阿里云
安全管家

产品简介

文档版本：20190716

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 什么是安全管家服务

阿里云安全管家服务是阿里云安全专家基于阿里云多年安全最佳实践经验为云上用户提供的全方位安全技术和咨询服务，为云上用户建立和持续优化云安全防御体系，保障用户业务安全。

我们在金融、电商、O2O、互联网+、游戏、保险、政府等各行业拥有丰富的最佳安全实践。

适用场景

如果您在阿里云上的业务存在以下需求：

- 需要从产品到服务的完整安全解决方案。
- 缺少熟悉云安全的专业技术人员。
- 希望通过外包服务降低安全运营成本。

您可以选择以下安全管家服务，其中：

- 应急版：适用于入侵导致业务中断，需紧急修复的场景。
- 护航版：适用于重大活动期间，针对重点业务的阶段性保驾护航的场景。
- 企业版：适用于有较高安全要求业务的用户，希望建设全方位的安全防护体系。

服务内容	应急版	护航版	企业版
安全事件管理	· 15分钟内响应 · 5个自然日内解决 · 15天内保障安全	· 紧急安全事件：15分钟内响应 · 非紧急安全事件：1小时内响应 （支持7＊24小时服务响应）	· 紧急安全事件：15分钟内响应 · 非紧急安全事件：1小时内响应 （支持7＊24小时服务响应）
安全检查	事件相关业务的安全检查	重点业务每天巡检	指定云上业务每天巡检
安全策略管理	针对本次事件提供安全策略改进建议	针对重点业务制定安全策略方案并协助策略配置	针对云上所有业务的发展需要制定安全策略方案并协助策略配置
漏洞管理	-	-高危漏洞－15分钟内响应 -中危漏洞－1小时内响应 -低危漏洞－4小时内响应 （以上均在7＊24时间内响应）	-高危漏洞－15分钟内响应 -中危漏洞－1小时内响应 -低危漏洞－4小时内响应（以上均在7＊24时间内响应）
安全架构咨询	-	1小时内响应	1小时内响应

2 安全管家服务白皮书

全面介绍安全管家服务的内容、流程、SLA定义等。

1.『前言』

1.1背景

伴随着云计算技术如火如荼的发展，越来越多的各行业企业或组织将自身的业务迁移到云平台上，让业务迎来了新一轮的技术变革，但在业务迁移上云的过程中，云上业务的可用性、安全性、完整性面临了新的挑战和问题。

云上租户面临的普遍问题如下：

- 缺少全局云安全方案，影响安全防护体系建设及防护效果

  传统厂商对云环境不熟悉，在安全技术防护体系建设过程中，原有的安全防御方案是否可以继续使用？如何在云上建立牢固的安全防御体系？
- 安全方案不确定性导致成本增加

  在制定整体安全解决方案时，关于现有业务安全问题描述分析缺乏，造成安全策略落地没有针对性，增加企业在安全管理工作中投入的成本。
- 专业安全管理人员缺失或难求

  对于缺少专业、高水平的安全人才的企业或组织，当发生信息安全事件后，不能保障及时响紧急安全事，给企业或组织带来影响和损失。

1.2安全服务的必要性

安全管理不是产品叠加，用户需要完整的企业安全解决方案和建立完整的企业信息安全策略，这是单个攻防类安全产品无法做到的。

安全管理是一个体系化和动态调整的管理过程，需要按照科学的方法论和指导思想持续运营，不可能做到一劳永逸。

安全管理需要的是适度管理以满足企业或组织的长远管理目标，在管理过程中，需要有轻重缓急之分的计划和长远的规划视觉。

安全技术是一个广泛而复杂的工种，需要专业的具备一定的安全水平能力的人专职，一般的企业很难依靠自身的技术力量根本解决在不同阶段遇到的安全问题。

各种行业和类型的企业对信息安全有不同的需求，必须进行具体的分析才能制定出适合自身要求的整体安全解决方案。

2.『服务定位-基于产品化管家式服务』

阿里云安全是致力于为云上客户提供全面的信息安全解决方案的互联网公司，它通过阿里巴巴十多年的攻防实战历练的技术能力和经验，开创了以“云盾”为核心品牌的安全产品体系，在网络、系统、应用、风控、安全管理等方面已形成一套完整而又丰富的技术安全解决方案。

阿里云安全管家服务（以下简称：安全管家）是阿里云云盾安全专家团队经过多年的技术实战和经验沉淀，根据客户的业务需求，以云盾安全产品为防护基础，面向云上租户提供全面的、专业的、客户化的安全服务及安全咨询安全服务，从而保障用户安全体系能正常运行和持续优化。提供强有力的技术能力支撑，保障客户业务稳定、安全运行。

阿里云云盾为云上客户提供的安全管家服务类型如下表：

服务类别	服务子项	服务描述
云安全体系 咨询服务	安全体系咨询	参照国内外云安全标准和最佳安全实践，基于客户业务的基础环境，为客户提供安全技术或管理方面的安全方案
云上业务安全风险评估服务	安全风险评估	经验丰富的阿里安全专家加入您的团队，通过定期的安全分析报告，更直观的帮助用户了解自己网络安全状况，解决用户难以全面掌握安全态势的问题
安全事件管理服务	日常安全事件和应急响应事件处理	服务通过对用户信息系统的实时监控，可以及时、准确的发现安全事件、定位事件源，并协助用户对安全事件进行处理，降低用户的损失。对突发的安全事件应急响应分析与处理，帮助客户快速解决事件，降低业务影响。
安全漏洞管理服务	漏洞管理服务	通过巡检及运营方式，帮助客户发现业务安全漏洞，提供漏洞修复方案，防止安全事件发生。

服务类别	服务子项	服务描述
安全产品运营服务	安全产品运营服务	提供专业的安全产品托管服务（包括云盾安全产品和第三方安全产品），为用户代维安全产品，帮助客户根据安全威胁管理安全产品策略，并根据情况，私人定制安全策略，为用户搭建牢固的安全防御体系。

3.『安全管家服务介绍』

阿里云安全管家服务是阿里云安全专家基于阿里云多年安全最佳实践经验为云上用户提供的全方位安全技术和咨询服务，为云上用户建立和持续优化云安全防御体系，保障用户业务安全。

