阿里云数据安全

白皮书

目录
Contents

01 概要

近年来，云计算在全球各行各业得到越来越广泛的应用，但是存放于云上数据的安全性仍然是用户担忧的核心问题之一。为此，阿里云对用户关心的云上数据安全问题进行了深入剖析，通过完善的数据安全管理和先进的技术支撑实现对用户数据安全的承诺，以增强用户对使用云服务的数据安全信心：

安全和可靠：

凭借阿里云丰富的安全实践和行业合规经验、完善的内部控制和云产品中丰富的数据安全功能，用户可轻松获得世界级的可靠性、安全性和合规性。

透明与信赖：

用户可清晰地了解其云上数据的传输、使用、存储、销毁机制，
并通过权威的认证和审计报告充分掌握阿里云的数据安全控制状况。

创新及分享：

阿里云通过不断的技术创新和云安全生态环境，努力为客户提供前沿的数据安全解决方案。

阿里云的行业领先经验

2.1 生态的阿里云

阿里云秉承开放资源，相互合作的态度，将阿里云的云计算、大数据和安全的基础能力开放给合作伙伴，实现云服务的多样化和高附加值，共同服务好云服务客户。在安全生态方面，阿里云已引入国内外行业安全合作伙伴，通过云市场提供VPN、下一代防火墙、IPS、UTM、堡垒机、加密、日志审计、数据库审计等安全服务，为云服务客户提供业界领先的、和客户现有IT环境安全控制措施体验一致的安全解决方案。

2.2 创新的阿里云

云计算是助力企业数字化商业（Digital Business）转型的推手，创业公司诞生在云计算平台上，传统企业通过云计算插上互联网的翅膀。全球视频直播，人工智能预测天气，IoT激励工业物联网升级，以前不敢设想的业务都借助云计算成为了现实。

先进生产力的代表——数据成为新的生产资料，通过计算发觉数据背后隐藏的密码，大规模协同缩短产品市场化时间。企业采用云计算做到集约化、精细化、生态化和全球化发展。

计算无边界——打破传统计算的模式、时间和组织的边界，瞬时开通/释放海量计算能力，让数字成为企业的信仰。 拓展商业边界——云计算平台不仅汇集了产品、服务，也是人才、智慧的聚集地。新产品层出不穷，新组合创造新消费市场。基于深度学习的精准天气预报，改变了人们出行方式，也改变了企业库存和销售行为。

2.3 安全的阿里云

阿里云最近开展的云计算调研显示，近九成的用户在评估云计算服务时，首要看重云计算服务对公司商誉及业务开展的影响，重点关注云计算服务商的内部控制能力与黑客防御能力。中小企业的首要需求是高可用性，而行业客户非常关心安全性，尤其是数据安全与合规性：

- 互联网行业 — 能否保持云上业务的稳定可用 、安全可靠；能否有效应对大流量DDoS攻击。
- 金融行业 — 数据是否会被非授权访问，是否会丢失。
- 政府机构 — 是否拥有国家认可的安全资质。

> “服务可以外包，风险不能外包，责任更不能外包。真正的安全不只是安全平台，
> 更重要的是企业使用安全平台的人”
>
> ——北京市海淀区经信办主任何建吾

02

阿里云的行业领先经验

事实上，阿里云在技术架构设计之初就同步考虑了安全因素，不仅将安全的基因融入到整个云平台和各个云服务中，更开发了一系列特有的云安全服务为云用户的数据安全保驾护航。

据统计，2015年，阿里云保护了全国30%的网站；阿里云安全团队共监控到DDoS攻击事件超过17万次，其中流量达到300Gbps以上的攻击次数超过100次，最大攻击峰值流量达到477Gbps。

