云WAF 产品白皮书V3.0

网世界 心归宿

网宿科技 全球领先的互联网基础设施平台

关注公众号，及时了解网宿产品与服务动态

400-010-0617 | www.wangsu.com

Content 目录

网宿云 Web 应用防火墙（Web Application Firewall，简称 WAF）是“网宿网盾”品牌旗下的专业云防护产品之一。不需要客户端部署软硬件，即可享受针对 SQL 注入、XSS、CSRF 等 OWASP TOP10 中的 WEB 应用安全威胁及目录遍历、网站扫描等其它安全威胁的防护，从而减少网站出现拖库、篡改、机密信息泄漏等安全风险。网宿 WAF 防护产品所涉及到的客户端会话识别技术、网络爬虫识别等技术，获得了多项国家技术专利。

“网宿网盾”是网宿科技发布的云安全全新品牌，其业务全景主要覆盖网络安全、业务安全、内容安全、DNS 安全、源站可用性、传输安全、安全管理和安全评估等八大领域，“网宿网盾”依托高容量节点和自主研发的安全技术，构建出一套云端智能安全体系。

1. 行业现状和挑战

随着互联网的高速发展，基于 Web 服务的应用程序被广泛应用于政府机构、商业、金融等各个重要领域。Web 应用为整个互联网的发展增添了不少活力，然而，由于各类 Web 应用系统的复杂性和多样性导致系统漏洞层出不穷，随之而来的信息安全问题也日益突出。

1.1. Web 应用攻击形势严峻

Web 应用面临的安全威胁主要如下：

- **网站被篡改**

网站被篡改数量日益增多，根据 CNCERT 发布的《2016 年中国互联网网络安全报告》显示，2016 年，我国境内被篡改的网站数量为 16758 个，其中政府网站被篡改数量为 467 个；而网站被篡改不仅会使网站蒙受损失，同时还影响政企公开社会形象。

- **网站敏感信息泄露**

网站敏感信息泄露事件频发，如 2016 年 12 月，京东 12GB 用户数据遭泄露，身份证、密码等信息无一逃脱；同月，雅虎再次爆出数据泄露事件，涉及 10 亿账户；而由于敏感信息泄露引发的侵权、欺诈等非法行为，不仅会造成被窃取用户的个人利益损失，也会造成企业的经济损失。

- **网站挂马**

根据 CNCERT 监测发现，2016 年约 4 万个 IP 地址对我国境内 82072 个网站植入后门，其中政府网站有 2361 个，境外有约 3.3 万个 IP 地址通过向网站植入后门对境内 6.8 万个网站进行远程控制。

1.2. 漏洞频发修复成本高

随着漏洞挖掘技术的不断发展，攻击工具日益专业化、易用化，一些被广泛使用的基础组件的漏洞爆发频率越来越高，如 Bash 的 ShellShock 漏洞、OpenSSL 的 HeartBleed 漏洞、Struts2 的远程任意代码执行漏洞等，影响范围广、修复成本高。

1.3. 国家立法安全政策

国家不断开展信息安全工作，对信息安全重视程度达到前所未有的高度。

2014 年，国家主席习近平在中央网络安全和信息化领导小组第一次会议提出“没有网络安全就没有国家安全”；

2015 年 11 月，工商总局印发《关于加强网络市场监管的意见》，全面加强网络市场监管，推进“依法管网”、“以网管网”、“信用管网”和“协同管网”；

2016 年上半年，经中央网络安全和信息化领导小组同意，中央网信办、教育部、工信部、公安部、新闻出版广电总局、共青团中央等六部门联合印发了《国家网络安全宣传周活动方案》。方案明确从今年开始，网络安全宣传周于每年 9 月第三周在全国各省区市统一举行；

2017 年 6 月 1 日，我国《网络安全法》正式实施。

1.4. 传统防护方式存在瓶颈

传统防御 WEB 应用攻击的方法是购买 WAF 硬件设备，这种方法虽然能一定程度上缓解攻击，但是存在以下瓶颈：

- **部署不便，运维难度大**

硬件设备的部署需要对网站的网络拓扑做变更，变更工作量大，且部署过程中存在系统和业务风险。当设备出现问题时，受限于物理空间等因素，难以及时解决。此外，遇到攻击，需要专业安全团队进行设备监控、策略调整和升级维护。