3.1服务内容

阿里云安全根据建立的云安全管理运维体系对客户的云安全系统进行实时的维护管理，针对云上客户的业务提供全面的安全运维服务。

阿里云云盾安全管家服务包括以下内容：

3.1.1云安全体系咨询服务

全面的安全管理是需要一个时时刻刻对网络施行监控的专家团队来解析网络结构中发生的每一个变化的，然而精通安全管理的专职人员目前在国内非常短缺，很少有企业机构能真正具有这样一支属于自己的专注于信息系统安全的团队，通常将信息系统安全的维护任务交由系统管理员团队承担。此外，安全管理工作复杂性和技术的不断发展与挑战要求安全管理专家们承担更多的责任，不断提高自己专业技能，这一切使系统管理员的工作日趋复杂沉重。除专业公司外，很少有公司拥有足够雄厚的实力来自理网络安全。越来越多的企业通过外包安全服务来保障服务来确保他们业务的安全运行。

阿里云安全管家服务团队针对客户云上业务情况，提供面向全面的云信息安全管理周期的模式和方法，基于行业认可的最佳策略、国内外云安全相关规范标准和程序化的流程，提供完善的咨询服务和丰富的安全管理服务，从而使企业把精力集中在最关键的信息安全需求上，保障云上业务的安全性。

3.1.2安全风险评估服务

您的网络安全状况如何？存在那些安全问题？哪里是高安全风险的地带？面对这些安全问题，应该如何去解决？

为了充分了解系统存在的安全风险，以及面临的网络安全威胁，就需要使用多种安全检查方法收集准确的基础数据信息，从而客观的从技术脆弱性角度分析出客户业务中存在的安全问题。

阿里云安全管家服务团队将根据客户公司的安全需求，然后实施最有效的诊断服务来评估客户业务安全现状，找出当前客户业务与安全最佳实践存在的差距，为客户制定相应的安全解决方案。

安全评估的主要对象分为以下几个层次，各部分相对独立，而又相互关联相互作用着，通过对每一层次各方面详细深入的分析、评估，才能提供一个完整的结果，对整体的信息系统体系进行说明。

安全风险评估服务主要包括以下内容：

服务类别	描述	方式
网络安全评估	-检查网络访问控制策略合理性 -探测高危端口 -对以上发现的问题进行安全分析，并制定修复方案，指导客户修复安全漏洞	人工检查和工具扫描
主机安全评估	-探测主机操作系统和应用软件的安全漏洞 -发现操作系统和应用软件的配置弱项 -对以上发现的问题进行安全分析，并制定修复方案，指导客户修复安全漏洞	人工检查和工具扫描
应用安全评估	-发现业务应用代码层的安全漏洞 -对以上发现的问题进行安全分析，并制定修复方案，指导客户修复安全漏洞	人工发现和工具扫描

为确保在安全评估过程中业务的可靠性和安全性，安全管家将根据客户网络系统评估业务情况，与客户一起确定检查计划、风险规避措施、应急预算措施和授权说明，防止并能够及时应对在检查过程中发生的意外事件。

3.1.3安全事件管理服务

3.1.3.1安全监测与巡检

管家服务提供安全日常监测和巡检服务，帮助分析和管理日益复杂的系统和应用平台每天遭受的安全攻击事件，并提供解决方案，以减轻用户的压力，使客户公司以最优的性价比得到最有效的网络安全管理。

日常安全巡检内容如下：

安全层面	内容
安全产品及策略	安全产品及策略启用状态、授权状态、配置状态和规范性

安全层面	内容
网络安全层	-访问流量趋势 -网络异常访问行为 -DDOS、CC攻击行为
云服务器操作系统层	-云服务器高危端口，例如：22、3389、3306等高危端口直接发布在互联网上 -云服务器配置弱项，例如：弱口令、root账号直接登录 -针对登录协议的暴力破解攻击事件、远程登录事件 -应用中间软件漏洞，例如：tomcat漏洞、Jboss漏洞 -服务器其他异常事件
应用安全层	-业务可用性监测-Webshell事件 -网站被挂马、暗链、被篡改监测等 -Web应用安全漏洞
数据层	-RDS SQL日志审计状态 -数据脱裤状态

3.1.3.2安全加固服务

计算环境中不断增长的系统平台面临各种安全威胁，包括数据窃取、数据篡改、非授权访问等。这时就需要专业的安全服务，以保障运行和存贮在这些系统平台上数据的机密性、完整性和可用性。

安全管家提供基于安全评估发现的问题实施安全加固指导服务，提高操作系统或网络设备安全性和抗攻击能力。在对系统作相应的安全配置后，结合定期的安全评估和维护服务就使得系统保持在一个较高的安全线之上。

3.1.3.3安全事件应急响应

“安全是相对的，没有绝对的安全”。任何管理和技术上的疏忽都有可能导致运营中断、数据泄漏、声誉受损以及监管并发问题。因此，在信息网络系统中，无法避免安全紧急事件的产生，对突发事件应做到忙而不乱，需要建立有序高效的汇报机制以及事件分析处理的制度，以最短时间，快速从事件中恢复、使影响降至最低，并避免再次发生。

安全管家的应急服务是依靠阿里巴巴多年的安全攻防实战技术能力和管理经验，参照国家信息安全事件响应处理相关标准，在发生安全事件后，按照预防、情报信息收集、遏制、根除、恢复流程，提供专业的7＊24远程紧急响应处理服务，帮助云上用户快速响应和处理信息安全事件并从中恢复业务，同时事后帮助您规划和设计最佳的云上安全管理方案，从根本上遏制安全事件的发生，降低业务影响。

3.1.3.3.1 服务参考依据

安全管家应急服务参考了国家标准，从服务内容上和服务流程上保障服务规范性和服务质量：

- 《信息安全技术-信息安全事件管理指南》-GB/Z 20985-2007
- 《信息安全技术-信息安全事件分类分级指南》-GB/Z 20986-2007
- 《信息安全技术-信息系统应急响应规范》-GB/T 20988-2007

