GOODWAF 产品介绍

三分钟快速了解产品

产品介绍：

免费云 WEB 应用防火墙（GOODWAF）

Web 应用防火墙（云 WAF）结合人工智能机器学习技术、通过灵活的部署方式，构建积极防御安全模型。阻挡诸如 SQL 注入或跨站脚本等常见攻击，避免这些攻击影响 Web 应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险。实时拦截包括 0day 和已知攻击在内的不可信流量，保护关键业务的 Web 应用。

产品优势：

防御全面预置丰富的攻击特征签名库，可检测数十类的通用 Web 攻击特征，轻松阻断多种 Web 攻击。

配置灵活内置丰富的策略配置项，可根据自身业务特点灵活制定精细化防护规则，满足专业安全运维需求。

技术领先领先的语义+正则+AI（人工智能）三引擎架构，精准识别多种威胁，大幅提升威胁检出率。

零部署、零改造一键接入，快速开通服务，5 分钟即可完成全部安全策略配置，更快防护网站系统安全。

安全防护：

防护 OWASP 攻击防护 SQL 注入、XSS 跨站脚本、Webshell 上传、反序列化漏洞、XXE 攻击等。

精准访问控制基于丰富的字段和逻辑条件组合，打造强大的精准访问控制策略。

防护可视化数据详细的防护日志查询，可实时展示 Web 攻击信息（如攻击趋势、攻击详情、攻击类型、攻击来源等）和拦截情况。

Bot 行为管理精准识别爬虫 Bot 流量，并提供蜜网、观察、阻断、封禁、人机识别等多种管控手段。

页面加速支持后缀名、精准匹配、模糊匹配、目录、游客等多种缓存类型，支持 JS/CSS/HTML 网页资源压缩和 WebP 图片优化，有效减少网络传输资源大小。

双链路节点接入支持电信、联通双链路节点接入，智能优化链路选择，防止单线路节点故障导致业务中断。

IPV6 改造支持支持 IPV6 地址接入、改造，无需具备 IPv6 地址，通过接入 IPV4 地址就能轻松实现 IPV6 改造。

使用场景：

防数据泄露

黑客对金融、电商、医疗等数据密集型网站进行扫描，通过 SQL 注入等攻击手段入侵网站数据库，窃取业务核心数据。

智能规则+AI 双引擎防护 Web 攻击，阻断黑客攻击请求，防止网站数据被拖库；

WAF 内置防撞库、暴力破解等算法防止网站用户名、密码等信息被黑客暴力猜解，防止数据泄露。

防网页篡改、木马后门

政务门户、企业官网等网站被植入木马后，网页内容被篡改或植入暗链，后果严重。

智能规则+AI 双引擎防护 Web 攻击，阻断黑客攻击请求，防止网站被入侵导致被篡改；

基于大数据平台分析提取后门木马的访问行为特征，检测恶意代码，防止网站被木马后门攻击。

0Day 漏洞修复

第三方框架或插件爆发 0day 漏洞时，通过下发虚拟补丁，第一时间防护由漏洞可能产生的攻击。

无须等待厂商发布补丁，WAF 专业的防护团队第一时间下发虚拟补丁，更新防御规则，实现防护。

降低业务升级带来的部署和运维成本，避免服务中断带来的风险。