阿里云安全大事记

2015年

云安全生态发布、云盾商业化、
访问控制（RAM）云加密服务

2014年

抵御全球最大DDoS攻击453.8G

2013年

ODPS安全设计、全球首个CSA－STAR金牌

2012年

ISO27001国际认证

2009年

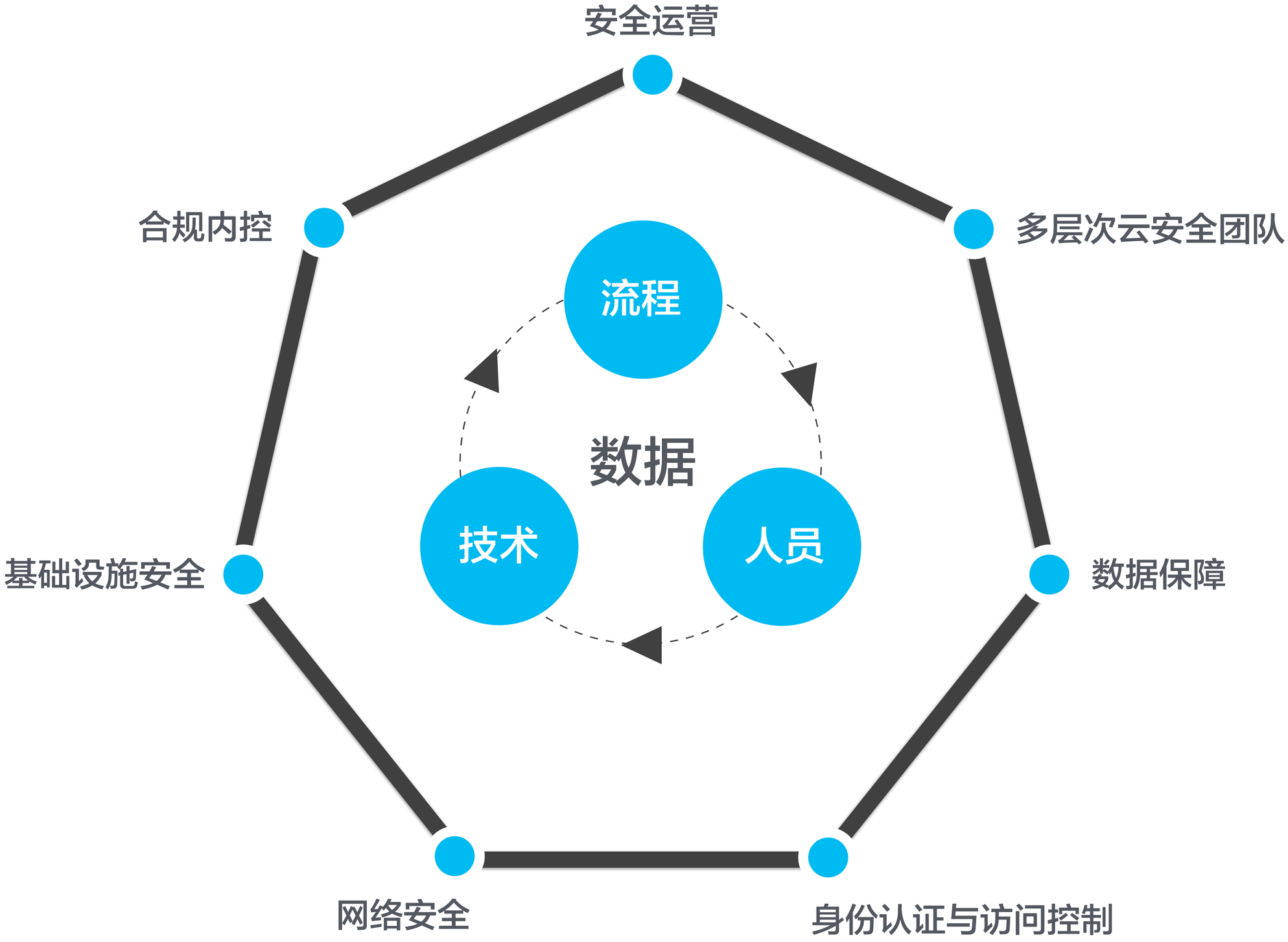
阿里云云安全团队成立、飞天安全设计

阿里云的每个用户都可以站在阿里云的肩膀上，充分享受阿里云丰富的安全经验和合规成果。阿里云更通过其掌握的云计算核心技术，结合先进的人工智能科技，配合行业专家经验，从人员文化、流程管理、技术发展三个层面打造出线上线下融合的云计算数据安全体系，努力消除用户对数据安全的疑问：

