目录

安全白皮书前言

北京金山云网络技术有限公司（以下简称“金山云”）为金山软件旗下子公司，成立于2012年，是国内优秀的云计算服务提供商。金山云以业内优秀的服务端技术，为用户和企业提供稳定性高、安全性强的云服务产品。

依托金山软件集团20余年的深厚积累，金山云从创立之初便将云安全放在首要位置，并持续加大云安全技术研发投入，已陆续推出基础防护、高防IP、服务器安全、漏洞扫描、Web应用防火墙、高级安全服务等云安全产品，为云上用户保驾护航。本白皮书中，我们将从云安全责任共担模型、安全合规性、基础设施安全、安全产品、数据安全、安全组织、运维安全、云安全工程能力等方面介绍金山云在安全领域的控制。

云安全责任共担模型

金山云有完善的云计算基础架构安全以及用户业务安全保护体系，可以对用户提供全方位的从物理到应用层面的防护。同时用户云上业务的安全，是云服务提供商和用户需要共同努力来解决的问题。金山云采取安全责任共担的机制，与用户共同保障用户安全。金山云负责通过各种技术与管理手段，例如SDL、漏洞扫描、监控、审计等方式来保障云计算基础架构层面的安全，即包括物理、网络、虚拟化架构、数据安全、控制台等；用户负责自身业务部署、运维的安全，金山云提供必要的安全产品和服务，保证用户业务层面的安全。

安全合规性

金山云将云安全的合规性放在战略位置，成立有专门的合规与风控团队，积极与国内和国际的合规性对标，给用户提供稳定性高，安全性强的产品，为用户带来更优质的安全体验。

目前已通过国家及国际的多项合规性认证，2015年12月，金山云获得ISO9001/ISO20000/27001管理体系认证以及国家信息系统安全等级保护测评第三级认证；2016年9月通过可信云服务安全认证；2016年10月获得国际云安全联盟CSA颁发的C-STAR认证；2016年12月金山云荣获首批增强型云计算服务能力证书，该增强型等级为该认证的最高等级；2017年12月获得国内首家CSA STAR Tech IaaS/PaaS双认证；2018年7月30日获得由中国信息通信研究院及数据中心联盟颁发的云服务用户数据保护能力资质证明。2018年12月金山云通过美国注册会计师协会（AICPA）SOC审计。

2018年5月25日，欧洲联盟出台《通用数据保护条例》（General Data Protection Regulation，简称GDPR），GDPR出台后，金山云一直在重点持续关注，在2019年金山云也会将GDPR放在合规工作的计划当中，积极与国际的合规性对标，提高金山云的安全体验。

ISO9001/ISO20000/27001管理体系认证

ISO27001信息安全管理体系、ISO9001质量管理体系、ISO20000 IT服务管理体系三大体系认证的顺利通过，标志着金山云在信息安全管理、服务质量 管理、IT服务管理等方面达到了更规范化、更标准化的水平，为公司全面质量体系的改进和完善奠定坚实的基础。 其中ISO27001是全球广泛采用的信息安全领域的管理体系标准，可有效保护信息资源，保护信息化进程健康、有序、可持续发展。金山云的信息安全管理体系涵盖了云主机、云存储、网络、数据库等云计算相关业务，并已具备有完善的系统的方法来管理信息安全风险，保证公司业务良好的持续运行。

信息安全等级保护

信息安全等级保护是由等级测评机构依据国家信息安全等级保护制度规定，按照管理规范和技术标准，对信息系统安全等级保护状况进行检测评估的活动。基于对国家信息安全保障方面制度的重视，为了最大限度的满足金山云用户对于等保的相关技术和管理要求，金山云积极配合公安部门开展等级保护相关工作，并获得公安部国家信息安全等级保护三级标准认证，此认证说明金山云在技术、管理层面均达到国家指标并有能力帮助客户具备三级等保所要求的，安全事件的发现、应对能力，信息系统受到破坏时的恢复能力。

可信云服务安全认证

可信云服务安全认证基于云服务的业务安全，从用户的角度出发，考察云服务提供商所提供的云服务的安全保障程度。该认证分为文档审核、技术测评、运维系统现场查验、技术专家评审、外部复审五个环节，每个环节都有严格的评审通过标准。此次金山云通过可信云服务安全认证，意味着金山云全部指标都达到国内顶级云服务评测系统的认证标准。其中对象存储标准存储和低频存储提供99.9%的可用性，归档存储提供99%的可用性，99.999999999%数据持久性两项重要指标均达到业界领先水平。

