华为云数据安全白皮书

文档版本 3.0

发布日期 2025-03-05

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

数据作为新型生产要素，是企业数智化转型的基础。随着企业数智化转型的加速，云计算服务的市场需求持续增长，一方面为企业带来了巨大的发展机遇，另一方面也伴随着诸多的挑战，尤其是在数据安全领域，敏感数据泄露、数据加密勒索、数据违规使用等安全风险成为企业上云过程中的主要顾虑。

华为云作为负责任的云服务提供商，深知数据安全的重要性，并将其视为企业发展的核心要素之一。华为云建立了一套完善的数据安全治理体系，包括组织架构、政策制度、流程规范、技术工具及度量监督，为客户数据提供系统化安全保障能力。对内，华为云不断强化安全技术和管理措施，通过实施多层防护体系，实现数据端到端的安全合规。对外，华为云为客户提供全生命周期的安全服务及安全特性，同时通过获取独立第三方机构的数据保护认证，向业界阐述华为云数据安全实践上的高标准能力和持续有效性。

同时，为了进一步消除客户数据上云的安全疑虑，华为云将持续坚持“数据中立”原则，持续落实“数据为客户所有、为客户所用”的主张，并持续贯彻“不以技术手段获取客户业务数据、不强迫客户与华为云进行数据交换、保证所有数据处理严格遵从法律法规要求”的理念，支撑客户使用数据驱动价值创造的同时构筑安全可控的云上数据安全防护能力。

另外，为了更好地保护客户个人信息并帮助客户构建云上业务的隐私保护，持续有效地开展隐私保护管理工作，华为云也建立了完善的业务隐私保护管理体系，可以通过“信任中心”-“隐私”模块中的《华为云隐私保护白皮书》进一步了解。

2 华为云数据安全架构

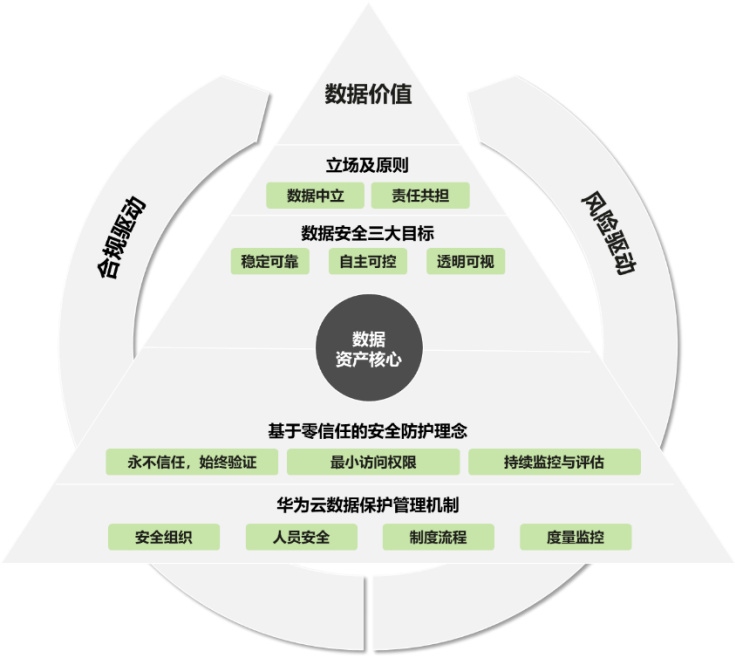

图2.1华为云数据安全架构

华为云坚持“数据中立”原则，贯彻“客户内容数据为客户所有，为客户所用，为客户创造价值”的主张，以数据资产为核心，以合规、风险为驱动，基于“永不信任，始终验证”、“最小访问权限”和“持续监控与评估”的理念，围绕“稳定可靠”、“自主可控”、“透明可视”三大目标构建数据安全体系。

华为云数据保护管理机制涵盖“安全组织”、“制度流程”、“人员安全”、“度量监控”四个方面，为系统有效地保护客户数据、支撑数据安全目标实现提供基础保障。

华为云通过“稳定可靠”、“自主可控”、“透明可视”三大支柱保护客户云上数据资产。其中：

- 稳定可靠是指华为云构建了稳定可靠的云平台基础设施，基于静态数据、使用中数据、传输中的数据三大数据状态，为客户云上的内容数据安全提供基础的防护能力；
- 自主可控是指华为云提供了全栈的数据安全服务和安全特性，客户可以基于自身的数据安全需求，自主决定数据驻留位置，数据上云下云以及实现数据生命周期的安全管理；
- 透明可视是指华为云通过一系列的数据处理透明可视能力，让客户可以进一步了解云上内容数据的处理操作，包括客户对远程客服支持的授权管理，以及客户对云上内容数据的操作等。

在复杂的云服务业务模式中，数据安全不再是单方面的责任，保障数据安全需要客户与华为云的共同努力。基于此，华为云参考业界常规做法，结合具体实践，也定义了华为云和客户的责任和义务，帮助客户理解双方数据保护的责任边界，避免出现数据保护的真空区。

3 华为云数据保护治理体系

3.1 组织职责

华为云构建了一套涵盖决策层、管理层、执行层、监督层、支撑层的数据安全管理责任体系，这是确保云端内容符合数据安全标准的关键架构。通过明确各层级的责任分工与协作机制不仅强化了内部安全管理流程，还促进了与用户的信任关系，确保了数据处理活动的透明度与合规性。各层级均需遵循严格的安全策略和操作规范，以预防数据泄露、保障用户隐私和维护系统完整性，从而为企业和个人用户提供坚实的数据安全保障。这一体系是组织中不可或缺的部分，它明确了各层级的责任和响应安全事件的流程，以及如何持续改进安全措施。

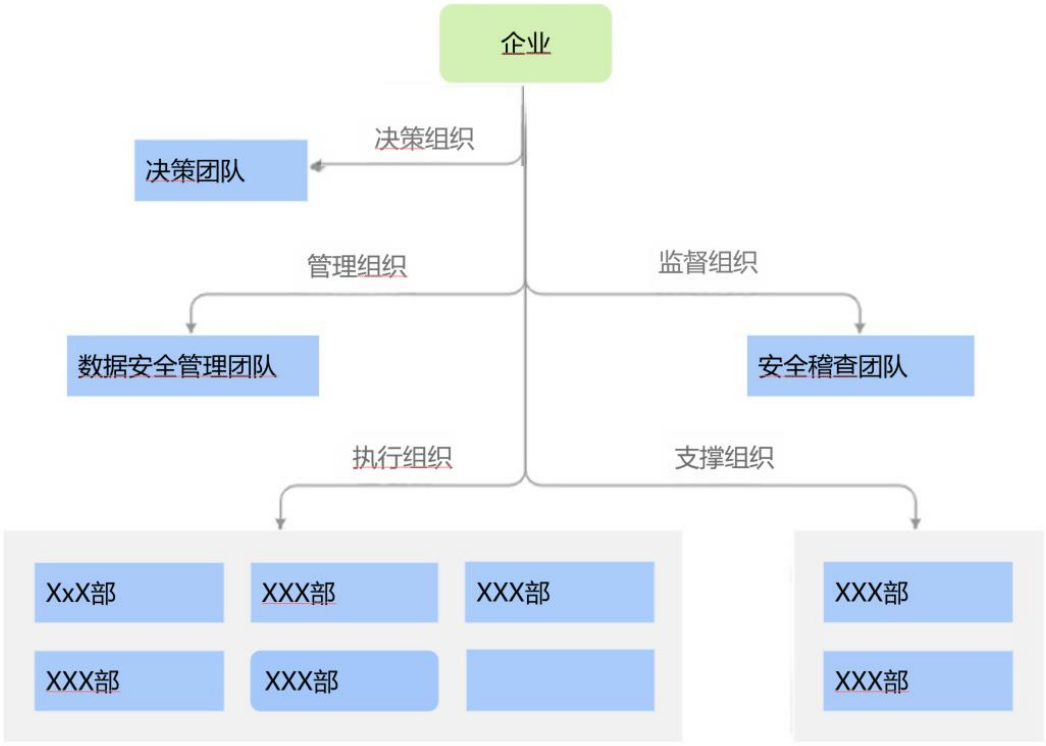

图3.1 华为云数据安全管理责任体系

- 决策层：负责华为云数据安全的战略和重大事项的决策；
- 管理层：数据安全管理负责人、数据安全管理组织负责数据安全日常管理工作，以及与外部监管组织的沟通与信任能力建设；
- 执行层：数据安全责任人负责本领域数据安全要求的落地及日常管理工作，并对本领域数据安全的结果负责；
- 监督层：通过任命独立的稽查团队，以查促建，验证各业务领域数据安全的落地效果，并督促各业务数据安全责任人对发现的问题进行跟踪闭环管理；
- 支撑层：数据安全运作的组织的统称，包括工具建设、人员能力建设、外部沟通支撑等。

3.2 人员管理

华为云实施了一系列完善的人员安全管理机制，包括定期的安全培训、严格的访问控制以及明确的安全责任分配。这些措施不仅提升了内部人员及合作伙伴的安全素养，也确保了所有操作符合高标准的安全实践要求，从而有效防范内外部安全威胁，保障数据安全。

图3.2 华为云数据安全管理机制

首先，华为云为员工和合作伙伴构建了完善的安全管理体系，包括员工入职到离职的全生命周期。通过持续提升相关人员的数据安全意识及安全能力，有效保障云平台的整体安全水平。所有员工在入职后都需要遵守员工行为管理细则，对于违反安全要求的员工，将根据安全违规问责机制进行处置。同时华为云会定期对全员开展安全意识和能力培训，不同岗位的员工还需接受其岗位相关的网络安全和隐私保护培训，以降低因不同岗位人员因安全意识和能力不足而引发的安全与隐私风险。

其次，在客户使用华为云服务的过程中，部分服务可能需要由华为云与供应商共同为其提供。华为云在引入供应商之前会进行安全尽职调查，并通过合同约束供应商采取安全措施来保护客户数据。同时华为云制定外包供应商信息安全管理规定并将其作为合同的附加条款，并明确供应商违反此规定的处罚措施。

3.3 制度流程

为了确保数据安全管理要求的有效落地，华为云从两方面将数据安全管理要求融入研发、运维、运营、供应链、市场与销售、工程交付及技术服务等各主业务流程中进行持续运作，以确保数据安全管理要求能够持续且有效地实施。这包括制定详尽的安全政策、操作指南和应急响应计划，并通过定期审核与更新，使安全管理机制与时俱进，适应不断变化的威胁环境，从而保障用户数据的安全与合规。

图3.3 华为云数据安全管理制度

首先，增加数据安全专属的流程，例如数据定级审核流程等。其次，将安全要求融入业务现有流程，避免数据安全要求在业务流程外运作，例如将数据安全要求融入研发运维流程等。另外，安全作为质量管理体系的基本要求，通过管理制度和技术规范来确保其有效实施。华为云通过内部审计和第三方独立机构的安全认证和审计等来监督和改进各项业务流程。

3.4 度量监督

华为云设计了一套全面的安全度量监督机制，以确保数据安全管理的有效实施。这一机制涵盖了从日常监控到高级审计的所有层面，通过对关键性能指标（KPIs）的持续跟踪，能够及时发现并解决潜在的安全隐患。

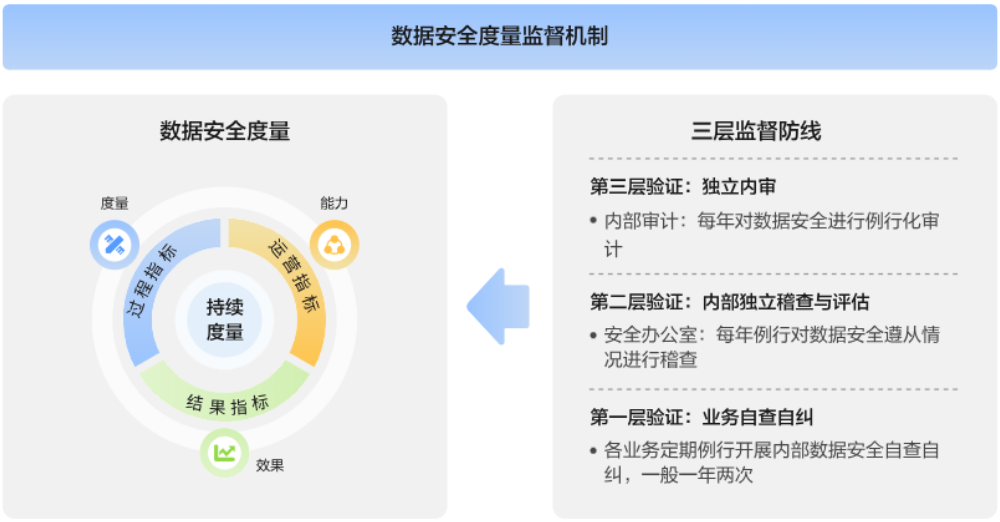

图3.4 华为云数据安全度量监督机制

华为云从度量、能力、效果三个维度制定相关指标，包括过程指标、运营指标和结果指标，以持续评估、监控数据安全控制措施的实施情况，并推动业务领域持续优化改进。

此外，华为云还建立了数据安全三层监督防线：

- 第一道防线是前线业务团队，由各业务领域数据安全专员，基于数据安全自检清单，定期组织业务例行开展自查自纠；
- 第二道防线，华为云独立安全团队稽查。安全稽查团队每年例行针对重点业务开展数据安全稽查，并负责对已识别问题的跟踪闭环；
- 第三道防线，华为集团独立审计团队，每年按需抽查重点业务或领域，开展数据安全相关的审计。

这种多层次的监督机制不仅增强了华为云自身的安全防护能力，也为客户提供了更高水平的数据安全保障，确保了安全要求能够在实际操作中得到严格执行。

4 华为云数据安全解决方案全景

华为云以数据资产为中心，围绕数据全生命周期，构建数据安全服务及安全特性，支撑客户实现数据安全的自主可控。

原则	提供能力	子能力	能力或产品
稳定可靠	静态数据安全	数据可靠性	● 存储服务可靠性保证 ● 服务可靠性保证
		数据隔离	● 虚拟计算资源隔离 ● 网络隔离 ● 服务隔离
		存储加密	● 静态数据加密
		数据安全销毁	● 数据逻辑销毁 ● 数据物理销毁
		访问管控	● 运维人员职责分离（SOD） ● 基于角色的访问控制（RBAC） ● 基于属性的访问控制（ABAC） ● 多因素认证（MFA）及审计
	传输中数据安全	传输加密	● 虚拟专有网络 VPN ● 应用层 TLS 及证书管理
		传输稳定可靠	● 专线服务
	使用中的数据安全	机密计算	● 擎天虚拟化平台
		同态加密	● 同态加密技术

