腾讯云安全白皮书

构建安全的云生态

腾讯云安全团队&腾讯研究院安全研究中心

2015.10

目录

图目录

表目录

第一章腾讯云安全生态概览

1.1 搭建开放的腾讯云生态

互联网从最初连接“人与信息”升级到连接“人与人”，其功能已发生重大变化。在“人与信息”连接的时代，用户使用互联网或者是进行搜索，或者是浏览信息。然而，互联网演进到连接“人与人”的时代，伴随 QQ、微信等社交软件的兴起，社交网络成为互联网发展中非常重要的组成部分。

腾讯认为未来的互联网会成为连接一切的工具。互联网将渗透到各行各业，会向着连接所有服务，甚至连接到所有硬件的方向不断演进。

随着互联网连接一切的发展，我们看到，在交通、金融、医疗、教育、旅游等领域，“人与人”的连接已经给相关产业带来了新的变化和诸多发展机会。越来越多的创业者，带着互联网思维进入到上述行业，希望改变现有行业的部分规则并为这些行业带来创新的活力。

腾讯看到各行各业中的领导企业，正在积极思考互联网+给产业带来的变革和为企业带来的创新机会。如何利用互联网+，优化行业的服务，为行业带来欣欣向荣的变革，进而提升整个行业的运转效率，是各行业需要思考的。通过对行业的变革和对服务的创新，真正让每一个老百姓，每一个普通大众可以享受到“互联网+”带来的新的能力和新的机遇。

作为互联网行业的领跑者，腾讯通过全面开放其基础服务，以云的方式给产业界和企业带来资源、服务和硬件三方面的连接能力。这些能力包括：计算、存储、网络、CDN、音视频的通讯能力、人脸识别能力、以及安全的防护能力。腾讯还为相关行业提供云应用的解决方案，比如游戏领域、移动应用领域、金融行业、音视频领域、政企行业，还包括智能硬件领域。

腾讯认为实现云服务的价值，搭建完整开放的生态圈非常重要。腾讯云通过技术耦合更多的互联网开发者，将能够打造一个涉及用户引入、商业模式、营销渠道乃至更多的有利因素于一体的完整开放的生态圈。腾讯云正在打造中国第一大云生态圈，全方位地服务于中国“互联网+”战略，将连接上百万的企业和创业者，推动全社会的升级转型。

1.2 安全是腾讯云的基因

安全是腾讯云的基因，是腾讯云实现服务价值的根本保障。安全性、稳定性、海量服务、大数据能力、贴心服务等是企业拥抱云计算最为关心的几大因素，其中又以安全性最为关键。

腾讯云非常关注客户对安全性的保障要求，这也是腾讯云技术与运营团队花费最大精力的地方。腾讯云依靠安全总体策略、云计算行业安全认证与合规、安全架构与安全服务、安全审计与管理四项措施，形成了完整的安全保障生态体系。

图 1 腾讯云安全保障生态体系

在安全策略上，腾讯云将保护客户业务/数据的机密性、完整性和可用性作为整个腾讯云的公司战略，提出云安全架构，依此架构制定防范安全威胁、消除安全风险的安全控制程序和技术手段，并通过管理流程保证控制措施和技术手段的执行。

在安全认证和合规上，除了不断地从技术层面提升安全防护能力，腾讯云还在持续推动企业内部信息安全管理规范化流程和操作。2014 年 10 月 30 日，在腾讯的“大云端 大生态”峰会上，面对腾讯全球合作伙伴，英国标准协会（BSI）为腾讯云颁发了 ISO 27001:2013 认证证书，这宣告腾讯云成为国内首家获得 ISO 27001:2013 认证的云计算服务企业，同时也意味着腾讯云的信息安全管理达到国际领先水平。

在安全平台和服务上，腾讯各项业务所承担的安全风险之高当属业内之最，却鲜有重大安全事件发生，足以证明腾讯的安全防护能力已达到行业领先的高水准。腾讯云安全可以提供包括 DDoS 防护、漏洞扫描、网站安全防护（WAF）、后门木马检测、DNS 劫持检测、暴力破解告警、异地登陆提醒等服务。腾讯云具备定期检测与实时告警的能力，并向所有客户开放。

在安全审计和管理方面，腾讯云建立了完善的安全审计和管理流程。在安全审计上覆盖了运维行为审计、内容合规审计、安全规范审计三个方面。在安全管理方面，针对人员管理、开发流程等部分建立了完善的管理制度和流程规范。

1.3 保障腾讯云安全的策略解析

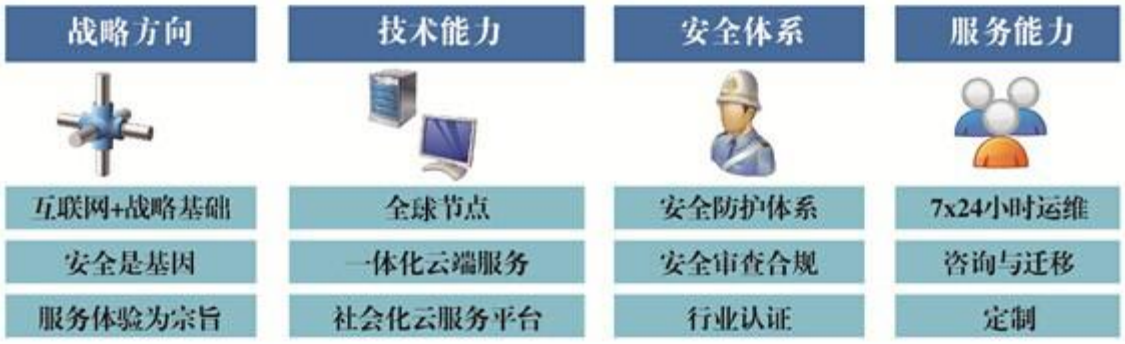
腾讯云安全发展的战略方向：腾讯云是腾讯公司布局互联网+的战略基础，作为国内提供公有云服务的主要供应商，腾讯云始终坚信“安全是云业务开展的基石”，以提供按需定制、安全可靠、全面丰富的服务体验为宗旨，助力客户实现业务创新和业绩增长。

支撑腾讯云安全的技术能力：腾讯云定位于打造迅速响应、高效沟通、专业严谨、开放共享的社会化云服务平台。腾讯云依托腾讯海量业务技术研发沉淀，不断创新云计算底层架构，积累了丰富的精细化互联网运营经验。目前腾讯云正在实现全球节点布局，为全球企业和开发者提供从数据到应用再到运维的一体化云端服务体验。

腾讯云安全建立的保障体系：安全被视为腾讯公司的命脉，基于腾讯安全强大的技术支撑，腾讯云建立了可信、可控、可溯的安全防护体系，实现了流程化、自动化、数字化的云计算服务安全管理手段，保障云平台和基础环境的安全、可用，支撑云服务安全合规和可持续性经营。

腾讯云安全的服务输出能力：腾讯云提供全天候的安全运维响应，保障客户业务/数据的机密性、完整性和可用性，以及客户数据和业务的便捷互迁。同时，腾讯云针对客户的特殊安全要求，通过智能化的分析系统实现广泛和专业的云安全定制化服务。

图 2 腾讯云安全策略



1.4 腾讯云安全生态的实现和不断完善

腾讯云安全生态的实现，得益于腾讯云在安全领域积累了丰富的经验，并拥有深厚的互联网安全基因。用户基数庞大的产品 QQ 和微信自诞生伊始，就和“安全”两个字联系在一起，这两块业务每天都在极大地帮助和促进腾讯积累云安全方面的经验。

腾讯云客户对安全标准的提升要求，让腾讯云安全生态变得日趋完善。腾讯的移动互联网开发者，特别是手游行业中的企业，对游戏从开发到运营的安全要求极高，腾讯云安全为他们提供了强大的安全保障服务，例如：对于手游 APP 的 APK 安装包进行加固，以保证游戏客户或者其他的应用客户不被别人剽窃，或者不被别人篡改，从而保障了用户的数据和资产安全。另外，腾讯云搭建的“大禹”DDoS 分布式防护系统，更是可以为开发者提供 T 级的 DDoS 防护能力。

腾讯云安全不但注重自身的安全，还努力推动国内云计算安全管理规范的制定，全面打造行业的安全生态体系。腾讯云通过和工信部的合作推动了“服务商可信认证”体系的建设。“服务商可信认证”体系已经在云服务领域得到了广泛认可，极大地推动了云计算在中国持续、健康、长远的发展。

1.5 腾讯云安全的核心理念

“可信、可靠、保障、贴心”，是腾讯云提供服务的核心理念，覆盖从物理环境、访问控制、配置管理、应急响应、安全审计、持续监控、供应链等多个环节的安全控制要求，提供多维度安全防护。

1.6 腾讯云安全的综合能力

腾讯云安全具备全面的综合能力。在腾讯云安全的总体战略的引领下，腾讯云安全从认证合规、云平台架构、云安全产品和服务、云安全内部审计流程、可信云物理和环境安全性、内部人员管理、供应商管理等七个能力方面实现了腾讯云安全对于客户的承诺。

腾讯云安全遵循认证/合规先行的原则，奠定了云计算行业可信云安全的保障基础。

腾讯云安全建立了“两层三面”的体系化架构，实现了多地调度、分权运维、高性能、高可用、高防御的能力。

腾讯云安全能够为客户提供多维度的网络攻击防护、入侵保护、业务安全能力开放、腾讯云安全认证等产品和服务。

腾讯云安全在云服务生命周期的每个阶段均实施了内部安全审计流程，从需求设计、到系统上线、再到系统运营的每一个环节均符合“安全是基石”的要求，以确保腾讯云的安全风险可控。

