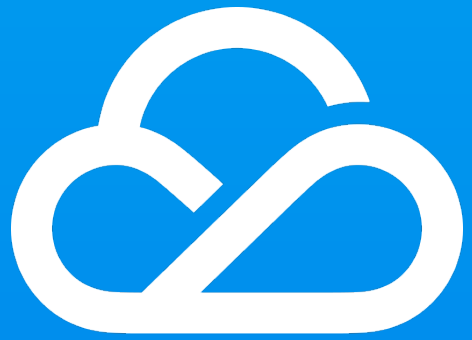


腾讯云

Web应用防火墙-产品介绍

目录

CONTENT

01 Web安全市场概况

中国Web安全现状-2019年上半年网站安全现状

CNCERT/CC 国家互联网应急中心

2019 年上半年我国互联网网络安全态势

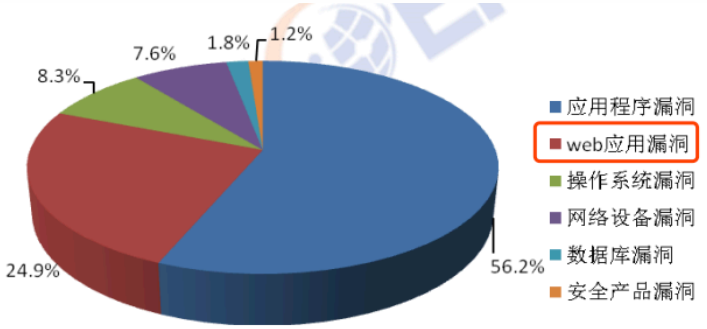


图 5 2019 年上半年 CNVD 收录漏洞按影响对象类型分类统计

图 6 2019 年上半年承载仿冒页面 IP 地址和仿冒页面数量分布

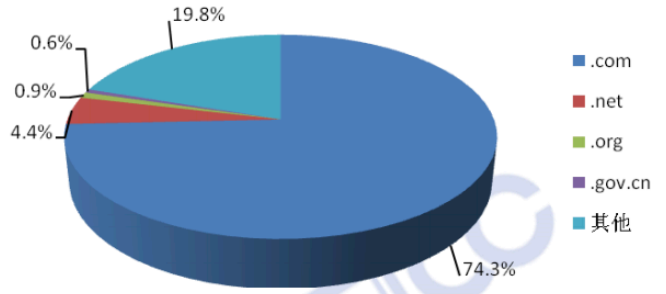
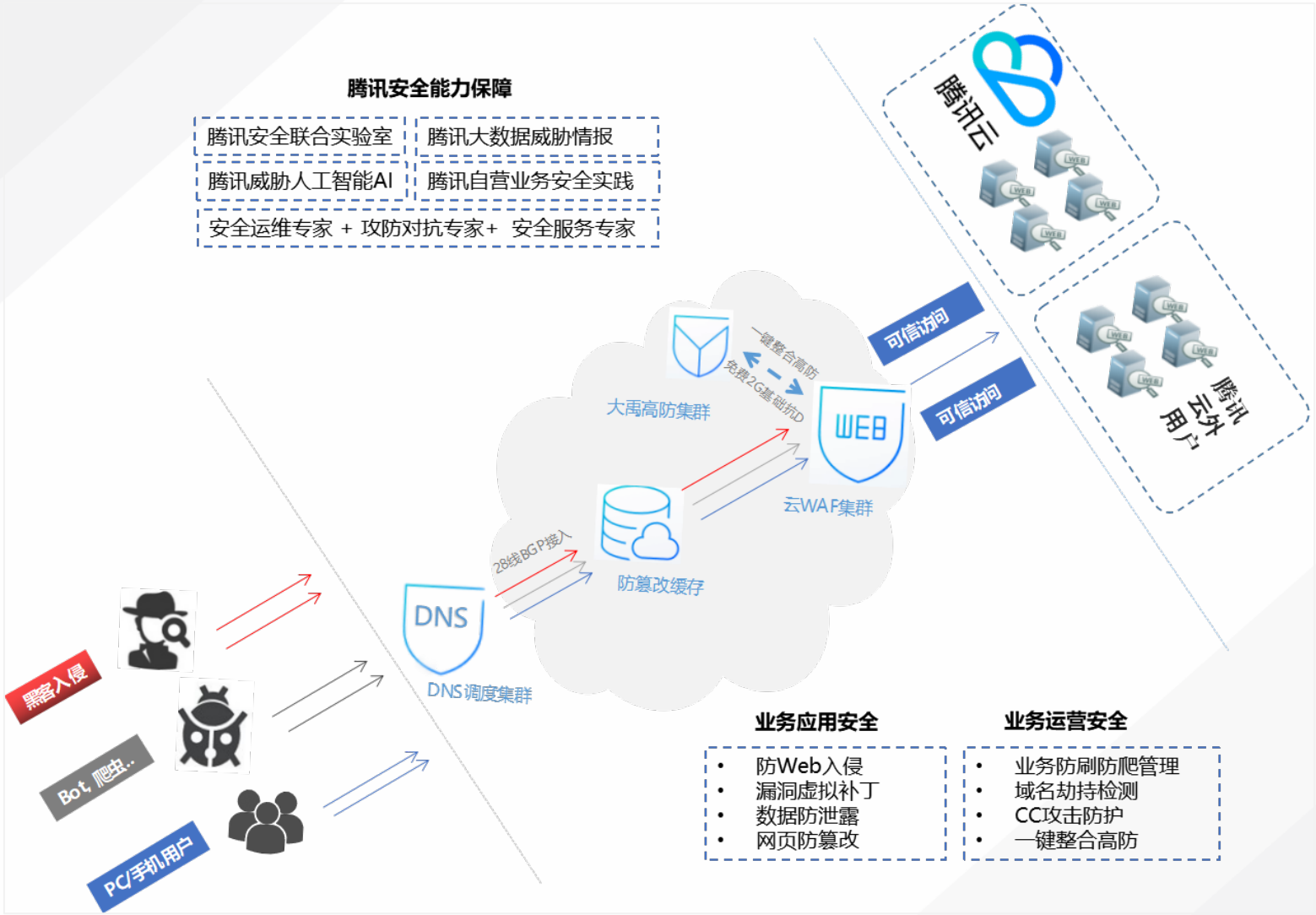


