阿里云安全白皮书 V1.2

前言

阿里云以打造互联网数据分享第一平台为使命，借助自主创新的大规模分布式存储和计算等核心云计算技术，为各行业、小企业、个人和开发者提供云计算（包括云服务器、开放存储服务、关系型数据库、开放数据处理服务、开放结构化数据服务、云盾、云监控等其他产品）产品及服务，这种随时、随地、随需的高效云产品和服务同时具备安全方面的优势。

阿里云提供这些云产品及服务的方式来自于阿里巴巴集团在电子商务行业的多年浸渍，而安全则是阿里云的首要和关键组件。本白皮书将介绍阿里云在云安全方面的方法，具体涵盖安全策略、组织安全、合规安全、数据安全、访问控制、人员安全、物理安全、基础设施安全、系统和软件开发及维护、灾难恢复及业务连续性十个方面的主题。在本文里面所描述的策略、流程和技术将以 www.aliyun.com 发布时为准。随着时间的推移，部分细节将随着产品和服务的创新而改变。

概览

阿里云遵循“生产数据不出生产集群”的安全策略，覆盖从数据存储、数据访问、数据传输到数据销毁等多个环节的数据安全控制要求，这些控制要求包含以下十个方面：

（1） 阿里云安全策略解读；
（2） 组织安全；
（3） 合规安全；
（4） 数据安全；
（5） 访问控制；
（6） 人员安全；
（7） 物理安全；
（8） 基础安全；
（9） 系统和软件开发及维护；
（10）灾难恢复及业务连续性

阿里云安全策略解读

“生产数据不出生产集群”------阿里云基于阿里巴巴集团十多年信息安全风险管控经验，以保护数据的保密性、完整性、可用性为目标，制定防范数据泄露、篡改、丢失等安全威胁的控制要求，根据不同类别数据的安全级别（例如：生产数据是指安全级别最高的数据类型，其类别主要包括用户数据、业务数据、系统数据等），设计、执行、复查、改进各项云计算环境下的安全管理和技术控制措施。

组织安全

阿里云安全团队由信息安全、安全审计、物理安全 3 个团队组成，阿里云通过这些团队高效、协同的工作来给广大用户、中小网站站长和开发者打造安全的云计算环境。

2.1 信息安全团队

阿里云全职信息安全团队由超过 50 名的 WEB 应用安全、系统和网络安全、安全开发专家组成。这个团队负责设计、开发和运营基于阿里云云计算环境的云安全服务（云盾）；防御各类对阿里云服务、系统和网络的安全攻击及入侵；制定和监督云服务的安全开发流程。同时作为阿里云信息安全管理体系所有者代表方在安全策略和流程方面的设计、归档和执行中扮演重要角色。

（1） 设计、开发和运营采用云计算架构和技术的云安全服务（云盾），对使用阿里云云服务的各类网站和应用，提供全自动防攻击和入侵的安全服务，例如防 DDoS、防入侵、以及网站安全检测；
（2） 依据不同数据类别及其安全等级设计访问控制策略，制定技术隔离措施和访问控制管理流程；
（3） 依据代码、应用、系统、网络访问流程，审核访问申请，自动化监控可疑活动（例如：数据的非授权访问及修改）并实时审计；定期复查其执行情况；
（4） 制定安全开发流程，并依据数据安全级别界定所有云服务的各环节安全开发要求，通过配置管理系统保证各开发环节遵循其对应的安全要求，并在上线前完成安全加固、通过安全审核；
（5） 借助自动化运行在阿里云网络内部和外部的漏洞扫描程序，及时发现问题区域，并在预期的时间表内整治安全漏洞。
（6） 遵循信息安全事件管理标准要求，依据对数据安全性的危害程度定义安全事件类别和响应流程，采用全天候系统和人工监控识别、分析和处理信息安全事件；
（7） 基于预防和纠正云安全威胁根本成因来制定所有安全策略和控制措施；
（8） 采用不断演练的方式评估安全策略和控制措施的适用性，并及时更新；
（9） 遵照阿里云安全策略，为员工开发和提供培训课程，包括个人信息保护、数据安全认证和安全开发领域；
（10）通过第三方安全论坛接受外部安全专家的安全评估和建议；