腾讯云安全对云机房的物理和环境安全建立了专门的管理体系，通过对物理环境进行安全区域划分、制定规范文档、监督实施执行及优化改进多个部分，实现了全体系的物理和环境安全的管控能力。

腾讯云建立起了严格的内部团队管理体系。腾讯在雇佣前、雇佣中、雇佣后都采取了一系列的措施来避免员工有意或无意的出现不当行为，并具有在出现问题后能及时发现和处理的能力。

腾讯云要求每个供应商都必须有风险管理信息系统、可维持其服务质量持续运行的规章制度以及演练记录，并且要求定期反馈演练记录或者规章规范实施证明，同时会与各个供应商核查 SLA 达标情况。腾讯云具备让每个供应商都必须第一时间通知其产品、服务存在的缺陷、漏洞等风险/影响以及对应解决措施的能力。

第二章可信的行业云认证和安全合规

云计算行业安全认证和行业合规是任何一家云服务提供商正式运营的必备条件，是提供云服务的资质保障。

腾讯云是国内首家获得 ISO27001:2013 认证的云服务提供商。同时还通过了工信部的可信云认证，其中，可信云认证的核心目标是建立云服务提供商的评估体系，为客户选择安全、可信的云服务提供商提供支持。

腾讯云还获得了公安部颁发的安全等保三级认证。这表明，腾讯云在计算技术网络系统、云数据库系统以及云主机服务系统三套核心系统上，从技术实力、安全性能、信息及业务影响力这三个层面均达到了企业范围的最高认证。

在合规性层面，腾讯云按照国家有关信息安全法律、法规规定，充分满足国家安全政策法规；并搭建了健全的内部安全保障制度；同时遵守第三方合法权益，有力地保障了腾讯云自身及第三方的合法权益。

更重要的是，腾讯云不仅在认证、合规上先人一步，更在社会责任担当中成为中流砥柱。在打击网络犯罪、保护数据安全、维护网络间正常运营以及对内容安全审查等方面，腾讯云都积极的履行了应尽的社会职责。

腾讯云通过在社会责任担当中取得的口碑，逐步扩大企业影响力，积极履行在云安全领域制度建设中的责任。腾讯云希望建立一套完善的云服务市场可信体系，助力云计算产业在国内健康、持续的发展，加速云服务第三方市场的规范进程，有效提升云服务品质，促使腾讯云生态链朝着更为健康的方向发展。

2.1 行业认证

ISO27001 认证：腾讯云是国内首家获得 ISO27001:2013 认证，符合信息安全管理体系国际标准的云服务提供商。腾讯云的信息安全管理体系涵盖了云计算基础设施、数据中心和云服务，包括云服务器、负载均衡、云数据库、对象存储、云安全、云监控以及云拨测等的信息安全管理，这确保腾讯云从底层应用开始，保障用户的信息安全。

可信云认证： 2015 年，腾讯云通过工信部可信云服务的数据库服务、云主机服务和云缓存三大类，共 16 项严格测试认证，获得数据库服务、云主机服务和云缓存的可信云认证。腾讯云通过可信云认证，表明腾讯云主机、云缓存和数据库服务在数据存储的持久性、数据可销毁性、数据可迁移性、数据私密性、数据知情权、服务可审查性、服务功能、服务可用性、服务资源调配能力、故障恢复能力、网络接入性能、服务计量准确性等方面已经拥有了最佳实践。

信息安全等级保护三级认证：信息安全等级保护是由公安部监制，由属地公安机关认可并颁发的，针对系统信息安全性能的认证，认证等级分为五级，其中三级标准，是企业范围内最高级别认证（四级为涉密系统，五级为国安系统）。腾讯云计算技术网络系统、云数据库系统以及云主机服务系统，均取得由北京市公安局颁发的三级等保认证，意味着腾讯云这三套核心系统获得国家等保三级的认可，并在技术实力、安全性能、信息及业务影响力均达到三级标准。

表 1 定级要素与安全保护等级关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

图 3 腾讯云荣获的行业安全认证证书

2.2 安全合规性

腾讯云的合规体现在三个方面：满足政策法规要求，健全的内部安全保障制度，全力保障第三方权益。

符合国家安全政策法规：腾讯云安全符合国家网络安全政策法规的要求，在内部安全保障制度和保密措施方面，制定了严格而完善的流程与制度。腾讯云对于客户业务承载内容审计核查，审计中如发现色情、诈骗等恶意非法内容会进行隔离等处罚操作。

健全的内部安全保障制度：腾讯云按照国家有关信息安全法律、法规规定，建立健全内部安全保障制度，实行安全保障责任制，为保护数据、业务的安全严格设置并不断更新各类监控和保密措施，保障云服务系统的稳定和安全。

保障第三方合法权益：腾讯云依照国家有关知识产权保护的法律、法规规定，制定涵盖著作权、商标、专利等各类知识产权的管理规范及保护措施，保障腾讯云自身及第三方的合法权益。

2.3 内部安全审计

在云计算行业安全认证与所有的行业合规性要求下，腾讯云在运维行为、内容合规、安全规范方面制定了更为具体和严格的审计基线和实施制度。

- **运维行为审计**

腾讯云安全团队会对母机、支撑组件、数据库等运维操作进行全部截屏。审计系统每日会检测截屏日志中的敏感、越权操作，腾讯云安全团队对检测发现的异常运维行为进行追溯和闭环。

- **内容合规审计**

为确保腾讯云内容的健康性和合规性，腾讯云会在客户明示同意的基础上，对客户业务承载内容进行审计，对于审计发现的色情、诈骗等恶意非法内容会进行隔离等处罚操作。同时，对于未备案域名的 HTTP 请求会进行拦截操作。

- **安全规范审计**

腾讯云会定期对安全规范落实情况进行审查，对于不执行安全规范要求的团队负责人进行追责。另外，腾讯云要求业务团队定期对风险预案进行演习，由相关安全/质量责任人审计执行情况。安全团队会对审计过程中发现的问题进行问责，并推动问题闭环。

2.4 腾讯云社会责任

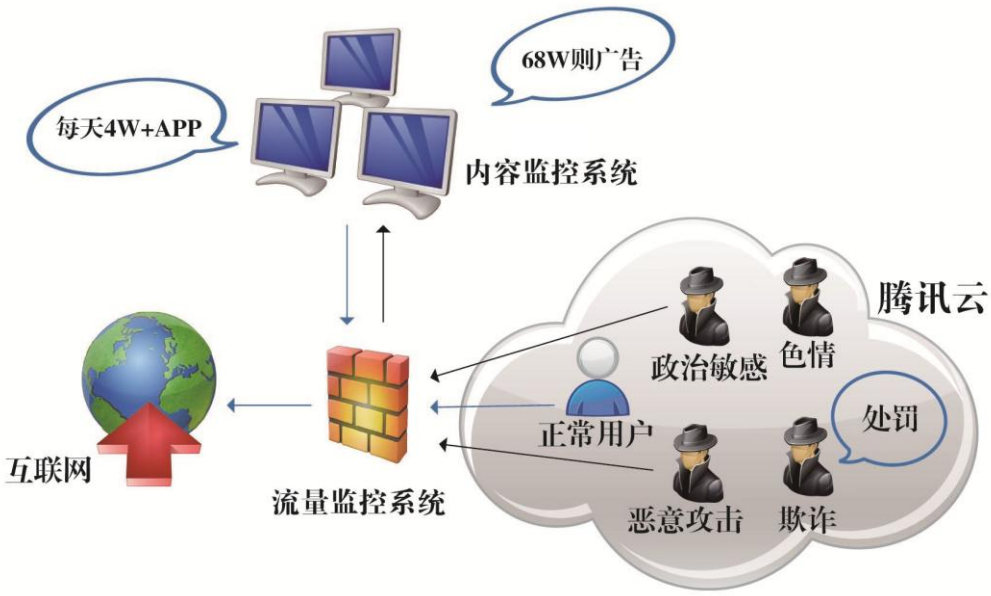
勇于担当社会责任，利用安全技术打击犯罪，维护网络安全，腾讯云表现出积极正面的社会形象。腾讯云安全团队与多地警方联手，严厉打击网络攻击、诈骗、色情等违法犯罪活动，并向社会公众提供了扫黑举报奖励。至今共收到超过 250 万条举报信息，并向 230 人颁发了举报奖励。腾讯云认为，保护用户的合法权益不受侵害，是一个互联网企业必须承担的社会责任。因此，对于一切网络犯罪活动，腾讯云安全的态度都是零容忍，将坚决配合警方严厉打击。

- **净化公共网络环境**

针对腾讯云平台上域名未备案状况可能带来的政策风险，腾讯云早在 2014 年就启动了现状梳理和域名封禁处理工作。凭借腾讯公司自研的流量监控系统，对平台上的 HTTP 请求进行分析上报，从中提取出域名列表信息；同时利用该系统的流量拦截功能，对向未备案域名的请求进行拦截，并返回备案处理提示信息。截止 2015 年 6 月底，共封禁了数百万个未备案域名。

为了响应国家互联网信息办公室“护苗 2015 网上行动”的号召，营造有利于青少年健康成长的网络环境，自 2015 年 5 月以来，腾讯雷霆行动对全平台涉及未成年人的色情信息进行了严厉打击，腾讯雷霆行动在全平台共清理和打击传播色情淫秽等有害信息帐号共计四万多个。腾讯云累计封停打击违规公众帐号 8 万多个，拦截各类恶意营销广告、恶意链接 500 多万个。在打击网络色情上，处置 LBS 服务 3000 多万次，删除淫秽色情及招嫖类信息 500 多万条。

