华为云金融网络安全白皮书

文档版本 1.0

发布日期 2022-05-16

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.....1
1.1 发布背景与目的.....1
1.2 名词定义.....1
2 华为云的认证情况.....2
3 华为云安全责任共担模型.....5
4 华为云持续提高自身安全能力，保障金融行业客户安全.....6
4.1 数据中心.....6
4.2 业务连续性.....8
4.3 外包管理.....9
5 华为云提供云服务，助力金融机构实现安全需求.....12
5.1 身份与访问管理.....12
5.2 网络安全.....13
5.3 系统安全.....13
5.4 运营安全.....13
5.5 数据安全.....14
6 华为云金融行业安全解决方案——金融专区.....16
6.1 金融专区介绍.....16
6.2 金融专区特点与优势.....17
7 结语.....18
8 版本历史.....19

1 概述

1.1 发布背景与目的

在科技发展的浪潮中，越来越多的金融机构在逐渐寻求业务转型并希望借助先进的技术以降低成本、提升运营效率、实现业务模式的创新。为了规范金融行业对于信息科技的运用，全球金融监管机构针对金融机构如何进行科技风险管理、科技外包管理等方面提出了一系列监管要求和指引。

华为云作为云服务供应商，致力于协助金融客户满足这些监管要求，持续为金融客户提供遵从金融行业标准要求的云服务及业务运行环境。

华为云通过对全球金融监管要求识别与解读，总结了金融机构在使用云计算时需考虑的关键领域，并就这些关键领域在本白皮书中向金融机构阐述华为云的云安全能力与安全实践，以满足金融机构对华为云云安全的期望，建立并巩固金融机构对华为云的信赖度。另外，本白皮书就金融机构需遵从的监管要求，向其提供可帮助其部署安全能力的华为云云服务，以实现金融机构的安全需求。

1.2 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **客户**

  指与华为云达成商业关系的注册用户。

- **外包**

  指利用其他服务供应商履行通常全部或部分由金融机构自行履行的职能。

- **服务供应商**

  指通过订立合同，履行通常由金融机构自行履行的职能的其他法人，包括任何从原始服务供应商或分包商分包或转包服务的法人。

- **云计算**

  根据美国国家标准技术研究院（NIST）的定义，是指一种基于互联网，能够按需提供共享计算机处理资源和数据的计算模式。

2 华为云的认证情况

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，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	产品介绍
ISO 20000:2011	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	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。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017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。
ISO 22301:2012	ISO 22301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。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS认证	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。
CSA STAR金牌认证	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。

认证	产品介绍
国际通用准则 CC EAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。
ISO 27018:2014	ISO 27018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。
ISO 29151:2017	ISO 29151是国际个人身份信息保护实践指南。ISO 29151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。
ISO 27701:2019	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。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 10012:2017	BS 10012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。
PCI 3DS	PCI 3DS标准旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS认证的通过表明华为云在3D协议执行环境的过程、流程、人员管理等方面符合安全标准。

地区性标准类认证

认证	产品介绍
网络安全等级保护（中国）	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守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
可信云金牌运维专项评估（中国）	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。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。
云服务用户数据保护能力认证（中国）	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
工信部云计算服务能力评估（中国）	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估（中国）	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。

