企业上云安全白皮书

文档版本 1.0

发布日期 2021-08-31

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 导读

1.1 背景

随着公有云技术的成熟，越来越多的企业选择将业务从传统的IDC、私有云迁移到公有云，降低IT成本，聚焦业务创新；同时随着公有云市场竞争的日益激烈，很多前期已经上公有云的企业，也会在多个公有云提供商之间切换业务或选择多云部署以降低成本和风险。

在云服务模式下，如何保障云上安全，成为大多数企业和客户的首要关注问题。云服务提供商致力于保障其所提供的IaaS、PaaS和SaaS各类各项云服务自身的安全及基础设施安全。但企业的云安全保障不能完全依赖于云服务提供商，企业需要基于业务需求合理使用和配置云服务能力以自建安全能力和安全防护体系，从而构建完整的云上安全体系。

云上安全体系的构建不仅依托于云服务提供商的安全能力，同时也需要客户在上云迁移阶段就采取一定的变革。上云安全变革涉及到企业应用整体安全治理体系的变化、企业安全组织架构的适配、企业安全文化和思维方式的塑造、持续的安全运营运维优化等。企业不仅需要上云迁移方法论，还需要一套覆盖安全治理、安全迁移方案实施等全面的方法论及技术体系来支撑，帮助上云之路更加顺畅。

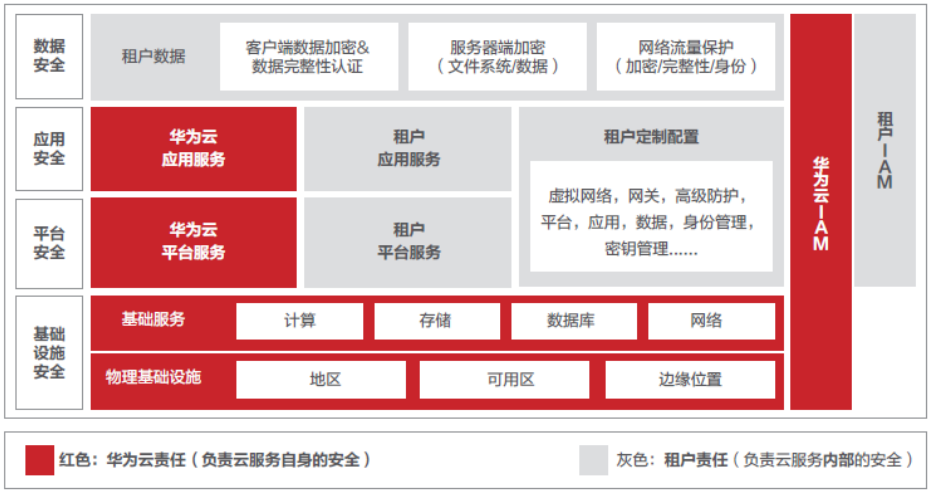
华为公司作为世界领先的ICT服务提供商，30 年来一直秉承技术上深耕细作、不断创新，服务上全心全意、持续提升的态度，致力于为行业、企业和个人提供先进、稳定、可靠、安全的产品和服务。作为华为公司的战略业务，华为云从成立伊始就继承了华为公司国际化的属性：满足全球各地区、各行业适用的法律法规及客户需求，构建可信的云服务。与此同时，为了帮助客户保护其云上资产，华为云希望协助更多企业构建云上安全防护体系，实现同客户长期双赢的重要实践。华为云基于多年在企业上云实践中的经验，吸收业界的优秀经验，总结提炼了上云安全建设步骤，用于指导和帮助客户企业上云安全工作的开展。

1.2 发布目的及目标读者

本文主要面向计划或正在进行上云迁移的企业的决策层、管理层、IT、安全和隐私保护等云服务相关技术岗位人员，旨在指导企业在上云迁移全过程中从规划、设计、实施、运营等多个方面实现上云安全，并构建自身的云上安全体系。同时让企业了解华为云为客户提供了多种专业服务和云产品助力其实现上云安全，并指导客户正确配置云服务。

1.3 责任共担模型

在云服务模式下，华为云与客户共同承担云环境的安全保护责任，为明确双方的责任，确定责任边界，华为云制定了责任共担模型，如下图所示：



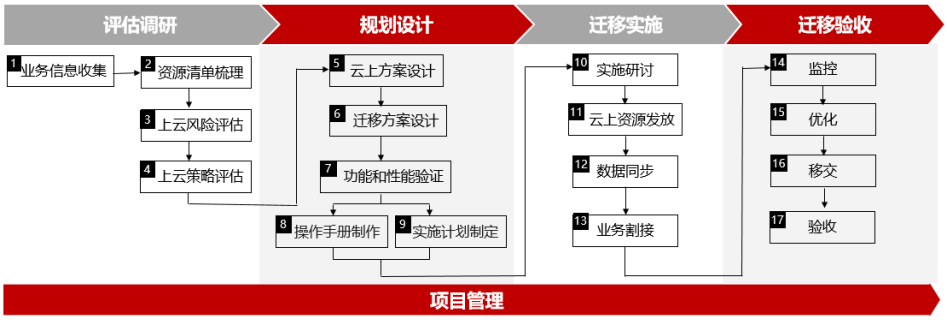
其中红色部分为华为云负责，灰色部分责任由租户承担。华为云负责云服务自身的安全，提供安全的云；租户负责云服务内部的安全，安全的使用云。

华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和IAM层的多维立体安全防护体系，并保障其运维运营安全。

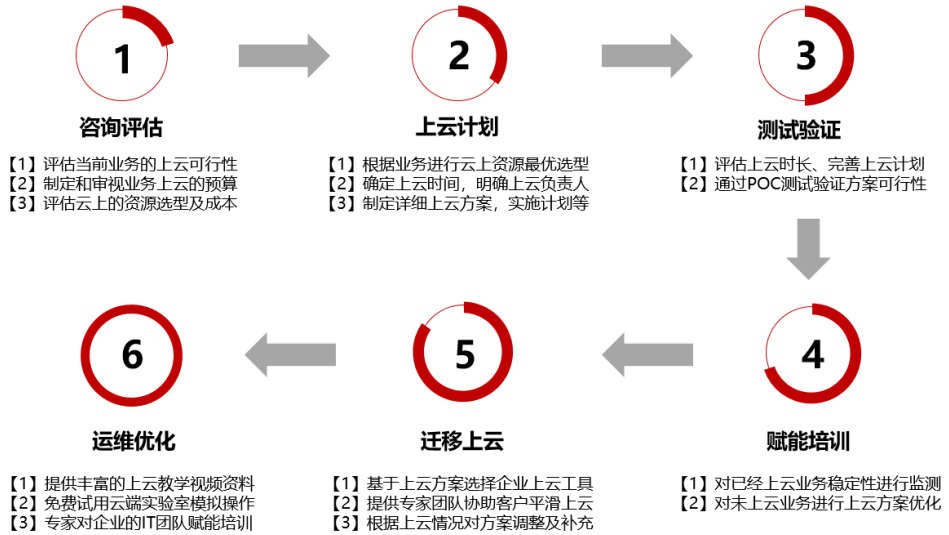
租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置，运维运营安全，以及用户身份的有效管理。

