腾讯云数据安全白皮书

2017 年 12 月

【服务声明】

2017年12月

本文档仅供参考。对于本文档中的信息，腾讯云不作明示、默示的保证。本文档基于现状编写。在本文档中的信息和意见，包括网址和其它互联网网站参考，均可能会改变，恕不另行通知。您将承担使用它的风险。

本文件未授予您任何腾讯产品的任何知识产权的法律权利。您可以复制和使用本文档内容作为您内部以参考为目的的使用。

这里所描述的一些例子只提供说明，是虚构的。不能基于此推断或预期任何事实上的关联或联系。

腾讯云，打造云端数据安全新时代

目录

图表目录

概要

随着云技术的日趋成熟，越来越多的企业将业务部署到云环境上运行，以获取更灵活的资源调配、扩展能力，从而更快速高效地部署业务，优化投资成本。与此同时，数据的重要性与日俱增，因此数据安全成为客户在选用云服务时的重大考量之一。但是，将数据托管于云端真的比传统的本地存储更不安全吗？答案是否定的。在腾讯云，客户对其托管于云端的数据拥有完全的控制权，腾讯云承诺绝不主动触碰客户数据。客户不但可以如同传统数据中心一样对数据采取访问控制、加密存储等数据保护措施，而且可以充分利用腾讯云提供的多层次全方位的数据安全保障，为云端数据保驾护航。

客户数据的定义

客户数据指客户因使用腾讯云服务而存储在腾讯云服务器当中的内容，包括但不限于数据、文本、音频、视频或图像等。

凭借腾讯集团多年的安全经验和积累，腾讯云为云平台搭建了强大的纵深安全防御体系，数据安全一直是其中至关重要的一环。腾讯云将数据安全的理念融入每一个产品的需求设计和开发过程中，并贯穿产品运营的每一个环节。腾讯云的安全保护和控制流程，例如数据分类标准、访问控制策略、IDC 机房安全控制等安全内控标准，均已经通过 CSA STAR、ISO 27001 等多个权威第三方独立安全评估的验证。

秉承腾讯“一切以用户价值为依归”的经营理念，腾讯云在保障云平台安全的同时，亦通过赋能客户全力协助腾讯云用户保障其云端数据的安全。为了方便客户更好地保护云端的数据，腾讯云提供了以数据为中心的一站式数据安全解决方案，以帮助客户实现云端数据的机密性、可用性和完整性，从而保障客户业务的正常运作。

为了积极响应 2017 年 6 月 1 日全面实施的《网络安全法》，腾讯云于 2017 年 6 月 3 日率先宣布获得网络安全等级保护（云等保）重要资质，成为《网络安全法》正式实施后首家通过云等保四级测评的云服务商。这意味着腾讯云可以提供金融级的高质量安全服务，帮助用户满足新法规下的严格合规要求。着眼数据安全领域，腾讯云始终以金融级数据安全为标杆，全力打造云端数据安全的新时代 。

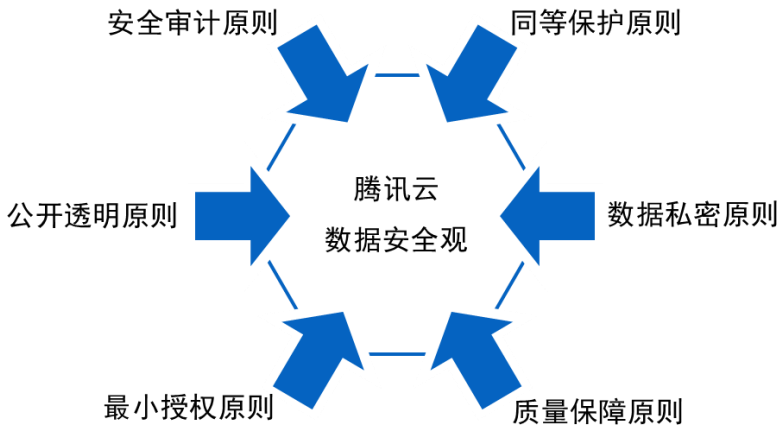
腾讯云数据安全观

数据保护承诺

数据是客户的重要资产，腾讯云承诺绝不主动触碰客户数据。腾讯云在《腾讯云服务协议》中明确声明“未经客户授权，腾讯云公司不得访问客户存储在腾讯云中的内容。但是，腾讯云公司可以在事先获得客户授权的前提下，访问客户的存储内容，以便客户顺利使用腾讯云服务。”在此数据保护承诺的基础上，腾讯云将数据安全的理念融入产品生命周期的各个环节，并指引腾讯云一路打造客户值得信赖的云服务。

数据保护六大原则

为了更好地践行腾讯云的数据保护承诺，腾讯云在数据保护的过程中谨遵“同等保护原则”、“数据私密原则”、“质量保障原则”、“最小授权原则”、“公开透明原则”、“安全审计原则”六大原则，并将这六大原则贯穿于腾讯云数据安全实践的每一个环节。



图表 1 腾讯云数据保护六大原则

同等保护原则

腾讯云在对云端数据进行保护时，因为并不知道客户在云端存储了什么类型的数据，所以对云端所有的客户数据，无论是企业用户还是个人用户的，都会采取相同的且最高级别的安全控制措施，以最大限度地保障每一位客户的数据安全。

公开透明原则

腾讯云秉承公开透明的原则，承诺客户有权利了解数据存储的位置以及使用程度等信息，包括但不限于：

- 数据存储在哪些数据中心，数据存储所在数据中心的地理位置；
- 数据有几份拷贝，是否有冷备份，备份的数据存储的数据中心位置；
- 数据位置是否可选，如果可选，可选的方式；
- 告知客户数据中心所在地的数据安全相关法律；
- 客户数据的使用人和使用的数据类型。

数据私密原则

客户数据在腾讯云内部属于最高安全级别的数据。在腾讯云，客户数据的控制权完全归客户所持有。腾讯云承诺，除非以下情况，腾讯云内部员工绝不会主动触碰任何客户数据：

- 因提供服务或排错的需要，并经过客户明确授权；
- 国家或地方政府部门关于犯罪事件的调查等符合国家法律法规的情况。

与此同时，腾讯云承诺通过有效的隔离手段，保证同一资源池内客户数据互不可见，从技术上保证租户不能访问、获取或篡改其他租户的数据。

质量保障原则

腾讯云为客户所购买的云服务制定了详细的服务等级指标，并向客户承诺通过各种安全控制措施和技术保障手段提供高可用性和高持久性的数据服务。腾讯云在服务等级协议（SLA）中明确了服务可用性和持久性等指标。如果腾讯云未能满足服务等级协议中约定的服务保障，则腾讯云会按照该服务等级协议向客户承担补偿责任。如果客户对可用性的要求高于 SLA，客户可主动对自身系统进行高可用性的设置，腾讯云公司将给与必要的协助。

