华为云网络安全和隐私保护 FAQ

文档版本 1.0

发布日期 2023-05-31

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 安全隐私治理

1.1 战略和规划

1.1.1 问：网络安全与隐私保护工作的目标或原则如何？

答：华为云网络安全目标和原则：华为云以数据保护为核心，以云安全能力为基石，以法律法规业界标准遵从为城墙，以安全生态圈为护城河，依托华为独有的软、硬件优势，打造业界领先的竞争力，构建起面向不同区域、不同行业的完善云服务安全保障体系，并将其作为华为云的重要发展战略之一。

华为云隐私保护工作的目标和原则：华为云秉承中立态度，严守服务边界，保障数据为客户所有、为客户所用、为客户创造价值；华为云承诺将确保相关业务遵从业务所在国家/地区适用的隐私保护法律法规。

1.1.2 问：网络安全与隐私保护组织架构如何？

答：华为把网络安全作为公司重要战略之一，通过自上而下的治理结构来实现。在组织方 面，GSPC 作为最高网络安全管理机构，决策和批准公司总体网络安全战略。GSPO 及 其办公室负责制定和执行华为端到端网络安全保障体系。GSPO 直接向公司 CEO 汇报。

秉承华为网络安全战略和规范，华为云安全团队对本领域安全工作进行自主规划和管理。全面实现云服务业务和云安全业务的研发运维运营组织合一，组织结构趋于扁平化，以便适应云服务必需的 DevOps/DevSecOps 流程。扁平化的组织结构和适应云服务的流程一方面满足云服务快速持续集成、交付与部署的进度要求，另一方面保证云服务达到必需的安全质量标准，有效控制安全风险。依托云服务安全工程能力、云安全服务与解决方案的设计和开发、云服务安全运维运营等职能，构建华为云服务的安全合规遵从和安全运维运营能力，切实保障华为云租户利益。基于云安全对华为云的特殊重要性，云安全团队直接向华为云总裁汇报。同时，华为云成立了专门隐私保护团队，明确业务的隐私保护责任人，并持续提升相关人员的隐私保护意识和能力，以支撑华为云业务中实现默认的隐私保护。

1.2 风险管理

1.2.1 问：风险管理流程如何？

答：云安全治理活动可以拆解为多个过程，每个过程都有相应的输入、控制和输出。由于全球合规为先的趋势越发明显，无论对于云服务提供商还是云服务客户都需要高度关注合规，有助于了解云安全治理态势的动态变化并及时进行应对；同时，管理好云资产和云服务的风险也至关重要，当前主流的风险管理大部分是基于资产和威胁出发的，华为云安全治理的对象也同样保持与其他权威标准类似的考虑，在云安全治理框架中核心控制的输入主要由安全合规和安全风险共同构成。

1.2.2 问：华为云遵从哪些法律法规？

答：华为云在遵从所在的国家和地区的安全法规政策、国际网络安全和云安全标准参考行业最佳实践的基础上，从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放透明的方式，共同应对云安全挑战，全面满足云服务用户的安全需求。

1.2.3 问：在满足合规的过程中，客户和华为云的职责分别是什么？

答：华为云致力于为客户提供安全合规的基础设施和服务，各项服务内置了安全功能，并通过持续的运维运营保障云服务的安全运行。华为云确保提供的基础设施和服务已通过独立第三方安全权威组织的测评以及安全认证机构的审核。

使用华为云服务的过程中，客户需针对云上业务的特性考虑内部应用及定制配置的安全性与合规性。客户是客户数据的所有者和控制者，负责各项具体的数据安全配置，应对其保密性、完整性、可用性及数据访问的身份验证和鉴权进行有效保障。同时，针对业务特性，客户需确保业务满足对应的监管要求。

可以下载《华为云安全白皮书》查看华为云与客户的安全责任详情。

1.3 隐私保护

1.3.1 问：平台会收集租户的哪些个人数据，并用于哪些用途？隐私声明从何处获取？

答：华为云在客户与华为云的互动过程中出于必要的目的收集客户的个人数据，例如为向客户提供服务。华为云会在如下场景收集客户的个人数据：在客户使用用户帐号时收集客户的用户名、手机号码、邮箱地址和帐号信息；在客户使用地址管理服务时收集客户的收件人姓名、详细地址、邮政编码、手机号码。更多场景请查看隐私政策声明：

中国站：https://www.huaweicloud.com/declaration/sa_prp.html

对于客户的个人数据，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、存储和使用客户的个人数据，并通过全面的数据保护措施确保客户的个人数据安全。

1.3.2 问：平台如何确保租户个人数据收集和处理的合法性？

答：华为云隐私政策声明介绍了收集和使用客户的个人数据的方式和目的，华为云仅在适用法律法规允许的范围内，根据华为云隐私政策声明，共享或披露客户的个人数据给第三方。如获得客户的明确同意后，华为云会向客户指定的第三方共享客户授权范围内的数据；华为云可能会将客户的个人数据向华为云的关联公司披露，以供它们为客户提供交易支持、服务支持或安全支持。

华为云隐私声明详见：

中国站：https://www.huaweicloud.com/declaration/sa_prp.html

1.3.3 问：客户如何访问或控制其个人数据？

答：对于客户的个人数据，客户应确保提交的数据都准确无误。我们会尽力维护客户这些数据的准确和完整，并基于客户向我们提供的信息及时更新客户的数据。

客户可以通过以下方式访问和修改我们持有的有关客户的个人数据：

- **帐号信息：**

如使用华为云网站，客户要添加或更新与客户的帐号相关的个人数据，请访问网站，输入帐号信息，登录帐号中心。如使用华为云应用，选择“我的”->“账号管理”->“基本信息”->“账号名”，添加或更新与客户的帐号相关的个人信息。