C-STAR云安全评估

C-STAR是全球认可的国内最高级别的云安全认证，该认证代表国际权威机构对金山云安全管理水平以及技术能力的认可。C-STAR云安全评估的管控要求极为严格，评估过程采用国际先进的成熟度等级评价模型，涵盖应用和接口安全、审计保证与合规性、业务连续性管理和操作弹性、变更控制和配置管理、数据安全和信息生命周期管理、加密和密钥管理、治理和风险管理、身份识别和访问管理、基础设施和虚拟化安全、安全事件管理、供应链管理、威胁和脆弱性管理等控制域的全方位安全评估。金山云在上述控制域都有完善的管控机制，以保证金山云业务安全合规和可持续经营。

云计算服务能力评估

为推动提升云计算服务能力、规范云计算服务市场，中国电子工业标准化技术协会信息技术服务分会（ITSS分会）依据《信息技术云计算 云服务运营通用要求》等国家标准开展了云计算服务能力评估试点工作。经审定，金山云荣获首批增强型云计算服务能力符合性证书， 该增强型等级为该认证的最高等级。该认证说明金山云的服务能力包括人员、流程、技术和资源等方面均走在云服务提供商的前列。

CSA STAR Tech IaaS/PaaS安全增强双认证

CSA STAR Tech认证是国际知名安全认证机构CSA（Cloud Security Alliance，云安全联盟）推出的针对云计算产品的安全能力认证，以CSA发布的安全技术标准《CSA云计算安全技术要求》为测试标准进行审核。作为CSA联合国内外云厂商共同研究并起草的安全产品标准，该标准明确了IaaS/PaaS/SaaS产品的安全能力级别要求，是云计算产品最权威的统一安全能力级别认证标准，标志着金山云安全能力和水平的进一步提升。

云服务用户数据保护能力认证

云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。金山云公有云于2018年7月30日获得由中国信息通信研究院及数据中心联盟颁发的云服务用户数据保护能力资质证明。

美国注册会计师协会（AICPA）SOC审计

SOC审计是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列鉴证报告，金山云现已通过美国注册会计师协会（AICPA）SOC1与SOC2审计，说明金山云的内部控制、云服务体系的安全性、可用性和保密性等均得到了认可。

基础设施安全

金山云始终将为用户提供安全的云服务作为核心目标，在安全技术和服务上持续投入，为保证金山云基础设施安全，在物理、网络、应用、认证机制等方面不断完善，目前金山云在云服务基础架构安全基础上，通过各项制度流程、技术手段进行全方位的安全防护。

物理与环境安全

机房的物理和环境安全直接影响到业务的可用性，金山云为机房的物理和环境安全建立了完善的标准和规范，主要从访问控制、巡检规范、故障处理等方面为机房的安全做基线。 机房的访问有严格的控制流程，进入金山云机房的人员可分为四大类，金山云运维人员、外包运维人员，厂家维修人员、参观人员，每一类角色都有专有的访问和审批流程。现场运维人员对需进入IDC 机房的人员进行入室登记并保存半年，以便按需进行审计。同时对于机房的核心机柜，金山云有机柜安全管理要求，包括核心机柜安全使用要求、机柜开通关闭管理流程等，对核心机柜的操作有详细登记信息并保存半年以上。 为了保证机房的稳定运行，金山云对机房进行例行巡检，主要包括机房环境巡检和机房服务器故障巡检。环机房境巡检7*24小时机房每天定点进行3次，*8小时机房每天定点进行2次，巡检机房的用电、温度、湿度是否在规定范围内，每次巡检都有巡检结论报告，并告知到相关部门。机器故障巡检7*24小时机房每天定点进行3次，*8小时机房每天定点进行2次，巡检内容包括服务器指示灯、液晶显示面板、报警声音等，所有巡检内容记录到巡检表做备案和审计。一旦有故障，严格执行应急响应流程，在规定时间和范围内通报发现的问题并做事故恢复。事故恢复有标准的故障处理流程，其中包括故障硬盘报废流程、故障内存操作规范、SSD及Flash卡操作规范、故障电源操作规范、设备连通性操作规范、多厂家备机替换操作规范等。运维人员严格按照规范操作，确保机房的稳定和安全。除了上述基线，金山云还有规范的服务器到货标准、机房设备签收和发送标准等。

网络安全

为了避免风险扩散，金山云基础架构中严格隔离办公网和IDC网络。同时通过在边界设备部署访问控制策略严格隔离IDC网络和租户网络，实现overlay网络与underlay网络的彻底隔离。 为了帮助用户构建完全逻辑隔离的、可自主掌控的专有区域，金山云提供基于VXLAN隔离的专有网络VPC（Virtual Private Cloud，虚拟私有网络）。虚拟私有网络是天然隔离的网络环境，通过网络ACL和安全组分别从子网和服务器维度控制网络访问，可以精确到协议和端口级粒度，同时VPC提供稳定可靠的IPsec VPN/专线连接虚拟私有网络至用户的数据中心，多维度、全方位满足网络安全的需求。

