阿里云安全产品介绍

—— Web应用防火墙

什么是云盾.WAF？

Web应用防火墙(Web Application Firewall, 简称 WAF)是一款网站必备的安全产品。

阿里云.云盾Web应用防火墙：基于云安全大数据能力实现运营+数据+攻防体系、综合打造网站应用安全

通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击；过滤海量恶意CC攻击；禁止恶意的接口滥刷，数据爬取；

避免您的网站资产数据泄露，保障网站的安全与可用性。

云盾.WAF的发展历程

十年Web攻防经验积累、淘宝/支付宝都在用、双11性能稳定

2005.4
阿里安全初创
Web攻防研究

2013.3
产品上线
对阿里云用户
开放

2015.11
经历淘宝/天
猫双11海量请
求考验

2016.4
集成CC防护
精准防护功能
商业化上线

云盾.WAF的应用场景

网站变卡、打不开

恶意海量肉鸡访问
网站资源被耗尽

账号数据、资金损失

官网充值、商品交易、恶意免费/低价成交、盗取用户账户数据

网站数据被恶意爬取
短信流量被滥刷

数据接口被刷、如短信流量滥刷
网站用户数据信息被恶意爬取

获取服务器管理员权限
篡改网站数据、页面

利用最新0day漏洞、命令执行注入、获取服务器管理权限、获取数据、篡改页面等各种危害

云盾.WAF 的产品功能

核心能力

0DAY漏洞防护：
推出最新曝出的Web 0day漏洞自动防御补丁规则、防护黑客的定向攻击

Web应用防护：
防御OWASP 常见威胁、避免注入类攻击导致的数据泄露

