

成都索贝数码科技股份有限公司
公有云系统网络安全等级保护三级
建设规划方案

2024年11月1日

目录

1. 安全建设依据	1
1. 1. 依据国际等级保护标准.....	1
1. 2. 依据安全建设目标.....	1
1. 3. 依据成都索贝数码科技股份有限公司实际需求	1
1. 4. 把握安全成本和效益的平衡.....	1
2. 安全建设现状	2
2. 1. 网络拓扑情况	2
2. 2. 等级保护标准差距分析.....	3
2. 2. 1. 合规性差距分析	3
2. 2. 2. 综合安全能力差距分析.....	4
3. 安全设计.....	5
4. 安全体系建设设计	7
4. 1. 安全通信网络建设	7
4. 2. 安全计算环境建设	7
4. 2. 1. 数据库审计系统	7
4. 2. 2. 主机安全加固系统	7
4. 2. 3. 漏洞扫描系统	8
4. 3. 安全管理中心建设	9
4. 3. 1. 运维审计系统	9
4. 3. 2. 云安全威胁分析感知系统	9
4. 4. 安全管理体系建设	10
4. 4. 1. 安全管理制度	10
4. 4. 2. 安全管理机构	11
4. 4. 3. 人员安全管理	11
4. 4. 4. 系统建设管理	11
4. 4. 5. 系统运维管理	11
5. 建设意义	13



1. 安全建设依据

1. 1. 依据国际等级保护标准

《信息安全技术网络安全等级保护基本要求》GB/T22239-2019 是我国针对等级保护的标准主体文件，是我国实行等级保护制度安全建设环节的国家标准。

1. 2. 依据安全建设目标

根据成都索贝数码科技股份有限公司的实际情况，此次建设具体参照第三级安全保护能力的详细标准内容。

建成后将实现：应能够在统一安全策略下防护系统免受来自拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

1. 3. 依据成都索贝数码科技股份有限公司实际需求

满足基本安全防护要求是保证信息系统具有相应等级安全保护能力的前提。但针对于成都索贝数码科技股份有限公司来说，相关信息系统是一个整体，除了依据本文提出的分层面采取各种安全措施，需从资源数据和监控数据的特殊性等方面考虑总体性要求，保证信息系统的整体安全保护能力。