信息安全团队也积极参与阿里云之外的安全团体工作：

（1） 举办和参与学术峰会（例如：阿里云开发者大会、云安全国际联盟亚太和中国区峰会）；
（2） 参与云安全国际标准的试点工作（例如：由英国标准协会和云安全国际联盟推出的 OCF 认证框架）；
（3） 面向广大互联网门户网站、安全厂商、浏览器共享基础安全防护信息（例如：以下厂商使用云盾的反钓鱼技术提升自身钓鱼侦测能力。腾

讯、新浪、奇虎 360、金山、趋势科技、遨游、微软（IE）、谷歌（Chrome）、苹果（Safari）、firefox、搜狗）；

（4） 与顶尖高校合作开发云安全技术(例如清华、南大等)；

2.2 安全审计团队

安全审计团队是阿里云另外的一个全职安全团队，阿里云维护多个国际、国内安全体系及标准的有效性，通过审核和审计以满足合规性要求，如 GB/T 22080-2008/ISO/IEC 27001:2005、《信息系统安全等级保护基本要求》、云安全国际认证 CSA-STAR。

2.3 物理安全团队

物理安全团队是设立在杭州，面向全国的一个员工团队，致力于保护阿里云遍布全国的数据中心物理安全及云计算业务基础设施的高安全性。

合规安全

3.1 第三方认证：

ISO27001：阿里云已取得 ISO27001 国际认证，我们的信息安全管理体系（ISMS）涵盖云计算基础设施、数据中心和云服务，包括弹性计算、RDS（关系型数据库服务）、ODPS（开放数据处理服务）、OSS（开放存储服务）、OTS（开放结构化数据服务）、云盾（云安全服务）以及云监控服务。ISO 27001 是一项被广泛采用的全球安全标准，采用以风险管理为核心的方法来管理公司和客户信息，并通过定期评估风险和控制措施的有效性来保证体系的持续运行。为了获得认证，公司必须表明它有一个系统的和持续的方法来管理信息安全风险，保障公司及客户信息的保密性，完整性和可用性。该认证的取得不但验证了阿里云云端技术框架、内部管理矩阵同国际信息安全最佳实践的符合性，同时也是对阿里云云产品和服务从设计到交付的透明度、云安全服务的自动化运营服务模式的肯定。

云安全国际认证（CSA-STAR）：阿里云已获得全球首张云安全国际认证金牌（CSA-STAR），这是英国标准协会（简称 bsi）向全球云服务商颁发的首张金牌。这也是中国企业在信息化、云计算领域安全合规方面第一次取得世界领先成绩。云安全国际认证（CSA-STAR）是一项全新而有针对性的国际专业认证项目，旨在应对与云安全相关的特定问题。其以 ISO/IEC 27001 认证为基础，结合云端安全控制矩阵 CCM 的要求，运用 bsi 提供的成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与；策略、计划、流程和系统性方法；技术和能力；所有权、领导力和管理；监督和测量等 5 个维度，综合评估组织云端安全管理和技术能力，最终给出“不合格-铜牌-银牌-金牌”四个级别的独立第三方外审结论。

“阿里云应为此项殊荣而感到骄傲。阿里云在引领中国云计算服务市场的过程中，开创了多种云计算服务提供的模式。”BSI 中国区董事总经理高毅民说，“在云安全评估过程中，我们的专家团队对阿里云云计算服务的能力水平和成熟度进行了充分的验证，在没有不符合缺失的情况下，将金牌授予阿里云。我们也确信市场会对其在安全和隐私领域的贡献给予回报。”

说到金牌认证的严谨性，云安全联盟（CSA）的 CEO Jim Reavis 认为，“我们很高兴，阿里云已经获得了第一个 CSA STAR 全球金牌认证，符合了它严格的安全要求。这个认证，证实了阿里云在安全云计算中的技术领导地位。我非常骄傲，能看到 CSA 安全的最佳实践被阿里云和其他处于领导地位的云供应商越来越多地采用。”

信息安全等级保护：阿里云已通过信息安全等级保护测评，测评涵盖弹性计算、OSS（开放存储服务）、基础网络、云搜索、云地图、云邮箱、云广告、云盾。信息安全等级保护是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