最小授权原则

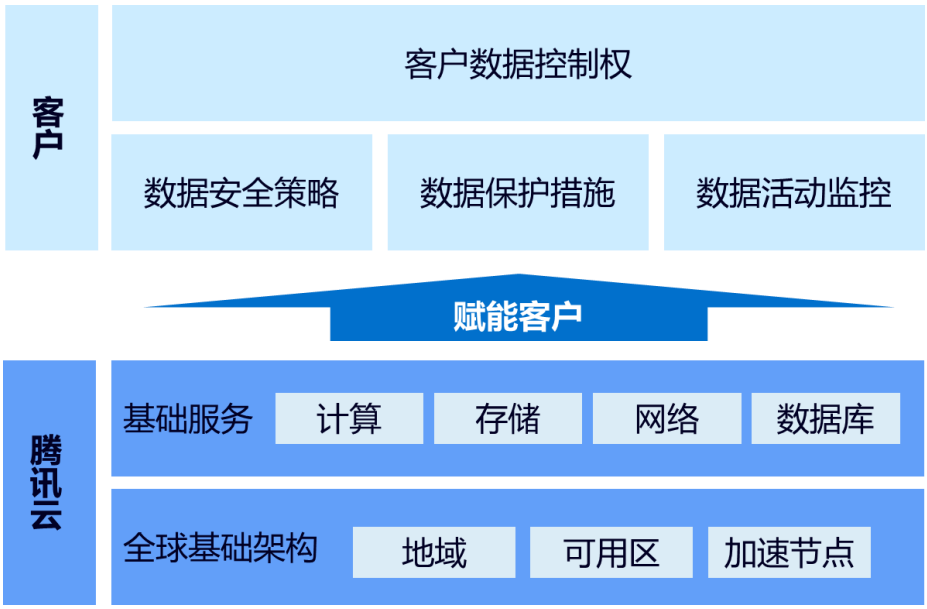
腾讯云遵循权限最小化原则，只在客户授权范围内赋予内部员工为提供相应云服务所必需的最小的操作权限，非授权范围内的数据活动必须进行严格的授权审批。腾讯云从内部管理制度和自动化、工具化的运维管理平台层面双管齐下，杜绝客户数据非授权访问情况的发生。

安全审计原则

腾讯云对数据活动中的任何操作都进行相应的记录并且对日志信息采取严格的保护措施，确保所有的数据操作可以被追溯和审查。在安全审计方面，腾讯云凭借在大数据分析和人工智能领域的先进技术，开发了自动化审计工具，用于发现明显异常操作并及时响应。同时，由安全专家组成的审计团队根据定制化的云安全控制活动项和实践经验亦会定期进行数据安全审计。

云端数据保护职责划分

云服务依托虚拟化技术，以资源共享的形式为客户提供其所需的网络、存储和计算能力等各种资源，从而帮客户节省巨额的运营成本。正是基于云服务架构的特殊性，如何厘定云服务提供商和云服务客户之间的安全职责界限是云安全的重要基础。腾讯云在《腾讯云安全白皮书》中详细介绍了腾讯云信息安全责任共担模型。就数据安全而言，客户对其托管于云端的数据拥有完全的控制权，并负责自身云端业务数据的安全管理，包括收集与识别、分类与分级、权限与加密等。因为腾讯云不知道客户在云中存储了何种数据，腾讯云在保障底层云平台安全的同时，通过提供全方位多样化的数据安全功能、工具和控制赋能客户，携手客户一起为云端数据构建更好更完善的安全保障体系。



图表 2 云端数据保护职责划分

客户的责任

正因为数据是客户的重要资产，在云中存储哪些数据，是否对数据进行加密，谁可以访问特定数据以及需要哪些凭证，是否需要按照业务需求进行数据备份，这些数据安全相关的控制措施的决定权均在客户手中。客户可以自行配置腾讯云提供的数据加密手段、访问管理功能、用户验证机制、数据备份与恢复工具等，以确保其对云端数据的保护满足业务和合规的要求。

腾讯云的责任

腾讯云负责云平台的安全，并协助客户保障其云端数据的安全。为了更好地保护客户托管于云端的数据资产，腾讯云从平台层和赋能层两个层面为云服务客户提供双重保障。平台层提供的保障全面覆盖数据安全事前防范、事中保护和事后追溯三个阶段，而赋能层则围绕数据全生命周期给出一站式的解决方案供客户选用，以帮助客户最大程度地降低在流程、技术以及合规方面的数据安全风险。腾讯云凭借腾讯在数据保护领域多年的经验，倾心打造了智能化一站式的数据安全解决方案 —— 数盾，赋能客户为数据全生命周期保驾护航。在此双重保障的基础上，腾讯云亦满足多方行业合规要求并符合云计算领域的多项安全认证，从严苛的第三方监管的角度保障了客户数据的安全。

图表 3 腾讯云数据安全模型

云平台数据安全保障

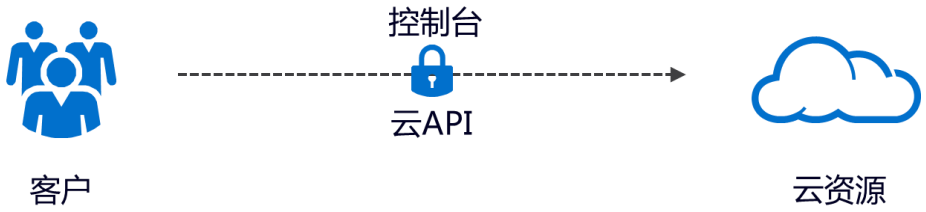
毋庸置疑，云端数据的安全离不开一个安全可靠的云平台环境。围绕以高速（speed）、稳定（stability）、安全（security）为竞争核心的 3S 品牌理念，腾讯云一直致力于按照服务等级协议的约定条款为客户提供安全、稳定、持续、可靠的网络、存储和计算能力等各种资源及安全保障，并持续提升云平台的安全服务能力。为了给数据安全提供充分的保障，腾讯云紧紧围绕事前防范、事中保护和事后追溯三个阶段，努力为客户数据打造一个安全可靠的底层平台。

