华为云数据安全白皮书

文档版本 v1.0

发布日期 2018 年 9 月

华为技术有限公司

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。

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： 华为 - http://www.huawei.com/cn/, http://e.huawei.com/cn/

华为云 - https://www.huaweicloud.com/

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

序言

随着云计算服务的不断发展与完善，越来越多的企业和客户将业务迁移上云。在云服务模式下，如何保障云上数据安全，成为大多数企业和客户的首要关注问题。华为云“不碰数据”确立了华为云数据中立原则。

籍此白皮书发布，将华为云在数据安全领域多年的实践和经验，分享给客户。同时华为云将持续提升数据安全防护能力，不断推出丰富的安全服务产品，助力客户商业成功。

目 录

图表目录

1 华为云助力客户安全实现数据价值

华为云践行 “不碰数据”的理念，结合多年积累的云安全技术和运营实践，形成了一套行之有效的数据安全战略和方法。

- 华为云恪守“不碰数据”底线

客户拥有其云上数据的所有权和控制权，没有客户授权，不碰客户数据，如 DEW 服务将密钥交给客户管理。华为云依靠业界领先的软硬件系统化的全栈、全生命周期的安全工程能力，筑起平台及服务的安全长城，保证在未经授权情况下，不拿客户数据进行变现。

- 华为云帮助客户削减数据安全风险

客户拥有其云上数据主权的同时须对其数据安全负责，华为云提供丰富的服务，供客户自主选择，帮助客户提升安全防护水平，削减数据安全风险。并且华为云围绕安全防护、合规运营、隐私保护开展持续有效的安全治理工作，确保自身不触碰数据的同时，帮助客户保障数据安全。

- 华为云助力客户发挥数据价值

大数据时代，越来越多的客户力求通过对数据的融合和挖掘，为其创造出更大的价值。华为云开放强大的人工智能和大数据平台，提供多维度的数据处理服务，在客户的选择与授权下，让客户的数据发挥价值。

华为云秉承数据中立原则，“不碰数据”，保障数据为客户所有、由客户使用、为客户创造价值：

第一，不用技术手段获取客户的数据。

第二，不会强迫客户跟华为云进行数据的交换。

第三，开放人工智能和大数据的平台，为客户处理数据，让客户的数据发挥价值。

2 可信、开放、全球化，使能客户安全实现数据价值

2.1 基于责任共担，明确数据主权

“云安全责任共担”已经成为业界共识。华为云参考业界常规做法，结合具体实践，定义了华为云数据安全责任共担模型。

图2-1 华为云数据安全责任共担模型

客户在使用华为云服务时，通常提供或产生以下两类数据：

- 客户内容数据

客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

- 账户信息

华为云在遵从国家法律法规要求的前提下，会收集客户的账户信息，包括但不限于客户的注册信息、操作日志等，具体信息参见《隐私政策声明》。

对于客户内容数据，华为云将为客户提供数据保护的服务和工具。对于客户的账户信息，华为云将依照《隐私政策声明》予以尊重和保护，在处理过程中，遵循数据最小化原则收集、存储和使用客户的账户信息，并通过全面的数据保护措施确保客户的账户信息安全。

- 我们的责任

作为云服务提供者，华为云恪守数据保护承诺与原则，确保云平台持续、高效、安全、稳定地运行。为客户提供安全、合规的云计算服务，使能客户保护数据安全。

- 客户的责任

客户是其数据的主体。客户依据自身业务发展的需要以及面临的数据安全风险，制定数据保护策略，并采取适当的措施，保障云上数据安全。华为云作为云服务提供者，向客户提供丰富的数据安全服务产品和解决方案，服务和方案的选择由客户自主完成。

2.2 以安全工程为基石，以合规治理为城墙，开放 AI 和大数据处理能力

- 安全是华为的战略，所有员工都是安全的责任人

网络安全与隐私保护是华为公司的战略。为保证安全战略的有效执行，首席执行官、董事会和全球主管亲自主持、制定并发布网络安全整体战略，所有华为员工都是安全的责任人。

依托华为强大的网络安全与隐私保护体系和宝贵的实践经验，华为云设置了网络安全与隐私保护组织，直线向总裁汇报，专门从事网络安全与隐私保护工作，并有独立的安全评估组织，对所有的服务产品、解决方案进行网络安全与隐私保护的验证。华为云的网络安全与隐私保护工作成果，得到了德国电信的认可，通过了 PSA 认证。