图 4 腾讯云安全平台对恶意内容净化的原理



- **打击网络攻击**

2014 年腾讯云安全就在打击 DDoS 攻击团伙的事件中，表现出对于社会责任的高度重视

和安全技术支撑。当腾讯云监控到攻击流量突增，攻击行为变得活跃，多个省份不断出现网络拥塞、网站访问异常的情况后，腾讯云安全团队在较短的时间内，对实施恶意攻击的行为进行全面的打击，保护了公共网络环境的安全。

2015 年 7 月，江苏网警和腾讯安全团队正式成立“DDoS 刑事打击联盟”，双方就近年来 DDoS 领域网络犯罪的发展趋势，及后续打击标准、思路进行了深入的讨论，并一致达成共识。在后续的打击工作中，江苏网警将充分发挥在打击互联网犯罪过程中的丰富办案经验，而腾讯也将全力提供技术支持，坚决遏制 DDoS 网络犯罪愈演愈烈的恶性趋势。

腾讯云在帮助行业伙伴抵抗 DDoS 攻击方面，屡屡创下奇迹，如帮助某知名网站抵御 DDoS 攻击。

案例：某在线住宿服务提供商网站遭遇严重 DDoS 攻击，腾讯云大禹系统 14 分钟完成清洗

对于中国的许多互联网企业来说，刚刚过去的 2015 年 5 月，绝对是一个不折不扣的“黑色五月。2015 年 5 月 28 日上午，在许多人对前一天的支付宝大面积瘫痪事件还心有余悸的时候，某旅行服务商网站也曝出了瘫痪事故，其官方网站和 App 客户端均无法正常使用。

在经历了数小时的抢修但仍然无法恢复之后，这家旅行服务商在网站首页挂出了紧急修复通知，并建议用户访问另一家在线住宿服务提供商的网站。然而在当天下午 17 点之后，被推荐的在线住宿服务提供商的网站首页，也开始出现无法正常访问的情况，据称是遭到了大流量的 DDoS 攻击。

正当不少网民都以为，这家在线住宿服务提供商也将步上家旅行服务提供商的网站后尘陷入瘫痪的时候，令人意想不到的事情发生了：在大约 17 点 30 分，一直在关注此事进展的媒体报道，这家在线住宿服务提供商的网站首页已经恢复正常。为什么那么多的网站都宕机了，唯独这家在线住宿服务提供商的网站却能在网络攻击中快速回血？这究竟是怎样做到的呢？

原来，在发现网站首页无法访问的异常现象之后，这家知名在线住宿服务提供商网站紧急接入了腾讯云大禹系统。而正是后者起到了过滤和清洗攻击流量、将正常流量引入网站的关键作用，只用了极短的时间就帮助这家知名在线住宿服务提供商的网站满血复活，重新投入了运营。

这家知名在线住宿服务提供商从发现异常到全面接入腾讯云大禹系统，全程仅耗时 14 分钟。

通过一系列社会责任的公益担当，腾讯云在业内活跃度、影响力显著提升，积极参与各项活动，并在建立完善云安全可信任体系中，发挥自身影响力，得到了进一步升华。

腾讯云在努力打造规范的云生态的同时，也树立起在互联网领域云安全的标杆。一方面不断提升自身安全技术能力，另一方面引入国际权威信息安全管理规范。而腾讯云并不满足于此，

在由工信部指导主办的 2014 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“服务商可信认证”体系，旨在促进云安全制度的完善和有序发展。

腾讯云在第三方认证和合规性上取得成绩，为腾讯云搭建安全稳定的云架构平台，提供了最有力、最可信的信誉保证，这样不仅对于客户而言，找到了一把可以衡量云服务商的标尺，而且对于业内云服务的有序发展，也起到了积极引领和示范作用。

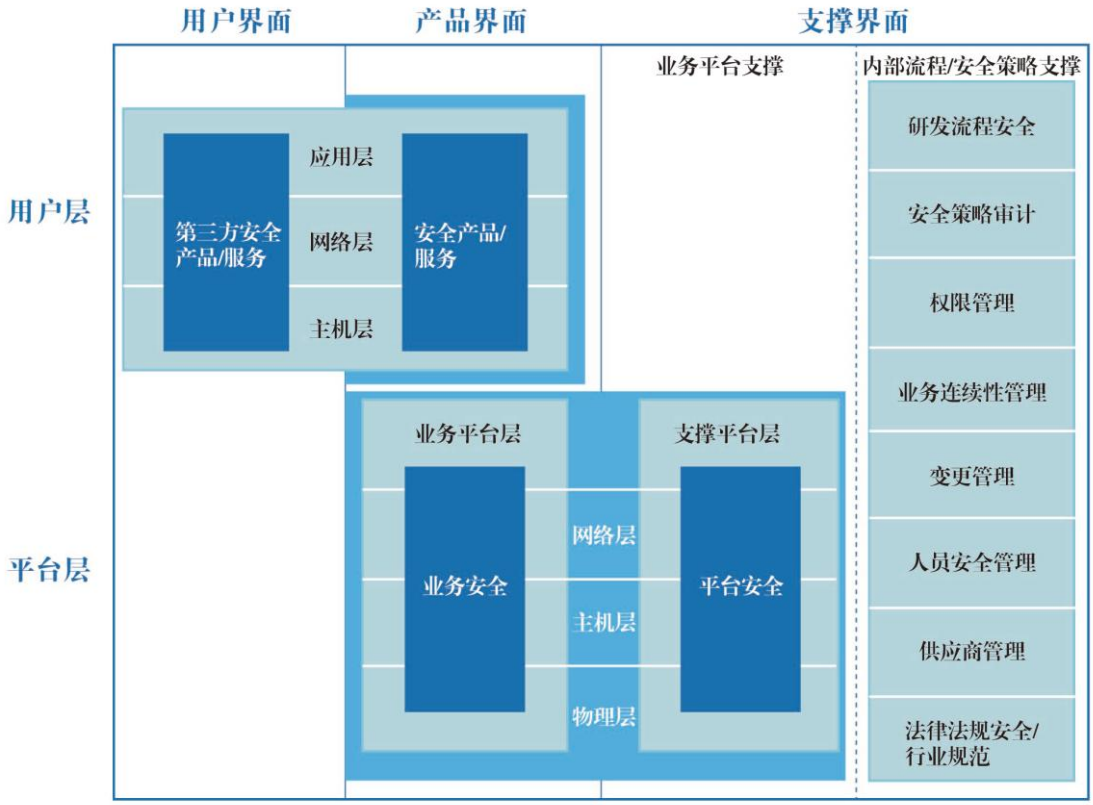
第三章健壮的腾讯云安全架构

3.1 腾讯云安全架构

取得第三方认证对于任何一家云服务商只是安全的一个标志，这些认证的取得则有赖于一个坚实、安全的云安全架构。这是保证腾讯云安全的基础，腾讯云安全团队不断为这一目标持续努力。

腾讯云将安全融入到了腾讯云业务的方方面面，腾讯云安全基于雄厚的技术底层支撑，建立了“两层三面”的体系化架构，实现多地调度、分权运维、高性能、高可用、高防御能力。

图 5 腾讯云安全“两层三面”架构



- **安全产品/服务层**

腾讯云在处理各种互联网安全问题的过程中，已积累相当多的技术和经验，腾讯云安全将这些宝贵的安全技术和经验充分融入到了优秀的云安全服务产品，客户可以方便快捷地使用这些安全服务保障业务安全。

- **业务平台安全层**

腾讯云提供了安全的云服务器、数据库等虚拟化计算资源，在资源抽象控制层进行安全加固，保障客户虚拟机的安全运行。

- **支撑平台安全**

腾讯云服务支撑系统相关的安全工作，保障了腾讯云服务系统的官网、时钟服务器、网管等组件的安全运行。

- **内部流程/安全策略支撑**

腾讯云从最初的研发实施控制、研发流程控制，到运维流程，到安全审计，再到访问权限、业务连续性、变更管理一系列内部管理体系中，严格遵守内部流程制度，确保了腾讯云产品和服务的有效运行。

3.2 腾讯云的基础安全防护

腾讯云通过采用多层次、多维度的实时监控和离线分析手段，为业务平台提供业务安全、信息安全等层面的安全服务。其中业务平台安全包括网络隔离、DDoS 防护、入侵检测和漏洞扫描四部分。腾讯云将这四个方面的防护内容最大程序基线化，并实现自动化安全运维管理。

在经历了五年多的安全实战保护中，腾讯云创造了接近两千日稳定运维的记录。为互联网、大型网游、游戏、高校、初创公司等诸多客户，提供了坚实的安全防护保障。其中，服务器的可用性达到了 99.9%，数据库的可用性达到了 99.999%。

腾讯云在网络隔离、入侵检测、漏洞扫描等方面，做了大量的基础工作。

- **网络隔离**

基于最小访问权限和攻击影响隔离的设计理念，腾讯云的网络架构进行了严格的安全隔离，要求不同客户之间的业务必须从链路层到应用层无法互访，以保护客户业务的机密性和完整性。

- **入侵检测**

腾讯云要求所有的腾讯云母机部署入侵检测软件，并实时检测软件的安装率，检测系统会基于特征码、行为等数据分析和挖掘等方法技术检测入侵行为。

- **漏洞扫描**

腾讯云要求所有 Web 系统必须部署漏洞防护系统，并要求漏洞扫描定期全量扫描腾讯云的 Web 业务服务器。腾讯云的安全团队与业界的安全组织和个人保持密切沟通，及时掌握业界最新出现的漏洞，并快速开发出相应的检测规则，完成漏洞的扫描检测并第一时间修复。

