# 腾讯云安全白皮书

2016 年 11 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】**

2016 年 11 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。

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，安全，值得信赖

# 序言

2016 年 3 月的第十二届全国人民代表大会第四次会议上，总理李克强在作政府工作报告时提到强化创新引领作用，为发展注入强大动力。政府与社会应当促进大数据、云计算、物联网广泛应用。加快建设质量强国、制造强国。到 2020 年，我国将力争在基础研究、应用研究和战略前沿领域取得重大突破，全社会研发经费投入强度达到 2.5%，科技进步对经济增长的贡献率达到 60%，迈进创新型国家和人才强国行列。

云计算被称为第三次信息时代的革命，以一个颠覆行业的姿态出现在个人电脑、互联网时代之后，再一次改变着人们的生活方式与思考模式。作为互联网新发展时代的主旋律，云计算必将成为“中国制造 2025+互联网”的推动器与基础支持。

作为中国云计算领域的领军者，腾讯云在 2016 年 7 月召开的“云+未来”峰会中，由腾讯公司控股董事会主席兼首席执行官马化腾先生阐述了腾讯云的战略规划，明确提出“互联网+”基础设施的第一要素就是云计算，区别于数据中心托管的传统概念，云计算已包含在“互联网+”和信息能源的发展趋势之中；马化腾先生同时强调云计算安全的重要性，他进一步表示腾讯云的平台级战略是成为一个设防的云上生态，为生态链上的合作伙伴创造一个安全的云端基础环境。

此外，当前的互联网业务时刻承受着各类黑产攻击，如网络黄赌毒的病毒式传播、个人隐私大量被窃取与滥用、线上黑产多样化蔓延等。应对如此庞大的黑色产业所带来的风险，无疑需要耗费更多的资源成本，这对于很多中小企业自身来说是难以企及的，他们更渴望从云计算平台中获得开放、灵活、可定制的智能安全防护能力。腾讯作为一个集团级别的开放平台，在过去 18 年间所积累的不只是黑产对抗经验，更输出了高度工具化的云端安全引擎，为互联网用户构建了以大数据与人工智能为核心的互联网业务安全防护体系，让选择腾讯云的企业时刻都能沉着应对各类黑产的挑战。

腾讯云作为行业标杆，将持续在云计算安全方面加强自身建设与内外合作，依靠自身实力优势和生态链上的专业伙伴共同打造一个安全的云端环境，以高速（Speed）、稳定（Stability）、安全（Security）、服务（Service）为核心品牌理念，助力中国云计算领域平稳快速的发展。

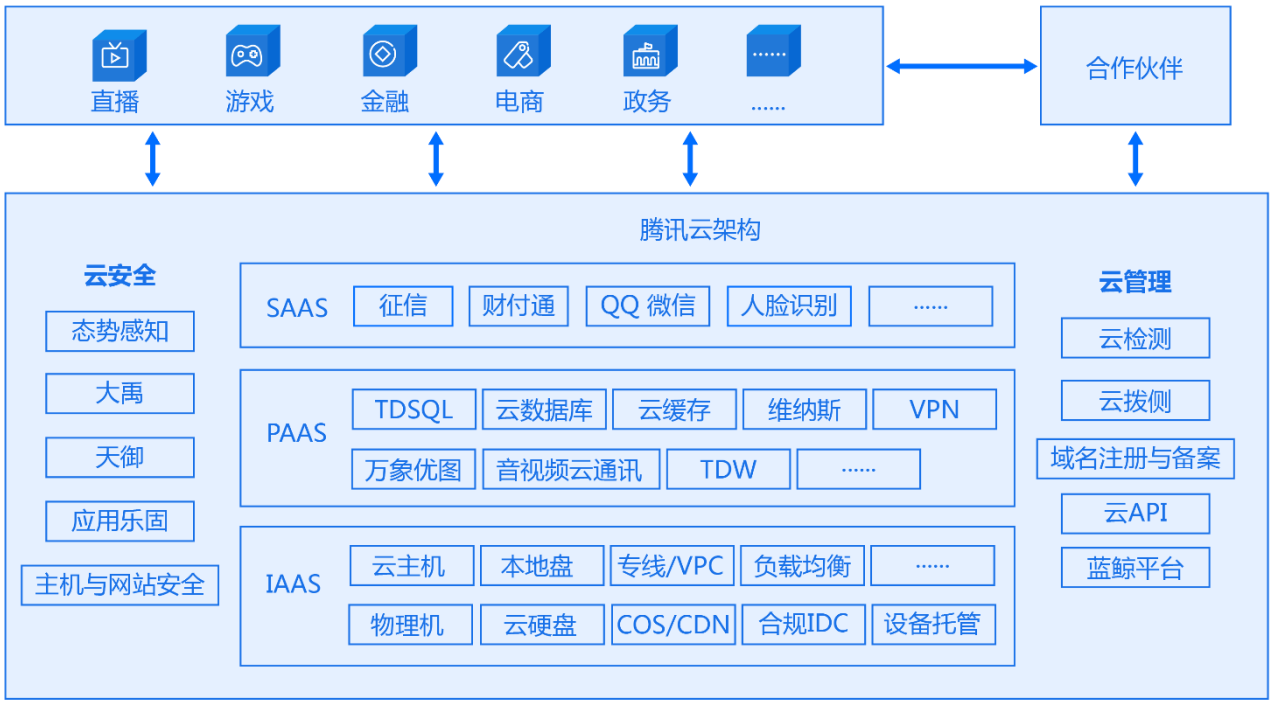
# 目录

# 图示目录

# 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计算整体架构：




**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，包括安全体检（漏洞扫描、挂马检测、网站后门检测、端口安全检测等）、安全防御（DDoS 防护、入侵检测、访问控制来保证数据安全与用户隐私）以及安全监控与审计，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。

腾讯云能够提供行业领先水平的私有网络、高性能数据库、专线接入等服务，并且，腾讯云将核心聚焦于安全领域，不断优化腾讯云产品自身的安全性能与其管理体系的安全管控能力。

此外，腾讯云还致力于云端大数据解决方案的整合，为企业提供了一站式数据分析与挖掘服务平台，覆盖基础平台、通用数据应用及行业解决方案在内的多个产品及服务。通过多维度定向与关联，腾讯云持续着力于数据的广度与深度的挖掘，形成海量的数据关联，并将其利用于对抗黑产的过程中，主动排查与规避风险，同时协助政府部门有效打击网络黑产。

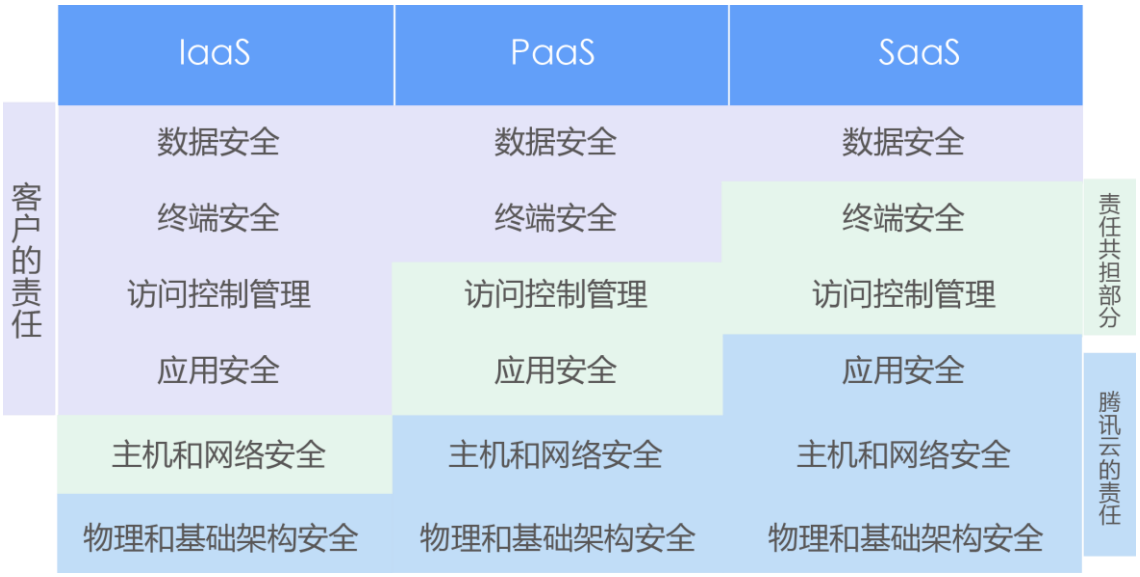
腾讯云一直坚持以创建安全、开放、共建的云生态与提供稳定、优质的服务为理念，来响应国家对于“网络安全和信息化工作扎实推进”的号召，促进整个云计算安全的构建。

# 二、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；您更可在第三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 2 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 [注1]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，类型主要包括云主机、云存储、负载均衡、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对数据安全、终端安全、访问控制管理和应用安全负责。

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、数据库管理系统、磁盘阵列网络等云产品底层系统

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。

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、数据库实例文件、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。此外，腾讯云提供基础的外部 DDoS 防护能力，以保护处于云计算平台网络中的各类资源不受来自互联网的拒绝服务攻击影响；客户有责任维护并管理已购买的云产品和内部数据，类似如因客户管理不当造成的云主机主动或被动向外发起恶意攻击（如 DDoS 攻击、网络嗅探、病毒木马攻击等）的情况则不在腾讯云的责任范围。

**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、音视频云通信等。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要对数据安全和终端安全负责。

应用安全和访问控制管理则由客户与腾讯云共同承担。其中，在应用安全层面：腾讯云通过对平台类云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云产品进行正确的使用配置，并根据更高的安全需要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云产品的账号和权限。


**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：腾讯云通过天御业务安全产品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。

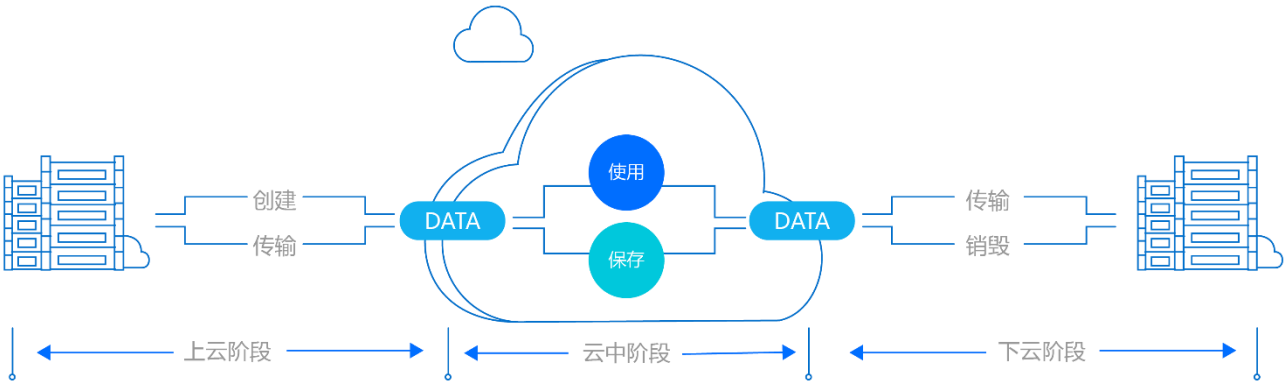
**整个 SPI 云计算架构中：**

数据的安全性是您（作为数据唯一的所有者）在利用云计算环境进行任何业务活动都需要慎重考虑的关键因素之一。因此，您需要负责确保数据被安全地识别与分类，并在云计算环境下整合数据防泄密、数据存储加密等必要的技术手段。腾讯云提供的专家服务和一对一的技术支持，能够帮助您设计有效、合理的云计算环境数据保护措施，让您在使用腾讯云提供的 IaaS、PaaS 和 SaaS 层云产品和服务的同时，获得至下而上的全面安全保障。

