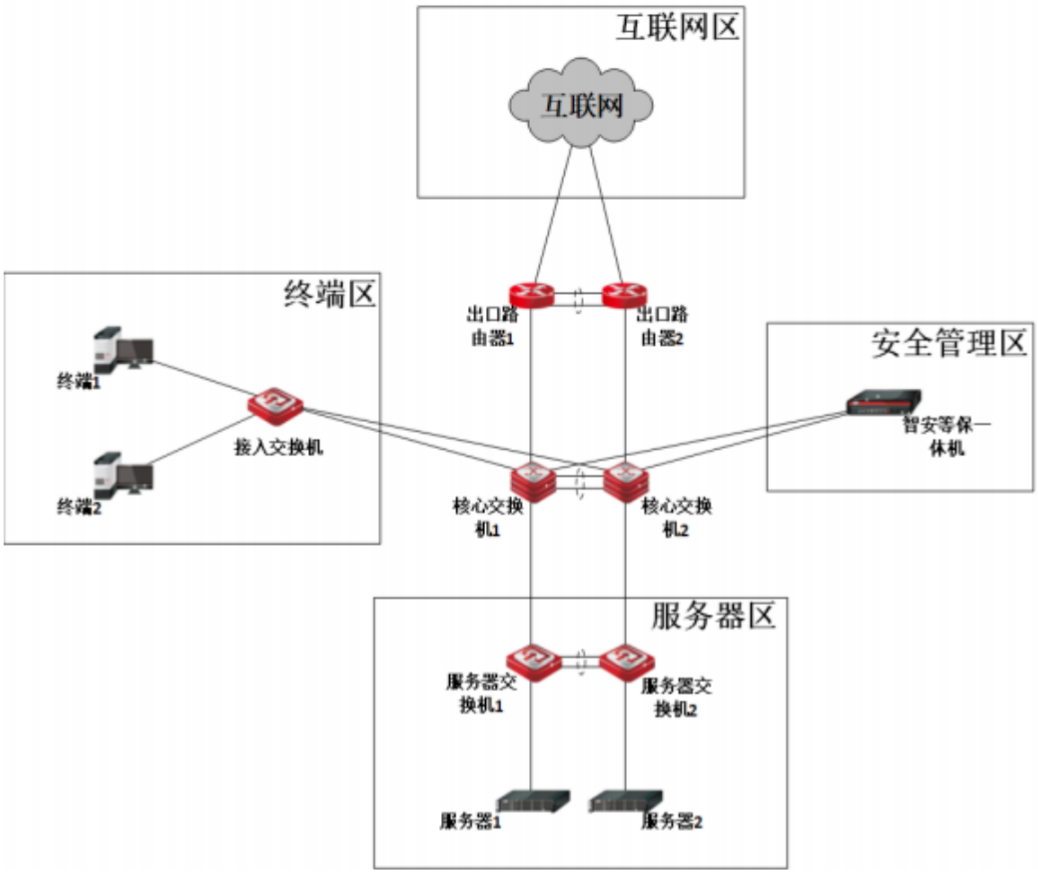
安全组件	等保二级	等保三级
DDoS 防火墙		√
云防火墙	√	√
WEB 应用防火墙	√	√
堡垒机		√
安全审计	√	√
主机安全	√	√

数据备份		√
漏洞扫描		√
管理中心	√	√

4.2.开阳云等保一体机(硬件一体机方案)

4.2.1. 【方案描述】

由开阳云提供全套软硬件部署及运维服务，满足客户本地私有化、定制化需求。开阳云等 保一体机部署在安全管理区，接入核心交换机，并需要将办公流量通过路由方式引导到一 体机的防火墙，经防火墙处理后再回到办公区，业务流量通过域名解析方式引导到一体机 的防火墙， 经防火墙处理后通过反向代理等技术回到业务区。



4.2.1. 【适用场景】

适用于有自建机房、对数据私密安全有要求的企业客户。只需将一体机旁挂到核心交换机 上，并做相应的网络初始化配置。即可完成等保一体机接入。完成一体机接入后，在安全 管理平台中配置测评系统相关信息， 即可满足等保测评要求。

4.2.2. 【方案优势】

数据私密安全：数据私有化隔离；容灾备份机制； 算法、密钥双重保险，数据安全可 靠；独享云资源，速度更快，性能更优。

企业自主掌控：客户完全自主掌控，轻松实现成员管理、认证配置、身份源管理；用 户信息和密钥信息本地存储。

4.2.3. 【产品配置】

产品名称	产品说明

硬件服务器	标准版(ZA-Scloud-A-100)： 配置： CPU：10 核 20 线程，内存： 64GB，硬盘： 4T 规格：支持接入 5 个一级域名 20 台主机 增强版(ZA-Scloud-A-200)： 配置： CPU：20 核 40 线程，内存： 96GB，硬盘： 16T 规格：支持接入 10 个一级域名 40 台主机 旗舰版(ZA-Scloud-A-300)： 配置： CPU：20 核 40 线程，内存： 96GB，硬盘： 16T 规格：支持接入 15 个一级域名 60 台主机
安全管理平台	统一提供底层基础硬件平台、安全虚拟化平台、安全资源池管理平台、 安全模块。安全虚拟化平台实现计算资源、存储资源、网络资源、网络 功能资源、安全功能等 IT 基础资源的虚拟化。集中管理安全功能
云防火墙	提供基础防火墙功能基本访问控制
WEB 应用防火墙	提供网站入侵防护、业务访问风险、网址传播护航等安全服务