2 企业上云迁移流程

华为云基于华为自身上云的成功实践和服务海量客户的经验，总结出一套行之有效的上云迁移流程，以指导企业上云。具体流程如下：



华为云配套提供了与该流程对应的企业上云全服务。该服务是华为云基于客户需求，通过分析客户特定的迁移内容，结合客户现网环境，综合考虑迁移风险、应急回退预案等因素后完成云迁移方案设计，由具有丰富经验的技术专家进行实施，直至业务应用平台完成切换，业务系统正常运行。具体的服务流程如下：

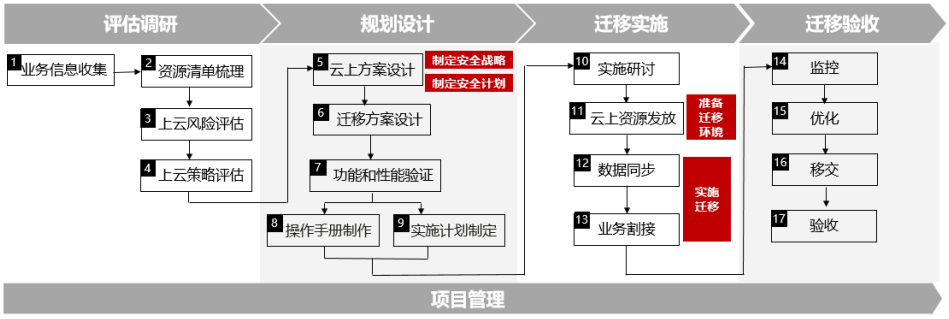


华为云上云迁移服务的优势：

- 原厂的专家团队：分布全球的服务团队，具备丰富的互联网、政企等行业服务经验，提供本地化的上云迁移服务。
- 完善的工具平台：基于从数据层、中间件层到应用层完整的迁移工具体系、丰富的原子化方案库、规范的交付管理平台。
- 成熟的交付流程：30多年ICT领域成熟的服务流程、高级别割接保障经验和大型项目管理经验，确保每一次上云迁移交付都安全可信。
- 灵活的产品方案：支持进行灵活的产品组合销售，针对客户系统和应用特点，为用户量身定制云迁移方案，将实施过程中对应用的影响降到最低。

3 企业上云安全建设指南

华为云以企业上云迁移流程为基准，基于多年在企业业务上云实践中的经验，吸收业界的优秀经验，识别上云迁移流程中建立安全体系的关键节点，并总结了实践步骤，帮助客户在上云过程中实现上云安全建设。企业上云安全步骤在上云迁移流程中各个阶段实施：



本节以企业上云迁移流程为基准，向企业提供上云安全建设步骤指南，指导企业构建云上安全体系。本节将从上云安全建设5个步骤为企业提供详细指导。

3.1 制定安全策略

企业的安全最终目标不会随着采用云服务而改变，但实现这些目标的方式将会改变。明确的云安全战略可帮助所有团队建立安全和可持续的企业云环境。企业的管理层和安全团队需要根据企业总体安全战略和业务战略制定云安全战略，并且需要在计划采用云服务时尽早考虑安全性。

企业的安全团队需尽早规划和思考如何使用云技术和云服务来实现安全工具和流程的现代化，并通过实施合理的云安全策略，实现云上业务系统的安全性、稳定性和可靠性。云安全策略是公司在云运营过程中的一些正式准则，这些准则能够对云资产安全的决策进行指导。企业需要结合自身的业务需求和安全需求制定对应的安全策略，同时需要考虑资产敏感度、上云潜在风险和风险容忍度、法律法规或标准的要求等内外部因素。

华为云建议可以从以下11个领域制定安全策略：

- **安全管理组织**：指定负责云上各个关键职能人员/团队，比如安全运营、系统安全管理等，并定义其职责。
- **身份与访问管理：**定义组织人员身份类型和身份验证方法，仅授予身份所需的权限，并持续审核和监控账号和权限的使用。
- **网络安全：**对业务所在网络进行安全分区管理，并进行相应隔离；在网络边界实施防护和监控机制；确保通信线路和设备的冗余以满足业务需求。
- **数据安全：**根据数据保护相关法律法规、标准中定义的分类分级要求对数据进行分类分级管理，并在数据生命周期各个阶段实施相对应的保护措施。
- **威胁与漏洞管理：**对云上业务定期执行漏洞扫描和分析，并及时对漏洞修补。
- **日志与监控：**对云上资源启用日志功能，集中收集和存储所有日志，并对日志进行监控和审核；监控安全状态，并记录网络攻击行为。
- **安全响应与恢复：**为安全事件管理提供资源支持，自动对安全事件进行上报和通知，预部署事件响应工具；定期开展安全事件演练与经验总结。
- **备份与恢复：**定义数据备份策略和保护措施，并对备份进行监控与审核。
- **开发安全：**对开发代码进行安全检查；系统上线前执行安全测试；保护研发资产的安全。
- **证书与密钥管理：**定义组织允许使用的加密算法和密码技术产品；对密钥和证书进行集中管理，并在密钥和证书的生命周期各个阶段实施安全控制。
- **隐私保护与合规：**识别隐私保护相关法律法规，对业务所涉个人数据进行识别并进行隐私风险评估；减少敏感数据在系统中的暴露风险；持续遵循合规要求。

若企业已建立较为成熟的安全体系，则可以现有的安全领域为基准制定云安全策略。企业同样可以参考业界广泛接受的安全管理体系划分安全领域，比如ISO 27001[1]、CSA CCM[2]、NIST CSF[3]。

说明

1. ISO 27001：ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
2. CSA CCM ： Cloud Security Alliance Cloud Control Matrix，即云安全联盟云控制矩阵，框架由16个领域的133个控制目标组成，涵盖了云技术的所有关键方面。
3. NIST CSF：NIST Cyber Security Framework，NIST网络安全框架由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型。

3.2 制定安全计划

3.2.1 基本定义

企业需要通过制定安全计划以定义各个安全策略的实现方式（包括但不限于标准、安全程序、安全控制措施、安全规范指南）、时间表和责任人/团队。云安全计划是上云计划中的组成部分，且企业应尽早将云安全计划纳入上云计划中，确保及时发现上云过程中的潜在风险并制定风险处理策略，该过程可能会导致上云计划的其他部分的调整。

安全计划应围绕组织已确定的安全策略进行制定，该阶段通常需要输出以下文件：

安全计划	说明
组织职能计划&安全技能计划	基于定义的安全角色和职责，确定各个角色所需的技能，并考虑通过何种方式帮助其获得技能，同时制定安全技能培训计划。
云上架构安全计划	根据已确定的安全策略，制定云上安全架构设计方案和方案实施计划，设计方案包括但不限于安全策略配置方案、云环境安全基准设计、计划使用的云产品清单。
安全操作规范	建立企业的云安全运营运维规范、云安全操作指导手册等规范文件，指导安全团队、云运营团队、安全运维团队、IT团队等相关利益者成功过渡到云环境，并避免因人员操作导致的安全风险。通过建立流程，以确保每个安全策略都得到正确配置并在治理良好的环境中运行。
灾备计划	根据企业与云厂商的责任划分，对灾备体系中各自的责任、分工、流程进行调整，制定业务连续性计划及灾难恢复计划。