图 8 2019 年上半年我国境内被篡改网站数量按类型分布

2019年上半年Web应用漏洞占CNVD收录漏洞的24.9%
2019年上半年自主检测发现4.6万个针对国内网站的防冒页面
2019年上半年境内遭篡改网站近4万个，其中被篡改的政府网站有222个

02 产品介绍

腾讯云Web应用防火墙：规则+AI双引擎，可靠Web安全防护专家



AI+规则双引擎防护Web入侵行为

有效降低“误报率”提升“覆盖率”，精准防护，打造腾讯云WAF安全防护核心竞争力。

开放腾讯Web安全防护能力

企业组织通过部署腾讯云Web应用防火墙服务，将Web业务的攻击压力转移到腾讯云WAF集群节点:

- ✓ 部署腾讯Web业务安全级别防护能力
- ✓ 共享腾讯安全大数据威胁人工智能能力
- ✓ 获取业界顶尖腾讯安全联合实验室及安全专家攻防对抗能力

Web业务应用安全防护：应用安全风险可控

腾讯云

黑客

Bot利用者

网站用户

SQL 注入
XSS
WEBS HELL
路径穿越
扫描器
文件包含
恶意采集
远程代码执行

Web入侵防护

- AI+规则双引擎识别Web入侵行为，精准有效，低“误判率”低“漏判率”，精准防护，且不影响业务

未发现漏洞！

虚拟补丁

漏洞虚拟补丁

0day漏洞
web漏洞

- 12h内更新高危漏洞防护补丁，24h内更新常见通用型漏洞防护补丁，受护网站无忧层出不穷的Web漏洞隐患。

缓存页面

防篡改缓存

篡改页面

- 对外发布云端缓存中的网页内容，实现网页替身效果,保障受护网页的更新可控可靠

Cell：**********
ID: ********************
...

隐藏脱敏

数据防泄漏

Cell：12345678888
ID: 99999719900018888
...

“撞库”
“拖库”