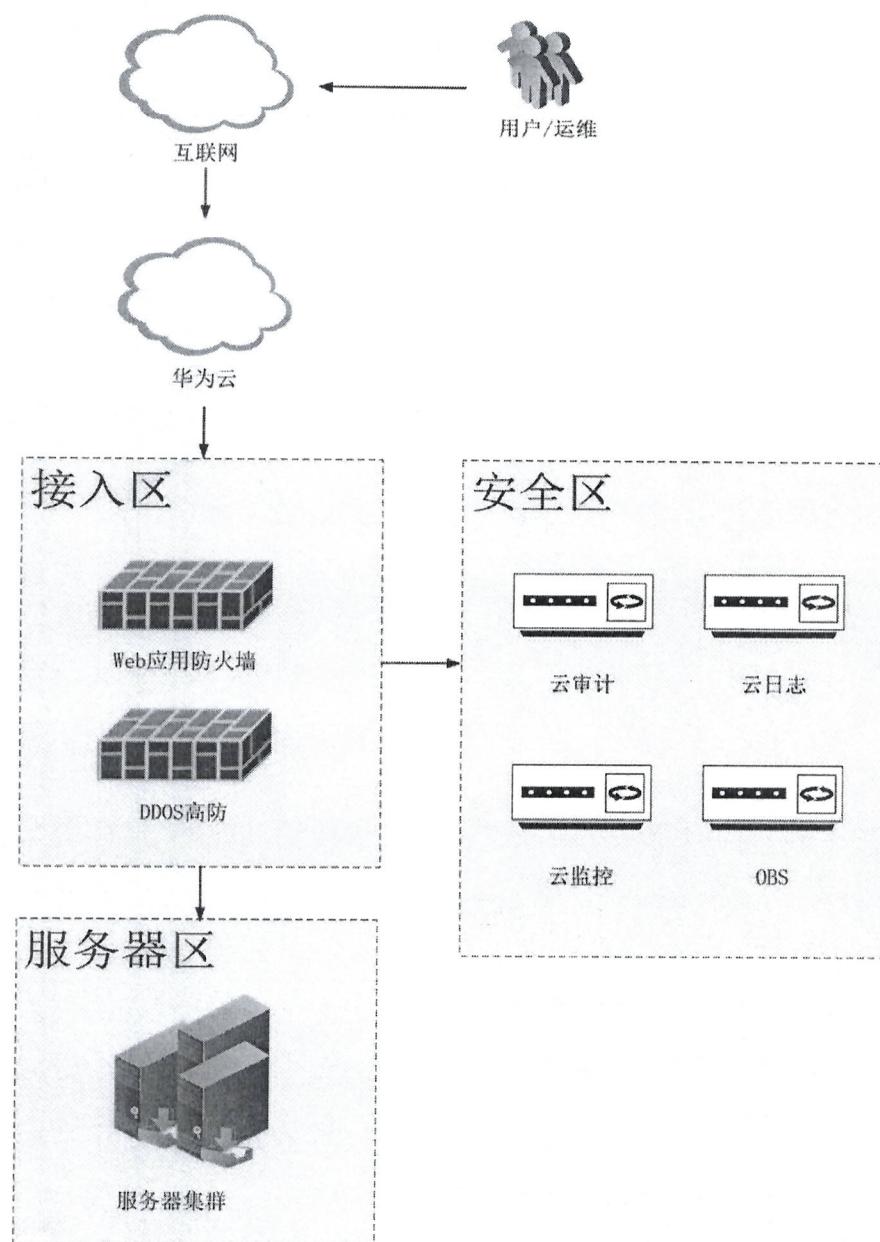
1. 4. 把握安全成本和效益的平衡

据国际标准组织 ISO 的信息安全管理者的 27001 标准要求，信息安全建设最核心的内容就是风险管理，并将风险始终控制在可接受的范围之内。因此不是无限制的进行安全建设规划，应在满足关键信息资产需求和达到国家行业相关标准要求的基础上找到安全成本效益平衡点。按照核心信息资产安全需求优先、分期分阶段建设的规划进行安全体系建设。