4.2.4. 【接入流程】

客户需进行网络配置将流量引导到一体机

4.2.5. 【计费方式】

硬件质保 3 年+系统授权服务时间 1 年+第二年开始按 10%的费用收取作为维保费用

4.3.私有化部署方案

4.3.1. 【方案描述】

由客户出硬件资源和网络资源，由开阳云提供软件部署及运维服务。满足客户本地私有化、定制 化需求。

4.3.1. 【适用场景】

1) 客户业务系统在云上 VPC 等专有网络中，互联网无法直接访问的场景。
2) 客户业务系统体量较大，一体机配置无法满足其需求的场景。

4.3.2. 【方案优势】

1) 数据私密安全：数据私有化隔离；容灾备份机制；算法、密钥双重保险，数据安全可靠；
独享云资源，速度更快，性能更优。
2) 企业自主掌控：客户完全自主掌控，轻松实现成员管理、认证配置、身份源管理； 用户信息和密钥信息本地存储。

3) 资源可扩展： 随着后期业务的增长或变化，可动态调整资源配置。

4.3.3. 【计费方式】

私有化部署费(按年收费) +等保服务费(与等保云 SaaS 服务费一致) +OEM订制费(可选，只收取一次费用)。

5. 客户案例

5.1.河北省某地级市政府

项目背景： 客户是河北省下辖的一个地级市， 位于河北省东南部，客户需要对市人民政府、市 司法局、市教育局等 37 个市级门户网站进行等保测评。

整改方案：客户通过购买我司【等保云产品】，将需要测评的域名和源站 IP 配置到 我司等保平台中，通过修改域名 DNS 解析后即可完成业务系统的流量接入，从而使用 DDoS 防护、 云防火墙、WEB 应用防火墙等安全服务。
针对主机安全、 日志审计和数据库审计等安全服务，则需客户在需要测评的服务器上安装我司提供的 agent，从而完成日志采集和安全防护。 针对堡垒机和漏洞扫描等安全服务，客户 只需在等保云平台上进行主机或 WEB 信息配置，即可完成资产的统一管理。
在我们安全专家的全程指导下,客户通过不到半天的时间,就完成了所有信息的配置和接 入。最终通过等保三级测评，获得等级保护备案证明于等级保护测评报告。

客户价值：客户通过开阳云的一站式等保服务， 省心省力的完成了所有的业务系统整改，满足了 等级保护安全建设标准，同时也提升了客户各政务网站的安全防护能力，有效抵御各类网络攻击。

5.2.四川省某投资集团

项目背景：客户是四川省委省政府批准组建的大型旗舰型企业集团。该集团拥有 200 多家子公 司，分子公司业务系统众多。集团自身的信息等保定级为三级，下属二级单位的部分业务系统， 例如账单管理系统的等保定级为二级。总公司和每个子公司均有自己的机房，业务系统独立， 信息化建设也各自进行。集团的信息中心负责集团的信息化建设， 没有额外的安全团队进行进 一步的信息安全专门管理工作。因此如何基于一套安全标准准则进行管理成为当前企业的需求。

解决方案： 由于客户是自建机房，并且对数据私密性有一定要求，因此，通过采购我司【开阳云 等保一体机】产品，并将等保一体机旁挂到客户的核心交换机上，从而完成设备的接入。客户 只需将待测评系统信息配置到一体机的安全管理平台中，即可完成业务系统的整改接入， 从而达到等保合规要求。在对客户业务系统的整改同时，我们的安全专家也对客户机房环境的等保 整改输出了详细的方案，确保客户的安全物理环境也满足等保合规要求。

客户价值：客户的信息部门认为，通过独立信息安全设备【开阳云等保一体机】的综合部署，能够快速满足等保的需求， 并且不影响到已有设备的使用。同时，一体机的部分功能能够切实应用到日常信息安全工作中， 例如日志审计模块，是进行系统审计的必备功能， 这让一体机成为了非常高性价比的信息安全投入。

6. 关于我们

成都傲游风口信息技术有限为创新的分布式云及安全服务商，以网络安全为主要产品及业务方向，提供一站式等保服务和一站式网络安全服务，致力于做客户在云时代的最佳安全防护合作伙伴，为客户提供一站式全球化云计算与网络安全解决方案。