ALIBABA CLOUD

# 阿里云

# 安全管家服务工作说明书

文档版本：20190527

阿里云

# 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。

www.aliyun.com

# 目录

法律声明 ..... I

目录 ..... II

1. 服务概述 ..... 3

2. 服务范围 ..... 4

3. 前提条件 ..... 5

4. 服务内容 ..... 6

4.1 安全咨询服务 ..... 6

4.2 安全评估 ..... 6

4.3 安全加固 ..... 7

4.4 安全检测 ..... 8

4.5 安全监测与巡检 ..... 8

4.6 安全事件应急响应 ..... 9

4.7 安全产品运营服务 ..... 9

5. 服务 SLA ..... 10

6. 服务流程 ..... 11

7. 客户责任 ..... 12

8. 项目变更 ..... 13

9. 验收标准 ..... 14

10. 完成标志 ..... 15

www.aliyun.com

# 1. 服务概述

安全管家企业版（以下简称安全管家）是阿里云安全团队经过多年的技术实战和经验沉淀，面上云上客户提供的安全托管运营服务，在客户自身安全团队能力不足到期情况下，将部分或全部的安全工作交付给阿里云安全团队来负责，由阿里云安全专家帮助用户进行安全方案设计及日常管理工作，保障云上业务的安全性。

www.aliyun.com

# 2. 服务范围

| 编号 | 服务范畴 | 工作范围 | 备注 |
| --- | --- | --- | --- |
| 1 | 安全咨询 | 基于云上安全最佳实践、结合客户业务的特点，为客户定制云上安全建议方案，<br>在线解答客户安全问题 | 阿里云为主，需要客户配合 |
| 2 | 技术安全评估 | 全面评估甲方阿里云上资产的安全性，包括云平台组件、网络安全、主机安全、应用安全等方面。 | 阿里云为主，需要客户配合 |
| 3 | 安全加固<br>[需单独购买] | 依据最佳实践对甲方云上系统的网络、主机、应用软件进行安全加固（不包括应用程序代码层加固。） | 阿里云为主，需要客户配合（代码层加固由客户自行完成。） |
| 4 | 周期性安全扫描 | 每季度一次对甲方云上资产进行安全扫描。 | 阿里云 |
| 5 | 产品运营指导 | 指导甲方配置和使用云盾产品。 | 阿里云指导，具体配置工作由客户自行完成 |
| 6 | 安全监控与巡检 | 针对甲方云上资产的安全事件、安全漏洞进行日常的安全巡检和安全监控，及时发现安全隐患。 | 阿里云 |
| 7 | 应急响应 | 帮助甲方在系统遭受入侵后进行应急处理。 | 阿里云为主导，需要客户配合 |

www.aliyun.com

# 3. 前提条件

为了保障服务效果和甲方云上系统的安全防护能力，安全管家服务依赖于以下前提条件：

- 甲方应明确需要安全管家服务的云上资产范围，并授权阿里云扫描和评估；
- 甲方需要提供必要的授权给阿里云工作人员，如云平台子账号、堡垒机或服务器的访问权限，便于阿里云安全人员开展工作；
- 安全事件的监测依赖于态势感知产品，如果甲方未开通态势感知产品，则安全监控和巡检服务效果会受到影响。

www.aliyun.com

# 4. 服务内容

## 4.1.安全咨询服务

安全管家企业版提供以下咨询服务内容：

- 针对每个客户建立安全管家服务钉钉群，及时在线沟通各种安全问题。
- 每年根据甲方的业务情况和云上资产安全情况设计一份安全建议方案。

## 4.2.安全评估

为了充分了解信息系统存在的安全风险以及面临的网络安全威胁，需要使用多种安全检查方法收集准确的基础数据信息，从技术角度分析出客户业务系统中存在的安全问题。

阿里云安全管家服务团队将根据甲方的安全需求，评估甲方业务安全现状，找出当前甲方业务与安全最佳实践之间的差距，并提出对应的解决方案。

安全风险评估服务主要包括以下内容：

| 评估类别 | 评估内容描述 | 方式 |
| --- | --- | --- |
| 云平台安全评估 | ● 评估云平台账号安全情况<br>● 评估云平台权限控制是否合理<br>● 评估是否存在敏感信息泄露情况（如 AK 信息泄露） | 人工检查 |
| 云平台组件安全评估 | 对甲方使用的云平台组件（如 RDS、OSS 等）进行安全评估，分析安全风险 | 人工检查 |
| 网络安全评估 | ● 评估网络安全分组划分的合理性<br>● 检查网络访问控制策略合理性<br>● 扫描并探测对公网开放的高危端口<br>● 网络层安全攻击和威胁分析 | 人工检查和工具扫描 |

www.aliyun.com

| | | |
|---|---|---|
| 主机安全评估 | • 通过扫描器全面探测主机操作系统和应用软件的安全漏洞<br>• 通过最佳实践基线检查发现操作系统和应用软件的配置弱项<br>• 对自动化的扫描工具结果进行人工分析验证 | 人工检查和工具扫描 |
| 应用安全评估 | • 通过扫描器发现 WEB 站点中存在的 OWASP 10 安全漏洞，发现业务应用代码层的安全漏洞<br>• 对人工对站点进行安全测试，并对扫描器发现的问题进行安全分析验证<br>• 对其他非 Web 应用进行安全评估<br>• 制定修复方案，指导甲方修复安全漏洞 | 人工检查和工具扫描 |

