阿里云
安全管家

产品简介

文档版本：20200624

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。
	该类警示信息可能会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，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	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。	单击**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。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	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。	switch {active|stand}

目录

1 什么是安全服务

阿里云安全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。

阿里云安全服务在金融、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。

背景信息

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。

云上用户普遍面临以下问题：

- **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，这些问题都急需解决。
- **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。

安全服务有以下必要性：

- 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方向。
- 安全技术是一个广泛而复杂的工种，需要具备一定的安全水平能力的专业人员，一般的企业很难依靠自身的技术力量从根本上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 产品优势

阿里云安全服务具有一键下单即刻服务、大数据加持获取全局威胁情报能力、服务规模化的优势。

一键托管，全栈运营

阿里云“安全管家服务”依托云平台“建设方”的技术优势，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，提供从边界到内网、从漏洞到策略、从配置到数据的全方面的安全运营服务，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。用户只要选择安全管家服务，即可享受全方位、托管式的安全运营服务，让用户可以更加关注业务自身安全。

大数据加持

阿里云安全集中汇聚DDoS高防、Waf、安骑士等安全防护数据，覆盖VPN网络、ECS、Web应用、数据库防护等多层面防护，通过多年实战积累的数据挖掘技术，深度、专业地挖掘每一条有价值的数据，为每一位云上用户提供最前沿的攻防实战情报数据，同时安全运营团队依托攻防情报数据，结合不同用户的防护要求及业务系统现状，可不定期调整安全防护策略，把安全风险降至可控范围，做到动态调整、动态防御、动态运营、动态管理。

规模化优势

阿里云付费用户早已超过百万，安全产品及服务的用户基础数量庞大。面前这样庞大的用户数量，体系化、专业化才能高效服务好每一位云上用户。规模化、体系化意味着运营成本降低，运营成本降低的红利直接影响每一位购买安全管家服务的用户。

分钟级的应急响应

云上安全监控加安全管家的应急响应体系，在发生安全事件的第一时间及时响应处理，帮助用户正确应对黑客入侵事件、清理木马后门、分析入侵原因，最大化的降低安全事件带来的损失，帮助客户快速恢复业务正常运行。

享受阿里自身同等级的安全保障能力

阿里云安全专家根据天猫、淘宝和支付宝多年在各类大型活动期间的安全保障实战经验，总结了多种解决方案以应对各种类型的安全问题，可为客户提供同样等级的安全服务及能力。

3 应用场景

主要可适用于以下三种场景：

建设完善的安全运营体系

- **场景描述**

  部分企业用户在信息化建设上云后，在安全运营能力建设方面相对迟缓，缺乏有效的漏洞管控能力，风险运营能力，风险处置速度跟不上信息系统建设速度，导致业务安全隐患较大。在这类场景中，阿里云安全管家服务可以为用户提供完善且成熟的运营体系，涵盖安全产品能力运营、安全漏洞风险运营、基础安全运营等能力，无缝衔接用户云上资产安全运营，一方面用户可以聚焦到业务能力建设，另一方面为用户运营体系建设赢得宝贵时间。

- **服务收益**

  依托成熟的运营体系，可以让企业用户更加聚焦到业务能力建设；用户在后续安全建设过程中，不仅有充分的准备时间，还可以通过安全管家专家的赋能，更加高效的建设运营体系。

提高安全运营资源的投入产出比

- **场景描述**

  安全运营资源不足包括云安全产品运营专业人员不足、基础服务运营人员和企业用户安全运营资金投入不足。在传统模式下，用户需要投入大量的安全专业人才来确保安全运营工作的顺畅，但随着资产规模的变大，安全相应的人才资源投入也逐步在变大。

- **服务收益**

  规模化、服务化、体系化最直接收益就是成本降低，降低企业运营成本的同时，企业用户还可以依托安全管家高水平技术人员能力提升整体安全产品防护能力、安全策略优化能力、安全漏洞风险运营等安全能力。

重大时期保障

- **场景描述**

  在重大会议期间（如两会、G20等）、节假日（如国庆、春节等）或企业新品发布、促销推广活动、IPO等重大活动期，对云上资产及关键业务做7*24小时保障，需要重点关注Web攻击、主机入侵、页面篡改、信息泄露等重大安全事件，一旦发生安全事件需及时快速处置。

- **服务收益**

  事前充分准备，确保万无一失，事中7*24小时护航，事后回顾总结，全方位提升安全防护能力。

上云及迁云过程中的安全架构指导

- **场景描述**

  企业在上云或迁云的过程中可能会面临业务层面、技术层面和管理层面上的一系列的安全问题，可以通过合理的部署云产品以解决这些问题，安全服务提供了云上安全架构设计指导和安全咨询服务，帮助企业合理设计云上架构，实现最大化的防护效果。

- **服务收益**

  企业上云或迁云过程中提供咨询服务和云上安全架构方案指导，助力企业快速上云，保障云上业务安全的稳定性。

4 服务目录

阿里云安全服务目录

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
3	等保咨询服务	整合云安全产品的技术优势，联合优质等保咨询、等保测评合作资源，提供了一站式服务，全面覆盖等保定级、备案、建设整改以及测评阶段，帮助高效地通过等保测评。	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
4	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
5	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
6	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

序号	服务名称	服务内容	收费模式	更多详情
7	安全加固	在客户授权委托的情况下，远程登录得到客户的业务系统服务器上，对外网或内网主机进行全方位的基线加固和组件升级，提前修补系统潜在的各种高危漏洞和安全威胁。	按次收费	详情介绍
8	PCI DSS合规咨询服务	PCI DSS对于所有涉及支付卡行业的安全方面作出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。	按次收费	详情介绍
9	安全培训	按需提供安全培训服务，包括：网站渗透测试、APP渗透测试、攻击路径、APP风险评估与加固、二进制漏洞分析与挖掘、网站安全开发等。	按次收费	详情介绍
10	安全通告	实时监测、周期性度量风险隐患，您可以根据通告信息，轻松掌握自有IT资产的安全漏洞状态，及时跟踪修补IT资产漏洞，提高企业脆弱性管理能力。	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
11	数据安全咨询服务	提供敏感数据发现、分类分级、敏感数据流向分析服务，通过数据安全组织、流程制度、技术手段形成安全管理的闭环，加强数据访问及权限审批控制。出具数据分级分类规范，提升数据安全防护能力，降低数据泄露风险。	按人/天收费	咨询安全专家
12	SDL开发安全服务	SDL开发安全服务的目标是将安全融入到整个产品或软件的开发生命周期中，同时让该流程适用于客户业务产品化场景，帮助客户从源头解决安全风险问题。	按人/天收费	咨询安全专家