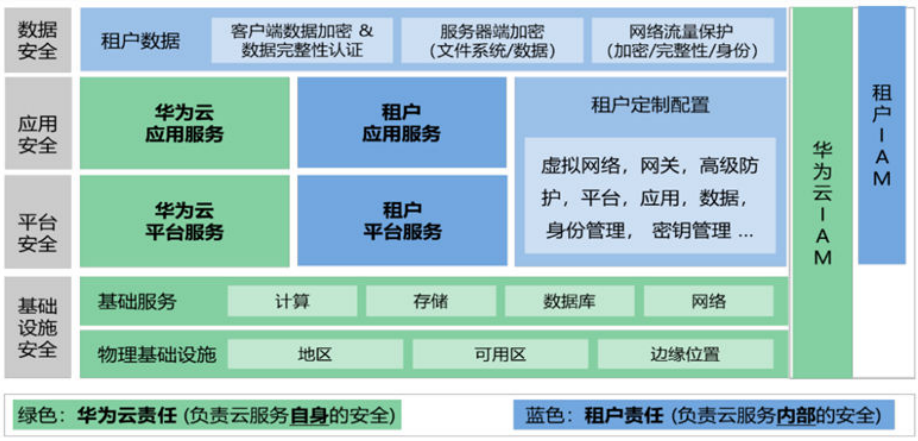
认证	产品介绍
网信办网络安全审查（中国）	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。
MTCS Level 3认证（新加坡）	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3 等级认证。
OSPAR认证（新加坡）	OSPAR是新加坡银行业工会（ABS）对外包服务提供商出具的审计报告。华为云通过了新加坡银行协会(ABS)关于控制外包服务提供商的目标和流程的指南（ABS指南），证明了华为云是符合ABS指南中规定的控制措施的外包服务提供商。
TISAX（欧洲）	TISAX（Trusted Information Security Assessment Exchange，可信信息安全评估交换）是德国汽车工业联合会（VDA）联合欧洲汽车工业安全数据交换协会（ENX）推出的汽车行业信息安全评估和数据交换安全标准。TISAX认证的通过，表明华为云已满足欧洲认可的汽车行业信息安全标准。

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**”。

3 华为云安全责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 3-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：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、数据层和用户身份管理（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：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。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

4 华为云持续提高自身安全能力，保障金融行业客户安全

金融机构在选择云服务供应商时需确保云服务供应商遵守适用的法律法规和标准。尽管金融行业可细分为银行业、保险业、证券业等子行业，不同金融子行业机构需遵从不同的监管标准，但监管机构对金融行业信息科技外包或使用云服务的要求是类似的。

华为云遵从全球多国金融监管机构对金融机构信息科技外包管理规定、云服务使用指南、业务连续性管理、外包管理等监管标准，参考行业最佳实践，持续提高自身的安全能力并改进安全保障体系，努力保障全球金融行业客户的安全。

4.1 数据中心

- **数据中心选址**

在数据中心物理保护方面，华为云设立了分区防护。对于可能的自然灾害制定了选址策略以消减风险。对于入侵、授权等风险，建立了监控机制及响应机制。华为云数据中心会考虑在政治稳定、社会犯罪率低、地理环境友好的地区选址，远离洪水、飓风、地震等自然灾害隐患区域，避开强电磁场干扰，并对于周围的隐患区域设定了最小距离的技术要求。

- **数据中心基础设施**

华为云已制定并实施了完善的物理和环境安全防护策略、规程和措施，满足GB 50174《电子信息机房设计规范》A类和TIA 942《数据中心机房通信基础设施标准》中的T3+标准。

华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS)，提供短期备用电力供应。华为云数据中心建筑防火等级均按一级设计施工，使用了A级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。

华为云数据中心的电力、温湿度、消防等环境运行状态通过日常巡检制度得到例行监控，安全隐患能被及时发现并修复，确保设备稳定运行。

华为云遵循ISO 27001附录A.17.2中信息处理设备应具有足够的冗余以满足可用性要求，通过设备、网络、供应商冗余以避免服务中断，并每年对此要求的落实进行审计以维持ISO 27001证书。

- **数据中心资产管理**

华为云已制定并实施资产的使用规则。根据ISO 27001标准，华为云对信息资产进行分类并由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。华为云会定期对资产清单进行一致性检查并保留检查记录。

华为云对信息资产进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级。同时规定了不同级别资产的安全实施要求。各业务领域遵照资产定级标准对其领域内资产标记安全等级。

- **数据中心物理介质管理**

华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程，要求存储介质及设备进出机房前需进行登记并得到授权。物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。