原则	提供能力	子能力	能力或产品
		多方加密	● 多方计算 MPC
自主可控	数据驻留位置		● 全球网络基础设施
	全生命周期可控	自主控制数据采集	● 数据安全中心（DSC）服务 ● 云日志服务 ● 云审计服务 ● 云堡垒机服务
		自主控制数据迁移传输	● 7 阶 12 步云迁移方法论 ● 消息通知服务 ● 分布式消息服务 ● 云数据迁移服务 ● SSL 证书服务 ● 虚拟专有网络 VPN ● 云专线服务 DC ● 云连接服务 CC ● 数据快递服务 DES ● 迁移中心 MgC
		自主控制数据存储	● 数据安全中心 DSC ● 数据加密服务 DEW ● 专属加密 Dedicated HSM ● 密钥管理 KMS ● 密钥对管理 KPS ● 凭据管理 CSMS ● 数据库动态加密存储 DBSS ● 对象存储服务 OBS
		自主控制数据使用	● 统一身份认证服务 IAM

原则	提供能力	子能力	能力或产品
			● 应用信任中心 ATC ● 云堡垒机服务 CBH ● 数据库安全服务 DBSS ● 可信智能计算服务 TICS ● API 数据安全 ● 数字水印 ● 数据脱敏
		自主控制数据销毁	● 云数据迁移服务 CDM ● 云审计服务 CTS ● 密钥管理 KMS
透明可视	客户服务响应		● 合同承诺 ● 个人数据主体权利请求 ● 云审计服务 CTS ● 云日志服务 LTS
	监管要求响应		● 法律法规要求响应
	合作伙伴要求		● 供应商管理机制
	审计认证		● 审计认证证书

5 构筑安全底座，保障云上数据安全

云上内容数据的安全防护能力，离不开安全可靠的云环境。华为云基于华为公司30多年的安全经验沉淀，并结合国内外云安全的优秀实践，构建了安全可靠的云平台基础设施，为实现客户云上内容数据的安全提供基础安全防护能力。

华为云基于静态数据、传输中的数据和使用中的数据三大数据状态，为客户云上的内容数据安全提供基础的防护能力。另外，华为云将日常管理及治理工作中的安全活动固化到相关业务流程及工具里，确保相关的安全要求和措施持续有效的落实。

5.1 密钥保护

华为云通过数据加密服务（DEW）中的密钥管理（KMS）功能提供安全、可靠、简单易用的密钥托管服务。KMS 通过使用硬件安全模块（HSM）保护密钥安全，帮助客户创建和管理密钥，所有的用户密钥都由 HSM 中的根密钥保护，避免密钥泄露。

- **密钥管理服务（KMS）**

密钥管理服务（Key Management Service）是一个安全易用的云上密钥托管服务，其密钥安全由硬件安全模块 (HSM) 保护，可与许多其他华为云服务集成以保护客户存储在这些服务上的数据，客户也可以借助密钥管理服务开发自己的加密应用。KMS服务与诸多云原生服务对接，提供云原生服务加密能力。

KMS覆盖存储、大数据、数据库、IOT等服务场景，软硬件全面满足国密算法，单客户性能达到5WTPS，单客户API调用性能四倍于业界平均水平。

KMS的核心功能包括：

1. 密钥生命周期管理：包括创建、查看、启用、禁用、计划删除、取消删除用户主密钥，并支持修改用户主密钥的别名和描述；

2. 云服务加密：支持OBS、EVS、IMS、SFS、RDS、DDS、DWS等存储类云服务加密；

3. 密钥轮换：广泛重复使用加密密钥，会对加密密钥的安全造成风险。KMS密钥轮换可保障加密密钥的安全性。

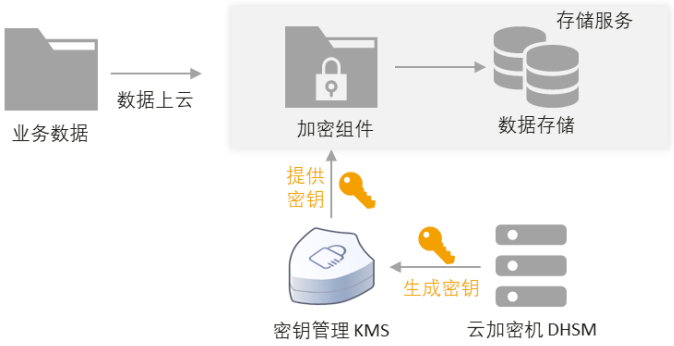

图5.1 KMS 服务架构

KMS支持三种模式，客户密钥自主可控，满足企业不同级别安全要求：

密钥全托管：密钥生成，存储，管理服务均由华为云提供，为客户提供一站式的密钥管理服务，密钥全托管模式在最大程度上降低客户密钥管理工作负担。适用于中小企业和个人用户。

密钥半托管（BYOK）：密钥生成导入由客户负责，密钥存储和管理由华为提供。密钥半托管模式适用于密钥由本地或第三方生成的客户、促进用户密钥生成自主可控。适用于政企、游戏、金融客户。

密钥客户全控制（HYOK）：密钥的生成、存储、管理均受客户自行控制，华为提供专属加密硬件。密钥客户全控制模式适用于处于强监环境下以及在云上存储重要敏感数据的用户，帮助客户实现密钥生命周期完全自主控制。适用于银行、政企和大型跨国集团客户。

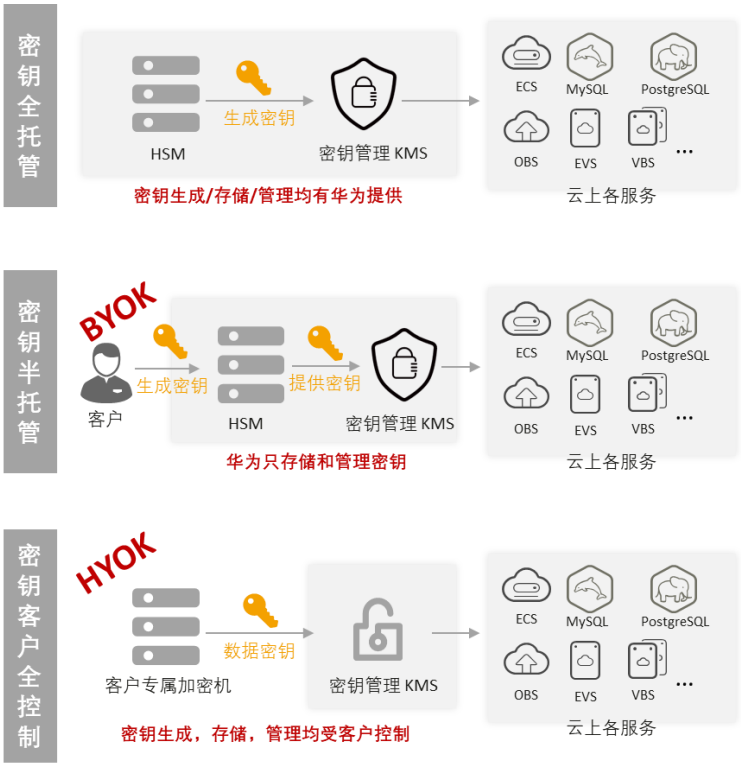

图5.2 KMS的三种服务模式

服务资源

- **密钥管理服务（KMS）**

5.2 静态数据安全

5.2.1 数据可靠性

数据的可靠性是华为云数据安全管理关注的一个关键领域。为了保障客户数据的稳定可靠，华为云的云硬盘、数据库、对象存储等诸多存储类产品均采取了相关的技术手段，为客户提供高可靠的数据存储能力。部分参考示例如下：

存储类型	可靠性保证
云硬盘 EVS	EVS 具有多副本（三副本）的数据冗余保护机制，将数据冗余存在多个物理位置，以保证数据的可靠性和一致性。EVS 采用副本同步写、读修复等措施，能够自动后台修复硬件故障，并快速自动重建数据，数据持久性可达 99.9999999%。通过 CBR 实现云硬盘的备份与恢复，且支持通过云硬盘备份创建新的云硬盘。
云备份 CBR	备份数据跨数据中心保存，数据持久性高达 99.999999999%。 CBR 支持创建多 AZ 存储库，将备份数据存储到同区域的多个 AZ。当某个 AZ 不可用时，仍然能够从其他 AZ 正常访问数据，适用于对可靠性要求较高的场景。
对象存储 OBS	数据持久性高达 99.9999999999%，标准存储单可用区存储每服务周期服务可用性不低于 99.99%；标准存储三可用区存储每服务周期服务可用性不低于 99.995%。 数据检查：存储前和存储后通过 Hash 校验数据一致性，确保存入数据是上传数据。 分片冗余：数据分片后多份冗余存储在不同磁盘，后台自行检测一致性并及时修复受损数据。
弹性文件服务 SFS	通过业务节点的高可靠性网络和节点的多冗余设计，SFS 的数据持久性可达 99.9999999%，服务可用性达 99.95%。通过 CBR 实现文件存储的备份与恢复。
关系型数据库服务 RDS	RDS 服务采用热备架构，提供自动备份和数据库快照两种备份恢复方法。RDS 自动备份会进行全量数据备份，且每 5 分钟会增量备份事务日志，这就允许租户将数据恢复到最后一次增量备份前任何一秒的状态。 故障系统 1 分钟自动切换。每天自动备份数据，上传到 OBS 桶，备份文件保留 732 天，支持一键式恢复。
镜像服务 IMS	使用多份冗余存储私用镜像，数据持久性高达 99.999999999%。

表5.1 华为云服务可靠性

其次，华为云云服务等级协议（SLA）中也针对云硬盘、数据库、对象存储服务等各产品提供了明

确的服务可用性承诺，若服务可用性未达到承诺的标准，将依据协议对客户做出补偿。

5.2.2 数据隔离

华为云在物理资源层、虚拟机层、网络层以及服务层设计了相应的数据隔离，从底层的物理存储计算资源至顶层的服务资源中，自下而上的实现了数据隔离能力，防止用户数据遭到未经授权访问，全面保障云上数据安全可控。

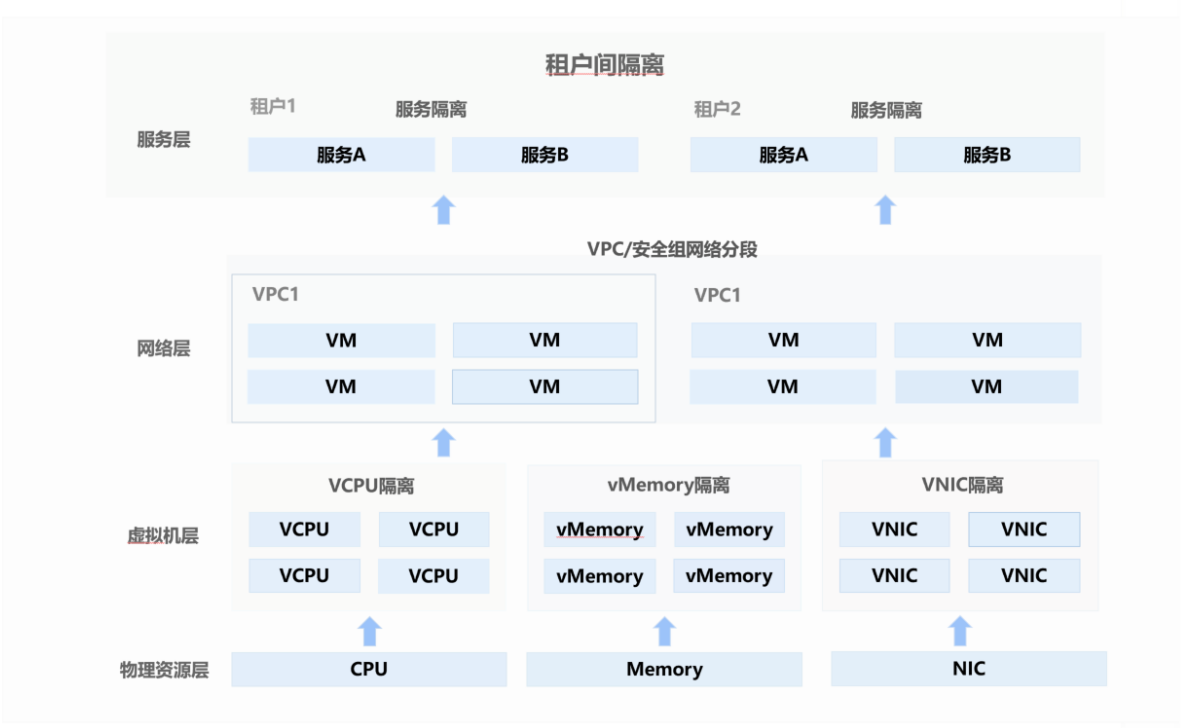

图5.3华为云数据隔离方案

- **虚拟计算资源隔离**

华为云将底层物理计算资源，如CPU、内存、I/O设备等硬件资源，抽象出vCPU、虚拟内存、虚拟I/O设备等虚拟化计算资源。通过虚拟化平台控制虚拟机对虚拟计算资源间的访问，从而使每个虚拟机只能访问自身的计算资源，从而保障数据安全。具体的虚拟计算资源隔离示例如下：

1. **CPU隔离：**CPU 隔离主要是指虚拟化平台与虚拟机之间的隔离，虚拟机内部的权限分配和虚拟机与虚拟机之间的隔离。CPU 隔离是通过Root和Non-Root两种运行模式的切换、各运行模式下的运行权限分配以及以VCPU（Virtual CPU）的形式呈现的虚拟计算资源的分配与切换等方式来实现的。通过CPU隔离机制，UVP可以控制虚拟机对物理设备以及虚拟化运行环境的访问权限，从而实现虚拟化平台与虚拟机之间以及不同虚拟机之间在信息和资源上的隔离，也就是说，一个虚拟机无法获取到其他虚拟机或虚拟化平台的信息和资源。

2. **内存隔离：**虚拟化平台还负责为虚拟机提供内存资源，保证每个虚拟机只能访问到其自身的内存。为实现这个目标，虚拟化平台管理虚拟机内存与真实物理内存之间的映射关系。虚拟机对内存的访问都会经过虚拟化层的地址转换，保证每个虚拟机只能访问到分配给它的物理

内存，无法访问属于其他虚拟机或虚拟化平台自身使用的内存。

3. **I/O隔离：**虚拟化平台还给虚拟机提供了虚拟I/O 设备，包括磁盘、网卡、鼠标、键盘等。虚拟化平台为每个虚拟机提供独立的设备，避免多个虚拟机共享设备造成的信息泄露。每个虚拟磁盘对应虚拟化平台上的一个镜像文件或逻辑卷，虚拟化平台控制只有一个虚拟机的一个虚拟磁盘设备跟一个镜像文件关联。实现了虚拟机使用的虚拟设备与虚拟化平台I/O 管理对象之间一一对应的关系，保证虚拟机之间无法相互访问I/O设备，实现I/O路径的隔离。

- **网络隔离**

华为云对云端数据的隔离是通过虚拟私有云（VPC – Virtual Private Cloud）实施的，VPC 采用网络隔离技术，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置：一方面，结合VPN或云专线，将VPC与租户的传统数据中心互联，实现租户应用和数据从租户内网向云上的平滑迁移；另一方面，利用VPC 的ACL、安全组功能，满足租户更细粒度的网络隔离需要。

VPC可为客户构建出私有网络环境。客户可以划分“DMZ”、“业务应用”、“业务数据”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。