- **防御策略更新慢**

硬件设备受限于数据来源和数据采集分析能力，无法很好整合数据资源，且具有封闭性，防御算法更新慢，难以形成联动防御，进而影响到 0 day 攻击的响应速度。

2. 产品介绍

2.1. 产品简介

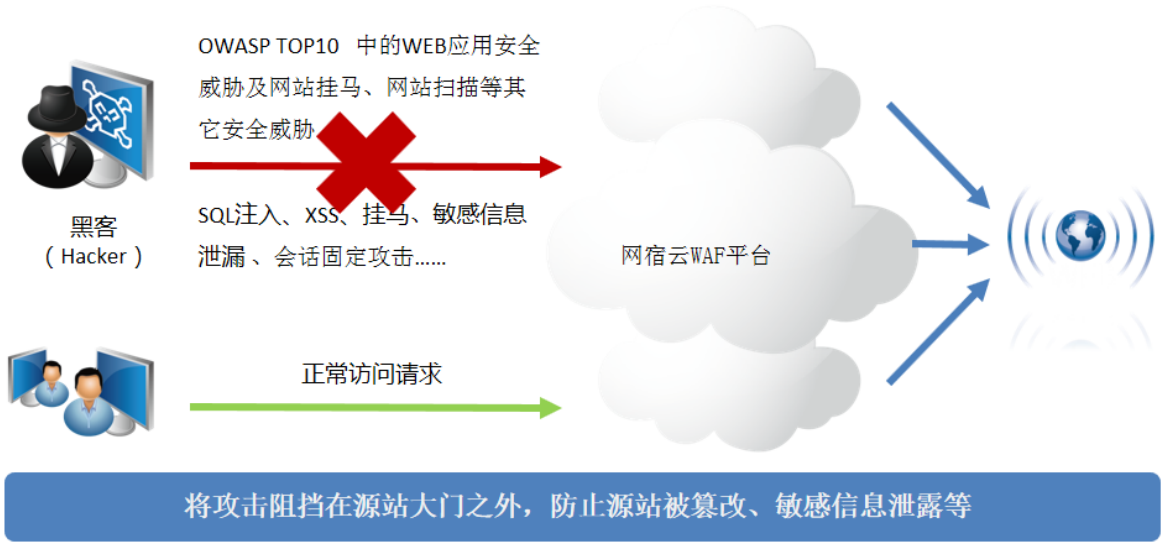
网宿云 WAF 依托全球部署的云安全节点联接形成云安全网络，结合云端大数据分析平台，提供 OWASP Top10(SQL 注入、XSS 跨站脚本、常见 Web 服务器漏洞、非授权核心资源访问等)、网站扫描、网站挂马等各类常见 Web 应用攻击的防护，同时，能够基于自学习防护引擎及时发现 0 Day 攻击并防护，避免用户网站被篡改、敏感数据泄露，从而保障网站安全。

2.2. 产品技术架构

- **产品网络拓补图**

网宿云 WAF，依托网宿全球部署的云安全节点联接形成云安全网络，并配以专有的攻击监控报警中心和智能决策中心，结合云端大数据分析平台，实时检测分析请求包，对 SQL 注入、XSS 跨站、命令注入等常见 Web 应用攻击进行阻断，对正常用户请求进行回源，避免用户网站被篡改、敏感数据泄露，从而保障网站安全。

网宿云 WAF 的网络拓扑图如下图所示：



◆ **产品防护架构**

传统 WAF 防护一般是依赖于协议合规校验、攻击特征的规则匹配等为主要技术手段来进行攻击防护，用于保证 Web 业务和资产的信息安全。然而，此类被动防御的技术手段存在着一些弊端，攻击特征的提取永远滞后于攻击本身，导致 WAF 不能及时应对如 0Day 漏洞的攻击和各类 bypass 攻击。