· 《信息安全技术-信息安全应急响应计划规范》-GB/T 24364-2009

3.1.3.3.2 安全事件定义

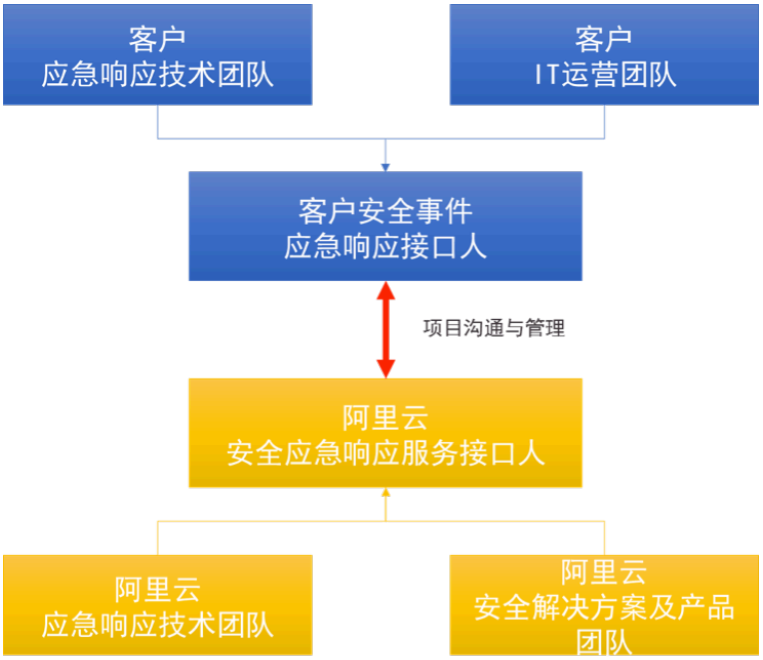
安全管家应急服务针对客户业务出现以下安全问题时，提供远程的安全技术支持服务，协助客户处理安全事件。

事件类别	描述
有害程序事件	计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件
网络攻击事件	后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件
信息破坏事件	信息篡改事件、信息伪造假冒的冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件
信息内容安全事件	通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件
信息内容安全事件	通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件

 说明:

本事件分类依据GB/Z 20986—2007《信息安全技术信息安全事件分类分级指南》。

3.1.3.3.3 服务人员与职责



安全管家应急服务由在阿里巴巴具有3年以上的安全攻防实战经验的安全专家为客户提供一对一专业的安全应急响应服务，整个服务过程中使用规范的服务流程和项目管理流程，帮助客户用最短的时间和成本解决遇到的紧急问题。同时在整个服务过程中，结合阿里云云盾提供的安全产品为客户制定完整的安全解决方案，为客户从根源上解决安全问题，帮助客户搭建安全防御体系。

3.1.3.3.4 安全应急响应服务内容

阿里云云盾提供的安全应急响应服务内容包括以下包括两个方面：

- 安全事件入侵分析和业务恢复

  当入侵事件正在发生或已经发生，阿里云安全管家服务团队安全专家协助客户进行事件调查、保存证据、查找后门、恢复业务、协助取证等内容，同时提供事件处理报告以及后续的安全状况跟踪。

- 其他紧急安全事件分析与处理

  只有出现了上述严重影响网络、主机正常运行的安全事件才启用紧急响应服务，其他日常安全事件均属于安全咨询及日常安全事件处理服务范围。

3.1.3.4重大活动护航保障服务

安全管家护航服务提供专业的安全技术保障，为客户定制重保方案，通过安全防御产品和人工服务相结合措施，全方位保障客户在重大活动期间（例如：国家重要活动期间、企业重大营销活动期间等）的业务安全。

3.1.4安全漏洞管理服务

安全管家为客户提供漏洞生命周期（VLM）的安全漏洞管理服务，漏洞管理包括操作系统漏洞、应用中间件漏洞、用户自身开发的代码漏洞，安全专家通过工具扫描探测和人工发现的方式去发现不同层面安全漏洞，安全专家从漏洞发现到漏洞修复全流程跟踪，帮助客户确实做好漏洞修复整改工作，防止不必要的安全风险。

漏洞生命周期管理流程包括以下内容：

- 漏洞识别：实时对业务系统进行漏洞识别，并建议集中的漏洞数据库
- 漏洞影响范围排查：0day漏洞出现时，及时调查业务影响范围
- 漏洞验证：根据漏洞描述信息，验证漏洞是否存在及严重等级
- 漏洞修复方案：根据漏洞描述及漏洞知识库积累，给出漏洞修复方案
- 漏洞复测：按照漏洞验证的方式重试，确保漏洞已修复

3.1.5安全产品运营服务

3.1.5.1安全产品运营

针对没有专业安全人员的企业，我们提供专业的安全产品托管服务（包括云盾安全产品和第三方安全产品），为用户代维安全产品，帮助客户根据安全威胁管理安全产品策略，并根据情况定制安全策略，为用户搭建牢固的安全防御体系。

3.1.5.2安全效果分析

在实施了安全产品和安全服务之后，利用阿里云大数据平台，构建深度分析模型，对云上业务资产评估和关键系统识别、业务安全威胁分析、弱点评估、已有控制措施分析、可能性及影响分析、综合风险识别等过程进行威胁情报分析，发现业务存在的残留风险，并根据风险问题排定风险优先等级，为组织进行安全规划和建设提供依据和参考方案。

3.2服务流程

3.2.1『安全管家服务流程』

服务流程重点说明：

- 用户购买安全管家任意版本后，安全管家会在1个工作日与您沟通，并建立交流机制，例如：电话、钉钉群、旺旺群、邮件等方式

- 安全管家根据服务的业务范围，与您了解当前业务架构、运维情况、安全情况等内容，并根据收集的信息内容制定并与您确定方案。
- 根据确定好的方案开始实施，根据不同版本提供不同的服务效果，第五章节有说明每个版本的SLA。
- 定期安全服务报告，协助客户分析问题、制定问题解决方案并解决。
- 安全管家对服务范围内业务进行周期性的巡检，确保安全效果。
- 安全管家将事前、事中、事后全流程跟进，从而实现更高质量的安全管理水平，降低安全事件发生率。