- 以安全工程为基石，确保平台和服务自身安全

华为云具备业界领先的软硬件系统化的全栈、全生命周期管理的安全工程能力。2018 年华为云高分通过 BSIMM 安全测评，安全工程能力进入全球前三，成为国内首家和独家获得此权威认证的云服务商。

华为云吸收业界普遍实践的 DevSecOps 经验，参考业界已发布的密码算法、密钥管理、会话管理、隐私保护等标准及最佳实践，并融入到服务产品开发上线流程，从分析设计、编码、测试、第三方软件管理、发布等阶段层层把关，逐步构建高度自动化的软件安全工程能力和工具链，保障各服务产品和组件均满足安全质量要求。

- 开放 AI 和大数据处理能力，助力客户实现数据价值

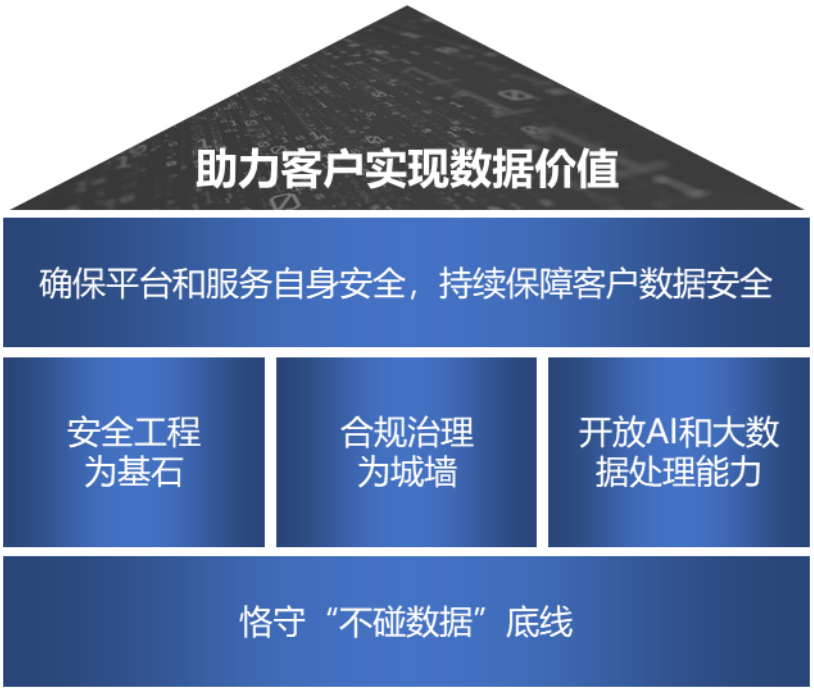
华为云提供丰富的服务和解决方案，助力客户数据的安全变现。例如，华为云 EI 智能，以服务的形式分享华为 30 年沉淀的数字化技术，让数据为客户发挥价值。利用华为全球众多国家和地区的网络资源布局，使客户享受一站式云连接网络服务，助力客户安全快速拓展海外业务。华为云首创自主掌控密钥的 DEW 加密服务，“把钥匙交给用户”的同时，还允许“用户自己配钥匙”，保障数据主权交给客户。

- 以合规治理为城墙，持续保障客户数据安全

华为云打造集预测、防护、检测、响应为一体的云数据安全治理体系，围绕安全防护、合规运营、隐私保护等方面开展网络安全治理工作，持续的风险监测和分析，智能协同多种安全防御措施，及时刷新安全策略、流程和技术，保障云上数据安全。

华为云遵从国际标准，实现全球化的合规治理。为帮助客户满足安全合规性要求，华为云积极贡献最佳实践，并通过安全合规服务，向客户提供必要的安全加固能力及应急保障。

图2-2 华为云数据安全体系



3 业界领先的安全工程能力，打造客户可信的平台和服务

3.1 软硬件系统化的全栈、全生命周期的安全工程能力

华为云提供从芯片到云端的全栈安全防护，包括芯片、系统、平台、应用、数据的各层安全措施，自研、定制化的芯片级安全协议、可信计算，保证客户数据从芯片开始就固若金汤。

华为云将安全活动贯穿服务产品的全生命周期，涵盖安全设计、安全编码、安全测试、安全验收、安全发布、漏洞管理等各个环节，保障服务产品的安全。

华为云成立独立于开发、交付团队的安全实验室，对各服务产品和组件进行严格的、基于风险的安全测试，不断提升平台、服务产品和组件的安全质量。该测试是产品交付上线的必要条件。