- **服务隔离**

不同VPC之间在默认条件下无法相互通信，从而实现客户间数据隔离，大大降低了不同租户间的数据泄露风险。另外，客户可以自由配置VPC内的子网、安全组等网络隔离策略，通过将不同的存储与数据库服务实例，如OBS实例、RDS实例，部署至不同安全组内，可以实现VPC内的存储资源隔离，降低存储服务间随意相互通信所导致的数据泄露风险。

5.2.3 存储加密

华为云参考业界加密算法优秀实践，制定并实施了密码算法应用规范，对加密级别、加密方法进行了明确规定。华为云根据规范，使用了 AES 强加密算法针对存储在云基础设施中的静态数据执行数据加密，有效保护云平台中的数据安全。同时，在密钥管理方面，华为云制定并实施了密钥管理安全规范，明确密钥管理各阶段的安全管理要求，对密钥生成、传输、使用、存储、更新、销毁等全生命周期的安全性进行管控。

5.2.4 数据安全销毁

在平台层面，在客户数据的销毁阶段，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、对象存储、文件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。

在物理介质销毁层面，为保证数据中心介质生命周期末期数据安全，华为云参照相关行业标准，实施了完善的存储介质处置机制。如参考NIST SP 800-88标准对存储介质进行处理，针对需要重复使用

的存储介质，进行随机数覆写、加密擦除等方式进行数据安全删除，针对不需要重复使用的存储介质则采取消磁、物理损毁等方式进行物理销毁。

5.2.5 访问管控

华为云执行规范化、标准化访问管控，授权运维人员实行基于角色的访问控制和严格的职责分离（SoD）管理，在未获得客户的授权前无法访问客户的数据

通过双因子认证后集中从堡垒机跳转到目标机进行操作，操作结束后目标机的口令将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。

同时，华为云还建立了集中、完善的日志审计系统，所有内部人员运维操作均将被系统采集并记录。华为云会例行对运维流程各项活动进行监控和审计，对异常操作也会及时告警、阻断，对于违规操作的人员会按相关处罚规定进行处罚。

5.3 传输中的数据安全

5.3.1 传输加密

对于华为云平台服务端到客户端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供：

- **虚拟专用网络（VPN）**

VPN用于在远端网络和VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为租户提供端到端的数据传输机密性保障。通过VPN在传统数据中心与VPC 之间建立通信隧道，租户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的Web 服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。

目前，华为云采用硬件实现的IKE（密钥交换协议）和IPSec VPN 结合的方法对数据传输通道进行加密，确保传输安全。

- **应用层 TLS 与云证书管理服务（CCM）**

华为云服务提供REST 和Highway 方式进行数据传输，这两种数据传输方式均支持使用传输层安全协议较新版本进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。

CCM是一个云上海量证书颁发和全生命周期管理的服务，提供SSL证书管理和私有证书管理服务。CCM 提供支持主流RSA与ECC算法的“国际证书”，还提供支持中国商用密码SM2及相关标准算法的“国密证书”。多年期SSL证书支持每年自动化更新替换周边云服务中的老SSL证书，降低过去手动更新证书带来的人力和时间成本。CCM提供丰富的API接口，满足业务多样化需求，为企业租户提供了巨大的灵活性。CCM通过密钥管理服务（KMS）和硬件安全模块（HSM）提供安全保护，可以稳定可靠保存密钥。

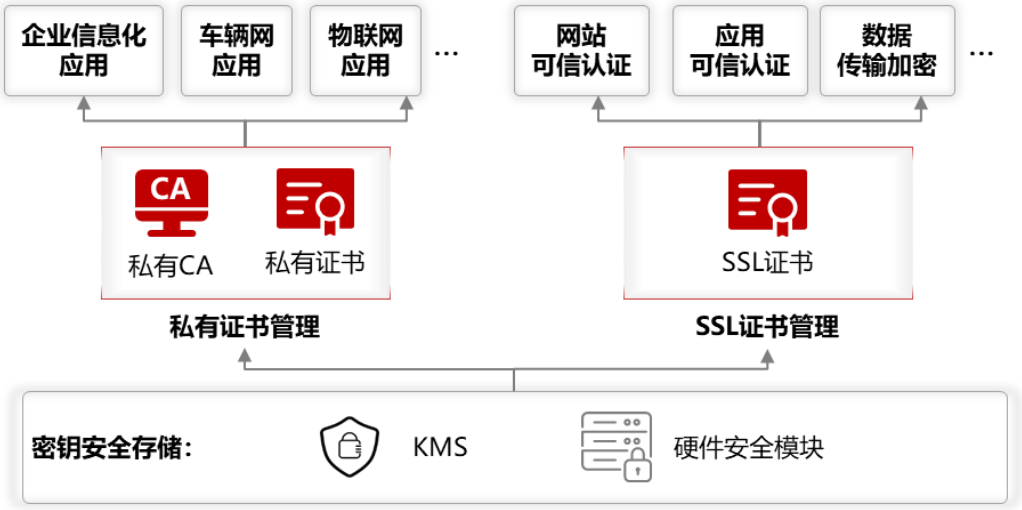

图 4.4 CCM 服务架构

CCM 的核心功能点包括：

1. 证书生命周期管理：支持公有 SSL 证书和私有证书的申请、签发、查询、吊销等，具备千万级以上的证书管理能力；

2. 私有 CA 托管能力：用户无需构建和维护复杂的 CA 基础设施，在华为云上按需付费即可轻松获得 CA 管理能力；

3. 周边服务对接：支持一键部署证书至主流云产品，到期自动更新替换；

5.3.2 传输稳定可靠

除了保障客户云上数据传输过程中的安全，华为云也致力于为客户提供高性能、高可靠、低延迟的网络传输服务。华为云为客户通过运营商专线接入云上虚拟私有云提供了多链路容灾能力。客户数据中心可通过不同运营商专线，分别接入不同接入点，实现多链路多接入点互备。当用户通过单一运营商专线无法成功访问资源时，多链路容灾技术则自动将流量切换至其他运营商专线，从而实现故障转移，保障访问的高可靠性。

- 云专线（Direct Connect）

云专线用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。云专线专用通道高安全，为业务安全保驾护航。云专线使用专属私密通道接入华为云VPC，网络隔离，安全性极高。

服务资源

- 虚拟专用网络 VPN
- 云证书管理服务 CCM
- 云专线 DC

5.4 使用中的数据安全

5.4.1 机密计算

为了保证客户云上数据处理过程安全可信，华为云结合可信设计原则与云平台基础架构特性，设计研发了华为云擎天机密计算平台，为客户提供所需的具有高安全、强隔离、高性能和低成本的ECS实例。其安全概念模型如下图所示：

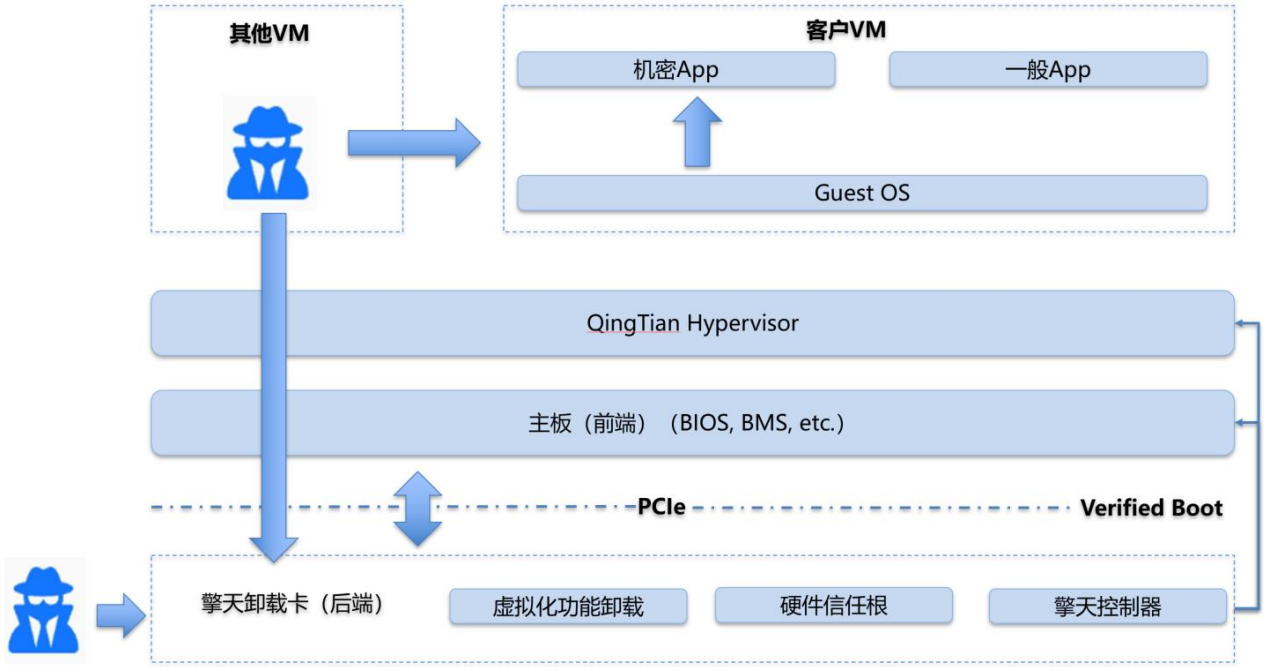

图4.5 擎天安全概念模型

在擎天虚拟化设计之初就希望做到为客户提供显著增强的安全控制和隐私保护能力，所以在机密性和完整性保护设计方面，擎天虚拟化平台基于“被动连接设计”、“单向访问控制”、“最小化攻击面”、“前后端硬隔离”、“硬件身份证明与信任”、“硬件密钥保护及端到端加解密”、“强制安全启动与完整性验证”等设计原则来构建最小的可信计算基（TCB, Trusted Computing Base），在两个维度上提供安全隔离保护。

隔离维度一：“客户的应用代码和数据”与“云厂商的运维人员和云系统软件”隔离

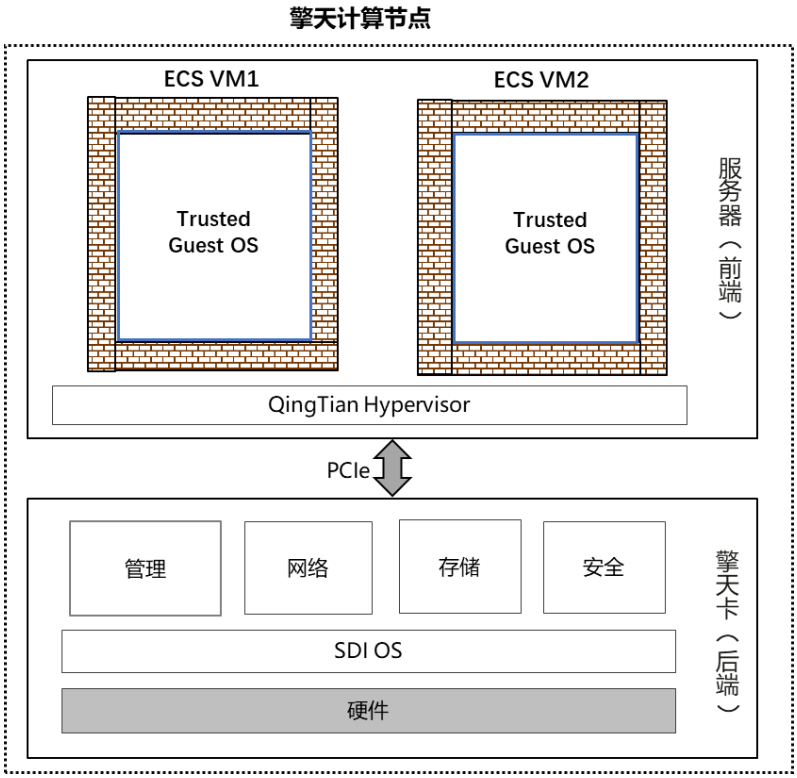

图4.6 客户的应用代码和数据”与“云厂商的运维人员和云系统软件”隔离

- **无运维人员访问：**为了确保客户实例之间以及客户实例与云基础设施之间的强隔离，QingTian Hypervisor 不提供任何可用于远程登录的机制，可消减 memory dumping 之类的攻击。云内部运维人员通常只能使用运维 API 来进行远程诊断，无法登录到前端 Hypervisor，无法访问前端服务器上客户实例内存数据。
- **防逃逸：**擎天系统是一种前后端分离式 VMM 架构，前端和后端系统是基于 PCIe 总线的物理隔离。华为云基于最小 TCB 设计原则，前端 Hypervisor 是极简设计，无网络协议栈，无本地存储，无 SSH 管理工具等。前端 Hypervisor 基于硬件虚拟化来创建和隔离客户实例，后端 SDI 卡设备使用 SR-IOV 直通访问 VM 实例（无管理软件介入）。相比传统虚拟化管理系统，QingTian Hypervisor 代码量不足 1%，这意味着擎天系统中软件安全风险会显著降低。
- **系统层防篡改：**华为云在擎天系统中使用强制的安全启动，后端 SDI 卡首先执行安全启动，而后再检查系统固件和前端 Hypervisor 镜像签名的完整性，验证通过后拉起前端 Hypervisor。对于客户侧 ECS VM，华为云支持客户在创建 VM 时使能 UEFI Secure Boot 标准安全启动，以及使能擎天 vTPM（遵循 TPM 2.0 技术规范）来实现依赖 TPM 标准的可信启动和远程证明功能。
- **防物理攻击：**华为云在擎天卡上使能 Volume 加密和 VPC 加密，使用硬件保护密钥，数据密钥使用权限由客户完全控制，数据离开/进入计算节点会由擎天卡实施加密/解密。

在此隔离维度中，华为云还基于擎天卡提供了租户独享的 BMS 裸机实例。对于裸机实例，服务器上没有运行 QingTian Hypervisor，客户可以完全独占访问底层主板系统并使用相关的硬件特性（例如 Intel VT，ARM TrustZone），以满足客户的强隔离需求。

隔离维度二：将“客户的应用代码和数据”与“客户自己的运维人员和低可信软件”隔离

在隔离维度一的安全设计基础之上，华为云在提供给客户的ECS虚拟机实例中进一步提供了QingTian Enclave来满足“客户的应用代码和数据”与“客户自己的运维人员和低可信软件”的隔离。

QingTian Enclave 是从客户ECS 实例内启动的一个隔离运行环境，它通过唯一的vsock安全通道连接到该实例。QingTian Encalve与ECS实例之间是基于硬件虚拟化实现的隔离。QingTian Enclave不仅继承与ECS实例相同的安全保护能力，而且采用如下方法将其设计为一个高强隔离的计算环境：