CC防护：
针对恶意肉鸡发起的消耗网站资源海量请求进行拦截，并对IP进行封禁处罚

业务风控：
防刷：针对用户注册及登录页面、避免网站的手机用户数据泄露、短信流量恶意消耗

防爬：避免恶意爬虫抓取网站数据

防撞库：缓解对登录页面的Web暴力破解

云盾.WAF的产品特性

产品特性

一键接入：
无需部署软、硬件；无需修改配置；
DNS切换、五分钟实现网站安全

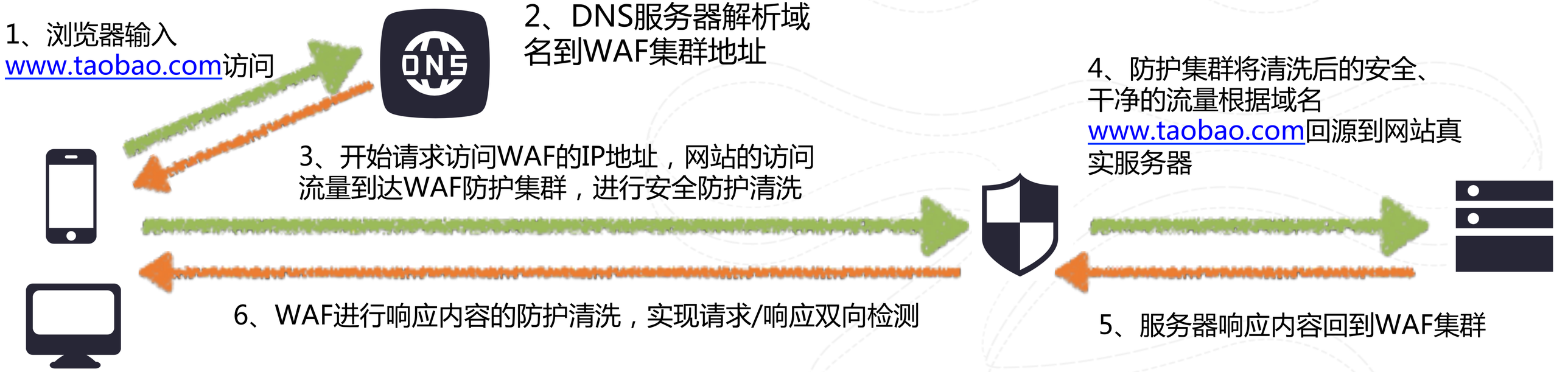
网站隐身：
隐藏源站地址、避免攻击者直接攻击服务器

协同防御：
共享国内30%网站的防护策略、最新0day漏洞攻击第一时间防护

精准防护：
针对黑客发起的定向攻击、根据攻击特征(IP/URL/UA/Referer）一键过滤

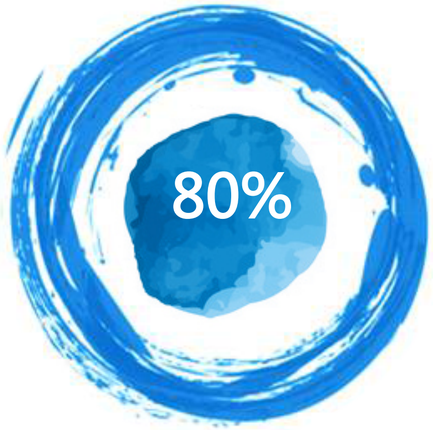
云盾.WAF的工作原理

以用户访问 www.taobao.com 站点为例：



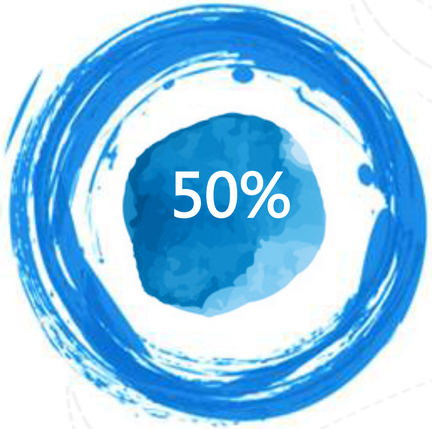
云盾.WAF的竞争优势.痛点分析

传统Web应用防火墙用户的几个痛点：



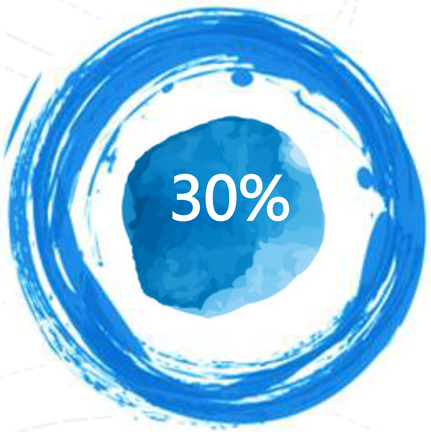
1：用不上

无法应用复杂业务
误报机率大



2：无专人后续运维

每天都有最新Web
漏洞更新、传统产品升级慢、流程
复杂；不能及时防护最新漏洞



3：紧急问题响应慢

一旦网站出现安全或访问问题，不
能第一时间定位原因、影响业务

云盾.WAF的竞争优势.服务

我们能提供什么?

