腾讯云安全白皮书

2024 年 1 月

腾讯云安全团队&腾讯研究院安全研究中心

腾讯云

【服务声明】

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，包括网址和其他互联网网站参考，均可能会改变，恕不另行通知。您将承担使用它的风险。

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，安全，值得信赖

序言

当下，随着网络空间的快速演进，新业态、新生态生机勃发，从二维空间到叠加了物联网和云的四维复合生态空间后，安全早已超越了技术的范畴，与整个产业的变化更加息息相关。

从安全威胁方面看，云时代因为攻击、信息造成千万的损失是过去的几十倍甚至百倍以上，技术浪潮在全面释放生产潜能的同时，也为攻击者找到了规避检测的方式。日益繁荣的网络黑产将云服务技术变成攻击武器，随着万物互联趋势，更是给了攻击者更多的攻击渠道和安全漏洞。从防护角度看，得益于大数据、人工智能和云计算的整合，云上安全智能化成为必然趋势。海量数据归档能力的提升、云端计算资源的丰富、AI 智能分析算法的成熟都让安全实时分析和智能决策成为现实。云时代的大步迈进，将让安全防护更加智能和强大。

作为中国云计算领域的领军者，腾讯云尤其关注云安全的重要性，提出“全景式腾讯云**智慧安全**方案：云管端协同布局”的战略规划。同时联合合作伙伴，构建智慧安全新生态，为生态链上的合作伙伴创造一个安全的云端基础环境。

“全链路的产品和引擎是**智慧安全**的基础。”数字时代构建全链路的智慧安全，必须要有全链路的产品覆盖与数据信息流整合，这方面腾讯拥有得天独厚的优势。当云作为平台和管道把大量企业连接到了云的空间后，我们看到了构建立体安全防御体系的机会：基于云、管、端的能力协同，实现联防联控，并有机会将更多安全能力服务化以触达用户，为用户提供丰富的云上业务防御产品和解决方案。

今天复杂的世界形势给全球广泛的领域带来了空前的安全挑战，谋求独立强大与合作共赢是众所周知的共识。因此，在数字经济时代，构建一个云安全生态依然需要集共同之力来完成。网络安全非常复杂，防御和攻击难度严重失衡，没有任何厂商可以独立应对。过去的经验也表明，全行业的生态合作与联动在现在和未来都不可或缺。

从安全的视角和经验来说，在关键位置建立门槛是有必要和实效的。网络空间的安全需要有匹配复合网络空间的立体防御系统，任何一张网都是由线构成，腾讯云也会跟更多行业伙伴一起共建安全大生态。

创立 20 多年的腾讯积累了大量的技术和安全实践能力，也是最早关注云计算生态安全企业之一。腾讯云希望依靠云管端协同的智慧生态，为用户持续提供安全的、可信的、智慧的云，助力更多企业高效迎接数字化浪潮，助力企业安全发展。

智慧安全

“智慧安全”即借助腾讯集团提供的智慧安全能力对安全数据进行分析和处理，从而有效地预防及阻止安全威胁的发生、甚至主动消灭威胁，以助力合作伙伴和广大企业解决在数字化建设进程中所面临的各项安全诉求。一方面，基于“智慧安全”的解决方案可以提升企业的业务安全和应对威胁的能力，助力客户聚焦核心业务、统领未来；另一方面，“智慧安全”也可以推动整个安全生态更加和谐、繁荣的发展。

腾讯云将坚持以**“共享、共建、共赢”**的原则，携手广大安全厂商、个人、企业、国家和社会共同创建“安全生态环境”，持续为营建更安全的互联网生态环境贡献力量，最终实现企业安全的目标，共同受益。**“共享”，即基础安全数据共享。**基础安全数据是整个安全生态链的数据基础。在整个安全生态链中，各方将坚持开放共享的原则，将脱敏后的基础安全数据共享给其他方，协助安全生态的建设与成长。**“共建”，即共同建设安全生态。**共建安全生态是各方共同的目标和职责。腾讯云提倡的安全生态是建立在腾讯、合作伙伴、客户三方共同建设的基础之上的。为了更好地建设安全生态，腾讯云会倾尽全力提供支持和保障。**“共赢”，即多方共同受益。**打造安全生态圈绝非一个零和游戏，腾讯云所期盼的是一个多方共赢的局面。安全生态的最终目的是构建安全和谐、富有价值的互联网环境，无论是合作伙伴、企业客户，还是国家及社会都能从中受益。

智慧安全在具有传统防御能力的同时，更提供了未知威胁感知、安全问题洞察、风险趋势预测、智能化辅助决策、安全协同等智慧安全能力。借助智慧安全能力及全面覆盖云管端的企业安全解决方案，个人、企业、国家和社会可以有效地解决面临的挑战，顺应企业安全发展趋势。

在管理层面，一方面智慧安全降低了企业安全管理运维人员门槛，另一方面，智慧安全汇聚了众多安全专家，解决了企业面临的企业安全人才匮乏问题。对于企业而言，安全管理运维人员只需要掌握智慧安全的管理运维知识，就能尽可能提前做好预防，尽量减小企业损失。企业减少了对人才和信息安全组织的投入，将会有更多的资源投入到企业主体经济的研发中，提升产品质量，增强核心产品竞争力，从而推动整个行业创新，最终造福社会。

在技术层面，智慧安全将全面整合软硬件资源，提供持续服务，具备威胁感知、风险趋势预测、智能化辅助决策、安全协同等核心安全能力。借助智慧安全的企业安全解决方案将能解决传统防护手段的局限，智能化分析预测会发现借助传统的特征化的检测手段无法识别的威胁，提前为企业预防、阻挡网络威胁，甚至主动将威胁扼杀。

在产品层面，智慧安全提供了全面覆盖云管端的企业安全解决方案，安全产品之间相互联动，共享安全数据全面增强了企业安全管理的薄弱环节，形成整体的防御体系。云管端产品相互联动，避免企业

安全建设出现的产品碎片化、孤岛化，解决方案局部化的窘迫局面，助力企业全场景安全护航，顺应企业安全产品全面联动的趋势，提升整体企业安全水平。

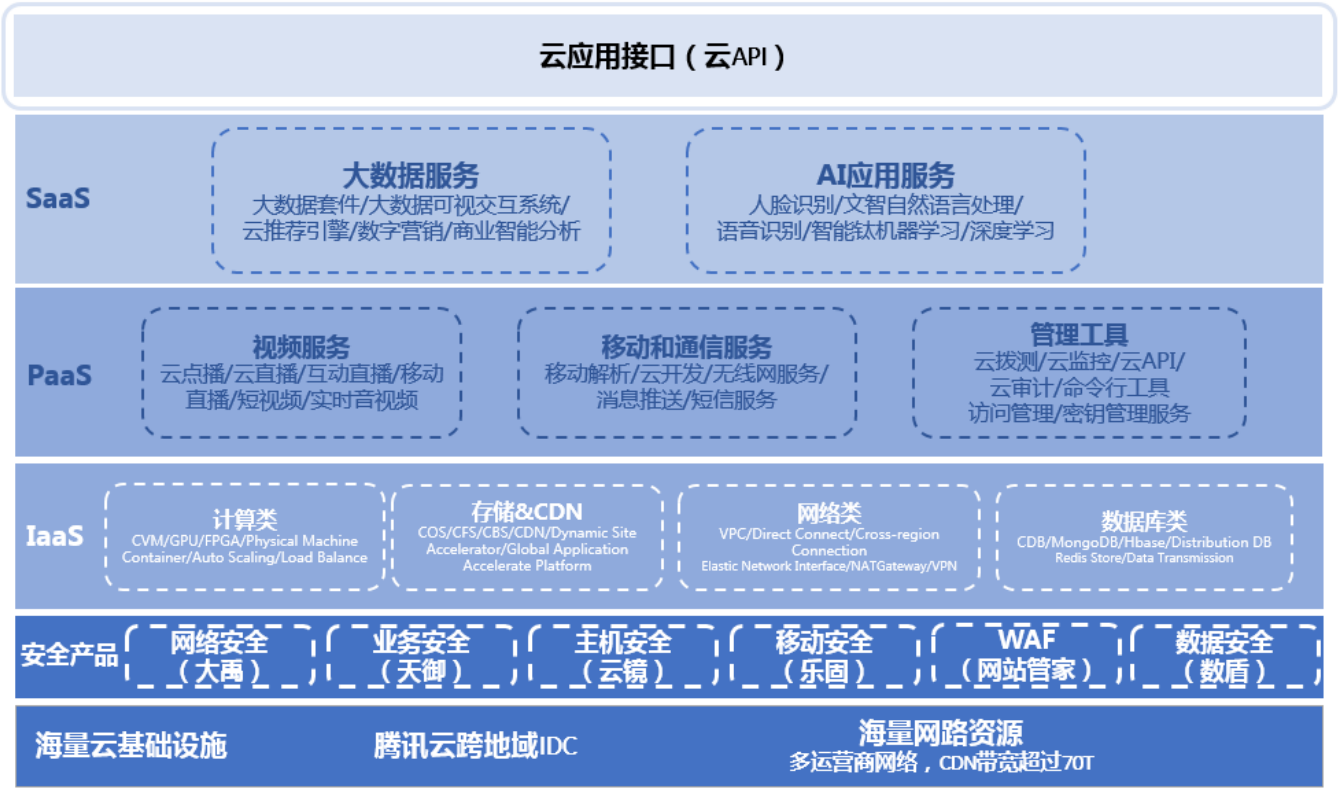
腾讯、合作伙伴、客户三方通力协作，期望借助智慧安全的安全能力，共享安全情报，共同建立安全、和谐的互联网安全生态，助力企业安全建设，解决国内企业安全建设面临的挑战，顺应企业安全发展趋势，最终实现共赢。

目录

一、腾讯云概述

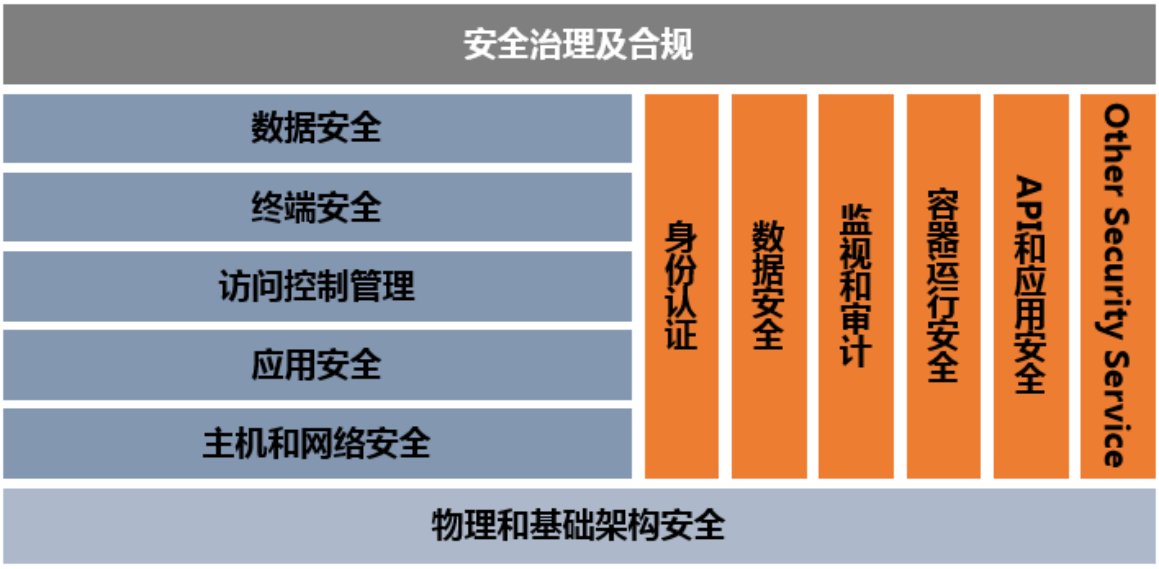
腾讯云已为数百万的企业级和个人开发用户提供值得信赖的云产品和服务支持，解决您在游戏、视频、移动、医疗、政务、金融和互联网+等多个领域发展的需求。

以下为腾讯云目前基于多年业务实践形成的云产品整体架构：



图表 1 腾讯云产品与服务架构

安全是腾讯云的基石。基于全面规划的整体架构，通过多元化的产品与安全属性，腾讯云实现了全方位的防护，在各个层面均部署了安全防护，包括物理安全、虚拟化安全、网络安全、主机安全、数据安全、应用安全、业务安全、安全审计和安全管理，形成事前、事中、事后的全过程防护。同时，腾讯云也在各个层面的产品中实现了对应的安全功能，涵盖鉴权、数据可靠性、监控等，不断优化产品自身的属性。



图表 2 腾讯云安全模型图

在后面的章节中，我们将具体为您介绍腾讯云在不同的安全层面如何对您进行保护，我们将依次介绍：基础安全（将主要介绍物理安全、网络安全和主机安全），数据安全，应用与业务安全（涵盖应用安全与业务安全），运营管理安全（包括安全审计和安全管理）。

二、云服务类型

参考和架构模型

腾讯云为您提供了三种不同的云计算服务，分别是：软件即服务（SaaS）、平台即服务（PaaS）和基础设施即服务（IaaS）。我们有时称他们为 SPI [注1]模型。现在，在构建云服务方面，有很多不断发展的技术，使得任何单一的引用或架构模型从一开始就过时了。看待云计算的一种方式是将其视为一个堆栈，SaaS 是位于 PaaS 之上，PaaS 位于 IaaS 之上。它们并不是简单的继承关系(SaaS 基于 PaaS，而 PaaS 基于 IaaS)，因为首先 SaaS 可以是基于 PaaS 或者直接部署于 IaaS 之上，其次 PaaS 可以构建于 IaaS 之上，也可以直接构建在物理资源之上。作为基于互联网的云计算服务，SaaS, PaaS, IaaS 面对了不同类型的用户。

