解决方案实践

等保三级解决方案

文档版本 1.0.0

发布日期 2022-09-30

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

应用场景

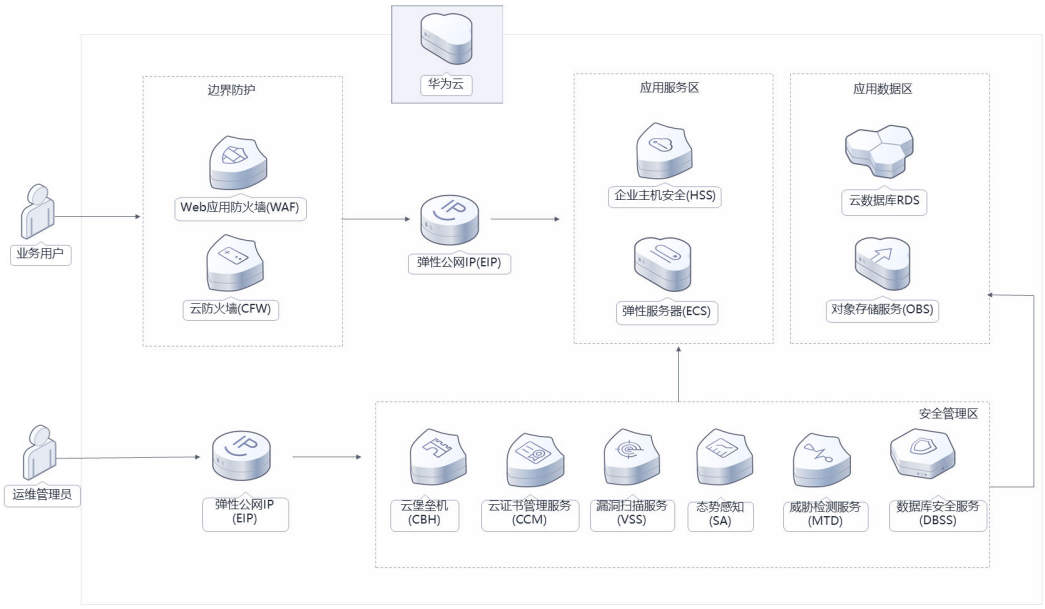
该解决方案依托华为云自身安全能力与安全合规生态，为用户提供一站式的等保三级安全解决方案，适用于在云上部署的关键业务系统：电商平台、政府门户网站、游戏、教育业务等场景。

方案架构

该解决方案支持一键式部署云防火墙CFW、企业主机安全HSS、web应用防火墙WAF、云堡垒机CBH、数据库安全审计DBSS等服务，帮助用户快速在华为云上搭建等保三级合规安全解决方案，轻松满足等保三级合规要求。

方案部署架构如下图所示：

图 1-1 方案架构图



该解决方案会部署如下资源：

- **Web应用防火墙WAF**：用来对业务流量进行多维度检测和防护。
- **企业主机安全HSS**：用来提升主机整体安全性，提供资产管理、漏洞管理、入侵检测、基线检查等功能，帮助企业降低主机安全风险。
- **云证书管理服务CCM**：实现网站的可信身份认证与安全数据传输。
- **态势感知SA**：用来对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。
- **威胁检测服务MTD**：用来识别云服务日志中的潜在威胁，并对检测出的威胁告警进行统计。
- **云防火墙CFW**：实现对云上互联网边界流量实时入侵检测与防御。
- **云堡垒机CBH**：集中管控运维管理人员实现操作可审计、可管控、可合规且高效运维。
- **数据库安全审计DBSS**：对数据库的行为进行操作审计，及时发现降低数据库泄露风险。
- **漏洞扫描服务VSS**：及时发现业务系统存在的漏洞，发现问题及时修复降低风险。

  此外，您可以通过使用**云监控服务**来监测弹性云服务器运行状态；通过购买**云日志服务**，对日志数据进行备份；开启**云审计**功能对云平台操作进行业务审计。