- 基于事前，事中，事后的防护策略，防止因为Web入侵导致的数据泄露问题

腾讯云

Web网站业务安全保护，一站式解决网站安全问题

腾讯云

CC攻击防护

- 阻断恶意请求，人机识别，有效防御CC攻击，保障正常业务访问的稳定性。

一键整合高防

- 一键接入腾讯大禹DDoS防护，不惧超大流量DDOS攻击

业务可用

运营风控

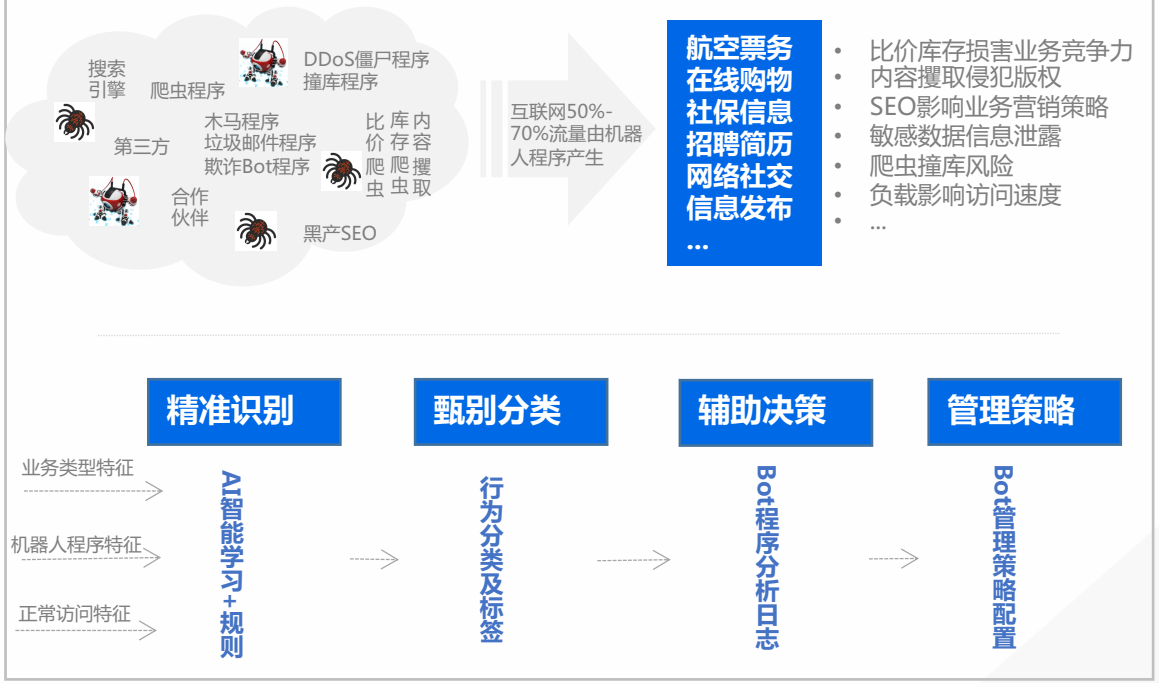
- 应对恶意机器人程序爬取带来的资源消耗，信息泄露及业务风险问题

BOT行为管理

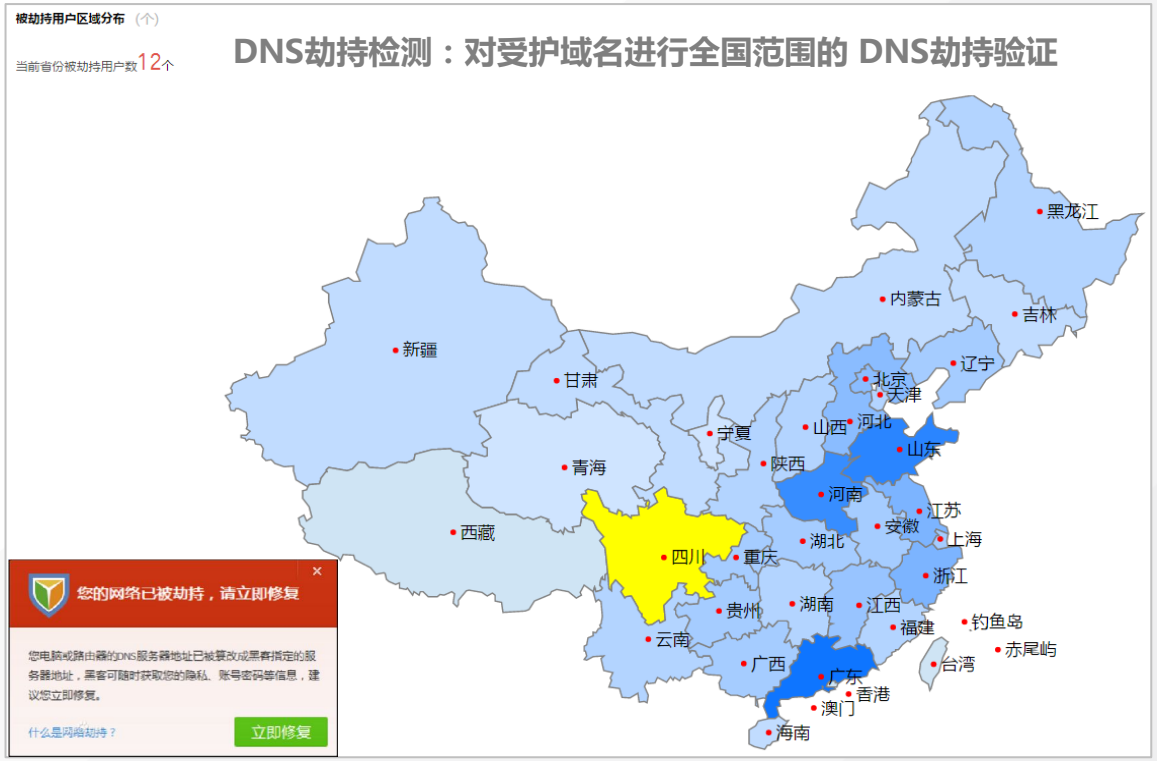
- 应对DNS劫持所带来的业务不可访问，用户访问被劫持钓鱼欺诈等风险问题。

DNS劫持检测

Bot 行为管理：甄别，分类，管理机器人程序行为

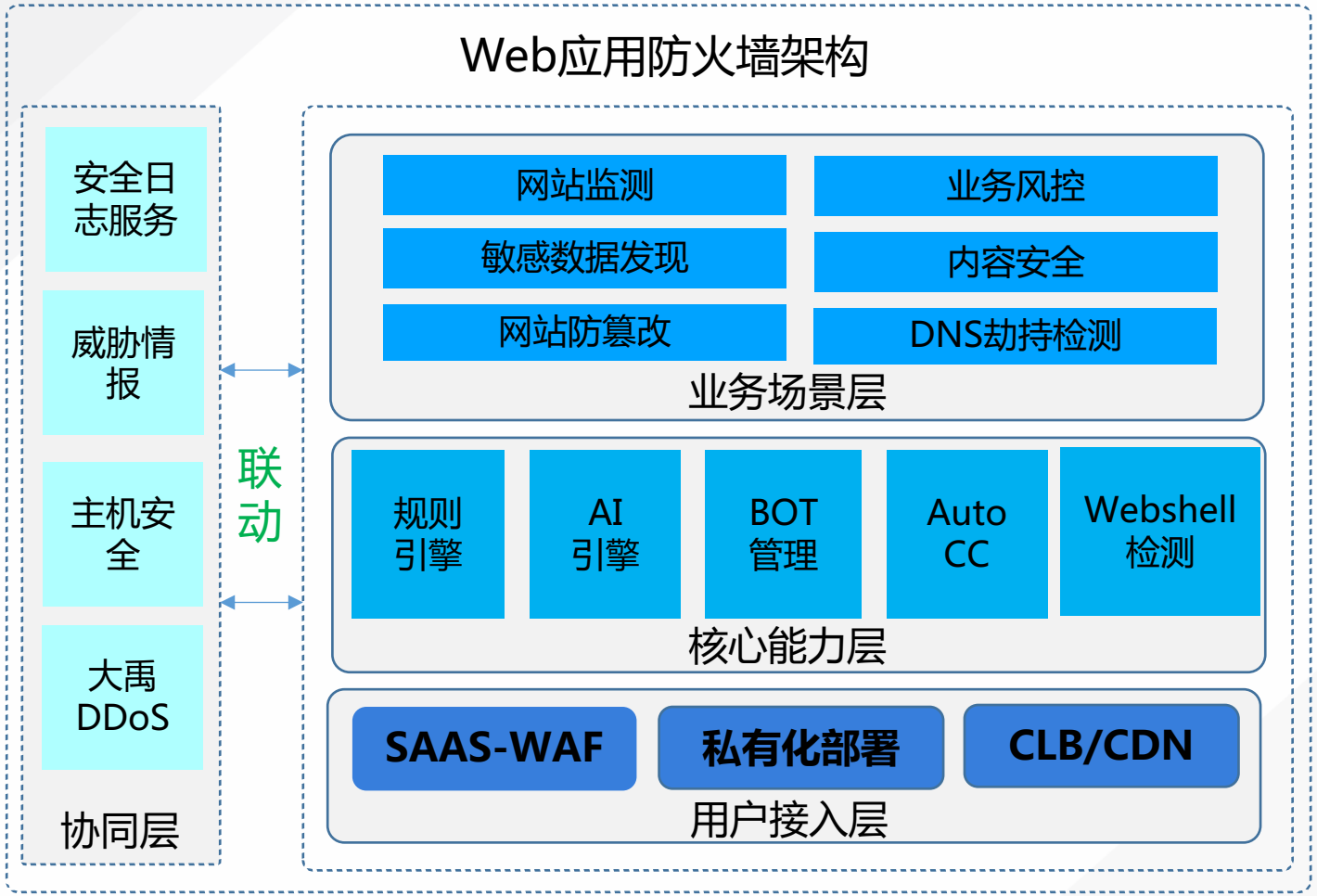


DNS劫持检测：对受护域名进行全国范围的 DNS劫持验证



腾讯云

腾讯云应用防火墙整体架构



用户接入层

WAF主要通过SAAS接入，根据业务场景不同，可选择私有化部署或和其他业务一起结合部署

核心能力层

- 规则引擎，零日漏洞更新
- AI引擎，自定义学习模型，入门简单，智能防护
- BOT管理，有效防护爬虫、机器人行为
- Auto CC，智能CC防护，多种验证方式
- Webshell检测，有效防御shell文件上传和传播