基于此背景，网宿云 WAF 采用了“黑名单（攻击特征库）+白名单（自学习防护引擎）”的防护架构：

➢ 黑名单技术

网宿云 WAF 基于平台的大数据分析引擎分析历史攻击事件，同时通过安全漏洞平台&漏洞社区进行漏洞采集，提取各类攻击的特征形成黑名单规则库（攻击特征库）；基于该黑名单规则库对访问请求进行实时检测和分析，如果请求中匹配了黑名单中的攻击特征则直接进行阻断。

➢ 白名单技术

网宿云 WAF 会通过自学习网站正常流量的特征，构建被防护网站的应用程序结构、正常用户访问的流量、正常业务逻辑的数据模型，形成白名单规则库；基于该白名单规则库对访问请求进行实时检测和分析，如果请求不符合网站的白名单特征则采用直接阻断或进一步严格检测等方式对异常请求进行处理。

基于“黑名单（攻击特征库）+白名单（自学习防护引擎）”的防护架构，利用了被动防御技术+主动防御技术，不仅能够解决已知的安全风险，同时能够快速应对新型攻击(旧漏洞攻击的变种与 0Day 攻击)。

2.3. 产品适用行业与场景

WAF 面向的行业及使用场景包括但不限于：

◆ **政企行业**

门户网站作为政府、企业提供给互联网用户获取信息服务的重要渠道，将面临网页被篡改、网页挂马、SQL 注入攻击等多种安全问题，同时也面临上级单位和测评机构的安全检测的压力。一旦发生安全事件，将严重影响其形象和公信力。

◆ **金融行业**

金融行业面临注入、跨站等多种安全问题，导致用户账号密码泄露，危及用户资金财产安全，进而严重影响企业的形象并承受经济损失。

◆ **电商行业**

电商行业为 Web 应用攻击的重点对象，经常遭受黑客攻击，譬如非法篡改交易数据、盗取用户个人账号信息进行网络诈骗等，不仅危害了用户的个人利益，同时也严重影响了商家的形象。

◆ **航空行业**

航空行业、互联网售票平台等都拥有大量的旅客个人信息以及出行/未出行行程信息，而这些信息经过黑色产业链，最终形成了退改签等诈骗活动，不仅危害了旅客的个人利益，也给各平台造成了经济损失。

3. 产品功能

网宿云 WAF 包括监控报警、WEB 应用攻击防护、自学习防护引擎、“高效”补丁漏洞修复、网站精准访问控制、防护数据可视化等功能，保障各行业的数据安全。

3.1. 监控报警

能够为用户提供多维度全方位的监控报警服务，包括攻击监控报警、网站可用性监控、安全预警和节点服务质量监控，保障用户能够第一时间掌握网站各种异常情况。

- **攻击监控报警**

网宿云 WAF 提供全方位的攻击监控报警功能，各安全节点通过动态学习客户的历史访问日志（如客户每个资源的访问量、行为特征等），建立访问基线。通过动态基线学习和日志分析，识别出攻击特征，当检测到异常访问时，根据报警规则发送相应攻击报警。

- **网站可用性监控报警**

包括 HTTP/HTTPS 监控、PING 监控。

- HTTP/HTTPS 监控

通过周期性模拟访客请求访问被监控站点，通过分布在全球各地的监控节点实时获取站点的响应状态和请求详情，如发现网站出现响应异常情况，将通过邮件、短信等渠道告知站点相关人员，帮助站点人员第一时间察觉网站异常。

➢ PING 监控

通过周期性探测被监控的主机或者站点连通性，获取站点/服务器的连通状态、丢包率、RTT 响应时间等信息，并结合实时报警模块，通过邮件、短信等渠道将链路异常信息告知客户相关人员。

◆ **安全预警**

网宿云 WAF 通过大数据分析平台对云端攻击数据进行分析，提取其攻击特征（如 IP、UA、Refer 等），并可查看采用同类型攻击手法的多网站数据及行业数据，进行安全事件关联分析，进而全网下发防护策略，联动防御，并对可能遭受攻击的行业提前配置安全防御体系，防患于未然。