# 三、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？*

## 3.1 安全的云上数据




**图表 3 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 3.2 节中将向您介绍一些数据保护的最佳实践供参考。

### 3.1.1 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。

### 3.1.2 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。

### 3.1.3 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逻辑擦除或物理擦除方式，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。

## 3.2 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。

### 3.2.1 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；

### 3.2.2 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、内部审批及相应技术支持，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。

### 3.2.3 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、虚拟控制层操作系统、数据库管理系统等。作为腾讯云公有云产品的使用者，您仍需要关注基于共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。

## 3.3 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。

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

# 四、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？*

## 4.1 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，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。

### 4.1.1 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，在任意单设备故障情况下，均能确保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、自动气体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，且均安装接地线，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。

腾讯云计算节点覆盖华南、华东、香港、海外等多个地区，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数据中心或不同区域，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。

### 4.1.2 访问控制制度

腾讯云对数据中心不同区域定义了的三类安全级别：

- **一般安全区域**，不存放公司运营设备，不涉及公司业务信息，不影响机房整体运营的公共区域，如园区等；

- **受限安全区**，存放非重要运营设备，不涉及财务及敏感信息，不影响机房整体运营的区域，如 IT 机房、库房等；
- **高度受限安全区**，存放重要设备，涉及公司财务及敏感信息，影响机房整体运营的区域，如基础设施区、数据中心机房等。

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，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。其中，门禁授权系统按照不同安全等级和不同功能的区域进行划分，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。

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；所有外部人员（访客、供应商技术人员、代维人员等）在机房、库房等受限区域进行操作时，均须通过正式审批授权并由安全专人陪同；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。

### 4.1.3 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，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。

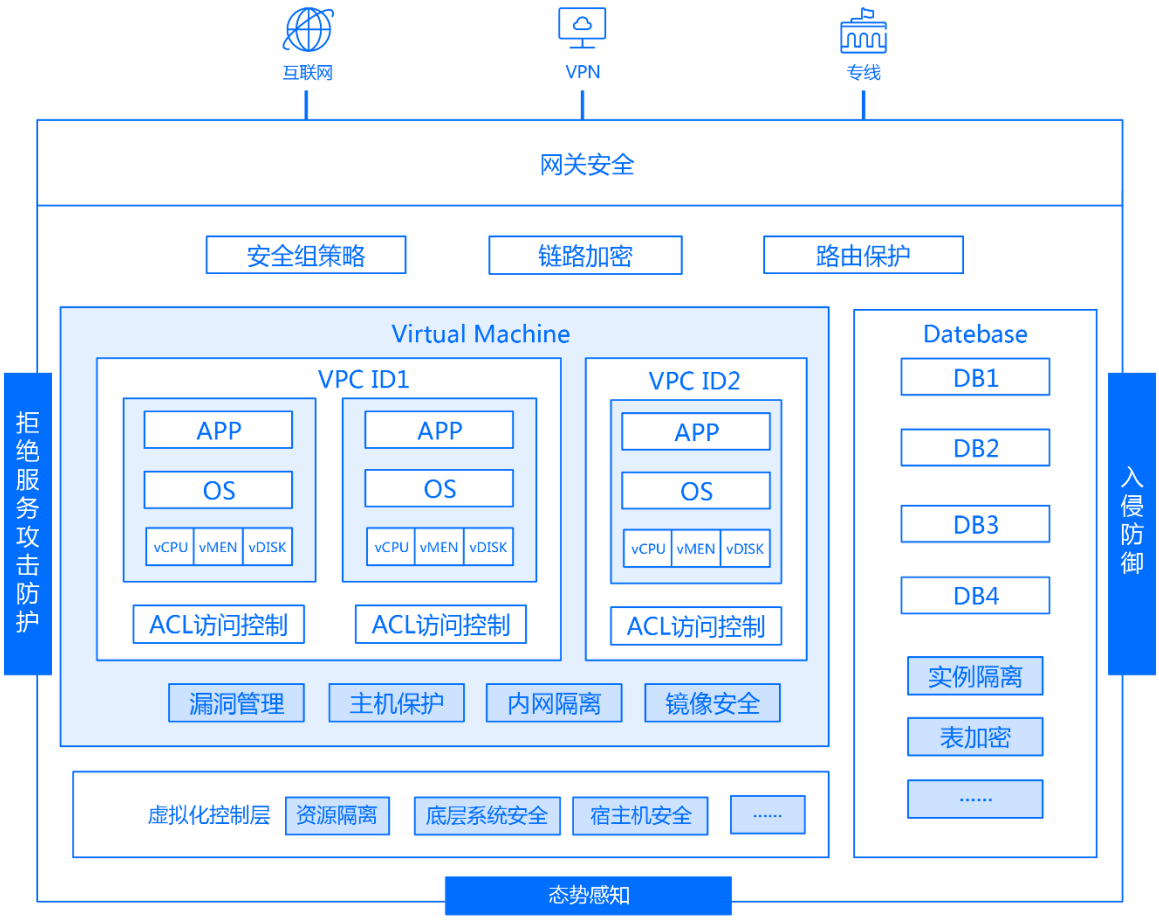
**物理安全审计**

同时，为了确保上述措施和规范的落地执行，腾讯云统一建立了定期安全审计管理制度，每个季度对物理安全现场操作和管理进行审计，并输出内部审计报告，跟进和推动物理安全审计风险点的改进。

## 4.2 网络安全

### 4.2.1 安全架构

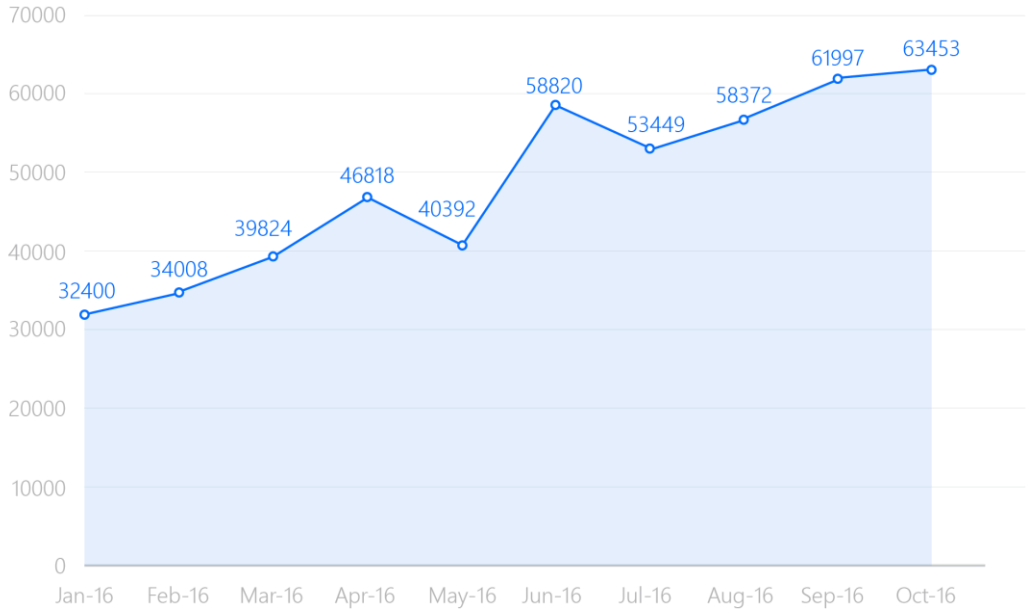
腾讯云提供成熟的网络安全架构，包含防火墙、分布式防护、入侵防御、web 应用防护等多重防护机制，以应对来自互联网的各种威胁。



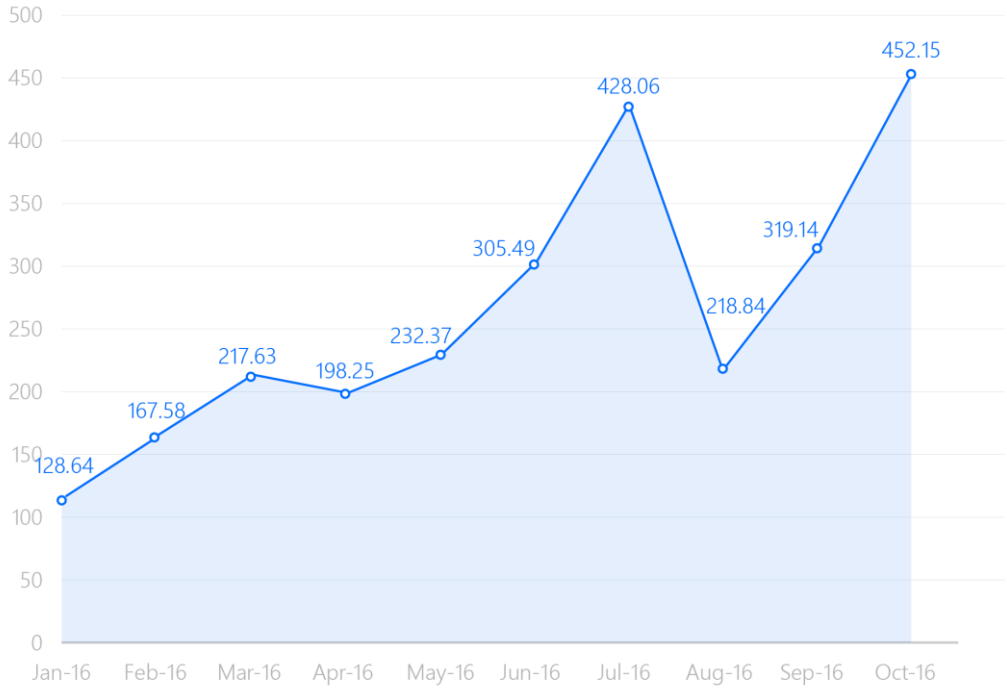

**图表 4 腾讯云网络安全架构示意图**

针对 DDoS 攻击，腾讯云为您提供高效的分布式防护能力。其中，BGP 高防，接入 21 线 BGP 线路，全面覆盖国内外主流运营商，带来极速、稳定的访问体验，同时拥有 4T 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；此外，针对网站类业务，我们提供