方案优势

- 安全合规

帮助用户快速、低成本完成安全整改，轻松满足等保三级合规要求。

- 一键部署

提供一键部署等保三级所需的安全服务能力，例如云防火墙、企业主机安全、Web应用防火墙等。

- 简单灵活

用户可以根据业务系统的需求灵活的调整方案的规格。

约束与限制

- 部署该解决方案之前，您需注册华为账号并开通华为云，完成实名认证，且账号不能处于欠费或冻结状态，如使用包周期部署确保余额充足。

2 资源和成本规划

该解决方案主要部署如下资源，每月花费如下所示，具体请参考华为云官网**价格详情**，实际收费以账单为准：

表 2-1 资源和成本规划（包年包月）

华为云服务	配置示例	每月花费
威胁检测服务MTD	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：基础包 • 购买量：1	5300.00 元
云防火墙CFW	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：标准版 • 购买量：1	2800.00 元
Web应用防火墙WAF	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：标准版 • 购买量：1	3880.00 元
企业主机安全HSS	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：旗舰版 • 购买量：1	200.00 元
数据库安全审计DBSS	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：基础版 • 购买量：1	3000.00 元

华为云服务	配置示例	每月花费
态势感知 SA	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：专业版 • 购买量：1	150.00 元
云堡垒机 CBH	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：50资产等保专享 • 购买量：1	1900.00 元
SSL证书SCM	• 区域：华北-北京四 • 计费模式：包年 • 规格：GeoTrust OV 单域名证书 • 购买量：1	192.15 元
漏洞扫描服务VSS	• 区域：华北-北京四 • 计费模式：包年包月 • 规格：专业版 • 购买量：1	300.00 元
合计	-	**17722.15元**