为了确保华为云以及各项云服务满足各区域法律法规、客户安全需求，华为公司依托内部专业的安全隐私和法务团队，以及一流的外部顾问资源，对相关法律法规以及技术要求进行跟踪、分析、研究，并将相关要求贯穿落实到从产品研发、上线、运营、运维等各个环节中，从根本上保障客户利益。

3.2 从“芯”出发，构筑硬件系统化的全栈数据安全

华为云在安全研发上长期大力投入，从芯片、平台、系统、应用、数据等领域，进行了安全防护技术研发与创新。打造全栈式纵深安全防护体系，保障客户数据安全。

- 芯片级可信计算和安全加密

华为公司在可信计算领域拥有深厚的技术积累，率先推出支持国密算法的可信服务器和可信云平台解决方案。基于可信计算模块芯片，华为云具备对云平台主机进行完整性度量及提供更多安全特性的能力，降低云主机的软硬件被篡改的风险，满足更高的安全需求。

华为云基于 Intel SGX 技术，构建芯片级、轻量型的密钥管理和数据加密能力。一方面摆脱对传统硬件存储模块（HSM）的依赖，另一方面，通过芯片级的安全环境进行高性能加解密运算，有效降低明文内存泄露风险，确保使用中的数据安全。

- 平台

华为云统一虚拟化平台（UVP），直接运行于物理服务器之上，通过对服务器物理资源的抽象，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。UVP 基于硬件辅助虚拟化技术提供虚拟化能力，为虚拟机提供高效的运行环境，并且保证虚拟机运行在合法的空间内，避免虚拟机对 UVP 或其他虚拟机发起非授权访问。

- 系统

华为 EulerOS 通过了公安部信息安全技术操作系统安全技术要求四级认证。EulerOS 系统集成先进的 Linux 技术，在 CPU 调度、内存、网络和存储等方面做了大量的优化，可以帮助客户实现有效资源重组，为客户提供了富有竞争力的开放式 IT 平台。该系统简单易用，在高性能、稳定性、可用性和可扩展性方面能满足客户日益复杂、多变的业务需求。EulerOS 能够提供可配置的加固策略、内核级 OS 安全能力等各种安全技术以防止入侵，保障客户的系统安全。

- 应用

华为云基于业界领先的安全工程能力，对应用开发的全流程进行系统化的、严格的安全管控，确保应用满足安全质量要求。各应用通过华为公司自研的 API 网关向客户提供标准化集成接口，具备严格的身份认证及鉴权、传输加密保护、细粒度流量控制等安全能力，防范数据被窃取和嗅探。并且，华为云通过深度学习、运行时应用保护、去中心化认证等技术的运用，进一步打造用户行为画像、业务风险控制等高级安全能力，实时监控和拦截异常行为，保护应用服务安全稳定运行。

- 数据

华为云将华为公司多年积累的信息资产保护经验复制上云，构建全数据生命周期的安全防护能力。通过自动化敏感数据发现、动态数据脱敏、高性能低成本数据加密、快速异常操作审计、数据安全销毁等多项技术的研究与应用，实现数据在创建、存储、使用、共享、归档、销毁等多个环节的管控，保障云上数据安全。

3.3 步步为营，全生命周期管理数据安全

华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。

安全设计

华为云服务产品和组件遵从华为安全设计原则、规范、基线，在安全需求分析和设计阶段中根据业务场景、数据流图、组网模型进行威胁分析，借助高度自动化的工具及丰富的案例库，极大地提升了方案设计的效率及完备性。设计中的数据安全实践具体如下：

- 数据隔离

华为云承载了众多客户的数据，各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。

以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性，服务设计的实现因服务而异。如块存储，数据隔离以卷（云硬盘）为单

位进行，每个卷都关联了一个客户标识，挂载该卷的虚拟机也必须具有同样的客户标识，才能完成卷的挂载，确保客户数据隔离。

- 数据加密

华为云的多个服务采用与密钥管理服务（DEW）集成的设计，方便客户管理密钥，客户可以通过简单的加密设置，实现数据的存储加密。目前 DEW 已经支持对象存储、云硬盘、云镜像、云数据库和弹性文件存储等多个服务，并且数量还在不断增加，极大地方便了数据加密操作。