- 我的数据在云上是否安全?
- 有谁在觊觎我的数据?
- 出事了，我该做什么?
- 云服务商的数据保护机制有没有漏洞?
- 那些人想对我的数据做什么?

阿里云的行业领先经验

阿里云建立了完整的数据安全保护体系(如下图所示)，帮助用户解答上述疑问。



03 阿里云数据安全实践

阿里云乐于分享行业领先知识，积极参与云计算和大数据国际、国家标准、行业标准的编制。并在多个国际标准组织内担任重要席位，以标准为抓手推动产业健康发展。

3.1 阿里云的数据安全理念

阿里云以行业领先的安全技术为基础，国内外适用的标准为依据，履行对用户的安全承诺，包括在需求设计、开发过程中融入安全需求；使用自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控，使用监控信息设置关键运营指标，并将数据安全及合规的概念融入运营机制中。

3.1.1 确保持续安全运营

在安全运营方面，阿里云提出了“**1+3**”的概念，即通过“安全融入设计、自动化监控与响应、红蓝对抗与持续改进”这3个安全手段，实现“保障用户数据安全”这1个核心目标。阿里云凭着“**1+3**”的强力运营管控，检测出逼近100%的内部漏洞与风险，追踪控制能力更是完全覆盖所有云服务。

“英特尔和阿里云的合作从2009年就已经展开，我们在计算、存储和网络等各方面都展开了深度合作。”
——Intel

“如果没有云计算，企业要花费几年时间，才能把基础设施搭建好，最终错过发展的机遇”
----空格ceo唐永波

•安全融入设计

阿里云充分考虑合规与安全风险，建立自动化、一体化的产品安全开发生命周期，丰富的安全实践和行业合规经验积累而成的阿里云基础安全开发包库，将“数据安全”要求具体嵌入产品开发生命周期的各个环节，每位负责设计开发的人员必须通过安全认证考核方可持证上岗执行编码工作，降低云产品在技术、流程、合规上的安全风险。

•自动化监控与响应

通过自动化的设计、开发、运维、监控、响应的能力，和基于大数据的自动化分析能力，不但具备完善的安全监控响应体系，还利用社会化漏洞举报平台、自建漏洞受理平台为核心，获取外部的安全情报。对各云服务的安全漏洞及威胁情报达到100%监控响应。通过不间断的内部安全攻防来验证监控及响应体系的完备性，让各安全环节不因人为失误而出错，使应急响应化被动为主动，帮助用户防范于未然。

- **红蓝对抗与持续改进**

阿里云云安全团队，邀请全球顶尖的安全专家持续实施攻防对抗，将攻防结果与生产环境中所遭受的威胁相结合，通过攻防对抗及监控响应后的不断跟进与取证分析，来发现和推动产品的漏洞修复、功能改进、架构调整。