API与应用安全

金山云有专业的安全测试团队会定期对金山云所有业务进行安全测试；首先，以白盒的方式对金山云所有的API与应用进行安全测试，来发现自身业务的脆弱点；另一方面也会以黑客的视角对其进行黑盒渗透测试，模拟外界攻击者来发现金山云的安全漏洞，两者相结合来保障金山云业务API与应用系统的安全。除此之外，金山云建立了安全应急响应中心，吸纳众多外界优秀的安全测试人员为金山云的安全添砖加瓦，共同建设金山云安全。

访问控制

为了保证金山云自身和用户信息的安全性，金山云有严格的认证机制和授权机制，确保信息的访问和使用符合安全策略，同时金山云有专门的审计团队对认证和授权机制进行审核，确保安全策略的顺利执行。

认证机制

金山云内部，每一位员工都有专属的员工账号，员工通过自己的账号访问公司网络，同时金山云强制员工定期更换密码并且严格规定密码长度和复杂度。在此基础上，员工访问IDC等公司内部信息需要通过双因子认证，确保公司内部信息的安全性和可审计。员工离职时，系统将回收员工权限，禁止该账号访问金山云网络。

授权机制

授权作为访问控制的重要一环，直接关系到自身及用户数据与业务的安全性。金山云内部，依据工作职责，按照最小权限原则，系统对员工账号进行分配和回收。按照岗位和职级进行授权控制，比如网络、主机、存储等核心业务的操作权，严格按照最小化原则以及职责分离进行授权，未授权员工没有权限进行访问。 外部用户只能访问自己申请的资源，用户之间的资源被严格隔离，同时在未经用户允许的情况下，金山云所有员工都没有权限访问用户资源。 对于公司的机密数据，金山云内部有完善的授权申请流程和审批流程，并定期进行流程的审计，确保数据授权的合理性和正确性。

访问控制审计

为了保障金山云客户账号的安全性，降低暴力破解的威胁，金山云内部有基于大数据分析的登录日志审计系统，可以自动识别被暴力破解账号，保障客户利益。 为了保证基础架构操作的安全性，所有访问IDC的记录均需通过堡垒机进行双因素认证和审计。除此之外，金山云规定各子系统保存操作日志不少于六个月，以满足必要的审计需求。

面向用户的安全产品

防DDoS攻击

DDoS攻击，即分布式拒绝服务攻击，将多个主机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力，其攻击范围非常广泛，涵盖各行各业。 金山云免费为用户提供最高5G的默认DDoS防护能力。在此基础上，金山云针对用户遭受大流量DDoS攻击的情况，提供高防IP产品，金山云高防IP具有充足的带宽储备，可提供Tb级DDoS攻击防护。完善的DDoS攻击检测、防御机制，可以为用户提供完整的4-7层攻击防御，包括TCP flood, UDP flood, 反射放大攻击，应用层CC攻击等常见攻击类型。在性能方面，金山云提供高性能设备进行秒级检测和清洗，同时有极高的检测准确率。防攻击服务每天为用户抵御近万次攻击，有效地保护了用户的业务连续性。金山云内部有全流量镜像以及攻击检测、报警机制，可以实时发现异常流量，进行报警、分析和清洗。

Web应用防火墙

金山云为用户提供Web应用防火墙以应对OWASP常见的Web威胁防护，保障用户网站的安全，该产品可防御常见的OWASP常见威胁、进行0day补丁定期及时的更新，帮助用户能够及时更新漏洞补丁，对网站进行安全防护；Web应用防火墙还具有精准访问控制、CC恶意攻击防护以及高级Web攻击防护的功能，提供强大的精准访问控制策略，可轻松识别可信与恶意流量，对指定地点进行一键黑名单封禁，阻断所有来自指定地区的访问请求。

入侵检测和防御

金山云为租户提供服务器安全产品，该产品可检测并拦截系统弱口令、数据库弱口令、webshell、暴力破解、木马防护、服务器漏洞、病毒检测、CC攻击防护等，帮助租户全方位检测和拦截各类攻击行为；并通过本地客户端和云端服务器的联动，实时同步最新安全数据，让租户及时知晓服务器的安全状态。