- **数据中心信息安全管理规范**

华为云参照ISO 27001构建了信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性等。

另外，对于数据中心的维护，华为云建立了数据中心运维管理相关的制度与流程，其中包含设备的具体管控措施、例行的维护计划等。

- **数据中心物理分区管控**

在数据中心设计施工和运营时，合理划分了机房物理区域（包括高度敏感区域），合理布置了信息系统的组件，以防范物理和环境潜在危险。同时分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求，并且制定并实施各区之间的数据流转策略及访问控制策略。

- **数据中心访问控制**

华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。华为云要求来访者必须由内部人员全程陪同，并且只能在一般限制区域活动。

华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7*24小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统，对非法闯入和其他安保事件及时进行声光报警。

- **数据中心设备资源容量与性能管理**

华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。

- **数据中心网络安全**

华为云从最初的网络架构设计、设备选型配置诸方面进行了综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。

华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD–Point of Delivery）、数据存储区（OBS–Object Based Storage）、运维管理区（OM–Operations Management）。除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险。

为了加强网络安全防护，阻止网络攻击扩散，华为云参考ITUE.408安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域，网络层面的划分和隔离，使用了DDoS异常和超大流量清洗、网络入侵检测与拦截（IDS/IPS）、Web安全防护等技术手段。

华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。

- **数据中心数据传输安全**

对于华为云平台客户端到服务端、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，为客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，客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IKE（密钥交换协议）和IPSecVPN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与证书管理：华为云服务提供REST和Highway方式进行数据传输：REST网络通道是将服务以标RESTful的形式向外发布，调用端直接使用HTTP客户端，通过标准RESTful形式对API进行调用，实现数据传输；Highway通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议（TLS–Transport Layer Security）1.2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。

4.2 业务连续性

- **业务连续性计划**

为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得ISO 22301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。

为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得ISO 22301认证。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。

- **应急预案**

华为云制定了完善的突发事件应急预案，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，确保云服务持续运行，保障客户的业务和数据安全。

- **灾难备份管理与灾难恢复**

华为云能够在多个地域内或同一地域内多个可用区之间灵活替换计算实例和存储数据。每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。另外，各可用区有各自独立的 UPS 和现场备用发电设备，每个可用区域所连接的电网也不同，所有可用区域与多个一级传输供应商冗余相连，进一步排除单点故障的风险。

客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从监管要求前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

- **安全事件管理与响应**

华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程，并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。

华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM–Security Information and Event Management）系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。

华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。

- **应急过程记录**

华为云会对应急处置中所有相关的信息和处理过程进行严格记录，所有过程资料应由专人存档保管。华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯。

- **外部沟通**

华为云配备了专人与行业机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点，保证灾难恢复时能及时获取外部支持。

4.3 外包管理

- **外包合同及分包管理**

华为云提供了线上的《华为云用户协议》以及《华为云服务等级协议》，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。如：由独立审计师对云服务供应商的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。

- **尽职调查**

华为云提供了线上的《华为云服务等级协议》，其中规定了所提供服务内容和服务水平以及华为云的职责。同时，华为云会安排专人积极配合客户发起的审计要求和尽职调查。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。华为云已通过ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR等多项国际安全与隐私保护认证，并且每年会接受第三方的审计。

- 技术能力：华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。
- 财务状况：华为云是华为的云服务品牌，自2017年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。
- 商业声誉：华为云一如既往坚持“以客户为中心”，让越来越多的客户选择了华为云。在中国多个行业，例如互联网、点播直播、视频监控、基因、汽车制造等行业，华为云已实现大突破。
- 适合金融机构的企业文化和服务政策：华为云在产品和服务规划和阶段会根据客户业务场景、法律法规及监管要求等方面对产品的安全和功能需求进行定义，并在研发设计阶段将功能实现，以满足客户的需求。