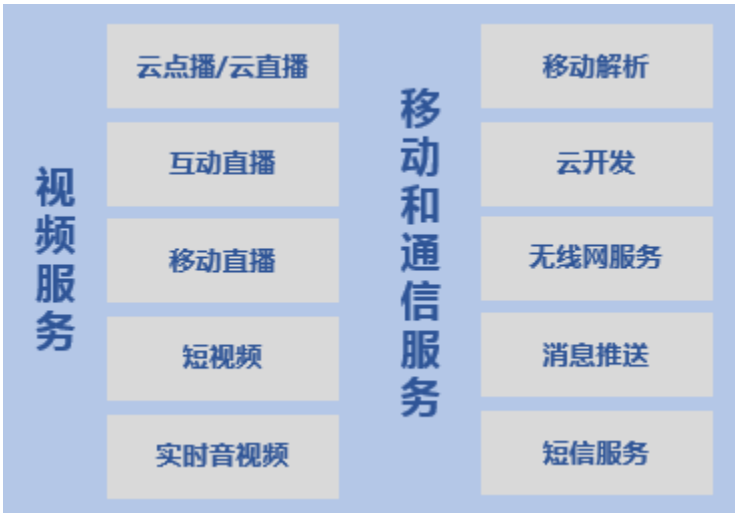
软件即服务[注2]（Software as a Service - SaaS）：

软件即服务是由腾讯云管理和托管的应用软件。您可以在各种设备上通过客户端界面访问，如浏览器、移动应用或轻量级客户端应用。您不需要管理或控制任何云计算基础设施，包括网络、服务器、操作系统、存储等等。如人脸识别产品，您仅仅需在腾讯云控制台对产品相关属性进行设置，便可使用该应用到您的业务场景中，不需要您对任何云计算基础设施和应用平台环境进行管理和控制。

注1：SPI 即云计算的三种服务模式 SssS（Software as a Service，软件即服务），PaaS（Platform as a Service，平台即服务）和 IaaS（Infrastructrue as a Service，基础设施即服务）。美国国家标准与技术研究院（NIST）在其 2011 年发表的文件《The NIST Definition of Cloud Computing》中定义了 IaaS、PaaS 和 SaaS。

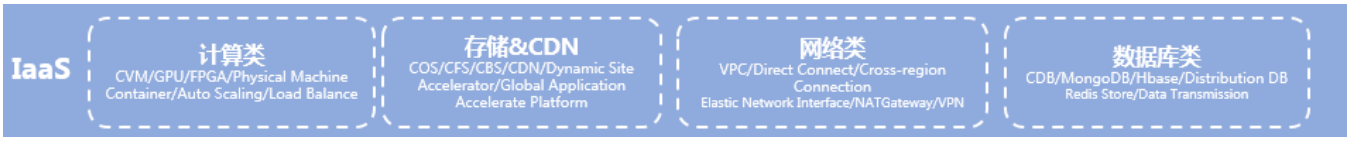
注2：所有定义均来自《CSA 云安全指南 V4.0》

平台即服务（Platform as a Service - PaaS）：



腾讯云抽象并为您提供开发或应用平台，如数据库、应用平台,文件存储和协作,甚至专有的应用处理。您不需要管理或控制底层的云基础设施，包括网络、服务器、操作系统、存储等，但您能控制部署的应用程序，也可能控制运行应用程序的托管环境配置。如云数据库类型产品，您可以通过腾讯云控制台和云 API 对数据库本身进行控制，也可以对部属数据库的虚拟环境进行配置，但您不用管理或控制底层基础设施。

基础设施即服务（Infrastructure as a Service - IaaS）：



腾讯云给您提供基础性的计算资源，包括处理 CPU、内存、存储、网络和其它基本的计算资源，您能够部署和运行任意软件，包括操作系统和应用程序。您不需要管理或控制任何云计算基础设施，但能控制操作系统的选择、存储空间、部署的应用，也有可能获得有限制的网络组件（例如路由器、防火墙，负载均衡器等）的控制。典型产品如云服务器（CVM）等。

安全即服务（Security as a Service - SecaaS）：

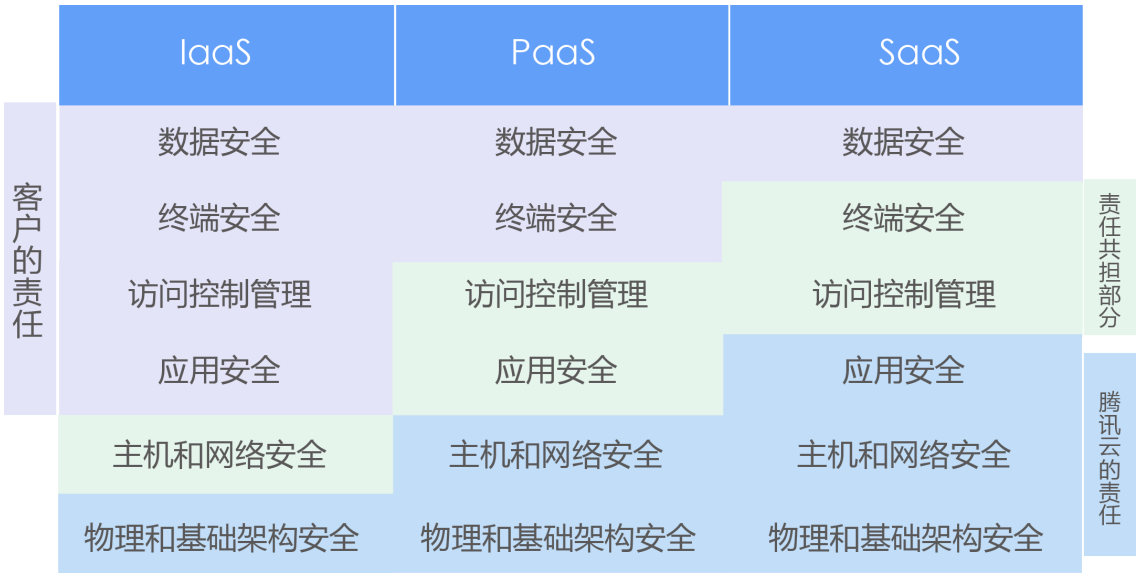
腾讯云提供安全能力作为云服务。这包括专门的安全即服务产品以及通用云计算产品中自带的安全特性。安全即服务涵盖了广泛的各种可能的技术，这些服务（通常是 SaaS 或 PaaS 服务）不一定只用于保护云部署; 它们同样有可能帮助保护传统的本地部署的基础设施。例如数盾，便是跨越 SaaS、PaaS、IaaS 为您提供全方位的保护。

三、安全责任共担模型

- *腾讯云能够提供什么层面上的安全保障?*
- *我还需要考虑哪些方面的安全控制?*

利用统一的底层架构和资源共享形式，腾讯云致力于为客户提供其所需的网络、存储和计算能力等各种资源。当前越来越多的客户在根据自身需求选择云计算服务提供商和其提供的产品与服务时，已将云计算安全作为首要考虑的选择因素之一。秉持云计算服务的开放、共享特性，腾讯云持续提升自身的云计算安全服务能力，并与客户一起对云端业务和数据构建更好更完善的安全保障体系。也正是由于这些云计算特性，腾讯云将在本章就目前已提供的 IaaS、PaaS 和 SaaS 三种云计算架构产品与服务，从业务运营角度初步介绍您与腾讯云之间的信息安全责任；您更可在第六章进一步了解腾讯云在数据安全层面为您提供的保护能力，以及您作为数据所有者可以实施的安全实践。

腾讯云基于信息资产和产品功能建立了如下的信息安全责任共担模型，其中定义浅蓝色部分由腾讯云负责，浅灰色部分为客户负责，浅绿部分则表示腾讯云和客户将共同承担相应的责任：



图表 4 腾讯云信息安全责任共担模型

腾讯云对上图中不同安全属性的解释如下：

- 数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括收集与识别、分类与分级、权限与加密等方面；

- 终端安全：业务相关的操作终端或移动终端的安全管理，包括终端的硬件、系统、应用、权限、以及数据处理相关的安全控制；
- 访问控制管理：对资源和数据的访问权限管理，包括用户管理、权限管理、身份验证等；
- 应用安全：指在云计算环境下的业务相关应用系统的安全管理，包括应用的设计、开发、发布、配置和使用等方面；
- 主机和网络安全：指云计算环境下的主机和网络安全管理，其中主机层面包括云计算、云存储、云数据库等云产品的底层管理（如虚拟化控制层、数据库管理系统、磁盘阵列网络等）和使用管理（如虚拟主机、镜像、CDN、文件系统等）；网络层面包括虚拟网络、负载均衡、安全网关、VPN、专线链路等方面；
- 物理和基础架构安全：指云计算环境下的数据中心管理、物理设施管理、以及物理服务器和网络设备管理等。

在本章节，腾讯云根据不同的 SPI 云计算服务类型向您介绍责任共担模型：

IaaS 架构模型中：

腾讯云为客户提供的是基础云产品，类型主要包括云服务器 CVM、负载均衡、黑石物理服务器、CDN 等。腾讯云负责整个云计算环境底层的物理和基础架构安全；而使用腾讯云的客户需要在数据安全、终端安全、访问控制管理和应用安全方面做好保护。

而主机和网络层面的安全管理则由客户与腾讯云共同承担。在该层面中，腾讯云对虚拟化控制层提供包括漏洞发现、补丁修复、升级更新、审计监控等安全管理措施；客户需对已购买的云主机的操作系统、云主机间的网络通信、以及由内向外的网络通信等加以安全控制。

以云服务器 CVM 为例，用户在使用云服务器 CVM 时，不需要关注基础设施（如物理和基础架构）相关安全责任。用户需要对使用云服务器 CVM 的主机操作系统进行及时更新，同时对 CVM 间的网络通信以及内外网访问进行足够的安全控制。与此同时，用户需要保障自身在云数据库 CVM 上存放的数据安全，对使用 CVM 的终端安全进行保障，做好访问控制策略和管理，对 CVM 上的应用安全负责。

PaaS 架构模型中：

腾讯云为客户提供的是平台类云产品，类型主要包括云数据库、云缓存等。腾讯云负责整个云计算环境底层的物理和基础架构安全，以及为平台类云产品提供支撑能力的主机和网络层的安全；而使用腾讯云此类产品和服务的客户需需在数据安全和终端安全方面做好保护。

而应用安全和访问控制管理则由客户与腾讯云共同承担。在应用安全层面：腾讯云通过对平台类产品的应用系统制定并实施详细的安全控制措施，来帮助客户减少信息安全的成本和投入；客户则需要负责对平台类产品进行正确的使用配置，如自身需要更高的安全需求，则需整合额外的安全能力（如身份管理等）。此外，在访问控制管理层面：腾讯云通过控制台能够为客户按需提供基于角色的访问控制、账号保护、多因子身份验证、单点登录等安全能力；客户则应根据业务需求和合规要求，自行管理并合理设置平台类的账号和权限。

以云数据库为例，用户在使用云数据库产品时，无需关注基础设施层面、主机层面和网络层面的安全需求。用户需要通过腾讯云官网控制台或云 API 对平台类产品进行正确的配置等，保证平台类产品在应用层面的安全；同时应该自行管理和分配平台类产品的帐号和权限，保障访问控制安全。

SaaS 架构模型中：

腾讯云为客户提供的是应用类云产品，类型主要包括云通信、云搜、优图人脸识别等。腾讯云负责从底层的物理和基础架构，到主机和网络层面，以及应用层面的安全；而使用腾讯云此类产品和服务的客户需要对数据安全负责。

访问控制管理和终端安全则由客户与腾讯云共同承担。与 PaaS 架构模型安全责任相似，在访问控制管理层面：腾讯云负责为客户按需提供基于角色的访问控制、账号保护、多因子身份验证、单点登录等安全能力；客户则应根据业务需求和合规要求，自行管理并合理设置应用类云产品的账号和权限，并确保在安全可控的环境下使用。在终端层面：腾讯云能够为客户提供终端设备类型识别、登录保护、应用安全评测与加固、应用分发渠道监测、安全 SDK、真机适配检测等终端安全保护能力；客户则应负责终端设备（如笔记本电脑、PC 终端、移动电话等）的使用限制和接入控制，并合理运用腾讯云提供的终端安全能力来获得完善的安全保护。

整个 SPI 云计算架构中：

对基础设施即服务来说，建筑、服务器、网络硬件和虚拟化这些元素需要由平台供应商管理。客户负有或共同承担对操作系统，网络配置，应用程序，身份，客户端和数据进行保护和管理的责任。

对建立在基础设施即服务部署上的平台即服务来说，供应商还要负责网络控制的管理和保护。客户仍然是负有或共同承担对应用程序，身份，客户端和数据进行保护和管理的责任。

对软件即服务来说，由对应的供应商提供应用程序，客户与底层组件之间被隔离开来。尽管如此，客户依然有责任确保数据正确分类，并共同承担管理他们自己用户和终端设备的职责。

四、风险与合规性

当您选择将自己的服务构建于云端，就意味着您从业务模式轻便化中获得效率的同时，也将面临数据安全及业务安全合规性的挑战。作为云安全的守卫者，腾讯云充分理解您对于合规性的考量与要求。

腾讯云创建至今，一直致力于完善云安全体系、建设安全合规能力、制定云安全标准与大数据安全标准。同时，通过多维度的深入与拓展，腾讯云创建的云安全生态已经进入新的发展时代。

4.1 行业云认证体系

4.1.1 云体系认证

CSA STAR 云安全认证

STAR 云安全评估是由国际权威的非盈利组织云安全联盟（Cloud Security Alliance）推出的，针对云安全特性的一项国际性认证。它将 ISO/IEC 27001 信息安全管理体系进行拓展，结合云安全控制矩阵（Cloud Control Matrix, CCM），将云安全的特有问题可视化，为用户提供了直观的安全架构评估总览。