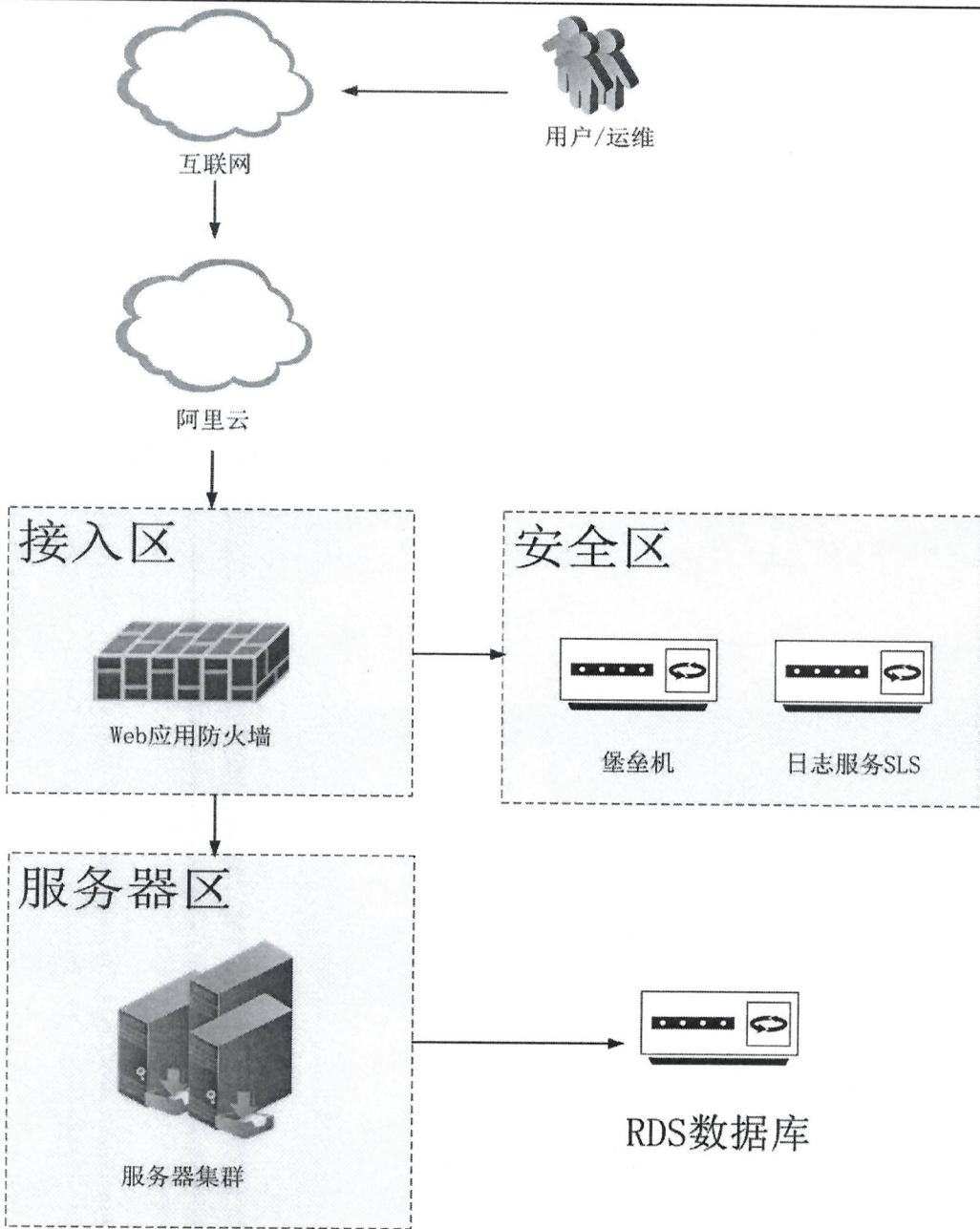
2. 安全建设现状

2.1. 网络拓扑情况

现阶段拓扑情况如下：



图一 华为云网络拓扑图



图一 阿里云网络拓扑图

2.2. 等级保护标准差距分析

2.2.1. 合规性差距分析

- 公有云侧安全防护不完善：根据《信息安全技术-网络安全等级保护基本要求》（GB/T 22239-2019）要求，云平台与云上业务系统应分开定级，同时云

平台不得承载高于自身安全等级的业务系统。当前除 WEB 应用防火墙、DDO 防护外，云平台上业务系统安全防护能力比较弱。

➤ **管理中心待建立：**已部署云日志、云审计，但与等保 2.0 第三级的安全功能要求相差甚远，无法应对多样的安全威胁。需补充主机安全加固、堡垒机、数据库审计等安全能力，从而具备入侵防护、漏洞发现、病毒查杀、终端管控、安全审计、集中管控、安全管理等安全能力。

2.2.2. 综合安全能力差距分析

➤ **预警取证不强力：**取证溯源是安全闭环的重要流程，也是合法合规的必要措施。当前威胁发现及时应急响应能力存在不足，面临安全人员匮乏，专业能力不足的问题。一旦出现安全问题，无法进行有效处置及安全预警。

➤ **管理工作难落实：**随着自身信息化的发展，业务和资产增多，安全人员需承担大量的安全管理、运维工作，若缺乏健全的管理制度、清晰的职能定位，安全管理、运维工作难以开展，安全管理责任难以落实。

➤ **建设模式不完整：**公有云上业务系统是重点攻击目标，数据全生命周期安全防护是守牢数据安全底线，切实防范数据篡改、泄露和滥用的重要保障。当前除在通信传输过程中采用 VPN 进行管道通信加密传输外，无数据从采集到销毁全生命周期过程的防护与监测措施，急需补足数据安全能力，逐步过渡到以业务+数据双核心驱动阶段。通过外防+内控的建设模式，抵御外部威胁，做好内部管控。

➤ **安全体系不健全：**网络安全是个动态的过程，除了增补安全防护设备，健全安全管理制度外，需以用户安全的全生命周期需求为导向，从暴露面监测、防御强化、威胁分析、应急处置、安全运营等五大维度，有机结合安全运营梯队、标准化运营流程、闭环的安全运营体系。

3. 安全设计

该阶段以满足等保合规要求为主要目标，通过增补公有云上安全防护措施，并配套部分必要的网络安全服务，构建基础的网络安全防护与合规能力。根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019），遵循“一个中心三重防御”的建设思路。