3.2.2『安全管家应急服务流程』

安全管家应急服务，我们拥有专业、快速反应的紧急事件响应队伍，在遇到网络安全的突发事件时能够迅速、准确地发现并解决问题，将损失降低到最小。

应急服务流程重点说明：

- 事件分析与处理：

  安全工程师迅速接入地分析问题，判断其严重级别，并继续同客户沟通，给出响应的应急解决办法，安全事件紧急处理过程如下：

  1. 判定安全事件类型
  2. 抑制事态发展
  3. 排除系统故障
  4. 恢复信息系统正常操作
  5. 客户信息系统安全加固指导
  6. 重新评估客户信息系统的安全性能

- 提交报告

  事件处理完毕后，根据整个事件情况写《应急报告》，文档中阐述整个安全突发事件的原因分析，处理方法和过程，处理结果，根据此次问题提出客户网络系统的安全问题，并给出相应的建议。确认后将报告提交给客户。

· 事件跟踪与回访

跟踪事件处理结果，提供更完善的解决方案，15天内不因该问题引发新的安全事件。

4.『服务亮点』

4.1一体化的专家“一对一”专属服务

安全管家提供主动式个性化服务，可全天候帮助客户处理安全问题和紧急需求。所有级别的专属咨询服务都将为您指定一名技术经理，即一名充分了解您业务的可信安全顾问。您的专属技术客户经理将根据当前云安全产品提供主动式通知并快速响应、解决发现的安全问题，为您打造私人定制化服务。

4.2集成化安全实现更好的安全性

安全管家服务含网络、系统、应用、业务、威胁情报等多方位问题的分析定位解决。通过全面的云安全产品防护，避免客户在业务出现问题时要找多家厂商来协调解决。结合持续化运营，实现一站集成化安全管控，提供从后台到前台全套的安全管理服务，实现安全产品的集成与协调。通过这种方式，既提高了解决问题的速度，同时也降低了客户解决问题的成本，用户只需安心使用服务，关注服务结果，将精力中心放到业务。

4.3提高用户安全建设的投资收益

“三分产品技术，七分安全管理”，优质的安全产品是安全防御体系的基础，但长期且高水平的安全状态需要持续运营管理，安全管家可帮助用户对云上业务的安全威胁进行分析，解决安全无人维护或管理的现实问题，提高用户的投资收益，支持业务生产力和协作。

4.4专业化的服务团队解决客户的疑难杂症

在经历了阿里巴巴集团自身业务十年来的安全护航后，阿里巴巴积累了大量的安全研究成果、安全数据和安全运营方法，形成了一支专业的云安全专家团队。云上租户业务在云安全专家的保障下，可以直接享受与阿里巴巴自身业务安全防御体系同等效果的服务，帮助客户事前发现、事后解决问题，从而保障自身业务的安全。

4.5安全事件快速响应，降低风险影响

服务通过对用户信息系统的实时监控，可以及时、准确的发现安全事件、定位事件源，并协助用户对安全事件进行处理，降低用户的损失和影响。

4.6有针对性的全天候安全保障

安全管家服提供务提供7＊24小时的服务响应级别，保障用户的网络及重要系统在任何时间发生任何安全问题都能够及时得到支持和救援，让客户安心。

5.服务SLA

作为一个规范的网络安全服务商，阿里云安全管家服务团队拥有完善的响应机制，同时也具备处理各种紧急事件经验的工程师。我们把安全管家服务分为三个版本，为客户提供符合客户实际需求的安全管家响应服务，且保证达到应有的服务效果，具体详细请参见下表：

服务内容	应急版	护航版	企业版
安全事件管理	· 15分钟内响应 · 5个自然日内解决 · 15天内保障安全	· 紧急安全事件：15分钟内响应 · 非紧急安全事件：1小时内响应 （支持7＊24小时服务响应）	· 紧急安全事件：15分钟内响应 · 非紧急安全事件：1小时内响应 （支持7＊24小时服务响应）
安全检查	事件相关业务的安全检查	重点业务每天巡检	指定云上业务每天巡检
安全策略管理	针对本次事件提供安全策略改进建议	针对重点业务制定安全策略方案并协助策略配置	针对云上所有业务的发展需要制定安全策略方案并协助策略配置
漏洞管理	-	-高危漏洞－15分钟内响应 -中危漏洞－1小时内响应 -低危漏洞－4小时内响应 （以上均在7＊24时间内响应）	-高危漏洞－15分钟内响应 -中危漏洞－1小时内响应 -低危漏洞－4小时内响应（以上均在7＊24时间内响应）
安全架构咨询	-	1小时内响应	1小时内响应

6.服务常见问题Q&A

6.1安全管家服务是否会拿走用户的数据?

安全管家不接触客户任何数据。在服务过程中，如果需要登录到客户系统时，需要用户授权或指导用户工程师协助完成。

6.2工具扫描时是否会对被扫描系统产生影响?

安全扫描服务由安全管家使用专业的安全扫描工具实现，通常情况下不会对被扫描系统产生任何影响。但在业务繁忙时段，如果系统负载过高，扫描行为可能会对被扫描系统造成影响。因此安全扫描服务通常会在非业务繁忙时段实施，以规避风险。

6.3安全管家应急服务处理非安全问题吗?

不提供非安全问题分析和处理服务。只针对以上定义的突发安全事件提供应急响应处理服务，客户的软件问题、基础网络问题、云服务器问题不在此范围内，如果您有其他问题，您可以提交工单，阿里云售后人员会为您服务。

6.4安全管家应急服务可以找到根本原因吗?

