腾讯云T-SecWeb应用防火墙-waf防火墙 web安全防护 Web威胁智能拦截

产品名称	腾讯云T-SecWeb应用防火墙-waf防火墙 web安全防护 Web威胁智能拦截
公司名称	昆山昱唯网络科技有限公司
价格	582.00/月
规格参数	品牌:腾讯云 产品:Web应用防火墙
公司地址	花桥国际商务城曹新路70号
联系电话	17601404160

产品详情

什么是 Web 应用防火墙

腾讯云 Web 应用防火墙（Web Application Firewall，WAF）是一款基于 AI 的一站式 Web 业务运营风险防护方案。通过 AI+规则双引擎识别恶意流量，保护网站安全，提高 Web 站点的安全性和可靠性。通过 BOT
行为分析，防御恶意访问行为，保护网站核心业务安全和数据安全。腾讯云 WAF
提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF，两种 WAF
提供的安全防护能力基本相同，接入方式不同。

SaaS 型 WAF 通过 DNS 解析，将域名解析到 WAF 集群提供的 CNAME 地址上，通过 WAF 配置源站服务器
IP，实现域名恶意流量清洗和过滤，将正常流量回源到源站，保护网站安全。

负载均衡型 WAF 通过和腾讯云负载均衡集群进行联动，将负载均衡的 HTTP/HTTPS
流量镜像到 WAF 集群，WAF 进行旁路威胁检测和清洗，将用户请求的可信状态同步到负载均衡集群进行威胁拦截或放行，实现网站安全防护。

腾讯云 WAF 可以有效防御 SQL 注入、XSS 跨站脚本、木马上传、非授权访问等 OWASP

攻击。此外还可以有效过滤 CC 攻击、提供 0day
漏洞补丁、防止网页篡改等，通过多种手段全方位保护网站的系统以及业务安全。

主要功能功能简介

AI + Web 应用防火墙	基于 AI + 规则的 Web 攻击识别，防绕过、低漏报、低误报、精准有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell 木马上传等 OWASP 定义的十大 Web 安全威胁攻击
0day 漏洞虚拟补丁	腾讯安全团队 7 * 24 小时监测，主动发现并响应，24 小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，受护用户无需任何操作即可获取紧急漏洞，0day 漏洞攻击防护能力，大大缩短漏洞响应周期
网页防篡改	用户可设置将核心网页内容缓存云端，并对外发布缓存中的网页内容，实现网页替身效果，防止网页篡改给组织带来负面影响
数据防泄漏	通过事前服务器应用隐藏，事中入侵防护及事后敏感数据替换隐藏策略，防止后台数据库被黑客窃取
CC 攻击防护	智能 CC 防护，综合源站异常响应情况（超时、响应延迟）和网站行为大数据分析，智能决策生成防御策略。多维度自定义精准访问控制、配合人机识别和频率控制等对抗手段，高效过滤垃圾访问及缓解 CC 攻击问题
爬虫 BOT 行为管理	基于 AI + 规则库的网页爬虫及 BOT 机器人管理，协助企业规避恶意 BOT 行为带来的站点用户数据泄露、内容侵权、竞争比价、库存查取、黑产 SEO、商业策略外泄等业务风险问题
30线 BGP IP 接入防护	WAF 支持防护节点 30 线独享 BGP IP 链路接入，节点智能调度，有效解决访问延迟问题，保障 1 ~ 18 线城市用户的站点访问速度，实现网站访问速度影响无感知的云 WAF 安全防护部署

为何需要 Web 应用防火墙

在以下场景中，使用 WAF 均可有效防御以及预防，保障企业网站的系统以及业务安全。

数据泄露（核心信息资产泄露）Web 站点作为很多企业信息资产的入口，黑客可以通过 Web 入侵进行企业信息资产的盗取，对企业造成不可估量的损失。

恶意访问和数据抓取（无法正常服务，被对手利用数据）黑客控制肉鸡对 Web 站点发动 CC 攻击，资源耗尽而不能提供正常服务。恶意用户通过网络爬虫抓取网站的核心内容（文学博客、招聘网站、论坛网站、电商内的评论）电商网站被竞争对手刻意爬取商品详情进行研究。羊毛党们试图搜寻低价商品信息或在营销大促前提前获取情报寻找套利的可能。

网站被挂马被篡改（影响公信力和形象）攻击者在获取 Web 站点或者服务器权限后，通过插入恶意代码来让用户执行恶意程序、赚取流量、盗取账号、炫技等；植入“ 黄、赌、非 ”链接；篡改网页图片和文字；对网站运行造成很大影响，损坏网站运营者的形象。对外公信力和形象蒙受损失。

框架漏洞（补丁修复时段被攻击）很多 Web 系统基于常见的开源框架如 Structs2、Spring、WordPress 等，这些框架常常爆出安全漏洞，但等待安装补丁的维护时段，则是一段艰难和危险的过程，很多攻击会漏洞公布之后一天内就遍地开花。

大流量 DDoS
造成业务中断为了使得竞争对手业务中断，或者造成关键门户网站不能访问，DDoS 攻击已经成为成本和门槛较低的攻击手段，对业务的连续性和品牌的影响极大，而且往往运营者在被攻击时很被动。

类型概述

腾讯云提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF。两种 WAF 的安全防护能力基本相同，但接入方式不同，适用场景不同，您可以根据实际部署需求选择不同类型的 WAF。

类别SAAS 型负载均衡型

适用场景 核心优势	适用所有用户，广泛覆盖腾讯云上和非腾讯云，通过 DNS 解析调度实现域名接入。
如何选择	若用户在腾讯云上和本地均有网站需要防护需求，或腾讯云上未使用七层负载均衡，推荐使用 SAAS 型 WAF。