事前防范

数据保护必须防患于未然，因此事前防范是数据保护中最为关键的一环。腾讯云内部建立了完善的数据分类分级标准，所有数据在创建时均按照该标准进行统一的分类分级。客户数据在腾讯云内部属于“绝密数据”，即最高安全级别的数据。出于对客户数据的高度重视，腾讯云在人员、流程、技术上层层把关做好事前防范工作，从源头上确保客户数据的机密性、可用性和完整性。

数据机密性

客户可以通过控制台和云 API 两种方式轻松访问及管理其购买的腾讯云产品和服务，例如上传一个新的文件到云端对象存储，或者创建一个云数据库实例。



图表 4 客户访问云资源过程中的数据机密性保障

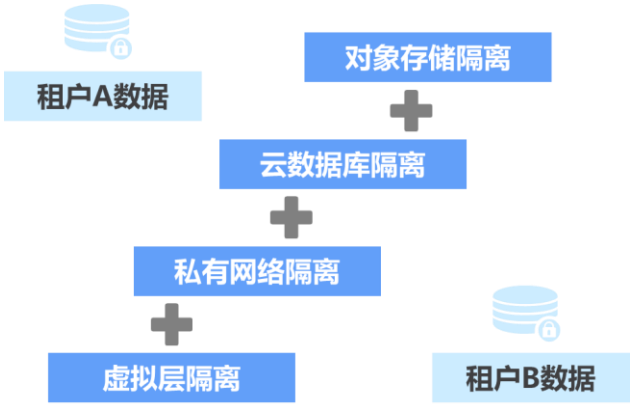
当客户通过自己的浏览器访问腾讯云控制台时，所有通过互联网的信息传输均经过 HTTPS 加密通道，采用 SSL/TLS 协议防止数据在传送过程中被窃

取、篡改，杜绝网络运营商的流量劫持、网页植入广告现象，同时有效抵挡中间人的攻击，大大提升数据的机密性。

与此同时，为了方便客户更加快速、高效、灵活地在云平台进行操作，腾讯云亦提供了云 API 供客户选用。除了使用云 API 直接请求，客户也可通过 SDK 或命令行工具调用云 API，以接口的形式访问并管理其腾讯云账户内的各类资源。类似地，客户通过云 API 与腾讯云之间的通信均支持 HTTPS 数据加密传输协议。

对于腾讯云内部的员工，除非客户所选取的服务需要处理客户的数据，腾讯云员工不会尝试访问任何客户数据。当腾讯云员工有需要访问客户数据时，因为腾讯云的内部办公网络和客户数据所在的生产环境完全隔离，腾讯云的运维员工必须经过堡垒机方可访问客户数据所在的生产环境，且所有运维账号均配备双因素认证机制。在授予权限时，腾讯云通过细颗粒度的权限划分确保只授予员工提供相应服务所需要的最小权限，所有额外权限的申请均需要经过多级的评审和批准。通过严格的内部管理制度配合自动化、工具化的运维管理平台，任何腾讯云内部人员在未获得客户的同意与授权时均无法触碰客户的云端业务数据。此外，腾讯云凭借其多年的运维管理经验，搭建了严格的权限职责分离矩阵，以避免冲突的权限被划分给同一员工。

当然，使用云服务与传统的第三方托管服务一项显著的区别在于云服务是基于资源池的，不同的云服务客户共享资源池内资源。因此，云租户之间的数据机密性保障也尤为重要。腾讯云谨遵“数据私密”的原则，通过多层次的技术隔离手段，保证同一资源池内客户数据互不可见，从技术上保证租户不能访问、获取或篡改其他租户的数据。



图表 5 腾讯云租户之间的数据机密性保障

虚拟层•数据私密保障：腾讯云应用成熟的硬件虚拟化技术在虚拟层为云服务器等资源提供完整的租户间虚拟资源隔离能力，不同用户的网络、内存、磁盘等资源均通过底层逻辑访问控制杜绝了互通互访的可能性，确保每位用户只能访问其已购买的云计算资源，有效实现多用户之间的数据隔离。

网络ACL和安全组

- 网络ACL是一个子网级别无状态的可选安全层，用于控制进出子网的数据流，可以精确到协议和端口粒度。
- 安全组是一种有状态的包过滤功能的虚拟防火墙，它用于设置单台或多台云服务器的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。

私有网络•数据私密保障：私有网络 VPC（Virtual Private Cloud）是在腾讯云上建立的一块基于 GRE 封装的逻辑隔离网络。客户可以在 VPC 内自定义网段划分、IP 地址和路由策略等，并通过网络 ACL 和安全组分别从子网和主机维度筛选流量，可精确到端口和协议维度，通过完全的网络隔离确保不同客户之间的数据隔离。

云数据库•数据私密保障：在客户使用云数据库时，腾讯云通过配置防火墙策略，采用白名单过滤机制对网络层进行了隔离。此外，腾讯云通过对数据库实例的权限控制机制来保证每个用户只能获取他对应的数据，而无法看到其他用户的数据。为了进一步满足资源独享、物理安全、行业监管等更高的需求，腾讯云还提供独享集群数据库，可以让客户独享物理集群资源，并灵活创建多种自定义规格的云数据库。

安全提示

密钥是构建腾讯云请求的重要凭证，并由客户自行管理。为了保障客户的财产和服务安全，腾讯云建议客户妥善保存和定期更换密钥，当密钥更换后，请及时删除旧密钥。

对象存储•数据私密保障：对象存储服务通过 bucket 的方式来组织对象数据。Bucket 中的对象的创建、操作请求，都需要用 bucket 所属用户的密钥计算得到一个签名，通过签名来校验请求的合法性和完整性。此外，用

户可以自行将 bucket 中的对象数据的访问读取权限设置成公有读或私有读。被设置为私有读对象的访问，亦需要签名校验。

专用宿主机

专用宿主机可以让客户以独享宿主机资源方式购买、创建云主机，以满足客户的资源独享、安全、合规需求；购买专用宿主机后，客户可在其上灵活创建、管理多种自定义规格的独享型云主机。

为了帮助诸如金融行业的客户满足数据安全方面的特殊要求，腾讯云同样提供多种私有云或混合云的解决方案，客户可以购买独享宿主机资源的云产品或直接购买基于云环境的物理服务器，进一步保障云端业务数据的机密性。