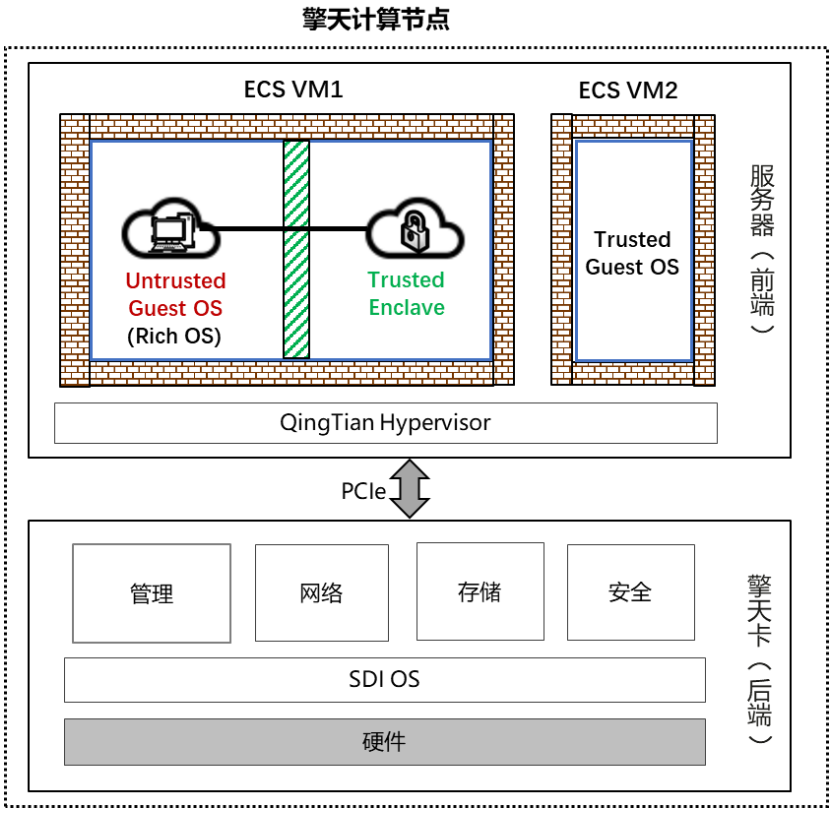

图4.7 将“客户的应用代码和数据”与“客户自己的运维人员和低可信软件”隔离

- **Enclave最小信任基：**普通客户实例通常有较大的TCB（如Rich OS），这往往导致较大的安全攻击面。QingTian Enclave方法并不是要消减Rich OS的攻击面，而是要彻底将Rich OS划分在QingTian Enclave的信任边界之外。所以针对Rich OS的安全威胁并不会影响Enclave环境中的应用和数据。为了消减Enclave环境的攻击面， QingTian Enclave不支持IP 网络访问，不提供持久化存储，也不支持SSH交互式访问等机制。

- **防客户自己的不可信系统软件：**QingTian Enclave与客户ECS主实例之间是基于硬件虚拟化实现的隔离，Enclave与客户实例之间没有共享的物理内存和CPU Core，仅有受Hypervisor保护的唯一vsock通道将Enclave连接到主实例。运行在主实例上的所有软件系统都无法访问Enclave环境中的代码和数据。

- **防客户自己的不可信运维人员：**由于华为云将客户主实例（如Rich OS）划分在QingTian Enclave的信任边界之外，那么登录到主实例上的运维人员（包括root或管理员用户）无法访问Enclave环境中的代码和数据。

- **Enclave完整性保护与证明：**在启动QingTian Enclave时，QingTian Hypervisor会验证Enclave镜像的数字签名，并度量Enclave镜像文件和数字签名公钥证书，度量结果会保存到QTSM（QingTian Security Module），QTSM是面向云场景提供的专有的管理可信度量结果的安全模块。

- **高易用性/兼容性：**华为云将QingTian Enclave设计为一个对开发者友好的平台，开发者无需具备CPU微架构专业知识和高级密码学知识就能轻松开发QingTian Enclave应用。当前QingTian Enclave已支持X86和ARM架构，开发者可以使用任何熟悉的开发语言框架，并支持基于容器镜像直接构建QingTian Enclave镜像。

- **云服务集成：**擎天系统支持对QingTian Enclave身份和可信度量结果的密码学证明，Enclave应用通过Attestation协议来证明其Enclave身份并与外部服务建立信任。华为云KMS、IAM服务内置了对QingTian Enclave Attestation的支持。Enclave应用开发者可以使用开源Enclave SDK访问KMS API来获取数据加解密密钥或安全随机数并保证端到端的安全。客户管理员可以通过预设的IAM授权策略或护栏策略来对KMS API施加基于Attestation的条件访问控制。

QingTian Enclave使能客户在ECS VM环境中创建出一个强化且高度隔离的计算环境，它新增了使能客户将自己的系统组件划分为具有不同信任级别的功能。这一安全特性自上线以来已获得诸多云上客户的青睐。客户基于QingTian Enclave开发的典型安全应用包括虚拟加密机vHSM、凭证管理箱、Web3数字钱包、机密AI应用、安全多方计算、安全密钥协商与端到端加密等。华为云也在持续构建丰富的QingTian Enclave开源工具（eg, qproxy）和安全解决方案（例如 Confidential Container），帮助更多客户实现应用代码和构建系统零改造的部署迁移。

5.4.2 同态加密

针对客户云上敏感数据的处理场景，华为云平台能够基于同态加密技术（Homomorphic Encryption, HE）对敏感数据实现加密计算，在对数据进行处理的同时确保数据原始内容无法被任何人访问，实现敏感数据“可用不可得”。客户可对敏感数据进行加密，将加密后的数据上传至云中处理，处理完成后客户利用密钥对计算结果进行解密即可获取计算结果。在敏感数据处理场景下，同态加密技术赋予华为云对密文的计算能力，密文计算无须由密钥方解密，提高数据的安全性的同时降低通信代价。

5.4.3 多方计算

华为云平台基于多方计算MPC（Multi-Party Computation），在保护客户重要数据与隐私数据安全的前提下，可对行业内、各行业间的多方数据进行联合计算和分析，在分布式的、无法互相信任的多个参与方之间建立互信联盟，实现跨组织、跨行业的多方数据分析和联合学习建模能力。多方计算技术MPC在保证了华为云客户原始数据机密性的同时，通过多方联合分析建模，促进多方数据融合分析，更大程度的释放数据利用价值。

6 提供全栈安全服务，使能客户云上数据自主可控

6.1 数据驻留位置

华为云持续加大全球数据中心和加速网络的布局，云网协同，联接人，联接物，联接应用，提供一致体验的全球一张网，让信息流高速分发处理，让业务快速全球触达。当前基础设施建设布局全球，覆盖170余个国家、地区，在30多个区域(自营+合营） 运营近百个可用区，涉及亚太、拉美、非洲、欧洲、中东等地域。目前已经上线220多个云服务，210多个解决方案，满足各类用户的业务。

得益于华为云在全球范围内构建了广泛的基础设施网络，使得企业能够根据自身业务需求灵活地选择最合适的地理位置来部署应用和服务。通过访问华为云官方网站，客户可以全面了解到华为云在全球各地的数据中心布局情况，包括各个数据中心的位置、规模、技术规格以及所提供的服务水平协议（SLA）。这样的透明度不仅增强了客户对数据存储地点的信任感，同时也为企业提供了必要的信息，以便他们可以根据自己的业务扩展策略、法律法规要求以及性能优化需要来做出明智的决策。

通过查阅这些信息，客户可以清晰地了解到哪些服务是在特定区域内可用的，哪些服务则可能需要跨区域使用。这对于那些有特定合规性要求的企业尤其重要，比如某些行业规定数据必须存储在特定国家、地区内。此外，对于追求高性能和低延迟的应用来说，选择靠近用户群的数据中心也至关重要。因此，华为云提供的这种详细的信息帮助客户更好地规划其IT架构，确保既符合业务目标又能满足技术需求。

6.2 全生命周期可控

华为云以数据为中心，围绕数据全生命周期，构建全栈的数据安全服务，关键数据实施纵深防御，通过全栈加密、密钥客户自持、远程运维客户授权等，支撑用户实现数据安全的自主可控。

6.2.1 自主控制数据采集

6.2.1.1 数据采集

针对应用层客户可以通过云日志服务（LTS）采集来自主机和云服务的日志数据, 采集到的日志数据在云日志控制台以清晰有序的方式展示。华为云在审计层面提供给客户云审计服务（CTS）、云堡垒机服务（CBH），能够采集客户在云上环境的所有操作及变更，可用于支撑安全分析、合规审计、资

源跟踪和问题定位等。

6.2.1.2 数据识别与分类分级

- **数据安全中心（DSC）**

客户可以通过使用华为云的数据安全中心（DSC）服务，自主可控地对数据进行分类分级。该服务内置并支持自定义敏感数据扫描规则，识别定位到敏感信息，对其分类分级。在开展数据分类分级时，客户可根据自身业务需求，自定义敏感数据类别、敏感数据识别规则及敏感数据等级，在此基础上实现敏感数据自动识别以及数据自动分类分级。

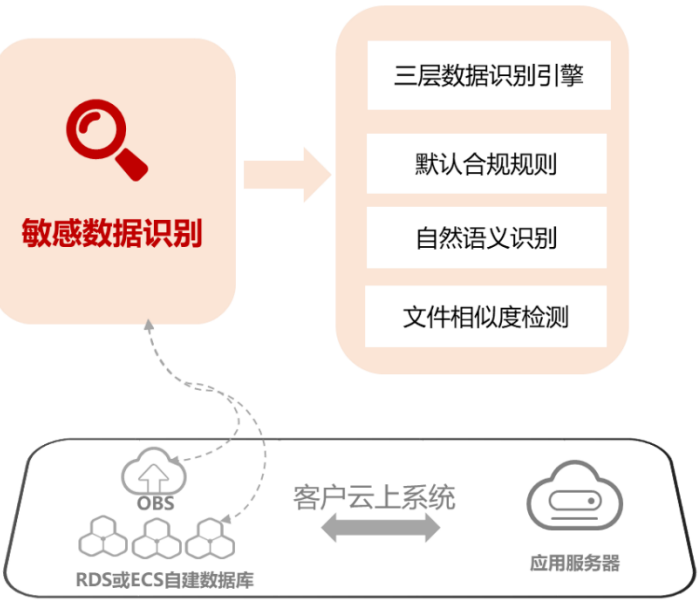

图 6.1 DSC 敏感数据识别

DSC 可以帮助客户从亿万级文件中发现隐私数据、从 TB 级数据中快速识别敏感字段。DSC 通过构建自动化三层数据识别引擎，在数据生成的时候就能呈现整体风险。DSC 支持 200 种数据格式，支持结构化数据和非结构化数据，真正做到场景全覆盖。

服务资源

- **云日志服务（LTS）**
- **云审计服务（CTS）**
- **云堡垒机服务（CBH）**
- **数据安全中心（DSC）**

6.2.2 自主控制数据传输

数据传输是指数据通过网络从数据源传输到数据终端。华为云通过云服务与自身上云实践能够帮助客户实现：数据迁移自主控制、数据传输自主控制、传输加密自主控制。

6.2.2.1 数据迁移自主控制

华为云基于自身上云的成功实践和海量客户迁移服务的经验，总结出一套“7阶12步”的上云迁移方法论，端到端覆盖数据迁入和迁出的各个场景与环节。为了确保客户的业务上云过程中的数据安全，华为云的上云迁移服务提供了各种安全工具、专业服务和解决方案，协助客户安全上云，并保障云上业务的持续安全。在迁移过程中，可以使用迁移中心 （MgC）迁移应用程序和数据并实现现代化，以优化成本并推动创新。

6.2.2.2 数据传输自主控制

华为云提供部分服务以帮助客户在云环境中实现数据传输的能力。如客户的业务发生变化，客户可以通过停止使用此类服务或选择其他传输类服务来控制数据的传输，例如消息通知服务（SMN）、分布式消息服务（DMS）、云数据迁移服务（CDM）等。华为云会在客户使用相关服务进行数据传输时，提供必要的安全能力帮助客户增强数据传输的安全性。

6.2.2.3 传输加密自主控制

华为云针对应用层、传输层、物理层等多种业务场景，提供了SSL证书管理服务（SCM）、虚拟专用网络（VPN）、云专线服务（DC）、云连接服务（CC）以及数据快递服务（DES）等多种传输加密解决方案。客户可以根据不用业务场景，选择适用于自身的传输加密机制，保障数据的安全传输。

针对这一阶段，华为云建议客户对传输中的数据进行加密，确保数据在传输过程中的安全性。

图6.2 华为云数据传输安全能力

- **SSL 证书管理服务（SCM）**

当客户通过互联网提供Web 服务时，可选择使用华为云提供的证书管理服务。华为云证书管理服务SCM联合全球知名证书服务商，可提供DigiCert、GlobalSign、GeoTrust以及CFCA国密证书（仅限中国站），客户通过给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数据传输。

- **虚拟专用网络（VPN）**

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、云连接等服务，实现不同区域之间业务的互联互通和安全数据传输。目前VPN 服务采用华为公

司专业设备，基于IKE和IPsec协议在Internet中实现虚拟私有网络，在本地数据中心和华为云VPC之间、华为云不同区域的VPC之间构建稳定可靠的加密传输通道。

- **云专线服务（DC）**

云专线服务（DC）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（CC）**

云连接服务（CC）是基于华为公司多年全球IT 运营经验，利用全球众多国家、地区的网络资源布局，打造的一站式云连接网络服务。云连接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。

- **数据快递服务（DES）**

数据快递服务（DES）是华为云提供的一种海量数据传输解决方案。用户可利用Teleport高性能存储设备或硬盘等，以物理手段将数据安全传输至华为云。Teleport设备自带基于AES256的加密功能，自动保持全盘加密状态，并由用户自行管理密钥。所有数据将在加密状态下进行传输，充分保障数据在传输过程中的安全。

服务资源

- **SSL 证书管理服务（SCM）**
- **虚拟专用网络（VPN）**
- **云专线服务（DC）**
- **云连接服务（CC）**
- **数据快递服务（DES）**
- **迁移中心 （MgC）**

6.2.3 自主控制数据跨境

客户在使用华为云服务时，可能基于业务目的需要将云上数据进行跨境传输。此时，客户需要考虑适用的法律法规要求，如欧盟《通用数据保护条例》（简称GDPR）、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《数据出境安全评估办法》、《促进和规范数据跨境流动规定》等，相关法律可能对特定类型的数据跨境提出具体的合规要求，客户需要对相关要求进行识别和管理。

华为云通过“法律洞察”、“梳理数据跨境场景”、“跨境风险评估”、“实施跨境合规举措”以及“定期评估审视”等措施保障数据跨境安全合规转移。华为云在全球开服国家均考虑了适用国家、区域对于数据跨境的法律法规要求，详情见信任中心。

- 中国

对于中国跨国企业或出海企业，涉及重要数据出境的，应依照中国相关法律法规开展数据出境安全评估申报；个人信息出境应基于数据出境的类型、规模等因素，按相关监管要求申报数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证。

同时应当确认境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全，避免数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险。

- 欧盟

对于欧盟数据跨境场景，企业可以进行数据保护影响评估（DPIA），以确保数据传输不会对数据主体的隐私和安全造成风险。同时通过签署标准合同条款（SCCs）或使用欧盟委员会认可的其他保护措施来实现个人数据跨境转移的合规性。

6.2.4 自主控制数据存储

华为云为客户提供多种功能与服务，包括：数据中心的区域查询、Region级和Global级服务的数据存储、数据存储安全保护、数据隔离、容灾备份等，帮助客户实现数据存储阶段安全的自主可控，具体如下：