➤ 安全通信网络

- 1) 采用密码技术或其他有效措施，保证系统管理数据、鉴别信息和重要业务数据在传输过程中的完整性、保密性。

➤ 安全计算环境

- 2) 在虚拟机上部署主机加固软件，实现主机病毒防护，并通过后台的管理中心实现统一管理。
- 3) 在安全管理中心部署漏洞扫描设备或购买漏洞扫描服务，定期对全网进行安全威胁检测，并根据检测结果进行整改加固，防范于未然。
- 4) 在安全管理中心或数据库服务器前放置数据库审计系统，实现对数据库操作行为的统一审计，发现数据库风险、及时响应，保障数据安全。

➤ 安全管理中心

- 1) 在安全管理中心部署运维审计系统，实现资产管理、运维过程的全程监控。
- 2) 在安全管理中心集中部署主机加固管理中心、云安全威胁感知系统。满足等保 2.0 第三级的安全功能要求，加强入侵防护、高级威胁防护、集中管控、安全管理等安全能力，有效应对当前严峻的网络安全形式和多样的高级威胁。

➤ 安全服务体系

- 1) 通过专业的网络安全培训服务，从网络安全意识、网络安全技术、网络安全管理类等维度开展网络安全培训工作，提升内部人员网络安全意识及相关技能。

-
- 2) 通过专业网络安全咨询服务，从安全管理组织、安全管理制度、安全运维服务等维度，建立健全一体化平台的安全管理制度。
 - 3) 通过安全风险评估服务，从漏洞扫描、安全配置核查、渗透测试、可信众测等维度综合评估信息系统风险隐患，有针对性的进行安全加固。

4. 安全体系建设设计

4.1. 安全通信网络建设

采用链路冗余技术，避免关键节点存在单点故障。采用 SSL/IPsec VPN 等安全加密技术，保证通信过程中数据的完整性和保密性。

4.2. 安全计算环境建设

4.2.1. 数据库审计系统

在安全管理中心部署数据库审计系统，通过流量镜像方式，在不影响业务的情况下实现对数据库的操作行为进行审计，并对触犯规则的恶意攻击和操作行为进行告警。

通过部署数据库审计系统，实现如下安全目标：

- **漏洞检测：**对几百种不当的数据库配置、潜在弱点、数据库用户弱口令、数据库软件补丁等等的漏洞检测；
- **威胁防护：**保护业界主流的数据库系统，防止受到特权滥用、已知漏洞攻击、人为失误等等的侵害；
- **双向审计：**对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时审计，而且还可对数据库系统返回结果进行完整的还原和审计；
- **精细监控：**提供细粒度的审计规则，如精细到表、字段、具体报文内容的细粒度审计规则，实现对敏感信息的精细监控；
- **数防泄露：**内置防统方规则，防止应用系统引起的统方数据泄密。

4.2.2. 主机安全加固系统

在安全管理中心部署主机安全加固系统，并在服务器上安装防病毒客户端，对病毒、木马和恶意软件等一切已知的对计算机有危害的程序代码进行清除，并

确保系统的病毒代码库保持最新，实现恶意代码的全面防护。

同时通过文件诱饵引擎技术，实现勒索专防专杀；通过内核级东西向流量隔离技术，实现网络隔离与防护；通过补丁修复、外设管控、文件审计、违规外联检测与阻断等安全能力，提供全面的服务器安全防护。

主机安全加固系统主要功能包括：病毒查杀、微隔离、Web 攻击防护、异常进程行为监控、可疑行为检测、网络对外连接审计、防暴力破解、WebShell 扫描检测、文件完整性监控、网站漏洞防护、网站后门查杀。

4.2.3. 漏洞扫描系统

在安全管理中心部署漏洞扫描系统或通过漏洞扫描服务。对系统、数据库和网站等进行深度扫描，全方位检测信息系统存在的主机、数据库、网站、软件等安全漏洞，安全配置问题，弱口令，不必要开放的账户、服务、端口等。

漏洞扫描是一款融合安全漏洞挖掘、渗透测试技术研究和漏洞检查方法的最佳实践的基础上，集网络端口与服务扫描、弱口令扫描、主机安全扫描、应用安全扫描、数据库安全扫描和安全基线配置核查于一身的功能，结合新安全风险评估理论分析的综合安全技术扫描和管理系统。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漏洞给出相应的修补措施和安全建议。是成为加强中国网络信息系统安全功能，提高内部网络安全防护性能和抗破坏能力，检测评估已运行网络的安全性能，为网络系统管理员提供实时安全建议等的主流工具。