3.3 腾讯云全面继承腾讯集团的安全能力

腾讯集团为腾讯云安全提供了全面有力的技术、安全、防护、管理等的全方位支撑。在此支撑下，腾讯云基于互联网安全实践总结了云服务安全基线，并且自动地对云服务安全基线进行审计、并实时发现安全问题。不但从制度、机制、管理措施等环节，甚至包括使用习惯等细微之处，腾讯集团都进行了有力而全面的支撑，使得腾讯云得以稳健成长。

- **网络隔离**

腾讯集团对腾讯各机房隔离从网络规划、实时、运营阶段均提出了严格的网络隔离要求。例如研发机房和运营机房必须物理隔离，再例如云机房和集团办公网必须物理隔离等。所有物理隔离必须做到完全禁止路由可达白名单，两个网络设备如需互联必须通过双方外网 IP 进行互访。腾讯集团的网络团队和安全团队会一起制定网络规格规范和要求，网络团队按照规范实施后，网络运营阶段由安全团队审计，同时安全团队在每个机房内部署有网络连通性拨测设备，实时发现网络隔离失效并产生告警。安全团队接口责任人会在最短时间内修复网络问题。

- **入侵防护**

腾讯集团在每个机房的入口部署了入侵防护设备，并及时更新样本库。同时安全团队会定期对每个入口机器进行人工入侵行为审计。腾讯集团要求每个服务器必须默认关闭高危端口，例如 ssh、mysql 等协议常用端口。如果业务需要，必须在安全系统备案。

同时，腾讯集团要求所有服务器必须维护一个端口矩阵，服务器责任人必须可以明确说明每个端口的作用和打开必要性。腾讯集团要求每个服务器必须默认安装入侵检测插件，不得删除。安全团队会实时审计入侵检测插件的在线情况。腾讯集团要求每个提供外网 IP 的服务器都必须安装相应要求的安全防护软件，以防止服务器被入侵。

- **企业 IT 的安全监控和安全防护**

腾讯集团对公司员工办公电脑覆盖多层安全监控和安全防护，隔离内外网风险，防止外网入侵攻击，确保内网环境安全。针对外网管理层面，腾讯集团会屏蔽恶意站点，并对外来文件下载检测，防止由外到内到直接入侵。在内部网络管理层面，通过办公与开发运维环境分离、禁用高危端口及服务，防止进一步渗透内网。针对员工办公终端，腾讯集团要求办公终端必须安装自研安全客户端，以实时检测病毒感染、账号登陆异常等行为。安全客户端必须定期更新漏洞库和定期对员工终端进行病毒扫描，以增加办公终端反入侵的能力。

腾讯集团对公司业务系统的登录行为进行了规范，要求必须实行身份认证，而且认证身份方式必须为双因子认证方式。

另外，对于员工的新终端数据的管理也十分严格。新员工在分配新终端前必须对终端的硬盘进行低级格式化，回收仓库的终端必须进行磁盘消磁，最大限度的防范硬盘数据的遗失和泄漏。

- **安全事件管理**

腾讯集团和相关网络监管部门建立相应的联络机制，以及时获知最新网络监管要求，减小法律法规相关的风险。腾讯云会在第一时间处理相关安全事件，保证腾讯云平台的安全稳定及客户数据业务安全。

第四章可信赖的腾讯云安全产品和服务

随着企业自身业务不断的发展，腾讯遇到了各种各样的安全问题。在处理各种安全问题的过程中积累了相当多的技术和经验，腾讯云安全将这些安全技术和经验打造成优秀的安全服务产品，为客户提供业界领先的安全服务。帮助客户免受各种攻击行为的干扰和影响，专注于自身业务的创新和发展，极大地降低了在基础环境安全和业务安全上的投入和成本。

腾讯云安全能够提供可信赖的云安全产品和服务，其中包含：网络攻击防御、入侵检测、漏洞扫描等。

4.1 提供多维度的网络攻击防护服务

腾讯云安全提供了多维度的网络攻击防御服务，包括：网络攻击防御主要服务提供 DDoS 攻击防护、DNS 劫持检测等。

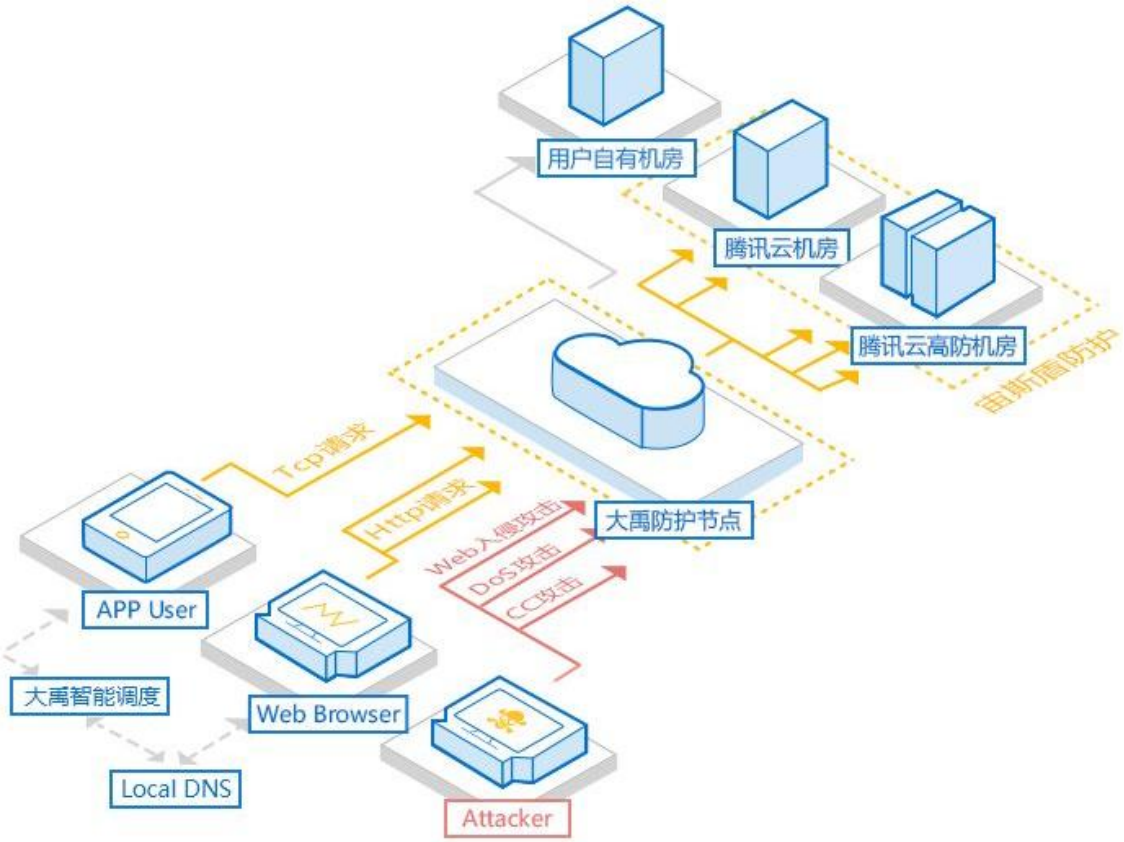
- **DDoS 攻击防护**

面对日益普遍的大流量 DDoS 攻击，腾讯云为客户提供了三种解决方案：

- **默认 DDoS 防护：**该方案采取了“集中检测+多级防护”的解决方案。通过在云机房出口部署自研检测设备集群—宙斯盾防护系统。宙斯盾系统是腾讯公司级 DDoS 攻击防护解决方案，为腾讯各大业务及腾讯云客户业务提供稳定可靠的 DDoS 攻击检测与防护能力，为业务的安全、稳定、健康运营保驾护航。其基于 DPI 检测技术，快速准确地发现针对业务的各种 DDoS 攻击；通过采用运营商黑洞路由、外网核心 ACL、专业清洗设备等多种手段，形成多层级的防护架构，有效防护各种 DDoS 攻击。

- **大禹分布式防护：**针对行业面临 DDoS 攻击流量越来越大的趋势，腾讯云安全团队自研并推出了一套业界领先防护方案——腾讯云安全分布式 DDoS 防护方案（简称大禹系统）。大禹系统专为 HTTP 类业务和移动端业务客户提供 T 级 DDoS 防护服务。大禹系统在全国部署了上百个攻击防护点，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，为客户业务的高可用性保驾护航。该方案采取了分布式防护的解决方案。通过在多地云机房外部署防护节点，分散流量，一方面提高攻击者的攻击门槛，另一方面增加 DDoS 防护的能力，同时还可以增加业务柔性，在面对大流量 DDoS 攻击时提高业务可用性。2015 年上半年大禹系统成功防御的外部攻击流量峰值达 300Gbps。