华为云服务为客户提供控制台和 API 两种访问方式，均采用加密传输协议构建安全的传输通道，有效地降低数据在网络传输过程中被恶意嗅探的风险。

- 数据冗余

华为云数据存储采用多副本备份和纠删码设计，通过冗余和校验机制来判断数据的损坏并快速进行修复，确保即使一定数量的物理设备发生故障也不会影响业务的运行，使华为云存储服务的可靠性达到业界先进水平，例如对象存储服务的数据持久性高达 99.999999999%。

- 隐私保护设计

华为云各服务产品的设计遵循《隐私保护设计规范》，该规范建立了隐私基线、维护隐私的完整性和指导隐私风险分析，制定对应措施并作为需求落入服务产品开发设计流程。

安全编码和测试

华为云严格遵从华为公司对内发布的多种编程语言的安全编码规范。开发人员在上岗编码前均须通过对应规范的学习和考试。同时使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。

华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，确保发布的云服务满足安全要求。

安全验收和发布

云平台版本、重要云服务上线前，需要通过华为公司全球网络安全与用户隐私保护官和首席法务官的严格审查，针对所服务区域的安全隐私要求的合规性进行分析、判断，确保为华为云以及华为开发的云服务满足各区域法律法规和客户安全需求。

漏洞管理

华为云构建了完善的漏洞管理体系，实现漏洞感知、漏洞处置、漏洞披露等全流程的跟踪与管理，确保云平台各服务产品和组件的漏洞得到及时的发现与修复，降低漏洞被恶意利用所带来的风险。

3.4 严进宽用，端到端管理开源及第三方软件的安全

为给客户提供丰富的云服务产品，构建良好的生态，业界云服务商均引入大量的开源和第三方软件，华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。

华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。

在使用中，须将第三方软件作为服务或解决方案的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或解决方案中使用独立的第三方软件是否引入新的安全问题。

华为云将网络安全能力前置到社区，在出现开源漏洞问题时，依托华为云对开源社区的影响力，第一时间发现漏洞并修复。漏洞响应时，须将开源及第三方软件作为服务和解决方案的一部分开展测试，验证开源及第三方软件已知漏洞是否修复，并在服务的 Release notes 里体现开源及第三方软件的漏洞修复列表。

4 开放 AI 和大数据处理能力，使能客户安全的实现数据价值

4.1 分享华为 30 年沉淀的数字化技术，让数据为客户发挥价值

华为云 EI 是企业智能的使用者，基于 AI 和大数据技术，通过云服务的方式，提供一个开放的、可信的、智能的平台，结合产业场景，使能企业应用系统能看、能听、能说，具备分析和理解图片、视频、语音、文本等能力，让更多的企业便捷的使用 AI 和大数据服务、场景化解决方案和 EI 智能体，加速业务发展，造福社会。华为云 EI 服务家族提供了基础平台服务、EI 大数据服务、EI 智能视频、EI 语音语义、视觉认知和行业场景解决方案的 EI 智能体等几大类智能云服务。

基础平台服务新增了深度学习服务和镜像，以及图引擎服务，具备强大的机器学习、深度学习和关系分析基础能力。在视觉认知领域新上线了人脸识别、图像识别和内容检测服务，提供更加广泛的面向计算机视觉的应用场景，扩展了语音语义的使用范围，包括新发布的语音识别、语音合成、自然语言处理和智能问答服务，使能自然语言输入和人机交互。具有行业场景解决方案的 EI 智能体服务包括智能水务、智能制造、智能电力、智能交通、智能金融、智能零售等，并在不断的丰富中。

4.2 层层防护，保障数据全生命周期安全

为保障客户安全的处理云上数据，华为云对数据生命周期的各阶段进行层层防护，并通过友好的操作界面和接口，方便客户使用与集成，满足不同行业客户对数据安全的个性化需求。

图4-1 数据生命周期各阶段关键防护措施

4.3 区分隔离，将数据创建起始阶段做好

数据创建是指产生新的内容，或对已有内容的替换、更新或修改。针对这一阶段，华为云建议客户首先做好数据分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施，在数据生命周期的起始阶段就做好数据的区分与隔离。

关键能力

- 自主位置选择

华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的法律法规要求等进行区域的选择，确保客户内容数据存储在目标位置。