业务场景层

根据业务场景不同，提供差异的产品解决方案，例如：DNS劫持检测，数据防泄漏、网站防篡改、内容检测等功能。

协同层

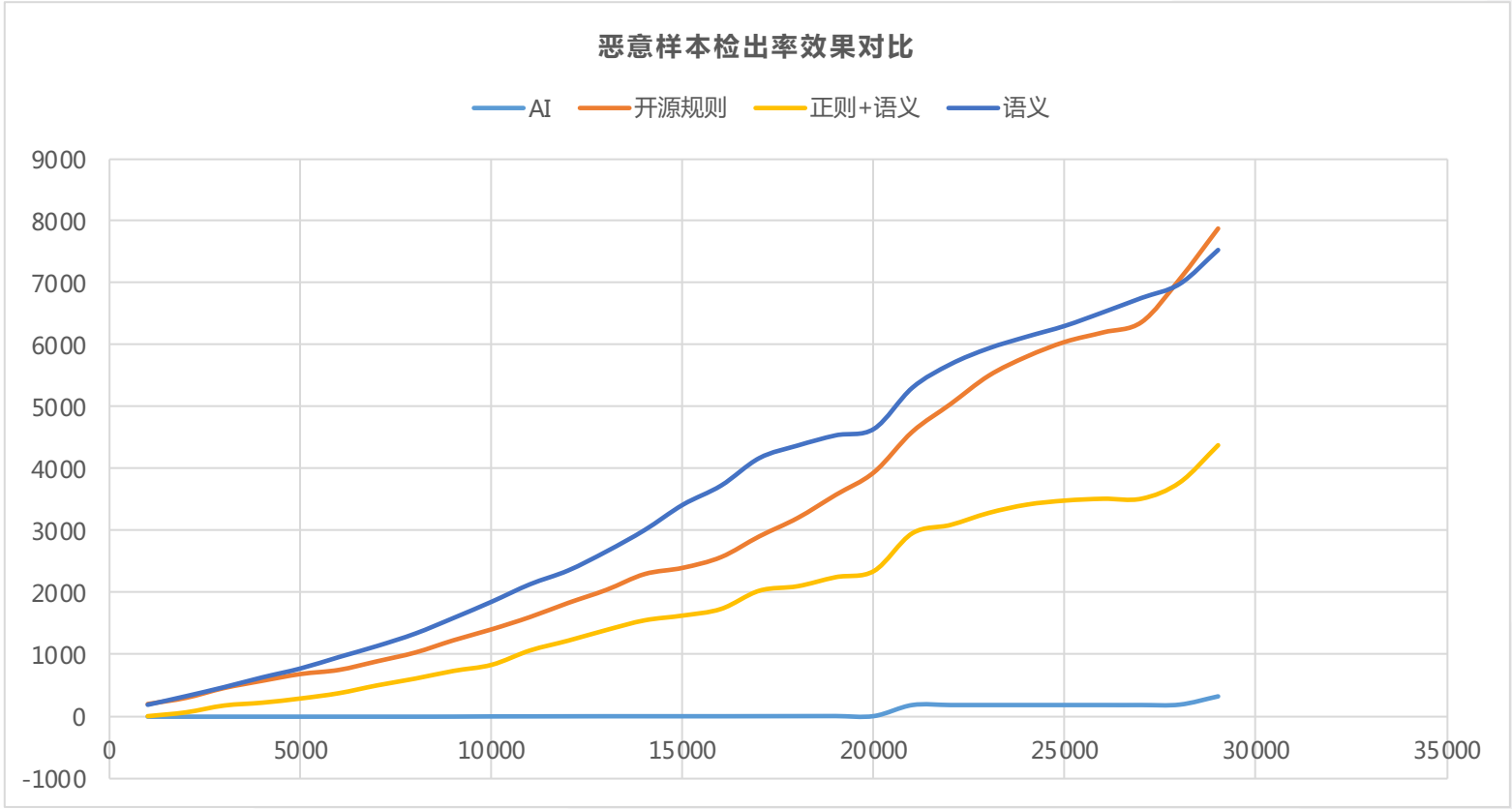
和云上安全产品联动防御，完成多点防御

03 核心优势

腾讯云 AI Web安全防护能力

腾讯云WAFAI引擎，通过智能解码，使用多种深度学习模型和算法策略，有效地进行异常检测和威胁识别，结合IP威胁情报数据，有效检测和拦截Web攻击行为。

测试集说明:
恶意载荷样本来自互联网收集，并大量选取了OWASP TOP 10攻击类型中，最典型也最常见的SQLI,XSS两种攻击类型数据，对各类引擎的检测能力对比。
腾讯云WAF的检测能力从78%提升到98%。