3.1.2 多层次的云安全团队

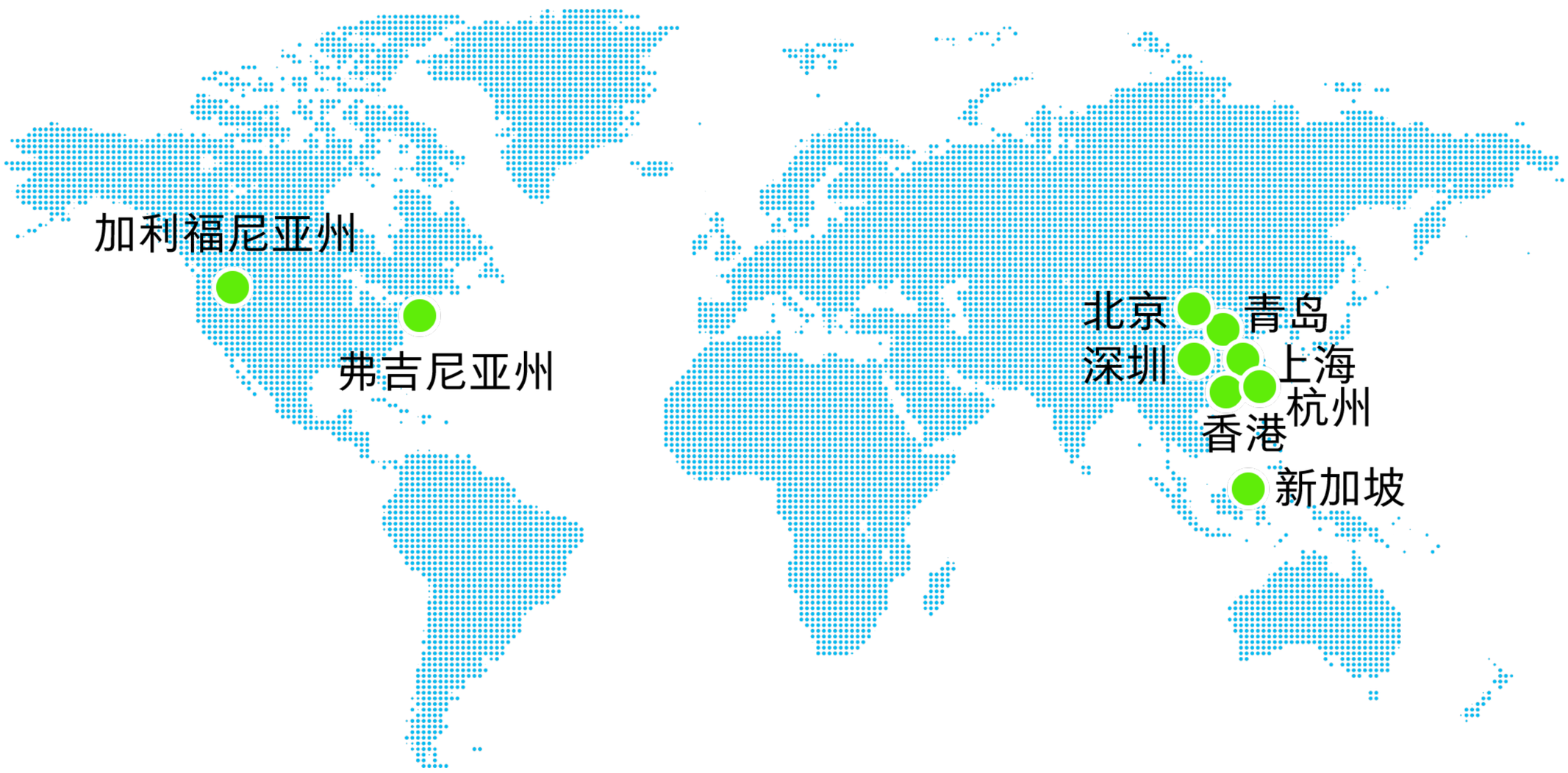
阿里云创建了云底层安全团队、云平台安全团队、合规内控及标准团队，保障用户的数据安全并协助用户满足企业运营的合规目标。

3.2 数据保障

阿里云的客户对于自身的数据，具有完全的知情权和控制权。

为保障每一位客户的权益，阿里云将数据安全保护设为默认优先选择；以明确目标、收集最小化、数据最少化、利用/保留/揭露最低程度等国际通行四大原则为基准，让数据安全不因易用而牺牲安全。

