Web 应用防火墙

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-08-27 11:05:03

什么是 Web 应用防火墙（网站管家）

腾讯云 Web 应用防火墙（网站管家）（Web Application Firewall）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。
腾讯云网站管家可以有效防御 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、检测 DNS 链路劫持检测、提供 0day 漏洞补丁、防止网页篡改等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

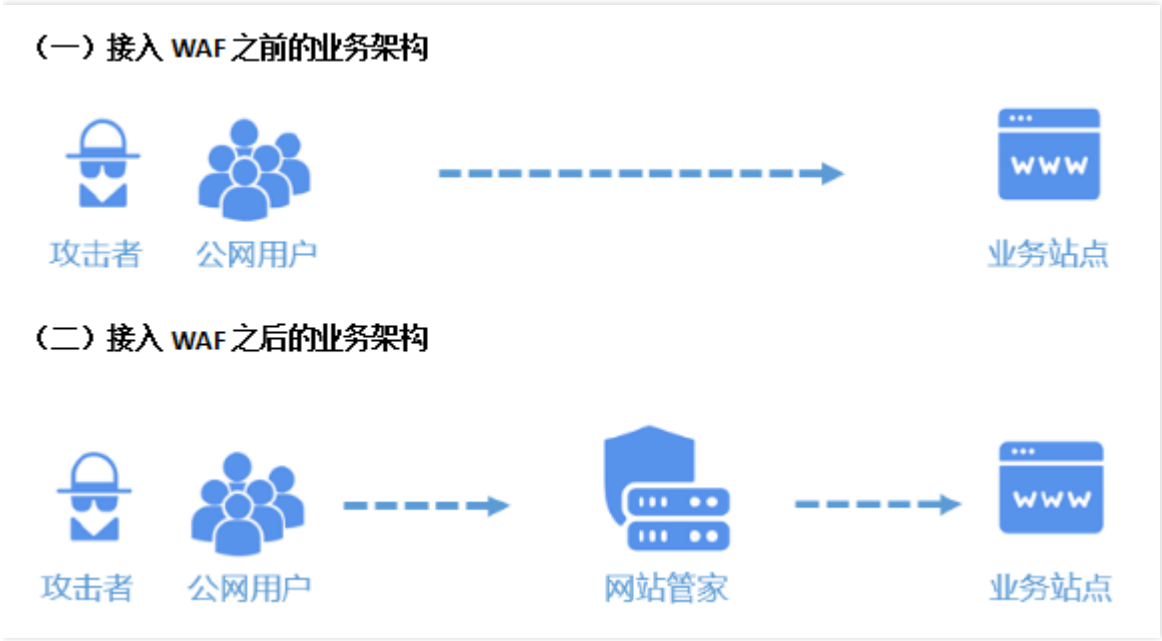
功能	简介
DNS 非法劫持检测	对客户提交的域名进行全国范围的 DNS 验证，感知并详细展示受护域名在各个地域的劫持情况，协助规避站点用户被恶意劫持给企业主带来的数据窃取及金融损失问题
30 线 BGP IP 接入防护	腾讯云 Web 应用防火墙（网站管家）支持防护节点 30 线独享 BGP IP 链路接入，节点智能调度，有效解决访问延迟问题，保障 1 ~ 18 线城市用户的站点访问速度，实现网站访问速度影响无感知的云 WAF 安全防护部署