- **Cookie：**

关于 Cookie 的管理，请参阅 Cookie 政策：

中国站：https://www.huaweicloud.com/declaration/sa_cookies.html

- **消息：**

如使用华为云网站，请访问网站，点击登录按钮，登录帐号，点击右上角帐号图标，查看未读信息。进入后，客户可以在客户的帐号右上角信箱图标处点击消息接收管理按钮，设置消息接收偏好。如使用华为云应用，客户可以在“我的”>“设置”关闭给客户推送的消息。客户也可以在客户的手机系统设置里，将华为云应用的通知全部关闭。

更多有关客户访问和控制个人数据的细节，客户也可以访问华为云隐私政策声明进行详细了解。

1.3.4 问：在远程运维模式下，是否存在个人数据跨境，会跨境传输哪些数据？

答：华为云在全球多个国家建立数据中心，在运营运维过程中可能涉及需要进行数据跨境传输的场景。这意味着，您的个人信息可能会因履行与您签订的合同所必需而被转移到您使用服务所在国家/地区或者受到来自这些国家/地区的访问，此类国家/地

区可能适用不同的个人信息保护法，甚至未颁布相关法律法规，在此类情况下，华为云会根据相关法律法规的要求和本协议履行合规义务，确保您的个人信息得到适用法律法规要求的和本协议约定的充分且同等的保护。

在远程运维模式下，可能将以下类型数据跨境传输到运维中心：

日志类数据：包括主机和虚拟机的系统日志、访问日志、服务运行日志等

指标类数据：系统指标（如 CPU、内存）、服务指标、租户监控指标（如主机和虚拟机的 CPU、内存、链接数）等服务上报的监控数据

1.3.5 问：华为云如何保护账户信息？

答：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。

1.3.6 问：在提供客户支持的过程中如何保证客户个人数据的安全性？

答：我们重视客户的个人数据安全。华为云采用适当的物理、管理和技术保障措施来保护客户的个人数据。

例如，华为云会使用加密技术确保数据的机密性；华为云会使用保护机制防止数据遭到恶意攻击；华为云会部署访问控制机制，确保只有授权人员才可访问个人数据；以及华为云会举办安全和隐私保护培训，加强员工对于保护个人数据重要性的认识。

另外，华为云还将个人数据保护管控措施融入了华为云个人数据处理全生命周期，客户可以在华为云个人数据保护实践页面了解详情：

中国站：https://www.huaweicloud.com/securecenter/privacy/personal-data-protection.html

1.3.7 问：注销云后，个人数据是否会被保留？

答：关于客户的注册信息，在客户注销后，华为云将依照《隐私政策声明》中声明方式，在适用的法律法规范围内，仅出于问题追溯、审计保留合理期限，到期后将清除客户的注册信息。

1.3.8 问：华为云在隐私保护方面获得了什么认证？

答：华为云已获得了 ISO27018、ISO27701、BS10012、ISO29151、ISO27799 等认证，在数据的处理、存储和数据分级分类方面符合相关隐私标准的要求。客户可以前往隐私认证中心页面查看详情。

中国站：https://www.huaweicloud.com/securecenter/compliance/compliance-center.html

1.3.9 问：华为云遵从 GDPR 吗？

答：华为云的网络安全与隐私保护框架融入了全球多个国家的隐私保护法律法规。除了 GDPR，华为云还参考了爱尔兰、西班牙、瑞士等欧洲主要国家的隐私保护法律法规来构建云平台的隐私保护能力，以保障欧盟公民的隐私权利。并且华为云会通过定期的内外部审查，确保我们为您提供符合当地法律、法规和行业标准的服务。

华为云获得了 ISO27018、ISO27701、BS10012、ISO29151、ISO27799 认证，在数据的处理、存储和数据分级分类方面符合相关隐私标准的要求。

1.3.10 问：针对客户提出个人数据相关权利的行使请求，平台通过哪些渠道进行答复？

答：华为云提供了数据主体权利请求渠道，并配备了专业团队响应数据主体的相关请求，当接收到请求后，在规定时间内完成响应和请求处理，并反馈处理结果给数据主体。

如果客户有任何疑问、意见或建议，可以通过客服热线联系；客户也可以直接通过个人数据权利主体请求页面，提出客户的相应请求：

中国站：https://www.huawei.com/cn/personal-data-request

1.3.11 问：如果发生数据泄露，华为云将如何应对？

答：为降低个人数据泄露事件可能给租户造成的影响和损失，华为云制定了个人数据泄露事件管理流程并成立了专门的隐私保护团队，按照适用法律法规要求，对个人数据泄露事件及时披露， 同时执行应急预案及恢复流程，以降低对客户的影响。华为云开放了多个个人数据泄露上报渠道，确保相关责任人在第一时间收到泄露事件，在发生个人数据泄露初期，相关团队会根据应急预案采取必要的技术措施避免对数据主体的影响进一步加剧，若根据当地法律、法规要求或合同约定个人数据泄露需向外部组织（包括监管机构或客户等）或受影响的数据主体进行通报时，将由专人参照模板进行通报。

1.3.12 问：如果客户有关于个人数据保护的问题，客户应该联系谁？

答：华为云设立了个人数据保护专职部门，来协助解决有关客户的个人数据保护问题。如果客户有任何疑问、意见或建议，可以直接通过个人数据权利主体请求页面与我们联系；客户也可以通过客服热线与我们联系。