客户可以自行选择其生产数据部署或存放的云服务地域（Region），未经客户授权，阿里云不会任意移动其生产数据的存储地域（Region）。



3.2.1 数据传输

对于数据的交换、转移与分享，阿里云提供标准的加密传输协议，以方便云平台与外界以及系统间传输敏感数据的需求。

阿里云提供了向外与互联网通信的HTTPS加密通道，其中管理控制台以及OpenAPI网关均支持HTTPS数据加密传输协议，采用SSL/TLS协议，可提供高达256位密钥的加密强度。且阿里云为全站HTTPS，任何于云平台内的数据传输皆受256位密钥加密强度的保护，完全满足敏感数据加密传输需求。

3.2.2 数据存储

加密是技术实施上对于数据安全最有效的关卡，阿里云加密服务为客户提供符合国家商用密码管理要求的加密服务，客户可轻松构建符合商密要求的安全应用；阿里云密钥管理服务（KMS）让客户能在密钥生成、存储、使用、管理上，享有无比安全又便捷的体验。在数据到达云平台，并准备写入云数据库(RDS)时，阿里云提供透明数据加密（TDE）的能力，做到写入加密、读出解密的安全机制。阿里云的分布式文件系统采用多副本技术保证用户数据的可靠性。

3.2.3 数据使用

阿里云访问控制服务(RAM)进行第一道把关；在成功访问后，可提供证书服务来加强用户在数据使用时的安全性，使用户数据的使用得到更多自由度；阿里云在平台上直接提供服务器数字证书，客户获取所需类型的数字证书后一键部署在阿里云产品，以最小成本将所提供服务从HTTP转换成HTTPS，实现高强度双向加密传输，防止传输数据被泄露或篡改。

> “包括阿里的内部员工，都无法获取我们的数据。”
>
> ——国华人寿信息技术部总经理

3.2.4 数据销毁

当客户删除数据或离开云服务时，阿里云将遵循严格的数据销毁标准，并物理销毁已废弃的硬件。

3.3 身份认证与访问控制

有效的身份认证与访问控制是确保客户数据不被非授权访问的关键。阿里云向客户提供了身份管理与访问控制服务(RAM)；而对于自身，除员工身份识别机制外，更基于内控要求也打造了领先行业的权限管理平台(ACL)。

3.3.1 对客户提供的安全服务

阿里云云安全团队，邀请全球顶尖的安全专家持续实施攻防对抗，将攻防结果与生产环境中所遭受的威胁相结合，通过攻防对抗及监控响应后的不断跟进与取证分析，来发现和推动产品的漏洞修复、功能改进、架构调整。

•身份识别服务

阿里云身份识别采用两套解决方案，包括Access Key (Access Key ID + Access Key Secret)与多因素认证(MFA)；阿里云也使用反欺诈技术，实时检测和防控可能的恶意登录、暴力破解、撞库等攻击。

> 阿里云相信：云安全的价值等同于健康对人的价值。安全是一种能力，更是一种责任，我们全心服务。

•访问控制服务

与验证客户身份搭配的是访问控制服务(RAM)，让客户创建、管理客户账号，并以User(独立身份管理)及Role(与本地身份联结)两种不同的模式执行。RAM设计了细粒度的访问控制，可根据授权需要，精确地允许或拒绝某个客户对特定的资源执行某项具体操作，并帮助客户达成集中式客户身份管理、集中式权限管理、统一访问控制、统一帐单的服务目标。

3.3.2 对云平台的安全保障

•内部身份识别

阿里云对所有开发、维护、客服以及其他可能会接触到阿里云内部系统的员工，进行入职背景调查及入职登记安全手机号码，并连接内控管理系统进行设备绑定；应用上，除了域账号密码及安全手机接收到的验证码，还需对重要关键系统验证动态Token。阿里云运用严密的身份识别机制，确保帐号与生产设备“不会误用”、“不被盗用”、“不能乱用”的三不原则！