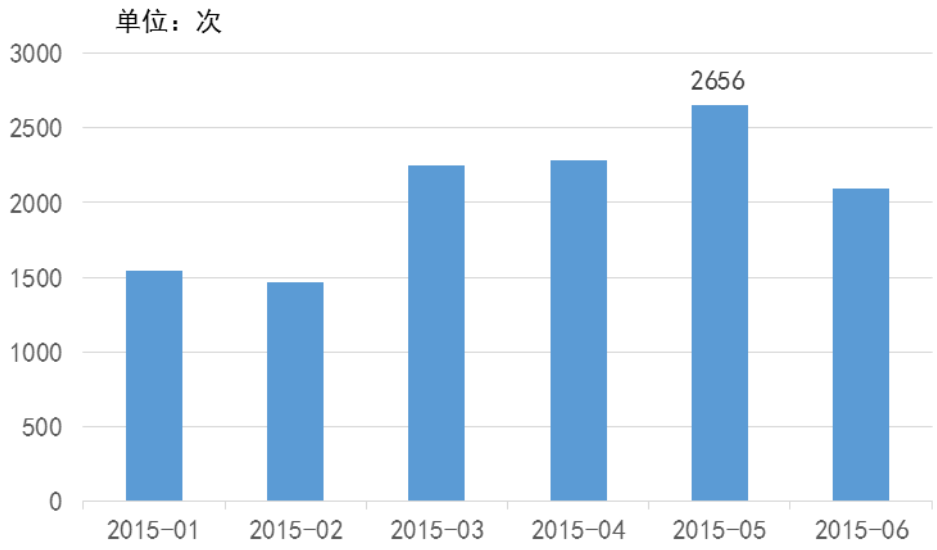
图 6 腾讯云安全分布式 DDoS 防御系统—大禹



- **DDoS 高防服务：**该方案为对全协议大流量 DDoS 防护存在需求的客户提供解决方案。DDoS 高防服务是默认 DDoS 防护方案的升级版，腾讯云将机房带宽和宙斯盾的防护能力提升至数百 G。

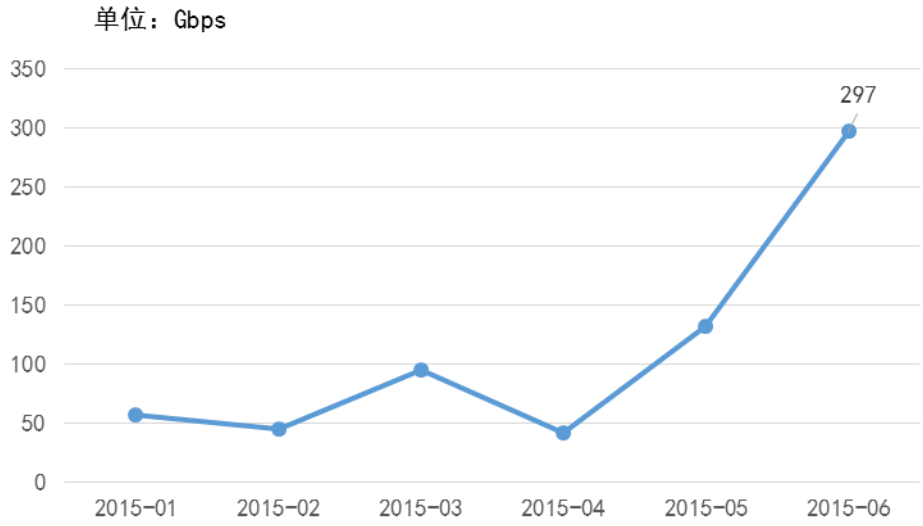
2015 年上半年，腾讯云安全经受住了最严峻的 DDoS 攻击考验，有数千台主机遭受外部黑客 1 万多次 DDoS 攻击。峰值月份受到 DDoS 攻击次数达到 2600 多次。

图 7 腾讯云 2015H1 遭受 DDoS 攻击次数月度数量统计



从 2015 上半年的统计数据显示，腾讯云平台被攻击的最大流量逐月都在上涨，最高峰值月份接近 300Gbps。

图 8 腾讯云 2015H1 遭受 DDoS 攻击流量峰值月度分析



- **DNS 劫持检测**

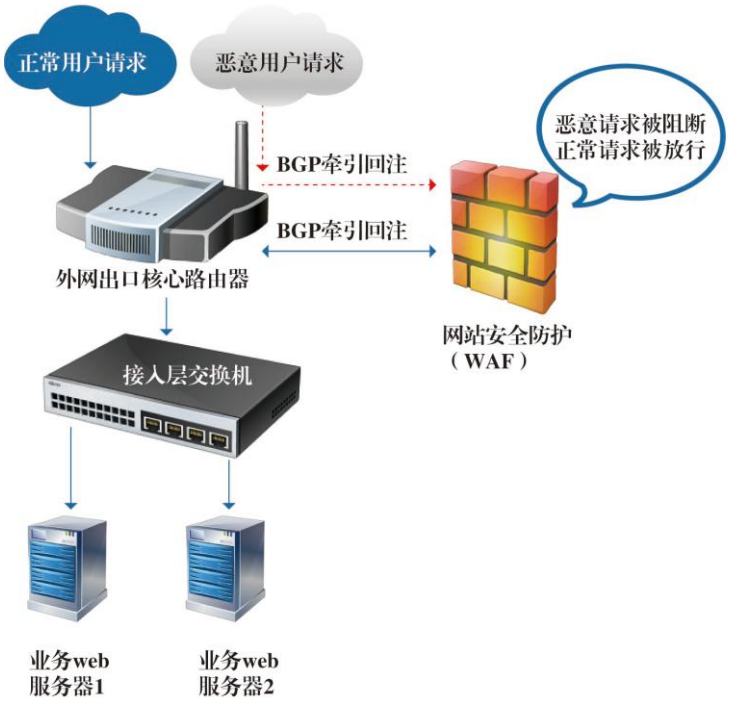
DNS 劫持是一种通过改变指定域名在运营商侧 Local DNS 配置的解析地址，将该域名的解析结果重定向到劫持 IP 的行为。为了快速发现针对业务域名的 DNS 劫持，腾讯云采取了分布式探测和集中分析防护相结合的架构模型。通过在全国部署 400+个探测指针，周期性地向本地的 Local DNS 发送域名解析请求，并对响应结果进行集中汇总和分析匹配，从而快速、准确、全面的发现域名劫持行为。

4.2 提供坚固的入侵防护

入侵是指黑客利用网站和服务器漏洞，或通过窃取账号、暴力破解等方式，绕过访问控制，非法获取服务器权限，执行命令，查看文件，甚至盗取数据，给业务造成重大损失的恶意行为。腾讯云安全提供了专业的入侵防护服务，首先，为了实现入侵行为快速发现，腾讯云采取了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。然后，在 Web 防护能力层面，腾讯云采取了扫描器主动扫描加 WAF（Web Application Firewall）防御的模式。在主机防护能力层面，还可提供暴力破解和异地登录提醒、后门木马检测等服务。

腾讯云提供的扫描和防护功能所需的样本库来自腾讯自身业务发现积累和 TSRC(Tencent Security Response Center)的行业收集两个渠道，具备全面性和实时性的优势。同时针对常见软件新发现的 0day 漏洞，腾讯云会第一时间更新检测和防护规则，为腾讯云客户提供持续发现和防护等能力的漏洞扫描和防御服务。

图 9 腾讯云安全 Web 漏洞防御系统-WAF



腾讯云安全入侵防护能力经受住严峻的考验。在 2015 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 45 万次，WAF 累计拦截 1.3 亿多次 Web 漏洞攻击；累计发现 Webshell 4 千多个。在主机防护层面，主机暴力破解自动拦截功能从 5 月份上线开通以来，截止 6 月份拦截暴力破解月度数量统计达到 1 亿多次。