6.2.4.1 数据中心的区域查询

客户可以选择在其中任何一个区域部署自己的数据。使用华为云时，客户可以借助华为云服务和工具来控制数据，决定数据的存储位置、保护方式以及访问权限。例如，客户可以利用数据中心的区域查询页面，来帮助查看是否满足数据驻留要求。

6.2.4.2 Region 级和 Global 级服务的数据存储

华为云服务的部署分为Region级和Global级，客户可以利用Region级和Global级服务的数据存储页面，来帮助客户了解有关客户数据位置的详细信息。

6.2.4.3 数据存储安全保护

华为云提供先进的数据加密技术，客户可以根据自己的安全需求和合规要求，选择不同的加密算法和密钥管理策略。华为云的数据加密服务（DEW）、对象存储服务（OBS）、弹性文件服务（SFS）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。

- **数据加密服务（DEW）**

数据加密服务是一款综合的云上数据加密服务，DEW包含DHSM、KMS、CSMS三个子服务，提供了专属加密、密钥管理、密钥对管理等功能，旨在为用户提供便捷、可靠、高效的数据加密能力。与此同时，DEW还拥有与其他云服务的广泛集成能力，并可通过为用户提供密钥全托管、密钥半托管、密钥客户全控制三种不同级别的密钥托管服务，助力用户实现密钥管理自主可控。用户甚至可以借此服务开发自己的加密应用，实施更灵活的数据安全控制。

整体来看，华为云数据加密服务（DEW）具备以下优势：

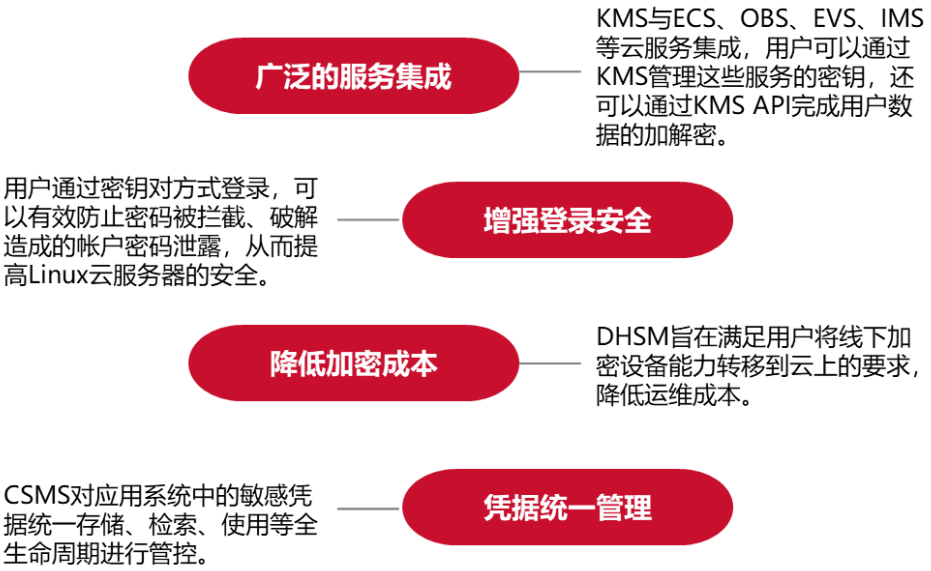

图6.3 DEW核心优势

- **专属加密（Dedicated HSM）**

专属加密服务（Dedicated HSM）是云平台基于云服务器密码机构建虚拟化密码资源池，实现IT、密码资源统一调度管控，为租户按需提供虚拟密码机的服务。解决了加密机入云、密码及IT资源统一调度、自动化管维的问题。DHSM提供经权威机构检测认证的加密硬件，支持SM1、SM2、SM3、SM4等密钥算法（仅限中国站），可处理加解密、签名、验签、产生密钥和密钥安全存储等操作，帮助用户保护弹性云服务器上数据的安全性和完整性，并满足监管合规要求。同时，租户能够对专属加密实例生成的密钥进行管理，也能使用多种加密算法来对数据进行加解密运算。DHSM提供满足FIPS 140-2 level3的硬件加密模块。

DHSM经过第三方机构认证，硬件密码算力保证不同加密协议下并发高速运算，对称算法支持SM1,SM4，非对称算法支持SM2，哈希算法支持SM3。

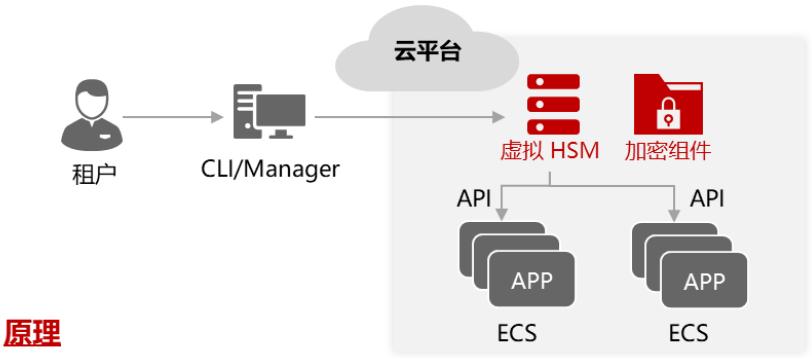

图 6.4 DHSM 服务架构

专属加密支持的密钥算法类型如下：

密钥类型	算法类型
对称密钥	AES
	3DES
	DES
	SM1
	SM4
非对称密钥	RSA_1024
	RSA_2048
	SM2
摘要算法	SM3
	SHA1
	SHA256
	SHA384

表6.1 专属加密支持的算法类型

专属加密的核心功能点包括：

1. 密码、IT资源统一管控：支持云平台对密码虚拟化资源池自动化统一管控调度，与IT资源协同
2. 动态弹性扩展：支持快速调整，支持复制、漂移，自动化运维
3. 数据加密：同时支持国际与国产加密算法，覆盖对称与非对称加密

- **密钥管理（KMS）**

提供安全、可靠、简单易用的密钥托管服务。KMS通过使用硬件安全模块（HSM）保护密钥安全，帮助用户创建和管理密钥，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。KMS服务与诸多云原生服务对接，提供云原生服务加密能力。支持OBS、EVS、IMS、SFS、RDS、DDS、DWS等存储类云服务加密。

KMS支持的密钥算法类型如下：

密钥类型	**算法类型**	**密钥规格**
对称密钥	AES	AES_256
	SM4	SM4
非对称密钥	RSA	RSA_2048 RSA_3072 RSA_4096
	ECC	EC_P256

密钥类型	算法类型	密钥规格
		EC_P384
	SM2	SM2

表6.2 KMS支持的算法类型

- **密钥对管理（KPS）**

提供安全、可靠、简单易用的SSH密钥对托管服务，帮助用户集中管理SSH密钥对，保护SSH密钥对的安全性。KPS利用HSM产生的硬件真随机数来生成密钥对，并提供完善可靠的密钥对的管理方案，帮助用户创建、导入和管理SSH密钥对。

- **凭据管理（CSMS）**

提供安全、可靠、简单易用的凭据托管服务。用户或应用程序通过凭据管理服务创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险，充分实现密钥管理自主可控。目前已与RDS和CCE对接，为客户安全地管理RDS和CCE Secret凭据。

CSMS 覆盖人机、机机场景，ECS、RDS、自建应用均可适用。所有的凭据管控都提供API，可以方便的集成进现有系统。单API调用性能超过500TPS，满足各种场景需求。

CSMS的核心功能点包括：

1. 凭据加密保护：通过KMS对凭据进行加密存储，加密密钥基于第三方认证的硬件安全模块（HSM）来生成和保护

2. 凭据安全检索：将应用程序代码中的硬编码凭据替换为对凭据的API调用，以便以编程方式动态检索和管理凭据，实现凭据安全管理。

3. 凭据集中管控：与IAM集成，通过身份、权限管理确保只有授权用户可以检索或修改凭据，与CTS集成，持续监控对凭据的操作访问。有效防范对敏感信息的非法访问和泄漏。

- **云硬盘备份（VBS）**

云硬盘备份（Volume Backup Service）为单个或多个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。备份数据加密，跨数据中心保存。

- **云服务器备份（CSBS）**

云服务器备份（Cloud Server Backup Service）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。备份数据通过多副本存储在多个数据中心，用于抵御数据中心级别的故障。

- **存储容灾服务（SDRS）**

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。

1.

服务资源

- **数据加密服务（DEW）**
- **云硬盘备份（CBS）**
- **云硬盘备份（VBS）**
- **云服务器备份（CSBS）**
- **存储容灾服务（SDRS）**
- **虚拟私有云服务（VPC）**

6.2.5 自主控制数据共享

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。在该阶段，客户可使用数据脱敏、数据水印以及安全多方计算相关的服务，保障数据 共享过程中的安全性。

6.2.5.1 数据脱敏

DSC 的数据脱敏支持静态脱敏和动态脱敏。用户可以对指定数据配置脱敏规则，实现 敏感数据静态脱敏，同时，也可以使用数据动态脱敏的 API 接口实现数据的动态脱敏，全方位确保敏感信息不被泄露。在数据共享环节，客户可针对不同类型的敏感数 据，使用不同的脱敏方式对敏感数据进行脱敏。例如，针对个人敏感数据，可使用字符掩盖方式进行脱敏，针对企业敏感或设备敏感数据，可使用关键字替代方式进行脱敏。

6.2.5.2 数字水印

数据安全中心提供数字水印能力，可针对文档、图片、JSON 数据嵌入或提取水印。数字水印广泛适用于政府部门、医疗、金融、科研等单位机构，一般用于版权保护、追 踪溯源。

1. 数据版权保护：对于需要将重要文档、图片等类型数据提供给第三方的场景，可对相关数据嵌入水印，在发生版权纠纷时可以通过数字水印明确版权所属。

2. 追踪溯源：数据共享给给内部第三方使用时，打上使用者信息水印，可识别使用者身份，提醒使用者遵守安全规范。当发生数据泄露事件时，数字水印可协助组 织追踪数据泄露源头，挖掘泄露原因。

6.2.5.3 可信计算

- **可信智能计算服务（TICS）**

可信智能计算服务 TICS 将帮助组织打破数据孤岛，在数据隐私保护的前提下，实现行 业内部、各行业间的多方数据联合分析和联邦计算。TICS 对接多种主流数据存储系 统，为数据消费者实现多

方数据的融合分析，参与方敏感数据能够在聚合计算节点中实现安全计算。多方分析利用 JOIN 算子进行数据隐私保护，将多方数据加密后完成计 算，计算结果加密返回给数据使用方，保障数据共享过程中的安全。

服务资源

- **数据安全中心（DSC）**
- **可信智能计算服务（TICS）**

6.2.6 自主控制数据使用

6.2.6.1 访问控制

在任何必要情况下，华为云如需访问客户的云上数据，华为云坚持先获得客户的明确同意。客户也可以使用华为云的统一身份认证服务（IAM）、云堡垒机服务（CBH）等针对应用访问、运维操作、云上资源访问等不同业务场景自行设置访问控制策略，防止其他未授权的访问。

- **统一身份认证服务（IAM）**

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；具备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；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。

- **云堡垒机服务（CBH）**

系统的运维人员通常权限较高，更易访问底层数据，在出现恶意操作或误操作时会对系统造成更大的损害。因此，华为云建议客户使用云堡垒机服务（CBH）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，支持开启多因素认证、国密配置（仅限中国站），保障远程登录安全，协助客户做好运维控制与合规审计。

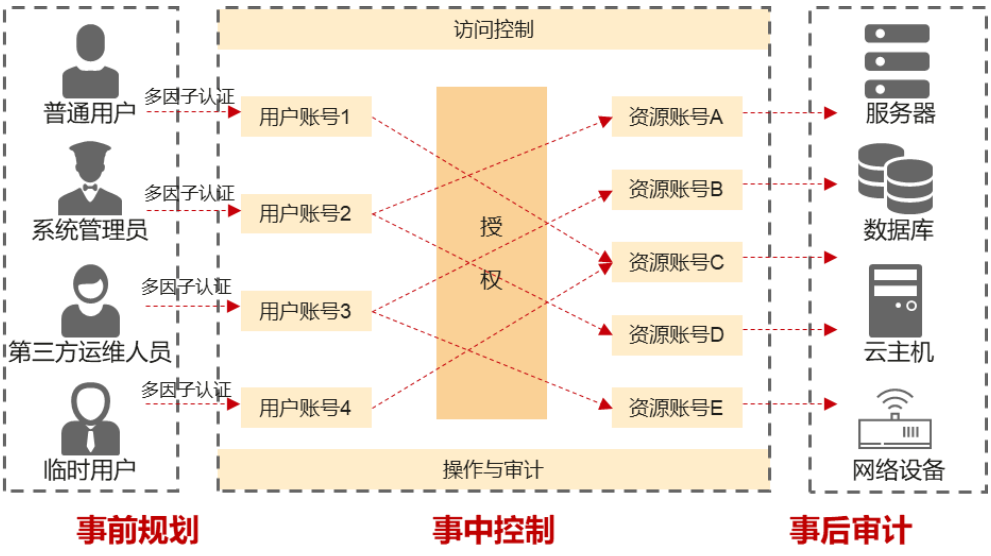

图6.6 CBH的服务架构

CBH核心功能点包括：

1. 用户管理：用户管理、角色管理、多因子认证、访问策略

2. 资源管理：密码托管、改密策略、运维授权、应用发布

3. 访问控制：单点登录、命令拦截、二次授权、工单管理

4. 操作审计：实时监控、操作回放、命令审计、报表分析

6.2.6.2 数据脱敏与数据防泄漏

- **数据库安全审计（Database Security Service）**

提供数据库安全审计功能，使用旁路模式审计功能，对数据库性能消耗极低。通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。同时，数据库安全审计可以生成满足数据安全标准（例如Sarbanes-Oxley）的合规报告，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。

旁路部署技术，无运维风险 ，操作简单，快速上手。RDS数据库免Agent审计模式，无需安装agent；从数据源端开启全量审计；支持审计SSL加密连接。完整的SQL解析、精确的协议分析。支持国产数据库。满足等保三级数据库审计需求，满足网安法，SOX等国内外法案。