中国站：https://www.huawei.com/cn/personal-data-request

1.4 数据安全

1.4.1 问：数据的分类分级规则如何？

答：华为云基于数据的机密性、完整性、可用性和合规性 4 个维度来评估数据的安全级别，安全级别主要考量数据破坏、泄露等行为对华为云造成的影响的严重程度。

1.4.2 问：客户数据通常有哪些？

答：华为云在向客户提供服务的过程中，通常会处理客户的以下两类数据：

- **个人数据：**

个人数据是指单独使用或结合其他信息使用时能够确定个人身份的信息。华为云在客户与华为云的互动过程中出于必要的目的收集客户的个人数据，例如为向客户提供服务。华为云会在如下场景收集客户的个人数据：在客户使用用户帐号时收集客户的用户名、手机号码、邮箱地址和帐号信息；在客户使用地址管理服务时收集客户的收件人姓名、详细地址、邮政编码、手机号码。更多场景请查看隐私政策声明：

中国站：https://www.huaweicloud.com/declaration/sa_prp.html

对于客户的个人数据，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、存储和使用客户的个人数据，并通过全面的数据保护措施确保客户的个人数据安全。

- **内容数据：**

内容数据是指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。

对于客户的内容数据，客户拥有其所有权和控制权，同时客户也需要对内容数据的安全负责，华为云提供丰富的服务，供客户自主选择，助客户提升安全防护水平，削减数据安全风险。

1.4.3 问：客户的云上数据存储在哪里？

答：客户自主决定存储位置。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，华为云未经授权不会跨区域移动客户的内容数据。客户在使用云服务时，建议客户依据就近接入原则、不同地域的法律法规要求等进行区域的选择，客户内容数据将存储在客户选择的区域。

1.4.4 问：客户的内容数据存储在哪里？

答：华为云布局全球多个地理区域和可用区，提供高速稳定的全球云联接网络、贴近客户的本地化服务。客户可以根据需求自主选择华为云的区域购买服务并进行业务部署。客户选择的区域即是内容数据的存储位置，华为云未经客户的授权绝不会跨区域移动客户的内容数据。例如，若客户位于新加坡，想要确保内容数据只存储在新加坡境内，那么客户就可以选择新加坡站点购买服务部署业务。

有关华为云地理区域和可用区的更多信息，客户可以在华为云官网查看华为云全球基础设施的分布。

1.4.5 问：华为云是否将客户的数据转移到其它地区或国家？

答：对于内容数据：客户可以决定内容数据存储的区域。没有获得客户的明确同意或者其他法律义务要求时，华为云不会将客户的内容数据转移到其他区域。客户若有将内容数据进行跨境转移的需求，且需华为云协助时，可联系和授权华为云，华为云根据客户的授权对数据进行转移。

对于个人数据：华为云通过遍布全球的资源和服务器为客户提供产品与服务，收集客户的个人数据可能存储在华为云及其关联公司、服务提供商/分包商所在的国家/地区。这意味着，客户的个人数据可能会被转移到客户使用的产品或服务所在的国家/地区以外的其他司法管辖区，或者受到来自这些司法管辖区的访问。此类个人数据存储地的司法管辖区可能采用保护程度不一的个人数据保护法律，甚至未订立相关法律。华为云会确保客户的个人数据得到适用的法律法规和《隐私政策声明》的保护。可参见问题 1.3.4 在远程运维模式下，是否存在个人数据跨境，会跨境传输哪些数据？

对于中国大陆的用户，客户的个人数据将被存储于中国大陆境内的服务器。

1.4.6 问：华为云如何保障客户的数据安全？

答：华为云在遵从法规和监管要求，借鉴国际及行业数据安全标准，参考行业优秀实践的基础上，从组织职责、政策要求、流程指导、技术工具、度量验证五方面建立并运行了一套完善、高可信、可持续的数据安全治理体系，系统有效的保障客户数据安全。

在技术层面，华为云通过数据安全中心服务（DSC）、数据加密服务（DEW）、数据库安全服务（DBSS）、云监控服务（CES）、云日志(LTS)、云审计服务（CTS）、云 Web 应用防火墙服务（WAF）、防 DDoS 攻击服务（Anti-DDoS Service）等服务保障数据安全，其中 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；云日志(LTS)提供日志收集、实时查询、存储等功能，帮助客户应对日志实时采集、查询分析等日常运营、运维场景；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；WAF 使用正则规则和语义分析的双引擎架构对 SQL 注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意 bot、等攻击实现实时的高性能防护；防 DDoS 攻击服务（Anti-DDoS Service）通过专业的防 DDoS 设备精准有效地实现对流量型攻击和应用层攻击的全面防护。

1.4.7 问：在公网传输数据时，华为云通过什么方式保护数据？

答：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虚拟专用网络（VPN）和应用层 TLS 与证书管理方式提供。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。

1.4.8 问：平台如何确保租户存储在平台上的数据的安全？

答：华为云高度重视客户的数据资产，把数据保护作为华为云安全策略的核心。因此华为云遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为客户提供切实有效的数据保护能力。客户可以在《华为云数据安全白皮书》中找到更多实践内容。

中国站：https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/best%20practices/DataSecurityWhitepaper_chn_cn.pdf

但是，值得强调的是，对于客户使用云服务产生的内容数据，华为云只是其托管者，客户对其拥有所有权和控制权。客户需要负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。例如在使用统一身份认证服务 IAM 和数据加密服务 DEW 时，由客户负责妥善保管客户自行配置的服务登录账户、密码和密钥，并负责执行密码密钥设定、更新和重设规则的业界优秀实践。更多提供数据保护的产品，客户可以打开安全服务页面了解。