黑石物理服务器

黑石物理服务器是一种按需购买、按量付费的物理服务器租赁服务，为客户提供云端专用的高性能、安全隔离的物理集群。

作为数据机密性保障的最后环节，腾讯云提供安全可靠的数据销毁机制。所有数据收集和处理的过程中产生的内存临时数据，腾讯云均会不可撤销地将其自动清除。当客户主动从腾讯云中将数据删除时，该部分数据会呈现为无法读取状态。腾讯云在进行资源再分配之前会遵循标准策略及合同要求及时进行严格的逻辑擦除或物理擦除，从而保证客户的鉴别信息、文件、目录、数据库记录等敏感信息所在的存储空间被及时释放或再分配给其他用户前得到完全清除。

当客户不再使用腾讯云服务时，根据腾讯云与客户达成的服务协议，如腾讯云服务到期或终止，对于客户因使用腾讯云服务而存储在腾讯云公司服务器中的数据等任何信息，腾讯云公司将为客户保留 15 天（简称“保留期限”），客户需在保留期限届满前完成全部数据的迁移。保留期限届满后，腾讯云服务系统将自动删除包括副本和备份在内的所有客户数据，删除后的所有数据无法复原。

当用于提供腾讯云服务的介质出现故障需要更换或者到达使用期限需要报废时，腾讯云将及时清除剩余信息，并交由消磁中心按照行业标准做法对存储介质进行消磁，密封存放两年之后再进行彻底的物理销毁。

数据可用性

对于客户存储于云端的数据，腾讯云采用数据实时热备、冗余存储、异地备份等方式来保障客户存储于云中的业务数据安全可靠，持续可用。腾讯云承诺所有云产品的业务可用性不低于 99.95%。

目前腾讯云在全球 21 个地理区域内运营着 36 个可用区，且计划陆续上线更多地域和可用区，为更多企业和创业者提供集云计算、云数据、云运营于一体的全球云端服务体验。

地域是指一个独立的地理区域，腾讯云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了便于就近读取数据，同时满足数据限制出境方面的合规要求，客户在购买腾讯云产品时，可以通过控制台轻松指定其所希望的数据存储的国家或地区。未经客户授权，腾讯云绝不会将数据转移出客户所选择的国家或地区。在全球化扩张的进程中，腾讯云谨遵“合规性和云服务发展并重”的理念，严格遵循全球各地数据保护相关的法律法规，帮助客户构建和运行安全合规的云生态环境。

图表 6 腾讯云全球基础设施

为了保证数据的高可用性，腾讯云将每个地域再分隔成多个相互隔离的可用区。可用区是指腾讯云在同一地域内电力和网络互相独立的物理数据中心，同一地域下的可用区通过低时延的内网链路相连。多可用区的设计能够有效降低单点故障的影响，保证可用区间故障相互隔离，进而为客户的业务连续性提供保障。

除了多地域多可用区的设计，腾讯云还具备极好的业务连续性管理能力。腾讯云在 2016 年 3 月获得了 ISO 22301 国际认证，成为国内首批通过 ISO

22301 认证的云服务商。腾讯云根据自身的运作特点，充分考虑云计算环境下体系实施的复杂性，设计和推行适合于腾讯云的业务连续性管理框架，大大提高了腾讯云的体系实施和管理水平，完善了适合于互联网运作模式的业务联系性管理流程制度和预案。

金融云

腾讯云针对不同的金融机构要求，匠心打造了三大金融云模式：公有云、金融专区和金融专有云。每一种金融云模式都符合金融监管机构的安全合规要求。

有关金融云的更多信息，请参考腾讯云官网的金融解决方案。

此外，腾讯云向不同垂直行业的客户提供优质的行业解决方案。腾讯云非常重视金融行业客户在数据备份与恢复方面的合规要求，腾讯金融云同时具备两地三中心、同城双活、异地备份等数据备份与恢复的能力。金融云所采用的分布式金融级数据库，兼容 MySQL，且针对金融类业务设计，具有数据强一致、异地自动同步、万级 QPS 高性能、自动扩容、灵活智能恢复等优势。网络层面，金融云采用 BGP 多线网络，可以实现秒级切换，确保快速的故障恢复能力。

数据完整性

腾讯云在服务等级协议中对数据存储的持久性，即合同期内数据保存不丢的概率，进行了明确的定义。以对象存储为例，腾讯云承诺对象存储服务的持久性高达 99.999999999%，远高于行业水平。

腾讯云在存储数据时采用多副本冗余存储和纠删码技术，在检测到完整性错误时立即采取必要的恢复措施，大大提高了数据的容错能力。同时，腾讯云提供专业团队 7x24 小时的运维服务，借助先进的服务器监控与诊断技术，能自动发现服务器的各类故障，并在第一时间自动触发修复流程，通过整合先进的远程管控工具，自动调度数据中心现场以及厂商资源，及时恢复服务器故障。

签名信息

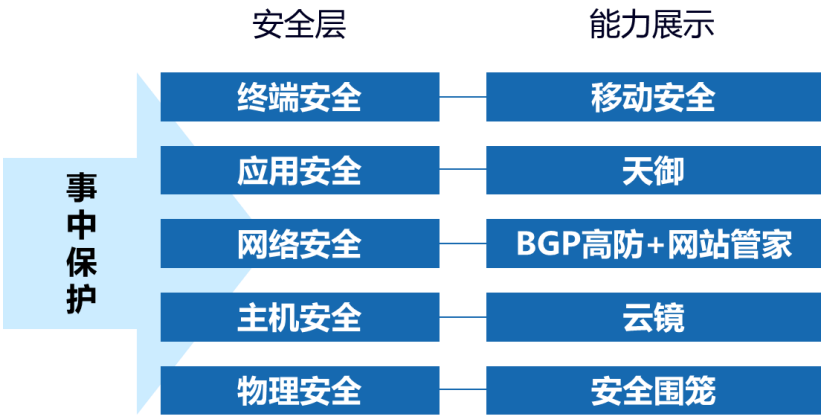
签名信息由用户所执有的安全凭证生成，安全凭证由 SecretId 和 SecretKey 组成，客户可以通过控制台自行申请安全凭证。