- **合同终止后供应商切换**

在服务协议终止时，客户可通过华为云提供的对象存储迁移服务（OMS）和主机迁移服务（SMS），将内容数据从华为云中迁移出去，如迁移至本地数据中心。OMS和SMS支持国内外主流公有云厂商，SMS还支持国私有云平台虚拟机迁移、x86物理服务器迁移（覆盖约40种主流操作系统）。

- **监督与检查**

金融机构对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。华为云会遵从与金融机构签订的协议中约定的要求，并会安排专人积极配合金融机构和金融交易实体监管/监管指定的代理人对华为云的审计和监督。

华为云的云服务和平台已获得众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。同时，华为云每年定期接受专业第三方审计机构的审核。如有必要，金融机构可以通过官方渠道向华为云申请获取证书以及审计报告的副本。

- **非驻场式外包运维**

华为云运维人员接入客户环境时需获取客户授权，且运维全过程会受到记录。

华为云内部建立了运维和运营账号管理机制。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行RBAC权限管理。保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。

- **操作记录留存**

华为云针对所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志也会进行管理，确保所有日志保存时间超过180天，90天内可以实时查询。华为云内部已

根据法规要求建立了法证调查管理机制，制定了规范的取证流程，以支持安全事件的法证调查。

- **客户数据管控**

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。

华为云支持根据客户要求对数据进行安全删除，安全删除的方式包括删除加密存储的加密密钥、底层存储回收并覆写、对报废的物理介质进行消磁/折弯/粉碎。

作为云服务供应商，华为云会识别并保护金融机构的个人资料。从公司政策、流程、操作层面制定了隐私保护策略，并采取匿名化、数据加密、系统及平台安全防护等措施，全面保护金融机构个人资料的安全。

- **客户业务连续性计划**

如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。

- **事件披露与监管上报**

为配合客户满足重大风险上报利益相关方的要求，华为云设置7*24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。除此之外，华为云已建立了数据泄露事件处理机制，如有必要，华为云会按照适用法律法规的要求进行事件通报。

如客户需进行监管上报的工作，华为云将配合客户提供相关材料。

- **漏洞处置与披露**

华为产品安全事件响应团队（PSIRT–Product Security Incident Response Team）于2010年正式成为国际应急响应论坛FIRST成员之一，通过该组织可实现与471个成员交流业界最佳实践和安全信息；华为PSIRT已经建立成熟的漏洞响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为PSIRT和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，能确保基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。对于需要通过版本、补丁修复的漏洞，通过灰度发布或蓝绿部署等方式尽量减少对租户业务造成影响。

为保护最终用户和租户，华为云秉承负责任的披露原则，对于涉及云平台、租户服务等的漏洞，在确保不会因主动披露而导致更大攻击风险的情况下，向最终用户/租户及时推送漏洞规避和修复方案和建议，与租户共同面对安全漏洞带来的挑战。

- **生产环境变更管理**

华为云生产环境的各要素，如机房设施、网络、系统平台软硬件和应用等的更改，包括设备增减、架构调整、系统软件更新（含网络系统，操作系统镜像和应用容器）、配置改变等发生变更，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都需通过类生产坏境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。

5 华为云提供云服务，助力金融机构实现安全需求

全球各国金融监管机构对其管辖范围内的金融机构发布了严格的监管标准，受监管的金融机构客户需要考虑与网络安全相关的监管要求和义务，并根据他们的需求，在其环境中进行安全设计与部署。

金融机构可使用华为云服务来部署安全能力、改善安全流程，实现其安全需求，以提高整体安全能力。

5.1 身份与访问管理

金融机构可通过华为云的**统一身份认证服务（Identity and Access Management，简称IAM）**对使用云资源的用户账号进行管理。IAM可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。

云堡垒机（Cloud Bastion Host，简称CBH）是华为云的一款统一安全管控平台，可帮助金融机构实现集中的帐号、授权、认证和审计管理。云堡垒机提供云计算安全管控的系统和组件，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。金融机构可以通过统一运维登录入口实现对服务器、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。金融机构员工登录公司系统、运维人员访问运维网络区域、员工从企业外部网络远程接入相关资源以及管理员接入管理平台等场景都可以使用云堡垒机实现访问控制及统一操作日志审计，确保网络和网络服务仅由已获授权的用户访问。