3.2 合规

（1） 阿里云同所有供应商均签署保密协议，并通过定期识别、记录、评审保密协议中数据安全的相关控制要求，（例如：如密、访问控制、防泄漏及完整性要求），防止不正当披露、篡改和破坏数据；
（2） 阿里云根据国家信息安全相关法律、法规要求设置并维护和各信息安全监管机构之间的联络员和联络点。应制定并实施程序，以确保所提供云计算平台、云计算产品、云计算服务符合国家关于知识产权相关法律和法规要求；

数据安全

阿里云管理的数据资产,包括客户和企业自身在安全政策下管理的数据资产。所有阿里云员工在处理数据资产时，必须遵守数据分类原则下的数据处理流程和准则。阿里云的数据分类不同于传统 IT 环境下基于数据密级的分类模式，不但在分类对象方面覆盖数据资产和包含数据的对象，而且在数据类型方面也通过明确定义数据处理权限、管理者的区域、前后关系、法律上的约束条件、合同的上的限定条件、第三方的义务来防止数据未经授权的披露或滥用。

阿里云的云服务运行在一个多租户、分布式的环境，而不是将每个客户的数据隔离到一台机器或一组机器。这个环境是由阿里云自主研发的大规模分布式操作系统“飞天”将成千上万台分布在各个数据中心、拥有相同体系结构的机器连接而成。

4.1 访问与隔离：

阿里云用户用过 https 协议登陆官网注册用户账号来选购云服务，同时阿里云通过 AccessId 和 AccessKey 安全加密对来对云服务用户进行身份验证；阿里云运维工程师对运维生产环境的访问则需经过集中的组和角色管理系统来定义和控制其访问生产服务的权限，每个运维工程师都有自己的唯一身份（EmployeeID），经过数字证书和动态令牌双因素认证后通过 SSH 连接到安全代理后进行操作，所有登陆、操作过程均被实时审计。

阿里云通过安全组实现不同用户间的隔离需求，安全组通过一系列数据链路层、网络层访问控制技术实现对不同用户虚拟化实例的隔离以及对 ARP 攻击和以太网畸形协议访问的隔离。

4.2 存储与销毁：

阿里云的云服务将客户数据存储在“飞天”平台提供的多种存储系统中，“飞天”存储栈支持多种非结构化和结构化数据的存储管理，比如“盘古”分布式文件系统，以及由“盘古”演化出的“有巢”分布式文件系统。从阿里云的云服务到“飞天”存储栈，每一层收到的来自其它模块的访问请求都需要认证和授权。内部服务之间的相互认证是基于 Kerberos 安全协议来实现的，而对内部服务的访问授权是基于 capability 的访问控制机制来实现的。内部服务之间的认证和授权功能由“飞天”平台内置的安全服务来提供的。

拿 ODPS 服务为例，当服务前端(Web Server)收到终端用户的数据处理请求时（比如收到一个 SQL 语句），首先会检查请求者身份和消息请求的真实性，然后通过远程过程调用将请求发送到服务后端。服务后端在处理请求之前，会检查调用者（服务前端）的身份和访问权限。如果检查通过，服务后端会产生一个执行计划，并通过远程过程调用将执行计划发送到“飞天”的作业调度系统。作业调度系统在处理请求之前，会检查调用者（服务后端）的身份和访问权限。检查通过之后，作业就会被调度运行。作业在运行时会通过远程过程调用来访问存储层上的数据，那么存储系统在处理请求之前，依然会检查调用者（作业的运行实例）的身份和访问权限。