- SecretId:用于标识 API 调用者身份;
- SecretKey:用于加密签名字符串和服务器端验证签名字符串的密钥。

此外，腾讯云 API 的每个请求都需要在公共请求参数中包含签名信息以验证用户身份，同时保证请求的完整性。

事中保护

为了确保客户在使用云服务的过程中，客户数据受到实时的保护，并及时发现潜在的数据安全事件，腾讯云在云平台的各个层面精心部署了全面的安全防护，并将腾讯云自身的事中保护能力转化为客户能够感知和应用的云安全产品，以帮助云用户快速高效地部署云端安全防护。



图表 7 腾讯云数据安全事中保护能力框架

物理安全

秉承“同等保护”的原则，腾讯云致力于为每一位客户提供安全、稳定、持续、可靠的物理设施基础。腾讯云依据数据中心相关的国际标准和监管要求，建立了一套全方位的数据中心安全管理体系，并定期进行严格的内外部审计，通过持续改进来保证云计算数据中心的物理和环境安全。特别地，为了帮助金融行业客户满足特定的合规要求，腾讯云从物理安全层面为客户配备了额外的防护措施。腾讯云金融专区的物理机房属于GB50174-A 类机房，通过专用围笼将不同客户的设备进行物理隔离，并且配备生物识别门禁系统和 24 小时视频监控系统，能够有效防止非授权人员接触客户的设备。

主机安全

在主机安全层面，腾讯云拥有自研的安全组件对所有宿主机进行加固，并通过木马检测、漏洞扫描及修复等措施第一时间对云平台上的恶意代码进

行检测和清除。与此同时，腾讯云主机安全防护产品“云镜”重点关注云主机自身遭受的黑客攻击行为，利用云控制台的展示功能，让客户更加直观地了解其部署的云产品中存在的如暴力破解、Webshell 攻击等异常行为。云镜基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异地登录提醒、木马文件查杀、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系，防止数据被窃取或泄露。

网络安全

在网络安全层面，腾讯云通过成熟的网络安全架构，包含防火墙、分布式防护、入侵防御、Web 应用防护等多重防护机制，应对来自互联网的各种威胁。腾讯云推出的高达 300G 的“BGP 高防（大禹）”服务利用机器学习与人工智能方式实时监控并分析各类流量信息，帮助客户抵御 DDoS 攻击的挑战。

此外，腾讯云拥有完善的云计算安全漏洞挖掘和漏洞分享机制，覆盖虚拟层、系统层和应用层的漏洞信息。腾讯云安全研究团队将漏洞防护能力以虚拟补丁的方式整合入腾讯云的 Web 应用防火墙系统中，确保云计算平台整体的安全性。腾讯云亦将这种 Web 安全防护能力整合成了安全产品“网站管家（WAF）”，帮助客户通过 Web 入侵防护、0Day 漏洞补丁修复、恶意访问惩罚、云备份防篡改等多维度防御策略全面防护客户自身网站的系统及业务安全。

应用安全

更多应用安全服务

除了业务安全服务“天御”，腾讯云亦提供多样化的风控安全和内容安全服务，包括借贷反欺诈、金融级身份认证、文本识别、图片鉴黄等。

如欲获取有关应用安全服务的更多信息，请参考腾讯云官网的相关介绍。

依托腾讯在 QQ、微信等应用安全方面的丰富经验，腾讯云提供的所有 SaaS 产品设计、开发、发布、配置和使用的每一个环节都经过严格的安全管理。为了助力腾讯云 IaaS 和 PaaS 的用户，腾讯云应用安全产品“天御”通过标准的接口和简单的开发，帮助客户云端应用快速获得多种业务风险场景下的安全保障。天御将腾讯云的大数据存储挖掘、数据实时计算和对

外接入三大技术能力全面整合，提供注册保护、登录保护和活动防刷等多种防护功能，确保应用系统中的各类异常行为特征都能被及时发现和响应。

终端安全

随着移动终端的日益普及，腾讯云提供了移动安全一站式解决方案，涵盖应用加固、漏洞扫描、盗版监控、真机测试、质量跟踪、安全支付等服务。除了传统的终端安全保护，腾讯云移动安全可帮助客户防止应用被盗版破解，及时发现应用漏洞，监控应用正盗版分发等，有效捍卫移动应用所有者利益。

事后追溯

应急响应

专家服务

依托腾讯集团多年积累的安全响应和黑产对抗经验，腾讯云提供安全咨询、渗透测试、应急响应三大专家服务，帮助客户解决上云前、上云中和上云后的各种安全疑虑。其中的应急响应服务可以在客户系统遭受木马病毒、数据窃取、服务停止等黑客攻击事件时，由腾讯安全专家提供专业的入侵原因分析、业务损失评估、系统恢复加固、以及黑客溯源取证的安全服务，减少因黑客入侵带来的损失。

依托腾讯安全应急响应中心强大的发现和处理安全漏洞、黑客入侵的能力，腾讯云制定了详细的数据安全应急预案并提供 7*24 小时的全天候安全运维响应，捍卫腾讯云用户的云端数据安全。腾讯云安全运维团队在监测到数据安全事件后，会立即启动响应机制，并进行多维度的预警和防御。针对任何数据安全事件，腾讯云安全团队携手腾讯电脑管家会持续在全网布控监测事件的最新进展，通过“云+端”的联动形成立体防御体系。

此外，在发生数据泄漏、丢失或攻击事件后，腾讯云会第一时间告知用户，并提供相应的应急方案和技术支持，以协助用户采取补救措施以将损失降到最低，同时可以为用户提供突发安全事件分析报告和安全状况分析报告，以消除用户的后顾之忧。

日志审计

腾讯云凭借在异常行为监控方面多年累积的经验建立了完善的规则库，对于数据的异常使用会自动触发实时告警。腾讯云亦设定了详细的运维安全责任“红线”，并定期开展内部的运维安全审查。为了确保所有生产环境内的操作可以被控制和追溯，所有后台运维操作记录均被详细地记录且由日志平台集中存储，由腾讯云内部审计团队定期对记录信息进行审核。由安全专家组成的审计团队根据定制化的云安全控制活动项和实践经验，对运维过程中的可疑操作进行问题排查与追溯。

赋能客户 共建云端数据安全新时代

基于云服务的特殊性，如何保障托管于云端数据的安全是每一个云服务客户极度关心的问题。客户在使用腾讯云服务的过程中，可依据自身的安全需求和合规要求选择相应的数据保护措施。但是，随着数据规模的增加，我们看到单点布防的传统数据安全往往已经不能满足大数据时代的安全发展需求。为了不断倾听和满足用户需求，引导并超越用户需求，赢得用户尊敬，腾讯云结合腾讯十余年数据保护方面的经验和数百腾讯业务的数据保护优秀实践，由数千人团队匠心打造了智能化一站式的数据安全解决方案 —— 数盾。