基于腾讯公司多年积累的安全实践，腾讯云于 2016 年 9 月获得 CSA STAR 全球金牌云安全认证，进一步确定了其国内领先的云服务提供商地位。

可信云服务认证

可信云服务（TRUCS）认证是由国内 100 多家行业会员单位组成的数据中心联盟组织，由中国信息通信研究院（工信部电信研究院）测试评估。通过多维度、透明的安全指标数据进行评测，为用户选择安全、可信的云服务提供了重要的、透明化的参考依据。其中《云服务用户数据保护能力》是云供应商

能否为客户在云上数据提供保护的重要依据。腾讯云公有云平台、金融云平台和专有云均通过云服务用户数据保护能力评估。

本标准从用户视角出发，提出了云计算用户数据保护参考框架，并根据相应的技术要求分成基本级和增强级两个级别。一方面为云计算企业建立规范完备的用户数据保护体系、保障用户数据安全提供指导，另一方面为第三方机构对云计算服务提供者的用户数据安全保护能力评估提供依据，同时也为用户选择数据得到良好保护的云计算服务提供参考。《云计算服务协议参考框架》中对于数据安全的要求包括数据持久性、数据可销毁性、数据可迁移性、数据私密性、数据知情权和服务可审查性。云服务数据保护能力分级参考框架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，使云计算服务提供者在达到数据“可信”的基础之上，实现对数据“安全”保护能力的全面提升。

腾讯云的对象存储服务、 数据中心间 VPN 服务、本地负载均衡服务、金牌运维专项评估、云数据库服务、 云缓存服务、云主机服务等均通过了可信云服务认证，为满足服务等级协议（Service Level Agreement, SLA）中承诺的数据存储的持久性、数据私密性、故障恢复能力、服务可用性等多方面指标进行了有效地背书。


大数据产品能力认证

大数据产品能力认证是由数据中心联盟主导，针对大数据产品的基础能力与性能推出的专项认证与行业标准。该认证覆盖了功能、运维能力、多租户、可用性、安全性、扩展性、兼容性等七个维度，共 38 个指标，包含资料审查、技术测试、厂商互评和专家评审四个评测环节，协助用户全面考察大数据产品的功能与特性。

腾讯云的大数据产品在 2016 年率先通过了大数据产品能力认证，成为首批通过该行业标准认证的企业里唯一的大型互联网企业，证明了自身在数据挖掘和机器学习引擎性能方面的能力积累。

信息安全等级保护认证

信息安全等级保护是我国信息安全保证的一项基本制度，是保护信息化发展，维护国家信息安全的根本保障。信息系统的安全保护等级是根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素将其划分为五个等级，五级为最高系统等级。

依据网络安全等级保护标准及有关规定，腾讯金融云平台通过了四级备案和测评，腾讯公有云平台、腾讯云平台客服系统、腾讯云平台计费系统、腾讯云平台运维管理系统通过了三级备案和测评。

美国电影协会 MPAA

美国电影协会（MPAA）建立了一套安全存储、处理和传递受保护的媒体内容的最佳实践标准。MPAA 最佳实践旨在让与 MPAA 协会成员保持合作关系的应用程序和云服务供应商了解在内容安全方面应遵循的要求。媒体公司可以利用这些最佳实践对内容管理进行风险评估和安全性审计。腾讯云已通过自评估的方式，确保其对客户内容的管理程序遵守美国电影协会（MPAA）内容安全模型指南。

MPAA 电影内容安全模板的组件参照了相关的 ISO 标准 (27001-27002)、安全标准（即 NIST、CSA、ISACA 及 SANS）和行业最佳实践。而 ISO 27001、ISO 27017、ISO 27018、PCI DSS 以及 CSA STAR 等是腾讯云的重要合规项目，已通过第三方审计认证。

4.1.2 ISO/IEC 系列认证

ISO/IEC 22301:2019 认证

ISO/IEC 22301 是第一份以业务连续管理（Business Continuity Management，简称 BCM）为主题的国际标准，提供了一种完整通用的 BCM 方法论，让企业能够达到国际上公认的最佳实践。该认证适用于所有行业中的大、中、小型公有及私有组织，并且特别适用于处于高风险和高度监管环境下的行业，例如金融业、IT 通信业、制造业等。在企业业务的运行过程中，往往会受到各种内在或外在因素的影响，严重时甚至会导致中断业务，而意外的中断会给企业带来重大损失。为了降低风险，业务连续性管理受到了越来越多的重视。

腾讯云是国内第一批通过该项认证现场审核的云服务商，通过构建正式的业务连续性管理流程，保障自身业务的连续与稳定；同时，腾讯云为您提供一个具有组织弹性和有效响应能力的框架，与建设恢复能力框架的整体管理过程，以保障客户的业务不中断，维护您的利益、声誉、品牌以及价值创造活动。

ISO/IEC 27001:2022 认证

ISO/IEC 27001: 2022 信息安全管理体系是国际上针对信息安全领域最权威、严格，也是最被广泛接受及应用的体系认证标准。通过该认证，就意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确的应对。

腾讯云是国内首家获得 ISO/IEC 27001:2022 认证的云服务提供商之一，通过这套“量体裁衣”的信息安全管理控制措施和保护信息资产的制度框架，遵循 PDCA 持续的改进路线，对您的信息安全做出承诺，提供可靠的信息服务与相关安全保障。

ISO/IEC 20000-1:2018 认证

ISO/IEC 20000-1: 2018 是针对 IT 服务管理制定的一套国际标准。该体系规范了企业的信息技术服务管理，从建立、实施、运作、监控、评审、维护与改进的模式，协助企业持续地识别与管理相关信息技术问题，强化与用户的沟通，建立一套自我完善的标准化服务体系。

腾讯云通过 ISO/IEC 20000-1: 2018 新版标准认证，包含云计算服务、托管服务及灾备服务等方面的认证范围。腾讯云严格以服务至上的态度，完善与您之间的信息技术服务与沟通的机制。

ISO/IEC 9001: 2015 认证

ISO/IEC 9001: 2015 是迄今世界上最为成熟的质量管理体系。该体系围绕企业产品或服务，提供指导性的纲领及规范，促进企业产品或服务完善全过程质量管理框架，是企业发展与成长的根本。

腾讯云是国内首家在云计算领域获得 ISO/IEC 9001: 2015 CNAS（中国合格评定国家认可委员会）和 ANAB（美国注册机构认可委员会）认可的企业，认证范围涵云计算服务、托管服务及灾备服务等。


ISO/IEC 27017:2015

ISO/IEC 27017:2015 是一种国际标准，也是 ISO/IEC 27002:2013 的补充，加强了云计算漏洞的威胁和风险的控制。这项认证提供了 37 条 ISO/IEC 27002 指导以及 7 条 ISO/IEC 27002 中不具备的控制方案。云服务提供商和云服务客户都可以利用这个指导进行有效的设计和实施云计算信息安全控制。

腾讯云的 ISO 27017 指导证书不仅表明了我们会始终采用国际公认的最佳实践，也证明了腾讯云 拥有专用于云服务的高精度控制系统。

4.1.3 隐私认证


ISO/IEC 27018:2014

ISO27018 是一个由国际标准化组织（ISO）于 2014 年颁布的国际标准协议，是首个专注于云中个人信息保护的国际行为准则。通过 ISO27018 认证可证明企业在保护企业数据、知识产权、文档和云端 IT 系统安全等方面达到了高标准的行业最佳实践。

腾讯云的个人信息保护管理体系已进入了全球范围内云服务商的先进行列，为腾讯云客户带来充分信任的基础和坚实的云安全保障。


DPTM 新加坡数据保护信任标记

DPTM，由新加坡信息通信媒体发展管理局（IMDA）颁发的隐私合规认证，可用于证明腾讯云已经遵循新加坡个人数据保护法 PDPA。通过 DPTM，可以向客户、业务合作伙伴和监管机构来证明腾讯云采用了负责任的数据保护实践，有能力合规管理其收集的个人数据。

此认证不仅是腾讯云综合实力的体现，更是表明腾讯云已成为出海企业数据业务合规的极佳选择。

4.2 安全合规性

随着云计算技术和安全技术的不断演变，以及行业监管要求的日趋复杂，安全合规性已然成为云服务提供商面临的一大挑战。腾讯云致力于建立高效的安全内控体系，紧随不同行业、领域、国家的合规要求，从制度流程及控制活动等方面完善自身的合规基础。

图表 5 腾讯云安全内控体系示意图

腾讯云构建了统一的云安全内控体系，以云安全管理章程与云安全管理手册为指引，从基础建设安全管理、互通性及可移植性、虚拟化平台管理、身份认证管理等方面制定相应的合规标准，并细化到安全、发现与弹性三大方面的具体安全合规控制要求，通过内控监视与测量程序进行纵向管理，确保整个腾讯云安全内控体系的有效与高速运行。

同时，腾讯云在安全合规上不断进行自我进步，形成了腾讯云自身安全合规体系建设思路，在内部形成闭环结构，对世界各地的法规要求进行积极快速的响应。不断建立和落实云安全合规体系。

4.2.1 识别外部合规要求与安全威胁

腾讯云服务范围遍布全球,为保障云服务的安全性,需要满足国内外不同的合规要求,并识别各种安全威胁。腾讯云主动、积极的对国内外合规要求进行响应，并主动对各种安全威胁进行识别，确保腾讯云安全合规。

4.2.2 采用先进的国际和行业标准

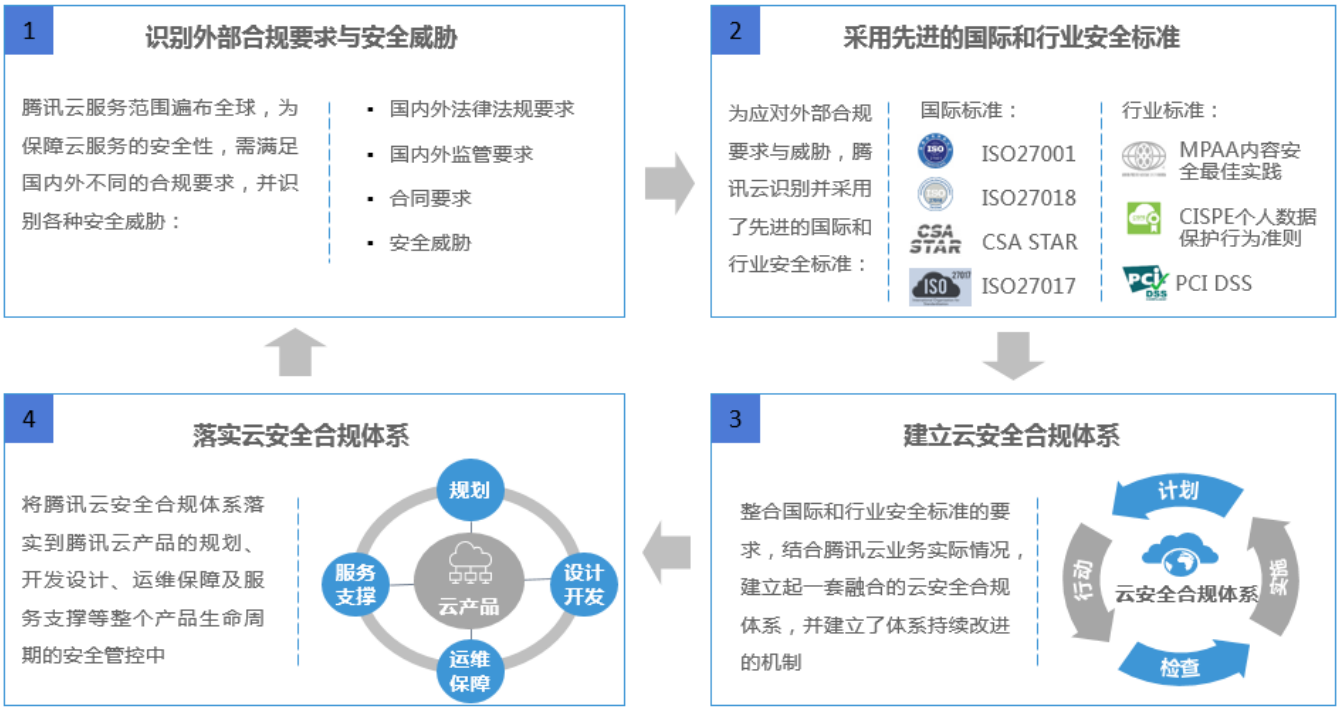
为了应对外部合规要求与威胁，腾讯云识别并采用了先进的国际和行业安全标准。

4.2.3 建立云安全合规体系

整合国际和行业安全标准的要求，结合腾讯云业务实际情况，建立起一套融合的云安全合规体系，并建立了体系持续改进的机制。

4.2.4 落实云安全合规体系

将腾讯云安全合规体系落实到腾讯云产品的规划、开发设计、运维保障及服务支撑等整个产品生命周期的安全管控中。



4.3 安全合规服务

腾讯云集结行业最资深的专家服务团队，为您提供安全、可靠、专业的安全合规产品和服务。

4.3.1 等保合规服务

腾讯云等保合规服务（Cybersecurity Classified Protection Compliance Service）联合各地等保测评中心，为您提供本地化、系统化、专业的等保测评服务；另外，腾讯云完备的安全合作生态，为您提供完备的安全产品及服务，帮助您测评整改，提升安全防护能力，快速满足国家实行的网络安全等级保护制度。您只需在线提交申请，接受腾讯云推荐的测评机构，并在云市场中下单，一站式启动测评流程。

