# 云小兵（阿里云）信息安全技术服务

信息安全技术服务，依托成熟的方法论和经验丰富的安全技术团队，从产品到服务双管齐下，从安全架构设计、安全产品选择、安全产品配置等方方面面，为企业的业务和数据安全保驾护航。

**1. 服务方式**

云小兵安全专家根据客户需求对网站进行一站式托管服务。

**2. 服务范围**

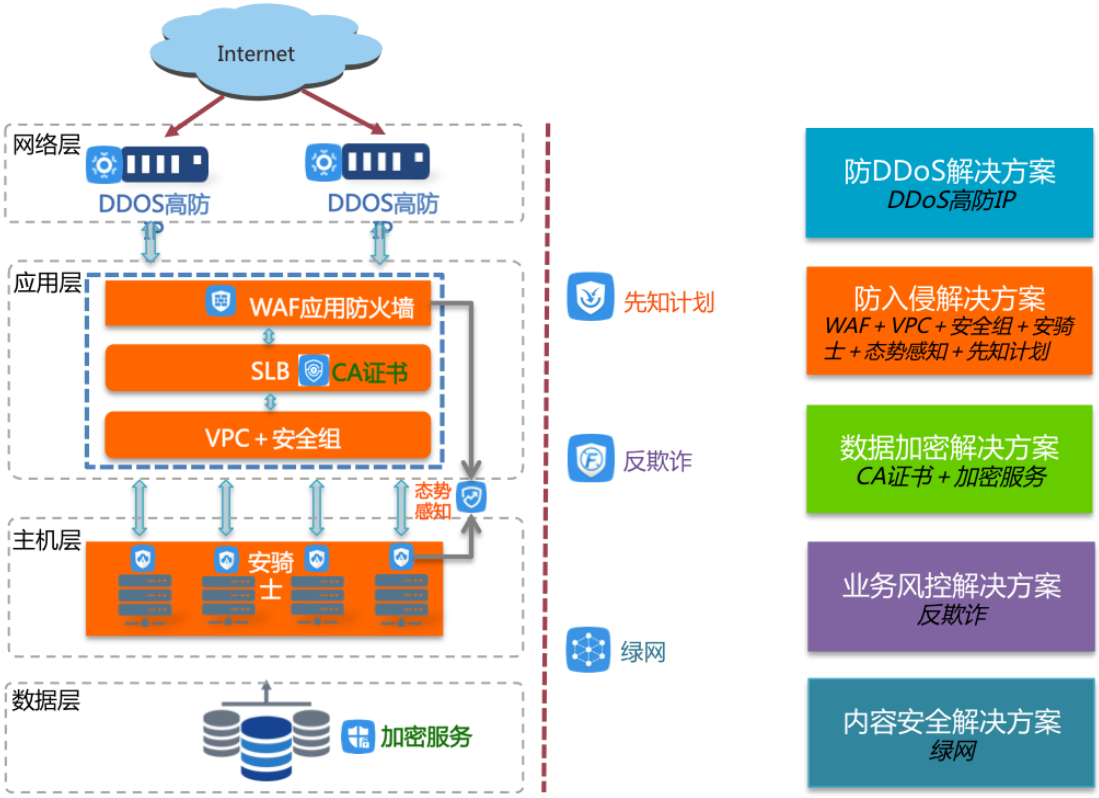
| 服务项目 | 内容描述 |
| --- | --- |
| 信息安全基础服务 | 包含安全架构咨询、安全事件咨询、安全工具配置、安全风险排查、漏洞通告等服务项。 |
| 网站安全托管服务 | 包含漏洞扫描探测、最新漏洞测试、挂马&篡改检测、紧急安全加固等服务项。 |

**3. 服务分级说明**

| 严重性级别 | 严重性说明 | 响应时间 |
| --- | --- | --- |
| **严重** | 用户关键业务、核心组件明显受损或服务不可用，需要立即处理。 | < 5分钟 |
| **紧急** | 用户关键业务、核心组件受到重大影响或重要功能不可用，需要尽快理。 | < 15 分钟 |
| **高** | 用户业务的重要功能受损或降级。 | < 20 分钟 |
| **中** | 用户业务的非关键功能异常。 | < 30 分钟 |
| **低** | 一般性技术或咨询问题。 | < 60 分钟 |

**4. 立体安全体系**

阿里集团十年攻防锤炼出成熟的各种云盾安全产品，通过这些安全产品的组合，可以形成防DDoS攻击、防入侵、数据加密、业务风控和内容安全等解决方案，如下（反欺诈已更名为数据风控）：