3 实施步骤

3.1 快速部署

本章节主要帮助用户快速部署等保三级解决方案。

步骤1 登录华为云解决方案实践，选择“**等保三级解决方案**”模板，单击“一键部署”，跳转至解决方案一键部署界面。

图 3-1 解决方案实施

步骤2 在推荐套餐一栏中，选择等保三级方案基础版，下滑进行参数配置。

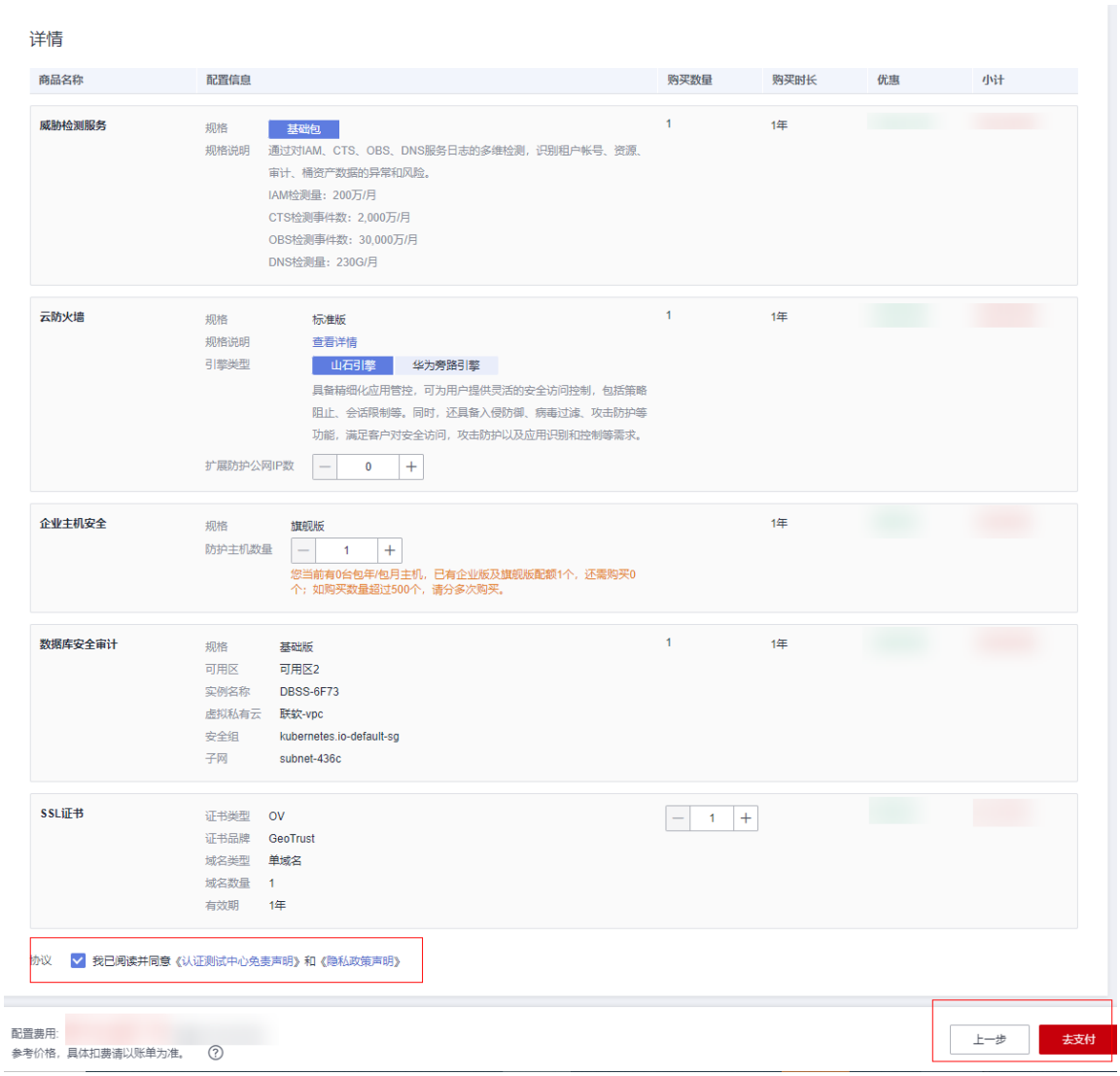
图 3-2 选择套餐

步骤3 在套餐商品配置一栏中，企业主机安全 HSS、态势感知 SA，会根据账号使用情况进行计算配置数量，其它服务需要审视需要防护的资源规格，例如云防火墙需要配置防护公网IP数量。配置完成后，单击下一步：

图 3-3 参数配置

步骤4 在详情界面中，勾选协议，单击“去支付”并确认订单后，即可完成资源创建。

图 3-4 高级配置



----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释：

- 认证测试中心CTC：是结合华为30年安全经验积累，并结合企业与机构的安全合规与防护需求，帮助企业与机构满足国家及行业法律法规要求，同时实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险，消除安全事件带来的损失。
- 云防火墙服务CFW：是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括：实时入侵检测与防御，全局统一访问控制，全流量分析可视化，日志审计与溯源分析等，同时支持按需弹性扩容，是用户业务上云的网络安全防护基础服务。
- 企业主机安全HSS：是服务器贴身安全管家，通过资产管理、漏洞管理、基线检查、入侵检测、程序运行认证、文件完整性校验，安全运营、网页防篡改等功能，帮助企业更方便地管理主机安全风险，实时发现黑客入侵行为，以及满足等保合规要求。
- Web应用防火墙WAF：对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，全面避免网站被黑客恶意攻击和入侵。
- 云证书管理服务CCM：是华为联合全球知名数字证书服务机构，为您提供一站式证书的全生命周期管理服务，实现网站的可信身份认证与安全数据传输。
- 态势感知SA：为用户提供统一的威胁检测和风险处置平台。帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力。
- 威胁检测服务MTD：威胁检测服务持续发现恶意活动和未经授权的行为，从而保护账户和工作负载。该服务通过集成AI智能引擎、威胁黑白名单、规则基线等检测模型，识别各类云服务日志中的潜在威胁并输出分析结果，从而提升用户告警、事件检测准确性，提升运维运营效率，同时满足等保合规。
- 漏洞扫描服务VSS：集Web漏洞扫描、操作系统漏洞扫描、资产及内容合规检测、安全配置基线检查、弱密码检测、开源合规及漏洞检查、移动应用安全检查七大核心功能为一体，自动发现网站或服务器在网络中的安全风险，为云上业务提供多维度的安全检测服务，满足合规要求，让安全弱点无所遁形。
- 数据库安全服务DBSS：是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库安全。

- 云堡垒机CBH：提供主机管理、权限控制、运维审计、安全合规等功能，支持Chrome等主流浏览器随时随地远程运维，保障运维安全高效。

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2022-09-30	第一次正式发布。