解决方案实践

防勒索病毒安全解决方案

文档版本	1.0.0
发布日期	2022-10-30

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

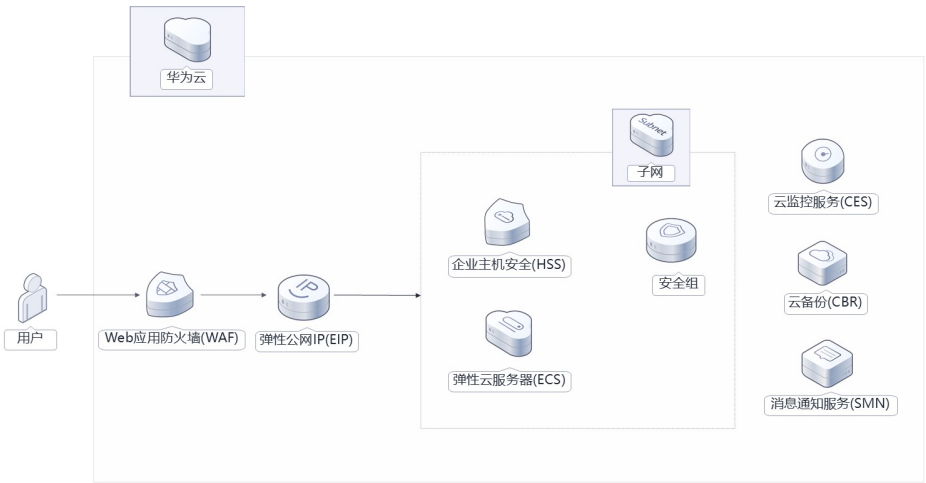
应用场景

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。一旦遭受勒索病毒攻击，将会使绝大多数的关键文件被加密。被加密的关键文件均无法通过技术手段解密，用户将无法读取资产中的文件，仅能通过向黑客缴纳高昂的赎金，换取对应的解密私钥才能将被加密的文件无损的还原，会对企业业务造成直接的经济损失。该解决方案能帮您为华为云上部署的服务器提供事前安全加固、事中主动防御、事后备份恢复的防勒索病毒方案，抵御勒索软件入侵，营造主机资产安全运行环境。

方案架构

该解决方案支持一键式部署web应用防火墙、主机安全服务，帮助客户快速构建主机资产安全运行环境，抵御勒索软件入侵。解决方案架构如下:

图 1-1 方案架构图



该解决方案会部署如下资源：

- 在应用系统所在的服务器ECS部署主机安全防护Agent。
- 部署Web应用防火墙，用于Web流量进行多维度检测和安全防护。
- 部署企业主机安全，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。

  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，使用消息通知服务（SMN）发送监控告警；通过购买云备份服务，对弹性云服务器进行数据备份，以便出现云服务器勒索行为对业务数据进行恢复。

方案优势

该方案具备以下优势：

- 全周期防护

  围绕事前、事中、事后三个阶段全栈保护勒索病毒防护技术问题。
- 一键部署

  提供一键部署放勒索方案所需的安全服务能力，例如部署主机安全、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。
- 主机安全防护Agent仅适用于64位云服务器，不再支持32位云服务器。

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

华为云服务	配置示例	每月花费
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
合计	-	**4080.00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“防勒索病毒解决方案”。

步骤1 登录华为云解决方案实践，选择“**防勒索病毒解决方案**”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，选择放勒索方案，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、Web应用防火墙需要审视是否需要额外配置域名拓展包以及宽带拓展包。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：

- 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。

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2022-10-30	第一次正式发布。