图 10 腾讯云 2015H1 扫描 Web 漏洞月度数量统计

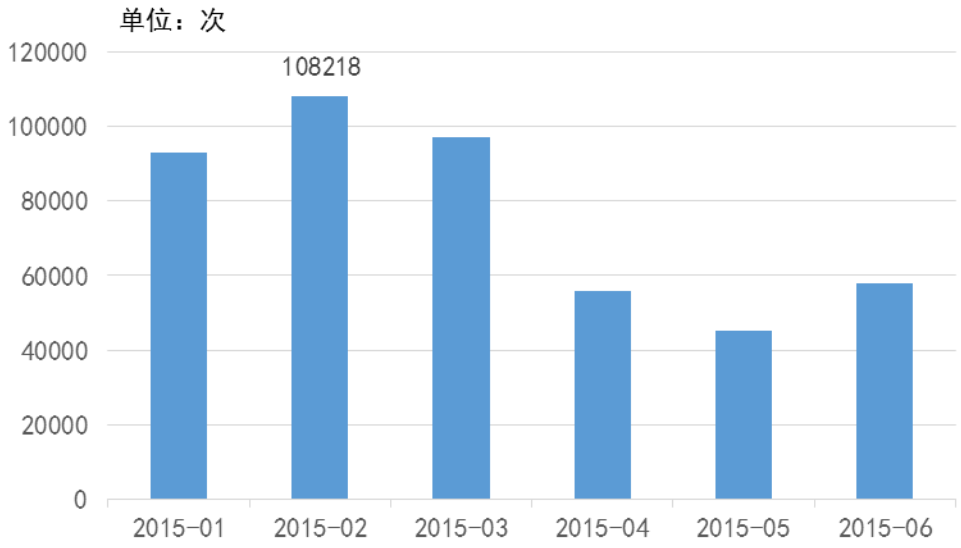


图 11 腾讯云 2015H1 WAF 拦劫恶意请求月度数量统计

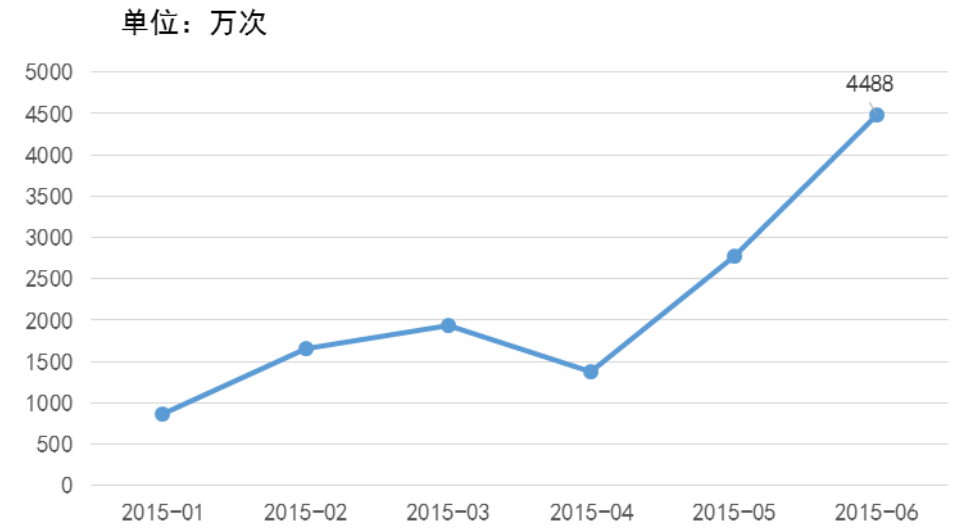


图 12 腾讯云 2015H1 检测发现 Webshell 月度数量统计

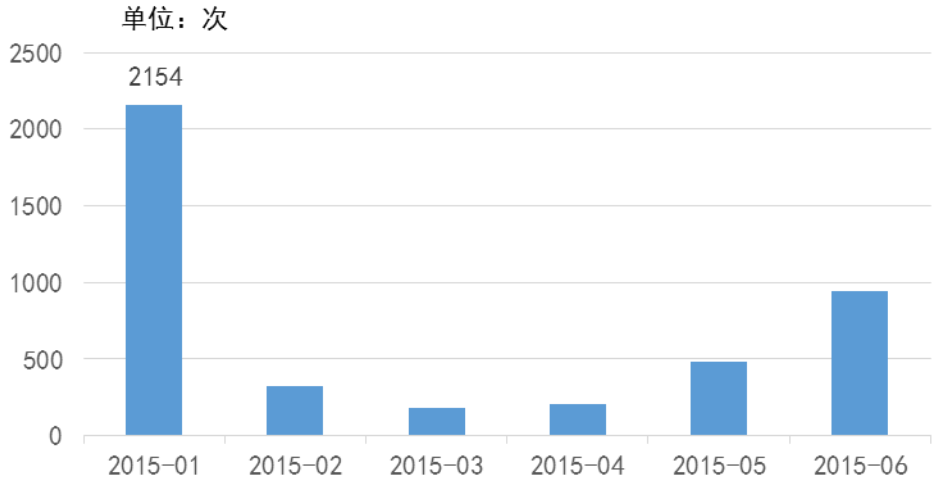
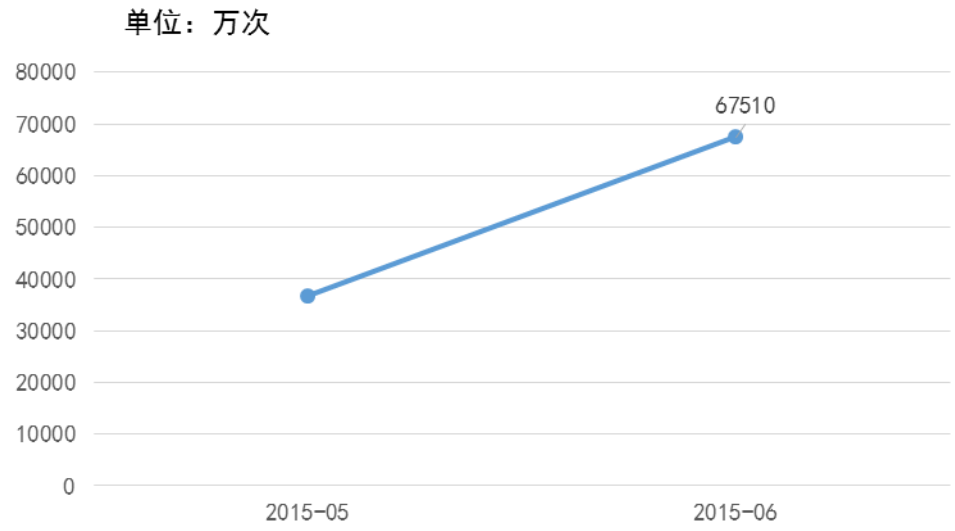


图 13 腾讯云 2015 5-6 月拦截主机登录暴力破解月度数量统计



4.3 提供开放的业务安全服务

腾讯云为客户提供的业务和信息安全类服务——天御，致力于将腾讯在业务和信息安全方面积累的技术和经验分享给客户。天御通过简单开放的接口，让客户快速获得专业的安全能力，目前天御提供关键词检测、文件检测，消息过滤、防恶意注册、防恶意登录、活动防刷和验证的服务功能。

- **关键词检测，**依托于腾讯平台多年积累的完备关键字库，可准确识别各类文本信息中的关键字。关键词匹配识别后，可提交人工审核，也可自动过滤，帮助客户构建合规、绿色的网络环境。

- **文件检测，**深度扫描用户上载、传播的文件内容，识别其中是否包含木马、违规图片等恶意内容，阻断恶意文件的传播，保护客户网络和主机的安全。

- **消息过滤，**一方面对客户用户产生的消息进行检测，识别其消息中是否含有广告、政治、色情等不良信息；另一方面对客户用户产生消息的行为模式进行分析，识别其中的恶意转发、推广等不良行为，加以过滤屏蔽。保护客户正常用户免受不良消息的滋扰。

- **防恶意注册，**通过腾讯大数据平台分析客户系统注册者的信息，识别其中的恶意注册用户和行为，对其加以标识，帮助客户对恶意行为进行预防和限制。

- **防恶意登录，**依靠腾讯大数据平台和对客户用户登录行为分析，识别出其中的恶意登录行为，对其进行限制或阻断，帮助客户保护其用户账户的安全。

- **活动防刷，**针对电商、O2O 服务商、互联网金融厂商等客户组织的节庆、拉新等返利活动提供防护服务，依托腾讯大数据平台掌握的海量信息，识别出活动参与者中的恶意刷取返利的“羊毛党”用户，对其进行限制，保护客户的活动资金安全。

- **验证码，**使用继传统码式验证技术革新之后的新一代安全验证技术。腾讯云提供的验证码类型丰富，并有专门团队针对各类恶意破解攻击进行算法对抗，具有高强度防御能力和安全稳定性，为客户的业务提供坚固的安全保障。

图 14 腾讯云业务安全开放的能力和服务

4.4 提供权威的云安全认证

腾讯云的安全认证,是腾讯云通过审核的客户安全状况，符合腾讯云安全要求以后对客户颁发权威的腾讯云认证，并提供腾讯云安全认证展示的服务，让客户的业务获得腾讯亿万用户的认可。

腾讯云安全认证包含了云安全服务开通审计、Web 内容安全审计、Web 漏洞检测、主机基线检测和 APP 刷量审计六大功能检测。

第五章完善的腾讯云业务保障流程

5.1 腾讯云研发流程控制

腾讯云十分注重内部保障流程的安全，在云服务生命周期每个阶段均实施了安全风险控制程序。从需求设计、到系统上线、再到系统运营每一个环节都融入了“安全是基石”的这一理念。从内部、从源头保证了腾讯云架构和腾讯云产品、服务的安全运营。

- **需求阶段**

在需求设计阶段中，腾讯云安全团队会对规划中的需求进行安全风险分析，以解析识别出产品规划中的安全风险和安全需求。腾讯云规定安全需求是与产品需求同等优先级。

- **设计阶段**

在内部设计阶段中，安全团队会对于产品经理的需求和产品架构师给出的架构进行安全评审。安全团队评估软件架构设计的安全性，并同腾讯云开发团队一起完成安全的云服务解决方案。

- **开发阶段**

在系统开发阶段，安全团队制定了安全开发规范，要求开发人员必须遵从，最大限度减少编码时出现安全漏洞。代码转测前，必须进行安全性自测，并且必须使用代码安全扫描工具进行代码安全性检测，确保代码的安全性和健壮性。

- **测试阶段**

业务团队除进行常规测试外，还会依照腾讯云安全控制基线执行安全测试。腾讯云安全团队会对软件做软件代码安全扫描和人工渗透测试，全面检测和挖掘潜在的安全问题。

- **发布阶段**

腾讯云要求软件发布时，必须经过产品、研发、测试、安全、运维等相关团队评估并且同意后，才可灰度发布。安全团队会检测安全需求的落地情况、代码测试结果、业务部署情况等综合检查。安全团队具备一票否决权，如果根据上述流程检查后存在问题将拒绝版本发布。

- **运营阶段**

安全团队通过实时监控业内安全漏洞信息，第一时间发现涉及腾讯云服务的安全威胁和风险，及时响应并予修复。

图 15 腾讯云研发安全流程

5.2 腾讯云外部漏洞发现与修复

腾讯集团制定了《腾讯外部漏洞报告处理流程》的制度。腾讯集团认为每个安全漏洞的处理和整个安全行业的进步，都离不开各方的共同合作。竭力促进企业、安全公司、安全组织、安全研究者一起加入到“负责任的漏洞披露”过程中来，一起为建设安全健康的互联网而努力。

腾讯云对于外部漏洞的发现与修复形成了一个自我检查，自我发现，自我修复的闭环。在腾讯外部漏洞报告处理流程中，包含了漏洞反馈与处理流程、安全漏洞评分标准、奖励发放原则和争议解决办法等一整套完整的体系。腾讯云根据漏洞危害程度制定了严格的安全漏洞评分标准，包括严重、高、中三个等级，并依据漏洞危害程度，制定了相应的漏洞处置方案，保障云平台安全。