密钥管理服务

金山云为用户提供安全易用的管理类服务。让用户无需花费大量成本来保护密钥的保密性、完整性和可用性，借助密钥管理服务，可以安全、便捷的使用密钥，专注于开发需要的加解密功能场景。用户可自行根据业务的发展动态调整创建的密钥个数，金山云为用户提供每月2万次的免费API调用。

脆弱性扫描

金山云为用户提供漏洞扫描服务，主要针对服务器及Web服务进行漏洞扫描，包括Web通用漏洞扫描、端口安全检测、第三方应用漏洞检测等功能。用户可自行选择金山云漏洞扫描服务来保障业务的安全性，降低系统被入侵的风险。

证书管理

金山云为用户提供证书管理服务，金山云证书管理与全球各大数字证书颁发及代理机构合作，在云平台上签发通过认证的数字证书，帮助用户网站完成HTTPS化并提供数据安全保障，提升数据传输安全等级。

数据安全

金山云围绕着数据的整个生命周期对数据进行全面的建设，金山云数据安全团队通过从访问控制、数据使用审计、数据流转监控、数据加密存储、数据传输安全和数据安全培训教育等方面，针对用户数据进行严格管理。

访问控制IAM

金山云为用户提供身份与访问控制服务IAM（Identity and Access Management），并通过IAM为用户解决因为共享密码带来的潜在的误操作风险或权限过大、资源无法隔离等问题，降低企业的信息安全风险和管理难度。

传输保护

金山云为保护数据在传输过程中不被窃取，针对公网的数据均使用https加密通道传输，同时保证核心数据在公司内网加密传输，可有效防止传输过程中的数据窃取。另外，金山云提供的对象存储产品KS3支持在数据传输过程中使用SSL加密，保证动态传输安全。

存储保护

针对用户数据的存储，金山云提供多种存储方式，比如对象存储（KS3）、关系型数据库（KRDS）、云数据库Redis（KCS）、云数据库MongoDB等，每一种存储方式都有完备的安全方案。 对象存储产品KS3提供EB级数据存储校验和AES256网银级加密，利用公私钥进行签名校验并对数据做多备份来保证数据的安全可靠，并支持通过HTTPS加密通道进行传输的功能。 关系型数据库KRDS是一种稳定可靠、可弹性伸缩的在线数据库服务，具有多重安全防护措施和完善的性能监控体系，并提供专业的数据库备份、恢复及优化方案，使企业能专注于应用开发和业务发展。 云数据库Redis提供即开即用、稳定可靠的在线缓存和键值存储服务，拥有主从双机热备机制，并提供自动容灾切换、实例监控、在线扩容等服务确保产品可靠稳定。 云数据库MongoDB是底层基于三节点副本集，能为客户提供故障切换，容灾迁移，在线备份等一体化的解决方案。云数据库MongoDB可以提供20多种业务监控和告警功能，有助于及时发现数据库在使用中的各种情况结合问题；同时还提供数据库备份和恢复等功能。 各数据存储产品均提供用户级别的数据隔离、访问控制、权限管理，多重保险来保证数据安全。

数据销毁

在用户主动删除数据或服务期满后用户需要销毁数据的，金山云将自动清除对应物理服务器上磁盘和内存数据，使得数据无法恢复。另外，用于存储数据的设备在报废弃置、委托第三方维修或转售前，金山云将采取磁盘低级格式化操作彻底删除用户所有数据，并无法复原，硬盘到期报废时将进行消磁。

隐私保护

金山云非常重视用户的信息安全，为了保障用户隐私数据的安全，金山云一直努力采取各种合理的物理、电子和管理方面的安全措施来保护用户信息。防止用户信息遭到未经授权访问、公开披露、使用、修改、损坏或丢失。金山云使用加密技术提高用户信息的安全性；使用受信赖的保护机制防止用户信息遭到恶意攻击；部署访问控制机制，尽力确保只有授权人员才可访问用户信息；同时金山云会对员工进行数据安全方面的培训教育，以加强员工对保护用户数据的安全意识。 对于用户使用金山云产品进行数据的存储时，金山云将以客户为维度进行相互隔离，在未经合法授权的情况下，其他客户无法访问其存储数据，金山云亦无权利无途径查看用户存储的数据信息。

安全组织

金山云始终将网络安全放在首要位置，组建了一支专业的安全团队来建设金山云的网络安全；金山云安全团队根据公司的整体战略来对金山云的安全建设方向进行规划和管理，保证云服务及云安全业务能够满足安全要求、保障金山云用户的利益。另外，金山云安全团队联合内部多部门成立安全委员会，自上而下的共同推进安全工作，通过安全委员会极大的提高了跨部门协作的效率，有效的控制了安全风险。