应用防护规则只针对有攻击性行为阻拦，避免过度规则的滥用、降低业务误报

特定接口防护规则专家级定制、让WAF真正被用起来

每日及时更新Web 0day漏洞防护规则避免服务器遭受黑客全网扫描、中招

针对高端企业用户提供VIP服务迅速响应、及时处理网站问题

云盾.WAF的竞争优势.数据模型

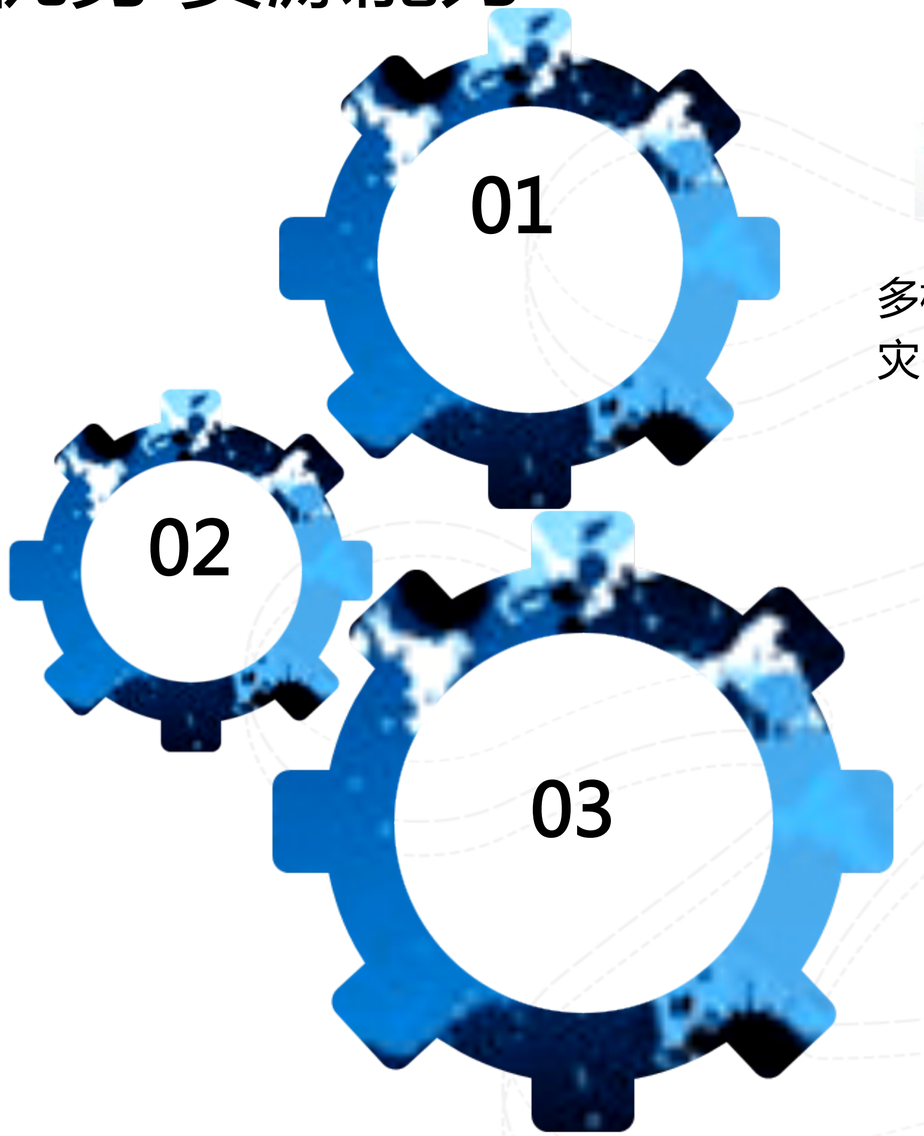
海量IP信誉库

不论是海量肉鸡的CC行为、还是黑客发起的Web定向攻击，都会发现明显的特征：
它们不会只攻击你一天；
它们不会只攻击你一个网站；
那么通过时间、攻击对象、攻击请求比例、以及攻击特点的数据统计，就能还原出一个关于IP维度的信誉库（更新频率要较快），能够对恶意IP直接拉黑

网站正常模型

通过规则的防护，肯定迟早会有黑客通过0day漏洞绕过
但如果对网站的正常请求进行学习，建立起合法请求的访问模型
那么一旦有异常的请求访问（与模型在请求架构上不一致），就可以认定为疑似攻击重点关注
可信模型的建立，就是基于大数据对日常访问日志的统计计算完成
如：URL请求的参数个数；参数类型；参数值长度等