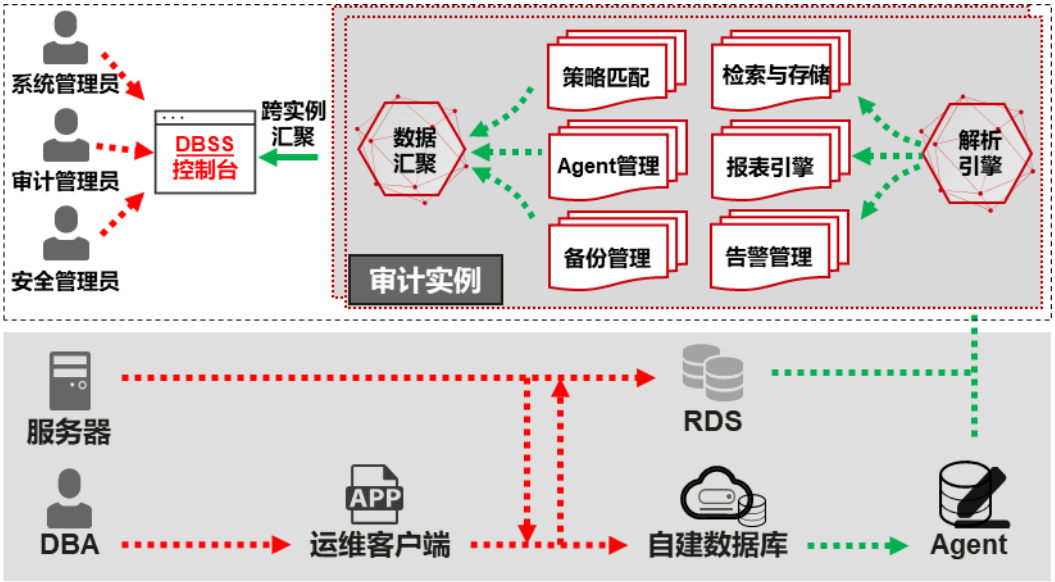

图6.7 DBSS能力概况

DBSS核心功能点包括：

1.细粒度行为审计：关联应用层和数据库层的访问操作，详实记录数据库访问行为

2.安全风险告警：勒索监测、SQL注入操作、风险操作监测、发现风险立即告警

3.多维度分析：行为线索、会话线索、语句线索

4.精细化报表：会话行为报表、风险分布情况报表、合规报表

- **数据库安全加密（Database Security Encryption）**

数据库安全加密服务支持动态加密存储，支持多种加密算法，对敏感数据进行加解密，满足等保、密评等评测要求。同时，提供独立于数据库的访问授权机制，有效防止越权访问及黑客拖库行为，保障数据库使用合规安全。

数据安全加密服务解决数据库密码泄露、APT攻击或内部管理失当导致的数据泄露问题。插件、免改造方案，适合新旧应用零改造上线。加密后的模糊查询正常执行，无需业务适配。通过密文索引加速技术，1000万量级数据表的密文列随机查询时间由21.7s 提速到 6ms。

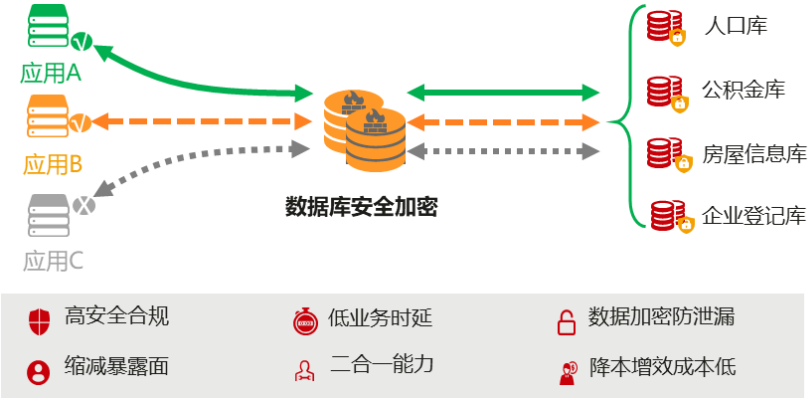

图6.8 DBSS能力概况

核心功能点包括：

1. 敏感数据识别：基于特征库自动扫描敏感数据，内置丰富敏感数据特征库
2. 敏感数据加密：支持多种加密算法，保证数据机密性
3. 细粒度访问授权：访问独立、三权分立、权限分离
4. 操作审计：敏感操作审计、生成操作日志、事件可追溯

- **数据安全中心（DSC）**

DSC的数据脱敏支持静态脱敏和动态脱敏。客户可以对指定数据配置脱敏规则实现敏感数据静态脱敏，也可以使用数据动态脱敏的API接口实现数据的动态脱敏，全方位确保敏感信息不被泄露。在数据使用环节，客户可针对不同类型的敏感数据，使用不同的脱敏方式进行脱敏，敏感数据保护服务中已预置多种字符脱敏模板。例如，针对个人敏感数据，可使用字符掩盖进行脱敏，针对日期或数字特定参数可使用脱敏方式进行取整运算。

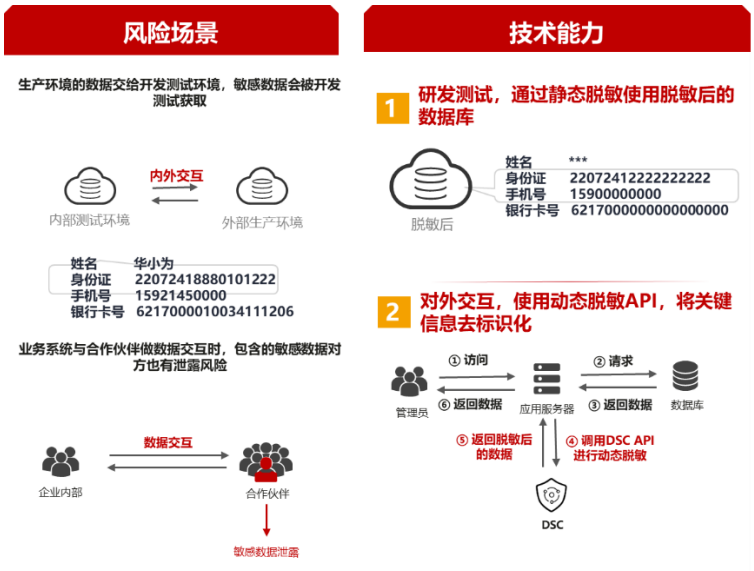

图6.9 DSC数据脱敏

6.2.6.3 可信计算

- **可信智能计算服务（TICS）**

华为云可信智能计算服务（TICS）面向政企行业，打破跨机构的数据孤岛，在数据隐私保护下实现多方数据联合分析和联邦学习。基于可信执行环境TEE、安全多方计算MPC、联邦学习、区块链等技术，实现数据在流通、计算过程中全链路的安全保护和审计回溯，推动跨机构数据的可信融合和协同，释放数据价值。其中，在数据使用过程中可以提供以下安全机制：

1. 可信计算节点：参与方使用数据源计算节点进行自主可控的数据源注册、隐私策略（脱敏、加密）设定、元数据发布等操作，为数据源计算节点提供全生命周期的可靠性监控和运维管理。

2. 联邦 SQL 分析：支持标准 SQL 语法，对接多种主流数据存储系统，为数据消费者实现多方数据的融合分析。参与方的敏感数据能够在具有 TEE 或 MPC 安全支撑的聚合计算节点中实现安全计算。

3. 可视化数据监管：此外，TICS 为数据参与方提供可视化的数据使用流图，支持插件化对接存储区块链，保障数据使用过程可审计、可追溯。

6.2.6.4 云数据运维

- **数据库安全运维（Database Security Operations and Maintenance）**

提供数据库安全运维功能，支持独立访问控制，自动识别和阻断高危操作。同时，提供多种身份认证方式，运维人员免密登录数据库，防止密码泄露。实现对运维人员的最小化权限控制、风险操作阻断和行为审计，保障生产数据安全和正常运维操作。

支持多种主流数据库、大数据组件、NoSQL数据库。基于主体、客体和行为三元组进行管控，精准实现访问控制。丰富的数据库漏洞信息及高危风险操作特征模板，精准检测数据库风险操作。灵活定义被保护对象，设置严格管控策略，非经审批不可改、不可删、不可见。支持短信验证、FreeOTP等多因子认证方式，保障准入安全。

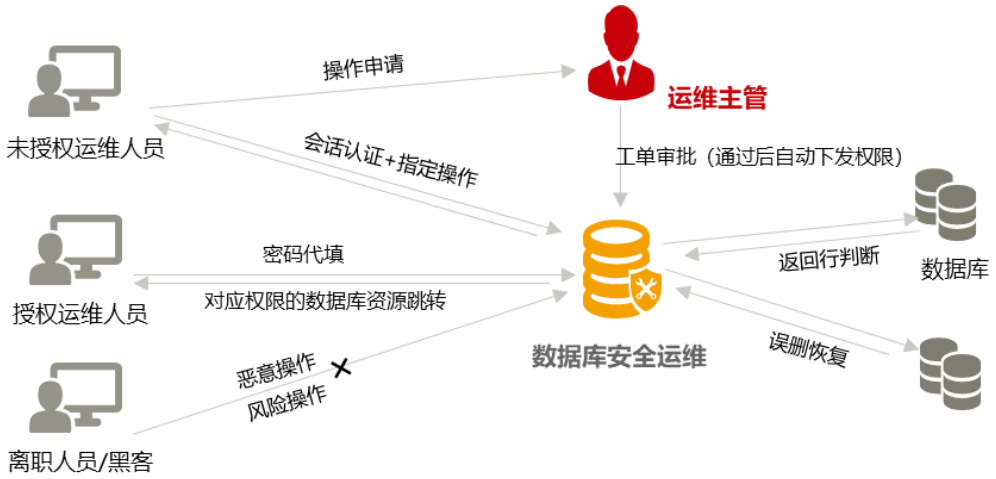

图6.10 DSOM 能力概况

DSOM的核心功能点包括：

1. 自动识别阻断：运维域数据安全能力，语句级访问控制，支持各种风险操作、高危操作自动识别和阻断

2. 内部威胁防护：数据访问权限精细化管控、多种身份认证、操作权限审批、权限自动回收

3. 审计日志和报表：审计日志内容全面，支持日志会话回放功能，支持自定义配置报表内容

4. 资产管理：支持密码代填，批量改密，可对数据库中误删的表、数据，进行备份和恢复

6.2.6.5 操作审计

华为云提供的云审计服务（CTS）会实时记录云上环境的所有操作信息，审计日志的存储、传输均采用高强度加密，且无修改、删除类功能或接口，保证审计日志数据的完整性。客户可以通过审计和监控等方式进行验证和回溯，确保只有被授权的人员处理云环境内的数据。

- **云审计服务（CTS）**

云审计服务（CTS）将实时记录客户云账户下资源的操作记录。云资源生成的每条审计日志均会记录什么用户，什么时间，通过什么IP发起了操作请求，帮助组织执行越权分析、关键资源变更分析等活动，并支持实时短信和邮件通知。审计日志的存储、传输均采用高强度加密，且无修改、删除类功能或接口，保证审计日志数据的完整性。审计日志的查看、访问权限将严格由系统管理员集中分配和管理。

- **云日志服务(LTS)**

云日志服务（Log Tank Service，简称LTS），用于收集来自主机和云服务的日志数据,采集到的日志数据可以在云日志控制台以清晰有序的方式展示，并且可以长期存储。采集到的日志数据可以通过关键字查询、模糊查询等方式简单快速地进行查询，从而高效追溯用户对主机和云服务的操作活动。

- **对象存储服务（OBS）**

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、代码编辑和接口

调用等多种使用模式，便利地对图片进行水印设置，并快速获取处理后的图片。

服务资源

- **统一身份认证服务（IAM）**
- **云堡垒机服务（CBH）**
- **数据库安全服务（DBSS）**
- **数据安全中心（DSC）**
- **可信智能计算服务（TICS）**
- **云审计服务（CTS）**
- **云日志服务(LTS)**
- **对象存储服务（OBS）**

6.2.7 自主控制数据销毁

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，对存储的数据进行清除。在数据销毁前，客户可通过华为云的云数据迁移服务（CDM）对内容数据进行迁移，实现对数据的自主控制权。在数据销毁时，华为云会对指定的数据及所有副本进行全面清除。相关内容可以参考华为云官网“宽限期保留期”。

6.2.7.1 客户内容数据迁离

- **云数据迁移服务（CDM）**

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。

6.2.7.2 数据销毁

华为云为客户提供自主可控的数据删除机制，当前为客户提供的数据删除机制主要涵盖以下场景：

✓ 针对存储及数据库等云服务，客户可在服务层面自行执行数据删除操作。

✓ 华为云建议客户对云上重要数据进行加密存储，当加密数据需要删除时，通过直接删除相关数据加密密钥从而删除数据，防止数据在被彻底删除前被恢复为明文后造成泄露。

✓ 在客户的云服务资源到期未续订或欠费的场景下，华为云仍然可提供自主可控的数据删除机制。当客户的云服务资源到期未续订或欠费时，华为云将向客户提供宽限期，宽限期内客户可正常访问及使用云服务。宽限期到期后客户仍未续订或未缴清欠款时，云服务将进入保留期。保留期内客户不能访问云服务，但对客户存储在云服务中的数据仍予以保留。当保留期到期后客户仍未续订或充值，华为云才将删除客户存储在云服务中的所有数据，给予客户充分的时间，自行决策删除与保留数据。

✓ 客户提交注销账户请求时，账户下的所有数据也将被删除。在以上数据删除场景，华为云将在平台层面将对待删除的数据及其副本进行全面的清除。

6.2.7.3 销毁留证

- **云审计服务（CTS）**

云审计服务将对云中用户的任何操作进行记录，了解到谁在什么时间对系统哪些资源做了什么操作。用户在执行数据销毁操作后，云审计服务将记录数据销毁操作详情。从而便于数据所有者、数据管理员等角色针对数据销毁操作进行查看、追踪、确认、取证等活动。

服务资源

- **云数据迁移服务（CDM）**
- **云审计服务（CTS）**

7 恪守数据中立原则，承诺云上数据处理透明可视

华为云坚持“数据中立”原则，秉承“数据为客户所有、为客户所用、为客户创造价值”的理念，绝不在未授权的情况下访问客户的数据，在客户明确授权访问时，确保数据访问活动的透明可视。让客户可以看到华为云员工对云上数据的处理操作，同时也把客户自己对数据的操作也记录下来，一并呈现给客户，使客户对云上数据的处理做到透明可视。

华为云通过规划数据处理透明可视的能力，让客户可以进一步了解云上内容数据的处理操作，包括客户授权华为方员工为客户提供客服支持、代运维等操作，以及客户对自己云上内容数据的操作。

华为云始终坚持保障云上内容数据处理对客户透明可视，客户拥有对上云内容数据的控制权。在遵守适用法律的前提下，华为云承诺不会在未经客户授权的情况下，访问客户的内容数据。

当客户需要华为云提供服务支持时，华为云将确保支持人员只能在得到客户的授权后才可以实施相关操作，并会保留相关操作日志以备客户审计查阅。

华为云遵从适用国家、区域的法律法规，持续关注内外部监管要求的变化，开展相关行业的安全标准评估，并向客户持续分享华为云的合规实践。

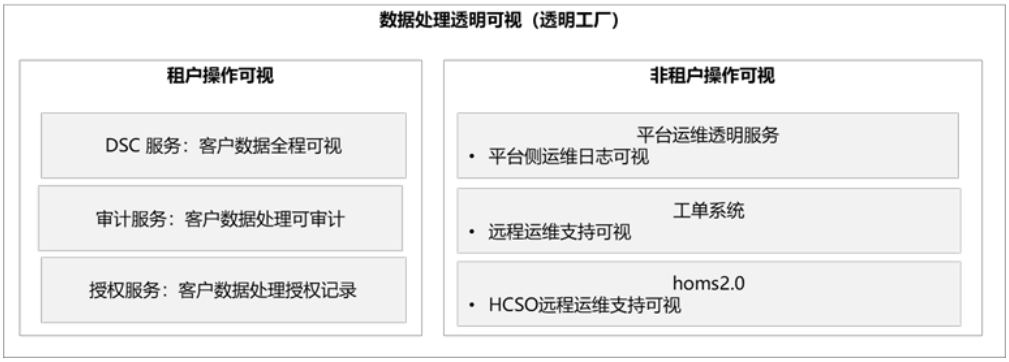

图7.1 数据处理透明可视

7.1 风险可视的数据安全运营平台

华为云以数据为中心，围绕数据全生命周期，构建全栈的数据安全服务，关键数据实施纵深防御，通过全栈加密、密钥客户自持、远程运维客户授权等，支撑用户实现数据安全的自主可控。