4.3.2 PCI-DSS 合规服务

腾讯云 PCI-DSS 合规服务联合第三方评估机构和咨询机构，为您提供专业、系统化、定制的 PCI-DSS 合规服务；另外，腾讯云完备的安全合作生态，为您提供完备的安全产品及服务，帮助您评估整改，提升安全防护能力，快速通过 PCI-DSS 评估。您只需在线提交申请，接受腾讯云推荐的第三方评估或咨询机构，并在云市场中下单即可，一站式启动服务流程。

4.4 隐私保护

腾讯云践行腾讯公司“一切以用户价值为依归”的经营理念，尤其重视与客户建立长久持续的信任关系。腾讯云以坚实的技术基础和完备的运营管理机制，确保客户的账户信息以及托管的客户内容得到全面的保障。

为了更好地为客户提供安全、可信的云产品和服务，腾讯云将在您进行账号注册、管理、或实名认证等过程中适当收集您的个人信息或企业信息，并严格按照《腾讯云隐私声明》和《腾讯隐私政策》[注1]进行收集、使用、存储和分享您的相关信息。

腾讯云不会尝试访问或披露您的客户内容。为确保您对自己的客户内容具有唯一的所有权和控制权，腾讯云将会竭力向您告知已实施的隐私保护和数据安全技术与管理措施。

在此，我们再一次声明，腾讯云致力于保护世界各地客户的个人信息，并遵守经营业务市场所属国家或地区的适用隐私相关法律。

腾讯云通过了新加坡数据保护信任标记（DPTM，Data Protection Trustmark），DPTM 作为新加坡信息通信媒体发展局 IMDA 颁发的认证，可以向客户、业务合作伙伴和监管机构证明腾讯云已经采用了负责任的数据保护实践来管理其收集的个人数据，同时也符合新加坡的个人数据保护法 PDPA 的要求。此认证不仅是腾讯云综合实力的体现，更是表明腾讯云已成为出海企业数据业务合规的极佳选择。

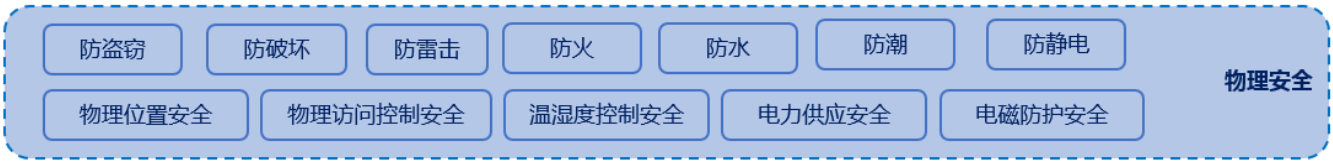
注1：《腾讯隐私政策》请见：http://www.qq.com/privacy.htm

五、基础安全

- *我的云环境是否会被别的用户访问?*
- *腾讯云如何保障云平台的业务持续性能力和云产品的高可用性?*
- *腾讯云提供哪些安全产品和服务?*

5.1 物理安全

作为云计算服务提供商，腾讯云着力为每一个客户提供安全、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，遵循策划-执行-检查-改进（PDCA)的安全管理体系通用流程模型，建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的监察审计，通过持续改进来保证云计算数据中心的物理和环境安全。



5.1.1 基础设施安全

电力、空调、消防和静电防护等基础设施安全对云计算数据中心机房来说是最为基础的环境设施，也是保证可用性最重要的方面之一。腾讯云在全球的各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。各数据中心电力系统和空调系统均采用高稳定性全冗余系统，任意单点故障，均不会影响数据中心的电力和供冷持续性；各数据中心均配备完整的消防系统，包括定点区域火灾侦测系统、自动灭火系统以及供紧急使用的手动灭火装置；各数据中心内部全部安装防静电地板，机柜、线槽等均安装接地线，用以防御静电给设备带来的损害。此外，腾讯云还要求所有机房管理人员定期接受安全教育培训和业务连续性应急演练培训，以确保数据中心基础设施的安全保障得到有效落实。

腾讯云托管机房分布在全球多个位置，这些位置都由地域（region）和可用区（zone）构成。每个地域（region）都是一个独立的地理区域。每个地域内都有多个相互隔离的位置，称为可用区（zone）。地域、可用区名称是对机房覆盖范围最直接的代言。**地域：**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。当前覆盖国内华南、华东、华北三个地区，并有针对东南亚地区的香港节点、新加坡节点，针对欧洲地区的德国法拉克福节点，及针对北美地区的美国硅谷节点、加拿大多伦多节点。我们将逐步增加区域供应以满足更多节点的覆盖。建议您选择最靠近您客户的地域，可降低访问时延、提高下载速度。用户启动实例、查看实例等动作都是区分地域属性的。**可用**

区：可用区（zone）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。目标是能够保证可用区间故障相互隔离（大型灾害或者大型电力故障除外），不出现故障扩散，使得用户的业务持续在线服务。通过启动独立可用区内的实例，用户可以保护应用程序不受单一位置故障的影响。用户启动实例时，可以选择指定地域下的任意可用区。

客户可根据业务发展需求和数据安全要求，自主灵活地将数据和系统部署于不同地域或不同可用区，以保证业务的容灾性要求。同时，客户从选择腾讯云开始，即可获得由腾讯云数据中心提供的基础架构及环境高可用特性，比如供电系统、空调系统、火灾检测防护系统、动力系统等具备的灾备和冗余能力。

5.1.2 访问控制制度

腾讯云对数据中心不同区域定义了的四类安全级别：

- **四级安全区域**：不存放设备， 不影响机房运营的公共区域，如园区等；
- **三级安全区域**：存放业务信息的相关文件，涉及业务信息的办公区域，如办公区、运营中心等；
- **二级安全区域**：存放非生产设备，不直接影响机房运营的区域，如库房等；
- **一级安全区域**：存放运营设备，影响机房整体运营的区域，如客户专属机房、基础设施区等。

各数据中心根据不同级别的区域安全要求制订了严格的基础设施和环境访问控制。根据数据中心人员类别和访问权限，在门禁授权系统建立了完整的人员访问控制安全矩阵，实现对数据中心的各类人员的访问、操作等行为的有效管控。对于内部或外部员工，定期检查授权的准确性。员工辞职时，会及时清除所有权限并收门禁卡等访问控制物品。对于访客，必须提前提供有效身份证件号码、访问原因、访问时间、访问区域等信息申请授权。审批通过后，方可在约定的时间访问数据中心指定区域，且访问期间全程专人陪同。

各类来访或工作人员出入数据中心均需进行身份核对和随身物品检查，并登记携带物品。从环境控制角度，各数据中心对车辆进出也有严格的管理规定和控制措施，所有员工个人车辆、供应商货车等都需进行车辆信息登记，且仅允许获得授权的车辆进入数据中心周边环境。 出租车等公共交通工具，原则上禁止进入数据中心园区。

腾讯云数据中心的监控管理方面覆盖各机房内部、工作交接区、园区出入口和园区内各建筑物的出入口，均配备了 7*24 小时无盲点的视频监控告警系统（所有监控记录均保存足够的时间并安全存储），并由保安室 7*24 小时值守；对于所有的数据中心操作人员和施工人员，腾讯云都要求其具备相应工作资质和经验，并定期对相关人员进行安全意识和能力培训。

5.1.3 安全检查和审计

安保巡检管理

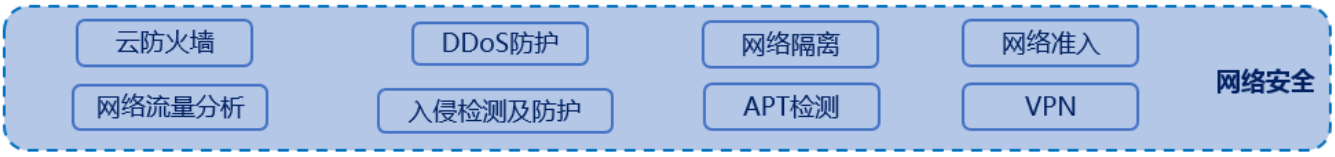
腾讯云各数据中心的安保人员每日均严格根据巡检清单和巡检计划对各机房和设备情况进行巡检，巡检频率不低于每 2 小时/次，巡检覆盖建筑物所有出入口、建筑物周边、楼宇内部等区域，并在每个检查点签名并记录检查时间，一旦发现安全违规事件，会立即启动数据中心机房管理紧急流程。

安全事件管理

各数据中心均已制订了物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。所有安全事件均会详细记录和分析，用于持续改进和提升现有安全管理规范和制度。

5.2 网络安全

腾讯云提供成熟的网络安全架构，包含防火墙、web 应用防护等多重防护机制，以应对来自互联网的各种威胁。



5.2.1 网络通信安全

客户在腾讯云云产品控制台上的通信都受到了 HTTPS 安全协议的加密保护。您也可以选择腾讯云提供的安全通道进行网络数据传输，如云计算平台内部实例之间的虚拟私有网络 VPC，以及通过互联网连接云计算平台的专线网络与 VPN。

此外，腾讯云的云产品所提供的云 API 接口具有 HTTPS 加密、签名校验、状态监测等安全能力，能为您的业务提供端口级别的通信安全保障。

5.2.2 网络隔离

腾讯云制定了严格的内部网络隔离规则，通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护；腾讯云确保非授权人员禁止访问任何内部网络资源；以及，所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机登录生产系统。

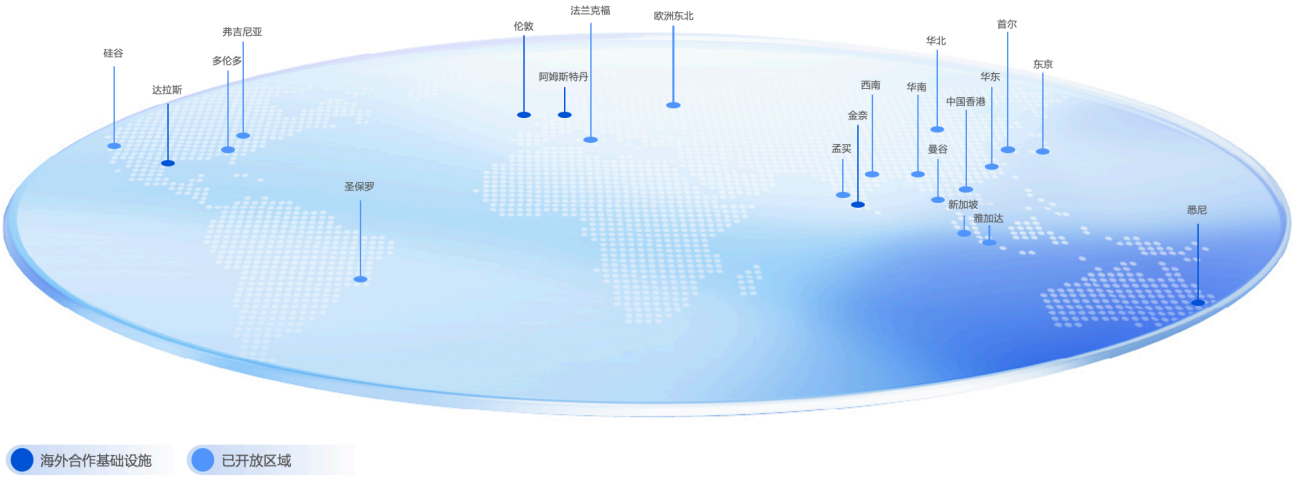
同时，针对云端用户层面的网络访问隔离，腾讯云提供虚拟化控制层资源访问控制策略、云平台内部私有网络间隔离策略、Web 控制台权限分配与身份验证、接口会话 ID 与访问密钥等安全机制，确保每位用户只能访问其已购买的云计算资源，有效实现多用户之间的访问隔离。

5.2.3 网络冗余

腾讯云数据中心遍布全球多个区域，覆盖中国、美国、南美洲、欧洲、亚太等地，网络出口分多个地域对接多个运营商，构建腾讯云网络跨地域的灾备能力，有效地降低运营商公网故障带来的持续性影

响。计划内还将陆续上线多个区域和可用区，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

腾讯云基础网络采用 N*N 的冗余建设方式，配合路由层级的路径优先和路由可达性的流量工程调度，确保网络服务不会因为单点设备故障而中断。腾讯云的计算节点也是采用 N*N 的冗余建设方式，单一计算节点在故障发生时通过调度器实时自动剔除，有效保障用户业务的可用性。



图表 6 腾讯云全球网络示意图

5.2.4 攻击防护

针对 DDoS 攻击，腾讯云为您提供高效的防护能力。其中，DDoS 防护（大禹），接入 30 线 BGP 线路，全面覆盖国内主流及中小运营商，带来极速、稳定的访问体验，同时在中国拥有 5T 以上防护带宽，是国内最大的 BGP 高防产品，可为游戏、金融、政府等各类客户提供稳定的防护。