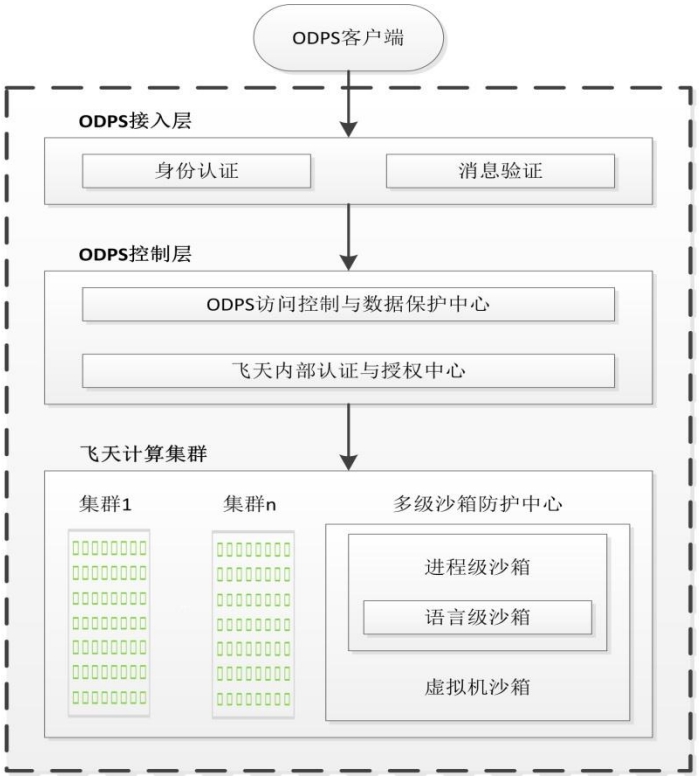

图 1:阿里云 ODPS 数据安全架构图

在上面的例子中，从云服务到“飞天”存储栈，每一层上的访问授权是支持最小权限原则的，每一个访问请求都只会使用刚好满足需要的权限，而不会使用过大的权限。比如，用户提交的 SQL 语句只需要读取某个表，那么相应的作业通过远程过程调用来访问存储层上的数据时，该作业的权限是只能访问该表所对应的数据文件，而不会更多。

阿里云采用碎片化分布式离散存储技术存储用户的结构化和非结构化数据，每一份在云端的数据都会被文件分片(chunk)，每个 chunk 会存三份副本，分布于不同机架上。针对用户云服务期满后的数据销毁问题，阿里云的云服务生产系统会自动消除原有物理服务器上磁盘和内存数据，使得原用户数据无法恢复。对于所有委外维修的物理磁盘均采用消磁操作，消磁过程全程视频监控并长期保留相关记录。阿里云定期审计磁盘擦除记录和视频证据以满足监控合规要求。

访问控制

为了保护阿里云客户和自身的数据资产安全，阿里云采用一系列控制措施，以防止未经授权的访问。

5.1 认证控制

阿里云每位员工拥有唯一的用户账号和证书，这个账号通过有线和无线网络接入用来识别每个人在阿里云网络内的活动情况并作为阻断非法外部连接的依据，而证书则是作为抗抵赖工具用于每位员工接入所有阿里云内部系统的证明。员工入职后，人力资源部会给予一个用户账号，并按照其岗位类别和职级进行授权，离职后，人力资源部将通过系统将禁止该账号访问阿里云网络。

阿里云密码系统强制策略用于员工的密码或密钥（例如登陆工作站）。包括密码定期修改频率、密码长度、密码复杂度、密码过期时间等。阿里云针对生产数据及其附属设施的访问控制除去采用单点登录外，均强制采用双因素认证机制，例如像证书和一次性口令生成器。

5.2 授权控制

访问权限及等级是基于员工工作的功能和角色，最小权限和职责分离是所有系统授权设计基本原则，阿里云员工访问公司的资源只授予有限的默认权限。例如访问邮件和阿里云内部办公系统。如根据特殊的工作职能，员工需要被授予权限访问某些额外的资源，则依据阿里云安全政策规定进行申请和审批，并得到数据或系统所有者、安全管理员或其他部门批准。所有批准的审计记录均记录于工作流平台，平台内的控制权限设置的修改和审批过程的审批政策确保一致。

5.3 审计

阿里云所有信息系统的日志和权限审批记录均采用碎片化分布式离散存储技术进行长期保存，以供审计人员根据需求进行审计。

人员安全

在入职前，阿里云在国家法律法规允许的情况下，通过一系列背景调查手段来确保入职的员工符合公司的行为准则、保密规定、商业道德和信息安全政策，背景调查手段涉及刑事、职业履历和信息安全等方面，背景调查的程度取决于岗位需求。

在入职后，所有的员工必须签署保密协议，确认收到并遵守阿里云的安全政策和保密要求，而在这些安全政策和保密要求中关于客户信息和数据的机密性要求将在每一位新员工入职培训过程中被重点强调。除去针对新员工信息安全课程的培训，阿里云依据员工工作的不同角色进行额外信息安全培训，确保不同角色员工管理的用户数据必须按照安全策略执行。最后，阿里云通过对员工进行企业价值观考核的方式检验每位员工是否以诚信、敬业的态度来管理每位客户的云端数据，保证其对客户、合作伙伴和竞争对手的尊重；