数据安全中心服务（Data Security Center，DSC）是新一代的云化数据安全平台。提供数据分级分

类、数据安全风险识别、数字水印溯源和数据静态脱敏等基础数据安全能力，通过资产地图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。使用数据安全中心，可以全方位的帮客户管数据，实现数据全生命周期的管理。

图7.2 DSC功能服务图

7.1.1 数据识别

- **数据资产发现**

DSC利用云原生的最大优势，一览云上所有数据资产分布及配置和出口风险，实现包括资产全可视，涵盖了云上所有数据资产，包含OBS/RDS/CSS/Hive/Hbase等，并通过风险关联分级分类结果，一览展示各个数据风险级别，根据云上资源VPC展示各个资产所在区域，和业务区域关联。

- **敏感数据识别**

支持自定义识别维度、自定义识别阈值、自定义分类、分级规则，通过正则和NLP在海量数据中识别敏感数据，时长缩减至分钟级。为数据保护提供依据：详细显示当前敏感数据分布与对应保护状态，为数据分级保护策略提供帮助。

- **数据分类分级**

通过华为云分类分级模板、行业领域模板、自定义模板快速实现数据分类分级。通过DSC定时扫描OBS/ DB/Hive等，发现敏感数据。结合专家知识库+AI算法自动快速识别敏感数据和个人隐私数据。

- **数据资产地图**

实现风险视图关联分类分级结果，一览展示各个数据风险等级，并根据云上资源VPC展现各个资产所在区域，和业务区域关联。

7.1.2 数据保护

- **数据脱敏：**数据脱敏：支持 API、20+预置脱敏规则、支持自定义脱敏规则
- **数字水印：**支持文档、图片、数据库水印，支持明水印、暗水印，支持 API
- **数据库审计与运维：**集中制定和管理数据库加密、动脱、运维、审计等 6 大类数据安全保护策略

- **云堡垒机：**提供统一的资产运维入口，确保所有运维可管理、可控制、可追溯
- **API 数据安全保护：**支持 API 访问控制、API 风险检测、API 数据保护（脱敏、水印等）
- **数据安全运营：** 提供资产统计、分类分级统计、威胁态势、响应处置的统一展示和管理平台

7.1.3 数据侦测

- **数据流转监测：**实时监测数据流转路径和数据泄露风险，支持联动响应处置，精准洞察泄露源头和途径
- **异常行为检测：**集中监控处理数据库攻击、API攻击等数据安全事件
- **告警事件管理：**集中监控处理各安全组件产生的告警信息
- **数据泄露溯源：**集中提供提取数据库、文档水印能力进行追踪溯源

服务资源

- **数据安全中心服务 DSC**

7.2 存储透明可视

华为云以区域（Region）为单位向您提供服务。区域即您的数据的存储位置，华为云绝不会在未经您授权的情况下，跨区域移动您的数据。您在使用云服务时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保您的数据存储在目标位置。对于区域服务，您可以在购买服务初期按需选择区域，服务部署位置及数据留存地可以通过华为云门户进行变更。

7.3 客户服务响应

华为云致力于提供一种透明化的客户服务体验，确保所有与客户内容数据相关的操作均处于客户的监督之下。通过规划数据处理透明可视的能力，通过云审计（CTS）和云日志（LTS）等服务华为云让客户能够深入了解云上内容数据的每一次处理操作，无论是华为云员工为客户提供的客服支持还是代运维服务，亦或是客户自己对云上数据的操作，都将清晰可见。这种透明度不仅增强了客户对服务的信任，还为客户提供了一个更加直观的操作界面，使得客户能够更轻松地管理自己的数据，同时确保任何支持行为都在客户的知情和授权下进行。

华为云通过不限于合同承诺、账户数据请求响应、内容数据请求响应的的手段来保障对客户的响应：

1. **合同承诺**

华为云在相关的合同、协议中明确了对客户的数据保护的责任和义务，华为云负责基础设施及云服务自身的适当安全性，制定并实施适当的安全策略和措施，以帮助客户防止数据泄露、损坏或任何未经授权的非法访问。

2. **账户数据请求响应**

华为云在收到客户关于数据访问、更正、删除或数据携带的请求时，将在法定时限内进行处理，并提供明确的反馈。

3. **内容数据请求响应**

在某些特殊场景下，客户需要向华为云申请支持服务，而华为云可能需要访问客户的云上环境才能帮助客户解决问题。为了避免非授权人员对客户云上数据的访问，客户可以通过“支持与服务”功能，创建工单向华为云运维工程师请求提供故障响应。

4. 华为云授权人员访问客户数据透明可见

由于云本质的特性所限，在某些特殊场景下，客户难免需要向华为云申请支持服务，在这种情况下，华为云可能需要访问客户云上环境才能帮客户解决问题。为了避免非授权人员对云上客户数据的访问，同时也为了更好向客户证明相关的支持人员只在授权范围和时间段内访问客户云上环境。华为云为客户提供了“共担可信授权”功能，确保客户授权最小化、华为云操作可审计。

“共担可信授权”功能介绍如下：

- 控制台授权支持 IAM 委托授权，通过授权方式和授权有效时间的设定，实现客户最小 化授权。如客户开启 CTS 审计服务，则整个操作过程可供客户审计；

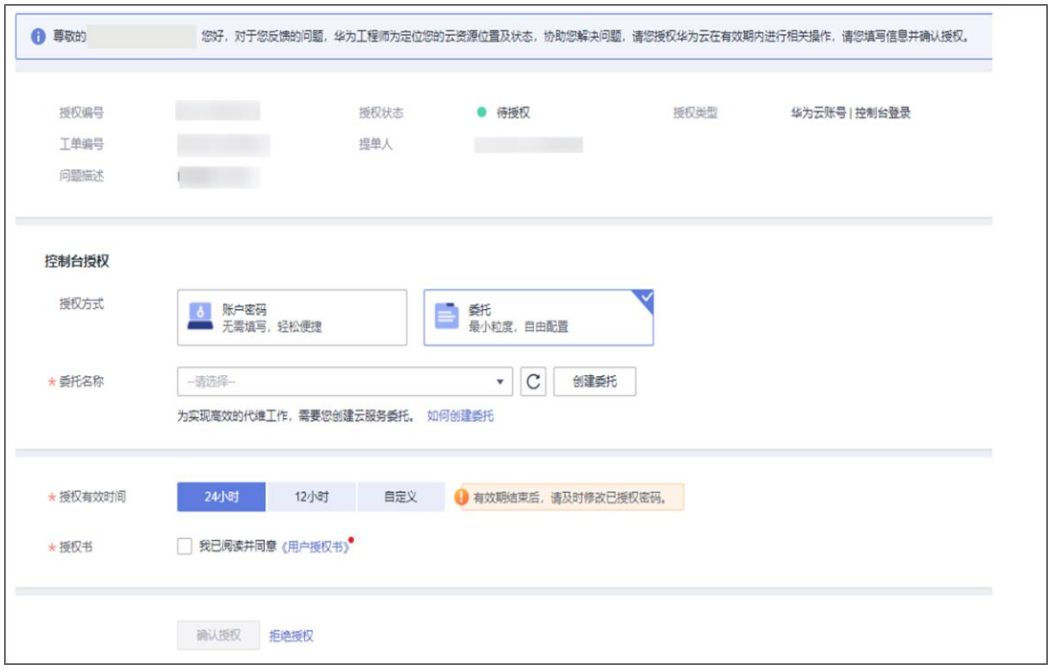

图 7.3 共担可信授权功能（一）

- 服务器授权支持 SSH 登录，客户可通过华为云堡垒机登录指定授权的机器进行操作，所有操作的命令和文件上传下载记录可以在控制台查看；

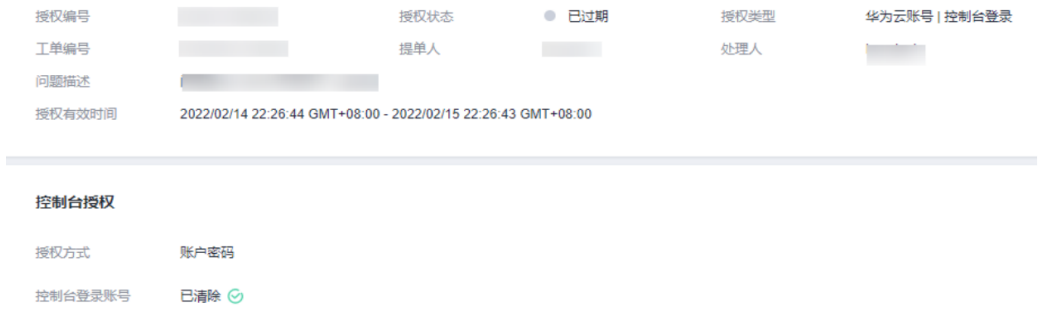

图 7.4 共担可信授权功能（二）

- 所有的授权人员（华为云）都无法访问到客户敏感个人数据。当客户授权到期或者客 户撤销授权之后，授权状态显示“已过期”，控制台登录账号被清除，华为云无法再访问客户数据。

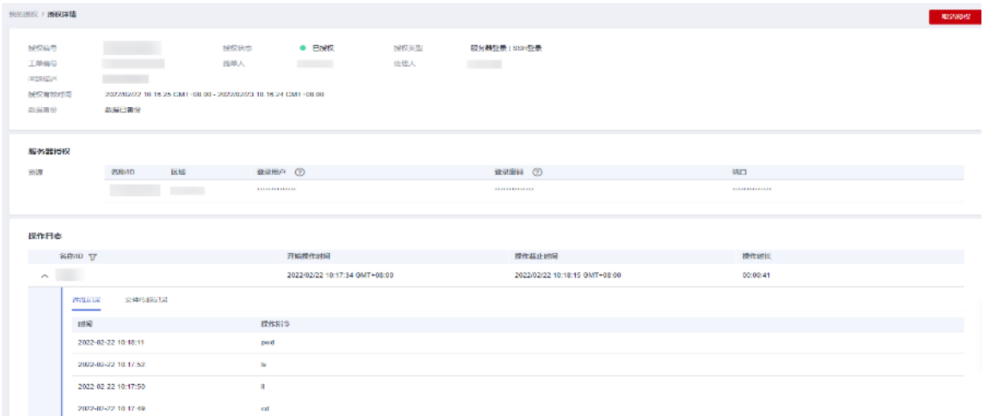

图 7.5 共担可信授权功能（三）

7.4 合作伙伴要求

面对合作伙伴的需求，华为云同样秉持着开放与合作的态度，致力于建立一个基于信任的合作生态。华为云理解合作伙伴对于数据安全和合规性的重视，并积极与合作伙伴分享华为云的合规实践和技术成果。无论是通过技术交流、联合解决方案开发还是共同参与行业标准制定，华为云都力求与合作伙伴携手前行，共同促进云服务市场的健康发展。华为云相信，通过持续的沟通与协作，可以建立起一个既符合监管要求又满足市场需求的合作模式，从而实现多方共赢的局面。

华为云建立了一套完善的供应商管理机制，在与供应商合作前华为云将对其进行尽职调查并且会对供应商是否持有相应经营许可和相关资质进行全方位的考察。在合作时华为云将与供应商签署保密协议，供应商与其员工签署保密协议，并在合同中规定其信息安全责任。规定中明确供应商的信息安全职责及在离岸外包服务场地涉及物理安全、网络安全、应用安全、终端安全等方面的信息安全要求。华为云在与外包供应商签署合作合同时，会将此规定作为合同基本条款的附加条款要求供应商遵照执行，并明确供应商违反本规定的处罚措施。

华为云在引入合作伙伴进行数据处理的透明可视，包括华为将数据处理活动分包给合作伙伴（涉及向第三方披露），华为将尽到向客户告知数据处理者/子处理者信息的义务；合作伙伴参与数据访问和处理，也将做到透明可视。

7.5 审计认证

通过华为云所获得的网络安全与隐私保护认证证书、审计报告和渗透测试报告（国际站、欧洲站），客户可以深入了解到华为云对云上数据安全保护所做出的努力，以及华为云具备强大的数据安全保护能力保障客户的云上数据安全。

华为云不仅定期进行自我评估，还邀请第三方机构进行独立审计，并将这些结果透明地分享给客户，帮助客户理解华为云是如何维护其数据安全与隐私的。

8 责任和义务

8.1 客户上云数据说明

客户在使用华为云服务时，通常涉及以下两类数据：账户数据和客户内容数据。

1. 账户数据指客户在注册账户及使用华为云服务时向华为云提供、产生的数据，例 如客户的姓名、电话号码、电子邮件地址、银行账户信息和账单信息等。华为云 在处理涉及客户个人数据时，会严格依据华为云官网的《隐私政策声明》和《华 为云用户协议》中的使用目的和范围进行处理，如客户想要更进一步了解相关信 息，可参考《华为云隐私保护白皮书》。

2. 内容数据主要是指客户使用华为云服务过程中存储或处理的业务数据，包括但不 限于数据、文件、软件、图像、音频、视频等类型的数据。作为客户云上的数字 资产，其安全性是所有客户业务上云的重要关注点。

8.2 华为云责任

作为云服务提供商（Cloud Service Provider，简称 CSP），一方面负责为客户提供 安全、合规的云基础设施、平台及服务，确保客户可以在一个安全的环境中存储和处理其云上的数据。另一方面为客户提供丰富的数据保护技术和能力，支撑客 户更好的构建其云上的安全能力，确保数据的安全合规。

1. 数据安全保护：华为云从组织职责、政策、流程、工具支撑、持续度量等五大关键要素制定了完善的数据安全治理落地机制，并从平台层面设计和实施了一系列安全防护措施，保护云上客户数据的安全。

2. 数据安全赋能：华为云为了进一步帮助客户增强云上数据安全的保护能力， 面向客户提供了丰富的服务、解决方案以及诸多的安全特性，使客户可以实 现云上数据安全的自主可控。如：访问控制和身份认证、数据加密、敏感数 据识别、数据库审计等服务、特性。

8.3 客户责任

客户是其数据的主体。客户应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。客户可以自主 选择使用华为云提供的云服务和解决方案，存储和处理数据，同时采用适当的云 安全服务或安全特性对云上数据进行安全加固，并实现对适用的法律法规要求的 遵从。例如，客户需要自行实施适当的安全配置，包括操作系统安全配置、网络 安全设置、数据加密策略，以及其他安全防护策略。

9 安全资质和认证

华为云除了将内部优秀实践孵化为各种服务助力客户增强云上数据安全外，还一直积 极参与到国内外数据安全相关标准的制定，为完善行业数据安全标准、提升业界数据 安全水平持续贡献自己的力量。