运维安全

漏洞管理

金山云拥有一套完善的漏洞管理机制，针对漏洞的响应、定级、处置等不同的环节，均由金山云的威胁情报与应急响应团队进行7*24小时全程跟进处理，以便对漏洞进行及时处理。 在漏洞来源方面，一是金山云自身业务的例行扫描和渗透测试，另一部分是来自外界的通报，金山云与各安全社区保持紧密联系，第一时间获取外界发现的安全漏洞。 除此之外，金山云与各大安全厂商建立良好关系，一旦发现可能危及客户的威胁情报或0DAY漏洞，均会第一时间通过安全公告告知客户，以便客户能够及时应对安全威胁。

安全事件管理

与漏洞管理机制相同，金山云对于安全事件的管理也建立了成熟的流程机制，金山云在获悉事件之后，会第一时间依照《金山云安全事件处理流程》进行追踪、追查和修复。若事件与用户有关，金山云会第一时间通知用户并做修复，同时会出具应对措施防止类似安全事件的再次发生。

业务连续性管理

业务连续性是衡量一个企业应对风险、自动调整和快速反应的能力，以此来保证企业业务的连续运转。云厂商承载着云上业务的运行，业务连续性对云厂商更为重要，金山云的业务连续性机制通过完整的业务连续性计划和定期演练以及数据的异地备份存储，保证业务的高可用、连续操作和灾难恢复的能力。

数据异地备份

金山云有若干个Region，分布在不同地理位置，目的是单个区域发生不可控事件比如自然灾害、运营商故障、网络攻击等问题时可以保证业务持续运行。云服务负载的用户数据全部在多个Region存储，互为备份，同时每个Region的存储机制都有实时报警功能，确保第一时间发现问题。多Region的存储和备份可以从根本上杜绝业务中断。

业务连续性计划

金山云的核心业务，比如云主机、云存储、网络等，都有成熟的业务连续性管理计划，针对每一类业务中断原因包括自然灾害、运营商故障、网络安全事故、硬件故障、误操作等方面，核心业务都有针对性的业务连续性方案，方案中从事件发生的RTO、RPO、业务中断影响、业务恢复方案、业务恢复流程、业务备份方案等方面建立全面的应对机制。确保关键业务在中断或失败后能够在要求的时间内做到信息的可用性和正确性。

演练和培训

金山云核心业务线有《业务连续性管理计划》和《业务连续性分析报告》并定期更新和审计，同时金山云定期对业务连续性方案进行演练，演练结果进行记录和通报，保证连续性计划的有效落地。 演练的同时，为了提高员工安全意识，金山云定期进行安全意识普及和信息安全培训。通过一系列安全教育，员工可获得全面的安全知识，从根本上降低企业业务中断风险，提高公司整体安全水平。

业务安全管理

只通过技术手段来保障金山云的安全是不现实的，需要加入必要的管理手段才能够更全面、深入的保障金山云的安全性，为此，金山云建立了一套完整的业务安全管理体系，同时也在不停的完善自身的制度与流程，尽可能的覆盖到每一种安全问题，让其都有对应的处理流程及管理手段，以规避安全风险；另一方面，金山云也在不断提高对业务的安全要求，以应对安全威胁越来越多的网络环境，保障金山云自身及产品、用户数据信息的安全。

云安全工程能力

安全设计

由于系统的安全问题很大一部分是由于不安全的设计引入的，所以金山云在系统投入开发之前就按照安全设计的核心原则进行评估，结合业务自身情况从不同层面、不同角度的对系统的攻击面、权限、基本隐私等方面进行分析，避免将不安全的设计带入开发过程中。

安全编码

在系统开发过程中，金山云严格遵守安全开发生命周期管理流程。在开发阶段，安全人员给出各类编程语言的安全编码规范，避免项目中出现不安全的代码；在测试和审计阶段，安全人员会给出安全测试点并人工审核代码漏洞，避免将漏洞带到线上；系统发布时，安全人员会给出整体安全评估结论，由安全部门、研发部门和运维部门一同讨论决定是否发布。

变更控制

对线上服务的稳定性、可用性、安全性造成已知或潜在影响的操作，均属于线上变更范围。金山云严格控制变更操作，防止由于变更操作影响服务的稳定，金山云将变更控制分为两类，一类是对上层用户无感知、对用户透明的升级，另一类是对服务可用性、稳定性和安全性有影响的操作，即用户感知或影响SLA的操作。金山云对这两类操作分别有不同的管控流程，变更操作遵守灰度发布上线，以确保服务的稳定和安全。