•内部访问控制

阿里云内部同时以权限管理平台(ACL)进行系统账户权限的控制与资源分配。尤其在权限管控上，能精确地将所有系统权限对应上职责列表与业务风险，颗粒度达到菜单的功能级和数据级，并能限定授权生效时间。群组与角色的设定会由阿里云内部各相关系统负责团队进行设定，若使用者要使用某系统，需经申请审批流程，并由负责人团队确认该使用者的权限是否依照职能的需求分配，待一切都确认完毕后，才进行权限分配设定。 当员工岗位发生变动，系统将自动回收对应权限。

3.4 网络安全保障

网络安全是保证数据安全传输和交换的基础。在云计算环境下，确保各级网络以及虚拟设备之间的有效隔离是确保客户数据安全的关键控制。同时阿里云平台兼顾负载均衡能力，确保客户数据的可用性。

3.4.1 对客户提供的安全服务

•网络隔离服务

专有网络VPC是阿里云于云服务生产网络中构建出的一个隔离的网络环境，客户可完全掌控自己的虚拟网络，包括选择自有IP地址范围、划分网段、配置路由表和网关等。不同的VPC之间彻底逻辑隔离, 客户可在自己创建的VPC内创建和管理云产品实例。阿里云也提供安全组设置能力。

> 阿里云将多租户的应用和数据进行隔离，就像一间五星级酒店被分割成多个房间，他们之间是相互独立和封闭的，从而确保不同租户互不干扰和数据隔离。
>
> ——阿里云安全资深总监

•安全组与多租户隔离服务

安全组是一个逻辑上的分组，由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通；但也可以授权两个安全组之间互访。安全组是一种虚拟防火墙，具备状态检测包过滤功能，且用于设置单台或多台云服务器的网络访问控制，是重要的网络安全隔离手段，用于在云端划分安全域。

阿里云所有服务都设计了严格的多租户隔离机制，使得共享同一计算、存储和网络基础设施的不同客户之间，无论是CPU、内存，还是存储和网络都默认相互隔离，既看不到对方的数据，也不会相互影响。

•安全解决方案

阿里云秉承开放资源、相互合作的态度，引入行业安全合作伙伴，共建云安全产业链生态，为客户提供业界领先的、和客户现有场内安全控制措施体验一致的安全解决方案。

3.4.2 对云平台的安全保障

•云平台网络隔离

阿里云把对外提供服务的“云服务网络”和支撑云服务的“物理网络”进行安全隔离；通过网络访问控制列表技术确保云服务网络无法访问物理网络。进一步说，阿里云的网络架构区分了生产、办公等几大区，云服务网独立于其他网络，从非生产网络不能直接访问云服务网的任何服务器和网络设备，保障云计算服务的网络安全。

•堡垒机

阿里云在生产网络边界部署了堡垒机，办公网内的运维人员只能通过堡垒机进入生产网进行运维管理。运维人员登录堡垒机时使用域账号密码加动态口令方式进行双因素认证。堡垒机使用高强度加密算法保障运维通道数据传输的机密性和完整性。

•远程运维

阿里云也为不在公司的员工提供了远程运维通道。运维人员预先申请VPN接入公司办公网之后访问堡垒机的权限。VPN拨入公司办公网络的接入区时使用域账号密码加动态口令方式进行双因素认证。再从办公网接入区访问堡垒机。VPN使用高强度加密算法保障运维通道数据传输的机密性和完整性。

•云平台DDoS防护

阿里云使用自主研发的DDoS防护系统保护所有数据中心，自动检测、调度和清洗，从遭受攻击到开始清洗响应时间不超过5秒，保证云平台网络稳定。

3.5 基础设施保障

基础设施的安全是数据安全的基石。阿里云为客户提供全球部署、多地域多可用区的云数据中心；采用多线BGP网络提高网络访问体验；分布式云操作系统为所有云产品提供高可用基础架构和多副本数据冗余；全球领先的热升级技术使得产品升级、漏洞修复都不会影响客户业务；高度自动化的运维及安全，为客户提供高可用、安全、可信的云计算基础设施。