◆ **节点服务质量监控**

网宿云 WAF 提供 7*24 小时全网节点监控，能够基于服务质量（如根据各节点的负载、流量等）智能调度服务节点，保障服务实时稳定可用。

3.2. Web 应用攻击防护

网宿云 WAF 提供对常见各类 Web 应用攻击的防护，主要包含以下几类：

以下将针对各类攻击进行详细介绍。

3.2.1.HTTP 请求合规检测

- 攻击原理

黑客常常发送不符合 HTTP 协议规范的请求，企图探测 Web 服务器信息，或绕过网站的防护策略实施攻击。

- 防护原理

网宿 WAF 支持对 HTTP 请求做合规性检查，针对 HTTP 请求，网宿 WAF 可以检查请求头部完整性，并对请求信息中的请求方法、协议版本以及请求的请求头长度、参数个数、参数名长度等进行限制。对于检测出的不合规请求，可以进行报警、拦截并记录相应日志，在保障 Web 应用正常服务的基础上，最大程度上过滤了对 Web 应用的不合规访问，降低了 Web 应用被攻击的风险。

Web 过滤防护过程如下图所示：

3.2.2.注入类攻击防护

注入类攻击主要包括 SQL 注入、命令注入、XPATH 注入、LDAP 注入、SSI 注入等。

➢ 攻击原理

注入类攻击是利用 Web 应用程序对请求输入数据过滤不严的弱点，对不同的目标进行攻击的手段。如 SQL 注入攻击是利用 Web 应用程序对涉及数据库操作的输入数据过滤不严的漏洞，将恶意的 SQL 命令注入到后台数据库引擎执行，达到窃取、控制数据甚至控制数据库服务器的目的。

➢ 防护原理

网宿云 WAF 采用自主研发的特征识别引擎，将完整的 HTTP 请求做最细粒度拆分，高效并行检测拆分后所有可能存在攻击的区域(如 URL、参数、请求体、请求头等)，判断各区域是否匹配攻击特征，能够对各类注入类攻击进行有效防御。例如，被防护某个站点的请求为 http://www.test.com?a=1' or 1=1，网宿云 WAF 对请求各个区域进行拆分检测后，判断出该 URL 请求中参数 a 的值为“1' or 1=1”，匹配了攻击特征库中 SQL 注入特征，则对该请求进行阻断。

3.2.3.跨站脚本类攻击防护

跨站脚本类攻击主要包括：XSS（跨站脚本攻击）、CSRF(跨站请求伪造)。

- 攻击原理

XSS 跨站脚本攻击，是指恶意攻击者利用 Web 应用程序对需要输出到网站页面中的用户输入过滤不严的问题，向网站返回的页面中插入自己的代码，达到修改响应页面内容、窃取用户 Cookie 等目的。

CSRF 跨站请求伪造，是指恶意攻击者让用户在不知情的情况下点击攻击者构造的恶意链接，以合法用户的名义发送恶意请求，完成了攻击者所期望的一个操作。例如，用户已登录某银行，同时又在另一个网站点击了非法者构造的图片（点击该图片则触发执行某银行转账的操作），该用户即在不知情的情况下自动完成被攻击的过程。

- 防护原理

XSS 跨站脚本：网宿云 WAF 采用自主研发的特征识别引擎，将完整的 HTTP 请求做最细粒度拆分，高效并行检测拆分后所有可能存在攻击的区域(如 URL、参数、请求体、请求头等)，判断各区域是否匹配攻击特征，能够对各类注入类攻击进行有效防御。例如，被防护某个站点的请求为 http://www.test.com?a= '><script>alert(document.cookie)</script>，网宿云 WAF 对请求各个区域进行拆分检测后，判断出该 URL 请求中参数 a 的值为“'><script>alert(document.cookie)</script>”，匹配了攻击特征库中 XSS 攻击特征，则对该请求进行阻断。

CSRF 跨站请求伪造：网宿云 WAF 通过判断用户的页面访问逻辑来防护，例如用户在执行某些关键操作时（如银行转账等），可设置请求的 referer 值必须为本站点的 URL 链接才是合法的。

