解决方案实践

等保合规安全解决方案

文档版本	1.0
发布日期	2023-04-19

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 方案概述

应用场景

等保相关法律落地后企业的合规建设

客户的痛点：

等级保护建设涉及法律和技术两个层面，专业度要求高。

- 入门难：等保是企业安全建设的法律要求，但企业缺乏对新等保要求的深入了解，不知道如何着手，拖延等保整改周期，造成人力和时间的浪费。
- 挑战大：传统安全防御体系难以防御云上威胁，也不适应弹性扩缩的需要，很多企业无专业的安全技术人员，选择合适的等保整改建设方案成为极大挑战。
- 无保障：等保咨询和测评机构繁多，服务范围和质量参差不齐，与企业难以建立互信、可靠、长期的合作关系。

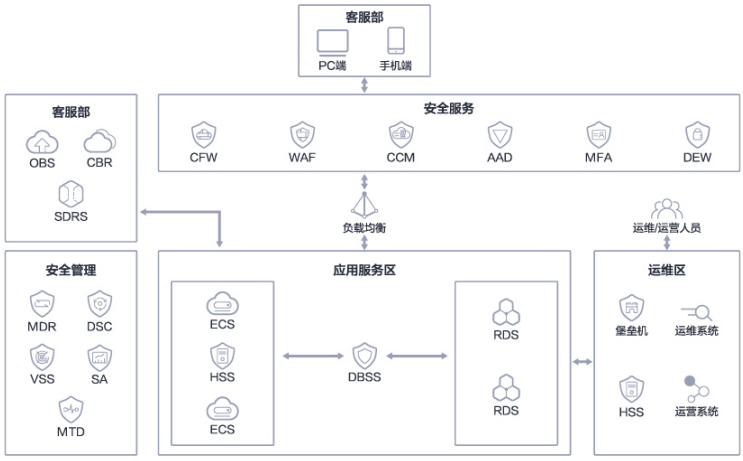
通过我们的方案实现的业务效果：

本章节介绍，华为云依托自身安全能力与安全合规生态，为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。

方案架构

根据等保2.0的基本要求，包含安全物理环境、安全通信网络与区域边界、安全计算环境、安全管理中心、安全管理制度5个层面要求。

图 1-1 架构图



- 安全物理环境

  主要包括物理位置选择，物理位置访问控制
- 安全通信网络&区域边界

  主要包括网络架构、边界防护、访问控制、通信传输、入侵防范、安全审计
- 安全计算环境

  主要包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、数据完整性和保密性、数据备份恢复
- 安全管理中心

  主要包括系统管理、审计管理、安全管理、集中管控
- 安全管理制度

  主要包括安全策略、安全管理制度与流程规范、人员组织、安全管理基线。

方案优势

- 一站式等保测评

  提供顶级备案、差距分析、规划设计、整改加固、等保测评、安全保障全流程闭环的一站式服务。
- 丰富的安全合规生态

  合作测评机构遍布30+重点省市，覆盖行业种类超10+，服务客户超2000+
- 全栈安全防护体系

  20+自主研发的云安全服务和200+伙伴安全服务，帮助客户构建立体云安全防护，满足等保合规要求。

2 资源和成本规划

表 2-1 等保二级

云资源	规格	数量	每年费用（元）
云防火墙	标准版	1	28000
Web应用防火墙	标准版	1	38800
主机安全	旗舰版	2	4000
威胁检测	初级包	1	10000
漏洞扫描	专业版	1	3000
云堡垒机	100资产基础版	1	37800
数据库安全服务	专业版	11	60000
安全态势感知	专业版	2	3000
SSL证书服务	企业型（OV）SSL证书 Globalsign（单域名）	1	3094.24
云审计	平台基础服务，不涉及版本	/	/
云监控	平台基础服务，不涉及版本	/	/
云日志	平台基础服务，不涉及版本	/	0.00125/GB/小时
等保测评二级	基础版	1	200000
总计：387694.24			

表 2-2 等保三级

云资源	规格	数量	每年费用（元）
云防火墙	标准版	1	28000
Web应用防火墙	标准版	1	38800

云资源	规格	数量	每年费用（元）
DDoS高防（选配）	BGPpro保底10G	1	9800
主机安全	旗舰版	2	4000
威胁检测	初级包	1	10000
漏洞扫描	专业版	1	3000
云堡垒机	100资产基础版	1	37800
数据库安全服务	专业版	11	60000
安全态势感知	专业版	2	3000
SSL证书服务	企业型（OV）SSL证书 Globalsign（单域名）	1	3094.24
数据安全中心（选配）	标准版	1	30000
数据加密服务（选配）	秘钥管理服务	1	0.015458元/个/小时
云审计	平台基础服务，不涉及版本	/	/
云监控	平台基础服务，不涉及版本	/	/
云日志	平台基础服务，不涉及版本	/	0.00125/GB/小时
等保测评三级	基础版	1	200000
总计：513494.24			

3 实施步骤

定级

系统运营单位按照《 信息系统安全等级保护定级指南 》自行申报。信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

表 3-1 信息系统安全等级保护定级指南

保护对象受到破坏时受侵害的客体	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	第二级
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

备案

第二级以上信息系统定级单位到所在地的市级以上公安机关办理备案手续。省级单位到省公安厅网安总队备案，各地市单位一般直接到市级网安支队备案，也有部分地市区县单位的定级备案资料是先交到区县公安网监大队的，具体根据各地市要求来。备案的时候带上定级资料去网安部门，一般两份纸质文档，一份电子档，纸质的首页加盖单位公章。

安全建设与整改

信息系统安全保护等级确定后，运营使用单位按照管理规范和技术标准，选择管理办法要求的信息安全产品，建设符合等级要求的信息安全设施，建立安全组织，制定并落实安全管理制度

等级测评

信息系统建设完成后，运营使用单位选择符合管理办法要求的检测机构，对信息系统安全等级状况开展等级测评。测评完成之后根据发现的安全问题及时进行整改，特别

是高危风险。测评的结论分为：不符合、基本符合、符合。当然符合基本是不可能的，那是理想状态。

监督检查

公安机关依据信息安全等级保护管理规范及《 网络安全法 》相关条款，监督检查运营使用单位开展等级保护工作，定期对信息系统进行安全检查。运营使用单位应当接受公安机关的安全监督、检查、指导，如实向公安机关提供有关材料。

4 修订记录

表 4-1 修订记录

发布日期	修订记录
2023-04-10	第一次正式发布。