同时，公司的 TSRC 也会通过各种渠道去收集产品的漏洞信息。TSRC 的漏洞发现渠道包括:乌云、合作的软件供应商、白帽子反馈，以及云计算行业安全技术圈中交流。

腾讯云的漏洞一旦被发现，必须在 24 小时内修复。

表 2 腾讯云安全漏洞评级标准

危害程度	漏洞程度	示例
严重	获取服务器权限	直接/有条件的任意代码执行 直接/有条件的任意命令执行
	获取数据库内容	SQL注入漏洞
高	直接盗取管理员/用户身份信息	存储型XSS漏洞
	越权访问	以管理员身份执行敏感操作
中	交互盗取用户身份信息	反射型XSS
	伪造利用用户身份信息	造成实质危害的CSRF
	信息泄漏漏洞	普通的信息泄漏漏洞

5.3 腾讯云权限管理

腾讯云所有的权限配置均遵循符合最小化的原则，保证腾讯云上信息系统的机密性、完整性和可用性。例如，腾讯云机房的核心交换机会专门单独上锁，机柜钥匙只由机房经理管理。

腾讯云要求工作职责必须分离到多种角色。例如软件开发和发布权限不得分配至同一员工。腾讯云要求所有的权限都必须有明确期限。对于职责必须的权限，例如开发跳板机登录权限，腾讯云要求开发人员的开发机跳板机的登录权限必须每隔三个月重新申请一次。对于职责转变的情况，腾讯云要求立刻撤销与该员工原职责相关的权限。

5.4 腾讯云业务连续性管理

腾讯云从基础架构的容灾性、网络和计算单元的可用性、数据的可靠性、日常运维的连续性管理等四个方面来保障业务的连续性。

5.4.1 基础架构容灾性

腾讯云的云机房部署在华南、华东、香港、海外等多个地区，客户可根据业务发展需求，自主将业务灵活地部署在不同区域，以保证业务的容灾性要求。云机房的基础架构建设及环境设计也为客户提供最底层的冗余和部署的高可用性，比如供电系统、空调系统、火灾检测防护系统、动力系统等都具备灾备冗余及高可用性。

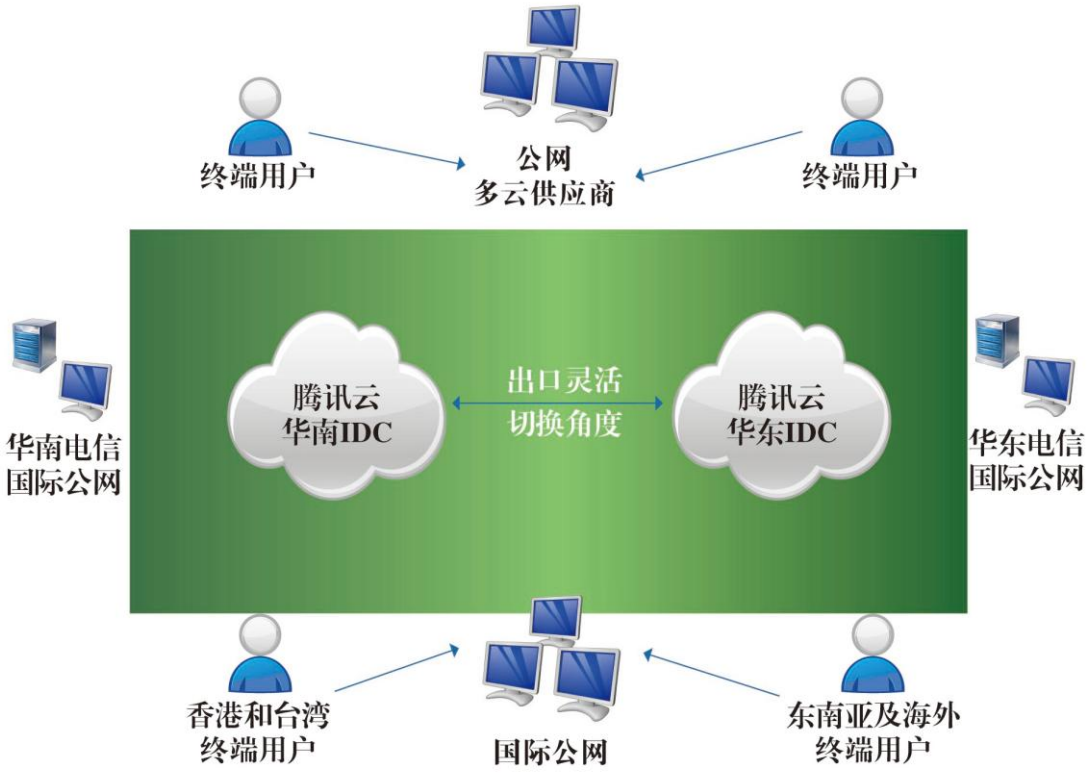
例如在供电系统方面，目前行业主流方案是成本和可靠性较低的 N+1 设计和成本和可靠性较高的 2N 设计。腾讯云数据中心的供电系统线路的各个环节（如市电进线、柴油发电机、UPS 系统、机柜 PDU 等）均是完全独立的 2N 设计。如果一路某个环节出现故障，供电系统将无缝切换到另一供电线路。

5.4.2 网络和计算单元可用性

腾讯云网络采用 NxN 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，保证不因为单点设备故障而导致网络服务中断。腾讯云的计算单元也是采用 NxN 的冗余建设方式，单一计算单元在故障发生时通过调度器实时剔除，保障业务的可用性要求。腾讯云 IDC 网络出口分多个地域对接多个运营商，通过建设腾讯云网络跨地域灾备能力，有效地降低运营商公网故障带来的持续性影响。

截止 2015 年上半年，涉及到安全防护的事件，运营商公网网络故障超过 83 例，BGP 跨网切换执行约 71 次，有效规避故障影响时长约 2,730 分钟以上。

图 16 腾讯云跨地区灾备能力



5.4.3 数据可靠性保障

腾讯云对云数据库、NoSQL 高速存储、云硬盘分别实施不同的数据可靠性措施。对云数据库，腾讯云全部采用 RAID 类型存储设备，同时再配合每天一次冷备和双机热备的方式来保障数据的可靠性，目前云数据库可以达到五个九的可靠性。对 NoSQL 高速存储和云硬盘，腾讯云同样全部采用有 RAID 的存储设备，同时在存储架构设计上确保数据的可靠性，存储系统会自动为每份数据保持 3 个备份，保障数据可靠性达到业内最高水平 5 个九。

5.4.4 日常运维连续性管理

腾讯云在数据中心建立了 7*24 的人员驻场服务，对基础设施、网络架构以及计算单元进行定时巡检。腾讯云要求运维人员定期模拟故障灾备场景演练，验证系统具备遇到不可预测故障时对应能力和方案，确保架构冗余灾备系统的可用性和可靠性。同时，腾讯云把业务的连续性纳入运维的故障响应管理机制中，进一步保障腾讯云服务的连续性和可靠性。

表 3 腾讯云 2015H1 演习的数据统计

时间周期	演练对象	次数
2015H1	应用服务灾备冗余演练	37次
	IDC机房环境灾备演练	27次
	网络架构灾备冗余演练	25次
	安全攻击防护测试	15次

5.5 腾讯云变更管理

腾讯云要求软件发布时，必须经过产品、研发、测试、安全、运维等相关团队的评估并且同意后，才可执行。要求发布后进行留守观察。同时发布系统会记录每一次发布操作的详细信息。腾讯云要求严格把握变更发布管控和发布结果跟踪验证，严格按变更流程操作，变更执行前必须有明确的变更影响范围评估和监控、回滚、结果验证方案。

腾讯云严禁私自使用外包、开源、非腾讯云授权安装的软件，如需使用必须经过安全、质量、法务等相关方的评估和测试。安全团队会定期审计发布系统日志，以发现非法发布的行为和不依照流程发布的行为，并予以处罚。腾讯云产品在发布变更、基础架构变更优化等操作时，都有固定的时间窗口，并有严格的测试验证流程，部分会造成客户感知的变更固定安排在低峰期执行，并及时做好客户服务沟通。同时，在客户重点业务推广阶段，运维团队会执行变更绕行策略为客户业务推广活动保驾护航。不但如此，腾讯云每个软件升级除经过研发、运维、安全、测试、客户经理等评估外，要求每次升级通过灰度即分批进行发布和验证，以最大程度地减小现网影响。

5.6 腾讯云售后服务管理

腾讯云提供 7*24 在线服务支持，建立了企业 QQ、QQ 群、微信公众账号、微信群、客服电话等服务渠道以帮助客户快速解决问题，为云服务的连续性提供人工保障。腾讯云还为客户建立了短信、邮件、微信、语音、站内信、公告等渠道推送通知、告警和安全事件等。

综上所述，腾讯云从最初的研发流程控制，到运维流程，再到访问权限、业务连续性、变更管理一系列内部管理体系中，严格遵守内部流程制度，确保了腾讯云产品和服务的有效运行。

第六章可靠的腾讯云物理环境

周密的内部管控措施再结合安全的云物理环境，是打造腾讯云生态圈的有力保障。

腾讯云对云机房的物理和环境安全建立了专门的管理体系，从体系的高度来管理物理和环境安全。管理体系包括：对物理环境进行安全区域划分、制定规范文档、监督实施执行及优化改进多个部分。

6.1 物理区域安全

为防范对腾讯云机房未经授权的物理访问、损坏和干扰，腾讯云制定下列措施和规范，对物理访问行为进行严格的管理。

- **对机房进行了安全区域的识别和划分**

腾讯云对不同区域定义了不同的三类安全级别。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。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。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、TBOSS、CFT 专区。