阿里云提供机密报告机制以确保员工可以匿名报告任何违反安全政策、商业道德的事件。

物理和环境安全

7.1 物理安全控制

阿里云数据中心在地理位置上呈分布式状态，涵盖中国本土内的两地三中心布局。对所有数据中心的所有资产设备，物资配件，耗材，人员，均采用了多种不同的物理安全机制。在技术和安全上对人员和设备的控制机制可能取决或遵循于实际运营商的条件，如建筑物的位置和区域风险差异，以及设备和人员进出控制流程等。但阿里云每个数据中心都包含以下标准的物理安全控制要求：

（1） 数据中心各线上设备区域系统、各核心骨干区域系统、各动力区域系统、各仓储系统、各报警监控系统的访问均需使用定制的电子卡，且电子卡由数据中心专门物业保管，特定授权需求方按需求领取归还，并配备紧急电子卡以备不时之需（如常规电子卡遗失），一旦发生遗失情况立即申请电子卡管理系统进行权限注销；
（2） 数据中心的物理设备（包括其对应的各种组件），配件耗材的安置或存放区域必须要与所有办公区域和公共区域隔离（如办公室或大堂）；
（3） 数据中心所有阿里云专属的所有物理设备、设备配件、网络耗材，以及设备厂商的维修设备、配件、耗材等进出数据中心，必须由阿里云内部授权人员发送盖有专人保管印章的设备进出单传真，数据中心现场核实无误后方可允许设备、配件、耗材等的进出；
（4） 仓储系统中的重要配件，如核心网络设备的网络模块，精密存储介质等，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；
（5） 仓储系统中的任何配件，必须由授权工单和授权人员方能领取，且领取必须在仓储管理系统中进行登记记录，阿里云专人定期对所有仓储系统物资进行综合盘点追踪；
（6） 数据中心内部的每个区域，或外部走廊区域，或仓库门口区域，都使用了摄像机，物业保安 7x24 小时分段巡逻，并对所有基础设施进行 7x24 小时集中视频监控；
（7） 采用全方位电子摄像机对阿里云的基础设施内外部区域进行视频监控，对设施区域中的其他系统进行检测（如动力和制冷）和监控跟踪入侵者；
（8） 所有人员活动记录电子保存（长期），所有视频记录被保存（3 个月），以备后期审计，同时提供额外的安全控制措施，如:特定区域采用铁笼隔离，掌纹识别技术；
（9） 只允许具备长期授权名单内的内部人员（实时更新），或审批通过的其他人员，以及授权认可的第三方固定人员名单内的人员（每月更新）进入数据中心，且非长期授权人员再以核实需求工单真实性的形式进行二次审核，准确无误后方可进入；
（10）非长期授权，非固定人员授权名单内的人员访问，必须要求阿里云内部需求方在流程系统上提交需求，由各层级主管提前审批通过后，方可同意其访问想要访问的内部特殊区域，并由对应数据中心的驻场人员全程

指导陪同。阿里云不定期对访问数据中心的人员登记情况进行审计，严格控制非授权人员访问数据中心；

7.2 环境控制

阿里云采用一系列措施来保障运行环境。

（1）电力

为保障阿里云业务 7*24 持续运行，阿里云数据中心采用冗余的电力系统（交流和高压直流），主电源和备用电源具备相同的供电能力，且主电源发生故障后（如：电压不足、断电、过压、或电压抖动），会由柴油发电机和带有冗余机制的电池组对设备进行供电，保障数据中心在一段时间的持续运行能力，这是阿里云数据中心一个关键的组成部分。

（2）气候和温度

阿里云任意一个数据中心，均采用空调（新风系统冷却或水冷系统冷却）保障服务器或其他设备在一个恒温的环境下运行，并对数据中心的温湿度进行精密电子监控，一旦发生告警立即采取对应措施。并且，设备冷风区域进行了冷风通道密闭，充分提高制冷效率，绿色节能。空调机组均采用 N+1 的热备冗余模式（部分数据中心采用 N+2 的冷、热双重冗余模式），空调配电柜采用不同的双路电源模式，以应对其中一路市电电源发生故障后空调能正常接收供电。且在双路市电电源发生故障后，由柴油发电系统提供紧急电源，减少服务中断性的可能，以防止设备过热。