- 隔离环境构建

当客户使用云硬盘、对象存储、云数据库、容器引擎等服务时，华为云通过卷、存储桶、数据库实例、容器等不同粒度的访问控制机制，确保客户只能访问到自己的数据。在客户自建存储的场景下，例如在虚拟机实例上安装数据库软件时，建议客户利用华为云的虚拟私有云（VPC）服务构建出私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在内部子网，并通过配置网络 ACL 和安全组规则对进出子网以和虚拟机的网络流量进行严格的管控。

服务资源

- 云硬盘服务
- 对象存储服务

- 云数据库服务

4.4 动态防护，把数据存储风险降到最低

数据存储是指将数据提交到某种存储库中，通常在数据创建时发生。对于云端存储的敏感及重要数据，建议客户使用加密措施进行防护，降低数据泄露的风险。

关键能力

- 存储加密

华为云将复杂的数据加解密、密钥管理逻辑进行封装，使得客户的数据加密操作变得简单易行。目前，云硬盘、对象存储、镜像服务和关系型数据库等多个服务均提供数据加密（服务端加密）功能，采用高强度的算法对存储的数据进行加密。

服务端加密功能集成了华为云数据加密服务的密钥管理功能（DEW），由 DEW 进行密钥全生命周期集中管理。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，确保了客户云上数据的安全。DEW 采用分层密钥管理机制，方便各层密钥的轮换。通过 DEW 的控制台或 API 进行关联设置，各存储服务加密数据时使用的加密密钥，能够由保存在 DEW 中的客户主密钥进行加密，该客户主密钥又由保存在 HSM 中的根密钥进行加密，构成了一条完整的安全、可信的密钥链。HSM 经过严格的国际安全认证，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取根密钥。DEW 还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。

当客户需要在云上延续传统物理密码机的使用经验或有更高的合规性要求时，可以使用华为云的云加密机服务。该服务将通过国家密码局认证或 FIPS 140-2 第 3 级验证的硬件加密机或其虚拟化实例提供给客户独享，满足客户更高的安全需求。

- 存储容灾

对于企业而言，要保持业务在各种灾难损害发生时的连续性，容灾机制不可或缺。容灾系统的构建涵盖网络、应用、数据等多个层次，其中数据层面的容灾机制着力于保持数据一致性、降低数据丢失率，是容灾系统的关键环节。华为云的存储容灾服务为弹性云服务器、云硬盘和专属存储等服务提供容灾能力，通过存储复制、数据冗余和缓存加速等多项技术，提供跨可用区的虚拟机级容灾保护。当生产站点故障时，通过简单的配置，即可在容灾站点迅速恢复业务，确保数据可靠性以及业务连续性。

服务资源

- 数据加密服务
- 存储容灾服务

4.5 环环相扣，让数据使用得到有效管控

数据使用是指数据被查看、处理或以不包括修改在内的其他方式采用。大数据时代，越来越多的企业力求通过对数据的融合和挖掘，为企业创造出更大的价值，同时也带来了信息泄露和法律法规遵从上的风险。为了避免上述风险，华为云从数据访问控制、安全防护、审计等方面为客户提供了相关服务，协助客户对数据的使用和流转做到更加细粒度的管控。

关键能力

- 访问控制

华为云的统一身份认证服务（IAM）为客户提供适合企业级组织结构的用户账号管理、身份认证和细粒度的云上资源访问控制。IAM 提供多因素认证（MFA）功能，提高账号登录和重要操作的安全性。IAM 支持数字签名和时间戳的机制，防止 API 请求被篡改以及重放攻击等情况的发生。IAM 支持与客户既有帐号管理系统的联邦认证，即允许用户在既有账号管理系统认证后访问华为云资源。

系统的运维人员通常权限较高，更易接触底层数据，在出现恶意操作或误操作时会对系统造成更大的破坏，因此，华为云建议客户使用堡垒机服务对运维活动进行管控。华为云的云堡垒机服务将华为公司多年的安全运维经验服务化后向客户输出，提供一站式的帐号管理、资产管理、访问控制和操作审计等功能，协助客户做好运维控制与合规审计。