上述云安全产品的主要功能如下：

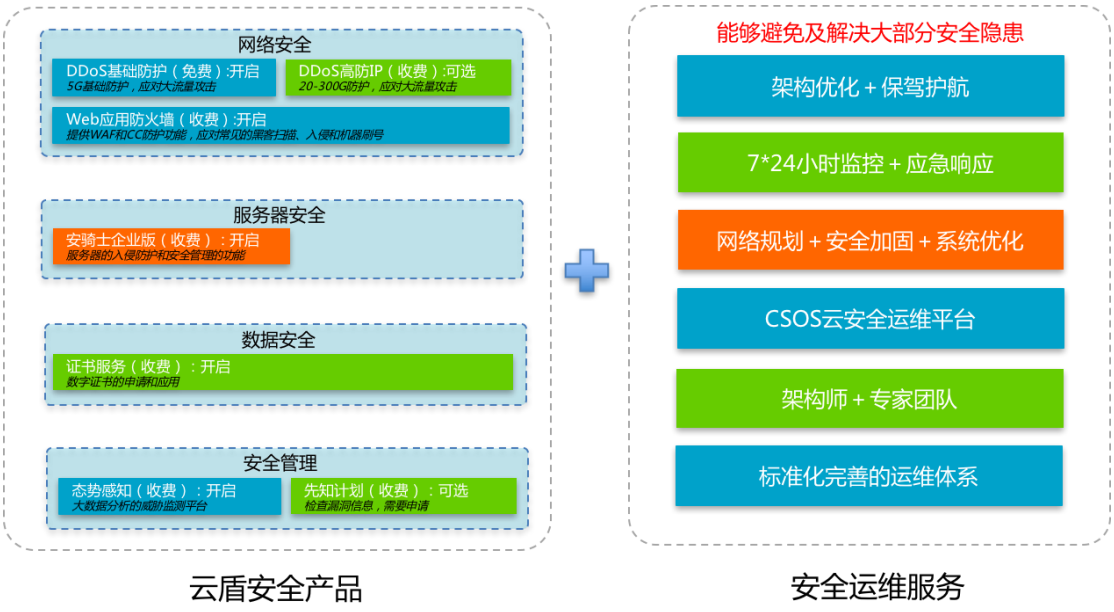
| 安全产品 | 分类 | 主要功能 |
| --- | --- | --- |
| DDoS 高防 IP | 网络安全 | 海量 DDoS 清洗、全业务支持、HTTPS 加密 |
| WAF | 网络安全 | 防御 SQL 注入、XSS 跨站脚本、常见 Web 服务器插件漏洞、木马上传等 OWASP 常见攻击、过滤海量恶意攻击、精准访问控制 |
| 安骑士 | 服务器安全 | 提供网站后门查杀、通用 Web 软件 0Day 漏洞修复、安全机选巡检、主机访问控制等。 |
| CA 证书服务 | 数据安全 | 签发数字证书，实现 HTTPS 化，使网站可信，防劫持、防篡改、防监听 |
| 加密服务 | 数据安全 | 云上数据安全加密、保护云上业务数据的隐私和机密 |
| 态势感知 | 大数据安全 | 收集原始日志和威胁情报，利用机器学习还原攻击，预测未发生的攻击 |
| 数据风控 | 业务安全 | 垃圾注册、刷库撞库、活动作弊、论坛灌水等风控管理，和验证码服务 |
| 先知 | 安全众测 | 私密的安全众测服务、帮助企业全面发现漏洞及风险，按效果付费。 |
| 绿网 | 内容安全 | 提供图片、视频、文字等多媒体的内容风险智能识别服务 |

我们需要使用一部分云安全产品，结合系统的安全运维，打造自身的安全体系，带来全方位的安全保障。

建议选用的安全产品为：

| 产品 | 版本 | 收费 | 建议 |
| --- | --- | --- | --- |
| WAF | Web 应用防火墙（高级版） | 另外收费 | 采用 |
| 安骑士 | 安骑士（专业版） | 另外收费 | 采用 |
| CA 证书 | CA 证书 | 另外收费 | 用现有证书 |
| 态势感知 | 基础版 | 免费 | 采用 |
| DDoS | DDoS 基础防护，开启安全信誉防护联盟规则 | 免费 | 采用 |
| DDoS 高防 IP | DDoS 高防 IP | 另外收费 | 可选 |
| 先知 | 先知 | 另外收费 | 可选 |

安全产品和安全运维结合的安全体系如下图：




**4. 安全访问管理**

为了提高系统的安全性，只允许下面两种方式：

（1） 正常业务访问：通过SLB负载均衡；

（2） 开发、运维人员访问：通过云堡垒机；

**5. 网段划分与安全组访问策略**

阿里云云服务器的安全组特性提供了类似防火墙的访问控制功能，通过设定各安全组之间的安全规则，可搭建复杂的多层访问控制体系，达到系统整体安全。根据业务特性和访问情况的不同，划分成如下几个网段：

网段与安全组对照关系如下：

| 网段分区 | 范围 | 网段 | 对应安全组 |
| --- | --- | --- | --- |
| Web 区 | Web 区，私网 | 10.10.1.x/24 | Web 安全组 |
| 应用区 | 应用区，私网 | 10.10.11.x/24 | 应用安全组 |
| 数据区 | RDS（通过白名单控制访问源），私网 | 10.10.2.x/24 | 数据安全组 |
| 测试区 | 测试系统，私网 | 10.10.17.x/24 | 测试安全组 |
| 管理区 | DMZ 区，公网 | 10.10.3.x/24 | 管理安全组 |

根据实际情况对各安全组制定对应的访问规则。