中国站：https://www.huaweicloud.com/product/security.html#section-3

1.5 意识教育

1.5.1 问：员工参加网络安全意识培训的情况如何？培训的证据从哪里可以获取？

答：华为云的员工在入职，在岗，晋升等环节都包含多种网络安全意识培训，使员工的行为符合华为云的安全标准。

2 安全隐私验证与沟通

2.1 蓝军评估/稽查/度量

2.1.1 问：平台日常会进行哪些安全测试工作？

答：华为云自己的安全运营团队通过漏洞扫描、渗透测试等方式进行安全测试工作，确保安全。

2.1.2 问：华为云平台是否有漏洞通知机制？

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

2.1.3 问：平台对威胁和漏洞的管理流程如何？

答：华为云有一套成熟的威胁和漏洞管理流程，能够实现快速定位和快速解决，减少对租户业务带来的影响。

2.1.4 问：评估与审计的要求、流程及执行情况如何？

答：华为云实行严格的审计活动，在推动网络安全流程和标准落地方面上起着关键的作用。华为建立了专门的安全审计团队，审计每年进行一次，重点关注华为云在法律和流程遵从、业务目标达成、决策信息的可靠性、安全运维和安全运营上的风险，确保审计发现得到整改。

2.1.5 问：华为云如何满足客户提出的在一定时限内修复漏洞的要求？

答：华为云拥有更完整的网络配置信息和设备操作权限，再结合华为云采用的 DevOps/DevSecOps 流程，使得华为云在漏洞修复的过程中能做到更快速、更直接的持续集成、持续部署。华为云已建立起从漏洞感知到现网修复的端到端漏洞响应工单系统，此系统会自动接收来自 PSIRT、在线扫描工具等众多漏洞收集渠道提交的漏洞，并自动根据漏洞的严重程度确定处理优先级，从而明确对应的漏洞修复 SLA 要求。

2.2 外部沟通

2.2.1 问：当发生个人数据泄露事件时，华为云的通报机制是什么？

答：当发生个人数据泄露事件，华为云根据国家规定、内部流程和透明的原则进行通报。

2.2.2 问：网络安全与隐私保护相关白皮书从何处获取？

答：网络安全与隐私保护相关的白皮书可以在华为云官网的信任中心获取，以下为相关链接：

中国站：

1、信任中心：https://www.huaweicloud.com/securecenter/overallsafety.html

2、华为云可信白皮书：https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/best%20practices/Trustworthiness_Whitepaper_chn_cn.pdf

3、华为云隐私保护白皮书：https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/best%20practices/Privacy_Protection_chn_cn.pdf

4、华为云安全白皮书：https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/SecurityWhitepaper_cn.pdf

5、华为云数据安全白皮书：https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/best%20practices/DataSecurityWhitepaper_chn_cn.pdf

2.3 认证与鉴证

2.3.1 问：华为云已取得哪些安全/隐私方面的认证？

答：华为云致力于构建安全可信的云服务，并确保基础设施和服务通过业界认可的独立第三方安全权威组织的测评以及安全认证机构的审核。

目前，华为云已通过了各种国际权威的认证和实践标准。以下列举部分：

• 安全相关的有 ISO 27001、ISO 27017、CSA STAR 金牌认证、中国公安部信息安全等级保护三级/四级认证、针对支付卡行业的 PCI DSS 以及 NIST CSF 网络安全框架等；

• 隐私相关的有 ISO 27018，ISO 27701，BS 10012、ISO 29151、ISO 27799 等；

客户可以在合规中心的【合规认证全景图】查看华为云已获取的更多认证。

中国站：除了这些第三方认证，合规中心还提供了【基于国家/地区的合规遵从性指导】和【基于行业的合规遵从指导】，以解决客户在合规过程中可能遇到的问题。

合规中心中国站：
https://www.huaweicloud.com/securecenter/compliance/compliance-center.html

2.3.2 问：客户可以获取华为云已通过认证的证书副本吗？

答：中国站：可以。华为云在信任中心提供了相关认证的证书副本。若客户想了解认证覆盖的范围和服务，或客户的业务正在进行相关认证时，需要从华为云获得必要的协助，可在合规页面的合规证书下载处申请下载证书副本。

中国站合规证书下载：
https://www.huaweicloud.com/securecenter/compliance.html

2.3.3 问：华为云可以提供什么审计报告？

答：中国站：华为云发布了 SOC1、SOC2、SOC3 及 OSPAR 审计报告，用户可有通过华为云官网的信任中心进行了解和联系华为云索取相关报告。

中国站：https://www.huaweicloud.com/securecenter/compliance.html

2.3.4 问：华为云有哪些合规服务可以帮助客户快速获取相关认证？

答：中国站：华为云持续关注法律法规的变化，并结合自身多年的安全合规经验开发出可以帮助客户实现业务安全与合规的服务，帮助客户快速获取相关认证。以数据库安全服务 DBSS 为例，DBSS 提供数据库安全审计功能，审计对象可覆盖到每个用户，对重要的用户行为和重要安全事件进行审计，可满足《网络安全等级保护》中对于应用审计的要求；同时，审计日志设置为至少存储 180 天，可满足《中华人民共和国网络安全法》的要求。此外，DBSS 还可以提供满足数据安全标准（例如 Sarbanes-Oxley）的合规报告。

除了安全服务，华为云依托自身安全能力与安全合规生态，为客户提供一站式的安全解决方案，例如等保合规安全解决方案可以帮助客户快速、低成本完成安全整改，轻松满足等保 2.0 的要求。

2.3.5 问：平台通过哪些第三方审计证据向客户证明其符合业界最佳实践的安全控制？

答：华为云通过获取全球通用的权威认证与鉴证报告表明其符合业界的最佳实践，如 SOC1/2/3 鉴证报告和 ISO27001、ISO27017、ISO27018、CSA STAR 金牌认证等。另外华为云针对全球不同地区的合规要求和行业标准，优化了其安全控制要求和手段，如新加坡的 MTCS Level3、国内可信云等。