网站高防，通过高效动态调度网络流量，有效组织起腾讯云全国上百个防护节点的冗余带宽和防护能力，提供最高 4T 的防御能力。截止 2016 年 10 月份，腾讯云累计本年抵御近 50 万次 DDoS 攻击，攻击峰值超过 400Gbps。

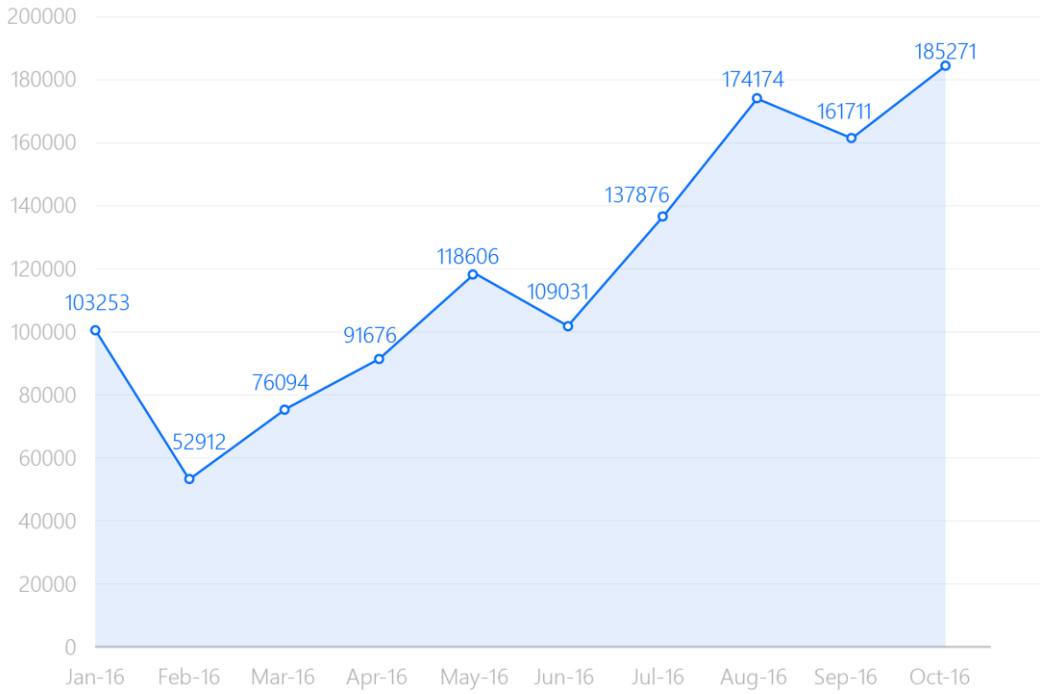



**图表 5 2016 年 1 月-10 月 腾讯云 DDoS 攻击防御次数统计**




**图表 6 2016 年 1 月-10 月 腾讯云 DDoS 攻击防御流量（Gbps）统计**

为了更好地保护客户网络安全，腾讯云提供了专业的入侵防护服务。在 2016 年上半年，Web 与主机防护层面都有非常出色的表现。在 Web 防护层面，累计检测发现 Web 漏洞 120 万个，WAF 累计拦截 3 亿多次 Web 漏洞攻击，累计发现 Webshell 超过 1 万个。在主机防护层面，主机暴力破解自动拦截功能从 2016 年 1 月-10 月拦截暴力破解月度数量统计达到 14 亿多次。




**图表 7 2016 年 1 月-10 月 腾讯云漏洞防护月度数量统计**

网络接入安全方面，腾讯云的所有外网接口统一由 Tencent Gateway（TGW）进行处理，TGW 具有可靠性高、扩展性强、性能高、抗攻击能力强等特点，提供了更加高效和安全的网络访问。内网接口可由腾讯云自动分配（基础网络），也可由用户自定义（私有网络）。

### 4.2.2 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。

### 4.2.3 网络隔离

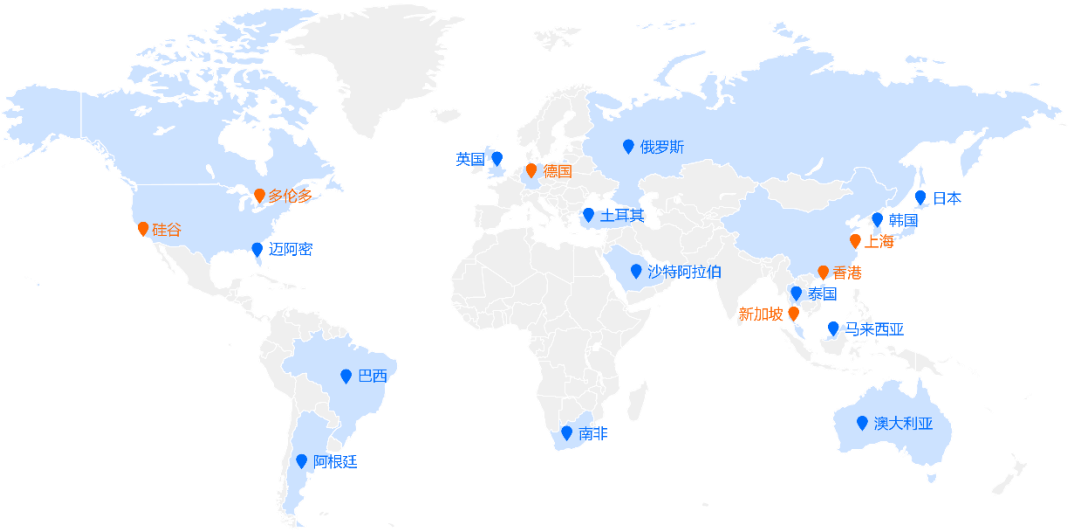
腾讯云制定了严格的内部网络隔离规则，通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护；腾讯云确保非授权人员禁止访问任何内部网络资源；以及，所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机登录生产系统。

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。

### 4.2.4 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，在全国拥有超过100+节点，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。

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 8 腾讯云全球网络示意图**

## 4.3 面向客户的基础云产品

### 4.3.1 大禹网络安全

基于多年的网络恶意流量检测和清洗经验，腾讯云为您提供集 DDoS 防御、DNS 劫持检测与网络安全认证等功能于一身的云安全防护能力——大禹网络安全（DAYU）。


图表 9 大禹网络安全功能示意图

**DDoS 防护**

根据不同客户的互联网业务需求，大禹网络安全提供以下 DDoS 防御能力：

- **基础 DDoS 防护：**腾讯云向所有主机提供最高 2Gbps 的免费 DDoS 基础防护，精准清洗来自互联网的 Syn Flood、ICMP Flood、UDP Flood 等大流量攻击；同时，在客户所购买的云主机等产品中，基础 DDoS 防护能力还能通过模式识别、身份识别等技术方式，结合重认证、验证码、访问控制等业务安全手段（请参考第六章相关介绍），精准有效抵御 CC 攻击。
- **BGP 高防：**BGP 高防可提供高达 4Tb 的防护带宽，能有效防御大流量 DDoS、CC 和其他各种拒绝服务攻击，客户可绑定至同一大区内已有的云主机或负载均衡，为该设备提供高防服务。一个

高防服务包可绑定一台设备，并且用户可自主更换高防服务包所绑定的设备，灵活为需要防护的设备提供防护。

- **网站高防：**网站高防是腾讯云安全团队多年来自研安全技术积累的成果，防御能力的峰值最高可达 4T，同时支持 HTTP 与 HTTPS 协议，可为电商、互联网金融等各类网站的开发商们提供专业的 DDoS 与 CC 攻击防护服务。网站高防还提供源站隐藏功能，在您的网站接入大禹网站防护后，该功能即自动开启，解析您的网站返回的将是大禹系统的防护节点 IP。使用源站隐藏功能后，您的网站源 IP 将不再暴露，攻击者将无法直接攻击您的网站服务器。此外，您只需将您的网站 DNS 结果配置为腾讯云提供的网站高防系统，即可快速接入。

大禹网络的 DDoS 分布式防御体系在全国拥有多个攻击防护点，高效动态地调度网络流量，为开发商业务的高可用性保驾护航。

**DNS 劫持检测**

DNS 劫持是一种通过改变指定域名在运营商侧 Local DNS 配置的正确解析指向，将该域名的解析结果重定向到劫持 IP 的劫持行为。Local DNS 劫持类型可大致分为运营商缓存、广告、恶意劫持等类别。其中，运营商缓存是运营商为了降低跨网流量及用户访问速度进行的一种良性劫持；广告劫持是运营商或恶意团体将用户正常页面指向到广告页面或在正常页面中插入第三方广告的劫持行为；恶意劫持是指通过改变域名指向 IP，将用户访问流量引到挂马，盗号等对用户有害页面的劫持。

腾讯云的 DNS 劫持检测由遍布在全国的数据中心和客户端超过 400 个探测指针构成，模仿真实用户周期性地向本地的 Local DNS 发送域名解析请求，基于域名解析结果，检测客户的网站是否被当地网络运营商劫持，从而快速、准确、全面的发现域名劫持行为。

**网站安全认证**

大禹网站安全认证，是腾讯云针对网站可信度推出的增值服务，包含了云安全服务开通审计、Web 内容安全审计、Web 漏洞检测以及主机基线检测四大功能检测。使用了大禹网站安全认证服务并通过腾讯云安全检测的网站，其 URL 将在腾讯社交平台上获得权威安全认证的展示，获得用户信任，提升您的品牌美誉度。


**图表 10 腾讯云网站安全认证示意图**

### 4.3.2 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。

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：

- **主机安全：**腾讯云凭借多年的安全经验实现入侵行为的快速发现，针对 web 应用和底层系统，采取分布式的数据采样加集中分析防护的模型，匹配入侵规则之后进行报警和防护。同时为您提供高效、精准的主机安全功能，包括主机安全监控、追溯查询、策略管理和升级服务等。您可以方便快捷地使用以下功能：

| 类别 | 功能 |
| --- | --- |
| 主机安全监控 | 木马检测 |
| | 账号安全检测 |
| | 异常行为监控 |
| 追溯查询 | 入侵取证追溯 |
| | 软件指纹采集 |
| 策略管理 | 自定义策略 |
| | 白名单<br>下发脚本 |
| 升级服务 | 策略库 |

- **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。腾讯云提供的公共镜像由内部专业安全运维团队制作并严格测试后向公众用户发布，可选择搭配内置的腾讯云安全组件，强化公共镜像安全。服务市场中的镜像由第三方服务商制作，入驻的服务商均需经过腾讯云严格甄选并签订入驻协议，镜像本身均经过服务商严格测试，并通过腾讯云官方审核后进行发布，以保证镜像内容的安全性。