横坐标是验证的样本数目，纵坐标是漏报数目

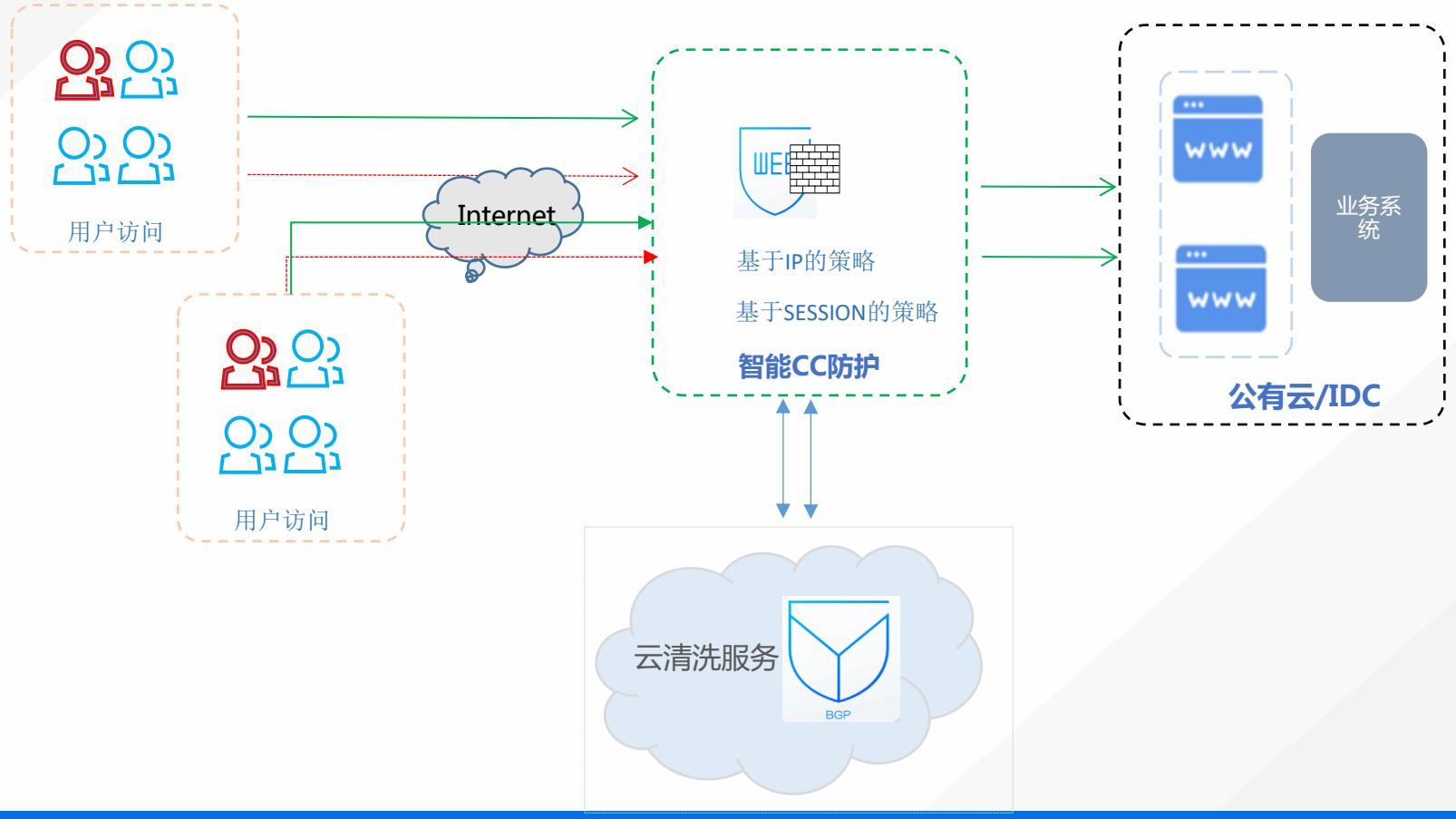
开源规则-72.82%　语义检测- 74.01%　规则+语义- 84.89%　AI引擎 - 98.77%

核心优势：

- 高检出率、快速响应、低运维成本
- 独立AI集群，资源有保障，AI大量计算过程不影响业务，RPC调度延时小于2ms
- 主动反馈，不同客户的模型不共享，用户反馈问题轻松处理

腾讯云智能CC防护策略

腾讯云智能CC防护，区别基于IP频率访问防御，支持基于AI行为分析的智能CC防护，同时支持基于 SESSION（cookie、post/get特征）防护，有效减低使用门槛，提升CC防御效果。一键腾讯云高防联动，构建完整网站DDOS攻击防护方案。