图表 8 一站式数据安全解决方案 - 数盾

作为一套“以数据为中心的审计和保护 DCAP（Data-Centric Audit and Protection）”方案，数盾不仅能针对数据生命周期内的创建、存储、传输、访问、使用和销毁等每个阶段，应用不同安全防护，还能通过密码加密、大数据动态加密、身份管理、认证管理、授权管理、实时防护、审计预警等功能的实现，配合腾讯云全流程安全生态环境，提供系统化的安全防护。此外，数盾还独创六把钥匙端对端验证机制，拥有提供 PB 级大数据处理能力、千亿级访问请求审计能力，并全套配备了 API 和模块组件，使得丰富的保护能力和架构能简快速接入，经过简单配置即可投入使用。

数据创建

客户在数据上云之前，往往面临一个很大的问题就是对敏感数据的探知不够深入或者缺乏完善的数据分类分级标准。腾讯云建议每一个客户对其云端数据进行完整的风险评估。对于识别出的重要或敏感数据，客户可以按需要选择额外的数据保护措施。在客户授权并提供访问入口的前提下，腾讯云在数据创建阶段提供敏感数据发现和数据分类分级服务，帮助客户做好数据保护的第一环节。

敏感数据发现

结合腾讯在大数据分析方面的经验以及不同行业的敏感数据发现规则，腾讯云的敏感数据发现服务借助自研扫描工具对客户的数据资产进行自动感知，准确识别网络、磁盘文件、数据库里留存的个人身份信息、组织文档、知识产权等敏感数据资产。该服务可同时分析结构化数据和非结构化数据，帮助客户识别敏感数据，保证数据的可见性，避免了客户从海量的数据中自行筛选敏感数据的繁重工作。

数据分类分级

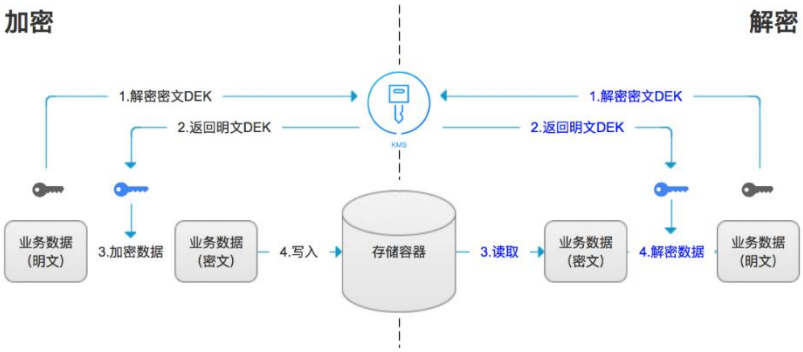
数据分类分级是数据保护的重要基础。基于敏感数据发现的结果，腾讯云可以帮助客户进一步分析数据间的关系，输出数据分类和风险定级的信息，并推荐数据分类分级的架构方案给客户。

数据存储

对于存储状态下的数据，腾讯云建议客户按照数据分类分级的结果，对于识别出的重要或敏感数据应采用更严格、更安全的保护措施，如数据存储加密、数据库表加密等。作为数据安全保护的最基本防线，存储加密可以显著提升拖库者的破解门槛，进而保护数据的机密性。腾讯云数盾依靠腾讯数十亿 QQ、微信账号数据加密的经验，为业界提供设计上过硬、实现上可信的密钥管理服务和数据加密服务。

密钥管理服务

若客户选择对业务数据进行加密，密钥管理往往是整个数据加解密过程中最关键也最繁琐的一步。基于此考虑，腾讯云提供密钥管理服务 KMS（Key Management Service）以帮助客户管理及备份其加密密钥，保障密钥全生命周期的安全。客户可以使用 KMS 创建用户主密钥，并通过该密钥再次加密业务使用到的数据密钥或其它密码、证书或配置文件等敏感数据。与传统密钥管理解决方案相比，腾讯云的密钥管理服务不但大大简化了密钥调用的流程，而且更加安全可靠，可以帮助客户更好地专注于数据安全的开发。



图表 9 KMS 加密案例示意图

数据加密服务

多种加密算法

腾讯云数据加密服务支持符合国家和行业标准的数据加密算法，包括：

- 对称加密算法：SM1，SM4，DES，AES
- 非对称加密算法： SM2，RSA(1024-2048)等
- 摘要算法： SM3，MD5，SHA1，SHA256，SHA384等

由于传统的物理密码机无法在腾讯公有云上直接部署，为了方便客户与腾讯公有云上的业务和产品进行无缝对接，腾讯云亦提供在同一个 VPC 网络下的完整的数据加密服务。腾讯云的数据加密服务采用国密局认证的物理加密机，且支持符合国家和行业标准的多种数据加密算法。腾讯云只提供加解密的技术支持，而密钥的使用权限和服务的身份权限认证完全由客户来把控。数据加密服务可以帮助客户彻底杜绝明文存储敏感数据情况的发生，大大提高非授权访问者获取敏感信息的难度。值得一提的是，通过云服务密码机的虚拟化技术，腾讯云提供比传统物理密码机更弹性、高可用、

高性能的数据加解密和密钥管理服务，帮助客户更加轻松地实现对重要业务数据的保护。

数据传输

为了保障云端数据在传输过程中的安全，腾讯云针对不同层级的数据传输提供了多种可信传输方案。

网络层可信传输

当客户办公室、第三方合作伙伴或者下游客户与腾讯云之间进行通信时，客户需要结合自身安全需求和实际管控能力，自行选用专线接入、IPsec VPN 或公网 Internet 的网络接入方式与腾讯云之间进行数据传输活动。腾讯云专线接入是由腾讯云和网络运营商合作伙伴共同提供的专线网络，专线接入能够确保客户的企业数据中心与公有云计算环境之间的数据通信始终处在独立的网络链路中，从物理层面实现与互联网其它流量的隔离，有效防御网络窃听、网络嗅探、网络截获、网络篡改等攻击行为，其高安全、高稳定的特性能够满足金融、政企等领域的监管与合规要求。腾讯云 IPsec VPN 可在互联网之上为客户提供安全的传输网络，采用 IKE 协议的预共享密钥进行链路加密，能够满足客户绝大多数情况下的网络安全性要求。此外，腾讯云 IPsec VPN 网关采用双机热备份配置，并允许配置多 VPN 网关实现更高带宽的安全网络接入。