- 数据库安全防护

客户可以采用华为云数据库安全服务（DBSS）为数据库提供替身式防护。DBSS 基于专利保护的反向代理模式以及机器学习机制，集数据脱敏、数据库防火墙和数据库审计功能于一体，一站式全方位保障云上数据库的安全。对于数据脱敏，DBSS 能够根据规则识别出敏感数据，并依据脱敏策略对非授权读取的敏感数据进行实时隐藏，既不损耗数据库性能也不改变原始存储。作为数据库防火墙，DBSS 能够实时监测和拦截 SQL 注入等恶意攻击，提升数据库的抗攻击性。

- 对象存储水印

当需要对数据进行版权保护、真伪鉴别、流转跟踪时，客户可以选择数字水印技术。华为云的对象存储服务具备对图片添加文字或图片类型水印的功能，支持通过控制台图形界面、代码编辑模式和接口调用多种使用模式，便利客户对图片进行水印设置，并快速获取到处理后的图片。

- 审计

对于对象存储、文件存储等服务，客户可以使用云审计服务来记录用户对数据的操作。对于关系型数据库服务，客户可以使用数据库安全服务来进行数据库列级的管理和访问活动记录。对于个性化的日志采集需求，客户可以使用云日志服务对任何文本日志进行采集与统一管理，日志查询简单快速，支持亿级数据秒级响应。

服务资源

- 统一身份认证服务
- 华为云堡垒机
- 数据库安全服务
- 云审计服务
- 云日志服务

4.6 精管严控，使数据共享得以安全实现

数据共享是指数据在用户、客户、合作伙伴之间交换使用。开放共享是数据融合挖掘的前提，能够消除信息孤岛，促进数据价值释放。为了保障自身的数据权益，建议客户对数据的访问和传输进行严格的管控，做到安全的数据共享。

关键能力

- 访问控制

华为云的 IAM 服务支持委托的方式实现不同帐号间的资源共享。通过创建委托并授予被委托方资源管理权限，被委托方可以使用自身帐号登录华为云并完成共享资源的接管。客户无需将安全凭证共享给被委托方，在确保帐号安全的前提下，实现了资源共享。

- 传输加密

当客户通过互联网提供 Web 网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。

针对客户业务混合云部署和全球化布局的场景，可以使用华为云提供的虚拟专用网络（VPN）、云专线服务、云连接等服务，实现不同区域之间业务的互联互通和数据传输安全。

目前 VPN 服务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。

云专线服务基于运营商多种类型的专线网络，在本地数据中心与华为云 VPC 之间构建专享的加密传输通道，各客户专线之间物理隔离，满足更高的安全性、稳定性要求。

云连接服务是基于华为公司多年全球 IT 运营经验，利用全球众多国家和地区的网络资源布局，倾力打造的一站式云连接网络服务，能够快速在多个本地数据中心与多个云上 VPC 之间建立私有通信网络，支持跨云 VPC 的互连，大大提升了客户业务向全球拓展的安全性和速度。

服务资源

- SSL 证书管理服务
- 虚拟专用网络
- 云专线服务
- 云连接服务

4.7 分类归档，实现数据的有效备份恢复

数据归档是指数据不再被活跃使用而进入长期存储。对于企业而言，数据的有效备份、归档以及快速恢复能力尤为重要，以便在发生误操作、故障、网络攻击、灾难等突发事件的情况下，及时进行恢复，避免数据丢失，保持业务的连续运行。

关键能力

- 备份归档

华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用对象存储服务的版本控制、云硬盘备份、云服务器备份等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，充分利用云服务模式下按需使用、弹性扩展、可靠性高的特点，结合备份归档软件和华为云基础设施，将客户云下数据备份归档到华为云。

通过与数据加密服务集成，备份数据也可以方便、快速地实现加密存储，有效保证备份数据的安全性。

- 恢复演练

为了提高数据灾难发生时的应急响应能力，客户可以定期依据计划进行恢复演练。华为云备份归档解决方案支持客户使用备份数据，在云上即时部署的系统中恢复数据，完成后即可释放资源，极大节省了恢复演练成本。

服务资源

- 数据加密服务
- 云硬盘备份
- 云服务器备份
- 备份归档解决方案

4.8 永久销毁，做到数据完全彻底被清除

数据销毁是指使用物理或数字方式，将数据永久销毁。当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。为了避免重要数据销毁后不可恢复，或因误操作丢失，建议客户在销毁数据之前慎重考虑，对拟销毁的数据做好备份（参考 4.7 分类归档）或迁离。