安全管家应急服务不承诺100%可以找到安全事件事发原因，该结果取决于客户的IT基础环境，包括服务器日志、应用服务日志保存完整性等方面，但阿里云安全应急响应服务工程师会尽力而为的在事发后的环境中，通过各方面的信息帮助客户排查分析原因，从根本上发现安全技术问题和安全管理问题，从而进一步帮助客户制定完整的解决方案，防止后续再次发生安全事件。

3 阿里云安全服务目录

阿里云安全管家服务目录。

序号	服务名称	服务内容	收费模式	更多详情
1	产品接入服务	· 协助客户完成云盾产品的接入 · 钉钉群提供产品使用、配置咨询	免费	目前面向特定的云盾产品客户免费提供
2	安全咨询	提供一系列的安全咨询服务，包括： · 安全管理体系咨询服务 · 等保合规咨询服务 · 安全开发管理（SDL）咨询 · PCI DSS合规咨询服务	按次收费	详情介绍
3	安全培训	按需提供安全培训服务，包括： · 员工安全意识培训 · 网站安全开发 · 渗透技术培训	按次收费	详情介绍
4	安全评估	对客户的业务系统进行全面的安全评估，通过： · 人员访谈 · 安全基线检查 · 主机及业务安全扫描 · 安全人工检测 提供安全评估报告及修复建议。	按次收费	详情介绍

序号	服务名称	服务内容	收费模式	更多详情
5	代码审计	对客户的业务系统源代码进行白盒检测，通过对代码的安全检查，发现存在于源代码中的安全缺陷，并提供代码修复措施和建议。	按代码量收费	详情介绍
6	应急响应	客户系统遭受黑客入侵后提供的安全技术响应服务，内容包括： · 清理系统木马后门、病毒 · 清理WEB站点中存在的WebShell · 分析入侵原因，查找造成入侵的安全漏洞 · 提供应急响应报告，帮助客户快速恢复业务	按次收费	详情介绍
7	安全管家	基于云上安全最佳实践提供的安全托管服务，能够给客户提供包括安全咨询、安全架构设计、安全评估与安全加固、安全监控、周期性安全检测、应急响应等一系列服务内容，全面满足客户在云上业务安全管理的需求。	按年收费	详情介绍

序号	服务名称	服务内容	收费模式	更多详情
8	安全护航	重大会议、活动期间的安全护航保障工作，根据安全目标为客户设计保障方案、对重点业务进行安全检测和防护、护航期间提供安全专家在线值守。	按天收费	详情介绍

4 安全应急响应服务

阿里云安全应急响应服务（简称“SOS服务”）是帮助云上用户业务在发生安全事件后，按照预防、情报信息收集、遏制、根除、恢复流程，提供专业的7*24远程紧急响应处理服务

阿里云安全应急响应服务（简称“SOS服务”）是依靠阿里巴巴多年的安全攻防实战技术能力和管理经验，参照国家信息安全事件响应处理相关标准，帮助云上用户业务在发生安全事件后，按照预防、情报信息收集、遏制、根除、恢复流程，提供专业的7*24远程紧急响应处理服务，帮助云上用户快速响应和处理信息安全事件并从中恢复业务，同时事后帮助您规划和设计最佳的云上安全管理方案，从根本上遏制安全事件的发生，降低业务影响。

5 安全应急响应服务白皮书

介绍安全应急响应服务的内容、流程、SLA定义等。

1.应急响应服务概述

1.1 概述

服务器被黑了怎么办?

找安全管家应急响应服务，购买地址： https://common-buy.aliyun.com/?commodityCode=yingji#/buy

安全管家应急响应服务（简称“SOS服务”）是由阿里云与安全合作伙伴提供的黑客入侵处理服务，旨在帮助用户正确应对黑客入侵事件，降低安全事件带来的损失。

1.2 服务应用场景

事件类别	详细描述
网络攻击事件	· 安全扫描攻击：黑客利用扫描器对目标进行漏洞探测，并在发现漏洞后进一步利用漏洞进行攻击 · 暴力破解攻击：对目标系统账号密码进行暴力破解，获取后台管理员权限 · 系统漏洞攻击：利用操作系统、应用系统中存在漏洞进行攻击 · WEB漏洞攻击：通过SQL注入漏洞、上传漏洞、XSS漏洞、授权绕过等各种WEB漏洞进行攻击 · 拒绝服务攻击：通过大流量DDOS或者CC攻击目标，使目标服务器无法提供正常服务 · 其他网络攻击行为
恶意程序事件	恶意程序主要类型及危害： · 病毒、蠕虫：造成系统缓慢，数据损坏、运行异常 · 远控木马： 主机被黑客远程控制 · 僵尸网络程序（肉鸡行为）：主机对外发动DDOS攻击、对外发起扫描攻击行为 · 挖矿程序：造成系统资源大量消耗
WEB恶意代码	网站恶意代码常见类型及危害： · Webshell后门：黑客通过Webshell控制主机 · 网页挂马：页面被植入待病毒内容，影响访问者安全 · 网页暗链：网站被植入博彩、色情、游戏等广告内容

事件类别	详细描述
信息破坏事件	· 系统配置遭篡改：系统中出现异常的服务、进程、启动项、账号等等 · 数据库内容篡改：业务数据遭到恶意篡改，引起业务异常和损失 · 网站内容篡改事件：网站页面内容被黑客恶意篡改 · 信息数据泄露事件：服务器数据、会员账号遭到窃取并泄露
其他安全事件	· 账号被异常登录：系统账号在异地登录，可能出现账号密码泄露 · 异常网络连接：服务器发起对外的异常访问，连接到木马主控端、矿池、病毒服务器等行为

二、事件应急服务内容

阿里云安全事件应急响应服务根据安全事件类型及客户的不同需求，可分为“事件处理”及“事件分析（远程）”和“事件分析（现场）”三种规格。

服务规格	服务内容
事件处理	服务器被黑客入侵后提供的远程应急处理服务，包括： · 排查主机是否被黑客入侵 · 对进行中的攻击进行处理，阻止黑客进一步攻击 · 全面查找和清理病毒、蠕虫、木马等恶意程序 · 全面查找和清理WEB站点中的WebShell、暗链、挂马页面等 · 对因入侵而导致的异常进行处理，帮助客户快速恢复业务 · 提供安全应急服务报告 说明: 服务有效期指提交事件处理对象的期限，而非指服务完成时间。本服务由阿里云授权的第三方安全公司实施。