应用层可信传输

为了便于客户在任何时间、任何地点、使用任何主流终端，安全、快速地接入云端业务系统，腾讯云亦支持 SSL VPN 远程访问技术。SSL VPN 不但可以通过加密方式保护在互联网上传输的数据安全性，还可以进行适当的访问控制，减少非授权访问情况的发生。

如果客户需要在腾讯云平台上搭建自身的应用程序，腾讯云亦提供安全套接层 SSL 证书的一站式服务，包括证书申请、管理及部署功能，与顶级的

数字证书授权 CA 机构和代理商合作，为客户的网站、移动应用提供 HTTPS 解决方案。

量子可信传输

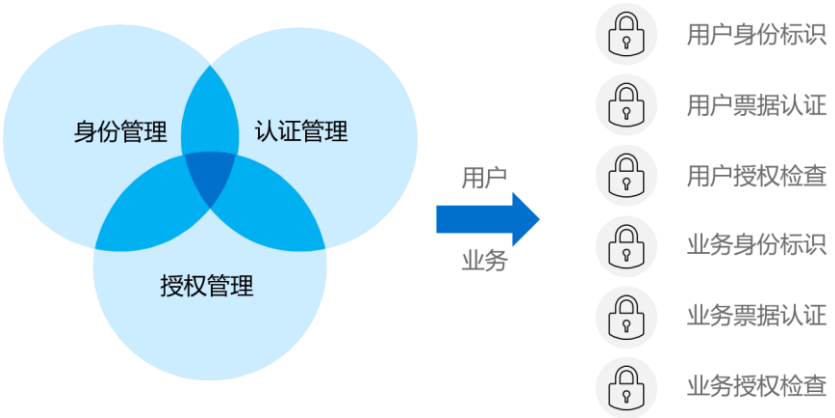
为了更好地解决信息传输过程中的安全问题，腾讯云亦支持量子可信传输。量子通讯技术利用量子力学原理产生真随机量子密钥对信息进行加密和解密，并采用光量子传输效应进行密钥分发，可以确保密钥传输过程中不被窃听或篡改，可以更加强有力地保障数据的不可破解性。

数据访问

主机安全是防止云端数据非授权访问非常关键的因素，腾讯云的“云镜”给客户提供了强大的主机安全防护功能。诚然，除了主机安全，客户应当严格管理用户对其云端数据的访问权限，确保只有特定的人员可以对特定的数据进行特定的操作。腾讯云结合腾讯多年的内审内控能力，提供全方位的用户\业务鉴权服务和监控审计工具供客户使用。

用户\业务鉴权

为了确保数据的合法访问，腾讯云提供身份管理、认证管理和授权管理三合一的用户业务鉴权服务。通过用户身份标识、用户票据认证、用户授权检查、业务身份标识、业务票据认证和业务授权检查六把钥匙形成端对端的鉴权体系，减少云端数据非授权访问的发生。



图表 10“六把钥匙”鉴权体系

安全提示

腾讯云能够确保所有通过控制台生成的的验证信息经过严格的加密处理，被安全地存储于云环境中。 但是，客户仍需要小心地分发、使用、销毁与业务相关的验证信息，避免客户数据被滥用或窃取。

以用户侧为例，每一个腾讯云用户在腾讯云都拥有唯一可辨识的用户 ID，腾讯云针对不同的场景提供多种用户认证机制，包括账户密码、多因素认证、SSH 密钥等。

- **账号密码**：当客户需要通过控制台或者登录后台服务器时，腾讯云提供最基本的账号密码登录功能。结合腾讯在 QQ、微信账号密码的管理经验，腾讯云的账号均配备了强密码安全策略以防范暴力破解等攻击行为；

安全提示

多因素认证MFA（Multi-Factor Authentication）是腾讯云提供的一项安全保护功能，用户可以通过控制台 - 安全信息设置自行绑定MFA设备。为了更好地保护云端数据，腾讯云建议对于特权账户或例如删除数据库实例等敏感操作开启MFA，对账户进行二次验证，进而有效防止客户的数据被非授权访问或误操作。

- **多因素认证**：对于特权账户或敏感操作，腾讯云亦提供多因素认证的方式供客户进行二次身份鉴别。客户可以在控制台自行选择开启登陆保护和操作保护。用户开启 MFA 登陆保护后，登陆腾讯云网站时，在输入完用户名和密码之后还要求输入来自其 MFA 设备的动态安全码进行二次验证。用户开启 MFA 操作保护后，用户在进行敏感操作时必须要通过输入 MFA 设备的动态安全码完成二次验证；
- **SSH 密钥**：当客户需要登录 Linux 云服务器时，除了通过账号密码的方式登录，客户亦可以选用 SSH 密钥对安全地与云服务器进行连接。基于公钥和私钥的 SSH 安全登录功能比普通的账号密码登录更安全可靠，客户可以通过控制台自行创建并管理自己的 SSH 密钥，且只有拥有私钥的人员才可以登录云服务器进行操作。

监控审计工具

当然，合法的数据访问中也可能存在恶意的数据请求，为了及时发现潜在的数据安全事件，客户需要对涉及客户数据的访问和操作进行监测，实时发现异常并告警，同时采取强制下线、锁定账号等若干紧急处理预案，避免数据泄漏、篡改等情况。鉴于此，腾讯云凭借在异常行为监控方面多年累积的经验建立了完善的规则库，并结合信用、行为、内容三大 AI 引擎，打造了可靠的运维安全审计工具和端到端数据库操作审计工具，助力客户更好地实现安全管控和风险处置。

- **运维安全审计**：结合腾讯内部运维安全的良好实践，腾讯云可以帮助客户在其云环境内部署堡垒机对腾讯云账号权限进行集中管控。客户的运

营管理团队人员仅能使用堡垒机新赋予的账号并通过二次身份校验（如动态验证口令）进行登录，自动获得适当的系统操作权限。所有后台运维操作记录均有统一的日志记录，并进行自动化安全审计。