## 4.3.安全加固

安全加固服务是根据针对需要全托管客户提供的增值服务，甲方需要在安全管家企业版的基础上单独购买。

安全加固服务基于安全评估发现的问题以及最佳实践经验开展。加固内容包括以下几个方面：

- 网络安全策略调整，如网络架构调整、安全组策略加固等
- 对RDS、OSS、RDS等云产品进行安全加固
- 对ECS操作系统进行安全基线加固和补丁升级
- 对Apache、Nginx等应用软件进行安全加固

www.aliyun.com

## 4.4.安全检测

随着时间的推移，信息系统可能会因为业务变化、操作系统货应用软件被发现新的 0day 漏洞、代码调整、配置变更等因素而带来新的安全隐患；因此，周期性的安全检测对于保障业务系统的长期安全是非常有必要的。

安全管家企业版每季度会为甲方进行一次安全扫描，扫描内容包括但不限于以下方面：

- 所有云上资产的开放端口情况
- 主机操作系统安全漏洞检测
- 应用软件安全漏洞检测
- Web应用安全漏洞检测

## 4.5.安全监测与巡检

阿里云云盾安全管家服务团队提供安全日常监测和巡检服务，帮助甲方分析和管理系统每天安全事件，并提供解决方案，让甲方的系统始终处于一个高度安全的状态。

安全巡检功能依赖于云盾安全产品，甲方需要开通云盾态势感知收费版本。

| 监控、巡检项目 | 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 |
| 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 | 云服务器端口开放情况（如 22、3389、3306 等非业务端口直接发布至互联网） |
| | 云服务器配置弱项（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（如 Tomcat 漏洞、JBoss 漏洞） |
| | 服务器其他异常事件 |

www.aliyun.com

| | |
|---|---|
| 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 |

## 4.6.安全事件应急响应

在甲方的信息系统遭受黑客入侵时，按照遏制、根除、恢复流程，提供专业的 7x24 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，并通过后续的安全管理提升安全性，遏制未来安全事件的发生，降低业务影响。

## 4.7.安全产品运营服务

针对没有专门的安全人员的甲方，提供专业的云盾安全产品指导服务，帮助甲方根据安全威胁管理安全产品策略，并根据情况，提供优化安全策略指导，为甲方搭建牢固的安全防御体系。

www.aliyun.com

# 5. 服务 SLA

- 5x8小时服务时间内提供钉钉群在线服务支持，<20分钟的快速响应；7x24小时服务时间内电话服务支持，接到电话<30分钟的上线快速响应。

  通过远程支持提供安全咨询和安全应急响应服务。

- 安全管家服务范围包括甲方提前告知并纳入服务范围内的阿里公有云资产。

  甲方云下资产或未提前告知并授权安全评估的云上资产不在服务范围内。

- 安全加固服务需要单独购买，根据ECS服务器数量定价。

  安全加固服务内容是针对云平台、云资源、操作系统进行加固，不包括业务层代码加固。

- 安全事件应急响应每年提供不超过4次服务。

www.aliyun.com

# 6. 服务流程

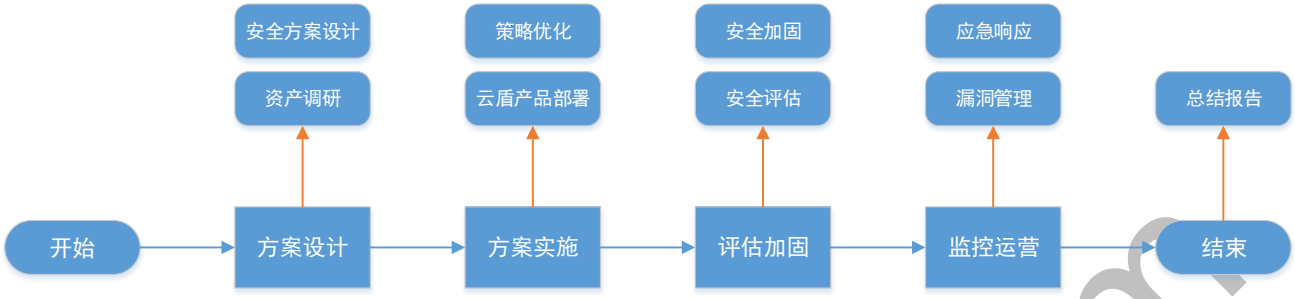


图 1 安全管家服务流程

www.aliyun.com

# 7. 客户责任

- 客户须指派一位项目接口人协助阿里云安全团队开展工作。
- 客户需要提供必要的授权，包括阿里云子账号。
- 客户应根据阿里云安全专家的建议开展安全建设工作，部署必要的安全产品。

www.aliyun.com

# 8. 项目变更

- 因甲、乙方单方或双方要求，对项目目标、服务内容、实施计划、交付项目等进行改变，以及因此类改变而可能引起的合同价格和合同其他条款变化，需要通过协商进行项目变更。
- 如甲方ECS数量出现大幅度增加的情况，且达到安全管家企业版新的报价规格时，甲方需要及时对安全管家企业版进行升级。

www.aliyun.com

# 9. 验收标准

根据安全管家企业版 SOW 和 SLA 要求提供必要的安全服务报告。

www.aliyun.com

# 10. 完成标志

以安全管家订单到期视为项目的完成标志。

www.aliyun.com