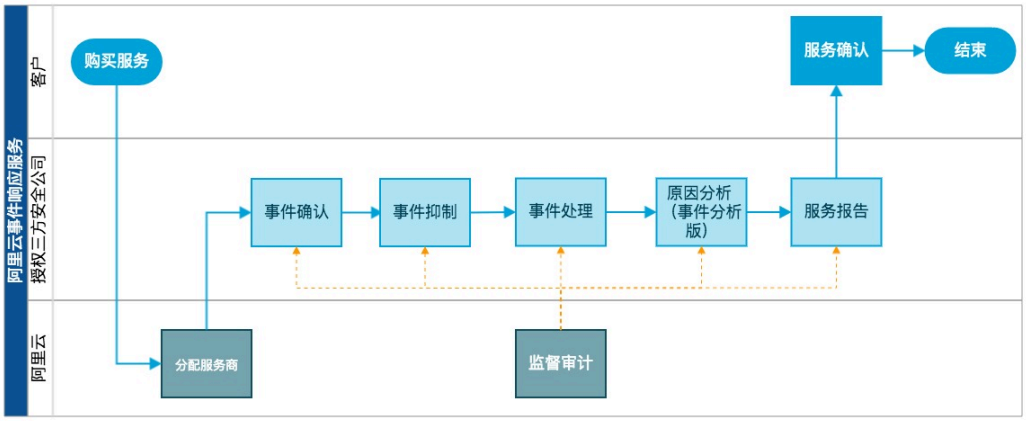
服务规格	服务内容
事件分析(远程)	安全技术人员远程提供的应急处理及分析服务，包括： · 排查主机是否被黑客入侵 · 对进行中的攻击进行处理，阻止黑客进一步攻击 · 全面查找和清理病毒、蠕虫、木马等恶意程序 · 全面查找和清理WEB站点中的WebShell、暗链、挂马页面等 · 对因入侵而导致的异常进行处理，帮助客户快速恢复业务 · 分析黑客入侵手法，尽可能找出入侵原因-分析黑客入侵后的行为，判断入侵造成的影响 · 提供修复建议，指导用户进行安全加固，防止被再次入侵 · 提供安全应急服务报告 说明: 购买服务后5天内提交的排查对象有效。本服务由阿里云授权的第三方安全公司实施。
事件分析(现场)	安全技术人员到用户现场提供的应急处理及分析服务，包括： · 排查主机是否被黑客入侵 · 对进行中的攻击进行处理，阻止黑客进一步攻击 · 全面查找和清理病毒、蠕虫、木马等恶意程序 · 全面查找和清理WEB站点中的WebShell、暗链、挂马页面等 · 对因入侵而导致的异常进行处理，帮助客户快速恢复业务 · 分析黑客入侵手法，找出入侵原因-分析黑客入侵后的行为，判断入侵造成的影响 · 提供修复建议，指导用户进行安全加固，防止被再次入侵 · 提供安全应急服务报告 说明: 购买服务后5天内提交的排查对象有效。本服务由阿里云授权的第三方安全公司实施。

3.事件应急服务流程

3.1安全事件响应服务流程

阿里云安全生态合作伙伴团队拥有经过阿里云认证的安全专家，能够帮助客户在遇到网络安全的突发事件时进行迅速、准确地发现并解决问题，将损失降低到最小。

安全事件应急响应服务流程如下：



流程描述说明如下：

购买服务：

1. 当客户系统发生安全突发事件后，需要SOS服务时，需要先购买安全事件应急响应服务。
2. 购买服务后需要在5自然日内页面上提交需要应急响应的资产清单或者在安全公司与客户取得联系后，通过钉钉提交需要处理的资产清单
3. 为避免进一步的损失，建议客户自行对被攻击的资产进行数据备份工作

分配合作伙伴：

当客户购买服务后，阿里云后台管理系统会根据客户购买安全事件情况，为客户分配合适的安全公司。

事件确认：

1. 安全公司的安全工程师与客户直接联系对接，通过与客户交流了解事件具体详情，并记录问题情况
2. 登录被入侵系统查看实际系统状态
3. 根据客户描述现象与系统实际现象，对事件进行确认，定性

事件抑制：

如果在响应过程中，发现黑客正在进行攻击，或者有其他可能会进一步破坏系统的行为，安全工程师将采取抑制手段， 抑制事态发展是为了将事故的损害降低到最小化。

在抑制环节，常见的手段有：

- 断开网络连接
- 关闭特定的业务服务
- 关闭操作系统

事件处理：

在对安全事件进行原因分析之后，安全工程师将进一步对安全事件进行处理，具体工作包括：

- 清理系统中存在木马、病毒、恶意代码程序
- 清理WEB站点中存在的木马、暗链、挂马页面
- 恢复被黑客篡改的系统配置，删除黑客创建的后门账号
- 删除异常系统服务、清理异常进程
- 在排查问题后，协助恢复用户的正常业务服务

入侵原因分析（仅事件分析版提供）：

从网络流量、系统日志、WEB日志记录、应用日志、数据库日志，结合安全产品数据，分析黑客入侵手法，调查造成安全事件的原因，确定安全事件的威胁和破坏的严重程度。

由于部分安全事件会因为黑客清理了日志或者系统未保留相关日志从而导致无法定位入侵原因，因此本服务将尽可能的分析出原因，但不承诺一定能分析出入侵原因。

提交报告：

事件处理完毕后，根据整个事件情况写《阿里云安全事件应急响应报告》，文档中阐述整个安全突发事件的现象、处理过程，处理结果、事件原因分析（针对事件分析版），并给出相应的安全建议，客户在获取报告后可以在对报告内容进行确认，也可以对服务过程向阿里云提出反馈或投诉。

结束阶段：

在安全事件处理结束后，阿里云将继续跟踪事件处理结果，对服务提供商的服务过程和服务质量进行审查。

4.服务SLA说明

服务条款	SLA	赔偿条款
事件响应时间	20分钟内响应(5*8)	未按时响应则退还订单金额的50%
事件处理时间	5台ECS处理3个自然日内完成；超出5台，每5台增加1个自然日以提交报告时间为准	如未按时处理完成，则退还订单金额的50%
服务效果	清理完黑客植入的木马、病毒	如木马、病毒无法清理，退还订单金额的100%