（3）火灾检测及消防

自动火灾检测和灭火设备防止破坏计算机硬件。火灾探测系统的传感器位于数据中心的天花板和底板下面，利用热、烟雾和水传感器实现。在火灾或烟雾事件触发时，在着火区提供声光报警。在整个数据中心，也安装手动灭火器。数据中心接受火灾预防及灭火演练培训，包括如何使用灭火器。

基础安全

8.1 云安全服务（云盾）

（1）云盾------防 DDoS 清洗服务

DDoS（Distributed Denial of Service）分布式拒绝服务俗称洪水攻击，而在云端该攻击表现为，通过仿冒大量的正常服务请求来阻止用户访问其在云端数据、应用程序或网站。对云端用户而言该攻击就像在出行高峰时段遇上了交通瘫痪，除了坐在交通工具中愤怒的等待别无他法；而对云服务商而言如果无法从大量的仿冒请求中鉴别出恶意访问流量并完成清洗，则不但会影响云服

务的稳定性更会动摇用户将数据和应用迁移上云端的信心。DDoS 攻击在 2011 年、2012 年连续被 CSA（Cloud Security Alliance）收录为《云端十大安全威胁》。

作为中国领先的云计算服务商，阿里云基于自主开发大型分布式操作系统和十余年安全攻防的经验，为广大云平台用户推出基于云计算架构设计和开发的云盾海量防 DDoS 清洗服务，该服务具有以下优势：

全覆盖:

云盾的防 DDoS 清洗服务可帮助云用户抵御各类基于网络层、传输层及应用层的各种 DDoS 攻击（包括 CC、SYN Flood、UDP Flood、UDP DNS Query Flood、(M)Stream Flood、ICMP Flood、HTTP Get Flood 等所有 DDoS 攻击方式），并实时短信通知用户网站防御状态。

云盾的防 DDoS 清洗服务由恶意流量检测中心、安全策略调度中心和恶意流量清洗中心组成，三个中心均采用分布式结构、全网状互联的形式覆盖阿里云所有提供云服务的数据中心节点。

全天候:

依托云计算架构的高弹性和大冗余特点，云盾防 DDoS 清洗服务实现了服务稳定、防御精准。

稳定：云盾防 DDoS 清洗服务可用性 99.99%

精准：恶意流量检测中心的检测成功率 99.99%，单个数据中心流量检测能力达到 60G bit/s 或 6000 万 PPS 以上；

恶意流量清洗中心的清洗成功率 99.99%;

全清洗：

对于阿里云云服务器用户提供单个 IP，3G 以内的所有类型的 DDoS 攻击流量清洗服务。

（2）云盾---安全体检

您了解自身网站的安全现状吗？那您了解它是否有漏洞、是否被入侵、是否已被偷偷植入木马导致数据丢失？

------现在您觉得您真的了解它吗？

绝大多数的网站入侵事件总是由黑客扫描网站开放的端口和服务，并由此寻找相关的安全漏洞并加以利用来实现入侵，最后通过在网站内植入木马来达到篡改网页内容或者窃取重要内部数据的违法目的。

云盾的安全体检从网站最常见的入侵行为入手，对构建在云服务器上的网站提供网站端口安全检测、网站 WEB 漏洞检测、网站木马检测三大功能。

网站端口安全检测：

该功能通过服务器集群对构建在云服务器上的网站进行快速、完整的端口扫描，使用最新的指纹识别技术判断运行在开放端口上的服务、软件以及版本，一旦发现未经允许开放的端口和服务会第一时间提醒用户予以关闭，降低系统被入侵的风险。

网站 WEB 漏洞检测：

该功能聚焦在对构建在云服务器上网站的 WEB 漏洞发现，检测的漏洞类型覆盖 OWASP、WASC、CNVD 分类，系统支持恶意篡改检测，支持 Web2.0、AJAX、各种脚本语言、PHP、ASP、.NET 和 Java 等环境，支持复杂字符编码、chunk,gzip,deflate 等压缩方式、多种认证方式（Basic、NTLM、Cookie、SSL 等），支持代理、HTTPS 、DNS 绑定扫描等，支持流行的百余种第三方建站系统独有漏洞扫描、同时，通过规则组对最新 Web 漏洞的持续跟踪和分析，进一步保障了产品检测能力的及时性和全面性。