关键能力

- 客户内容数据迁离

华为云提供的云数据迁移服务（CDM），支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。

- 客户内容数据销毁

在客户内容数据的销毁阶段，华为云会对指定的数据及其所有副本进行全面的清除。当客户确认删除操作后，华为云首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。

- 客户销户

华为云支持客户对账户进行注销。当客户提出账户注销的申请并通过华为云对账号的验证后，客户内容数据进入保留期，保留期内，客户不能访问及使用云服务，但对客户存储在云服务中的数据仍予以保留。保留期届满后，客户内容数据会得到彻底的清除，无法进行恢复。

服务资源

云数据迁移服务 CDM

5 全球化的合规治理，保障客户数据安全无忧

5.1 安全治理，动态协同保障云上数据安全

华为云打造集预测、防护、检测、响应为一体的云数据安全保障体系，动态协同多种安全防御措施，保障云上数据安全。

图5-1 华为云数据安全防护关键措施

预测

华为云构建了统一的分析和预警平台，全面掌握数据安全态势，快速识别、响应安全事件，同时通过对告警、事件、资产等信息的关联分析进行风险评估以及安全态势预测，由此可预先制定安全防护策略，做到防范于未然。

华为云构建了完善的漏洞管理体系，实现漏洞感知、漏洞处置、漏洞披露等全流程的跟踪与管理，确保云平台各服务产品和组件的漏洞得到及时的发现与修复，降低漏洞被恶意利用所带来的风险。

防护

- 物理和环境安全防护

华为云严格遵从国际、国内相关标准要求，对数据中心进行合理的选址及设计施工，同时进行统一垂直管理，实施分层分级的安全防护，从围栏到 DC 建筑，从 DC 建筑到模块，从模块到机柜，从机柜到服务器，安全防护措施逐级增强，确保云数据中心的物理和环境安全。在严格执行物理访问控制的同时，通过智能的 7×24 小时监控，及时发现并修复安全隐患，确保数据中心稳定运行。

- 网络安全防护

华为云帮助客户构建网络安全防护体系，防止数据被窃取或泄露。

华为云在互联网边界部署 Anti-DDoS 设备，来完成对异常和超大流量攻击的检测和清洗。同时在关键网络分区边界部署入侵防御设备，识别来自互联网以及客户间的攻击行为，并能够进行自动化、精确的阻断。

所有云平台主机均安装安全防护软件，进行主机层面的弱密码检测、配置管理、入侵检测、应急响应等，构建合规、安全的主机环境。

针对向外提供 Web 服务的系统，使用 Web 安全防护设备抵御应用层攻击行为，确保 Web 服务的安全。

- 运维管理

华为云制定并落实严格的规范、流程和管控措施，实现了运维操作的统一接入、统一认证、统一授权、统一审计。

运维人员首先通过双因子认证接入运维环境，再集中从堡垒机跳转到目标机进行操作。目标机的口令被堡垒机回收并定期更新，确保运维人员无需也无法获取口令。严格的运维接入阻断了未授权的内部访问，是客户数据安全保护在关键环节。

华为云对于运维人员实行基于角色的访问控制权限管理，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保运维人员不触碰客户的数据。

检测

华为云联动分析各安全设备的告警信息，结合机器学习技术和专家经验构建相应的模型，检测未知数据安全风险，并及时采取有效措施进行防御。

华为云遵从法律法规要求，具备集中、完整的日志审计系统。内部人员运维操作均被日志平台采集并记录。华为云的日志审计系统有强大的数据保存及查询能力，确保所有日志内容保存时间超过 6 个月。华为云设置独立的内审部门，定期对运维流程各项活动进行审计，及时发现、纠正违规行为。

响应

华为云秉承快速发现、快速定界、快速隔离与快速恢复的“四快”原则，根据安全事件对全网及客户的影响，对事件进行分级响应。华为云设置 7X24 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。

5.2 秉节持重，遵从全球化数据安全合规认证与标准

华为云积极参与业界数据和隐私保护标准建设及认证工作，贡献在数据安全保护方面的优秀实践和经验。一方面,客户可以通过认证和报告验证华为云安全防护措施的有效性，另一方面，华为云将数据安全防护的实践和经验共享给客户，帮助客户保护云上数据安全。