6 等保整改服务

介绍阿里云等保整改服务。

一、背景

等级保护是我国在信息安全保障领域的一项基本制度，开展信息系统安全等级保护工作不仅是加强国家信息安全保障工作的重要内容，也是一项事关国家安全、社会稳定的政治任务，是企业义不容辞的信息安全义务。

纳入等保保护监管范围的企业需要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，信息系统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进行定级及备案工作。

等级保护整改服务是面向等保客户提供的专业辅导服务，其目标是通过差距报告解读、安全咨询、安全整改等服务内容，加强和完善客户在管理和技术方面的安全保障能力，缩小安全现状与等级保护要求之间的差距，协助客户顺利完成等保测评备案工作。

本服务由阿里云安全合作伙伴提供，阿里云提供服务指导及服务质量监督工作。

二、服务内容

1. 等级保护整改方案咨询

   根据差距评估结果，结合用户的业务现状，设计满足等级保护要求的整改方案

2. 安全产品选型及部署指导

   根据安全整改方案，协助客户完成安全产品的选型和采购、部署工作

   对云盾安全产品进行接入及优化配置以满足等保要求

3. 系统安全整改工作

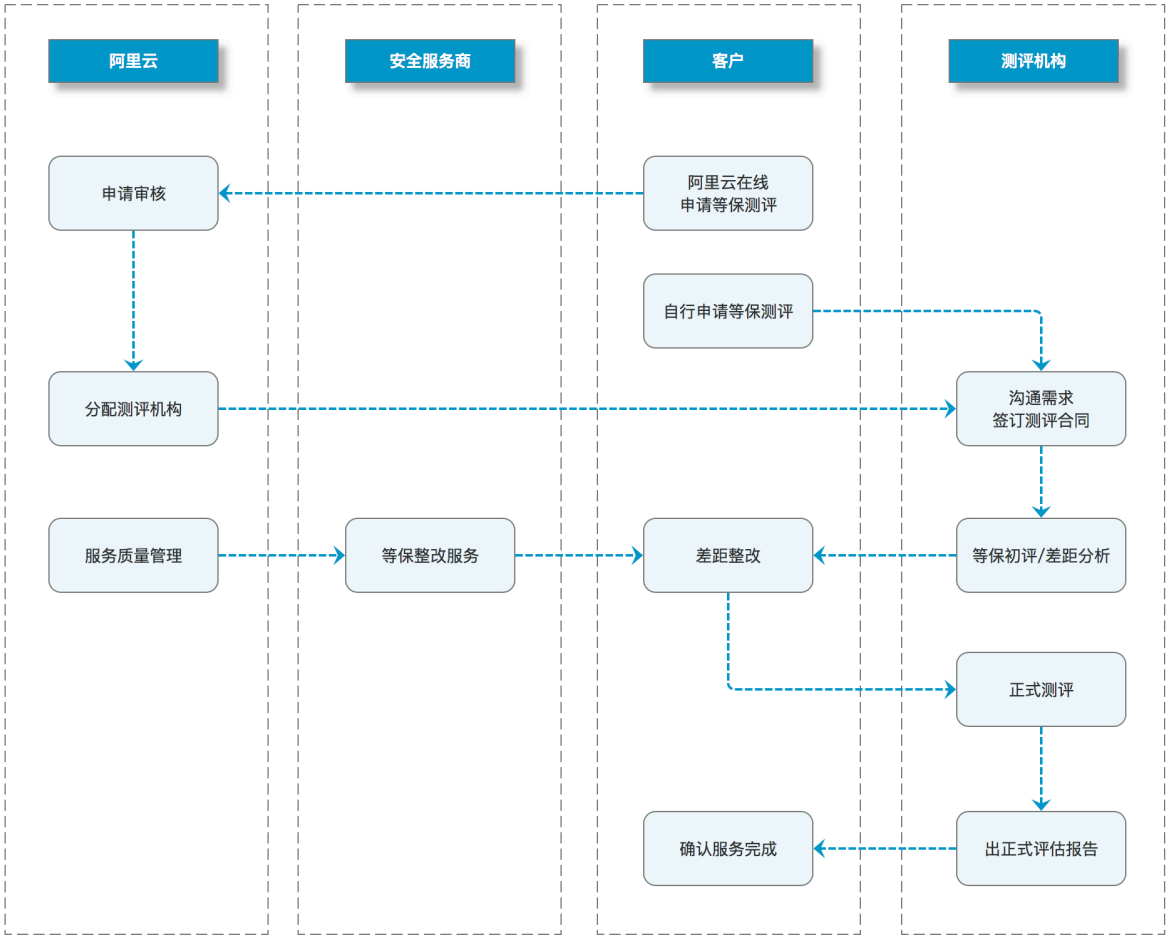
   根据差距评估结果和阿里云最佳安全实践，对网络、主机、数据库根据等保要求进行技术整改

4. 安全管理咨询

   根据等级保护对安全管理的要求，提供部分安全管理制度设计和执行指导。

三、服务流程及输出结果

1. 安全整改服务与等保测评的流程关系如下图所示：



2. 服务输出结果

- 《安全整改建议书》
- 《XXX客户等保整改服务报告》

四、常见问题

1. Q：服务的实施方是谁?

A：本服务是由阿里云授权的第三方专业安全服务提供商提供的，阿里云对其提供技术指导及服务质量监督。

2. Q:整改服务一定要在测评开始后才能买么?

A: 等保测评服务也可以在初评开始前购买并使用。

3. Q: 整改服务的服务周期是多久?

   A: 从购买时开始提供整改服务直到客户完成正式测评工作，或者是从购买开始起一年的服务期，以先到的作为本服务截止时间。

   如客户是2018年5月1日购买服务，2018年8月1日通过正式测评并拿到测评报告，则本服务在8月1日截止，如客户一直未能进行正式测评服务，则选2019年5月1日作为服务的截止时间。