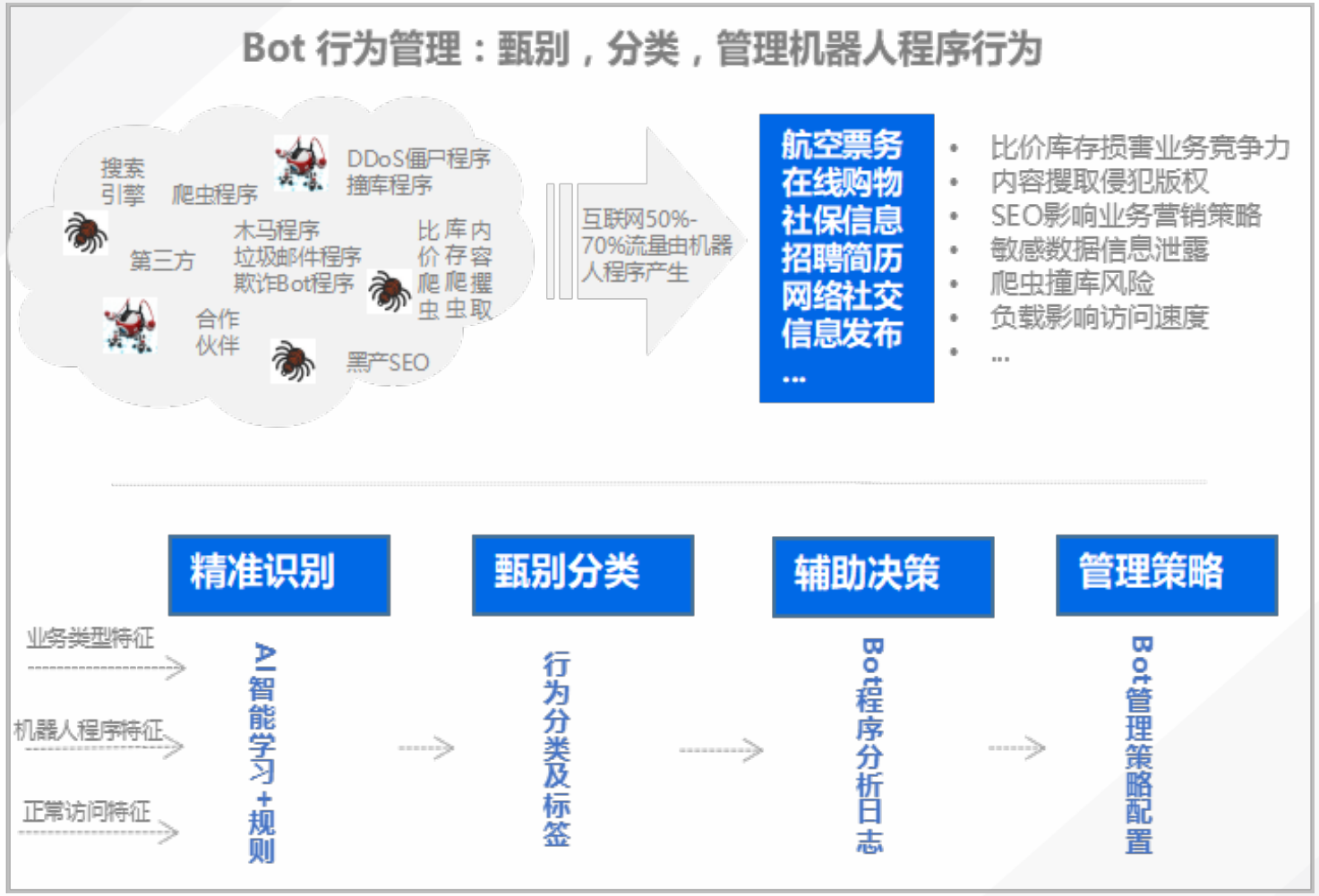
CC防御策略

- 基于IP频率的行为策略
- 基于SESSION的防御策略
- 智能CC防御
- 腾讯云高防联动

智能CC分析策略

- 访问源+HOST异常检测
- QPS历史行为和阈值检测
- HOST响应（499和504）分析检测

爬虫基础防护

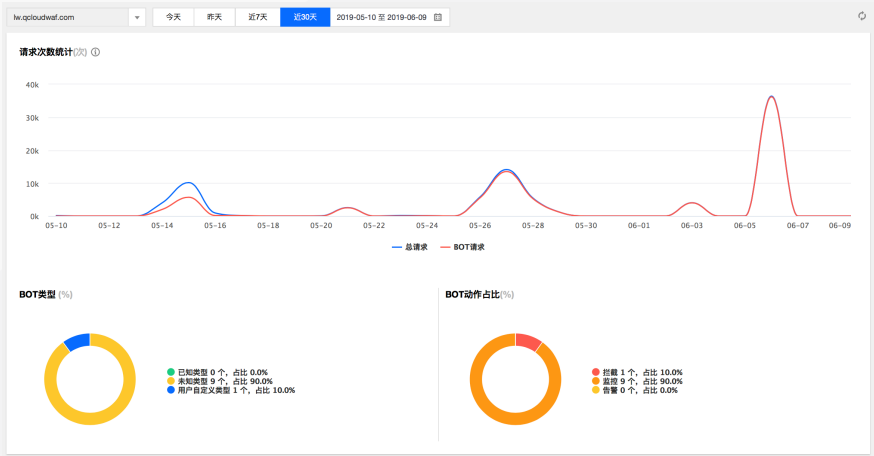


- 1000+BOT行为模型

  Feed fetcher, 广告,截屏工具，搜索引擎，站点监控，链接查询，工具类，漏洞扫描类，病毒查杀,网页爬虫，速度测试等爬虫类型

- 用户自定义BOT行为

  针对referer特征，UA特征，请求速率，次数，参数，路径特征，IP范围等定义Bot行为识别规则



爬虫防护高级防护对抗

腾讯云

体积 200KB

混淆前约200KB，集成到APK后执行proguard操作将更低

内存消耗 32KB

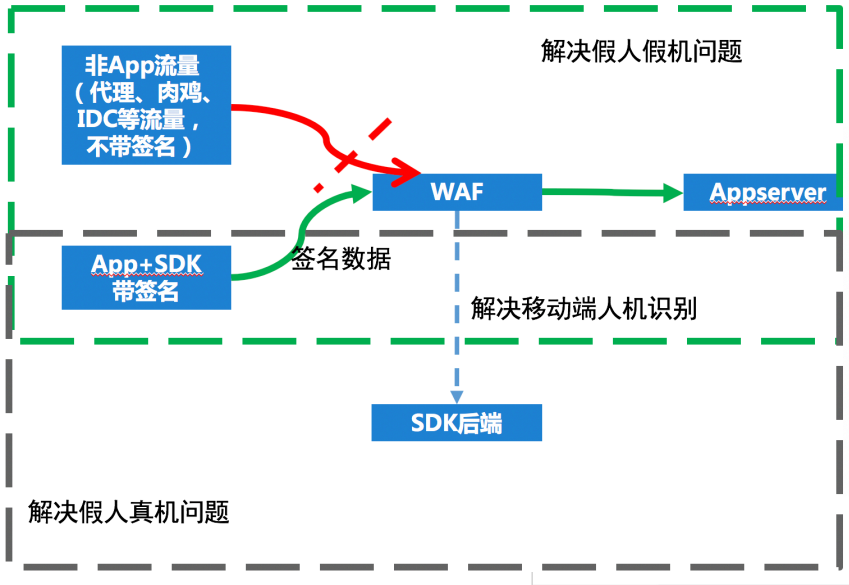
独立工作线程，避免主线程卡顿，仅采集过程工作，其它时间休眠

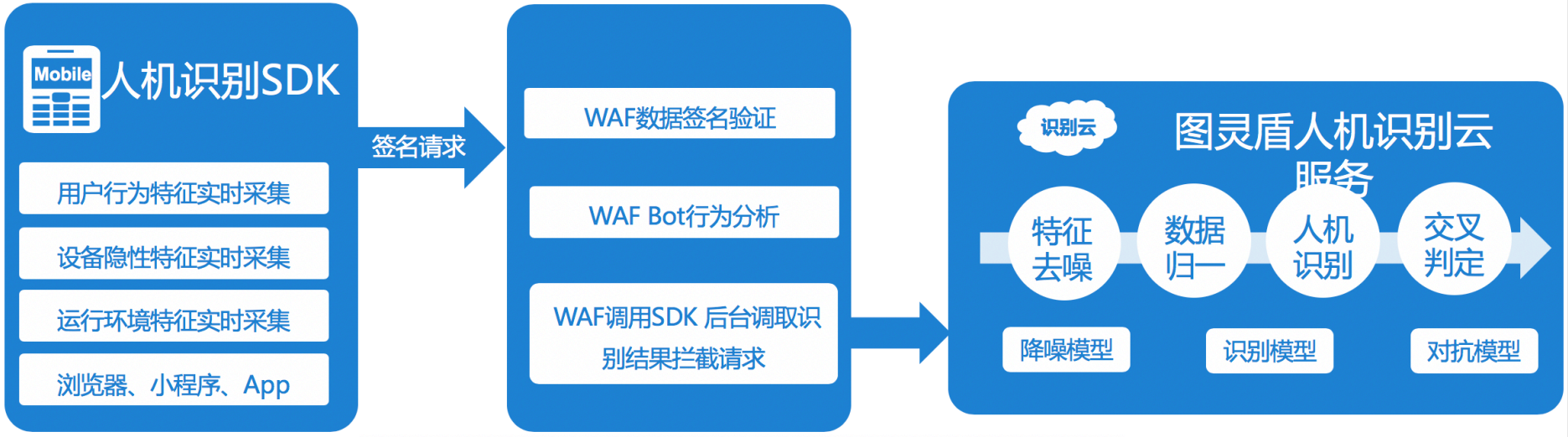
流量消耗 0.7KB 每单位时间(S)

平均单个用户采集6s数据即可判断，数据经过加密压缩传输，安全性有保障

响应时间 毫秒级

经过多次改良算法，计算时间大幅度缩减，可以做到毫秒级响应





高级对抗策略

- 通过在应用端集成行为分析SDK，对行为进行签名，保证行为可信
- 应用威胁情报，将全网已经受到的攻击云及时同步到业务端进行自动防护
- 识别真实设备，精准防护和拦截

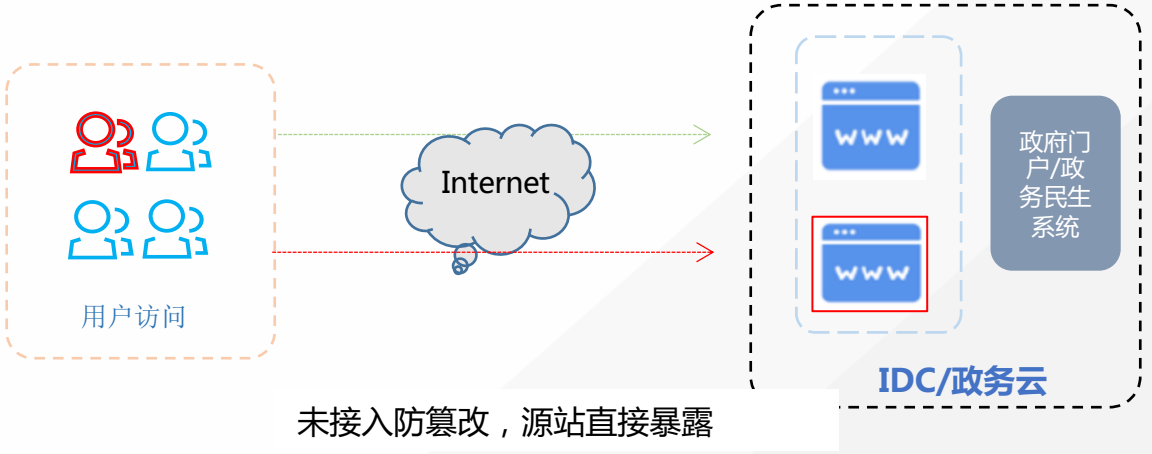
腾讯云