3.2.4.扫描类攻击防护

- 攻击原理

扫描类攻击主要包括“扫描器扫描”和“恶意爬虫”两类。黑客攻击网站的第一步经常是通过利用爬虫或扫描工具，获取网站信息，探测网站存在的漏洞。

- 防护原理

网宿云 WAF 能够直接识别常见的恶意爬虫和扫描工具发出的请求，直接阻断其访问。例如，Appscan 扫描器发起的请求一般在头部 User-Agent 参数值中会包含 appscan 字符串，网宿云 WAF 可对请求头部进行检测并识别出扫描器攻击。

对于比较新型的恶意爬虫和扫描工具，网宿 WAF 可以利用庞大的攻击特征库拦截工具发出的恶意请求。

3.2.5.网站挂马类防护

- 攻击原理

网站挂马主要指攻击者在利用漏洞获取网站服务器权限后，在网站上安装攻击者自己的程序，以便后续的攻击过程中可通过这个程序实现对网站的控制及管理。

- 防护原理

网宿 WAF 对网站挂马的防护主要分为两个维度进行全面检测：

1. 阻止后门木马被上传

网宿云 WAF 可通过多种途径防止后门木马程序被上传到网站上。一方面可以对上传的内容进行检测，对于已知的后门木马程序及一些包含可疑代码的文件进行识别及拦截；另一方面，可以禁止 ASP、PHP 等动态脚本上传。

2. 阻断已上传后门木马被利用

针对已经上传到被防护站点的后门木马(可能是在网站部署安全策略之前或是攻击者通过内网或其它系统/程序漏洞方式)，网宿云 WAF 基于大数据平台分析提取后门木马的访问行为特征，并对被防护站点的历史请求日志进行分析是否符合后门木马访问特征(例如后门木马文件可能是孤立文件，且只有少数 IP 访问等)，并对可疑的请求响应内容进行后门木马关键字匹配，来检测是否有攻击者试图访问已存在的后门木马。

3.2.6.授权和认证类攻击防护

➢ 攻击原理

Web 应用的权限划分及其实现往往存在疏忽和缺漏，留给黑客可乘之机。黑客可以使用精心构造的请求绕过网站的权限控制，获取用户或者网站管理的权限，并以此为基础进行进一步的攻击。这类的攻击主要包括 Cookie 安全、会话固定、会话劫持、目录遍历等几类。

Cookie 篡改及盗用：攻击者通过修改 Cookie 获得用户未授权信息，进而盗用身份的过程。

会话固定攻击：攻击者利用服务器的 Session 不变机制，诱导受害者使用攻击者指定的会话标识，从而获取合法会话标识的过程。

会话劫持：攻击者通过获取用户会话标识后，伪装成合法用户登陆目标账号进行攻击。

目录遍历： 攻击者通过在 URL 或者参数中构造“../”等，完成目录跳转，来获取服务器上本不可访问的文件访问权限。

➢ 防护原理

网宿云 WAF 能够对这些未经授权的恶意请求进行检测并阻断。具体如下：

会话劫持：网宿云 WAF 可对涉及用户权限的会话标识进行保护，防止会话标识被攻击者窃取导致的会话劫持。

Cookie 安全：网宿云 WAF 可对网站下发的 Cookie 设置额外的安全保护策略，检测并预防攻击者对 Cookie 的篡改及盗用。

会话固定：网宿云 WAF 可通过对会话标识的管理，防止以窃取用户权限为目的的会话固定攻击。例如，网宿云 WAF 会把用户是否登录成功等信息加入会话标识中，避免黑客诱导用户用指定会话标识登录而获取用户的账号登录权限。

目录遍历：网宿云 WAF 可检测并阻断跨目录越权访问的请求，保证网站的重要信息在未经授权的情况下不被访问。

3.2.7.Web 框架类攻击防护

- 攻击原理

Web 框架类攻击主要是指针对常见的 CMS 建站系统和开源 Web 应用开发组件的攻击。由于这些建设系统或开源组件被广泛应用在各类网站的开发建设中，一旦被曝出漏洞且没有提前采取防护措施，后果将不堪设想。