考虑到企业业务目标、项目限制和其他因素可能会导致企业平衡安全风险与其他风险，因此最初的安全策略配置方案可以从最低的安全标准开始，但应尽量对所有安全策略进行配置。企业可随着时间的推移再逐渐提高安全标准，以确保持续降低风险。

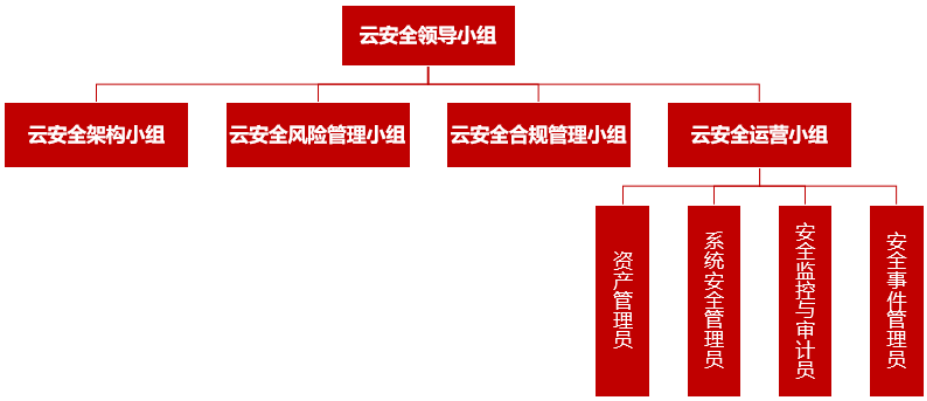
3.2.2 企业上云安全策略指导

企业上云安全策略指导可为实现企业的安全策略提供明确的操作指导，企业可参考安全策略指导选择能够践行其安全策略的云产品并对其实施最佳配置。该指导能够帮助

企业在华为云上提高安全性并降低风险、依托华为云建立完整的安全体系并实现云上安全。

3.2.2.1 安全管理组织

企业需建立云安全团队，记录、传达云安全团队中的角色和职责，帮助对应的人员了解其职责，并确保他们掌握对应的技能来承担责任。云安全团队通常包括云安全领导小组、云安全架构小组、云安全风险管理小组、云安全合规管理小组、云安全运营小组，如下图所示：



各个小组具体职责如下表所示，企业可根据自身情况，参考该架构建立云安全团队：

小组	职责
云安全领导小组	负责制定整体的云安全方针，协调各方资源建立、实施、检查、改进云安全管理体系，保证云安全管理体系的持续适宜性和有效性。
云安全架构小组	负责设计、构建并持续维护云环境的安全架构，以保证设计与总体业务IT标准保持一致，并与其他利益相关方合作，使云架构与服务层、内部SLA和业务目标保持一致。
云安全风险管理小组	负责整体把控云安全态势，并根据内外部因素变化持续改进安全策略，对系统存在的安全风险进行管控，及时采取控制措施并报告管理层。
云安全合规管理小组	负责审视云服务提供商的合规状态，并利用云服务的功能获取日志记录、配置数据等输出企业合规证据和合规报告，以应对内外部的审查。
云安全运营小组	负责对云环境进行日常安全维护与管理，持续监测应用程序和基础设施的安全状态，及时识别、通报和处理安全事件。

3.2.2.2 身份与访问管理

对资产的访问实施权限管理：需要根据工作职责限定人员对于关键业务系统的访问权限，并通过适当的系统和流程保证权限的正确设置，以免非必要人员或非授权人员访问到关键系统和核心敏感数据。权限管理应遵循按需分配、最小授权、职责分离原则。

- **使用统一身份认证服务IAM限制账户对关键系统的访问权限。**租户管理员可以通过IAM管理用户账号，并且可以控制这些用户账号对租户名下资源具有的访问和操作权限，实现精细的权限管理。
- **使用云堡垒机CBH限制对运维账号的使用和访问。**运维用户可通过CBH统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。CBH可用于集中管控运维账号访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置。
- **使用应用信任中心ATC对应用设置细粒度的访问控制策略。**ATC是围绕零信任理念打造的安全服务，实现应用维度威胁全景拓扑，可依据用户身份、访问行为、应用健康度进行细粒度的动态授权控制。用户可可快速创建基于用户身份和基于时间、地点等属性的控制策略，限制恶意用户权限。

制定强身份验证机制对用户的访问进行认证：应制定有效的账户密码规则，以确保不会使用容易被破解的密码，并定期更改密码。较高风险的活动应采用更严格的认证方法，通常应采取多因子认证机制对用户进行身份认证。

- **使用统一身份认证服务IAM多种身份验证机制。**IAM 支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM 还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者由于其访问钓鱼页面等而导致账号信息泄露。IAM同时支持多因子认证机制。
- **使用云堡垒机CBH加强系统用户身份认证管理。**CBH采用多因子认证和远程认证技术。引用多因子认证技术，包括手机短信、手机令牌、USBKey、动态令牌等方式，安全认证登录用户身份，降低用户账号密码风险。CBH可以对接第三方认证服务或平台，包括Windows AD域、RADIUS、LDAP、Azure AD远程认证，支持远程认证用户身份，防止身份泄露。
- **使用弹性云服务器ECS的密钥对保证远程登录安全。**弹性云服务器ECS支持用户在登录时使用密钥方式进行身份验证，以保证弹性云服务器安全。用户可通过ECS管理控制台创建密钥对，公钥自动保存在系统中，私钥由用户保存在本地，每次SSH登录到弹性云服务器时，将需要提供相应的私钥。

禁止使用供应商提供的默认系统密码：供应商提供的默认密码或默认设置可能被非法使用以威胁云环境、系统、软件的安全，因此须要在日常使用中注意更改默认密码。

- **使用统一身份认证服务IAM强制要求新用户修改默认密码。**使用IAM创建新用户时，可通过邮件发送一次性登陆链接给新用户，新用户使用链接进行登陆时需要设置密码，另外在管理员自定义新用户的密码时可选择强制用户在激活后修改默认密码。
- **使用企业主机安全服务HSS检测系统账号口令。**HSS提供基线检查功能，主动检测主机中的口令复杂度策略，给出修改建议，帮助客户提升口令安全性。同时检测账户口令是否属于常用的弱口令，针对弱口令提示用户修改，防止账户口令被轻易猜解。

启用并配置登录失败处理功能：应配置结束会话、限制非法登陆次数、限制同时登陆和登录连接超时自动退出等相关措施。

- **使用统一身份认证服务IAM配置登录失败处理措施。**IAM支持配置会话超时策略，如果用户未对界面操作超过设置的时长，会话将会失效，需要重新登录。另外，IAM支持配置账号锁定策略和账号停用策略，当用户在限定时间内达到登录失败次数后其账户会被锁定一定时间，而当用户在设置的有效期内未能成功登录后其账户会被停用。

定期审计账号的使用：应及时删除或停用多余的、过期的账号，避免共享账号的存在。

- **使用企业主机安全服务HSS进行主机账号管理。**HSS支持检测主机系统中的账号，列出当前系统的账号信息，帮助客户进行账号安全性管理，及时发现非法账号。
- **使用云堡垒机CBH管理运维账号。**CBH支持对运维账号的管理，如删除无用账号，停用多余、过期运维账号。