2.3.6 问：华为云的每个认证覆盖哪些区域？哪些云平台服务？

答：华为云安全认证覆盖所有 region 及可用区，140+云服务。华为云地区性认证，如 MTCS 覆盖当地所有 region 和可用区，及在当地上线云服务。认证的服务范围可以从华为云官网的信任中心进行下载，详细链接如下：

中国站：https://www.huaweicloud.com/securecenter/compliance.html

2.3.7 问：华为云获得了什么政府层面的安全认证？华为云安全认证涵盖了什么行业？

答：中国站：华为云安全认证覆盖信用卡行业、医疗行业、金融行业、汽车行业、政务等；获得政府安全认证包括：中国政府的网络安全等级保护、网信办网络安全审查等，新加坡政府的 MTCS Level3 认证；同时华为云发布多份合规白皮书，适配全球各地法律法规要求，包括：巴西、马来西亚、新加坡等。

中国站详细链接如下：
https://www.huaweicloud.com/securecenter/compliance.html

2.3.8 问：华为云怎样维护相关认证？

答：华为云每年按照安全认证要求进行年度复审和证书更新。

2.3.9 问：华为云提供什么服务，帮助客户获得云相关的认证？

答：中国站：华为云在中国可提供等保认证的支持服务。另外，如客户在认证过程中需要获取华为云的支持，可与华为云客服人员进行联系。

3 服务/方案的安全与隐私合规

3.1 供应链安全

3.1.1 问：华为云供应商清单从何处获取（包括：数据中心供应商，软件供应商，硬件供应商等）？

答：由于涉及商业机密问题，不能直接提供供应商清单。华为云委托进行个人数据处理的供应商类别包括商品或技术服务类，广告、调研、分析、回访等服务类；同时华为云可能会将个人数据共享给业务伙伴，包括云商店独立软件或服务供应商，产品或服务。委托供应商处理个人数据、将个人数据共享给第三方，均已在服务详情页面（服务声明）中披露。

3.1.2 问：对供应商提出了哪些网络安全保护要求和监督审查机制如何？

答：华为云按照自身的网络安全与隐私要求对供应商提出要求和监督。华为云在采购前将会对供应商资质进行评估，仅经过资质认证的供应商才能进入华为云的采购范围。在供应商引入前，需签署合同、服务协议级保密协议，约定双方的责任与义务、服务水平等要求。在供应商引入后，华为云通过供应商安全体系稽查检查供应商安全协议执行、能力状况和问题闭环管理，稽查内容包括供应商安全组织、安全研发测试、漏洞管理等领域。

3.2 开发与部署安全

3.2.1 问：产品是如何确保满足安全和隐私保护相关的需求的？

答：华为云在产品设计之初就考虑了安全和隐私保护相关需求。华为云制定并严格遵守服务可信设计的八大原则，在架构设计阶段对产品的安全防护策略进行设计，在开发时遵循华为内部制度要求的网络安全敏感特性并需通过指定部门的评审，使用安全

编码规范和优选编译器进行代码编译，开发完成后使用指定工具对代码进行安全扫描，并进行安全扫描。

3.2.2 问：开发过程中是如何确保代码的安全性？

答：华为云在开发时遵循华为内部制度要求的网络安全敏感特性并需通过指定部门的评审，使用安全编码规范和优选编译器进行代码编译，开发完成后使用静态代码安全扫描工具对代码进行安全扫描和告警分析，对于扫描出的“必须清理项”和“高风险项”必须清零。

3.2.3 问：开发过程中是如何确保漏洞或后门能被及时检测及发现的？

答：所有云服务发布前都经过了多轮安全测试与多轮审核，包括但不限于根据安全测试用例开展的 Alpha 阶段的认证、鉴权、会话安全等微服务级功能和接口安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。

3.2.4 问：测试数据的来源是何处?是否会使用客户数据进行测试和 AI 训练等？

答：原则上不允许开发及测试环境使用生产环境数据。若有需要且合规的情况下，在生产数据用于测试环境前，需去除其中的认证凭证数据和保密的业务数据，并对生产数据中的个人数据进行匿名化处理。华为云坚持数据中立，绝不在未授权的情况下访问和使用客户数据。

3.3 交付与运维安全

3.3.1 问：华为云的哪些服务具备安全合规特性？

答：华为云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，同时也为致力于为客户提供先进、稳定、可靠、安全的产品及服务。客户可以参考华为云服务的安全特性页面，配置华为云服务以满足安全合规目标：

中国站：
https://www.huaweicloud.com/securecenter/security/security_features.html

3.3.2 问：华为云如何确保内部人员/运维人员不接触租户的数据？

答：华为云的管理区和租户资源区在不同的网络分区和网络平面，并且华为云会从 CPU、内存和 I/O 三个方面实现资源安全隔离，确保租户面和管理面隔离。华为云对接入平台的人员执行严格的权限访问控制，对云平台的操作也进行了严格的访问控制，只有授权人员才能在授权期间访问生产环境，并且现网的重大变更操作也需要通过评审才能实施。同时，华为云实施全面的运维运营操作审计机制，所有内部人员运维操作均将被记录，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。华为云承诺绝不会在未经授权的情况下访问租户的内容数据。