华为云的**云审计服务（Cloud Trace Service，简称CTS）**可以实时、系统地记录用户通过云账户登录管理控制台执行的操作。金融机构可根据企业对日志保留期限的要求购买不同规格的**对象存储服务服务（Object Storage Service，简称OBS）**以实现日志的备份。

华为云提供的**云日志服务（Log Tank Service，简称LTS）**提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务，金融机构可以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。

5.2 网络安全

金融机构可以使用华为云提供的**虚拟私有云（Virtual Private Cloud，简称VPC）**服务，实现不同区域之间网络隔离。VPC可为租户构建出私有网络环境，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，并通过配置网络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，满足租户更细粒度的网络隔离需求。

针对金融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（DC）**、**云连接（CC）**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。

金融机构可通过华为云的**漏洞扫描服务（Vulnerability Scan Service，简称VSS）**实现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、弱密码检测等功能，自动发现网站或服务器暴露在网络中的安全风险，以实现对其云上的业务进行多维度的安全检测。

金融机构可通过部署**Web应用防火墙（Web Application Firewall，简称WAF）**对网站业务流量进行多维度检测和防护。Web应用防火墙可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，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、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意攻击和入侵，保护Web服务安全稳定。

金融机构可通过Anti-DDoS流量清洗服务实现对网络层和应用层的DDoS攻击防护，AntiDDoS为客户提供精细化的防护服务，客户可以根据业务的应用类型，配置流量阈值参 数，并通过实时告警功能查看攻击和防御状态。客户如需更大流量攻击的检测和清洗 服务，可通过华为云的**DDoS高防（AAD - Advanced Anti-DDoS）**服务来实现。

5.3 系统安全

针对主机安全防护，华为云的**企业主机安全服务（Host Security Service，简称HSS）**可实现对主机系统的全面安全评估，评估后通过将现有系统存在的账户、端口、软件漏洞、弱口令风险进行展示，提示客户进行加固，消除安全隐患，提升主机整体的安全性。企业主机安全服务还提供入侵检测功能，在发现账户暴力破解、进程异常、异常登陆等事件后快速进行告警，客户可通过事件管理全面了解告警事件，帮助客户及时发现资产中的安全威胁、实施掌握资产的安全状态，使用入侵检测技术检测和防止入侵网络。

华为云为金融机构提供**存储容灾服务（Storage Disaster Recovery Service，简称SDRS）**，可帮助金融机构在容灾站点迅速恢复业务，缩短业务中断时间。该服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

5.4 运营安全

华为云为金融机构提供统一的管理界面，供金融机构查询并管理其购买的华为云资源。金融机构也可使用华为云的企业主机安全（HSS）的资产管理功能对其资产进行统一管理。

华为云的**云监控服务（Cloud Eye Service，简称CES）**为用户提供一个针对弹性云服务器（ECS - Elastic Cloud Server）、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，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。

应用运维管理服务（Application Operations Management，简称AOM）是云上应用的一站式立体化运维管理平台，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，帮助金融机构及时发现故障，全面掌握应用、资源及业务的实时运行状况。

华为云可提供Anti-DDoS流量清洗服务、Web应用防火墙服务、**数据库安全服务（Database Security Service，简称DBSS）**、云审计服务（CTS）可帮助用户精准有效地实现对流量型攻击和应用层、数据层攻击的全面防护，以及事后对安全事件进行审计。