此外，您可使用镜像制作功能定制镜像并导入自己的实例，且只有本人账户可以使用；也可与建立联系的其他腾讯云用户共享各自的自定义镜像。需要注意的是，由于其他用户共享的镜像不经过腾讯云审核，可能存在安全风险，因此建议您不要接受出自未知来源的镜像。

- **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，从系统漏洞、虚拟层漏洞、应用层漏洞等方面进行全面而深入研究，形成有效的漏洞处置手段，为客户提供更安全的产品。同时 ，腾讯安全应急响应中心 TSRC（Tencent Security Response Center）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。
- **安全加固：**安全加固组件是腾讯云提供的一套先进的主机入侵防御服务，可及时有效发现服务器的异常情况，包括后门木马检测，黑客入侵检测，以及发现未经授权登录和暴力破解。一旦存在异常情况，安全加固组件可以实时发现并提醒您，可有效避免服务受损、核心数据被盗的风险。
- **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，内容包括每一个产品的业务容灾特点、详细的应急响应流程、人员的详细职责和联系方式、恢复点目标 RPO 和恢复时间目标 RTO 等内容，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。腾讯云也为不同的用户提供具有针对性的业务运营层面的连续性服务支持，包括协助您设计不同业务场景需求、策划业务连续性演练方案等，使您能够在实现至下而上的业务稳定性保障的同时，更好地满足监管机构及企业自身的业务连续性合规要求。
- **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。此外，腾讯云还为更高要求的用户提供具有宿主机隔离能力的云产品——专用宿主机 CDH，在物理层面实现资源隔离，确保满足如金融行业等强监管要求。

***网络类产品：***

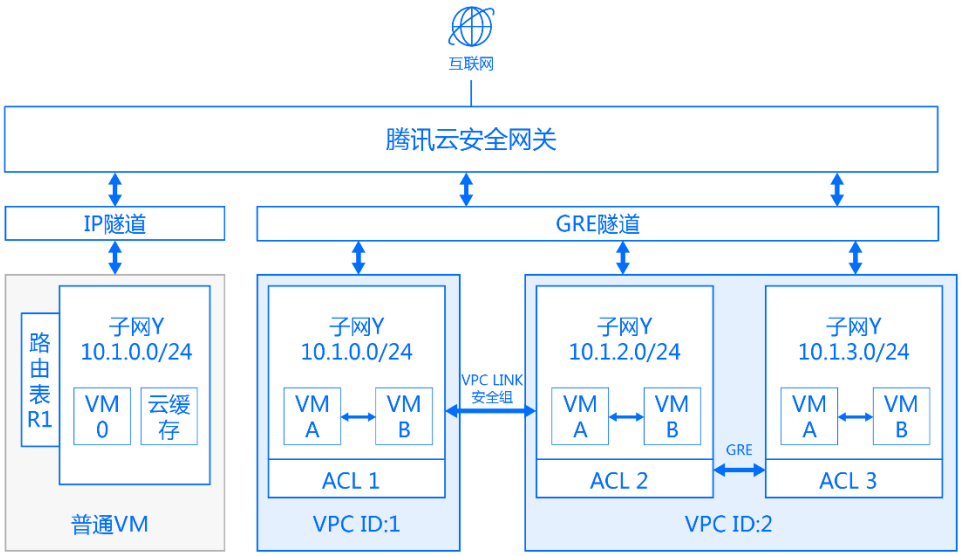
私有网络 VPC（Virtual Private Cloud）帮助您在已购买的云平台资源中构建出多个独立网络空间，并自定义网段划分和 IP 地址、自定义路由策略等；同时，您可以通过部署基于互联网 IPSec VPN 的隧道将云平台私有网络与您企业内部的其他资源连通。

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。

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。通过 NAT 网关和访问控制策略能够保护云平台私有网络内的资源不被非授权访问和攻击，可以有效避免暴露您的云平台网络部署信息。
- **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 ACL 是一个子网级别的无状态可选包过滤虚拟防火墙，可以精确到协议和端口维度，有效控制进出子网的数据流量；安全组是一种有状态的包过滤虚拟防火墙，它用于控制单台或多台云服务器的出入流量，同样可以精确到协议和端口维度。
- **网络隔离：**云用户的网络隔离是云计算平台的一项重要安全功能。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。VPC 私有网络还具有主机维度的安全防火墙功能，您可控制云主机的出站、入站流量，配合网络 ACL 功能让您的资源安全可控。




**图表 11 VPC 安全功能示意图**

### 4.3.3 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**：COS 针对 Bucket 提供防盗链配置功能，可配置黑名单和白名单，以约束访问来源，当恶意的访问来临时，防盗链可以替您将恶意访问抵挡在门外，大幅度减少流量盗刷。
- **多种攻击防护**：将 COS 协同 CDN 使用，还可以有效为您抵御 CC 攻击和 DDOS 攻击，过滤恶意攻击数据包，清洗出正常流量，有效避免因攻击而导致的业务无法正常使用。
- **完善的权限体系**：COS 提供协作者机制和资源分权限管理体系，当您的团队操作资源时，可以有效将各种权限拆分再细化到每一个角色，保证了团队合作中权责清晰，进而使数据处在一个安全和私密的环境之中。

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 12 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。若您的业务已经具备了特定的 URL 鉴权算法，腾讯云 CDN 可以为您提供定制化服务，保证您的鉴权方法无缝迁移至 CDN 节点。

- **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：**将 COS 协同 CDN 使用，还可以有效为抵御 CC 攻击和 DDOS 攻击，过滤恶意攻击数据包，清洗出正常流量，避免了因攻击而导致的业务无法正常使用。

### 4.3.4 云数据库

腾讯云目前提供多种数据库产品，云数据库 CDB（Cloud DataBase CDB）是腾讯云提供的关系型数据库云服务，基于 PCI-e SSD，高达 245509 QPS 的性能。CDB 同时支持 MySQL、SQL Server、TDSQL（兼容 mariaDB）引擎。

腾讯云还提供兼容 Redis 协议的缓存和存储服务云存储 Redis CRS（Cloud Redis Store），完全兼容 MongoDB 协议的高性能 NoSQL 数据库云数据库 MongoDB（Cloud MongoDB Service）和完全兼容 HBase 协议的云数据库 HBase（Cloud HBase Service）。

此外，我们还拥有自主研发的极高性能、内存级、持久化、分布式 Key-Value 存储服务云缓存服务，Memcached（Cloud Cache Service Memcached），适用于高速缓存的场景，兼容 Memcached 协议，支持自动水平拆分的高性能分布式数据库 DCDB for TDSQL——即业务显示为完整的逻辑表，数据却均匀的拆分到多个分片中，每个分片默认采用主备架构，提供灾备、恢复、监控、不停机扩容等全套解决方案，适用于 TB 或 PB 级的海量数据场景。

在云数据库安全层面，腾讯云具备以下安全性能，为您的服务保驾护航：

- **数据库实例隔离：**云数据库采用物理机，并在此基础上采用 VPC 网络和 Cgroup 技术，对网络与机器上的实例实现了严密隔离。同时，采取严格的权限管理措施，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。因此，我们不但能保证数据库实例之间的隔离，也能保证数据库实例在网络中的安全。

- **服务高可用和数据高可靠：**腾讯云根据不同的数据库产品通过实时双机热备，宕机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产品的服务高可用性。通过主从数据实时热备和冗余存储等方式来提供数据高可靠性。

# 五、运营管理安全

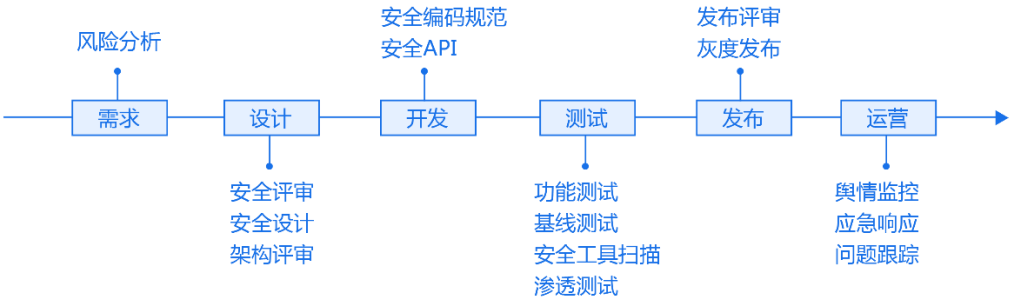
- *我如何对云产品的运行状态进行监控？*
- *我在使用云产品的过程中若发生问题如何寻求帮助，能否得到及时响应？*

## 5.1 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。

### 5.1.1 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：



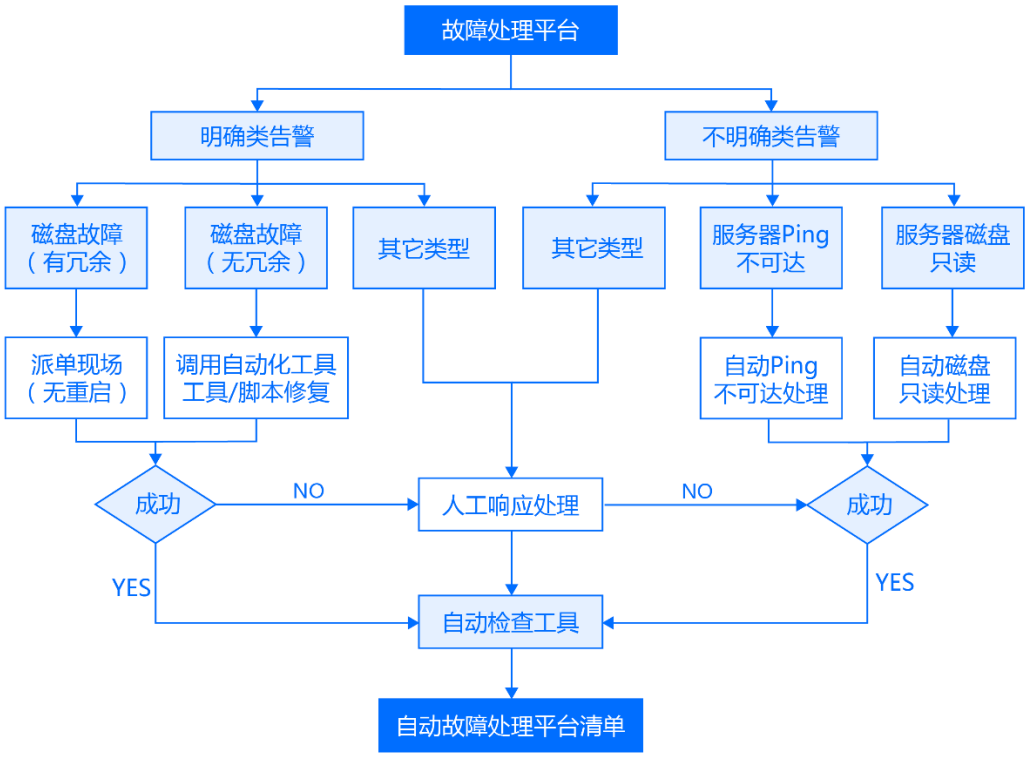

**图表 13 腾讯云安全开发流程示意图**

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 14 腾讯云故障自动化响应与处理示意图**

### 5.1.2 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。

### 5.1.3 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。

### 5.1.4 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、虚拟化控制层、关键应用服务等），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。