- **建立物理访问控制管理制度**

腾讯云对云机房不同级别安全区域的物理访问制定了不同级别的访问控制管理制度，以保障云机房的物理安全。这些制度包括：交接区安全管理；人员出入管理；车辆出入管理；监控管理；门禁钥匙管理；受限区域作业许可管理。

- **交接区安全管理：**交接区实施 7*24 小时无盲点的监控，监控录像存储时间不少于 2 个月。交接区要求与信息处理设施隔离，在交接区域各通道门安装并启用门禁系统。

- **人员出入管理：**根据人员类别及安全区域，建立人员控制访问安全矩阵，对进出 IDC 的人员进行控制。人员出入 IDC 需进行身份核对和随身物品检查，并登记携带物品。

- **车辆出入管理：**原则上公共车辆不允许进入 IDC；已授权进入 IDC 的车辆如个人车辆、货车等，需进行车辆信息登记；物流送货车辆，只允许进入交接区。

- **监控管理：**IDC 园区出入口，园区内各建筑物单体出入口，要求 7*24 小时无盲点的监控并配备保安室并提供 7*24 小时值守；各个功能间，依据设备及敏感信息的重要性及来访的频率，实施不同的安全监控措施。

- **门禁钥匙管理：**门禁管理系统要支撑按区域的门禁授权；门禁卡最长时间不超过 1 年；1 年后需重新确认持卡人身份及权限。

- **受限区域作业许可管理：**在受限区域内操作，需保持大门常闭状态，并确保办公完成后锁好；外部员工在受限区域工作需要有人监守。并对操作人员作业资格和施工人员做具体要求。

6.2 设备安全

腾讯云从电力、空调、消防和静电防护等几个方面保障了云机房的设备安全。腾讯云的电力系统和空调系统都是全冗余的系统，在任意单点故障情况下，均能确保机房电力和供冷的持续性。腾讯云的消防系统安装有火灾探测系统、自动气体灭火系统以及手动灭火器，机房管理人员还会定期接受火灾预防及灭火演练培训。腾讯云的机房内部全部安装防静电地板，机柜、线槽等全部安装接地线，用以防范静电给设备带来损害。

6.3 安保巡检管理

腾讯云要求安保人员（保安）正常状态下必须配备相应的工具/设备，巡检前，保安必须对工具/设备进行检查安全，并且必须定期进行巡检，巡检频率不低于每 2 小时/次；各 IDC 配备安全巡检清单及巡检计划，要求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，启动紧急流程。

6.4 安全事件管理

现场应制订物理安全应急预案，并定期进行安全演习或演练。一旦发生物理安全事件，预案能够立即生效以最大可能保护客户资产，必须以确保人身安全为第一要素。

6.5 物理安全审计

对上述措施和规范的落地执行，腾讯云建立定期的安全审计管理制度，定期对物理安全现场执行和管理进行审计，并输出审计报告，跟进和推动审计风险点的改进。

图 17 腾讯云物理和环境安全管理体系

第七章全面的内部人员和供应商安全管理

7.1 腾讯云完备的内部人员管理体系和流程

腾讯云团队的建设，依托腾讯集团完备的内部人员管理体系和流程的约束。腾讯在雇佣前、雇佣中、雇佣后都采取了一系列的措施来避免员工有意或无意的出现不当行为，并在出现问题后能及时发现和处理。

- **雇佣前**

在国家的法律允许范围内，腾讯集团对新招聘的员工做资格和背景调查，犯罪记录、不诚信记录等不良记录都会在雇佣员工的时候被考虑，以规避员工盗窃、滥用、误用数据与设施等恶意行为的风险。

- **雇佣中**

腾讯集团规定新入职的员工都必须参加信息安全的培训，并要求通过考试。对重要职位的员工，腾讯云要求必须签署保密协议。同时安全审计团队会持续地对员工的行为进行审计，确保员工的行为合乎公司的规范。腾讯云也提供了投诉和举报途径，对腾讯云员工的不正当行为（如泄密、收受贿赂），客户可以通过公开的途径向腾讯云的安全审计团队投诉。

- **雇佣后**

腾讯集团的《离职员工管理办法》中规定离职流程中有一项信息安全确认，确保腾讯云离职员工所拥有的系统权限都已经撤销，相应的帐号和密码都已被回收或者修改，保障与客户有关的信息不会被泄漏。同时离职的员工仍然需要遵守与公司签订的保密协议，确保不会泄漏与腾讯云相关的机密。

7.2 腾讯云面向供应商风险安全管理体系

人员的安全管理从两个方面入手，在管理腾讯云自身员工的同时，加强和强化供应商安全管理尤为重要，两方面结合是造就腾讯云内部安全的一道有力的保障。

腾讯云制定了严格的供应商准入要求、选择机制以及市场份额控制机制。腾讯云要求每个供应商都必须有风险管理信息系统、可维持其服务质量持续运行的规章制度以及演练记录，并且要求定期反馈演练记录或者规章规范实施证明，同时会与各个供应商核查 SLA 达标情况。腾讯云要求每个供应商都必须第一时间通知其产品、服务存在的缺陷、漏洞等风险/影响以及对应解决措施。

腾讯云建立定期审计制度，检查每个供应商 SLA 的完成情况以及合同义务履行情况，并对每个供应商的服务进行风险评估。对于评估服务风险较大的供应商，会采取一定的措施以减小影响腾讯云服务持续运行的风险。

第八章未来云安全的发展趋势

进入“互联网+”时代，网络安全、信息安全在国家战略上的地位越来越凸显，加上近两年数据泄露事件频发，保证客户的信息安全也变得越来越重要。

腾讯云认为，作为“互联网+”重要一环的云计算，实际上云计算能提供远高于本地数据中心的高可用性、数据安全、隐私保护以及异地数据灾备服务，确保互联网服务的运营和数据安全万无一失。

腾讯云致力于云计算安全的不断探索和不断提升，我们认为未来云安全的发展将呈现出以下四个趋势：

1、**业务安全开放将促进云上的安全平台和通用安全服务的全面发展。**随着企业把越来愈多的业务应用放在云端，企业需要获得更高的业务安全服务的保障。目前云上的业务安全服务包括：关键词检测、文件检测，消息过滤、防恶意注册、防恶意登录、活动防刷和验证码等和客户业务相关的通用化服务功能，同时在此平台上还能够帮助客户根据自己的业务情况配置个性化业务安全的功能，从而促进云上安全平台和通用安全服务的全面发展。

2、软件定义安全（Software Defined Security，以下简称 SDS）将提升云计算安全平台的纵深防御能力。随着 SDN 技术的不断普及，SDS 技术是未来安全防护技术发展的重要方向。SDS 技术将网络安全设备接入、部署进行技术解耦实现资源池化，使云客户可以通过编程方式定制安全规则按需接入，增强了云安全网络防护服务的柔性和弹性。同时对于平台自身，软件定义打破了安全设备的封闭性和有界性，强调构建安全联动机制。其使得安全防护系统可自动、甚至自适应地制定规则防御网络攻击，构建更加有效的纵深防护体系。相信未来 SDS 技术可以在兼顾最小开放原则的同时，可使各安全设备和各应用软件间更加有效地联动，进而提升云平台整体的安全性。

3、数据协作安全。云计算行业安全认证规范和行业合规的提升，将刺激企业用户对数据控制和数据安全需求的不断增长。在数据协作的安全性方面，大量数据将通过各种云计算服务交付，可能会流经多个网络，而相关的数据隔离和数据控制优化功能也在不断涌现。同态加密是未来解决这个难题的有效方式。对经过同态加密的数据进行操作得到一个输出，将这一输出进行同态解密，其结果与用同一方法操作未加密的原始数据得到的输出结果是一样的。

4、云计算在企业中大规模普及和深入应用，虚拟私有云（VPC）将成为解决混合云安全问题的简化方案。随着越来越多的企业开始使用云计算服务，混合云已经成为一种重要的企业业务部署方式，并将长期在企业中存在。在混合云的环境中，影响安全的因素变得更多，安全问题也变得更加复杂。首先，需要考虑公有云和私有云两个环境各自的安全

问题；其次，由于混合云中公有云与私有云的安全边界的定义变得模糊，因此混合云的网络安全规则将会变得非常复杂；再次，不同类型的云应用也会衍生出新的安全问题，并且安全问题将和客户业务一样具备多样性。针对这种趋势，VPC 方案将是一种简化混合云安全问题的解决方案。其可以通过 OverLay、VPN、双因子认证等技术，使云客户可以统一管理公有云和私有云网络，简化客户业务在混合云下的部署场景，进而简化混合云下安全策略的制定工作。

总之，对关键数据节点的逻辑划分能力为企业和机构提供了更高的信息灵活性。有一点可以确认的是，未来建立在云计算上的各种新的应用，必然与其对应安全方案的发展相辅相成，是一个不断探索、不断发现、不断完善和不断提升的过程。

第九章结语

综上所述，腾讯云在安全策略、认证合规、云安全架构、产品/服务、内部流程保障、物理环境、人员和供应商管控各个环节，做到了周密完整的安全保障，使腾讯云安全生态圈形成完整闭环。

为了让客户获得腾讯云的全面安全保障，腾讯云通过构建安全云基础架构，建立完善的云安全管理流程和制度打造出了业界领先的云安全产品和服务。

长期的实践证明腾讯云安全能力具有全方位、多维度安全防护的优势。更重要的是，腾讯云全是由具备多年安全经验与历练的腾讯安全团队建设和运维，他们为客户提供的安全服务和产品，为客户的业务顺利发展保驾护航。

腾讯云致力于为客户提供专业、稳定、可靠的服务。

腾讯云，安全，值得信赖。