3.3.3 问：如何针对变更过程中的安全及隐私保护风险进行管理？

答：华为云会对所有变更进行风险分析，针对风险分析的结果实施不同的风险控制措施，保护变更过程中的安全与隐私。

3.3.4 问：在变更过程中哪些情况需要对租户进行通知？

答：华为云建立了成熟的变更机制与变更流程，变更根据对客户的影响情况分为四级。针对可能导致华为云系统不可用、客户业务工作无法进行或重大 IT 基础设施的变更评审时，华为云变更评审委员会会对变更方案进行网络安全和隐私风险审核，并向所关联的云客户提供评估后的相关信息，通过包括电话、短信、官网挂出公告等方式。

3.3.5 问：运维平台的访问控制策略（账号、权限及口令如何进行管理）？

答：华为云的运维主体在进行系统权限管理时，遵循职责分离、工作相关、合理授权和审批受控等原则，实施最小化授权。密码策略遵循行业标准。

3.3.6 问：账号、权限的定期清理和审视机制如何？

答：华为云建立了权限定期审阅机制，每月对运维管理平台内的用户权限/每季度对运营账号中心内的用户权限进行审阅。若发现异常，相关责任部门会跟进处理以调整账号权限。当员工离职或调岗时，其拥有的账号在指定时间内清除权限或账号。

3.3.7 问：针对基础设施的日志是如何进行采集、存储，并进行安全事件的监测、分析和响应的？

答: 华为云会通过日志大数据分析系统对日志进行快速收集、处理、实时分析，并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。

3.3.8 问：安全管理平台收集的日志的范围是哪些？是否会收集包括客户数据的日志？

答：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，用于检测相关性能指标，确保租户底层的设备运行正常。华为云的安全日志不记录敏感的个人数据，如日志中包含个人数据且与网络安全威胁直接相关且必要的信息，均视情况进行数据加密或匿名化处理。

3.3.9 问：在运维运营阶段，华为云有哪些优秀实践或产品可以帮助客户？

答：在 DevOps/DevSecOps 云服务流程中，运维运营与研发同等重要。华为云对运维运营尤为重视，在运维安全、漏洞管理、安全事件管理和业务连续性与灾难恢复管理等方面均有诸多具体实践。以运维接入为例，华为云通过数据中心部署的 VPN 和堡垒机，实现运维管理平台的统一运维管理和审计，并根据具体场景设置了不同的安全管控措施。客户可以通过《华为云安全白皮书》的“运维运营安全”章节获取更多信息。

另一方面，华为云基于经验和实践开发了各种运维，并开设相关的赋能培训课程，帮助客户实现运维安全和运维智能化。针对运维场景的产品推荐，客户可以访问运维运营安全页面进行了解：

中国站：https://www.huaweicloud.com/securecenter/operationsafety.html

3.3.10 问：华为云的漏洞管理策略是什么，华为如何保证漏洞及时修复、补丁及时安装？

答：华为云建立了多种收集漏洞信息的渠道，形成漏洞管理机制每年进行刷新，并配合自动化的漏洞扫描工具进行 7×24 小时的边界漏洞扫描和每月的内部管理面漏洞扫描。每个发现的漏洞均需根据漏洞 SLA 制定漏洞修复计划及漏洞修复时限，修复完成后由各部门研发负责对漏洞补丁进行测试。华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看安全公告以了解漏洞影响的范围，处置方式及威胁级别。对于重大安全漏洞，安全运维团队实现分钟级的受影响服务和模块的范围界定；同时会根据现网情况，采取必要的漏洞缓解措施，例如限制端口访问、实施 WAF 漏洞规则等方式对受影响的服务进行防护或隔离，以降低漏洞被利用的风险。

3.3.11 问：华为云的漏洞修复过程是否会对租户业务造成影响？

答：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。同时，华为云还持续更新操作系统及容器镜像，通过镜像和容器的滚动升级完成系统漏洞修复，不会对租户业务造成影响。

4 基础设施的安全与隐私合规

4.1 数据中心安全

4.1.1 问：华为云提供的基础设施足够安全吗？

答：华为云将基础设施安全视为构筑多维全栈的云安全防护体系的核心组成部分。为了让客户可以更放心地上云，并利用安全的华为云服务聚焦在业务发展上，华为云参考业界最佳实践在数据中心、网络等基础设施的设计和管理上充分考虑安全性与合规性。

华为云在数据中心机房建设和管理过程中，充分考虑机房选址、访问控制、监控措施以及数据中心业务连续性等，以保障华为云基础设施的安全性和可靠性。详细的数据中心安全设计和实践，客户可以访问数据中心页面了解：

中国站：https://www.huaweicloud.com/securecenter/security/datacenter.html

更多华为云基础设施的安全设计和实践，客户可以下载《华为云安全白皮书》了解。

4.1.2 问：数据中心的运营、运维安全如何保护？

答：华为云数据中心内所有基础设施均以 2N 原则冗余备件，以便满足基础设施快速扩容的需求，且华为云数据中心的容量规划应满足业务未来 5 年以上的需求。华为云通过系统对访问控制、消防系统、环境控制和物理安全进行监控，降低潜在安全风险。

数据中心的设备妥善安置且被保护，设置明显、不易去除的标识，对数据中心的环境参数也实时监控，当发现异常时实时告警，并通知相关责任体系处理。

4.1.3 问：如何保护终端资产如电脑、系统、软件的安全性？

答：华为云的办公电脑只允许安装经过公司允许的软件。因业务需要需要使用其他非标准软件时，必须经过公司杀毒软件扫描，同时禁止在办公电脑安装/使用任何盗版、破解软件。

华为云通过防病毒软件提供病毒防护及 Windows 系统内的防火墙；HIDS 主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。并且华为云终端设备均安装了

DLP 数据防泄漏软件，并由公司统一配置管理。华为云统一配置终端上的软件防火墙，普通用户无法修改。

4.1.4 问：网络安全相关的物理与环境安全的要求包括哪些？若数据中心为租赁模式，如何确保这些要求的落实？

答：华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，满足 GB50174《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。