5.3 面向客户的基础云产品

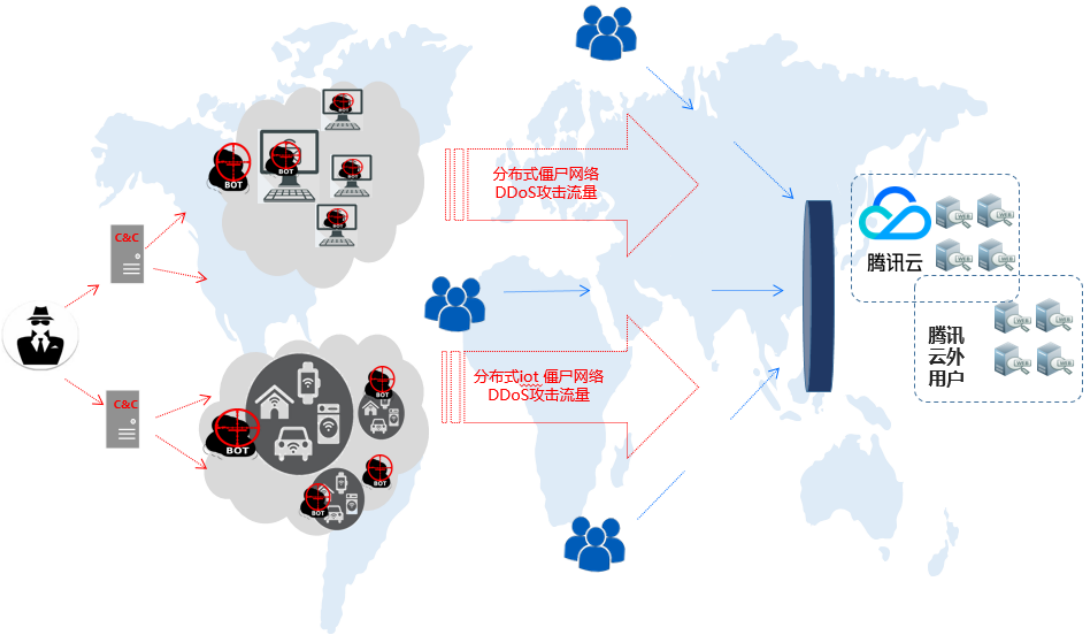
5.3.1 安全类产品

I. 大禹网络安全

腾讯云 DDoS 防护（大禹）是腾讯云针对游戏、互联网+、金融、网站等用户遭受大流量 DDoS 攻击而蒙受的业务经济及品牌损失问题而推出的防护解决方案。针对越发严峻的网络安全挑战和接连不断 DDoS 攻击威胁，腾讯云推出了大禹 GDS（Global Defense System）全球一体化 DDoS 防护体系：事前整体规划与设计，事中提供强大的防护能力，事后分析溯源。根据不同客户的互联网业务需求，大禹网络安全提供多样化防护解决方案：

- **DDoS 基础防护**：DDoS 础防护是腾讯云免费为所有云 CVM、LB 等设备提供的 DDoS 防护服务。
- **BGP 高防包**：BGP 高防包能轻松有效应对 DDoS、CC 攻击，确保业务稳定正常。BGP 高防包主要的优势是可以直接把防御能力加载到云产品上。
- **BGP 高防 IP**：BGP 高防 IP 保证被防护用户在攻击持续状态下，仍可对外提供业务服务。

- **DNS 高防**：DNS 高防具备防范常见的网络攻击的能力，并能有效拦截大规模的 DNS 攻击。



图表 7 腾讯云大禹防护示意图

II. Web 应用防火墙---网站管家

腾讯云网站管家是一款基于 AI 的专业为网站及 Web 服务的一站式智能防护平台。其防护原理是通过将原本直接访问 Web 业务站点的流量先引流到腾讯云网站管家防护集群，经过云端威胁清洗过滤后再将安全流量回源到业务站点，从而确保到达用户业务站点的流量安全可信。

腾讯云网站管家是在国内首家应用机器学习检测技术的 Web 应用防火墙(WAF)。基于 AI 引擎的 WAF，将 Web 攻击检测技术从正则引擎、语义分析，推进到基于机器学习的 Web 攻击检测时代，成为 WAF 技术的一大转折点。其大幅提升了复杂、变形未知 Web 攻击检测能力；更为重要的是，基于 AI 的 Web 攻击检测的引入，将逐步推动建立基于自学习，自进化，自适应的 Web 攻击检测及防御体系的目标成为现实。

腾讯云网站管家通过 Web 入侵防护、0Day 漏洞补丁修复、恶意访问惩罚、云备份防篡改，Bot 行为管理，DNS 劫持检测等多维度防御策略全面抵御恶意攻击，保障受护网站的系统及业务安全运营。

- **Web 攻击防护**：腾讯云网站管家可以有效防御常见 Web 攻击。
- **漏洞虚拟补丁**：腾讯云网站管家主动检测并及时发现高危漏洞，并生成针对漏洞的防护规则。
- **数据防泄漏**：针对数据窃取行为，腾讯云网站管家提供基于事前，事中，事后的防护策略。

- **CC 攻击防护**：网站管家内置 CC 攻击防护算法，阻断恶意请求，过滤垃圾访问，有效防御 CC 攻击。
- **BOT 行为管理**：腾讯云网站管家对友好及恶意 BOT 爬虫进行甄别分类，采取针对性的管理策略。
- **DNS 劫持检测**：网站管家于腾讯检测探测点与云端数据分析能力，帮助组织规避 DNS 劫持问题。
- **网页防篡改**：用户操作同步更新网站管家缓存后才对外发布，保障受护网页的更新可控可靠。

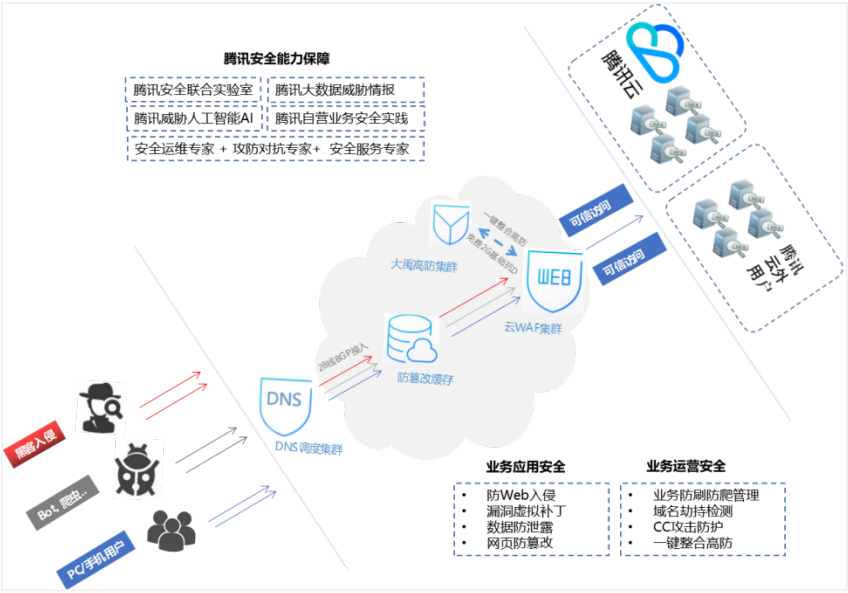


图 8 网站管家防护示意图

III. 漏洞扫描

腾讯云 Web 漏洞扫描是用于检测网站漏洞的安全服务，具有强大的漏洞扫描能力，覆盖庞大漏洞数据库，扫描功能多样化为用户提供 7*24 小时的安全检测、安全评估、安全监控服务，并为企业提供专业的修复建议， 从而避免漏洞被黑客利用，影响网站安全。目前 Web 漏洞扫描已广泛应用于 IT、金融、通信、政府、能源、军工等多个行业，受到众多机构和企业认可。

腾讯云 Web 漏洞扫描拥有强大的漏洞扫描能力与庞大的漏洞数据库，能提供多种漏洞扫描功能，支持并发检测多个 Web 应用和周期性常态化检测，帮助客户构建强大的安全风险评估体系。

- **漏洞扫描服务**： 漏洞扫描服务覆盖巨大的漏洞数据库，支持通用漏洞扫描和特种漏洞扫描两类。
- **扫描分析报告**：腾讯云在进行漏洞扫描服务之后会为客户提供细致的扫描报告。
- **安全应急服务**：漏洞扫描拥有专业的安全专家团队，能为您提供专业安全应急服务。
- **修复闭环管理**：漏洞扫描服务可为客户提供专业的修复建议，同时对漏洞的修复情况进行跟踪，实现漏洞生命周期的全程闭环管理。

5.3.2 云计算与网络

计算类产品：

腾讯云推出的云服务器 CVM（Cloud Virtual Machine）是一款高速、稳定的云虚拟主机，作为腾讯云主要的产品之一，可在云中提供大小可调的计算容量。在行业内，腾讯云服务器拥有自己的创新与领先特点。*高效-快速创建：*90%的云服务器在 10 秒内创建完成，单地域支持每分钟数千台云服务器的创建。*易用-跨可用区热迁移：*可以在同一个地域不同可用区下进行服务器热迁移，同时保证服务不中断。*可靠-高效容灾：*腾讯云独有的通用放置群组，不仅单地域提供多个可用区，在可用区内还可以提供跨物理机、跨机架、跨交换机三层容灾，拥有全面的容灾维度。

若您因行业监管要求，对资源的隔离度有更高的需求，腾讯云可提供专用宿主机 CDH（CVM Dedicated Host ）。除一般 CVM 提供的安全特性外，CDH 能够实现宿主机层面的资源隔离，网络、内存、磁盘均租户专用。CDH 也支持磁盘消磁，以满足您对于敏感业务数据保护、磁盘消磁等的合规需求。

云硬盘 CBS（Cloud Block Storage），是腾讯云为云服务器 CVM 提供的低时延、高性能、高可靠的块存储。如同对待电脑硬盘一样，您可以对挂载到 CVM 实例上的块存储做格式化、创建文件系统等操作。

弹性伸缩 AS（Auto Scaling）根据您的业务需求和策略，自动调整计算资源。可根据定时、周期或监控策略，恰到好处地增加或减少 CVM 实例，并完成配置，保证业务平稳健康运行。

腾讯云在计算类产品中提供以下安全性能：

- **镜像安全：**镜像是对当前云服务器实例运行环境的一个拷贝，主要用于批量部署新环境，一般包括操作系统和已安装的软件。腾讯云提供下列两种镜像： 1) 公共镜像：由腾讯云官方提供，由基础操作系统和腾讯提供的初始化组件构成，所有用户均可使用；2) 服务市场镜像：由第三方服务商提供，经过腾讯云进行内容审核与安全校验后发布到服务市场的镜像，所有用户也均可使用。
- **漏洞管理：**腾讯云凭借安全联合实验室提供的强有力的技术支持，构建了一套包涵漏洞多重挖掘、漏洞处置和漏洞库收集的完整深入的漏洞管理体系。同时 ，腾讯安全应急响应中心 TSRC（Tencent Security Response Center）是面向所有公众开放一个漏洞提交平台，以借助大众的力量，协助腾讯一起完善漏洞的发现和处置。
- **业务连续性：**为保证客户业务的持续可用，腾讯云为每一个云产品（包括计算与网络、存储与 CDN、云数据库以及安全类的云产品）制定了详细的容灾恢复预案，并严格按照要求进行定期演练确保容灾恢复预案的及时性与可行性。

- **租户隔离：**腾讯云在虚拟化控制层为云服务器 CVM 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控制杜绝了互通互访的可能性。

网络类产品：

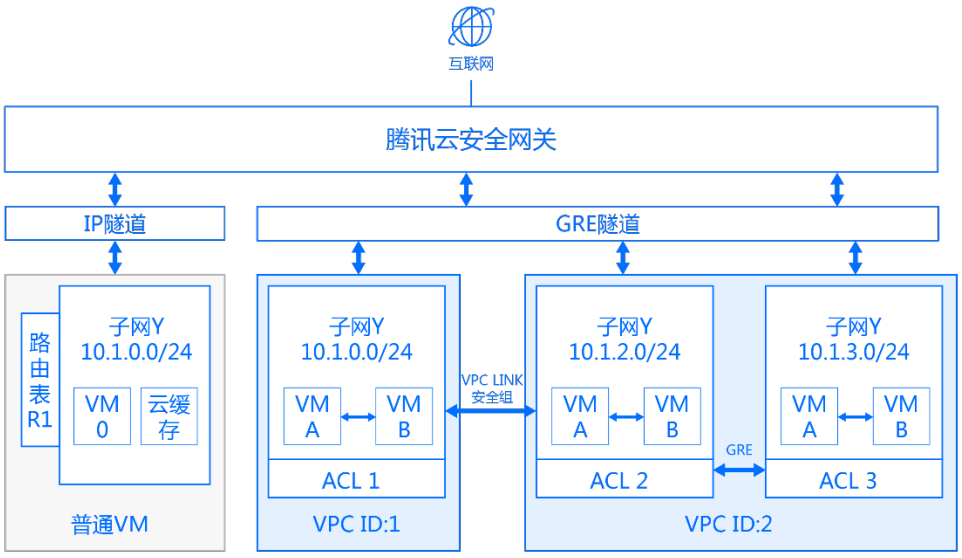
私有网络 VPC（Virtual Private Cloud）帮助您在已购买的云平台资源中构建出多个独立网络空间，并自定义网段划分和 IP 地址、自定义路由策略等；同时，您可以通过部署基于互联网 IPSec VPN 的隧道将云平台私有网络与您企业内部的其他资源连通。

专线接入 DC（Direct Connect）是腾讯云为企业级用户提供的高可靠专用网络接入服务，您能利用专线接入将腾讯云与贵公司内部网络、额外的数据中心、第三方合作伙伴等相连接，实现大容量高可靠网络互联的混合云部署。

负载均衡 CLB（Cloud Load Balance）则可以帮助您将来自互联网的业务流量在云平台中的多个 CVM 实例或其他资源间自动分配，它可以让您的业务系统实现更高水平的应用程序响应及容错能力。

网络流日志（Flow Logs，FL）为您提供全时、全流、非侵入的流量采集服务，您可对网络流量进行实时的存储、分析，助力您解决故障排查、架构优化、安全检测以及合规审计等问题，让您的云上网络更加稳定、安全和智能。

弹性网卡（Elastic Network Interface，ENI）是绑定私有网络内云主机的一种弹性网络接口，可在多个云主机间自由迁移。您可以在云主机上绑定多个弹性网卡，实现高可用网络方案；也可以在弹性网卡上绑定多个内网 IP，实现单主机多 IP 部署。