云盾.WAF的竞争优势.资源能力



天然容灾

多机集群模式、 多地防护节点、天然容灾

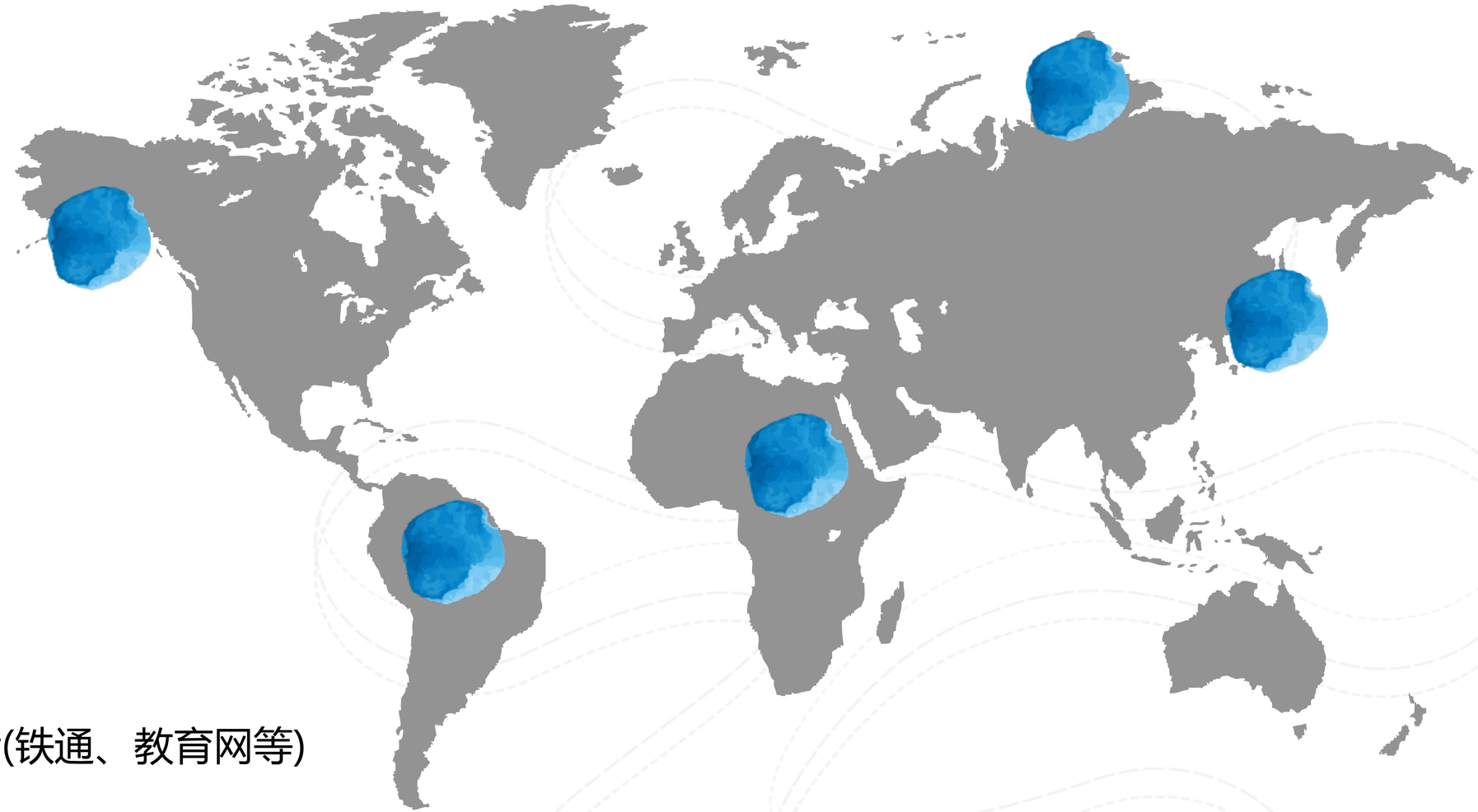
弹性扩容

针对业务正常的流量突增
提前弹性扩容、保障网站能够正常运行、防护有效

攻击阈值大

防护集群最多可支持每秒百万攻击请求防御、资源复用、解决传统安全设备痛点

云盾.WAF的竞争优势.稳定快速



BGP线路支持8线接入，包括(铁通、教育网等)

防护集群由N台机器主-主 工作模式，秒级摘除故障设备、天然多机热备

防护节点遍布国内多个城市与海外节点、多地容灾、加快访问速度

云盾.WAF 与硬件WAF对比

	硬件WAF	云WAF
规则的升级	依赖于厂商的规则更新能力， 一般需要客户主动升级	依托于云上的威胁情报能力， 实时升级0day防护规则
性能	所购买硬件的性能限制， 如需扩容，则需重新购买硬件	可以随着业务的增长， 方便的扩容处理能力
可靠性	需要客户再购买双机热备系统	云WAF天然就是一个集群系统， 无法额外付费
应急响应	一般只提供设备，服务需单独购买	专业攻防团队进行漏洞研究、 捕获0DAY并生成防护规则