3.2.2.3 网络安全

对网络划分区域：根据业务实际情况划分不同网络区域，明确定义每个域的边界，并按照方便管理和控制的原则为各网络区域分配地址。避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

- **使用虚拟私有云VPC实现不同区域之间的网络隔离。**VPC可为客户构建出私有网络环境。客户可以划分“DMZ”，“服务”，“数据”等区域，并使用安全组隔离VPC内的IP地址段、子网、安全组等子服务，客户可使用VPC及安全组的相关网络访问控制策略保证网络边界访问的安全性。

确保网络访问权限最小化：根据业务实际情况优化每个网络区域的访问控制列表，并保证访问控制规则数量最小化。避免暴露多余的公网IP，同时不应对外开放或未最小化开放高危端口、远程管理端口。

- **使用虚拟私有云VPC控制访问规则和开放端口。**VPC的安全组可为具有相同安全保护需求并相互信任的云服务器提供访问策略。客户可通过配置VPC的网络ACL和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控。

应保证网络满足业务高峰期需要：确保网络设备的业务能力、网络每个部分的带宽满足业务高峰期的需要。

- **使用弹性负载均衡ELB分发访问流量。**ELB将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。
- **使用Anti-DDoS流量清洗服务提升带宽利用率。**Anti-DDoS为弹性公网IP提供四到七层的DDoS攻击防护和攻击实时告警通知，提升用户带宽利用率，确保用户业务稳定运行。

控制内外部流量的访问：使用防火墙控制内部和外部网络之间的计算机访问流量以及内部网络中敏感区域的输入及输出流量，并对所有网络流量进行检查，阻止与已制定安全标准不符的传输，以避免系统组件受到来自不可信网络的非授权访问。

- **使用云防火墙CFW实现入侵检测与防御。**CFW集成华为全网威胁漏洞库，并通过自带的入侵防御引擎（IPS），对恶意流量进行实时检测和防御。同时提供全场景流量日志、访问日志、入侵攻击日志记录，并通过报表分析呈现，支持审计及高级威胁溯源分析。
- **使用虚拟私有云VPC控制公网对云服务器的访问。**VPC可实现在流畅地访问的同时隔离租户，在此基础上支持灵活配置VPC之间的互联互通，并能实现敏感环境内组件不可通过互联网直接公共访问，同时VPC可通过访问权限控制功能提供基于主机侧和网络侧的多重安全防护。
- **使用NAT网关为VPC内的弹性云服务器构建公网出入口。**NAT网关位于外部因特网与云上VPC之间，通过部署NAT网关可掩盖内部网络的IP地址，降低虚拟环境遭受攻击的风险。
- **使用WEB应用防火墙WAF过滤恶意攻击流量。**启用WAF之后，网站所有的公网流量都会先经过WAF，恶意攻击流量在WAF上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。

3.2.2.4 数据安全

对敏感数据进行加密保存：根据法律要求和业务特性，对数据进行分类分级，并对不同级别的数据制定相应的标识与控制措施。针对敏感数据，采取加密、掩码等方法进行保护，以降低这类数据被未授权的读取及披露的风险。

- **使用数据安全中心DSC识别敏感数据。**DSC可根据敏感数据发现策略来精准识别数据库中的敏感数据，并支持从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对结构化数据和非结构化数据进行扫描、分类、分级，解决数据“盲点”。
- **使用数据加密服务DEW对敏感数据进行加密。**DEW与OBS、云硬盘（EVS）、镜像服务（IMS）等服务集成，可以通过密钥管理服务（KMS）管理这些服务的密钥，并对云服务中的数据进行加密，还可以通过KMS API完成本地数据的加密。

在公共网络组件间的数据传输应进行加密：通过公网传输数据时，应实施数据加密措施，需要结合配置正确的无线网络及新版的加密及验证协议以保护数据不被他人轻易获取，保障数据在传输过程中的安全。

- **使用云专线DC建立本地数据中心与虚拟私有云VPC之间的专属连接通道。**DC可建立数据中心与VPC之间高速、低延时、稳定安全的专属连接通道，保护数据中心与VPC之间的数据传输安全。
- **使用虚拟专用网络VPN实现不同区域之间的数据传输安全。**VPN 采用华为公司专业设备，基于 IKE 和 IPsec 协议在Internet 网络上虚拟出私有网络，在本地数据中心和华为云 VPC 之间、华为云不同区域的 VPC 之间构建安全可靠的加密传输通道。

对数据的操作行为实施限制或监控机制：根据数据的分级分类，应对数据的修改、批量操作等行为实施限制措施或建立监控机制。

- **使用数据库安全服务DBSS对数据库行为审计。**DBSS提供旁路模式数据库审计功能，用于监控用户异常、正常、攻击行为，可以对风险行为进行实时告警。同时，可以对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。
- **使用云堡垒机服务CBH专业版识别并拦截数据库高危命令。**CBH专业版支持通过执行命令运维数据库，包括数据删除、修改、查看等运维操作。CBH提供数据库控制策略功能，用户可设置预置命令执行策略，动态识别并拦截高危命令（包括删库、修改关键信息、查看敏感信息等），中断数据库运维会话。同时自动生成数据库授权工单，发送给管理员进行二次审批授权。

3.2.2.5 威胁与漏洞管理

及时发现并修补安全漏洞：安全漏洞可能使他人非法获得系统访问特权，应通过可信渠道获取最新的安全情报。安全漏洞可通过及时安装安全补丁的方式修复漏洞，以防恶意个人或软件非法利用从而破坏业务系统和数据。

- **使用漏洞扫描服务VSS自动发现网站或服务器的安全风险。**VSS集成了Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大功能，可以自动发现网站或服务器暴露在网络中的安全风险，提供多种维度的安全检测服务。同时，华为云安全专家会第一时间针对紧急爆发的通用漏洞CVE进行分析并更新规则，提供快速、专业的CVE漏洞扫描。VSS还支持扫描前端漏洞，如SQL注入、XSS、CSRF、URL跳转等。
- **使用数据库安全服务DBSS和Web应用防火墙WAF识别SQL注入攻击及漏洞。**DBSS提供基于智能算法的SQL注入攻击检测、风险识别功能。WAF通过对HTTP(S)请求进行检测，识别并阻断SQL注入，保护Web服务安全稳定。

- **使用威胁检测服务MTD持续发现恶意活动和未经授权的行为**。MTD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。

在关键节点处检测和清除恶意代码：应在关键网络节点处对恶意代码进行检查和清除，并维护恶意代码防护机制的升级和更新。

- **使用Web应用防火墙WAF检测恶意代码**。WAF在防护引擎中预置丰富的攻击特征签名库，可检测多种通用Web攻击特征，并进行攻击拦击；攻击特征签名库根据攻击类型实时升级更新。
- **使用Anti-DDoS流量清洗服务实施DDoS攻击防护**。Anti-DDoS提供网络层和应用层的DDoS攻击防护（如泛洪流量型攻击防护、资源消耗型攻击防护），并提供攻击拦截实时告警，利用所拥有的海量IP黑名单库和每日更新特征库，保障业务稳定可靠。