- 防护原理

网宿 WAF 能够防护已知的 Web 框架类漏洞，例如：aspcms、phpcms、dedecms、ecshop、phpweb、FCKEditor、eWebEditor、struts2、phpmyadmin 等。同时，还可以基于对大量监控数据的实时分析，可以第一时间发现并防护新出现的漏洞，保障网站底层框架的安全。

3.2.8.敏感信息泄露防护

- 攻击原理

攻击者会通过各种方式去窃取网站的敏感信息，一方面是窃取站点内容的敏感信息并加以利用，如密码、配置、备份、数据库等；另一方面是获取站点异常的敏感信息并加以利用，如攻击者可构造

错误的数据库语句使得站点返回数据库错误信息，根据错误信息提示获取到站点所使用的数据库软件以及对应版本等信息，便可以利用该版本数据库存在的漏洞进行攻击。

- 防护原理

网宿云 WAF 采用多种机制进行敏感信息泄露防护，一方面可以检测并阻断对敏感信息的请求，另一方面可检测并阻断包含网站敏感信息的 HTTP 响应。主要的防护机制包括：

1. 服务器敏感信息防护：网宿 WAF 可阻止网站因异常或配置错误向外界泄露包含程序、系统敏感信息（如 Web 服务器错误信息、数据库错误信息、应用程序错误信息等）。
2. 状态码防护：针对服务器经常返回的 4 和 5 等敏感响应码，网宿 WAF 也可支持告警或者拦截，进一步避免服务器敏感信息泄露。
3. 敏感文件下载防护：网宿 WAF 可阻止攻击者对网站上敏感信息（如密码、配置、备份、数据库等）进行下载尝试。
4. 网宿云 WAF 还支持客户自定义敏感关键字，如响应中存在敏感关键字，网宿云 WAF 将自动阻断非法内容被用户浏览。

3.3. 自学习防护引擎

网宿云 WAF 的自学习防护引擎(自学习白名单技术)，通过学习网站正常流量的特征（如数据类型、数据边界、数据取值等）和业务访问逻辑，构建出被防护网站的应用程序结构、正常用户访问的流量数据模型，能够排除和过滤异常用户访问及发现潜在攻击。

自学习防护引擎示例：

1) 某购物站点有个页面 http://www.xx.com/xx.php?num=x，其中请求参数 num 代表购买某物品的数量；

2) 网宿云 WAF 平台会通过自学习防护引擎去学习该购物站点的正常业务访问特征，针对 http://www.xx.com/xx.php?num=x 页面进行自学习的结果中，包含一条白名单规则：参数 num 的数值类型是正整数；

3) 若有客户端请求 http://www.xx.com/xx.php?num=1'or 1=1，网宿云 WAF 平台解析请求发现参数 num 为字符串，不符合正常业务模型，则对该请求进行阻断。

网宿云 WAF 的自学习防护引擎，是一个动态的主动防御机制，它所构建的网站结构模型和正常客户的行为基线能随着源站应用的变化而自动学习调整，可在无人工干预的情况下自动进行调整与更新。白名单一旦形成，若后续的访问不符合白名单特征，网宿云 WAF 可及时的进行告警并采用直接阻断、严格检测等方式对异常的请求进行处理，防止潜在的攻击到达源站。

3.4. “高效补丁”漏洞修复

目前 Web 应用安全漏洞日益增多，但是大多数漏洞并不能得到及时修复：一方面是因为企业网站并未及时安装漏洞的补丁程序，另一方面是因为 0Day 漏洞的出现，当 Web 应用安全漏洞被公共平台发布之后，厂商并未及时提供相应的补丁程序。而这些未被修复的漏洞，会被黑客利用进行攻击。