通过部署漏洞扫描系统，实现如下安全目标：

- **漏洞扫描：**对系统进行深度扫描，全方位检测信息系统存在的安全漏洞，安全配置问题等；
- **漏洞分析报告：**提供多维度的对比信息，产生更直观、规范的报告；
- **降低误报：**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，极大避免扫描过程中的漏报和误报。

4.3. 安全管理中心建设

4.3.1. 运维审计系统

在安全管理中心部署安全运维审计系统，运维流量必须经过堡垒机后才能到达各主机、网络、安全等设备，实现运维过程的全程监控与审计。主要功能如下：

- 对以 SSH, TELNET, FTP, SCP、SFTP、远程桌面 RDP、VNC、X11、HTTP、HTTPS、ORACLE、MSSQL、DB2, INFORMIX, MYSQL 等应用协议的集中管理与审计；
- 实现所有运维人员、服务器、网络设备、安全设备、数据库的集中管理；
- 自动改密可以对主流的 windows、linux、unix、交换机、路由器等设备，对用户最担心的密码安全方面设计了完善的策略；
- 完整记录运维管理员的运维过程，哪个账号通过哪个 IP 地址登陆了什么设备、在设备上面做了什么操作、目标设备的返回结果都会完整记录；

4.3.2. 云安全威胁分析感知系统

在安全管理中心部署云安全威胁分析感知系统，通过流量镜像的方式，进行深度威胁检测。

传统的安全设备都是基于特征库，检测和发现已知漏洞和已知威胁，对于未知威胁和未知漏洞却束手无策。而云安全威胁感知系统使用深度威胁检测技术，对流量进行深度解析，发现流量中的恶意攻击，提供了全面的检测和预警的能力。相对于仅依靠特征检测的传统安全产品，本产品可发现零日漏洞利用、未知恶意代码等高级攻击手段，能检测到传统安全设备无法检测的攻击，为用户提供更高级的安全保障。实现 web、邮件、病毒和木马威胁深度检测，利用 0day 漏洞攻击检测、异常行为分析、云端高级分析等。同时产品内置动态沙箱分析技术发现文件中的恶意行为，内部虚拟机可实现完全模拟真实桌面环境，所有恶意文件的注册表行为、敏感路径操作行为、进程行为、导入表信息、资源信息、段信息、字

字符串信息及运行截图等行为都将被发现，综合分析这些恶意行为，判断其中的可疑操作，再结合加权值分析技术，在保证发现所有恶意行为的同时，极大降低了误报。。产品基于丰富的特征库、全面的检测策略、智能的机器学习、高效的沙箱动态分析、海量的威胁情报，能实时发现网络中发生的各种已知威胁和未知威胁，检测能力完整覆盖整个 APT 攻击链。

通过部署云安全威胁感知系统，实现如下安全目标：

- 攻击预警：在攻击到达云主机之前进行检测，并进行实时的攻击预警；
- 邮件检测：对邮件协议进行深度分析，记录并分析每个邮件，并对其中的附件进行分析并检测，发现其中的安全问题；
- 恶意文件检测：对应用协议解析，在协议中分离文件，通过对病毒木马进行扫描，快速发现各种已知特征的恶意文件攻击行为；内置动态沙箱分析技术发现文件中的未知威胁；
- 取证溯源：对 WEBHELL 后门、高危恶意代码样本传播、内部主机被控回连进行预警，对攻击进行取证分析，帮助持续完善安全防护策略。

4.4. 安全管理体系建设

4.4.1. 安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修

订不足及进行改进。

4.4.2. 安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

4.4.3. 人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。

4.4.4. 系统建设管理

根据基本要求制定系统建设管理制度，包括：系统定级、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、系统备案、等级评测、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

4.4.5. 系统运维管理

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应

等级安全状态中。

5. 建设意义

- 1、全面提升成都索贝数码科技股份有限公司的信息安全防护能力，保证该单位整个网络信息系统的安全顺畅运行。
- 2、建设符合等级保护三级要求和 ISO27001 体系标准的信息安全管理体系。
- 3、维护好成都索贝数码科技股份有限公司的对外形象。避免因信息安全事件出现的经济损失、形象损失。
- 4、确保信息安全事件的事后追溯，责任定位。安全运维工作的持续高效运转。及时响应并满足上级单位及行业主管单位安全检查及相关管理规定。