3.5.1 对客户提供的安全服务

•实时监控与漏洞扫描修补

提供给云服务客户实时全景安全监控与漏洞管理服务，对主机漏洞，甚至是配置项漏洞也能做到实时监控和发现，支持实时回扫，缩短漏洞修复周期，减少漏洞解决时间。同时提供补丁管理能力，让客户一键批量修复高危漏洞。定期的内外部渗透测试，持续改进阿里云在基础建设、平台、软件整体上的安全能力。同样的，阿里云也将此经验化做服务，让云服务客户能对其应用进行渗透测试。

•黑客/恶意软件威胁保护

提供给云服务客户专属的威胁态势感知服务，搭配多种告警方式，结合反欺诈模块及主机入侵防护，能主动侦测欺诈威胁、识别恶意病毒、防恶意登录、实时对登入环节存在的暴力破解及撞库等风险进行检测，也能实时检测支付、转帐等环节存在的异常情况，进一步防止相关风险，确保能够即时预警威胁的发生，让云服务客户提前防范可能遭受的威胁，确保客户数据不被窃取。

> 云盾作为新一代安全解决方案，通过阿里云的大数据计算能力，不仅能抵挡攻击，更能全网态势感知，控制风险，能够真正帮客户应付黑客威胁。

•分布式拒绝服务(DDoS)防护

提供云服务客户实时的全面安全监控服务，做到动态防御，并能通过配置高防IP，将攻击流量引流到高防IP，阻挡过最大攻击峰值流量477Gbps的世界级攻击，确保云服务客户源站的稳定可靠。

•日志与审计

阿里云提供面向云服务客户的操作审计自助服务，所有日志均长期保存，定期复核，并可将日志保存至指定的存储空间；云服务客户可以自行实现安全分析、资源变更追踪以及合规性审计。

3.5.2 对云平台的安全保障

•实时监控与防护

在阿里云的安全运营机制下，实现近于100%的内部漏洞扫描、修补、风险追踪能力，也几乎断绝外来威胁的入侵途径。

•安全威胁大数据检测

云平台利用自身强大的实时监控能力，搭配黑客情报、反欺诈模块，以及云平台的态势感知和分析预测模型，有效阻绝接近所有的黑客入侵，以及恶意软件植入问题。

•分布式拒绝服务(DDoS)防护

阿里云安全团队每日监控到针对云服务自身及云服务应用程序编程接口（API）DDoS攻击事件数以千计，平台会自动检测、调度和清洗，成功防御所有的DDoS攻击。

•云平台日志及审计

阿里云生产环境的所有运维操作只能通过堡垒机进行，所有操作过程完整记录下来实时传输到集中日志平台，通过阿里云违规事项审计规则，主动发现异常或违规行为。

•IDC运维

阿里云与行业内的领先数据中心合作，通过严谨的物理防护以及定期的审计，保证业务不受非法的内部漏洞与外部威胁干扰。

3.6 阿里云的安全合规经验

为了达成“企业数据不丢失、业务发展不损失”的“两不”目标，阿里云运行着一支管理安全、合规与内控的专家团队。此专家团队已帮助阿里云在合规认证领域上，取得了诸多“第一”，还将独立第三方认证和审计机构持续进行的常规认证和审计结果与用户共享，以帮助用户履行自己的合规职责。

阿里云除了向用户提供安全、合规的云计算服务体验，同时与用户积极分享阿里云的合规实践，协助用户达成其所在行业的特定安全合规需求。

阿里云拥有自主构建的合规内控体系和标准，实现对内部控制要求的标准化、控制方案的产品化，并正逐步实现系统化、无人工干预的内控证据发现机制。此外内控团队借助可疑行为数据模型早期发现可能的数据安全隐患点，第一时间预警和干预数据安全违规行为。