部署Web应用防火墙检查所有流量：在面向公众的 Web 应用程序前部署可检查和防范网页式攻击的自动化技术解决方案，不断检查所有流量。

- **使用云防火墙CFW对恶意流量进行实时检测和防御**。CFW集成华为全网威胁漏洞库，并通过自带的入侵防御引擎（IPS），对恶意流量进行实时检测和防御。同时支持无缝集成第三方厂家威胁检测分析引擎，云上云下统一生态，客户原线下安全策略资产无缝平移。

3.2.2.6 日志与监控

跟踪并监控对网络资源和关键数据的所有访问：通过系统的活动记录机制和用户活动跟踪功能可有效降低恶意活动对于数据的威胁程度。当系统出现错误或安全事件时，通过执行彻底地跟踪、告警和分析，可以较快地确定导致威胁的原因。

- **使用云审计服务CTS记录、查询和追踪云环境中的活动**。CTS可为客户提供云服务资源的操作记录，供用户查询、审计和回溯使用。
- **使用云监控服务CES实施实时监控和告警**。客户可利用CES对用户登录日志进行实时监控，当遇到恶意登陆行为，可触发告警并拒绝该IP地址的请求。

对用户行为进行安全审计：对重要的用户行为和重要安全事件进行审计，审计覆盖到每个用户。对审计记录进行保护并定期备份，避免受到未预期的删除、修改或覆盖。

- **使用云审计CTS记录和存储对云资源的操作记录**。CTS支持对各种云资源（包括网络设备、网络节点）操作记录的收集、存储和查询功能，且默认支持在服务界面中7天内的事件审计操作记录的存储和检索，同时支持操作审计日志记录转储至OBS以永久保存。
- **使用云堡垒机CBH执行运维和安全审计**。CBH全程记录用户运维操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

持续监控业务系统的性能并及时汇报异常情况：监控性能的程序应包括预测功能，在问题未对系统性能造成影响时，应能及早识别及纠正。同时该程序应有助于工作量预测，以便识别趋势，并提供容量计划所需的信息。

- **使用云监控服务CES监控业务资源状态**。CES为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，帮助用户精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。
- **使用应用运维管理AOM监控云上应用及云资源状态**。AOM提供覆盖应用性能、应用状态、基础设施状态、云资源使用情况的一站式立体运维平台，可实现实时

监控应用及云资源，采集各项指标、日志及事件等数据分析应用健康状态，提供告警及数据可视化功能。

- **使用应用性能管理APM监控云应用性能和故障**。APM通过拓扑可视化展示应用间调用关系和依赖关系，并能够针对应用的调用情况，对调用次数、响应时间和出错次数进行全方面的监控。APM还可以通过对服务端业务流实时分析，展示事务的吞吐率、错误率、时延等关键指标，帮助用户解决应用在分布式架构下的问题定位和性能瓶颈等问题。

记录攻击和异常行为并对其分析：应在关键网络节点处检测、防止或限制网络攻击行为；应采取技术措施对采集的安全日志进行持续监控和分析，实现对网络攻击特别是新型网络攻击行为和异常行为的识别和分析。

- **使用Web应用防火墙WAF和云日志服务LTS记录并分析攻击日志**。WAF通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入等攻击，启用WAF全量日志功能后，客户可以将攻击日志、访问日志记录到华为云的云日志服务LTS中，通过LTS记录的WAF日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。
- **使用态势感知SA对攻击进行统计和分析**。态势感知通过汇集全网流量数据和安全防护设备日志信息，能够实时检测和监控云上安全风险，实时呈现告警事件的统计信息，并可对各种威胁事件进行汇聚统计。利用大数据分析技术，态势感知可以对攻击事件、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。

集中管理日志：对云上资源启用日志功能，集中收集和存储所有日志，并对日志进行监控和审核。

- **使用云日志服务LTS对日志统一管理和分析**。LTS可以采集主机和云服务的日志数据，采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。LTS支持通过在一定时间段内日志中关键字出现的次数对日志数据关键字进行监控与告警，如果关键字达到阈值将会触发告警，实时监控服务运行状态。

3.2.2.7 安全响应与恢复

自动对安全事件告警：根据事件响应需求定义各类事件告警类型、告警级别和通知对象，确保对应的人员及时对安全事件进行取证、调查和处理。

- **使用态势感知SA自定义威胁告警通知**。SA通过“实时监控”云上威胁告警事件，并接入Anti-DDoS、HSS、WAF等服务上报的告警事件，提供告警通知和监控，记录近180天告警事件详情。客户可以设置每日定时告警通知和实时告警通知，通过接收消息通知及时了解威胁风险。
- **使用云监控CES获取云服务状态告警通知**。CES提供对监控指标的告警功能，当云服务的状态变化触发告警规则设置的阈值时，系统提供邮件和短信通知，用户可以在第一时间知悉业务运行状况，还可以通过HTTP、HTTPS将告警信息发送至告警服务器，便于用户构建智能化的程序处理告警。
- **使用云审计CTS对关键操作进行告警**。CTS支持对某些特定关键操作通过消息通知服务（SMN）实时向相关订阅者发送通知，该功能由CTS触发，SMN完成通知发送，包括高危操作、成本敏感操作、业务敏感操作、越权操作等的感知和确认。

自动化事件遏制和恢复：根据过去事件的经验，在事件发生后自动化启动预定义变更流程及特定的补救措施。

- **使用态势感知SA专业版实施预置的防护策略**。SA的安全编排服务支持在事件发生后，通过实施预置的安全编排策略，提前防御并处置威胁风险端口。SA支持在用

户资产遭受端口安全攻击时，能一键式下发预置的防护策略，并且一键识别用户资产端口风险，推荐用户进行安全服务配置，简化安全运维，提升安全运维效率。

3.2.2.8 备份与恢复

在适当的时间范围内备份数据：在适当的时间范围内使用适当的方法备份数据，以便在原始数据不可用或损坏时随时可以使用备份数据。

- 使用**对象存储服务OBS**、**云备份CBR**、**云服务器备份CSBS**进行数据备份归档。华为云提供多粒度的数据备份归档服务，可将云上的文档、硬盘、服务器进行备份。客户也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，避免在灾难发生时不丢失数据。
- **使用云数据库RDS对数据库恢复**。RDS支持的恢复方式包括实例级恢复和库表级恢复。实例级恢复支持使用已有的自动备份或手动备份，恢复整个实例的数据；库表级恢复支持通过自动备份文件，将数据库表恢复到指定的时间点。

3.2.2.9 开发安全

对开发代码安全检查：在开发阶段对开发代码进行审查，识别可能导致安全问题的编码缺陷和漏洞，提高代码和最终开发软件的安全性。

- **使用软件开发平台DevCloud对代码进行检查**。DevCloud代码检查（CodeCheck）支持在线进行多种语言的代码静态检查、代码架构检查、代码安全检查、编码问题检查等，辅助客户管控代码质量。代码检查支持跨函数的深度检查，并能准确定位到代码缺陷所在行，提供影响说明、修改示例和建议，同时支持批量处理代码缺陷。另外，代码检查提供华为典型检查规则集，并支持用户自定义检查规则集。
- **使用数据安全中心DSC检测密钥泄露**。DSC支持检测Github代码中是否包括Access Key并判断可能受影响的华为云账户，用户可根据AK泄露事件推荐策略对事件进行处理，减少密钥泄露的风险。