4. Q：本服务支持退款么?

   A: 在服务正式开始前可以申请退款，一旦服务正式开始提供产生工作量则不提供退款服务。

5. Q：如果一次测评没通过，还可以继续提供整改服务么?

   A：在一年的期限内，本服务将持续提供直到客户通过等保测评。

6. Q：我应该购买多少主机数量的服务?

   A：请按照参加等保定级系统所包含的实际ECS数量进行购买。

7 服务器安全托管服务

介绍阿里云服务器安全托管服务。

1.服务简介

服务器安全托管是由阿里云/阿里云授权安全合作伙伴为您提供的针对云上ECS主机的安全托管服务，服务内容包括专家安全体检、系统加固、人工技术支持、安全巡检等服务。通过将云服务器的安全维护工作托管给安全专家，客户能够以较低的安全成本，大幅度提升服务器的安全性，抵御各种黑客攻击，保证客户系统的安全性。

*服务实施方：阿里云安全授权合作伙伴

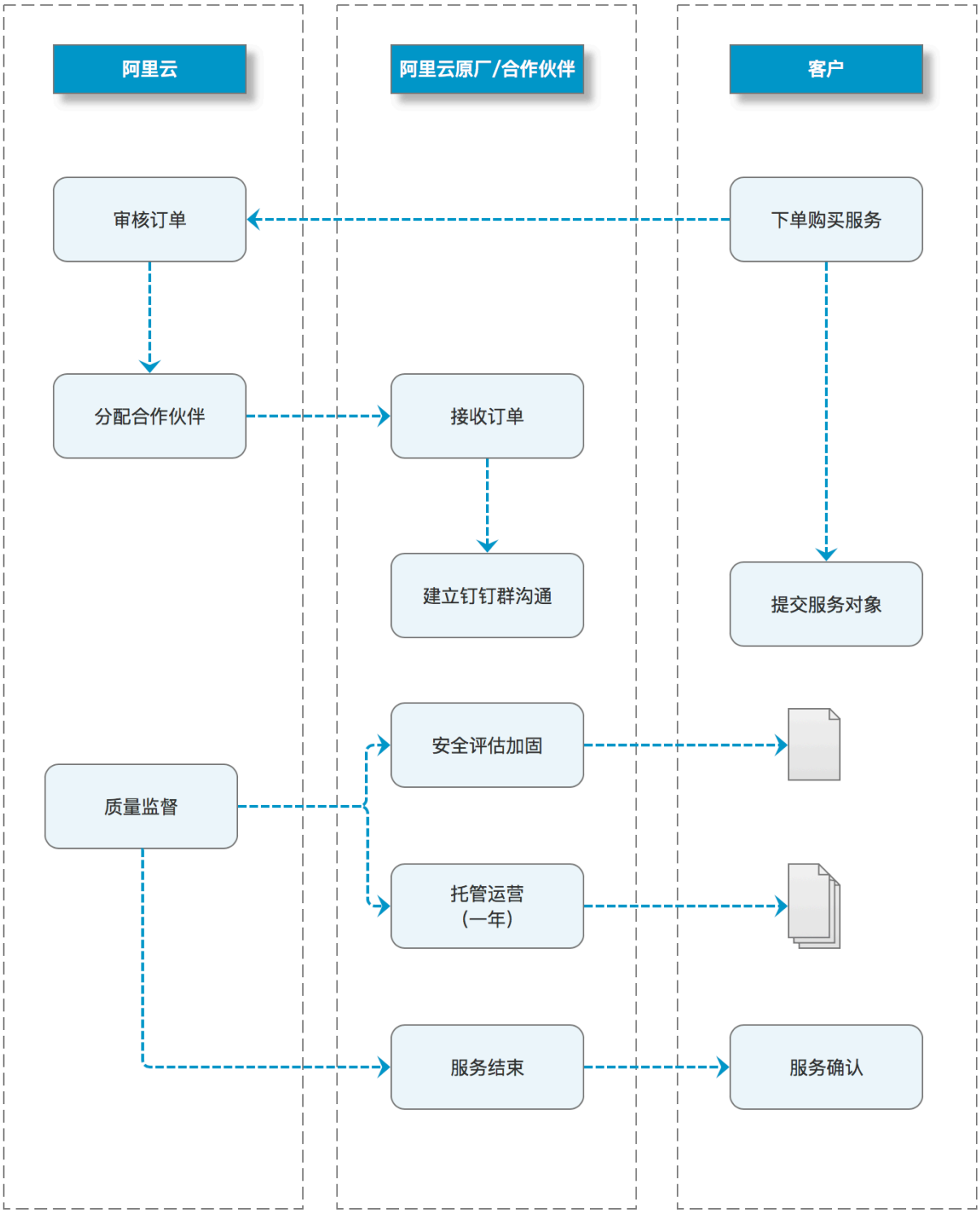
2.服务内容说明

购买服务器安全托管服务后，您将享受到以下服务内容

服务名称	服务内容描述	规格
安全检测	· 对服务器及在服务器上运行的网站(每个服务器不超过3个）进行安全扫描 · 对服务器的安全配置和网站进行人工安全检测 · 对检测到的安全漏洞提供修复指导服务	每年1次
安全加固	对服务器的操作系统基于最佳实践进行加固，加固内容包括： · 系统服务、网络访问控制、账号安全、系统安全策略等方面，提升服务器的安全性 · 对运行在服务器中的ngnix、apache、mysql、sshd、redis等各种主流应用软件进行安全加固 · 对于业务应用层漏洞，提供安全代码加固建议，指导客户进行代码层修复	每年1次

服务名称	服务内容描述	规格
漏洞修复	定期为服务器操作系统进行补丁更新 出现影响服务器安全的高危0day漏洞时，提供应急漏洞修复服务。	根据实际需要提供
应急响应	在服务器遭受入侵时提供应急处理或指导建议，包括： · 查找和清理挖矿程序、病毒、蠕虫、木马等恶意程序 · 查找和清理各种Webshell、挂马页面等 · 分析黑客入侵手法，尽可能定位入侵原因	每年不超过2次

3.服务流程


阿里云
阿里云原厂/合作伙伴
客户
审核订单
下单购买服务
分配合作伙伴
接收订单
建立钉钉群沟通
提交服务对象
安全评估加固
质量监督
托管运营
(一年)
服务结束
服务确认