什么是SOC鉴证报告

SOC鉴证报告是由美国注册会计师协会制定的专门针对外包服务组织的系统和内部控制情况，经由会计师严格审计后出具的鉴证报告，可以向用户充分证明外包服务组织的内部控制设计合理性和执行有效性。

SOC1报告针对外包服务组织与用户财务报告相关的系统和内部控制情况；

SOC2报告针对外包服务组织系统的安全性、数据保密性、处理完整性、系统可用性和隐私保护。

2012.07
阿里云通过ISO 27001认证

2012.09
阿里云信息系统通过信息安全等级保护三级测评

2013.05
阿里云获得全球首张云安全国际认证金牌

2013.07
阿里云获得首批工信部数据中心联盟组织的可信云服务认证

2016.03
阿里云成为国内首个通过新版ISO 20000认证的云服务商

2016.04
阿里云成为bsi全球首个通过ISO 22301认证的云服务商

2016.04
阿里金融云通过服务组织控制（SOC）独立审计

2016.05
阿里云产品通过CNAS云计算国家标准测试

2016.06
阿里云通过支付卡行业数据安全标准（PCI－DSS）认证

2016.06
阿里云通过新加坡国家标准MTCS T3级认证

04 结语

阿里云致力于打造公共、开放、安全的云计算服务平台，竭诚为客户提供稳定、可靠、安全、合规、透明、公开、对等的云计算基础服务。在提供云服务过程中，阿里云始终捍卫用户的数据安全，帮助用户保护其系统及数据的安全，提升用户数据的可用性、保密性和完整性。

05 阿里云安全合规沟通资源

阿里云用户可以随时通过如下渠道，获取和了解阿里云关于数据安全的最新消息：

1、阿里云信任中心-合规性

详细介绍阿里云通过的合规及标准，参照的最佳实践

https://security.aliyun.com/rule.html

2、阿里云业务安全中心

获取国家制定的互联网相关法律及规定、阿里云云服务客户需要遵守的平台规则，以及阿里云的举报平台，包括“违法和不良信息举报”、“知识产权侵犯举报”、“欺诈、钓鱼举报”、“恶意行为举报”和“其他举报”。阿里云邀您一起关注云平台的健康发展，保障云环境，共建云生态。

https://report.aliyun.com/

3、阿里云信任中心-安全产品与服务

获取阿里云为客户提供的保护云端系统及数据的技术手段，包括云产品的安全功能、云盾安全服务和安全生态中第三方安全厂商提供的安全产品

https://security.aliyun.com/service.html

4、阿里云信任中心-数据安全

概要地介绍阿里云基于国内外以及行业的信息安全标准和最佳实践要求建立的数据安全体系

https://security.aliyun.com/data.html

5、阿里云信任中心-基础设施安全

概要地介绍阿里云云底层架构信息

https://security.aliyun.com/base.html

6、阿里云安全生态市场

获取阿里云引入的丰富的云安全产品及服务，提供完整安全解决方案

https://market.aliyun.com/security

阿里云安全合规沟通资源

7、客服中心

使用智能客户、提交工单、社区问答，询问相关信息

https://help.aliyun.com/contact/contact.htm

8、帮助中心

使用帮助中心搜索相关文档

https://help.aliyun.com/?spm=5176.7618386.201511181.1.p2OmhD

9、电话咨询

致电客服询问相关信息

售前咨询 95187转1　　售后咨询 95187　　备案咨询 95187转3

10、阿里云官方微博

关注官方微博获取最新信息

“阿里云安全”http://weibo.com/678750615

11、阿里云官方论坛

阿里云官方的云安全论坛

http://bbs.aliyun.com/thread/215.html

12、阿里云官方博客

关注官方博客获取最新信息

https://yq.aliyun.com/articles

其他有关详细信息，请参照阿里云官网及相关白皮书。

为了无法计算的价值

MORE THAN JUST CLOUD