以租赁模式运行的数据中心，华为云按照自建机房的标准对供应商提出要求，并把要求明确在与供应商签署的合同中，确保供应商按照要求提供服务。

4.1.5 问：访客或外部人员进出数据中心的权限申请流程如何？相关记录从何处获取？

答：华为云严格管理人员进出数据中心，访客仅可在审批通过后，由华为云工作人员全程带领访问数据中心的低保护区域、普通受控区等区域。访客禁止访问数据中心的信息系统，在需要访问特别受控区时，需要数据中心管理人员批准才可访问。数据中心访客记录指定专人负责每月定期审视。

一般情况下华为云不对外直接公开数据中心访客记录。如客户需访问华为云数据中心，请联系专属客户经理。

4.1.6 问：华为云怎样维护资产的安全？

答：华为云根据 ISO 27001 标准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。

4.1.7 问：资产在报废时如何处理其中的数据？

答：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。

4.2 平台安全

4.2.1 问：云基础设施的安全架构如何？

答：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、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，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。具体可参考《华为云安全白皮书》

4.2.2 问：逻辑上和物理上隔离生产环境和非生产环境？

答：华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段。生产环境与非生产环境之间采用物理和逻辑网络边界，生产与非生产环境员工职责分离，同时高度限制对云环境的物理和逻辑访问。

4.2.3 问：云基础设施的网络安全分区是如何划分的？

答：华为云根据业务功能和网络安全风险将数据中心划分为多个安全区域，实现物理和逻辑控制并用的隔离手段，提升网络面对入侵和内鬼的分区自我保护和容错恢复能力。云基础设施的网络安全分区分为：DMZ 区、公共服务区、资源交付区、数据存储区、运维管理区。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，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的 OM 区，攻击面最小，安全风险相对容易控制。

4.2.4 问：如何确保云平台管理面和租户面之间隔离/无法相互访问？

答： 为保证租户业务不影响管理操作，为保证管理操作和租户业务互不影响，华为云将其网络的通信平面基于不同业务职能、不同安全风险等级和不同权限需要划分为租户数据平面、业务控制平面、平台运维平面、等，以保证关乎不同业务的网络通信流量得到合理且安全的分流，华为云的管理区和租户资源区在不同的网络分区和网络平面。另外，华为统一虚拟化平台从 CPU、内存和 I/O 三个方面实现资源安全隔离。详细信息可参考华为云安全白皮书。

4.2.5 问：华为云如何确保租户之间的资源、网络、数据等得到有效的隔离？（租户之间无法相互访问）

答：华为云租户之间通过多层安全控制手段实现资源隔离。华为统一虚拟化平台 UVP 通过 CPU 隔离、内存隔离和 I/O 隔离等技术手段实现租户虚拟机资源安全隔离，租户不能访问其它租户的资源。同时，主机内由 Hypervisor 确保虚拟机在网络层的逻辑隔离，多台主机之间的网络依然使用传统的物理网络设备（路由器、交换机等）进行物理隔离。华为云对云端数据的隔离是通过虚拟私有云（VPC）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。详细信息可参见华为云安全白皮书。

4.2.6 问：租户资源到期、租户销户场景下，如何清除租户数据？

答：华为云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。

4.2.7 问：华为云如何确保虚拟机镜像在生命周期管理过程中的安全性和完整性不被破坏？

答：华为云对虚拟机公共镜像进行加密，并存储在安全的位置，同时对镜像实施访问控制等多种安全管控措施，以确保镜像的可用性、机密性和完整性。华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞，最终生成安全的公共镜像，并通过镜像服务（IMS）持续提供给租户。IMS 提供了安全的加密算法和功能，在基于镜像创建虚拟机时，系统会自动检查镜像完整性，以确保创建的虚拟机包含完整的镜像内容。同时提供相关加固和补丁信息以供用户对镜像进行测试、排除故障及其他运维活动时参考。

4.2.8 问：操作系统是否进行了安全加固？

答：华为云会根据行业标准和实际情况生成操作系统的安全基线，操作系统按照安全基线进行配置，仅提供必要的端口、协议和服务，以满足业务需求。另外，针对漏洞等其他情况，华为云按照既定的安全补丁管理流程，对操作系统进行修复，其中包含了基线的更新，确保基线的安全性。

4.2.9 问：华为云是否在所有系统上安装了支持或连接到云服务产品的防恶意软件程序？

答：华为云使用 IPS 入侵防御系统、Web 应用防火墙（WAF -Web ApplicationFirewall）、防病毒软件以及 HIDS 主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS 入侵防御系统可以检测并预防潜在的网络入侵活动；Web 应用防火墙部署在网络边界以保护应用软件的安全；防病毒软件提供病毒防护及 Windows 系统内的防火墙；HIDS 主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。

华为云向租户提供企业主机服务（HSS）、Web 应用防火墙服务（WAF）、威胁检测服务（MTD）、云防火墙（CFW）等服务来帮助其检测、预防和实施恢复控制以防止恶意软件。

4.2.10 问：在将物理服务器、应用程序或数据迁移到虚拟服务器时，是否使用安全且加密的通信通道？

答：华为云通过虚拟专用网（VPN）在传统数据中心与虚拟私有云（VPC）之间建立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。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。华为云服务使用 REST 和 Highway 数据传输，支持使用 TLS1.2 版本进行加密传输。