- **数据库操作审计**：针对数据库这样的核心资产，腾讯云提供高性能的数据库操作审计工具，用于帮助企业对可能存在的数据库非授权访问进行风险控制，提高数据安全等级和合规能力。客户可以通过控制台开通数据库操作审计功能，并自定义审计策略，匹配到审计策略的 SQL 语句将展现在可视化审计日志页面，供客户直接进行查看。

此外，为了便于对数据安全事件的追溯，客户需要详细记录云中的每一个数据活动。日志服务是腾讯云提供的一站式的日志数据解决方案。客户无需关注扩缩容等资源问题，五分钟快速便捷接入，即可享受从日志采集、日志存储到日志内容搜索、统计分析等全方位稳定可靠的日志服务。腾讯云的日志服务帮助客户轻松解决业务问题定位、安全审计等日志相关问题，大大降低日志运维门槛。

数据使用

在数据使用过程中，对其中的敏感数据进行脱敏处理可以确保数据的合规使用。同时在数据流出、发布的阶段，可对数据叠加水印，用作数据泄露之后的溯源、定损和存证之用。

敏感数据脱敏

随着《网络安全法》的正式实施，国家及监管机构对于个人信息的保护愈发重视，监管力度也一再加强。为了帮助客户满足数据隐私保护方面的各种合规性要求，腾讯云提供一站式的云端敏感数据脱敏方案。客户可以根据不同数据使用场景（开发、测试、分析等）制定有针对性的数据脱敏方案，并且在云端快速部署直接对用户身份信息、代码等敏感数据进行脱敏处理，灵活调用，大大降低了数据脱敏过程的时间和成本。

泄露溯源水印

在数据泄露事件频发的今时今日，图片水印是一种有效的控制手段保障数据安全。图片水印不但可以提供威慑作用，保护数据的所有权，同时也可以提供数据泄露之后的溯源、定损和存证之用。腾讯云的溯源水印功能包含图片明水印和图片暗水印两种方式，可以满足不同客户的实际业务需求。

数据销毁

数据下云过程中，腾讯云提供通用的标准格式来备份迁出客户数据，确保数据的可移植性和可操作性。大部分情况下，客户可以通过控制台或者腾讯云提供的工具自行完成数据迁移下云的过程，而无需腾讯云的协助。作为值得客户信赖的云服务提供商，腾讯云会严格按照服务协议中的条款在数据下云之后及时彻底删除客户数据。

除了由腾讯云提供的“数盾”数据安全解决方案，腾讯云亦是一个开放的云平台，坚持倡导数据安全生态合作。腾讯云以云服务市场的形式引入安全方面的第三方合作伙伴，该服务市场中已上架了丰富的数据安全产品和解决方案供客户选择使用，包括众多行业内优秀的数据安全产品如：加密机、数据防泄密、数据备份与恢复等。

结语

为了将腾讯云打造成为客户值得信赖的云服务供应商，腾讯云在客户云端数据安全保护的实践中稳步前行，内部流程持续优化，控制技术不断更新。腾讯云的数据安全实践以强大的安全研究团队为核心，通过专业的安全运维团队提供 7*24 小时的服务支持，并建立了独立的安全合规团队，牵头和参与国家网络安全标准化工作，谨遵“合规即服务”的理念，推出面向云端客户的安全合规服务。

合规服务

为了帮助客户快速满足国家及行业的合规要求，腾讯云提供完整、系统化的“等保合规”及“PCI - DSS 合规”咨询和测评服务。

如欲获取有关合规服务的更多信息，请点击附录内腾讯云官网相关链接。

图表 11 腾讯云多层次安全团队

腾讯云通过了 CSA STAR、ISO 27001：2013、网络安全等级保护、PCI DSS、ISO27018：2014、可信云云服务用户数据保护能力评估、CSA STAR TECH 等多项权威第三方认证，同时能够为云平台上行业多样、业务繁多的各企业用户提供助力安全合规的服务。在协助企业安全合规的过程中，腾讯云全力提供云平台的安全运行保障的证据，同时为满足合规要求向企业用户提供业务系统必要的安全加固能力。除了以上资质，腾讯云亦通过提供最新的 SOC 报告（System and Organization Controls Reports），向云用户机构、独立审计师、监管机构、公司股东及其他相关利益方公开腾讯云最新的服务组织内部控制情况。SOC 2 报告是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则针对云服务体系的安全性、可用性和保密性相关的控制设计适当性出具的报告。AICPA 在 2017 年 4 月发布了最新的 2017 版信托服务标准。腾讯云作为领先的云服务提供商，在 2017 年 SOC 审计过程中已经使用了 2017 版的信

托服务标准，是国内第一家率先遵循了 2017 版信托服务标准的云服务提供商。

此外，腾讯云通过了国内权威云计算评估体系 —— 可信云的《云服务用户数据保护能力》测评，该测评标准是“可信云服务”系列标准在数据安全领域的深化，从用户视角考量腾讯云作为云计算服务提供商所提供的数据安全事前防范、事中保护和事后追溯能力，彰显了腾讯云在客户数据保护方面的优秀实践。

作为腾讯连接互联网生态的重要桥梁和开放战略的重要组成部分，腾讯云在加强云基础设施投入的同时，一直把安全作为云计算服务的生命线，其中数据安全更是腾讯云安全研究团队的重点研究对象。随着智能化一站式数据安全解决方案“数盾”的推出，腾讯云正将腾讯海量业务积累下来的 AI 能力应用到数据安全领域，并会一如既往地给客户提供更强有力的数据安全解决方案，助力企业实现“互联网+”的转型。腾讯云希望通过与企业和政府携手并肩，有效打击网络黑产，打造真正安全、智能、便利的云端安全生态。

附录

腾讯云用户可以通过以下渠道获取和了解腾讯云关于数据安全的更多信息：

- 腾讯云安全白皮书

https://cloud.tencent.com/document/product/363/11671

- 腾讯云合规资质

https://cloud.tencent.com/act/event/compliance.html

- 腾讯云等保合规服务

https://cloud.tencent.com/product/djbh

- 腾讯云 PCI - DSS 合规服务

https://cloud.tencent.com/product/pci-dss

- 腾讯云全球基础设施

https://cloud.tencent.com/act/event/global-base.html

- 腾讯云产品白皮书中心

https://www.qcloud.com/whitepaper/product

- 腾讯云云市场

https://market.cloud.tencent.com/

- 腾讯云客户工单系统

http://console.cloud.tencent.com/ticket

- 腾讯云客户数据常见问题

https://cloud.tencent.com/document/product/301/11471