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网**“信任中心-合规中心”**。

华为云部分标准类认证/鉴证示例：

认证	描述
CCRC 数据安全管理认证	CCRC（中国网络安全审查技术与认证中心）数据安全管理认证旨在帮助组织强化数据安全实践，符合国家标准，确保组织满足认证依据的网络数据收集、存储、使用、加工、传输、提供、公开等处理活动的基本原则和要求。
中国公安部信息安全等级保护四级	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵循的通用安全标准，分为 1-5 级，5 级最高，4 级是目前云服务提供商所能获得的最高级别。 华为云通过中国公安部信息安全等级保护四级表明，华为云的关键 region、节点，系统安全方案按安全等级保护四级标准要求设计和建设，实现多层次纵深防护体系。
中国数据中心联盟（DCA - Data Center Alliance）可信云服务认证、金牌运维	金牌运维评估是面向已通过可信云服务认证的云服务提供商的运维能力专项评估。此评估共有 213 项审查内容，申请测评的企业满足 180 项及以上才能通过评估。 华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
可信云《云服务用户数据保护能力认证》	云服务数据保护能力评估是可信云安全类专项评估之一，此项评估旨在对云服务提供商所提供云产品的数据保护能力进行客观、全面、体系化的评估。 华为云通过了可信云用户数据保护能力认证，证明华为云切实落实安全承诺，恪守业务边界，做中立云服务商的战略定位。
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。 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

认证	描述
	准）认证的云服务提供商。该标准认证的通过，证明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，实现传输、存储、处理支付卡用户信息时的安全合规。
ISO27001	ISO27001 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。
ISO27017	ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO27018	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO22301	ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
CSA STAR 认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。 华为云通过的 CSA STAR 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。
ISO27701	ISO27701 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。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012	BS10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
ISO 29151	ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。

10 数据安全展望

10.1法规和标准的持续更新

智能世界正在加速到来，数据不仅从生产结果变为了生产“资源”，并进一步转变为创新“智源”，数据对经济发展、社会治理、公众生活产生了重大而深刻的影响。然而，数据汇聚、高频流动、高度开放也加剧了数据安全合规风险，对国家安全、社会稳定、企业和公共利益以及个人合法权益构成了严重威胁。

在这一背景下，世界主要经济体国家、地区先后推出了数据安全法规和标准，以提升数据安全的监管能力，促进数据安全、合规、有序的驱动价值的创造。根据联合国贸易发展组织(UNCTAD)统计，目前全球 77%的国家、地区已经开展数据安全、隐私保护相关的立法；G20 集团、金砖国家均建立了数据安全领域的互信与合作机制；联合国教科文组织（UNESCO）、国际电信联盟（ITU）等国际组织也在积极推动和制定全球性数据安全标准。

但由于地缘政治、经济文化差异、数字化水平不一等原因，数据安全治理规则很难在全球范围内达成共识，并形成“布鲁塞尔效应”。尽管世界主要的经济体国家普遍意识到全球数据安全治理及合作的重要性和紧迫性，但鉴于数据在国家竞争中的重要战略地位，数据安全与数据的跨境流动仍不得不受限于各国陆续颁布的法律法规的约束。这对于数字经济与数字贸易发展带来了很大的制约。

对于云服务提供商而言，除了遵从所适用国家、区域的法规政策和标准，积极践行行业最佳实践外，还应积极参与到全球数据安全法规、标准制定及更新中，并因地制宜为用户，特别是跨国用户提供数据资产的主导权和控制权的能力，并与生态伙伴一道，开放合作，全面满足云服务用户的安全合规需求。

10.2 数据跨境流动与本地化服务

随着数字化进程对数字经济的影响不断加深，数据已成为新的生产要素和战略资源，数据跨境流动不仅是数字贸易也已成为数字经济的核心要素。但数据跨境流动，也引发了国家安全、数据主权、隐私保护等一系列问题。全球超过 100 多个国家对数据和隐私保护进行了立法，以强化跨境数据流动监管。近年来，数据跨境违规处罚案例越来越多，甚至出现高达十亿美金的监管处罚案例，企业数据跨境流动合规的复杂性和风险性正在加剧。

为此，以经济合作与发展组织（OECD）为代表的国际组织和美欧为代表的主要国家，不断探索行之有效的数据跨境流通机制。《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）、《区域全面经济伙伴关系协定》（RCEP）、美国与欧盟于 2023 年 9 月达成了《欧美数据隐私框架协议》、中国于 2024 年 3 月发布了《促进和规范数据跨境流动规定》明确提出了整套具有法律约束力的数据跨境流动原则及执行机制。

对于云服务提供商而言，在支撑用户全球数字化运营的同时，需要更加深入理解并适应不同国家的法律、文化背景和规则，并基于“一国一策”的理念，构建更加灵活全球数据跨境治理架构，以应对不断变化的监管环境和地区差异，从而为用户业务全球化提供有力支撑，为上云用户提供更多选择。同时，TOP 云服务提供商也应积极推动或参与到全球数据跨境流动协议的制定，为数据有序跨境流动减少阻碍。

10.3 技术创新与演进

网络威胁、安全态势以及攻防对抗力量的变化，推动网络安全技术持续创新。零信任、隐私计算、可信数据空间、后量子密码等技术推动数据安全防护体系迈向智能化新阶段。

10.3.1 零信任架构

2010 年，Forrester Research 分析师约翰·金德维格首次提出“零信任”的概念以来，零信任价值愈发凸显。据 Gartner 的统计，截至 2024 年底，全球有超过 60%的组织已经完全或部分实施了零信任策略。

零信任能够将有限已知位置的静态策略保护，扩展到分布式、大范围的数据流动的动态防护。零信任坚持“永不信任，始终验证”原则，有效限制了 APT（Advanced Persistent Threat，高级持续威胁）、勒索软件等攻击，有效控制数据泄露和勒索“爆炸半径”，实践证明是一项行之有效的数据安全防护举措。

华为云通过内部实践不断优化，将内部使用的零信任相关应用孵化成面向客户的产品和服务，打造出了 1 个安全运营中心+7 层防线的“零信任”安全体系。该体系基于华为云统一的云原生安全架构，通过智能极简的安全运营中心—安全云脑（SecMaster），物理安全防线、身份认证防线、网络防线、应用防线、主机防线、数据防线、运维防线在内的七层防线纵深防御，实现资产和安全一体化、安全防护一体化、安全运营一体化，助力企业云上业务和数据“安如磐石”。

10.3.2 可信数据空间

数据空间技术体系自诞生以来，历经近几年的发展以及在行业的探索和实践，已经逐渐被国内外的政府机构、行业界、产业界、学术和研究机构等所理解、接纳并形成共识。数据空间技术和生态体系是目前为止解决数据可信流通最合适的解决方案之一。

目前，全球多个主要国家已经开展可信数据空间项目研究和实践，如欧盟的 Gaia-X（Giga-smart Access Interoperability for All）项目、美国的健康信息交换（Health Information Exchange ，HIE）项目等。2024 年 11 月中国国家数据局发布的《可信数据空间发展行动计划（2024-2028 年）》，以保障数据要素的全链路可信流通，实现跨机构数据的协同和融合，安全释放数据价值。

华为云基于自身实践，探索出一套数据空间的理念框架，设计方法与解决方案，并为用户提供交换数据空间（Exchange Data Space，简称 EDS）服务，帮助用户构建主权可控数据交换空间，通过融合企业内外部数据，促进数据价值的量化和分配，形成数据产生、交换、消费的良性循环，充分释放数据价值，实现数据交换“可信、可控、可证”。

10.3.3 数据安全与 AI 融合

在新一轮科技革命和产业变革浪潮中，人工智能作为关键的驱动力量正深刻影响着社会的未来走向。同时，各类基于 AI 新型攻击种类与手段不断出现，包括深度伪造（Deepfake）、黑产大语言模型、恶意 AI 机器人、自动化攻击等。人工智能的高速发展也加剧了数据安全风险，数据安全亦是人工智能健康发展的关键保障，利用人工智能又能全面提升数据安全的综合能力。未来越来越多的 AI 系统，不仅要支持生成式 AI 的溯源证真能力，还将关注 AI 系统的自身安全，AI 模型的安全，AI 的输入和输出数据可信等安全技术要求，降低 AI 系统误用风险，保护 AI 创造的价值。

华为云面对“即要安全的 AI，又要 AI 的安全”问题，通过人工智能全面赋能数据安全管理和技术的各个环节，并通过各类人工智能技术与传统解决方案的融合，为云上客户构建智能化的数据安全体系。华为云将盘古大模型安全实践服务化，推出了华为云大模型安全解决方案，打造了覆盖 AI 环境安全、数据安全、内容安全、算法模型安全、AI 应用安全，统一安全运营的端到端的大模型安全解决方案。护航“千行百业，百模千态”，助力用户构建安全可信、以人为本的大模型服务。

10.3.4 可信与隐私计算

数据的本质存在多样性、易修改、易复制、易破坏，数据进入流通领域很容易导致安全担忧。同时，随着个人隐私保护意识的觉醒和法律监管日趋严格，用户对数据安全和隐私保护提出了更高的要求。既要保护数据安全，维护个人隐私权益，又要打破数据孤岛、释放数据流通价值，成为数据应用的一大挑战。

隐私计算通过密码学、可信计算、联邦学习、安全硬件等，保护多方协同下的数据安全与隐私，使数据可用不可见，可算不可识，保护数据全生命周期的安全，充分释放数据价值。据 Gartner 预测，到 2025 年，50%的大型机构将采用隐私计算来处理不可信环境或多方数据分析用例中的数据。

华为云结合自身实践，推出的可信智能计算服务 TICS （Trusted Intelligent Computing Service 简称 TICS），其基于多方安全计算、可信联邦学习、机密计算、数据空间、数据胶囊和区块链等技术，实现数据要素流通全链路数据安全和隐私保护，助力跨机构数据的协同和融合，打破数据孤岛，安全释放数据价值，推动跨行业的可信数据融合和协同。

另外，华为云在构建可信基础设施能力过程中，也已向业界推出了具备机密计算能力的云服务。其采用专用硬件和固件来保护客户应用代码和数据在处理过程中免受外部访问，做到硬件级的安全保护。华为云机密计算通过将客户代码数据与云基础设施进行隔离，以及将客户代码数据与客户自身进行隔离，帮助云上客户使用完全机密的方式来部署应用和处理数据，实现全链路数据安全与隐私保护，实现数据的“可用不可见”。

10.3.5 区块链技术

现有中心化数据计算将面临巨大挑战，基于区块链技术的边缘计算有望成为未来主要的解决方案之一。区块链拥有数据的不可篡改和可追溯机制，保证了数据的真实性和高质量，这成为深度学习、人工智能等数据高质量应用的基础。区块链还可以在保护数据隐私的前提下实现多方协作的数据计算，有望解决“隐私保护”和“数据孤岛”问题，将大大优化现有的数据应用，在数据流通和共享上发挥显著作用。

华为云认为区块链是构建信任的基石，实现信用传递、价值传递的可信网络的重要技术之一。华为云一直积极探索区块链的技术研究和场景应用，并基于华为云分布式并行计算、存储、网络、安全、加密、容器等核心技术领域多年积累，推出了华为云区块链服务（Blockchain Service 简称 BCS）。华为云区块链服务（BCS）链，聚焦构建安全、可靠的区块链基础设施，让用户高效的搭建区块链网络及行业应用，实现资金流、物流、信息流的可信快速流动，高效可信协同，助力降低协作成本，提升效率。

10.3.6 后量子密码

随着量子计算技术飞速发展，作为衡量量子计算能力的量子体积数呈“指数级”增长，则可以非常有效地解决计算意义上的困难问题，例如大整数因子分解问题和离散对数问题，进而使得 RSA 和 Diffie-Hellman 之类的相关算法被彻底攻破。这将意味着，传统基于数论难题的公钥密码算法及其协议和系统的安全性均面临量子计算的威胁，这对互联网安全会造成巨大的影响。

随着美国网络安全和基础设施安全局（CISA）、国家安全局（NSA）与国家标准与技术研究院（NIST）联合发布后量子密码候选标准算法和指南的推出，全球各主要国家的后量子密码算法迁移已经被提上议事日程。华为预测，到 2030 年 100%ICT 系统将具备量子安全或向量子安全迁移的能力，量子计算飞速发展，到 2030 年后，传统的安全算法面临被量子计算机破解风险，向抗量子计算攻击的后量子算法（PQC）及量子密钥分发（QKD）演进已刻不容缓。

华为云将在量子密码技术领域进行积极的探索，研究和实践引入后量子密码增强产品安全性的各种可能性和可行性，计划尽早将量子安全算法引入产品和服务中，以确保华为云产品、云底座的长期安全性。

10.4 数据安全体系化运营

数据的可变性、流动性、应用场景的复杂性以及威胁的持续性，决定了数据安全保护的复杂性、艰巨性、长期性。近年来，数据已经成为网络攻击的重点对象，数据勒索链条式、产业化犯罪愈演愈烈，其以高度的破坏性和逐利性，给国家、社会、企业和个人带来了重大经济损失和数据安全风险。而传统的安全运营周期长、研判弱、协同难等困境难以应对数字时代的数据安全风险。

针对数据安全保护出现的挑战，尤其是凭证泄露、数据勒索重大数据安全风险，华为云坚持以“三分建设、七分运营”理念，基于云上统一安全能力和底座，打造出以数据为中心，以风险为驱动，零信任安全模型的纵深防御体系。该体系以华为云安全云脑（SecMaster）作为新一代安全运营中心，结合云原生数据安全中心 DSC (Data Security Center，简称 DSC)，提供数据分级分类、数据脱敏、数据水印、API 数据保护等一体化基础数据安全能力，并通过资产地图整体呈现云上数据安全态势，从而使数据安全威胁检测和响应更智能、更快速、更立体，让企业可以安心上云、放心在云上进行智能化升级，真正做到“攻击不瘫、数据不丢、监管合规”。

10.5 数据安全生态合作与共赢

时至今日，全球数字经济的发展赢来重要历史机遇，数智化和全球化已经成为无可逆转的发展潮流。作为战略资源的数据安全的保护工作的形势也日益严峻，尤其是数据黑灰产业链不断升级壮

大，数据安全攻击的团伙式网络犯罪呈逐年上升的态势。其危害性空前，不断冲击已有的数据安全治理手段，其问题已突破传统的网络界限，且跨越了国家、地区的界限，已成为泛在的全球威胁。

面对错综复杂的数据安全威胁，单打独斗的时代已经一去不返，合作安全、生态共赢才是解决问题的正确选择。华为云提倡全行业、全生态开放协作，共同应对数智时代数据安全挑战，共同创造安全的数字世界。华为云将持续与政、产、学、研、用等各领域的产业组织和生态伙伴开放合作，持续向产业界贡献标准提案、产业理解、难题解决方案，推动产业发展和技术进步。华为云将以“协同创新、融合共赢”发展路径，以责任共担模式为用户提供全方位的安全保障，同时，结合“云生态＋安全生态”，立体创新，持续提升产品和解决方案的竞争力，与行业共建，共同营造开放合作共赢的数据安全生态。