网宿云 WAF 可提供“高效补丁”漏洞修复，在客户未对漏洞进行永久补丁修复之前，可以通过调整防护策略形成对应虚拟的防线，实现漏洞快速防护，为客户提供更多的时间进行补丁修复，保障业务的持续性。且当 0Day 漏洞出现时，网宿云 WAF 会将“高效补丁”防护策略同步下发至全网，形成“全网联动”的防护体系，实现漏洞快速防护。

3.5. 网站精准访问控制

针对用户对某些 IP 或 URL 访问控制的特殊需求，网宿云 WAF 支持基于 IP 和 URL 的双重访问控制策略，即 IP 黑/白名单和 URL 黑/白名单。

1. 静态 IP 黑名单

   黑名单中的 IP 访问网站将直接被拦截。适用于明确某个 IP 是攻击者的场景。

2. 动态 IP 黑名单

   WAF 可根据客户端触发告警的情况，动态将其 IP 加入黑名单列表中进行一段时间的封禁，适用于攻击者进行扫描探测或持续性攻击的场景。

3. IP 白名单

   白名单中的 IP 访问网站不进行攻击检测，直接放行。适用于用户公司出口等特殊场景。

4. URL 黑名单

   所有用户访问黑名单中的 URL 将直接被拦截。适用于网站某个 URL 不希望被用户访问的场景。

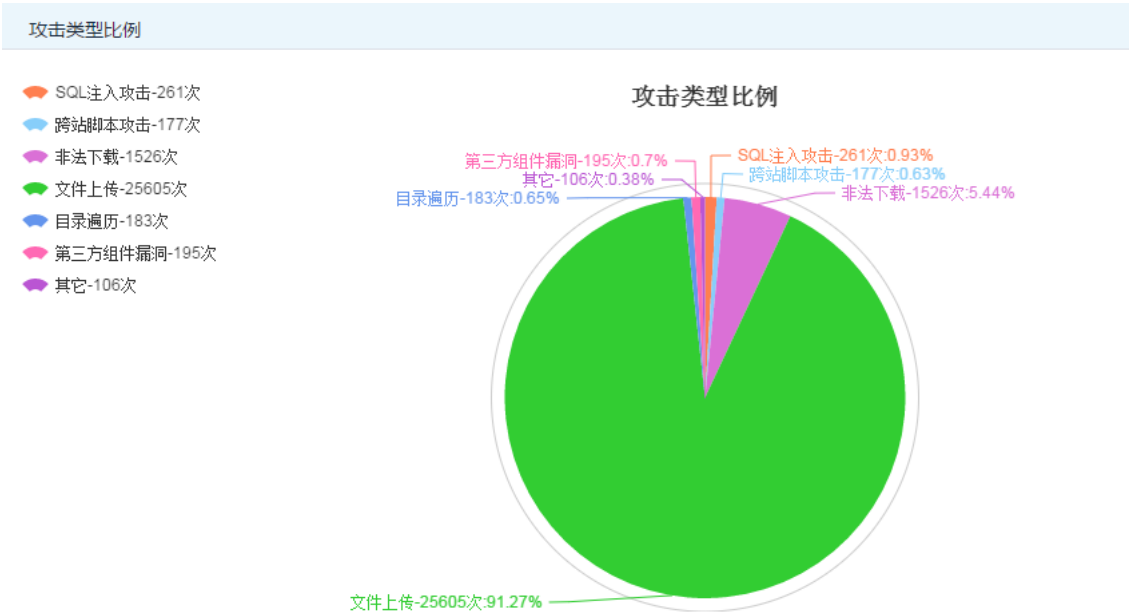
5. URL 白名单

   所有用户访问白名单中的 URL 不进行攻击检测，直接放行。适用于网站某个 URL 不需要 WAF 防护的场景。

3.6. 防护数据可视化

网宿云 WAF 可实时展示攻击信息（如攻击趋势、攻击详情、攻击类型、攻击来源等）和拦截情况。用户可以实时查看防护效果，并根据攻击趋势了解业务安全状态。

(1) 实时展示攻击拦截趋势，客户可以直观地了解各个时段的安全防护状况，并以饼状图展示网站遭受的攻击类型。



(2) 提供被拦截的 IP 详细信息，包括 IP 所在地、攻击类型、攻击次数等，以利于客户对后续对攻击者的处理。

序号	攻击IP详情	所属区域	总访问次数	攻击类型	攻击次数
1	[redacted]	中国大陆	1,213,256	目录遍历 网站扫描 跨站脚本攻击 SQL注入攻击 缓冲区溢出 非法下载	118008 82986 43624 38622 15359 181
2	[redacted]	香港	169,866	网站扫描 目录遍历 SQL注入攻击 跨站脚本攻击 缓冲区溢出 非法下载	49926 7404 2536 1967 480 30
3	[redacted]	中国大陆	72,175	网站扫描 目录遍历 SQL注入攻击 跨站脚本攻击 缓冲区溢出	35036 1953 978 600 242

攻击详情

序号	攻击时间	URL	攻击次数
1	2017-05-24 16:35:00	http://www[redacted]	49
2	2017-05-24 16:35:00	http://www.[redacted]	176
3	2017-05-24 16:30:00	http://www[redacted]	460
4	2017-05-24 16:30:00	http://www.[redacted]	496