防篡改——一键网站镜像

腾讯云WAF+网站防篡改解决方案，通过镜像整个网站，实现网站防篡改保护，即使在源站未启用的情况也可以使用户访问不受影响。

腾讯网站防篡改保护

- 腾讯云网站防篡改镜像网站，**静态访问无需回源，动态访问安全回源**；极端情况网站被篡改，不影响用户正常访问
- 静态资源更新，手动进行，保障**用户访问页面经过审计**
- 资源刷新更新和Web防护记录日志，行为可追溯



未接入防篡改，源站直接暴露

接入防篡改，访问镜像，保护源

接入便捷

- SAAS接入，无需在WEB服务器上安装插件
- 一键添加网站目录即可，根据需要更新资源

04 案例和接入

WAF典型案例

金融类客户

腾讯云为微众银行全系列业务提供web应用防火墙服务，保障微众银行各项业务的快速发展。

腾讯云WAF为华侨永亨银行完善的网站漏洞入侵防护，保障华侨银行业务安全运行。

互联网客户

腾讯云为贝壳找房部分业务提供WAF服务，满足贝壳高并发场景下，拦截垃圾访问，保障业务正常。

为同程旅游提供基础安全防护和BOT防护，有效的保护网站安全运行，保护核心数据资产。

电商客户

使用智能CC防护、BOT防护进行黑产对抗对商品购物车、订单查询、支付页面保护。

腾讯云Web应用防火墙，为贝贝网提供网站商品图片信息、商品价格信息和交互记录数据防爬保护。

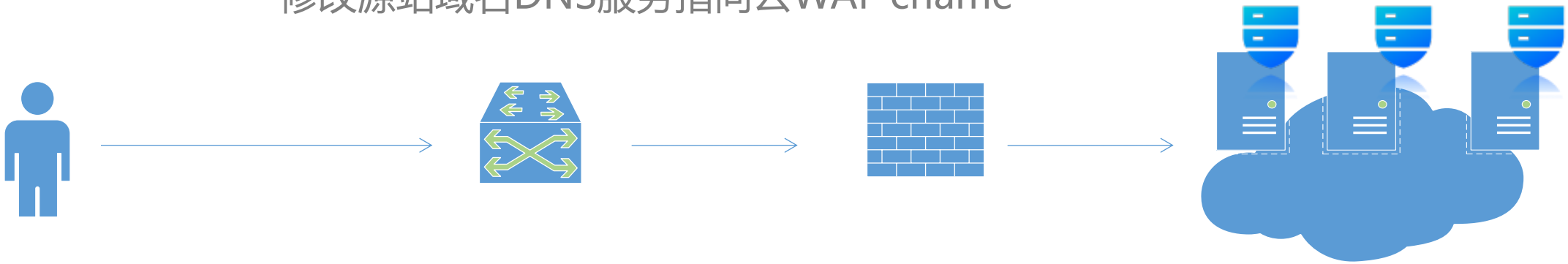
民生政务网站

为广东省政务云政务外网站点内容不会被黑篡改，民生服务正常可用，民众访问满意畅通，民生数据不被入侵窃取泄漏

结合腾讯云提供一体化的云平台方案及安全防护方案，云WAF保障政务云Web安全防护

抗DDOS+云WAF+主机安全方案

修改源站域名DNS服务指向云WAF cname



用户

高防包
(抗DDOS)