### 5.1.5 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，确保在您提出问题或请求的当天达到 95%的成功解决率。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。

## 5.2 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。

### 5.2.1 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。

### 5.2.2 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。

### 5.2.3 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。

一个典型的 API 接口请求如下：

```
https://domain/v2/index.php?Action=DescribeInstances
&SecretId=xxxxxxx
&Region=gz
&Timestamp=1402992826
&Nonce=345122
&Signature=mysignature
&instanceId=101
```

**图表 15 腾讯云云 API 接口示意图**

注：Action=DescribeInstance 表示查询云服务器实例的详情

instanceId 为指令参数，其余为通用参数

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 API 公共参数（如 Nonce 和 Timestamp）防止重放攻击，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。

# 六、业务安全

- *能否通过腾讯云产品防止我的用户恶意刷单？*
- *若有用户在我提供的服务平台上发布非法言论或视频，我该怎么办？*
- *我的业务同时面向移动端用户，能否对此进行保护？*

基于腾讯多年的业务安全对抗经验和业界最具权威的黑产数据库，腾讯云致力于为客户提供更有价值的安全服务。当行业内仍在思考如何优化安全能力建设的投入产出比时，腾讯云已经完成安全能力的业务输出，将自身的信息安全技术与经验转化为客户能够感知和应用的云计算安全产品。

您即刻便能以极低的消费成本，获得需要数年时间和大量资金才能自建完成的业务安全技术支撑。

## 6.1 应用安全保护

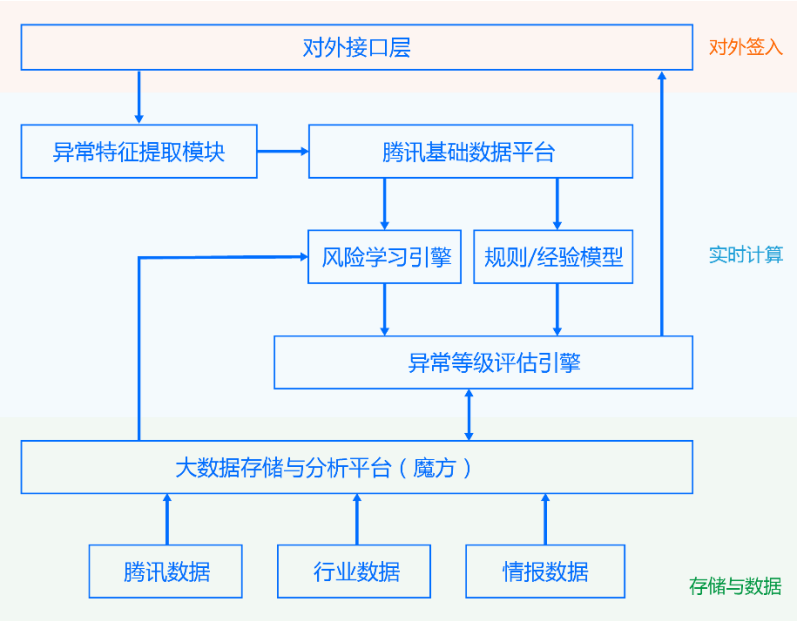
天御业务安全防护（Business Security Protection）是腾讯云针对互联网业务场景提供的多功能安全产品。


**图表 16 腾讯云天御 BSP 功能示意图**

任何互联网化的商业行为都可能受到来自攻击者或竞争者的恶意行为攻击。区别于传统以应用或系统本身为防护目标的安全思路，天御 BSP 让您的应用通过标准的接口和简单的开发，快速获得多种业务风险场景下的安全保障。准确、高效、便捷的安全特性让天御 BSP 正在迅速成为商业用户首选的云计算业务安全防护手段。

基于腾讯十多年的技术模型创新和数据分析能力沉淀，腾讯云设计出了一套业务层面的互联网安全防护技术框架。该技术框架作为天御 BSP 在注册保护、登录保护和活动防刷等产品服务的核心基础，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，确保各类异常行为特征都能被及时发现和响应。




**图表 17 腾讯云天御 BSP 安全防护技术框架**

天御 BSP 基于腾讯云先进的安全技术架构，能够带来毫秒级别的服务响应和数万级别的并发会话，并可配合预定策略实现安全能力动态扩容；同时，无论是注册保护、登陆保护、活动防刷等用户交互安全服务，或是消息过滤、图片鉴黄等内容安全服务，天御 BSP 利用强大的机器学习能力为您提供准确、全面的业务安全保障。

### 6.1.1 用户交互安全

真实有效的用户群体是互联网业务运营的根基。天御 BSP 通过腾讯云大数据分析能力，以及多年的黑产数据库积累、用户交互行为特征分析，建立了一套用户交互安全的风险模型，实现预先风险识别和告警；风险模型对用户交互的异常行为极为敏感，能够多维度分析用户的账号信息、数据来源、登录方式、跳转页面等信息，及时有效地识别出真机批量注册、自动机批量注册、账户盗用、垃圾账号申请、撞库登录、盗号登录、自动批量登录等多种恶意交互行为，并提供相应的防护措施建议，帮助您或您的企业减少因互联网业务层面的用户隐私泄漏、财产损失和商誉受损等严重风险带来的损失。

此外，腾讯云还为金融行业客户量身定制了反欺诈服务，依靠天御 BSP 的黑产情报雷达系统的丰富情报收集和自动学习能力，能够全面掌握互联网金融相关的黑色产业特征，包括黑产行为模式、从业人员规模、团伙地域划分、专业工具使用等，并结合客户业务场景和实际需求提供针对性的反欺诈打击策略。

用户交互安全服务可为您提供如下的业务安全能力：

1. **黑产情报收集：**腾讯云 7*24 不间断黑产情报收集雷达，帮助您及时、全面的掌握互联网黑产的行为特点、人员规模、团伙地域划分以及专业工具等信息，并为您的业务活动提供针对性的安全打击策略；
2. **反代理 IP 保护：**恶意用户在注册或登录时会利用 VPN 网络或 proxy 代理等方式隐藏真实 IP 信息，并绕开传统的 IP 频控安全策略。用户交互安全服务深度识别来自 Web、HTML5、App 等渠道的批量代理行为，并可提供信息溯源；
3. **设备指纹识别：**通过用户交互安全服务 API 对接腾讯生态多年积累并持续更新的设备指纹库（包括手机、移动智能设备、平板电脑、个人电脑终端等），快速识别恶意用户所采用的恶意/虚假设备信息；
4. **安全数据分析：**基于腾讯生态积累的黑产大数据，能够为客户提供覆盖社交、游戏、电商、O2O、支付、互联网金融、自媒体等多领域超 500 个业务场景的安全行为分析，深度挖掘“羊毛党”用户的恶意行为特征；
5. **防刷引擎保护：**在传统的 IP 限制、账号限制、验证码等防刷策略之上，活动防刷服务利用腾讯生态的黑产大数据样本，通过组合矩阵最大程度来识别并阻止“羊毛党”用户的对抗行为；
6. **反欺诈打击策略：**

- 贷前检测：腾讯云能够帮助互联网业务的银行、证券、保险、P2P 等行业客户在新用户提交信贷申请时进行欺诈行为判断。反欺诈服务能够精准识别出虚假申请、冒用身份申请、高危用户申请、机构代办、多头借贷、组团骗贷等风险行为；
- 贷后监控：腾讯云的反欺诈服务会实时更新补充现有的欺诈信息库。金融客户可针对自己存量的信贷用户定期进行反欺诈检测，能够获悉信贷用户是否存在跨平台逾期问题、多头借债以及用户异动等恶意行为，让您的企业第一时间获悉接待人的信用健康状况，减少坏账逾期等风险的发生。

7. **风险分级验证：**根据用户提供的账号、代理、设备等多维度信息，综合判定注册用户的风险等级并提供相应的管控手段：
   - 可信等级：正常使用业务；
   - 可疑等级：建议增加多因子交互验证机制；
   - 恶意等级：注册请求拦截/强制增加额外的交互验证。

### 6.1.2 消息过滤

互联网业务运营在交互过程中将产生大量用户生成内容（User Generated Content），如何对这些内容进行安全识别则成为一大难题。针对论坛发帖、消息评论、弹幕留言、聊天对话等多种信息交互场景的内容安全，天御 BSP 消息过滤服务应运而生。其特有的反干扰引擎，通过其文本预处理和 OCR 识别等方式，将符号、图标、拼音和外文等干扰信息进行还原，轻松识别恶意用户或黑产团伙的“障眼法”；同时，消息过滤服务基于腾讯生态积累的业界最全的脏词库和多模型匹配技术，为您提供业界领先的脏词扫描技术。


图表 18 腾讯云天御 BSP 消息过滤功能示意图

消息过滤服务通过特征收集和智能学习方式，构建以下三大特征模型，主动识别用户的恶意转发、推广等行为：

1. **设备指纹模型：**利用腾讯生态的海量黑产数据库，从手机、移动智能设备、个人电脑终端等多个方面收集了恶意用户的设备指纹信息，提高实时恶意行为的门槛；
2. **文本特征模型：**消息过滤服务的文本特征主要包括获利特征、引流文本特征、噪音文本特征等内容。通过这些文本特征的识别发现可疑的用户内容；
3. **图片引流识别模型：**消息过滤服务集成 OCR 图片识别能力，可以对广告/色情类图片发挥良好的识别效果。

### 6.1.3 图片鉴黄

天御 BSP 图片鉴黄服务采用全球领先的腾讯优图 DeepEye 主动色情识别技术引擎，为您提供 7*24 不间断鉴黄服务。DeepEye 引擎日均识别上亿张图片，通过智能深度学习算法不断学习错判样例，目前已经达到 99.9%以上的色情识别准确率；同时，针对业界难题——色情与性感图片界定，采用分离图谱技术实现更加智能和精准的判别，确立了 DeepEye 引擎在图片鉴黄领域的行业领军地位。

图片鉴黄服务在进行内容识别之后，会进行图片的置信度评分，针对高置信度（最低误判率显著低于人工审核误判率）图片可直接定义为色情内容，对于次高置信度图片可按评分优先级进行人工二次审核确认；图片鉴黄服务可结合其他用户信息（如黑产大数据），为您识别出恶意用户的行为特征，立体化打击色情传播。

此外，腾讯云更能通过 DeepEye 引擎为提供直播服务的客户进行动态内容鉴黄，能够确保直播视频在对外呈现之前均经过内容鉴定。同时，对于违规的色情直播行为进行及时截图、发现和通知回调业务处理，并可根据需求自定义鉴别的时间段、房间信息、鉴别频率等，从而实现对重点直播房间的监控。