华为云提供多种服务帮助客户安全迁移数据。如主机迁移服务（SMS）、云数据迁移服务（CDM）等，同时云商店也提供了丰富的迁移服务。

4.2.11 问：当前针对 Web、API 及应用的安全攻击是如何进行检测和拦截的？

答： 华为云利用 API 网关结合 Anti-DDoS、入侵防御系统（IPS）、Web 应用防火墙（WAF）等多层高级边界防护机制针对不同的威胁和攻击进行有效防范，并通过负载均衡器对 TLS 加密传输进行解密，多层高级边界防护机制可对 API 网关流量明文进行监控，对攻击执行阻断。在高级边界防护的基础上，API 网关作为云服务特有的安全边界还提供包括 ACL 规则限制、防重放攻击等多种防护措施。详细内容可参考《华为云白皮书》

4.2.12 问：华为云是如何保证基础设施的高可用的？

答：华为云按照业界最佳实践，在全球各地部署了多个数据中心，同时两地互为灾备中心如一地出现故障，系统在满足合规政策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。

华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划并定期对其进行测试。该计划主要针对重大灾难，如地震或公共健康危机等，让云服务能够持续运行保障客户的业务和数据安全。

4.2.13 问：平台的业务连续性相关证书从何处获取?

答：中国站：客户可以从华为云官网的“信任中心-合规证书下载”进行下载。具体链接：

中国站链接：https://www.huaweicloud.com/securecenter/compliance.html

4.2.14 问：平台通过提供哪些服务或能力保障租户账户的安全？

答：华为云通过统一身份认证服务（IAM）服务保证租户的账户安全，详细可浏览华为云 IAM 产品介绍页面。

4.2.15 问：华为云通过什么方式为租户提供数据加密服务？

答：华为云提供数据加密服务（Data Encryption Workshop）是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等服务，安全可靠的为客户解决了数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与多个华为云服务集成。具体详情可参考

中国站：https://www.huaweicloud.com/product/dew.html

4.2.16 问：平台如何通过 KMS 系统为租户分配密钥的？

答：用户通过华为云服务加密数据时，需要指定一个 KMS 用户主密钥。华为云服务会生成一个明文的数据加密密钥和一个密文的数据加密密钥，其中密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。华为云服务使用明文的数据

加密密钥来加密数据，然后将加密后的密文数据与密文的数据加密密钥一同存储在华为云服务中。

4.2.17 问：华为云怎样实现租户需要的审计功能？

答：华为云通过云日志服务（LTS），云监控服务（CES），云审计服务（CTS）等服务为租户提供审计功能，租户可以按需使用。

4.2.18 问：安全事件的处理流程是什么？

答：华为云有一套成熟的安全事件处理流程，如在发现事件时，第一时间进行处理，如事件影响到客户，华为云会专人通知客户并和客户沟通确认解决方案，确保对租户的影响减到最少。

4.2.19 问：是否会定期对安全事件响应计划进行测试？

答：华为云每年会对安全事件的响应计划进行测试。

4.2.20 问：如果客户的企业要实现业务上云，客户应该如何做才能保障其安全性？

答：中国站：在云服务模式下，华为云致力于保障其提供的 IaaS、PaaS 和 SaaS 各类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， 作为客户，客户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的关键节点采取相应的安全措施。

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。

客户可以通过华为云《企业上云安全白皮书》详细了解上云安全建设过程中客户具体需要做什么以及如何做（https://res-static.hc-cdn.cn/cloudbu-site/china/zh-cn/TrustCenter/WithePaper/Enterprise_Cloud_Adoption_Security_WhitePaper.pdf）。此外，客户也可以查看华为云的上云安全建设实践以了解有哪些服务和方案可以帮助客户快速实现业务安全上云：
https://www.huaweicloud.com/solution/sag/enterprise-cloud-security-overview.html

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的关键节点采取相应的安全措施。

4.2.21 问：除了云自身的安全保障，客户还可以选择哪些安全服务提高云上业务的安全性？

答：中国站：华为云基于多年安全经验，以数据安全为核心，开发了一系列多维立体、纵深防御的软硬一体化的安全服务。

客户可以在安全服务页面找到帮助客户管理系统安全态势的产品，如态势感知 SA，威胁检测服务 MTD；客户也可以找到如企业主机安全 HSS、云防火墙 CFW 等保护客户云中负载和应用服务的产品。此外为了保护客户的云上数据资产，华为云研发了非常多的数据安全产品，如数据安全中心 DSC、数据加密服务 DEW 等。在协助客户实现安全合规方面，华为云提供了如管理检测与响应 MDR、等保安全解决方案等服务。

通过这些安全产品和安全解决方案的加持，结合华为云自身的安全保障，客户可以快速构建一个完整的云上安全体系。

4.2.22 问：如果客户云上的业务要满足安全合规，客户需要做什么？

答：在云服务模式下，云服务提供商（CSP）和云客户基于责任共担模型进行安全合规云环境的构建。即华为云负责云服务自身的安全合规遵从，客户和客户的企业负责云服务内部的安全合规遵从。

华为云关注内外部合规要求的变化，遵从华为云服务自身适用的法律法规，开展所服务行业的安全标准评估，并且向客户分享华为云的合规实践，保持应有的透明度。

作为云客户，对于客户企业自行部署于华为云上、不属于华为云提供的各项应用和服务，客户需负责遵从其适用的法律法规，并自行开展所服务行业的安全标准评估。

关于华为云已通过的认证、遵从的法律法规以及合规实践指导，客户可以访问合规中心以及安全合规相关资源中心了解更多。

中国站：

1、合规中心：
https://www.huaweicloud.com/securecenter/compliance/compliance-center.html

2、安全合规相关资源中心：
https://www.huaweicloud.com/securecenter/resource.html

nter/resource.html

历史版本

日期	版本	描述
2023 年 5 月	1.0	首次发布