华为云的云审计服务（CTS）为租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。记录的操作类型有三种：通过云账户登录管理控制台执行的操作，通过云服务支持的API执行的操作，以及华为云系统内部触发的操作。CTS会对各服务发送过来的日志数据进行检视，确保数据本身不含敏感信息；在传输阶段，通过身份认证、格式校验、白名单校验以及单向接收机制等手段，确保日志信息传输和保存的准确、全面；在保存阶段，采取多重备份，并根据华为网络安全规范要求，对数据库自身安全进行安全加固，杜绝仿冒、抵赖、篡改以及信息泄露等风险；最后，CTS支持数据以加密的方式保存到OBS桶。

态势感知（Situation Awareness，简称SA）是华为云为金融机构提供的安全管理与态势分析平台。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，为金融机构呈现出全局 安全攻击态势，帮助金融机构识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联DDoS高防、企业主机安全服务、Web应用防火墙和数据库安全服务等，集中呈现安全防护状态。

5.5 数据安全

金融机构可通过华为云的数据存储加密服务实现对数据的加密，华为云将复杂的数据加解密进行封装，使得金融机构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。

华为云为金融机构提供了**数据加密服务（Data Encryption Workshop，简称DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除金融机构外的任何人无法获取密钥对数据进行解密，确保了金融机构云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为金融机构创建和管理密钥，HSM拥有FIPS140-2（2级和3级）的主流国际安全认证，满足用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法窃取金融机构根密钥。DEW还支持金融机构导入自有密钥作为金融机构主密钥进行统一管理，方便与金融机构已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。

对于传输中的数据，当金融机构通过互联网提供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。针对金融机构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（DC）、云连接（CC）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。

金融机构可以使用华为云提供的**云备份（Cloud Backup and Recovery，简称CBR）**服务实现对云硬盘（EVS - Elastic Volume Service）、弹性云服务器（ECS - Elastic

CloudServer）和裸金属服务器（BMS - Bare Metal Server）的备份保护。云备份支持基于快照技术的备份服务以及利用备份数据恢复服务器和云硬盘的数据。同时云备份支持同步线下备份软件BCManager中的备份数据以及对备份数据的完整性校验。

华为云为金融机构提供上云迁移服务。华为云将基于金融机构提供的信息，与金融机构一同商定并确认具体业务目标及范围，通过需求分析为金融机构设计迁移方案并制定迁移计划和迁移演练等。

金融机构可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称OMS）**和**主机迁移服务（Server Migration Service，简称SMS）**将本地数据中心数据迁移至华为云。OMS和SMS支持国内外主流公有云厂商，SMS还支持国私有云平台虚拟机迁移、x86物理服务器迁移（覆盖约40种主流操作系统）。

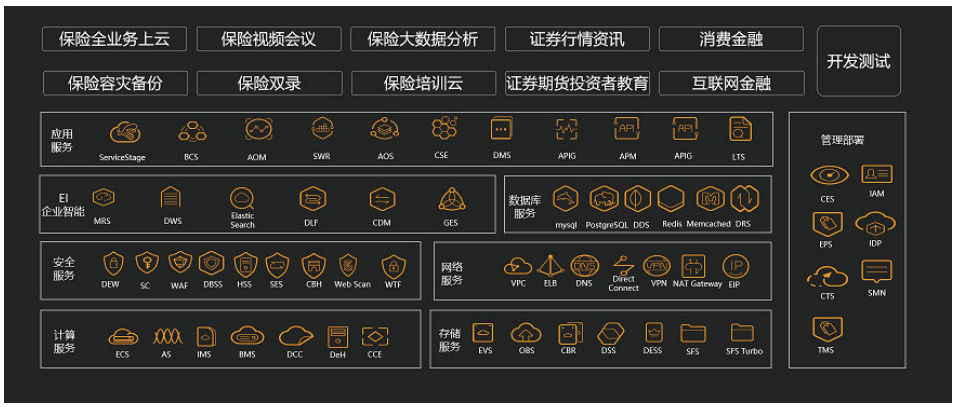
6 华为云金融行业安全解决方案——金融专区

华为云通过结合业界先进的云安全理念、世界领先的 CSP 优秀安全实践经验和优势，摸索出了一整套行之有效的云安全战略和实践。坚持数据中立原则，从网络、业务、数据及管理技术等多维度联动防护，为金融客户构建稳定、可靠的安全解决方案。