### 6.1.4 验证码

腾讯云为客户同时提供字符验证和交互验证两大类别的验证码安全服务，用户可通过灵活、便捷的设计实现字符和交互验证在不同场景的动态切换。该验证码服务通过美观友好的界面、全终端适配的特性以及防自动破解的动态更新机制，在带给用户优秀的交互体验的同时，确保您的互联网业务系统得到更安全的保护。


**图表 19 腾讯云天御 BSP 验证码功能示意图**

## 6.2 移动安全保护

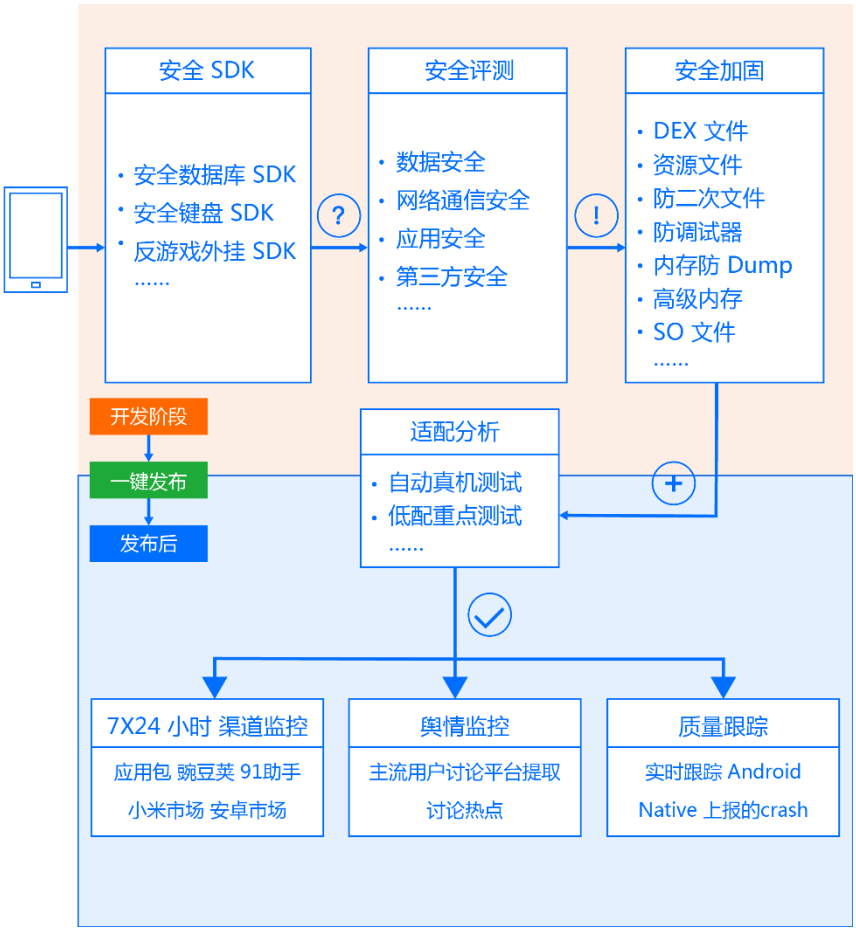
在移动互联网业务爆发式增长的同时，也带来更多用户隐私和业务风险等安全挑战。腾讯云不断在该领域进行探索研究，致力于为您的企业和用户提供全面的移动安全保护机制。

### 6.2.1 乐固

腾讯云乐固（LEGU）获得了数据中心联盟主导的 2016 年第一批移动安全加固能力认证。乐固是针对个人和企业开发者的一站式移动安全解决方案，您可利用腾讯云控制台提交自己的 APP 应用，获得应用加固、漏洞扫描和盗版监控三大安全保障。此外，通过简单配置后腾讯云即可为您提供安全 SDK、真机测试、质量跟踪等其他安全相关服务。

腾讯云在遵循最新的 OWASP MOBILE TOP 10 的漏洞评估基础上，采用自有漏洞扫描引擎技术并结合多年移动安全攻防经验，为您的移动业务和应用 APP 提供数据层、网络层、应用层、第三方库等多维度漏洞审计能力；同时，能够通过自动化方式为您的应用 APP 提供防逆向、防反编译、防调试器等安全加固。而且，乐固提供了海量真机帮助您发现应用 APP 的机型适配问题，解决 android 机型适配难题；此外，不同的开发者也可根据研发需求和应用环境自行选择集成乐固提供的安全 SDK，从而为自己的应用提供额外的数据库、键盘、外挂对抗等底层保护。此外

当您的应用 APP 成功上线后，利用控制台即能实时了解应用 APP 在各大软件市场中的下载情况、分发情况，并能直观获悉自己的应用 APP 是否存在盗版或篡改；同时，若您的应用 APP 在发布前选择集成提供的质量跟踪模块，便能实时掌握包括 Android Native 上报信息的各类 crash 数据，降低应用 APP 的运维成本，提升应用 APP 的运营质量。




**图表 20 腾讯云乐固功能示意图**

### 6.2.2 智能硬件安全

越来越多的智能硬件制造商在受益移动互联网带来的商业机遇的同时，也意识到隐私安全、产品安全、业务安全等已经成为用户关心的热点。由于智能硬件制造商普遍缺少强大的安全团队支持，从设计、研发到产品发布等多个环节都存在众多的安全隐患。腾讯云在为此类客户提供智能硬件专属服务器等基础设施外，通过多年的研发经验和创新能力，还为客户提供智能硬件安全设计和安全访问协议的支持，并可帮助客户进行 API 接口和 APP 应用安全加固，从而实现智能硬件产品到后端业务服务的全面安全保障。

更多信息请参阅：https://www.qcloud.com/solution/smart.html

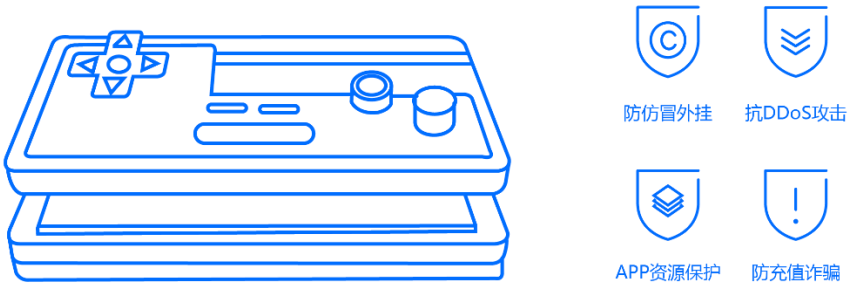
## 6.3 业务安全解决方案

在前面的介绍中，腾讯云为客户的互联网业务运营提供网络层面、主机与系统层面、业务层面和移动端的全体系安全产品和服务。针对不同客户的不同业务场景，腾讯云设计了多种可扩展的云安全解决方案，在腾讯云的专家服务支持下，客户能够获得定制化的安全防护机制，并能更加了解自身业务的风险特性[注1]。

### 6.3.1 游戏业务安全解决方案

腾讯云为游戏行业用户量身定制了多种游戏业务解决方案，当游戏开发者在享受腾讯云所带来的急速稳定的计算、存储和连接能力的同时，更能获得游戏运营过程中的全面安全保障。腾讯云提出的“云. 管. 端”立体游戏安全方案，包含手游 APP 安全服务、游戏网络保护服务和游戏内容保护服务三大解决方案，通过腾讯云安全产品如反外挂服务、反欺诈服务、云主机安全、消息过滤、DDoS 攻击防御服务、BGP 高防服务、APP 加固服务等，实现游戏业务层面的安全防护。

注1：由于篇幅限制，本文中仅介绍游戏、直播、金融和电商解决方案。腾讯云还为医疗、电商、广告等行业提供解决方案，具体请参见腾讯云官网或咨询销售人员。

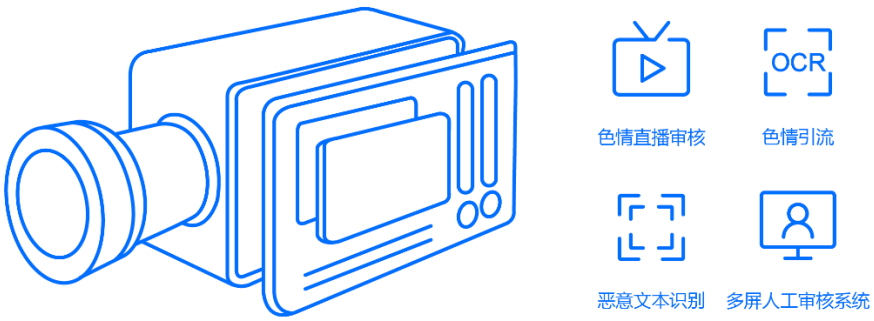



图表 21 腾讯云游戏业务安全解决方案示意图

### 6.3.2 直播业务安全解决方案

腾讯云直播业务安全解决方案，主要为直播行业客户解决直播内容人工漏审、色情引流、恶意评论和内容识别四大安全问题。您可以根据自身业务安全需求进行定制化，也可以选用腾讯云推荐的标准服务快速搭建自己的安全解决方案。其中在游戏直播、美女主播、在线教育等多种业务场景下，基于天御 BSP 业务安全的色情直播审核服务能够让您根据时间段、房间等属性设定不同的鉴黄参数，对直播视频进行实时截图审核和内容回调，第一时间对存在问题的直播房间进行告警或封停处理。

此外，直播过程中观看者与主播们会产生大量的字符类交互信息（包括聊天、弹幕、评论、发帖等）。腾讯云将垃圾消息过滤、内容合规审计等业务安全功能集成在直播业务安全解决方案里，其反干扰引擎能够帮助直播服务提供商实时监控和识别具有符号、图标、拼音、外文等干扰内容，结合业界最全的脏词库扫描技术和多模型匹配技术，全面过滤恶意广告、垃圾消息和非法言论，净化直播业务运营环境。