执行安全测试：应执行安全测试，发现并消除已知的缺陷。在系统上线前，应对系统进行验收测试，以验证系统已排除已知的恶意代码或漏洞码。

- **使用软件开发平台DevCloud管理测试活动**。DevCloud云测（CloudTest）提供一站式测试解决方案，覆盖功能测试、接口测试、性能测试，多维度评估产品质量。客户可使用DevCloud的移动兼容性测试服务，其提供TOP流行机型、数百名测试专家，使用图像识别和精准控件识别技术，全自动化测试并生成测试报告（包含系统日志、截图、错误原因、CPU、内存等），帮助客户快速定位修复问题。

保护研发资产的安全：应对源代码、开发文档、产品版本包等研发资产进行控制和保护，包括限制对研发资产的访问和变更、使用加密传输方式、加密存储研发资产。

- **使用软件开发平台DevCloud保护研发资产**。DevCloud支持客户对项目文档、代码仓库等研发资产进行权限管理，以防止非授权访问。DevCloud代码托管（CodeHub）支持权限管理、分支保护、IP白名单，限制代码仓库的访问人员、以及代码修改权限，并对所有关键操作进行审计记录。对于用户通过HTTPS/SSH访问代码仓库，将使用SSH Key或者仓库用户名及密码进行访问。另外，DevCloud的分布式代码托管服务采用专属云存储、全网TLS传输等技术，并具有网络安全团队专业认证，保证云上代码安全。

3.2.2.10 隐私保护与合规

识别个人数据以分析隐私风险：识别业务运行中收集的个人数据，确保仅在合理的以及数据主体已经同意的目的范围内处理个人数据。

- **使用数据库安全服务DBSS从海量数据中迅速识别个人数据。**DBSS支持数据库中的敏感数据发现，提供内置或自定义隐私数据保护规则，客户可在此基础上分析已经收集的个人数据是否为满足业务目的所必需的，数据收集的目的是否合法、具体和明确，是否已告知数据主体并获得数据主体的同意，并符合相关个人数据处理要求。
- **使用数据安全中心DSC精确高效识别个人数据。**在AI和专家知识库的双重加权下，DSC可精准识别敏感数据和文件，覆盖结构化和非结构化两种数据类型，支持数十种个人隐私数据类型，包含中英文。

隐私数据脱敏：对数据库中的隐私数据进行脱敏，防止数据库敏感信息泄露。

- **使用数据库安全服务DBSS进行数据脱敏。**当需要对输入的SQL语句的敏感信息进行脱敏时，客户可以通过开启DBSS的隐私数据脱敏功能，以及配置隐私数据脱敏规则来对指定数据库表以及来自特定源IP、用户和应用的查询进行脱敏。
- **使用数据安全中心DSC进行数据脱敏。**用户可以通过DSC的20+种预置脱敏规则，或自定义脱敏规则来对指定数据库表进行脱敏，DSC支持RDS，ECS自建数据库等云上各类场景。另外，DSC可基于扫描结果自动提供脱敏合规建议，支持一键配置脱敏规则。

持续遵循合规要求：让业务在云上安全合规地运营，并确保使用的云平台及云服务的合规性。

- 使用**华为云等保合规安全解决方案**实现等保合规。华为云依托自身安全能力与安全生态，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，轻松遵循等保合规要求。华为公有云系统通过等保三级测评，部分关键Region 、节点的安全保护等级为第四级。租户系统等级测评的安全物理环境部分可以沿用华为云平台安全保护等级测评报告结论。
- 访问**华为云信任中心**查看华为云合规资质及合规遵从说明文档。华为云已获得80+全球性、区域性和行业特定的安全/隐私方面的权威认证，如：ISO 27001，ISO 27701[1]、PCI DSS[2]认证等，访问信任中心页面可以查看华为云已获取的权威认证及合规遵从说明文档。

说明

1. ISO 27701：规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。
2. PCI DSS：支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

3.2.2.11 证书与密钥管理

对密钥进行管理和保护：采用符合法律法规和国际标准的加密算法和密钥等，并通过定期轮换密钥和管理程序来管理密钥的生命周期以及密钥的备份，确保密钥存储在安全的位置并通过安全通道进行分发。

- **使用数据加密服务DEW对密钥全生命周期集中管理。**通过使用硬件安全模块HSM保护密钥安全的托管，帮助客户轻松创建和控制加密密钥。HSM经过严格的国际安全认证，能够做到防入侵、防篡改。客户密钥不会明文出现在HSM之外，避免

密钥泄露。并且在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密。对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录。

对证书集中管理：集中管理每个证书的用途、有效期等信息，并及时对证书替换。

- **使用SSL证书管理SCM对SSL证书全生命周期进行管理。**SCM提供上传证书和私钥功能，实现在华为云平台统一管理各种证书、提交审核、查看证书绑定域名和到期时间、修改证书名称、删除已过期的证书等一站式服务。同时支持用户在SSL证书管理平台上一键推送证书到华为云其他云产品中。
- **使用云证书管理服务CCM对私有证书（PCA）进行管理。**CCM支持用户建立完整的CA层次体系，包括根及多级中间CA等，为用户提供高可用高安全的私有CA托管能力。同时，支持用户方便快捷地创建和管理私有证书，用于识别和保护组织内的应用程序、服务、设备和用户等资源。

3.2.3 企业上云安全策略产品实践

华为云为客户提供了一系列云产品以帮助客户践行安全策略，以下是各个安全领域下华为云提供的对应的配套云产品清单，用户可通过**《华为云云服务基线配置指导》**正确配置对应的云服务：

安全领域	华为云云服务	功能介绍
身份与访问管理	**统一身份认证服务（IAM）**	提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及操作权限。
	云堡垒机（CBH）	严格控制主机等资源的访问权限，确保合适的人得到合适的权限。
	应用信任中心（ATC）	可依据用户身份、访问行为、应用健康度进行细粒度的动态授权控制。
网络安全	**云防火墙（CFW）**	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。
	虚拟私有云（VPC）	用户在华为云上申请的隔离的、私密的虚拟网络环境（利用VxLAN协议使得VPC之间严格的逻辑隔离）。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务。
	弹性负载均衡（ELB）	将访问流量自动分发到多台云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错。
	流量清洗服务（Anti-DDoS）	抵御大流量DDoS攻击，避免云上服务器被攻击后导致业务瘫痪。