云盾.WAF的配置方法

Step 1：添加域名及服务器公网IP

添加域名

域名：www.taobao.com

协议类型：http https

源站IP：1.1.1.1

请以英文“,”隔开，不可换行，最多20个。

Step 2：获取域名对应的Cname地址

www.taobao.com

http: 正常

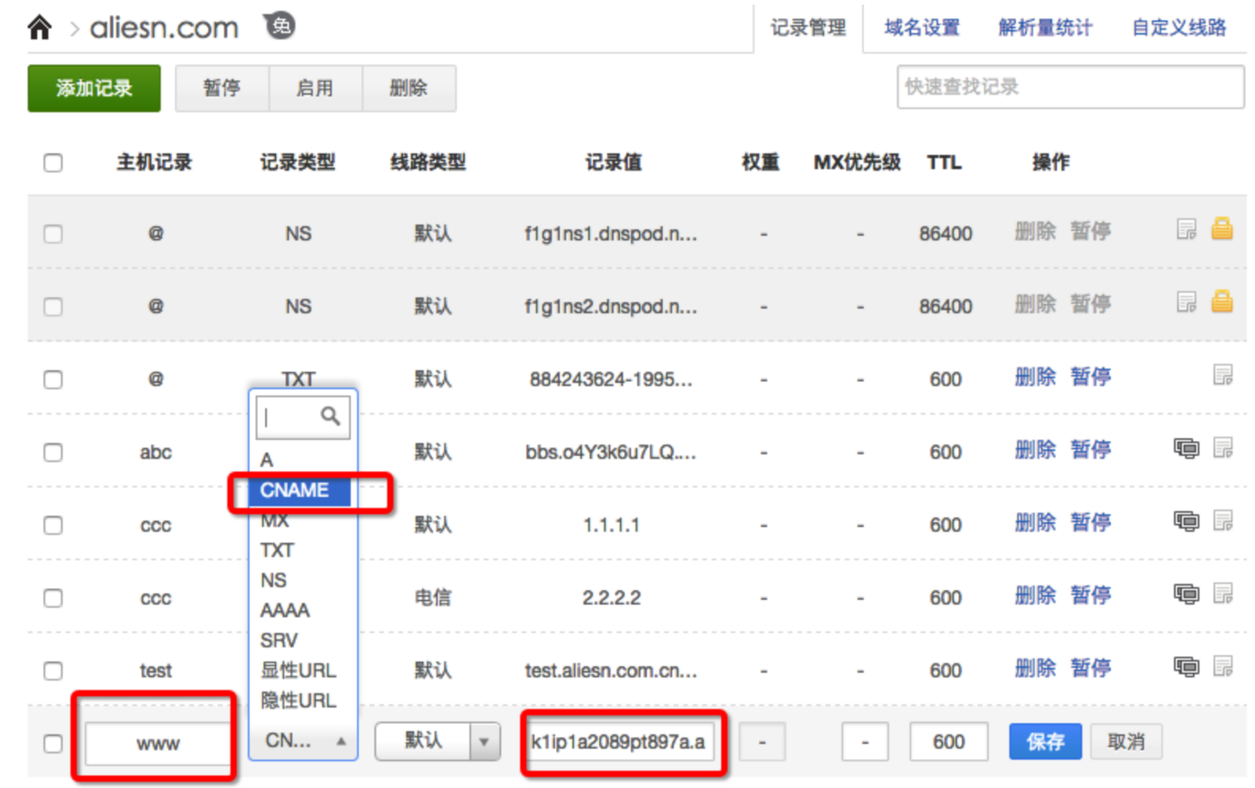
https: 未上传证书

最近两天内无攻击

Cname: QAD0Z47QdglGeZEBZrJJugtY89K0LVsU.alicloudwaf.com

站点IP: 1.1.1.1

Step 3：针对域名添加对应的Cname记录，将流量牵引到WAF防护集群



云盾.WAF的不同版本

旗舰版

全年VIP服务客户、多城部署容灾
海量请求、秒杀等业务场景
参数规格均可定制、满足特殊需求
专家在线诊断攻击、保障业务正常

企业版

对安全有比较高的要求
业务风控、防刷、防短信流量恶意滥刷
专家为网站量身定制防护规则
大数据业务/安全数据展示

高级版

关注网站的Web安全
具有HTTPS业务
针对黑客定向攻击
需要根据攻击特征制定过滤的规则

WAF 产品典型客户

阿里云 aliyun.com

IT桔子

电魂 ELECTRONIC SOUL

大麦 damai.cn

TAL 好未来

红岭创投 HONGLING CAPITAL

芸泰网络 芸芸众生 健康安泰

中华人民共和国人力资源和社会保障部 Ministry of Human Resources and Social Security of the People's Republic of China