**图表 22 腾讯云直播业务安全解决方案示意图**

### 6.3.3 金融业务安全解决方案

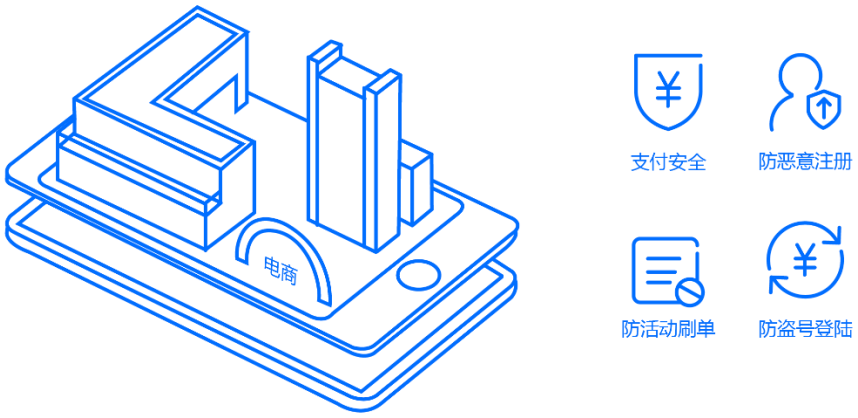
腾讯云非常重视金融行业客户对云计算环境的安全要求，目前腾讯云针对不同的金融机构要求，提供三大金融云模式：公有云、金融专区和金融专有云（更多信息可参考腾讯云官网的金融解决方案）。每一种金融云模式都符合金融监管机构的安全合规要求，无论是异地备份、两地三中心等业务连续性措施，还是主机/网络安全管控，以及数据传输加密和存储安全等方面，腾讯云所提供的金融云都能为各类金融行业客户提供适合的安全解决方案。

同时面对金融行业急速发展的互联网业务，腾讯云结合对金融市场安全需求的理解和自身业务安全能力，为金融行业客户定制提供包括支付安全、账户安全、信贷风控和反欺诈等多种金融业务安全功能。


图表 23 腾讯云金融业务安全解决方案示意图

### 6.3.4 电商业务安全解决方案

腾讯云电商安全解决方案旨在为每一个电商客户提供从用户注册到支付购买整个业务运营周期的安全保障，着重解决了电商行业面临的恶意注册，盗号登录，活动刷单和欺诈支付等风险。同时，针对成熟型、初创型和敏捷型等不同架构的电商网络，腾讯云在帮助客户确保业务稳定性和从容应对高并发访问的同时，提供完整的 DDoS 和 CC 攻击防护、DNS 域名防劫持保护、多等级容灾备份、混合云安全接入、移动应用评估加固等安全能力，全力为每个电商客户的业务发展保驾护航。




**图表 24 腾讯云电商行业安全解决方案示意图**

# 七、腾讯云安全生态

## 7.1 您可靠与安全的合作伙伴

腾讯云作为国内领先的云计算服务提供商，正经历云计算平台全面开放后的快速成长。经过多年实践累积，腾讯云聚集了大量专属的信息安全资源，从人才储备、产品创新、技术提炼，再到用户体验，以自身的实力证明，腾讯云是您最可靠、安全的合作伙伴。

### 7.1.1 精英团队

腾讯云的经营与管理理念是以人为本，以用户为核心。腾讯云不断将相应领域的精英团队进行整合，并通过持续的技术创新及激励模式吸引与维持了大量国内与海外的专业人士，共同为您的业务与数据保驾护航。

- **安全研究团队**


图表 25 腾讯联合实验室展示图

腾讯在创立伊始即着手互联网安全领域的部署，2016 年 7 月正式发布了中国互联网首个安全联合实验室矩阵，集合云鼎实验室、科恩实验室、玄武实验室、湛泸实验室、反病毒实验室、反诈骗实验室和

移动安全实验室七大专业实验室[注1]，致力于全面的互联网安全技术与攻防体系的研究及应用。通过不断地吸引、招募来自高校和社会的优秀群体，七大实验室矩阵汇聚了国内安全领域顶尖的“白帽”安全专家和研究人员，成为腾讯云安全强大的助推器。

其中，云鼎实验室作为腾讯云的信息安全体系建设核心团队，专注于云主机与云内流量的安全研究与运营，以及云端 app 安全方案和虚拟化安全技术研究。在云主机安全层面，云鼎实验室重点关注云主机自身发起的攻击行为，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；在云内流量安全层面，云鼎实验室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，帮助客户抵御高可持续攻击（Advanced Persistent Threat）；此外，云鼎实验室联合其他实验室进行全面的云计算安全漏洞挖掘和漏洞分享，覆盖虚拟化控制层，系统层和应用层的漏洞信息，云鼎实验室将漏洞防护能力以虚拟补丁方式整合入腾讯云的 web 应用防火墙系统中，可确保云计算平台整体的安全性。

同时，基于腾讯公司开放共建的主旨，腾讯的安全前锋团队也在不断发挥着社会价值。2016 年上半年，腾讯安全团队已经为苹果、谷歌、微软、Adobe 提交过上百个漏洞，其中 BadTunnel（由玄武实验室提交）被称为影响 Windows 系统最广泛的安全漏洞。今年 9 月，科恩实验室正式宣布，以全球首次“远程无物理接触”的方式成功获取特斯拉汽车行车系统的车电网络核心权限，将该漏洞所有细节提交给特斯拉官方并获得高度认可。此外，在 2016 年世界黑客大赛 Mobile Pwn2Own 中，代表腾讯安全团队出战的科恩实验室更是表现惊艳，仅用时 8 秒便攻破发布不久的 Apple iOS 10.1 移动操作系统，10 秒攻破 Google 的 Nexus 6p 手机系统。值得一提的是，这两次破解均是相应目标在全球范围内首次被攻破。最终腾讯安全科恩实验室凭借总积分第一，获得该项赛事“Master of Pwn”（破解大师）称号。这也是继 2016 年腾讯安全 Sniper 战队在黑客“世界杯”Pwn2Own 获得破解大师的称号之后，华

注1：腾讯安全联合实验室官网：http://slab.qq.com/

人再度夺此桂冠。腾讯云相信，通过不懈的挖掘与价值的输出，定能助力提升全社会的互联网及云计算安全意识。

- **安全运维团队**

基于用户为核心的运营理念，腾讯云建立了一套完整的服务体系，包含补偿政策，7*24 小时专业的服务支持，以及快速的响应机制，由云技术与安全的专家团队形成您可靠的后台保障，随时响应您的问题，并在第一时间运用专业技术进行解决。

作为一个高效的运作团队，腾讯云通过严格的技术及业务考核模式，有效维持服务团队的优质与专业。腾讯云着力不断优化自身的服务运维体系，将自动化运维流程引入其中，提高整个运维管理的流程速率，最高程度地缩短响应周期，让您感受到更为快捷的服务。

除此以外，腾讯云也持续与业界基础运维领域的专业第三方协作，如基础故障的排除与标准化生产环境中的漏洞防护部署等，以更加高效与专业的角度为您提供相应的服务与运维。

- **安全合规团队**

以技术团队为核心，运维团队为基础的同时，腾讯云建立了独立的安全合规团队，由拥有多年云计算安全实践经验的专业人员组成。作为腾讯云安全体系的规划者与监督者，腾讯云安全合规团队整合了行业安全标准及相关法规要求，针对腾讯云提供的服务、产品与内部环境，建立了体系内部的安全合规架构，并定期执行安全审计与监察，助力云生态安全、持续、有效地运行。

腾讯云安全合规团队持续关注行业安全技术及标准的更新动态与发展方向，进一步深度参与云产品开发与安全技术管理等优化过程，以严谨、务实的态度巩固腾讯云的安全架构。

- **腾讯云团队的荣耀**

腾讯云的安全研究、运营服务、安全合规团队相互协作，形成了一个互助共生的整体，经过数年的开发与实战，不断创造着一个个腾讯云荣耀的时刻。

2014 年举办的全球云计算大会中国站的评奖环节中，经由独立第三方研究机构、产业联盟、行业组织、专业媒体、国际组织、主办单位等多方人士组成的评审委员会评审，腾讯云凭借技术实力，荣获“2013-2014 年度中国领先品牌奖”，腾讯获“2013-2014 年度全球最佳实践奖”，再一次得到了国际上的肯定。

2015 年由工信部指导的第二届 2015 可信云服务大会上，腾讯云脱颖而出，一举获得可信云 2014-2015 年度“虚拟网络技术创新奖”及 “视频云服务奖”两项大奖，印证了腾讯云整个团队持续的开拓以及不懈的努力。


**图表 26 腾讯云荣誉信息示意图**

未来，腾讯云也将一直致力于更新这份荣誉的记录，为您持续提供安全、可靠的前沿技术与专业服务。

### 7.1.2 多元产品

腾讯云拥有近 30 款云产品，包含云服务器、云数据库、云缓存 Memcached、负载均衡、弹性 web 服务、云安全等多维度、丰富的产品类别与模式，可供您根据自身的行业特性与需求进行组合，形

成行业解决方案，助力您轻松跨入“互联网+”时代。如下，是腾讯云可以为您提供的多元化的产品线，横向覆盖多个领域，纵向拓展产品线的不同功能：


**图表 27 腾讯云产品分布示意图**

### 7.1.3 前沿技术

基于多元化的产品，腾讯云在过去十多年的开发过程与互联网业务运营中，不断积累抗拒绝服务攻击、入侵保护，业务安全等一系列的安全能力与技术。并且，通过多年为数家国内大型互联网企业提供抵御恶意攻击的解决方案，腾讯云在成功协助企业预防相应风险与避免财务损失的同时，也收获了丰富的安全防御实战经验与案例。

我们将基于数年累积的先进技术与实践经验，为您提供最大程度的保障：

- 腾讯云的优势在于，拥有经过大量对抗网络黑产实践所积累的黑产数据库，从起初的简单盗号、挂机，到现今更加多维的方式如微信垃圾消息、社工诈骗、DDoS 攻击、红包诈骗等，依托腾讯生态渠道，腾讯云汇聚与总结了大量安全防护信息，并将之进行有效分析与关联，形成腾讯云业

务防御前线的庞大支撑。同时，通过对黑产数据库多维度的分析，腾讯公司与腾讯云持续与相关政府部门合作，防护网民的数据与财产安全，进一步促进整个网络的健康、和谐发展。

- 优图人脸识别是有腾讯优图团队研发的，基于人的脸部特征信息进行身份识别的一种生物识别技术，实现了在主流 PC 端和移动端的快速检测，支持强光、弱光、黑夜等复杂环境下正脸、侧脸多角度的人脸检测，以及海量的人脸信息标注。本着共享的运营模式，我们也积极将先进的人脸识别技术用于协助政府进行视频与图片鉴黄等工作。
- 腾讯云的分布式防护拥有国内最大的 4Tb 防护带宽，能够有效抵御各类 DDoS 攻击及 CC 攻击。并且，腾讯云在全国布局了 100+节点，涵盖移动、联通、电信等主流运营商以及铁通、长宽等十几家中小型运营商，解决了服务的兼容性问题的同时，通过高效动态调度网络流量，有效组织起腾讯云全网各点冗余带宽和防护能力，最大程度地保障您的服务高用性。
- 此外，基于覆盖率广泛的分布式节点，腾讯云可以提供目前业界最高频率的 DNS 劫持检测，更加高效地监测您的云服务安全。

### 7.1.4 海量用户

依托腾讯公司在国内互联网产业丰富的资源，以及腾讯云自身多元化的产品，我们也积累了自己的海量用户，覆盖社交、游戏、视频、金融、电商等领域。通过与不同领域用户的服务交互过程，腾讯云累积了不同类型的、海量的安全实践经验，包含各类风险事件的应对方法，有效固化了腾讯云自身的安全体系与产品安全功能，进一步形成整个腾讯云安全运维的扎实基础。