图表 9 VPC 安全功能示意图

针对网络类产品，腾讯云实现了以下安全功能：

- **网关安全**：NAT 网关是内部网络访问公网的一种方式，能在内外网隔离时，将私有网络中内网 IP 地址和公网 IP 地址进行转换。。
- **网络 ACL 和安全组**：通过私有网络的网络 ACL 和安全组可实现端口和实例层级的资源访问控制，全方位提高网络安全性。。
- **网络隔离**：腾讯云通过 IP 隧道+VPC 私有网络的方式来实现网络隔离，每个租户分配不同的 VPCID，确保在 VPC 私有网络内您能够自由组网且不会受到来自其他租户的访问和影响。。
- **网络分析**：通过分析 VPC 内的网络流量，可以快速发现并定位网络安全威胁，提升系统安全性。您可以快速发现并识别 IP 扫描、异常端口访问、端口轮训访问、安全组嗅探等多种高风险行为，快速定位高危 IP 并通过安全组、网络 ACL 等规则进行封锁，从而大幅降低网络安全风险。

5.3.3 存储与 CDN

对象存储服务 COS（Cloud Object Service）是面向企业和个人开发者提供的高可用，高稳定，强安全的云端存储服务。任意数量和形式的非结构化数据均可放入 COS，并在其中实现数据的管理和处理。COS 支持标准的 Restful API 接口。COS 实现了以下安全功能：

- **防盗链机制**：针对存储桶提供防盗链配置功能，可配置黑名单和白名单，大幅度减少流量盗刷。同时支持跨域访问控制，严格管理跨站访问的来源。

- **多地域存储**：用户可以根据业务热点选择就近存储地域，减少资源获取延迟。同时，支持跨区域复制等功能，多地多副本存储帮助客户实现异地容灾。
- **完善的权限体系**：使用腾讯云 CAM 提供用户和资源分权限管理机制。可将操作和资源按指定条件分配权限，同时针对每个资源还支持通过 ACL 方式管理访问权限。
- **加密保护**：全线支持 HTTPS 加密连接。针对每个对象，可选使用包括腾讯云 KMS 服务在内的多种服务端和客户端加密的方式。

内容分发网络 CDN（Content Delivery Network），即全网内容加速服务，利用遍布全球的加速节点，将业务内容发布至最接近用户的边缘节点，使用户请求能够就近得到快速响应，无需进行多次网络转发，避免请求受地域、带宽、服务器能力等因素影响导致的高延迟、低可用性等问题。

图表 10 腾讯云内容分发网络节点示意图

同时，CDN 在访问控制、安全协议与网络攻击防护方面实现了以下功能：

- **访问控制**：提供通过 Referer 黑白名单或 IP 黑白名单的设置来对请求进行过滤。支持丰富的 URL 鉴权方法，如当您需要对某资源设置访问时效性时，可通过时间戳防盗链实现。
- **安全协议**：腾讯云 CDN 支持全网 HTTPS、HTTP2.0 安全协议。
- **多种攻击防护**：CDN 衍生的 SCDN 安全加速服务，支持自编写多种规则进行访问控制，支持针对回源请求进行 WAF 防护，以及具备一定的 DDoS 防御能力。

5.3.4 云数据库(TencentDB)

云数据库 TencentDB 是腾讯云数据库的总体品牌，目前包含了腾讯云提供的全部数据库服务，

例如：关系型数据库 CynosDB、MySQL 、MariaDB、 SQLServer、 PostgreSQL ，以及分布式数据库 TDSQL，弹性缓存 Redis、云数据库 MongoDB ，时序数据库 CTSDB，以及数据传输服务，数据备份服务，智能 DBA 等。

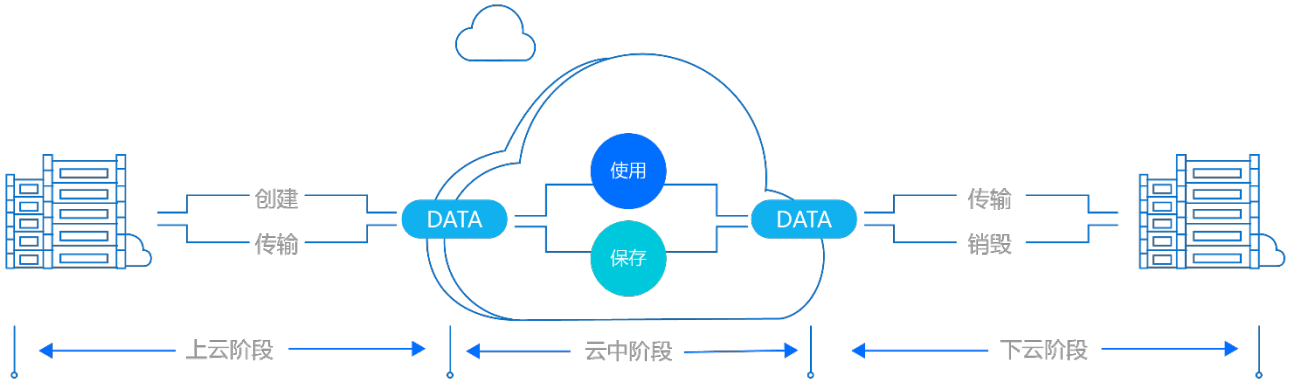
作为云的核心产品，数据库 TencentDB 确保客户数据安全，如：

- **数据库实例隔离**：通过严格的权限管理措施，从内核层面确保无论是运维还是研发人员，都无法直接通过腾讯云其他机器登录到数据库机器。
- **数据库身份鉴别和访问控制**：腾讯云数据库实例的访问都存在严格的身份鉴别和访问控制措施。
- **访问安全与数据加密**：云数据库提供业内主流的安全访问解决方案，以及数据加密能力。相关解决方案密钥均安全的存储于 KMS 密钥中。
- **安全审计能力**：提供全面的安全审计和风控机制，审计范围覆盖到服务器上的每个操作系统用户和数据库用户；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；审计记录保存 1 年以上，且存储在安全等级更高的位置，避免受到未预期的删除、修改或覆盖等。
- **服务高可用和数据高可靠**：腾讯云提供数据库双机热备，故障自动检测和故障自动迁移，秒级切换等技术手段来保证数据库的服务高可用性。同时，我们还提供自动全量备份和增量备份，同城双活等方案，确保即便实例所在硬件都同时出现故障时，也可以通过冷备文件来恢复数据。

六、数据安全

- *我的生产数据在腾讯云上安全吗?*
- *我在注册或使用时提供的个人隐私信息是否得到保护?*
- *为了更好地保障我的数据安全，能否提供一些数据管理上的建议?*

6.1 安全的云上数据



图表 11 云上数据简单示意图

当客户选择使用云产品和服务作为业务运营的技术基础时，必然会将相关的数据置于公有云服务提供商的云计算环境中。普遍情况下，客户的数据会经历三个主要阶段：上云阶段、云中阶段和下云阶段，每一个阶段中客户数据的保护侧重点均有不同。

作为公有云服务提供商，腾讯云通过建立领先的安全技术手段和全面的安全管理体系，确保您的数据不会因为腾讯云平台本身而产生保密性、可用性和完整性的问题。此外，腾讯云建议所有客户应通过部署有效的控制措施来保证数据、应用、终端和账号的安全，在本章第 6.2 节中将向您介绍一些数据保护的最佳实践供参考。

6.1.1 上云阶段数据保护

上云阶段为客户在选购了云产品并进行恰当的开发、测试、配置等工作后，将必要的业务数据/生产系统迁移至云产品中的过程。这个过程中，您可根据您的安全需求和实际管控能力选择合适的数据传输方式与传输协议（如 HTTPS、SSH 等）；同时，您可选择腾讯云提供的网络服务产品来获得更高的安全性保障：

腾讯云专线接入（Direct Connect）是由腾讯云和运营商合作伙伴共同为您提供的专线网络，专线接入能够确保您的企业信息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他流量的隔离，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，能够满足您绝大多数情况下的网络安全性要求。此外，腾讯云 IPsec VPN 具备网关层双机热备份配置，并允许配置多 VPN 网关实现更高带宽的安全网络接入。

您可在上云阶段直接创建新的数据，创建时应参照您的企业既定的数据分类分级标准来赋予新的数据相应的重要性级别，以此确定数据的使用方式和存储位置，以及是否需要在存储时进行加密保存。

6.1.2 云中阶段数据保护

云中阶段是客户利用已部署的云计算环境进行业务生产活动的过程。该过程中会处理大量的用户信息、业务资源、缓存文件等敏感数据，因此需要完善的安全管控机制来确保云环境下数据自身的安全。

您的业务数据在腾讯云中属于最高级别的保密数据，完全归您唯一所有。腾讯云建立了细粒度的数据分级分类管理标准，并在物理层面、网络层面、系统层面和应用层面设计了完整的身份验证和访问控制能力，配合基于大数据的异常行为监控机制，保护您的业务数据不会受到非授权访问和破坏；同时，在自动化、工具化的运维管理手段配合下，任何腾讯云内部人员在未获得您的授权时均无法触碰您的云端业务数据。

每一位公有云客户都共享腾讯云提供的底层物理硬件。腾讯云通过严格的开发设计确保不同客户之间的业务数据和生产环境能够实现有效的逻辑隔离，包括虚拟机镜像隔离、数据库实例隔离、私有网络

访问隔离、对象存储文件隔离等。如果您的业务有更高级别的安全要求，腾讯云同样能够为您提供独享宿主机资源的云产品[注1]或可直接购买基于云环境的物理服务器[注2]。

腾讯云利用多种安全技术和管理手段来帮助您保护数据安全。利用腾讯云提供的防拒绝服务攻击（Anti-DDoS）能力，配合入侵防御、DNS 劫持检测、网站安全防护、病毒/木马保护等多层安全机制，实现您的云端数据不受来自互联网或其他租户的恶意攻击。同时，腾讯云也根据各云产品的特性，采用主从数据实时热备、冗余存储、多地备份等方式来保障您的业务数据安全可靠，持续可用。

6.1.3 下云阶段

您的企业进行业务变更或未来 IT 规划需要暂时离开公有云计算平台时，可以选择在任何时间对云端数据和生产环境进行备份迁移。腾讯云提供的云产品允许您采用通用的标准格式来备份迁移您的数据，且您能采用与上云阶段相同的传输方式和传输协议，或使用腾讯云专线接入、IPsec VPN 等网络服务产品，确保您的数据在下云阶段时安全可靠。

当您的公有云服务终止后，腾讯云将遵循严格的数据擦除方式，在对您此前购买的计算和存储资源进行回收利用前彻底删除您的所有数据。

注1：即专用宿主机 CDH (Cvm Dedicated Host)：专用宿主机可以让您以独享宿主机资源方式购买、创建云主机，以满足您的资源独享、安全、合规需求；购买专用宿主机后，您可在其上灵活创建、管理多种自定义规格的独享型云主机。详情请访问腾讯云官网或咨询销售人员。
注2：即黑石物理服务器 CPM (Cloud Physical Machine)：黑石物理服务器是种可以按需购买、按量付费的物理服务器租赁服务。
详情请访问腾讯云官网或咨询销售人员。

6.2 用户数据保护实践

帮助客户更好的实现安全合规是腾讯云的核心价值之一。腾讯云建议所有客户均应综合评估自身实际情况和安全需求，并设计有效的控制措施来进一步提升云计算环境的数据安全。

在此，腾讯云将从验证信息、业务数据与日志信息三个关键内容角度，向您介绍如何更好的保护自己的业务数据。

6.2.1 验证信息保护

作为获取数据的钥匙，验证信息能够阻止客户数据在未经授权情况下被访问和使用。因此，验证信息保护应是客户在业务经营活动中的重点安全管控措施之一。

腾讯云能够确保您在控制台创建/修改的验证信息是安全加密并被有效隔离存储在云环境中。 但是，您仍需要小心地分发、使用、销毁与业务相关的验证信息，避免您的数据被滥用或窃取。腾讯云建议：

1. 避免通过邮件、网页、即时通讯、纸质等方式明文传输关键的验证信息；
2. 应避免使用共用账号，同时回收具有最高权限的账号，并根据最小权限原则和业务需求创建不同的账号信息；
3. 采用密码作为验证信息时，密码应具有一定的复杂度，并定期更换；
4. 可配合使用多因素认证[注1]的方式，如使用动态密码设备或手机动态密码进行二次认证；
5. 及时清理已停用或无效的验证信息；
6. 记录完整的验证信息使用记录，定期分析异常使用记录或设定实时预警阈值。

腾讯云为客户提供的认证信息类型包括：

注1：多因素认证，MFA (Multi-factor authentication)， 是一种访问控制方法。用户只有在成功提交两类或多类认证信息后才能进入系统或使用资源。这些认证信息一般包括以下三类信息中的两类或以上才能称为 MFA，即知识（Something they know），所有物（Something they have）或用户固有信息（Something they are）。例如，用户设定的密码是知识类，动态密码口令牌或手机动态密码可视为用户所有物，生物认证信息，如指纹或虹膜认证，则属于固有信息。也有人把只包含两类认证信息的认证方式称为双因素认证，即 2FA（Two-factor authentication）。

- 账号密码：腾讯云提供多账号管理功能，并配合强密码安全策略以防范暴力破解等攻击行为；
- 二次验证：腾讯云提供动态密码验证能力，确保执行敏感操作时（如删除实例等）的账号安全；
- SSH 密钥：腾讯云提供基于公钥和私钥的 SSH 安全登录功能，安全性比普通口令更高；

6.2.2 业务数据保护

腾讯云不会触碰或知悉客户在云环境中的客户内容，客户内容被腾讯云内部定义为绝密级别，没有客户授权任何人无权访问。对于云上的业务数据的的管理和保护，腾讯云建议每个客户根据自身适用的安全标准（如 ISO/IEC 27001: 2013、ISO/IEC 27017: 2015、等级保护要求等）以及各自企业既定的安全保护机制来定义和实施云上业务数据的保护。包括但不限于：