网站木马检测

在检测技术上通过对 HTML 和 javascript 引擎解密恶意代码，同特征库匹配识别，同时支持通过模拟浏览器访问页面分析恶意行为，发现未知木马，实现木马检测的“0”误报。

8.2 漏洞管理

阿里云在漏洞发现和管理方面具备专职团队，在漏洞发现方面除却自主开发的漏洞检测工具外更拥有一批具备发现“0day”漏洞的安全专家，通过自动和手动的渗透测试、质量保证（QA）流程、软件的安全性审查、审计和外部审计工具进行安全威胁检查。

阿里云漏洞管理团队的主要责任就是发现、跟踪、追查和修复安全漏洞。通过数字化的“漏洞分”运营，对每个真实的漏洞进行分类、严重程度排序和跟踪修复。阿里云与各安全研究社区的成员保持联系，受理外部漏洞举报。

8.3 安全事件管理

阿里云建立了安全事件管理平台来实现影响系统或数据的机密性、完整性或可用性的安全事件管理流程，这个流程包含安全事件的受理渠道、处理进度、事后通告过程，安全事件的类别不但覆盖安全攻击和入侵事件，更将重大云服务故障纳入安全事件管理范围予以关注。

阿里云安全团队人员实行 7*24 小时工作制。当安全事件发生时，阿里云安全人员将记录和根据严重程度进行优先级处理。直接影响客户的安全事件将被赋予最高优先级对待。在安全事件事后分析阶段通过追查安全事件根本成因来更新相关安全策略，以防止类似事件再次发生。

8.4 网络安全

阿里云采用了多层防御，以帮助保护网络边界面临的外部攻击。在公司网络中，只允许被授权的服务和协议传输，未经授权的数据包将被自动丢弃，阿里云网络安全策略由以下组件组成：

（1） 控制网络流量和边界，使用行业标准的防火墙和 ACL 技术对网络进行强制隔离；
（2） 网络防火墙和 ACL 策略的管理包括变更管理、同行业审计和自动测试；
（3） 使用个人授权限制设备对网络的访问；
（4） 通过自定义的前端服务器定向所有外部流量的路由，可帮助检测和禁止恶意的请求；
（5） 建立内部流量汇聚点，帮助更好的监控；

8.5 传输层安全

阿里云提供的很多服务都采用了更安全的 HTTPS 浏览连接协议，例如用户使用阿里云账号登陆 aliyun 的默认情况为 HTTPS。通过 HTTPS 协议，信息在阿里云端到接受者计算机实现加密传输。

8.6 操作系统安全

基于特殊的设计，阿里云生产服务器都是基于一个包括运行阿里云“飞天”必要的组件而定制的 linux 系统版本。该系统专为阿里云能够保持控制在整个硬件和软件栈，并支持安全应用程序环境。阿里云生产服务器安装标准的操作系统，公司所有的基础设施均需要安装安全补丁。

系统和软件开发及维护

9.1 云服务安全基线：

阿里云在云服务设计阶段就制定针对其不同的服务特点设计安全基线，例如：

（1） 弹性计算：

不同云服务器用户通过安全组手段进行隔离，同一安全组内的不同云服务器可相互访问，不同安全组的云服务器不可相互访问；

安全组通过 iptables 实现不同云服务器间、云服务器和物理机间的安全隔离要求；

通过 ebtables 方式隔离由云服务器向外发起的异常协议访问，防止云服务器被入侵后成为 DDoS 攻击源；

通过 ARP tables 及云服务器生产系统阻断 ARP 攻击；

（2） 开放存储服务：

采用碎片化分布式离散存储技术，对每一份碎片化后的数据实体保存均遵循（不同机架）随机算法，对数据碎片的索引文件同样采用碎片化分布式离散存储技术保存，杜绝 IDC 环境下通过盗取物理磁盘所面临的数据丢失风险；