6.1 金融专区介绍

华为云面向金融行业规划构建多地多AZ金融专区，打造金融行业数字化底座，助力金融业务智能化升级。华为云金融专区采用A类机房，选址在北上深布局建设，形成两地三中心架构，满足金融行业业务连续性要求，实现业务就近接入的性能及体验要求。金融专区目前上线有50+服务，服务大类包括计算、存储、网络、数据库、EI企业智能等，基本满足金融客户业务云化的需求。金融专区也在持续根据客户需求推送其他服务上线，支持不断满足客户在金融专区业务的部署需求。

图 6-1 华为云金融专区云服务架构



金融专区提供2种专区模式：

序号	专区模式	特点	适用客户
1	行业共享	满足金融行业监管规范要求，与其他行业完全隔离，金融行业共享资源，实现客户业务快速上线。	互联网金融客户、保险、证券等中小型金融类客户

2	全栈专属	在金融专区内采用全栈独享建设模式，为金融客户提供专享云服务。	银行、保险、证券等大中型金融类客户

6.2 金融专区特点与优势

- **等保遵从**

华为云基于行业优秀实践、国际标准及国家标准，打造全面满足云用户的安全需求的云平台， 华为云高等级保护服务系统通过等保四级备案和测评；华为云公共云平台通过等保三级备案和测评。金融专区遵循《 云计算技术金融应用规范技术架构 》、《 云计算技术金融应用规范安全技术要求 》、《 云计算技术金融应用规范容灾 》相关技术标准建设 ，专区物理机房在选址、建筑结构、供电、制冷、消防、布线、物理访问控制、防盗防破坏、监控巡查、防雷消防、通讯等方面符合 GB 50174 2017 A 、 JR/T 01312015 A 、 JR/T 0071 2012 有关要求，采用独立的模块化设计，物理资源严格隔离。

- **高可用性**

拥有双路独立市电、2N配置的供电和配电系统、UPS 不间断电源、集装箱式柴发、2N配置的水冷热交换系统、冷池技术、自动消防预警系统、金融级气体消防服务和智能联动系统。同时，支持同城双活异地容灾及跨云容灾，保障金融业务的不间断稳定运行。

- **安全可信**

使用金融围拢、生物识别双因子认证、红外双监探测等，保障业务和数据安全，提供DBSS、云堡垒机等服务，所有操作可记录、可审计、可追溯。金融专区通过等保四级测评、拥有PCI-DSS、SOC1/2、ISO27001、ISO22301等一系列金融级安全认证。

- **良好性能**

华为云金融专区支持百万级大并发流量和千万级PPS网络包转发，满足毫秒级低时延，提供全闪存裸金属服务和异构计算能力。

- **高标准运维**

7*24小时对机房运行情况进行监控，实时动态可视化管理、规范化和精细化管控，并且会每年定期组织应急切换和容灾演练。同时，客户可自主监控系统运行和运维。金融专区为客户提供7*24小时技术支持服务、等保合规咨询、专属安全服务和专属架构师一对一服务等。

华为云金融专区通过打造安全可信的数字化底座和极致性能的主引擎，为金融业务发展创新保驾护航，矢志成为金融客户服务实体经济的最佳选择。

7 结语

华为云致力于为金融行业客户提供符合监管要求的安全的云环境，并持续改进华为云安全保障体系与安全能力以提高与金融监管标准的契合度。本文描述了华为云在金融监管重点领域下的安全实践，有助于金融行业客户详细了解华为云对于金融行业监管要求方面的遵从性，让客户安全、放心地使用华为云。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署符合金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对相关金融行业监管要求及其他适用法律的遵从性。

8 版本历史

日期	版本	描述
2022年3月	1.0	首次发布