5	2017-05-24 16:30:00	http://w[redacted]	105
6	2017-05-24 16:25:00	http://ww[redacted]	42
7	2017-05-24 16:25:00	http://www.[redacted]	561
8	2017-05-24 16:25:00	http://www[redacted]	487
9	2017-05-24 16:20:00	http://ww[redacted]	1,189
10	2017-05-24 16:20:00	http://[redacted]	946
11	2017-05-24 16:20:00	http://w[redacted]	157
12	2017-05-24 16:15:00	http://w[redacted]	473

4. 产品价值

4.1. 零部署、零维护

使用网宿云 WAF，无需改变网站现有拓扑架构，不需添加任何硬件，只需简单地做一层 CNAME，即可享受专业的 WEB 应用攻击防护服务。同时，WAF 的监控平台提供 7*24 小时全网监控，能够基于服务质量智能调度服务节点，保障服务实时稳定可用。并能够快速发现各类攻击并报警和采取应急响应措施，有效地保证服务的质量和稳定性，真正做到零部署、零维护。

4.2. 完善的防护架构，全方位保障网站安全

与其他 WAF 产品单一的防护架构不同，网宿云 WAF 基于黑名单(攻击特征库)和白名单(自学习防护引擎)技术，自主研发了一套被动与主动相结合的防护架构，可根据客户站点的实际情况量身打造定制防护服务，确保客户站点与数据的安全，减少由 Web 应用安全问题带来的声誉与经济损失。

4.3. 大数据安全分析，轻松应对新型攻击和 0day 威胁

网宿为数万个网站提供安全防护服务，拥有丰富的攻击规则库，且网宿 WAF 的协同防御机制能够针对不同网站的攻击数据进行关联分析，当攻击者对网宿 WAF 防护的任意一个网站发起新型攻击时，网宿云 WAF 会将防护规则同步至全网，形成“单点攻击，全网联动”的防护体系。

4.4. 高效应急响应能力，保障业务稳定

网宿 WAF 提供专属服务团队为用户一对一 7*24 小时的贴身服务，出现 0day 攻击时能够快速响应并进行全网升级防御，保障用户的业务不受影响。

关于网宿

网宿科技 始创于 2000 年 1 月，主要提供互联网内容分发与加速（CDN）、云计算、云安全、全球分布式数据中心(IDC) 等服务。

2009 年 10 月，网宿科技在深交所上市，股票代码 300017。

网宿科技拥有遍布全球的 1000+ CDN 加速节点，在北京、上海、广州、深圳等地设有分公司，在美国、香港、印度、爱尔兰、马来西亚、济南、南京、杭州等地建有多家全资子公司，并在厦门及美国硅谷设立了研发中心。现有员工 3000 多名，研发以及技术人员占总人数 60% 左右。客户群覆盖各类互联网门户网站、视音频网站、网络游戏公司、电子商务网站、政府网站、企业网站以及运营商等，公司服务的客户超过 3000 家，是市场同类公司中拥有客户数量较多、行业覆盖面较广的公司。