安全领域	华为云云服务	功能介绍
	Web应用防火墙（WAF）	对网站业务流量进行全方位检测和防护，智能识别恶意请求特征和防御未知威胁，避免源站被黑客恶意攻击和入侵，防止核心资产遭窃取，为网站业务提供安全保障。
	NAT网关（NAT）	NAT网关是VPC与Internet、与私网之间的窗口，支持跨子网部署和跨AZ部署，VPC内弹性云服务器可共享EIP访问Internet或共享私网IP访问IDC及其他VPC。
数据安全	**数据安全中心（DSC）**	基于数据识别引擎，对其储存结构化数据和非结构化数据进行扫描、分类、分级，并识别敏感数据。
	数据加密服务（DEW）	提供专属加密、密钥管理、密钥对管理等功能。
	数据库安全服务（DBSS）	可以对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。
威胁与漏洞管理	**漏洞扫描服务（VSS）**	集Web漏洞扫描、资产内容合规检测、弱密码检测三大核心功能，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，遵循合规要求。
	数据库安全服务（DBSS）	提供SQL注入攻击预警功能。
	企业主机安全服务（HSS）	提升主机整体安全性的服务，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。
	威胁检测服务（MTD）	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。
	Web应用防火墙服务（WAF）	可阻挡如SQL注入、跨站脚本攻击，具有防数据泄露、漏洞修复、防CC攻击、防网页篡改四大功能。

安全领域	华为云云服务	功能介绍
日志与监控	**云审计（CTS）**	提供云账户下资源的操作记录，通过操作记录可以实现安全分析、资源变更、合规审计、问题定位等场景。可以通过配置OBS对象存储服务，将操作记录实时同步保存至OBS，以便保存更长时间的操作记录。
	云日志（LTS）	提供日志收集、实时查询、存储等功能，无需开发即可利用日志做实时决策分析，提升日志处理效率，帮助用户轻松应对日志实时采集、查询分析等日常运营、运维场景。
	云监控服务（CES）	为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。
	云堡垒机（CBH）	实现对云上服务器的操作运维审计等。
	数据库安全服务（DBSS）	审计数据库操作行为，提供包含等保合规等多种专项报表，用户能够基于各种维度进行分析和溯源。
	应用运维管理（AOM）	实时监控应用及云资源，采集各项指标、日志及事件等数据分析应用健康状态，提供告警及数据可视化功能。
	应用性能管理（APM）	实时监控并管理企业应用性能和故障的云服务，帮助企业快速解决分布式架构下问题定位和性能瓶颈分析难题
安全响应与恢复	**安全态势感知（SA）**	利用华为云大数据量、高准确度的威胁信息库，实时监控云上8大类威胁告警及200+子告警事件，并进行大数据关联分析、检索、排序，实现威胁事件的分钟级告警响应，追踪溯源和调查取证。
	管理检测与响应（MDR）	通过云服务方式，提供华为云安全标准化的运维运营服务。 帮助企业与机构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并消除安全事件带来的损失。

安全领域	华为云云服务	功能介绍
备份与恢复	对象存储服务（OBS）	提供高性能、高可靠、低时延、低成本的海量存储系统。
	云备份（CBR）	为云下的VMware虚拟化环境，云内的云服务器、云硬盘进行备份，通过备份快速恢复数据，保证业务安全可靠。
	云硬盘备份（VBS）	为云硬盘创建在线备份，无需关机/重启。针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。
	云服务器备份（CSBS）	为云服务器下所有云硬盘创建一致性在线备份，无需关机。针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。
开发安全	**软件开发平台（DevCloud）**	提供端到端的研发工具服务，实现全生命周期覆盖，实现开发测试环境、类生产环境、生产环境的一致性。全方位系统安全加固，核心研发数据加密传输和存储，基于角色的企业级安全管控，全面保障企业研发数据的安全。
证书与密钥管理	**数据加密服务（DEW）**	提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块HSM保护，并与许多华为云服务集成。用户也可以借此服务开发自己的加密应用。
	SSL证书服务（SCM）	为HTTP网站提供转向HTTPS，加密应用层数据。
	云证书管理服务（CCM）	PCA支持用户建立完整的CA层次体系，包括根及多级中间CA等，为用户提供高可用高安全的私有CA托管能力。
隐私保护与合规	数据库安全服务（DBSS）	提供个人隐私数据脱敏保护等高级特性。
	数据安全中心（DSC）	提供数据安全风险识别、数据静态脱敏等基础数据安全能力。
	等保合规安全解决方案	华为云依托自身安全能力与安全生态，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，轻松遵循等保合规要求。

除此之外，为满足客户不同场景下的安全需求，华为云提供了12种细分场景的安全服务，服务内容包括识别风险、分析问题根因、提供解决建议、配置和维护安全产品等。客户可根据自身需求选择对应的华为云安全服务：

服务项	服务内容
网站安全体检	远程提供安全监测服务支持HTTP/HTTPS协议进行实时安全监测；支持网页木马、恶意篡改、坏链、对外开放服务、可用性、审计、脆弱性等七个维度对网站进行监测；支持WEB安全漏洞扫描及域名劫持进行实时安全监测；定期推送网站安全体检报告
主机安全体检	通过日志分析、漏洞扫描等技术手段对主机进行威胁识别；通过基线检查发现主机操作系统、中间件存在的错误配置、不符合项和弱口令等风险
安全加固指导	对主机服务器、中间件进行漏洞扫描、基线配置加固；分析操作系统及应用面临的安全威胁，分析操作系统补丁和应用系统组件版本；提供相应的整改建议，并在用户的许可下完成相关漏洞的修复和补丁组件的加固工作
安全监测服务	通过远程查找及处置主机系统内的恶意程序，包括病毒、木马、蠕虫等；通过远程查找及处置Web系统内的可疑文件，包括Webshell、黑客工具和暗链等；提出业务快速恢复建议，协助用户快速恢复业务
应急响应服务	业务系统出现安全问题的情况下，提供24小时安全应急响应服务，由安全团队协助处理中毒、中木马等应急处理事宜，每次处理完成后华为侧提供应急响应报告，分析问题根因，并提供改进建议。
安全配置服务	根据客户业务需求，如主机IP、主机系统版本、域名、流量、加密、数据库防护等级等信息。 输出安全解决方案并制订安全防护体系包括安全服务规格、数量、策略
安全防护服务开通与部署	安全服务交付，如主机安全、WAF、高仿DDoS、堡垒机、漏洞扫描等服务的部署。 云安全设置，提供云安全设置服务，包括安全组、防火墙策略等等的设置操作。
定期策略更新与维护	从主机安全、应用安全、网络安全、数据安全、安全管理等方面定期完成漏洞检测、基线扫描、策略优化、巡检监控等操作，并输出整改建议报告。
安全漏洞预警服务	根据最新的安全漏洞、病毒木马、黑客技术和安全动态信息，结合客户实际的操作系统、中间件、应用和网络情况等，定期将相关安全信息如安全漏洞、病毒木马资讯、安全隐患/入侵预警和安全事件动态等内容，以电子邮件方式进行通报，并提出合理建议和解决方案等。
主动安全预警服务	主机存在被入侵并对外攻击问题，主动邮件或电话知会客户排查；针对主动发现的影响客户使用的安全问题，进行主动通知工作。

服务项	服务内容
安全设备维护服务	对各类安全设备开展基础维护，包括设备配置定期备份、设备特征库升级、设备版本升级、设备切换、设备配置调整等。
漏洞管理服务	通过华为云主机安全、漏洞扫描等安全服务，对实现云上业务系统的web应用、操作系统、中间件等漏洞的统一管理。