为何需要 Web 应用防火墙（网站管家）

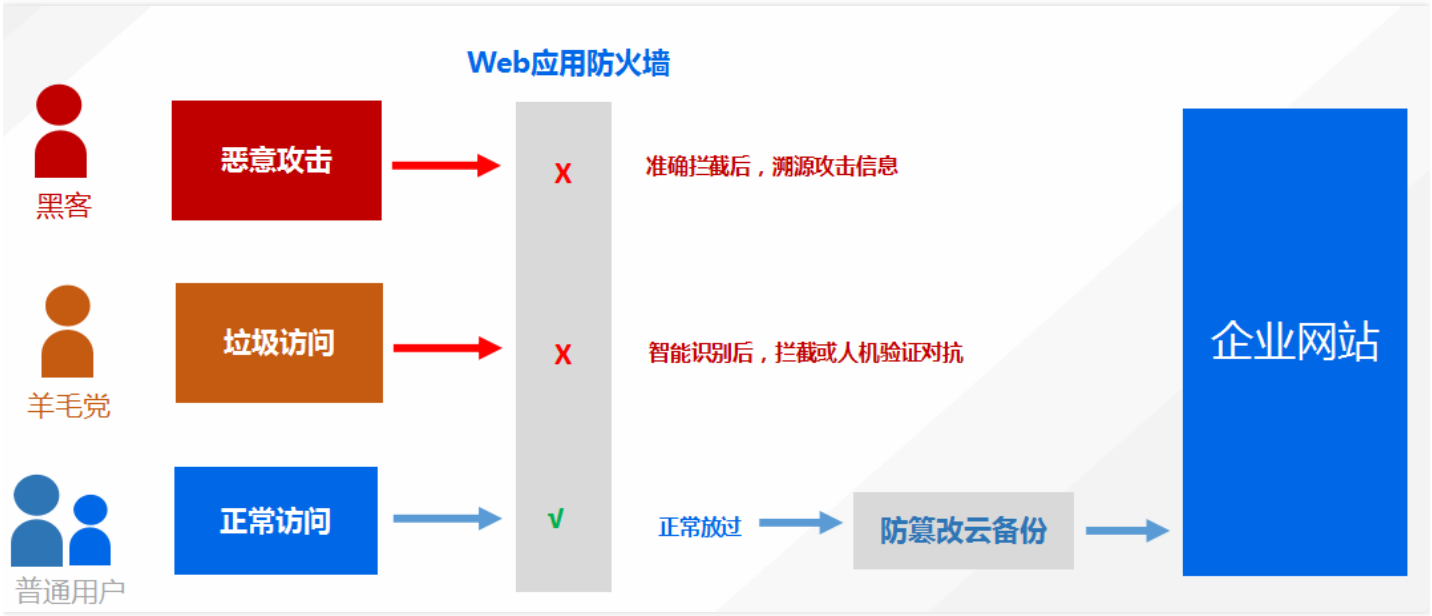
在以下场景中，使用腾讯 Web 应用防火墙（网站管家）均可有效防御以及预防，保障企业网站的系统以及业务安全。

- **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。
- **非法劫持（无法感知被劫持情况）**
  为了获取流量，或者为了增加广告收入，网站的正常 DNS 请求得不到正常的回应，或者访问的内容被恶意修改，都是网络上常见的劫持现象，网站运营者往往只有在客户投诉的时候才能知道，无法从服务端感知此类现象。
- **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。

基本防御流程



腾讯 Web 应用防火墙（网站管家）防御示意图：



产品优势

最近更新时间：2019-10-08 10:46:54

Web 应用防火墙（网站管家）优势如下：

优势	简介
快速威胁感知	拥有敏锐的威胁感知触角，可以充分应用腾讯大数据威胁情报，第一时间感知威胁。
持续威胁对抗	拥有强大的威胁对抗技术，由腾讯安全团队联合实验室持续输送安全防护能力。
业务风险防护	可以为您提供 BOT 行为管理、DNS 劫持监测、垃圾访问过滤等功能，以满足业务安全运营防护需求。
最低防护延迟	30线 BGP 线路接入防护，降低服务延迟，保障受护业务访问速度。
无缝扩展防护	一键无缝接入百 G 抗 DDoS 攻击能力，轻松应对敏感大流量 DDoS 攻击问题，无惧突发风险。

应用场景

最近更新时间：2018-12-07 15:59:28

政务网站防护

- 一键接入防御，轻松配置，隐藏并保护源站，保证网站内容不会被黑客入侵、篡改。保障网站信息正确，政府服务正常可用，民众访问满意畅通。

电商网站防护

- 持续优化防护规则、精准拦截 Web 攻击，全面抵御 OWASP Top 10 Web 应用风险。
- 在高并发抢购场景下，可智能过滤恶意攻击及垃圾访问，保障正常访问业务流畅。

金融网站防护

- 一键接入防护，可跟大流量 DDoS 防御有机结合，同时具备 Web 安全防护。
- 有效监测 DNS 链路劫持，防止网站流量被恶意指向。
- 可有效检测撞库等异常访问，保护用户信息不外泄。
- 云端资源优势，自动伸缩，轻松应对业务突发，大流量 CC 攻击。

防数据泄密

- 避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。
- 防 CC 攻击：防恶意 CC（http get flood），通过在四层和七层阻断海量的恶意请求，保障网站可用性。