华为云通过国内外权威的数据安全相关的认证主要有：

- 中国公安部信息安全等级保护四级
- 可信云《云服务用户数据保护能力认证》
- ISO/IEC 27001
- ISO/IEC 27017【1】
- ISO/IEC 27018
- ISO 22301【2】
- CSA STAR 金牌认证
- PCI DSS（支付卡行业数据安全标准）
- 中国数据中心联盟（DCA – Data Center Alliance）可信云服务认证、金牌运维，其中云主机获取最高级五星+认证
- 德国Trusted Cloud认证【3】
- 德国TÜV Trusted Cloud认证【4】
- 德国TCDP认证【5】
- 下面以几个认证为例，介绍一下华为云在数据安全方面的合规与标准遵从。

- CSA STAR 金牌认证

华为云通过的 CSA STAR 金牌认证表明了华为云已建立起一套科学有效的管理体系，能够系统的、持续的管理安全风险，具备保障自身及客户的数据保密性、完整性和可用性的能力。

- PCI DSS 认证

华为云是国内首家全平台、全节点通过 PCI DSS（支付卡行业数据安全标准）认证的云服务提供者。该标准认证的通过，验证了华为云能够为客户提供金融级的数据安全保障，使得客户可以在符合 PCI DSS 标准的华为云上部署金融支付业务，帮助客户实现传输、存储、处理支付卡用户信息时的安全合规。

- 可信云《云服务用户数据保护能力认证》

华为云凭借全面的安全防护能力和对用户隐私数据保护机制的落实，首批通过了可信云用户数据保护能力认证。

- ISO/IEC 27018 认证

华为云通过的 ISO/IEC 27018 认证表明了华为云已拥有完备的个人数据保护管理体系，在数据安全管理方面处于全球领先水平。

5.3 机制健全，严格保护账户信息

华为云理解并尊重客户对其账户信息所拥有的各项权利，并通过技术上的合理努力及严格的管理措施确保账户信息的安全。在对账户信息进行处理时，严格遵从相关法律法规的要求，并参考行业最佳实践，保障账户信息安全。

华为云仅在以下情况处理客户的账户信息：

- 根据客户签署的《华为云用户协议》和《隐私政策声明》及其他云服务协议，为客户提供服务。
- 根据所适用的法律法规的规定或主管机关的要求，处理账户信息。

华为云要求处理账户信息的相关岗位人员在上岗前须签署保密承诺。在处理账户信息时，严格管控并记录操作日志，做到事前预防、事中控制、事后可追溯的数据安全机制。

华为云尊重和保护客户作为数据主体对其账户信息的合法权益，包括知情权、数据访问权、数据更正权、数据删除权等。对于客户提出的上述权利诉求，华为云承诺通过合理努力，为客户权利提供通道，并积极响应。

6 结语

随着云计算服务的不断发展，越来越多的企业将业务迁移上云，同时数据安全防护面临的挑战更趋严峻。面对复杂多变的网络环境及安全挑战，华为云恪守 “不碰数据”的理念，遵从责任共担模型，依托华为特有的软硬件全栈技术优势，打造可信的云服务，与客户共同构建数据安全能力。

华为云以数据保护为核心，以安全工程为基石，提供满足全栈、全生命周期安全的产品和服务，以合规治理为城墙，对标全球化的权威标准与能力要求，实施完善的安全治理体系，让客户可以放心地在华为云上开展业务。保障数据安全的同时，开放华为多年积累的 AI 及大数据处理能力，使能客户创造价值，实现华为云和客户的双赢。

籍此白皮书发布，将华为云在数据安全领域的丰富实践和经验，分享给客户，分享给业界，以期推动云数据安全领域的进步。同时华为云将持续提升安全防护能力，发布高质量的云服务和解决方案，助力客户商业成。

A 版本历史

日期	版本	描述
2018 年 9 月	1.0	

B 参考

【1】华为与德意志电信（Deutsche Telekom）的合营云已经通过 ISO/IEC 27017 认证。

【2】华为与德意志电信（Deutsche Telekom）的合营云已经通过 ISO 22301 认证。

【3】华为与德意志电信（Deutsche Telekom）的合营云已经通过德国 Trusted Cloud Service 认证。

【4】华为与德意志电信（Deutsche Telekom）的合营云已经通过德国 TÜV Trusted Cloud 认证。

【5】华为与德意志电信（Deutsche Telekom）的合营云已经通过德国 TCDP 认证。