3.3 准备迁移环境

企业在正式实施迁移上云之前，需确保迁移目的端环境符合企业的合规性和安全性要求。根据企业已确定的云上产品清单，安全团队根据云环境安全基准设计方案对云上环境进行配置，并持续审核配置以确认云环境满足安全基准，这将有效减少在迁移部署期间的安全风险和降低业务迁移上云后再进行安全配置的风险。

企业可在已配置的安全云环境中进行迁移测试，包括业务性能压力测试和联调测试，以验证云上业务功能和性能符合企业要求。华为云可为客户提供云压测产品——**云性能测试服务（CPTS）**对客户计划在华为云部署的业务系统进行性能压力测试。针对多模块系统，华为云为客户提供数据 迁移工具——**云数据迁移服务（CDM）**以帮助客户导入模拟数据进行业务功能性测试，以验证云上业务系统流和端到端的时延及反馈满足业务要求。通过迁移测试，企业可以对计划使用的华为云产品有较为深入的了解，并验证业务功能和性能，以便安全且顺利地实施正式迁移。

3.4 实施迁移

企业在实施迁移过程中会可能面临业务中断、数据丢失、数据迁移不一致等风险，华为云提供多种迁移工具帮助企业应对迁移实施过程中的安全风险，并能有效缩短迁移中断时间和提高迁移效率，减少对业务运行的影响。

实施迁移常见风险	应对策略	华为云解决方案
业务中断	• 选择在业务量小的时间窗口进行迁移。 • 数据迁移过程始终保持源端在线，最后一次增量同步和业务切换时才中断业务。	• 使用主机迁移服务SMS迁移X86物理服务器，或者私有云、公有云平台上的虚拟机，在迁移过程中客户无须中断业务，只需在最后一次数据同步和割接时短暂的中断业务，保证业务平滑迁移。 • 数据复制服务DRS具有在线迁移特性，通过增量迁移技术，能够最大限度允许迁移过程中业务继续对外提供使用，有效地将业务系统中断时间和业务影响最小化。
网络中断	• 建设使用专用网络，专线可有效提高网络稳定性及迁移速率	• 使用云专线DC搭建用户本地数据中心与华为云VPC之间的专属通道，云专线DC具备高速、低时延、稳定安全的特性，能够保障迁移过程网络的稳定性及迁移速率。 • 使用对象存储迁移服务OMS迁移线上数据，OMS通过实时侦测网络，并在异常时自动重试，以提高传输可靠性。 • 对象存储服务OMS支持断点续传，迁移过程中如果出现短暂的网络中断，OMS支持手动重启迁移任务，重启后会从中断的位置继续开始迁移任务。

实施迁移常见风险	应对策略	华为云解决方案
迁移前后数据不一致	• 对迁移源端与目的端进行身份校验。 • 使用全量同步配合多次增量同步的迁移策略，最后一次增量同步和业务切换时才中断业务。 • 迁移前做好源端数据备份。	• 主机迁移服务SMS、对象存储迁移服务OMS使用AK/SK校验迁移Agent身份，充分认证身份的合法性。 • 数据复制服务DRS提供数据迁移对比功能，可根据需要查看对象级对比、数据级对比等，以确保源和目标数据库的数据一致性。
迁移过程中数据泄露	• 使用安全的传输通道传输数据。	• 主机迁移服务SMS源端到目的端的传输通道使用SSL协议加密，且SSL协议的证书和密钥动态生成，以保证数据传输的安全性。 • 对象存储迁移服务OMS支持通过HTTPS协议加密在线传输数据，确保数据在传输过程中的安全。

3.5 持续安全运营

在健全的安全体系（组织、技术、管理、运行）的基础上，企业需要对安全进行持续化监控与改进，做到风险可控，实现云安全纵深防御、主动防御、韧性防御的云安全能力。

华为云结合自身多年安全运营经验，总结了适用于云租户持续安全运营的方法论，如下图所示：

- 识别
  - 全面识别信息资产，并通过风险评估识别信息资产的脆弱性；
  - 建立威胁情报平台，通过威胁模型进行威胁分析，实现早期预警，主动威胁做出快速反应；
  - 实施全平台漏洞扫描，查找云平台、网络设备、服务器主机（操作系统、数据库、中间件等）存在的漏洞，结合补丁管理系统，自动化修复漏洞，并持续跟踪，反馈资产脆弱性状态；
  - 参考法律或相关规范的安全配置标准，结合企业实际情况，针对云平台、用户应用系统进行安全基线检测。
- 防护
  - 制定安全策略并进行策略配置，并根据内外部情况定期对策略进行审视和变更，领域包括网络安全、端点安全、云平台安全、应用安全和数据安全；
  - 通过巡检、特征库升级、补丁安装、病毒查杀等方式加固安全防护能力；
- 监控
  - 采集网络设备、安全设备、服务器等设备和系统的安全日志，并制定安全事件监控规则，对安全事件进行持续性监控与分析；
  - 采集网络系统流量和日志信息，并通过专家对采集的数据进行安全分析，及时感知平台中的安全事件并提出解决方案。
- 响应与恢复
  - 识别安全事件，根据事件的类别和级别分配对应的处理人员，及时维持或恢复平台的运作；
  - 事件处理完成后，回溯所发生的安全事件以及经验教训，对现有的流程进行重新评审并优化；
  - 编制应急预案并定期开展应急预案培训、应急预案测试与演练。

安全是一个持续改进的过程。如果组织不持续关注安全态势，组织安全能力也会随着时间的推移而衰退。企业需要持续改进安全状况和组织响应事件的能力，这有助于限制安全事件对企业的业务运营和资产的潜在影响，同时使企业能够快速创新并适应不断变化的商业环境。

华为云向客户提供多款产品，以帮助客户持续运营安全：

云服务/云产品	功能
云审计服务（CTS）	为客户提供云服务资源的操作记录，供用户实现安全分析、资源变更、合规审计、问题定位等功能，支持对关键操作进行实时短信、邮箱通知。
云监控服务（CES）	为客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台，使用户全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。
应用运维管理（AOM）	帮助客户实时监控应用及云资源，采集各项指标、日志及事件等数据分析应用健康状态，提供告警及数据可视化功能，帮助客户及时发现故障，全面掌握应用、资源及业务的实时运行状况。
威胁检测服务（MTD）	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，持续发现恶意活动和未经授权的行为。
态势感知（SA）	利用华为云AI技术，结合大数据的海量处理能力，通过智能监控和关联分析，自动化检测多类云上安全风险，实时管理风险检测结果及威胁告警。
数据安全中心服务（DSC）	提供数据分级分类，数据安全风险识别，数据水印溯源，数据脱敏等基础数据安全能力，通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。
管理检测与响应服务（MDR）	通过云服务方式，向客户提供华为云安全标准化的运维运营服务，帮助企业与机构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并消除安全事件带来的损失。

4 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，为此华为云向企业提供了上云安全建设指南，以帮助客户在上云迁移过程中降低安全风险，并建立云上安全体系，同时，为帮助客户更好地践行安全策略，华为云提供了各种安全领域的工具、专业服务和解决方案，助力客户实现上云安全和提升云上安全能力，降低安全风险。

5 版本历史

日期	版本	描述
2021年8月	1.0	首次发布