用友旗下企业 畅捷通 Chanjet 小微企业 财务及管理服务

中证信息技术服务有限责任公司 China Securities Information Technology Service Limited Company

国华人寿 GUOHUA LIFE

华数TV 广电宽频

中国化工网 www.ChemNet.com.cn

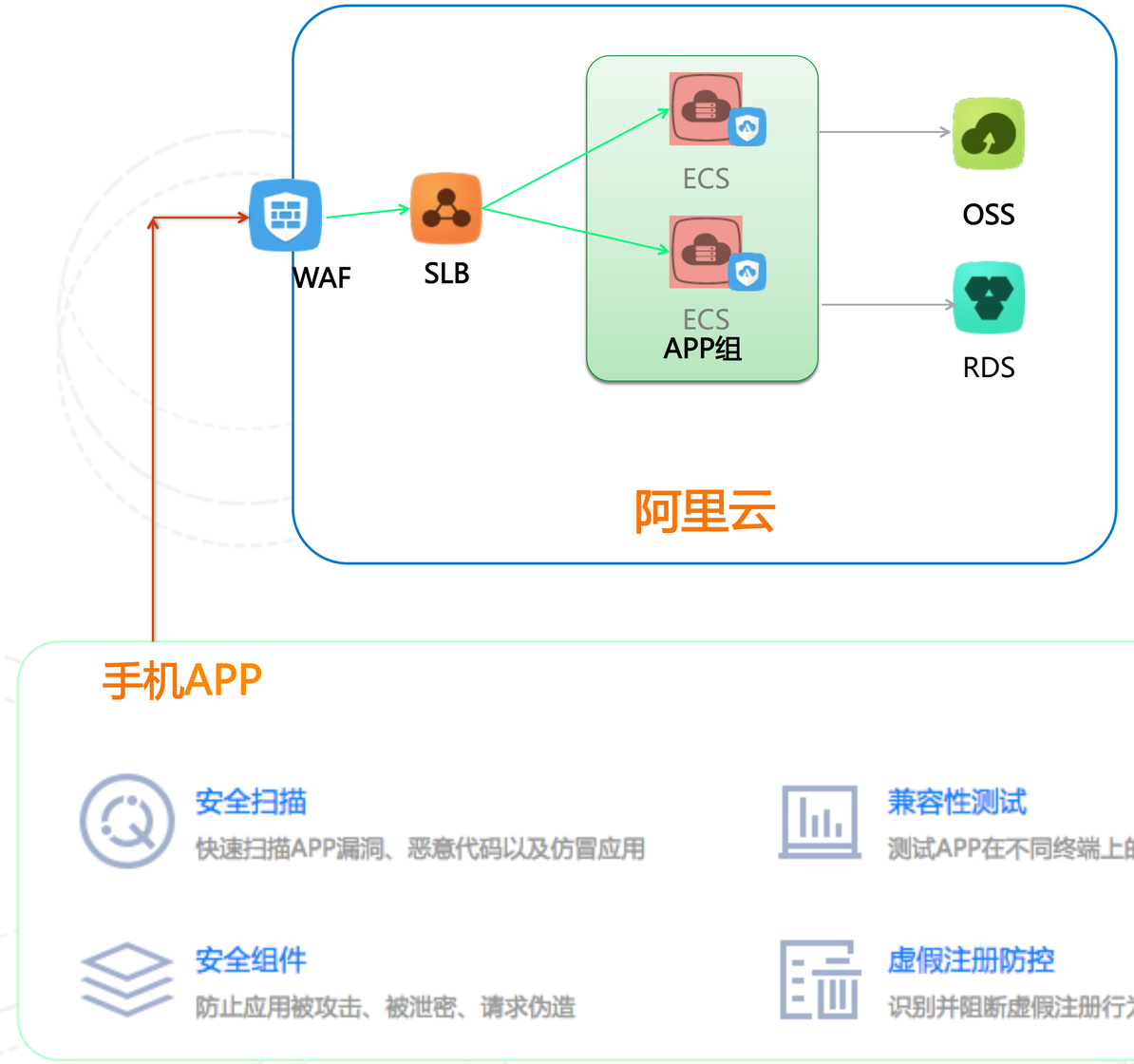
某医疗行业

客户挑战：

- 某医疗行业服务商为大量医院开发智慧医疗APP，部分医院遇到疑似黄牛抢号问题，区域医疗平台也发现有恶意的攻击

云盾方案：

- 通过对APP进行加固保护APP的核心源代码，并对通信做了加密，保证核心代码和程序逻辑难以反编译和破解；
- 使用WAF防御恶意的黑客攻击行为，保护APP应用的安全



Thanks!