1. 有效识别云上的业务数据并依照符合业务运营安全需求的方式进行数据分类；
2. 在数据分类完成的基础上，定义并赋予不同类别数据相应的重要等级（或风险等级）；
3. 持续更新资产信息，如有条件可建立云数据资产管理系统或与已有企业内部资产管理系统进行对接改造；
4. 针对不同重要等级的数据信息制定不同的数据安全规则。较高重要等级的数据信息应采用更严格、更安全的保护措施，如数据存储加密、数据库表加密、传输加密等。但请注意由于加密和解密都需要一定的时间和计算能力，因此数据加密有可能影响数据的使用效率；另一方面，若客户选择对业务数据进行加密，则需要对密钥进行系统且妥善的管理；
5. 通过互联网访问业务数据时，建议通过部署防火墙、入侵防护系统、抗拒绝服务系统等限制访问来源和目标对象；当客户期望将所购买的公有云平台与企业内部网络连通时，腾讯云强烈建议采用安全的连接方式（如 VPN、专线、加密链路等），确保不会因不安全的链接导致企业内部网络出现互联网缺口；

6. 合理运用腾讯云提供的私有网络（Virtual Private Cloud）产品，设计和规划云计算平台内部的安全区域。可利用私有网络功能实现如核心生产、运维管理、开发测试、对外交互等不同逻辑区域的安全划分与访问隔离。

6.2.3 日志信息保护

腾讯云负责分析和处理公有云产品底层产生的非用户层面日志信息，包括物理环境设施、网络设备、服务器硬件、数据库管理系统等。作为腾讯云公有云产品的使用者，您仍需要关注基于公有云计算平台的业务运营活动中所产生的各类日志信息（访问记录、操作日志、系统状态信息、告警信息、错误提醒等），以实现更好的安全管控和风险处置。腾讯云建议：

1. 合理利用腾讯云各类云产品提供的日志记录功能，结合腾讯云控制台实现云产品操作与访问的实时监控；
2. 需要针对部署在云产品之上的操作系统、应用程序、数据库实例等设定有效的日志管理功能；
3. 可设立集中的日志收集和分析系统并对该系统进行安全加固和权限管控，根据日志所含的信息敏感程度实现不同日志信息隔离保存或加密；
4. 严格限制日志信息的访问权限，如需在互联网中传输应采用安全的链接方式（如 VPN、专线、加密链路等）确保日志信息不被丢失或篡改；
5. 有条件的情况下，可部署安全的堡垒机来获取完整的操作痕迹，帮助您的企业实现问题追溯和行为审计。

七、运营管理安全

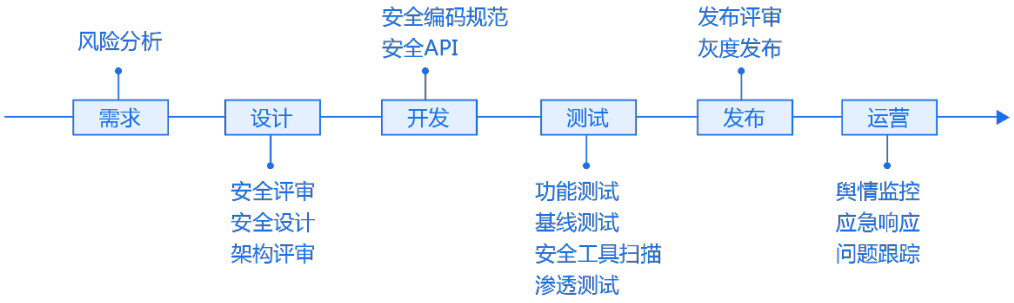
- *我如何对云产品的运行状态进行监控?*
- *我在使用云产品的过程中若发生问题如何寻求帮助，能否得到及时响应?*

7.1 腾讯云的运营管理能力

您的数据在享有来自腾讯云提供的底层安全能力的同时，也将获得全面的业务运营安全保障。依托于腾讯云多年的安全运营经验和庞大的服务团队，能够为您所购买的云产品提供包括系统流程与变更、账号与权限、监控与审计多方面的运维支撑服务。

7.1.1 流程管理

在为您提供的每一个云产品的背后，腾讯云着力将 ISO/IEC 20000 信息技术服务管理标准和 ISO/IEC 9001 质量管理体系标准融入到整个产品 SDL 安全开发流程中，关注需求、设计、研发、测试、交付、运维等不同环节，在产品开发各个阶段中消除信息安全和隐私问题，确保所有的云产品在其生命周期内均能获得足够的安全管控与评估：



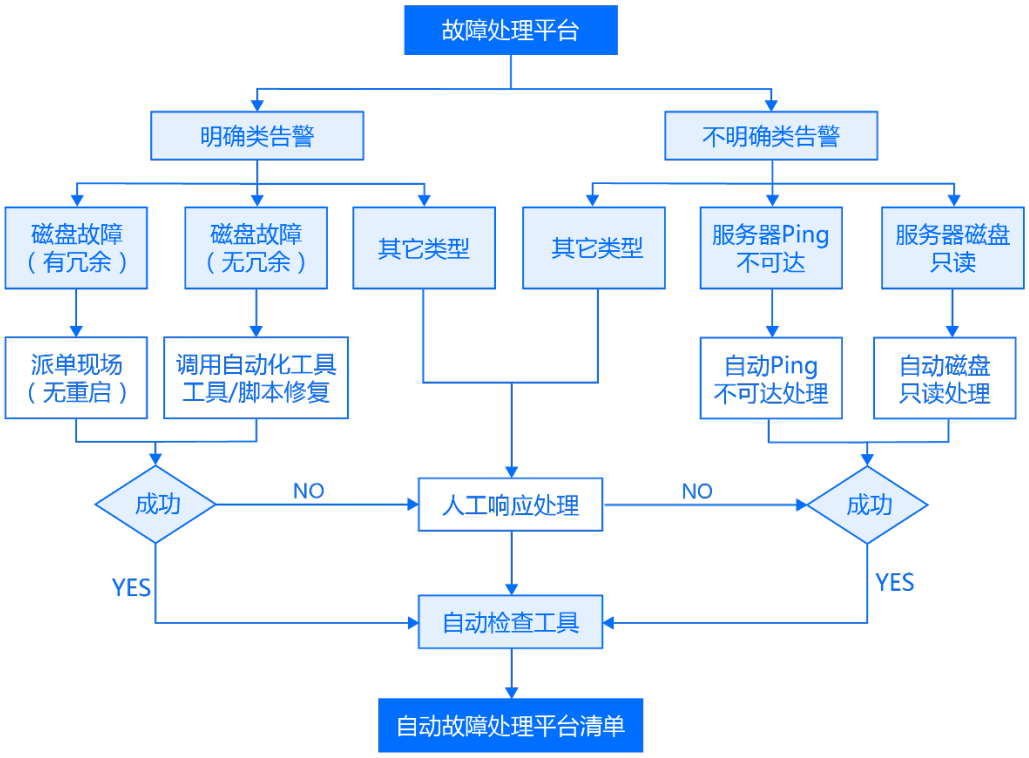
图表 12 腾讯云安全开发流程示意图

为了保证最终的用户安全，腾讯云严格按照安全开发生命周期方法开发云平台及云产品，目标是将信息安全融入到整个腾讯云的软件开发生命周期中。我们的软件开发生命周期主要由以下几个部分组成:

- 安全培训(training)：针对开发人员推广安全编程意识，严格要求相关人员遵循安全编码的规范；
- 需求分析(requirements)： 针对业务内容、业务流程、技术框架进行沟通，寻找安全嵌入的最优方式；
- 系统设计(design): 对系统设计进行威胁建模，对采用的架构进行安全技术评估；

- 实现(implementation)： 开发过程中，提供腾讯自行设计的安全开发组件供研发人员使用；
- 验证(verification)： 通过渗透测试和代码审计发现漏洞；
- 发布(release)： 经过信息安全部门的最后检查确认后，系统才能发布到线上环境,以防止产品携带安全漏洞在生产环境运行。

腾讯云运营服务团队不断将成熟的运维流程转化为抽象控制模型，目前已实现服务交付、控制、发布、解决和关系流程的高度自动化。在更加细化的流程控制活动中，腾讯云把不同的标准化工具进行合并/串接，无需人工干预即可实现各个运维流程的输入输出自动对接和分支汇总能力。自动化流程控制不仅降低了整体的运营成本，也极大的减少人工失误和恶意操作所带来的安全风险。并且，结合自动化流程告警控制，迅速地对错误或失效的操作进行告警和修复。



图表 13 腾讯云故障自动化响应与处理示意图

7.1.2 运维管理

腾讯云每年平均处理超过 1200 万次的运维请求，通过内部运维管理机制严格控制变更时间窗口，所有运维请求均能在指定的时间内完成。如此海量的运维操作，在成熟的自动化/工具化的运维管理平台下变为井井有条的常规工作，让云产品在功能迭代、补丁升级、漏洞修复等关键环节，能够持续为您提供无风险、不间断的业务运维支撑。

在您所购买的任何云产品中，您拥有的业务数据在腾讯云内部均受到最高级别的保护。腾讯云提供完备的运维安全保障机制，确保运营服务团队在未获得您的同意与授权下无法直接访问您的信息资产。同时，腾讯云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。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，对运维过程中的风险告警和可疑操作进行问题排查与追溯。

此外，腾讯云根据运维请求的重要/紧急程度、变更范围等属性进行影响等级划分。针对影响较高的运维变更操作，将及时通过官网、论坛等渠道发布变更通告，并向可能受到影响的客户发出变更通知（短信、邮件或电话提醒），以便您能更好的协调您的业务资源。

7.1.3 权限管理

腾讯云在云产品的运营中，提供强制的、细粒度的权限管理能力。结合自动化的运维管理机制，腾讯云建立了统一的运营管理门户，所有的生产环境操作均受到严格的权限控制和监控。

每一位成员在加入运营管理团队前，都将接受来自腾讯云严苛的背景调查和能力评价，只有满足所有必要条件的候选人才能正式成为腾讯云的员工。腾讯云将根据员工的技能类别、技术程度等方面安排适宜的工作岗位与权限，并提供全面的内部培训帮助员工提升工作能力和专业素养。腾讯云设计了完整的信息安全培训体系，确保员工从入职之际开始，就能不断获得安全意识和安全技术的提升。

腾讯云运营管理团队的人员变更均由统一运营管理门户实现自动化权限控制：入职时自动赋予基本的默认权限，调职时自动修改岗位权限，离职时自动禁用所有权限。员工可在统一运营门户中申请所需的临时或固定权限，在获得多级评审和批准后，系统将自动赋予其新的权限。临时权限在使用期限结束后自动回收。

腾讯云不允许任何可能存在冲突的权限被同时获取，这依赖于腾讯云内部复杂的权限分离矩阵机制。腾讯云会定期组织内部权限审核工作，确保权限不会被滥用、误用。

7.1.4 监控与审计

腾讯云通过大数据处理和可视化分析，实现对所有内部运营活动的全面自动化监控。监控的对象包括所有的后端系统组件（如网络设备、物理服务器、数据库及管理系统等），并可根据系统组件的不同功能和使用情况设置告警阈值，一旦出现监控告警则迅速通知相关人员进行评估与处置。

腾讯云生产环境已全面部署堡垒机，通过堡垒机将腾讯云后端系统组件的管理员账号权限进行集中管控。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由日志平台集中加密存储，由腾讯云内部审计团队定期对记录信息进行审核。

7.1.5 服务支持

腾讯云完善的运营安全能力同样能够为您提供云产品的全天候技术支持。

腾讯云拥有多地域互备的客户服务中心，能够 7*24 不间断处理来自您的建议与咨询。在标准服务的基础上，针对大型客户或特殊客户我们能够确保提供一对一的专家服务，帮助您更好地应用腾讯云提供的云产品。

腾讯云十分关注客户体验 ，为了更好地了解和满足您的需求，腾讯云主动通过多个渠道来获取反馈信息：

- **来自监管机构**：通过与各地通管局、网监局的共同协作，及时获取与腾讯云自身或您的业务活动相关的安全通告；
- **来自内部反馈**：腾讯云已建立的舆情监控系统能够获得内部人员的实时安全问题反馈；
- **来自互联网**：腾讯云客户服务中心对诸如 V2EX、微博等互联网信息渠道进行监控。

腾讯云客户服务中心为您提供业界领先的服务响应时效和处理质量。您的满意是腾讯云不懈的追求，运营管理团队同客户服务中心通力协作，全年能够累积达到 99%的客户满意度。

7.2 面向客户的运营管理类产品

腾讯云能够帮助您实时掌控业务活动，所有已购买的云产品均可通过腾讯云 web 控制台进行监控和管理。Web 控制台为您提供云账户管理、访问权限设置、产品功能配置、网络配置、健康状态和安全状态监控、告警设置、日志管理等各项云平台运维功能。

7.2.1 云监控

云监控服务可在您的云计算控制台中配置使用。基础监控功能可在极少的人工干预下通过智能化数据分析、实时化故障告警和个性化数据报表配置，全面覆盖云产品的健康指标（如云服务器 CPU 利用率、内存利用率、磁盘利用率以及云数据库、Memchache 高速存储等各项云服务负载）和性能指标，为您提供立体可视的云产品数据监控；基础监控功能支持多产品、多策略、多通知渠道的异常告警设置，不仅能够在第一时间让您获悉您的业务状态，更可通过监控触发弹性伸缩能力，确保当危险指标达到告警触发条件后可根据预先配置实现自动性能扩容，满足业务运营可用性要求。

- **日常巡检**：为日常巡检提供可视化图表分析，方便监控、对比、发现异常；
- **异常定位**：快速圈定异常范围，找出异常原因。可选择任意两段时间数据对比，帮助排查故障；
- **告警通知**：提供第一时间告警通知给告知接收人。