## 7.2 率先打造开放的云安全生态

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。

### 7.2.1 开放共建为核心

如同“云+未来”峰会中首席执行官马化腾的阐述，以腾讯云的视角解读，云是一种分享的经济形态，将整个社会中的不同功能与服务能力分享到各个阶层，形成跨界的联合。所以，我们以大数据为基础，将整个平台的计算、网络、存储、安全等资源毫无保留地分享给各个领域的合作伙伴，构建完整的产品服务体系。作为腾讯生态圈中开放的能力：多年累积的人才资源、安全联合实验的研究成果、多维度的安全产品（如手机/桌面安全管家、麒麟云等）、微信/QQ/腾讯云等积累的海量用户等，腾讯云将多平台宏观整合的数据，以不同安全技术手段协助您更加便捷、低成本的享用这些能力与服务。

放眼整个公司，腾讯云的生态建立在开放的环境上，我们始终以自身产品及服务安全为核心，由整个腾讯安全体系为支持，与合作伙伴共建一个安全的生态，为不同类型的客户实现不同形式的“云+”服务，构成宏观云生态上的互联共生。

### 7.2.2 深度合作为延续

腾讯云眼中合作共建的生态环境是分阶段发展的，通过参与制定行业标准，与业界领先的厂商进行合作，横向拓展腾讯云在各方面的安全能力，让客户在面对泛滥的互联网资源时能够极大地减少思考时间与筛选成本，并为您提供经过严格筛选的、精准定制的云计算安全服务。

腾讯云着重与认可的专业厂商进行深度的安全功能集成与服务整合，不追求数量上的极致，而着眼精准的定位，垂直深耕腾讯云的安全防护体系，完善与强化云端与客户端的安全功能，为您提供以腾讯云为核心的整合服务。

此外，腾讯云以云服务市场的形式提供安全合作伙伴的产品和服务。该服务市场中已上架了丰富的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安全产品如：VPN、加密机、入侵检测、数据防泄密、UTM、堡垒机、日志审计、数据库安全审计等。

开放共建、深度合作是腾讯生态战略的实施态度，我们将打造可持续的云安全生态，为您提供全产业链的安全解决方案。

# 八、行业云认证和安全合规

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。


**图表 28 腾讯云认证与合规路径示意图**

- 2014 年 10 月 30 日，腾讯云成为国内首家获得 ISO/IEC 27001: 2013 信息安全管理体系认证的云服务提供商。
- 2015 年，腾讯云获得数据库服务、云主机服务和云缓存的可信云认证。
- 2015 年，腾讯云计算基础网络系统，腾讯云数据库系统，腾讯云主机服务系统通过信息安全等级保护三级测评。
- 2016 年 2 月 14 日，腾讯云获得 GB/T 24405.1-2009（等同 ISO/IEC 20000-1: 2005）IT 服务管理体系认证，包括云计算服务、托管服务及灾备服务等。
- 2016 年 3 月 2 日，腾讯云成为国内首家在云计算领域获得 ISO/IEC 9001: 2008 质量管理体系 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）双认可的企业。
- 2016 年 3 月 31 日，腾讯云成为国内首批通过 ISO/IEC 22301: 2012 业务连续性管理体系认证的云服务商。
- 2016 年 4 月 25 日，腾讯云成为通过数据中心联盟主导的大数据产品能力认证的首批企业里唯一的大型互联网企业。
- 2016 年 9 月 30 日，腾讯云成为首家获得 CNAS 以及国外 UKAS 双认可的 ISO/IEC 27001: 2013 认证证书，并以金牌评估等级通过云安全联盟 CSA 认可的云安全管理体系 STAR 认证。

## 8.1 行业云认证体系

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。

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。

ISO/IEC 22301:2012 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 27001:2013 认证

ISO/IEC 27001: 2013 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 27001:2013 认证的云服务提供商，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 20000-1:2005 认证

ISO/IEC 20000-1: 2005 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: 2005 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: 2008 认证

ISO/IEC 9001: 2008 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: 2008 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）双认可的企业，认证范围涵盖云计算服务、托管服务及灾备服务等。


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《信息安全等级保护管理办法》（公通字[2007]43 号）的有关规定，腾讯云计算基础网络系统，腾讯云数据库系统，腾讯云主机服务系统已通过信息安全等级保护三级测评，严格遵循国家在信息

系统安全建设方面的技术保障和安全管理要求，建立了自身的长效机制，进一步保证安全保护工作的持续进行。

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。

## 8.2 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 29 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。

## 8.3 行业标准制定

获取外部行业认证，建立内部安全合规体系，腾讯云还持续参与行业安全标准的制定及推广，从而进一步开放核心安全技术，与不同的行业专家和国家标准机构合作，共同完善云计算和大数据相关的安全标准体系。

此前，由工信部指导主办的 2014 年可信云服务大会上，腾讯云宣布联合工信部电信研究院旗下的数据中心联盟共同发布了“服务商可信认证”体系，旨在促进建立一套完善的云服务市场可信任体系与标准，加强云计算产业在国内健康、持续的发展。

2016 年，腾讯云正在与云安全联盟 CSA 合作，通过自身多年的行业累积，协助云安全技术层面测评标准的制定。同时，腾讯云正在参与国家信息安全标准化委员会的标准研讨和制定（如大数据安全能力评估标准等），促进行业安全应用及规范的普及。

# 九、共建创未来，安全在云端

关于腾讯云甚至整个云生态的未来，我们将在现有安全技术巩固与强化的基础上，加快业务安全建设，扩大黑产对抗优势，以高素质的安全能力与持续的开放理念为核心，共建安全的云端未来。

## 9.1 关注安全技术，巩固防御机制

对于云计算的未来，腾讯云持续着力虚拟化安全、安全产品云端化、云主机安全与云内流量安全等方面的技术研发：

- 腾讯云持续关注云自身的虚拟化安全问题。由于虚拟化架构的特殊性，当网络边界被模糊化时，一旦关键漏洞被恶意利用，极有可能会将风险贯穿至整个云计算系统导致出现重大的安全影响。腾讯云一直致力于虚拟化中漏洞挖掘和风险处置，结合腾讯安全联合实验室在虚拟化安全领域的研究，为客户提供更加完善的解决方案。
- 面向用户的安全也是腾讯云一直以来的工作重心，腾讯云致力于安全产品云端化，比如将漏洞检测系统、入侵防御系统、堡垒机等安全产品整合入云计算平台中，使您更加直观和便捷地获得云化的安全保护机制。
- 云主机安全与云上流量攻击防御是云鼎实验室重点开展的安全研究领域。腾讯云将结合海内外优秀的防御实践，利用自身丰富的安全产品与服务，建立立体化的安全防御体系，实现云主机前端到后端全方位的安全连动。在用户使用伊始，腾讯云即刻利用自身庞大的黑产数据分析能力感知异常情况，实现自动化威胁联防联控，将您的业务风险降至最低；同时，以基于云主机层面的安全监控、追溯查询和策略管理，关联腾讯云的反馈机制与升级修复服务，从而实现多方位的风险自主检查与实时预警。
- 此外，DDoS 攻击防护依然是腾讯云安全研究的重点之一。为了解决传统防御事中或事后处理方式带来的延迟和成本问题，腾讯云将通过研发更加有效的立体连动机制，在攻击发起初期即实现

异常流量与风险可能的有效识别，在向您预警的同时给出更加合理的处置建议，最大程度上减少防御成本投入，有效保障您的业务安全和稳定的运行。

## 9.2 持续对抗黑产，夯实业务安全

为了保障您在云端的业务安全，腾讯云将进一步优化业务安全防护能力，全面覆盖活动防刷、注册保护、登录保护、反欺诈、消息过滤、图片鉴黄、验证码等方面。通过整合业务安全防护中不断积累的黑产对抗经验，将单一的安全数据单元关联形成立体的安全数据矩阵，持续完善腾讯云已有的黑产数据库，进一步扩大我们在黑产对抗中的行业优势。

基于大数据分析的结果，形成用户可视化的安全分析平台，腾讯云能够让客户的管理层更加直观地了解企业自身在云平台上的运维问题、安全风险及潜在的业务机会。腾讯云不仅关注暴露的问题与风险本身，更能站在您的角度，协助企业规划未来业务发展方向。

## 9.3 提升安全素质，共建云端生态

安全是腾讯云的核心，我们始终以高素质安全为目标，开放自身乃至整个腾讯公司的安全技术与服务，全面整合安全人才资源、黑产数据、技术研发等关键资源，持续提升云计算、云存储、云网络等安全管理与技术能力，不断开放更多的云端业务安全解决方案。

如同在 2016 年“云+未来”峰会上表达的宗旨，腾讯云将秉承开放的理念，与更多全球化行业合作伙伴共建云安全生态，为您提供整合的一站式解决方案，输出更多互联网+的行业云能力。

我们期许在不久的未来，通过精品聚焦安全服务与垂直深耕安全能力，打造出国内第一大云生态圈，连接上百万的优质企业和创业者，全方位地服务于中国“互联网+”战略，实现社会智慧化转型。

腾讯云，安全，值得信赖。

# 附录

## 附录 I：腾讯云隐私声明（2016）

腾讯云非常重视客户的隐私。您在使用我们的服务时，我们可能会收集和使用您的相关信息。我们希望通过本隐私声明向您说明，在使用腾讯云服务时，我们如何收集、使用、储存您的相关信息，以及我们为您提供的访问、更新、控制和保护这些信息的方式。该隐私声明与您所使用的腾讯云服务息息相关，希望您仔细阅读。

- 适用范围

本隐私声明适用于腾讯云账户信息。在注册、管理腾讯云账户，或进行实名认证的过程中，您需要提交真实、合法、有效的信息，包括但不限于名称、联系人、电子邮箱、QQ 号码、联系电话、联系地址、银行账户信息、工商登记信息等。

本隐私声明不适用于客户存储在腾讯云系统中的内容，即客户内容，包括客户的终端用户的个人信息。除服务协议规定的情形外，腾讯云不会披露、移动、获取或使用您的内容。您可通过腾讯云服务协议了解更多关于您存储在腾讯云系统中的内容的相关政策。

- 腾讯云如何使用账户信息

腾讯云是腾讯公司的关联公司，腾讯云在收集和使用账户信息方面的实践也遵守腾讯《隐私政策》。请注意，如果您拥有腾讯其他账号，在特定场景下，您的腾讯云账号的个人识别信息可能会与您在腾讯拥有的其他账户信息相关联，比如您使用 QQ 号码注册腾讯云账号。

您使用或继续使用我们的服务，即意味着同意我们按照腾讯《隐私政策》和本隐私声明收集、使用、储存和分享您的相关信息。

如对本隐私声明或相关事宜有任何问题，请通过 http://kf.qq.com/与我们联系。

腾讯云