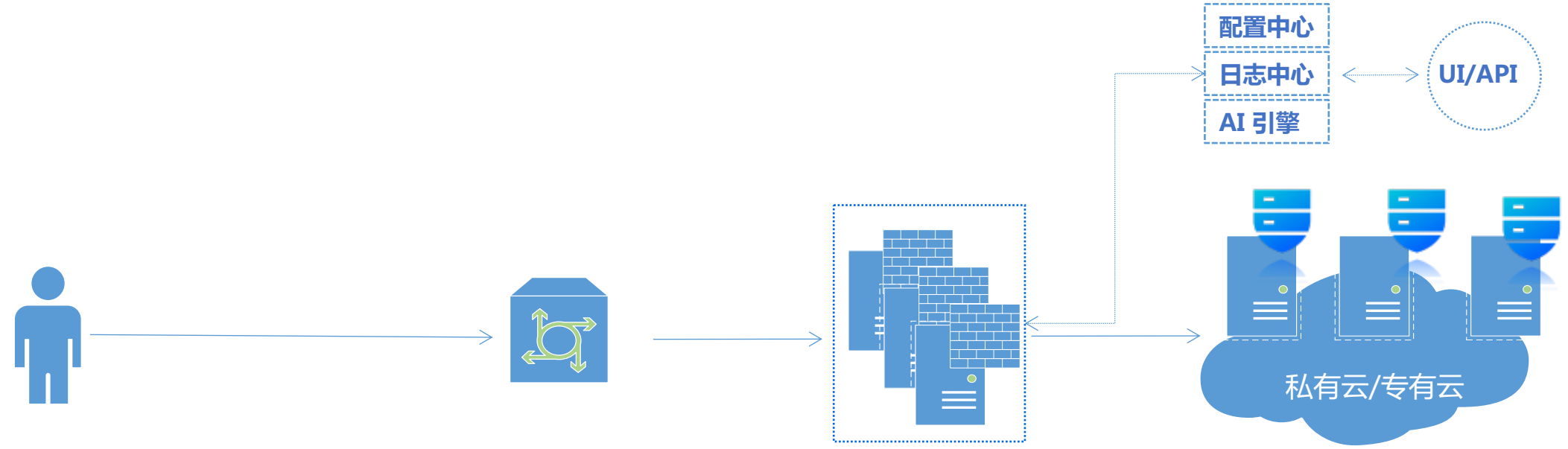
云WAF关联高防包

云WAF
(应用层安全防护)

源站：源站IP

源业务主机

支持私有化部署



应用先进检测技术

高可用，防护能力弹性伸缩

防护体系扩展能力强

FAQ

问题 1： 非腾讯云内的服务器能否使用Web应用防火墙(WAF)？

Web应用防火墙支持云外机房用户接入。Web 应用防火墙可以保护任何公网的服务器，包括但不限于腾讯云，其他厂商的云，IDC等，

注意： 在大陆地区接入的域名必须按照工信部要求进行 ICP 备案。

问题 2： Web应用防火墙（WAF）是否支持 HTTPS防护？

Web应用防火墙全面支持 HTTPS 业务。只需根据提示将 SSL 证书及私钥上传，或者选择腾讯云托管证书，Web 应用防火墙即可防护 HTTPS 业务流量。

问题 3： Web应用防火墙（WAF）QPS 限制规格是针对整个实例，还是配置的单个域名的 QPS 上限？

Web应用防火墙QPS 限制规格是针对整个实例。配置防护三个域名，则这三个域名累加的 QPS 不能超过规定上限。如果超过已购买的实例的 QPS 限制，将触发限速，导致丢包。

问题 4： Web应用防火墙（WAF）的源站 IP 可以填写 腾讯云CVM内网 IP 吗？

目前Web应用防火墙不支持填写CVM内网 IP。

问题 5： Web应用防火墙（WAF）可以直接利用高防包么？

可以，在高防包配置页面可以直接选择Web应用防火墙（WAF）实例的IP即可让Web应用防火墙具备高防能力

问题 6：Web应用防火墙（WAF）如何同 CDN 或 高防包 一起接入？

Web应用防火墙可直接将高防包叠加，CDN的源站指向Web应用防火墙（WAF）实例的VIP即可。

最佳部署架构：

客户端 > CDN > Web应用防火墙（WAF）+高防包 > 负载均衡 > 源站

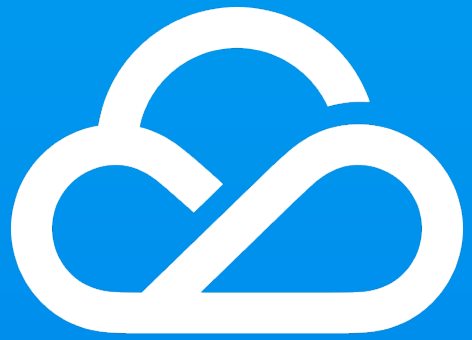
在客户需要CDN和高防能力时，只要将Web应用防火墙接入后提供的 CNAME 配置为CDN 的源站即可，同时可以将高防包叠加到Web应用防火墙（WAF）实例上。这样，即可实现经过 CDN 之后，被转发至Web应用防火墙（WAF）同时具备大流量DDOS的清洗能力，最终转发至源站，对源站行全面的安全防护。

问题 7：Web应用防火墙（WAF）能够保护在一个域名下的多个源站 IP 吗？

支持，一个 Web应用防火墙（WAF）域名防护最多支持 20 个。

问题 8：Web应用防火墙（WAF）配置多个源站时如何负载？

如果配置了多个回源 IP，Web应用防火墙（WAF）采用轮询的方式对访问请求进行负载均衡。



腾讯云

谢谢