通过 access ID 加 access key 实现存储请求加密、支持端到端链路加密和云端服务器熵编码、支持客户端加密数据存储、云端访问权限控制（private、public、完全公开）；

支持安全策略定制（可组合源 IP 限制、访问时间段限制、userID 控制、操作命令限制）；

（3） 关系型数据库服务：

在用户授权情况下实现对 SQL 注入攻击的监控和报警、支持数据库审计；

采用 IP 白名单控制非授权用户；

采用最大连接数控制、最大请求数控制、最大结果集控制实现异常连接控制；

9.2 安全咨询和审计

阿里云云平台及云服务安全策略是为个人或团队在应用程序、系统和服务开发过程中确定安全风险中提供安全衡量标准。阿里云的安全政策规定安全团队需要发布安全指导手册和风险评估报告。在应用程序和服务的设计、开发、部署和管理方面，阿里云的安全团队通过以下方式介入云服务的安全管理：

（1） 按照适当性和有效性要求，评估项目设计水平的安全风险和相应的控制措施；

（2） 实施安全审计，评估代码构建防护等级以确定其具有抵抗安全风险的能力；
（3） 在项目生命周期的设计阶段，通过不间断的咨询来专注项目相关的安全风险以及制定解决措施；
（4） 根据相关威胁的研究，提供高层次的与项目相关的安全风险评估；

阿里云认为许多类安全问题出现在产品的设计水平，因此应考虑在一个产品或服务的设计阶段予以解决。安全设计审查有以下目标：

（1） 通过对有关威胁的研究，提供与项目有关的安全风险的一个高层次的评价；
（2） 作为项目的决策者必须作出明智的风险管理决策；
（3） 提供安全控制决策指南和实施计划，例如，正确实施指导选择加密或认证协议；
（4） 提供确保开发团队有关的漏洞等级、攻击模式和解决措施策略方面的教育；
（5） 在项目涉及创新的功能或技术的情况下，安全的团队的责任在于探索研究与技术相关的潜在的安全威胁，攻击模式和技术，特殊脆弱性等特点。

9.3 阿里云软件生命周期中的安全

阿里云的安全开发流程参照软件安全开发周期（SecurityDevelopment Lifecycle）建立：

（1） 安全需求分析环节：根据功能需求文档进行安全需求分析，针对业务内容、业务流程、技术框架进行沟通，形成《安全需求分析建议》；
（2） 安全设计环节：根据项目特征，与测试人员沟通安全测试关键点，形成《安全测试建议》；
（3） 安全编码环节：整合 OWASP 指南、CERT 安全编码等材料，编制各类编程语言的安全编码规范，避免开发人员写出不安全的代码；
（4） 代码审计环节：开发代码扫描工具并结合人工审核代码漏洞，对产品代码进行白盒、黑盒扫描；
（5） 系统发布：安全部门依据上述环节评价结果决定代码是否发布；

灾难恢复及业务连续性

为了减小由硬件故障、自然灾害或者是其他的灾难带来的服务中断,阿里云提供所有数据中心的灾难恢复计划.该灾难恢复计划包括降低任何单个节点失效风险的多个组件,具体如下:

（1） 数据负责与备份:阿里云云服务上的用户数据在一个数据中心的多个系统内部进行复制存放,并在某些情况进行多个数据中心进行复制存放；

（2） 阿里云的数据中心运行在分布式地理位置,其目的在单个区域因为灾难和其他安全事件保持服务的连续性，各数据中心之间高速的光纤互联也为快速的故障转移提供了带宽支持；
（3） 阿里云除了提供冗余数据和区域不同的数据中心措施以外，阿里云还有业务连续性计划，该计划主要针对重要灾难，例如地震事件或公共健康危机，该计划的目的是让云服务能够为我们的客户保持持续性运行；
（4） 阿里云定期对灾难恢复计划进行测试，例如，将一个地理位置或区域的云平台基础架构和云服务处于离线模拟一个灾难，然后按照灾难恢复计划的设计进行系统处理和转移。在此测试过程中，验证在故障位置的业务及营运功能，测试结果将被识别和记录用来持续改进灾难恢复计划。

总结

如上所述,本白皮书阐述了阿里云构建一个由十个核心组件组成的多层次安全策略来支持海量云用户平台,包括阿里云经营的云服务和产品。