此外，自定义监控功能将进一步帮助您掌控您所购买的云产品各项指标。腾讯云为您提供简化的操作管理模式，无需复杂编码和额外资金投入，即可根据不同业务需求自定义相关指标并上报至控制台；您可实时了解所关注的业务质量，提前发现重要系统异常状况，实现业务精细化运营。

7.2.2 云拨测

为了帮助每个客户更好的监测全球业务的可用性和稳定性，云拨测作为腾讯云专有的服务质量检测网络，可在各种业务场景中对您的网站、域名、后台接口等进行分钟级的周期性监控，协助您对异常状态快速响应。

- **站点拨测监控**：根据全国二十多个主要省份和主流运营商的监测点，对网站访问可用率及延时提供综合视图展示。并可设置告警阈值，触发后实时告警；
- **业务端口拨测监控**：支持对于任意 TCP 端口进行周期性的连续访问，监控端口的状态，可配置 HTTP/HTTPS、TCP、PING 等多种协议的拨测任务；
- **域名、IP 连通性拨测监控**：通过 PING 的方式对域名进行周期性探测，自动化检测不容低于和运营商访问的连通性。

7.2.3 云 API

作为腾讯云为客户提供的开放生态的基石，云 API 能够覆盖所有可通过该方式对外提供服务的云产品并持续迭代，因此 API 接口安全变得尤为重要。

腾讯云为您提供的云 API 支持 HTTPS 传输加密，通过多种 SDK 签名机制（如 PHP、Python、Java、.Net、Node.js 等）进行接口鉴权，并利用 Timestamp 限制请求签名有效期，防止重放攻击，同时签名加密除了支持 HmacSHA1，还支持更安全的 HmacSHA256，实现 API 请求的安全性和合法性保证。

在提供云 API 安全能力的同时，腾讯云整合云 API 监控管理功能，您可以通过控制台设置您业务所需的 API 接口状态监测；同时，腾讯云为您提供 API 接口保护能力，可有效杜绝云 API 失效或滥用的风险。

7.2.4 访问管理

访问管理（Cloud Access Management，CAM）是腾讯云提供的一套权限管理，用于帮助客户安全地管理腾讯云账户的访问权限，资源管理和使用权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。

- **管理访问权限**：您不必通过分享主账号相关的身份凭证，即可授权给其他人员访问主账号的资源。
- **授予精细权限**：您可以针对不同的资源给不同的人员授予不同权限。例如可以允许某些子账号拥有某个 COS 存储桶的读权限，而另外一些子账号或者根账号可以拥有某个 COS 存储对象的写权限等。
- **二次身份校验**：您可以为主账号和所属子账号开启二次身份校验以提升账号安全。

- **联合身份**：可以允许已在第三方身份验证体系（例如，在您的企业网络中或通过 Internet 身份提供商）获得密码的用户获取对您腾讯云账户的临时访问权限。
- **已支持多数腾讯云产品**：有关支持 CAM 的腾讯云产品的列表，请参阅 支持 CAM 的产品 。
- **最终一致性**：CAM 目前支持腾讯云的多个地域，通过复制策略数据实现跨地域的数据同步，虽然 CAM 对策略的修改会及时提交，不过跨地域策略同步会导致策略生效延迟；同时，CAM 使用缓存来提高性能，在某些情况下可能增加耗时，在之前缓存的数据过期之前，策略更改可能不会生效。

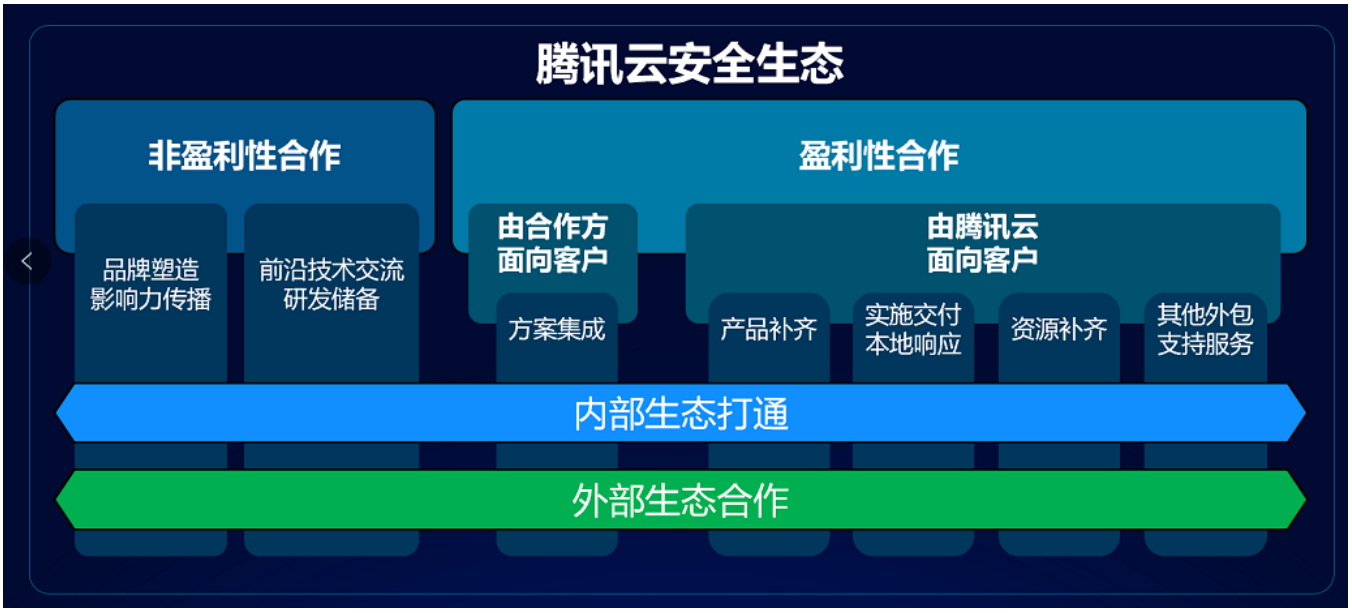
7.2.5 云审计

云审计（Cloud Audit）是一项支持对您的腾讯云账户进行监管、合规性检查、操作和风险审核的服务。您可以记录日志、持续监控并保留您账号以及所属子账号所操作的相关的账户活动。云审计记录的事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

- **简化合规**：借助云审计，您可以自动记录和存储账号及所属子账号最近 7 天内在腾讯云 API 或腾讯云控制台上已执行操作的事件日志，从而简化合规性审核。
- **跟踪集**：跟踪集是操作记录的一个增强功能。通过跟踪集，您可以进行历史事件溯源，包含记录操作日志种类信息，操作日志存储路径等。
- **用户与资源活动可视化**：云审计可视化记录了腾讯云控制台操作和 API 调用来提高用户和资源活动。
- **安全分析和问题排查**：借助云审计，您可以通过查询特定时段内账号及所属子账号所发生更改的全面历史记录，发现并解决安全性和运行问题。

八、腾讯云安全生态

云计算环境下的信息安全不再单纯依赖某一类技术或某一些人才就能完整实现。与云计算本身的“开放”特性一样，云计算服务提供商务必需要将内部和外部资源有效整合，秉持合作共赢的发展目标，才能为客户构建一个完善与健硕的云安全生态。



图表 14 腾讯云安全生态

8.1 内部生态——资源整合，“云管端”安全体系构建

作为全球最大的互联网公司之一，腾讯本身更了解企业最关心的安全问题。依托腾讯公司云管端的全局部署、七大实验室的顶尖技术、二十年安全能力的沉淀，以及海量数据的强大支撑，腾讯云致力于为整个安全生态提供全球卓越的安全解决方案。

图表 15 腾讯云安全的优势

三管齐下 – 云管端全面防护

随着云计算技术的日趋成熟，腾讯公司一直致力于打造“云、管、端”互联网产业生态平台。

腾讯云凭借腾讯公司丰富的资源和强大计算能力，进行最快速的威胁感知与溯源分析，助力整个安全生态。此外，随着云计算在各行各业的应用日趋广泛，腾讯云亦为企业云端部署保驾护航，提供从网络、主机到数据以及业务安全等全面的安全防护。

对于企业而言，作为连接内外网的关键环节，边界安全亦不容忽视。腾讯云依托哈勃分析系统[1]的核心技术，结合大数据与深度学习，可高效检测未知威胁，并通过对企业内外网边界处网络流量的分析，感知漏洞的利用和攻击，精准检测高级威胁。

着眼终端，腾讯公司将百亿量级云查杀病毒库、引擎库以及腾讯 TAV 杀毒引擎、系统修复引擎应用到企业内部，可有效防御企业内网终端的病毒木马攻击。腾讯的终端安全管理系统集终端杀毒统一管控、修复漏洞统一管控以及策略管控等安全管理功能于一体。腾讯云依托腾讯公司终端防护能力，可帮助企业管理者全面了解并防护企业终端安全。

在云管端的全面布防之下，腾讯云将内部资源充分整合到企业安全生态的建设中。

图表 16 基于企业业务纵深以及全生命周期的智慧安全体系

[1] “哈勃分析系统”是“腾讯反病毒实验室”自主研发的安全辅助平台，集精准鉴定、极速响应、全网监控能力于一身，并依靠海量分析集群、基于大数据处理的智能检测技术和业内顶尖的反病毒分析团队三大“法宝”保障用户网络安全。

七大实验室 – 国际顶尖研究团队

腾讯安全联合实验室旗下涵盖反病毒实验室、反诈骗实验室、移动安全实验室、科恩实验室、玄武实验室、湛泸实验室、云鼎实验室七大实验室，专注于安全技术研究及安全攻防体系搭建，安全防范和保障范围覆盖了连接、系统、应用、信息、设备、云六大互联网关键领域。秉持开放的心态，腾讯安全联合实验室汇聚了全球众多顶尖白帽黑客，持续为互联网安全产业进行技术输出，依托腾讯安全联合实验室，是腾讯云安全的核心竞争力之一。

图表 17 腾讯安全实验室矩阵

二十年经验 – 安全能力沉淀

腾讯在安全领域拥有长达 20 年的经验，不断吸纳前沿技术，发展了全面的安全能力。

为了助力客户更安心地部署云上业务，腾讯云积累了完善的主机安全、DDoS 防护、Web 应用防火墙等安全能力。其次，面对云计算物联网和 AI 技术的迅猛发展给企业的数据安全带来的全新挑战，腾讯云凭借腾讯在数据保护领域多年的经验，匠心打造了一款以数据为中心的全流程保护方案——数盾，通过数据审计、隐私保护、威胁抵御、量子加密等产品构建了一站式全流程的保护体系。此外，腾讯拥有极强的数据清洗能力，确保企业数据的完整性、准确性。随着企业安全和业务的关系日益密切，腾讯云依托腾讯自身的广泛业务数据和收集的黑产情报，能够精准识别潜在的业务安全风险，保障企业免受经济损失。

在边界侧，腾讯云可以依托腾讯哈勃沙箱分析采用虚拟执行技术，对边界流量解析提取出来的附件进行异步并发分析处理，一台真实物理服务器可以模拟几十个虚拟机，支持灵活的横向扩展以应对高并

发的业务需求，可实时报警、异常恢复，在无人监管模式下稳定运行，兼具网络流量检测、邮件网关检测、网闸/摆渡以及 APT 防护能力。

随着移动终端的日益普及，腾讯云亦拥有全面的移动安全防护能力，涵盖应用加固、漏洞扫描、盗版监控、真机测试、质量跟踪、安全支付等多种场景。

8.2 外部生态——多方合作，共建开放、协作、共赢安全生态体系

腾讯公司秉持“共享、共建、共赢”的原则，持续倡导构建更加和谐、繁荣的企业安全新生态，并携手合作伙伴共同推动安全产业的逐步成熟与健康发展，在行业发展、技术能力、市场运营等多方面相互融合，共同构建更加安全、更加有价值的互联网生态。

- **共享市场机会**：腾讯云为安全生态合作伙伴提供了丰富的市场机会。第一，安全生态合作伙伴可以借助腾讯云市场展现自己的产品、解决方案和服务，与腾讯一同分享腾讯云上潜在客户和销售机会。提升产品销售运营过程效率，降低成本。第二，腾讯云服务资源遍布全中国乃至全球，安全生态合作伙伴可借助腾讯资源网络，将业务迅速部署至全球范围。第三，腾讯云已同政府、教育、医疗、制造、能源、交通及各大企业建立了广泛的合作关系，合作伙伴有机会共享相关市场资源，腾讯将很乐意促进客户、合作伙伴和腾讯的共赢。

- **提供技术支持**：腾讯云向安全生态合作伙伴开放云技术服务接口，将自身能力赋能合作伙伴，助力合作伙伴商业成功。同时，腾讯云也将与安全生态合作伙伴共享安全技术能力和安全工程能力，输出安全经验，共享安全资源，通过培训、认证、开发接口、技术文档、安全标准、流程规范、安全测试等多种方式赋能给合作伙伴，从而帮助合作伙伴提升自身的安全能力。

- **联合安全咨询服务**：腾讯云与国际知名咨询机构建立了深入合作，帮助用户设计行业安全解决方案及商业模式，加速行业数字化转型。同时，腾讯寻求与各行业优秀厂商开展深度合作，为教育、医疗、制造、能源、交通等行业开发安全解决方案，实现商业共赢。

- **开放云生态资源：**腾讯云除开展安全技术与咨询服务合作外，还在云安全标准、开源社区积极参与、主动贡献，为云计算产业健康发展贡献力量。此外，腾讯云还开放各种基础能力及安全服务，为软件及应用开发者提供安全服务。

附录

附录 I：腾讯云隐私声明

查看腾讯云隐私声明：*https://cloud.tencent.com/document/product/301/11470*

如对隐私声明或相关事宜有任何问题，请通过 https://console.cloud.tencent.com/workorder/category 或拨打 4009-100-100 与我们联系。

腾讯云