

部署指南

等保二级解决方案

文档版本	1.0.0
发布日期	2022-04-30



版权所有 © 华为技术有限公司 2022。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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.....	1
2 成本预估.....	3
3 约束限制.....	4
4 数据规划.....	5
5 快速部署.....	7
6 名词解释.....	9

1 方案概述

应用场景

华为云等保二级解决方案适用于如下用户场景：

1. 接到相关部门通知需要做安全整改。
2. 新业务需要做安全防护。
3. 业务遭受攻击导致企业效益受损，或无法正常办公。

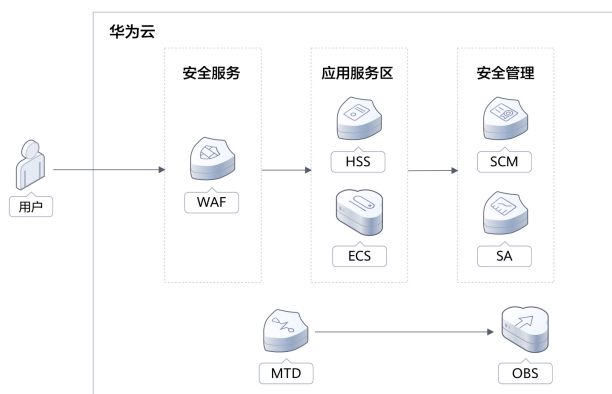
解决方案

该解决方案能帮您快速在华为云上搭建等保二级合规安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。

部署架构

解决方案架构如下：

图 1-1 方案架构图



该解决方案将会部署如下资源：

- **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。
- **SSL证书 SCM**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。

方案优势

1. 安全合规
帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。
2. 一键部署
提供一键部署企业主机安全、Web应用防火墙、SSL证书、态势感知、威胁检测服务。
3. 降本增效
持续提升安全效率，减少安全运维人员的投入。

2 成本预估

该解决方案默认部署在华北-北京四region。以下花费仅供参考，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 成本预估（仅供参考）

华为云服务	计费说明	每月花费
企业主机安全 HSS	规格：旗舰版。	200.0元/个
Web应用防火墙 WAF	规格：标准版。	3880.0元
SSL证书 SCM	规格： - 证书类型：OV - 证书品牌：GeoTrust - 域名类型：单域名 - 有效期：1年 配置费用：2139.74元/个	/
态势感知 SA	规格：专业版。	150.0元/个
威胁检测服务 MTD	规格：初级包。	1000.0元
合计		约 5230.0元/月（不含SSL证书费用）

3 约束限制

- 该解决方案部署前，需注册华为云账户，完成实名认证，且帐号不能处于欠费或冻结状态。
- 购买实例的账号需具有“**SES Administrator**”和“**BSS Administrator**”角色。
BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。

4 数据规划

该方案需要的产品列表和配置示例如表4-1所示。

表 4-1 数据规划

产品	配置示例
企业主机安全 HSS	● 区域：华北-北京四 ● 计费模式：包周期 ● 规格类型：旗舰版 ● 购买量：（根据现区域包周期的主机数量总和进行计算）
Web应用防火墙 WAF	● 区域：华北-北京四 ● 计费模式：包周期 ● 规格：标准版 ● 购买量：1
SSL证书 SCM	● 区域：华北-北京四 ● 证书类型：OV ● 证书品牌：GeoTrust ● 域名类型：单域名 ● 有效期：1年 ● 购买量：1
态势感知 SA	● 区域：华北-北京四 ● 计费模式：包周期 ● 规格：专业版 ● 购买量：（根据所有区域主机数量的总和进行计算）

产品	配置示例
威胁检测服务 MTD	• 区域：华北-北京四 • 计费模式：包周期 • 规格：初级包 • 购买量：1

5 快速部署

步骤1 登录[华为云解决方案实施库](#)，选择模板华北-北京四部署，跳转至解决方案一键部署界面。

图 5-1 解决方案实施库



步骤2 解决方案配置。

图 5-2 方案配置



步骤3 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，其它服务按默认即可。勾选协议，点击“去支付”并确认订单后，即可完成资源创建。

图 5-3 确认订单

详情

商品名称	配置信息	购买数量	购买折扣	优惠	小计
威胁检测服务	规格: 标准版 规格说明: 通过SIEM、CTI、CIS、CNS服务日志的本地检测, 实时威胁检测、溯源、研判、资产关联的运营和响应。 资产: 资产关联的运营和响应。 SIEM数据量: 50万月 CTI数据事件数: 100万月 CIS数据事件数: 3,000万月 CNS数据量: 700万月	1	1折	¥2,000.00	¥18,000.00
Web应用防火墙	规格: 标准版 规格说明: 查看详情 域名扩展包: 0 带宽扩展包: 0 本次购买: 10个防护域名配置, 其中1个一级域名 本次购买: 30Mbps/100Mbps/2,000 QPS	1	1折	¥7,780.00	¥69,800.00
企业主机安全	规格: 旗舰版 防护主机数量: 1 您当前有10个主机安全, 已有企业版及旗舰版数量0个, 还需购买0个; 如购买的数量超过500个, 需分多次购买。	1	1折	¥400.00	¥2,000.00
态势感知	规格: 专业版 最大容量: 2 网站数量: 1 所有企业版主机的总和, 建议根据实际需要增加容量, 不支持缩小。 您当前有10个主机安全, 已有企业版及旗舰版数量0个, 还需购买0个; 如购买的数量超过500个, 需分多次购买。	1	1折	¥400.00	¥3,000.00
SSL证书	证书类型: OV 证书品牌: GeoTrust 域名类型: 标准版 域名数量: 1 有效期: 1年	1	1折	¥438.28	¥2,138.74

1

我已阅读并同意《云认证中心/流量认证》和《隐私政策声明》

配置费用 ¥18,000.00 (含税费)
参考价格, 最终以账单/发票为准。

上一步

2 去支付

----结束

6 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。
- SSL证书 SCM：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。