网站内容安全防护 服务白皮书V1.0

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

网宿内容安全防护服务是“网宿网盾”旗下一款针对网站内容安全打造的防护服务，结合网宿大数据分析技术、安全防护技术、内容安全库和分布在全球的 1000+节点优质资源，在云端形成一张安全防护网络，支持全链路防篡改、双向防敏感信息泄露、全程防劫持、防资源盗链、清除广告植入、智能图片鉴黄等功能，为企业提供全方位的内容安全保护。

“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

随着互联网的快速发展，人们可以通过网络获取新闻、交流互动、娱乐生活等信息，满足了广大群众对文化生活日益丰富的需求，然而这些日益增长的内容中充斥着大量不可控的因素，面临诸多挑战.

- **网站被篡改数量日益增多**

网站被篡改现象越来越多，包括篡改嵌入暗链、黄色信息、非法言论等，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。

- **劫持现象愈演愈烈**

网络劫持现象愈演愈烈，包括域名劫持、广告弹窗等，给网站和用户都带来了烦恼。

网络“盗链”现象猖狂

某些非法网站通过抓取盗用正规网站上的视频、图片等内容提供访问服务，。导致正规网站消耗了大量的带宽和版权，而真正的点击率很小，严重损害了正规网站的利益。

- **网络色情暴力内容泛滥**

互联网海量信息鱼龙混杂，大量的色情图片、暴力等不良信息严重影响用户体验，危害人们的身心健康，同时也损害企业的社会形象。

2.产品介绍

2.1. 产品简介

针对网站内容篡改、敏感信息泄露、广告植入、资源盗链、上传黄色图片等现象，网宿内容安全产品基于大数据分析，提供全链路防篡改、双向防敏感信息泄露、全程防劫持、防资源盗链、智能图片鉴黄功能，为企业提供全方位的内容安全保护。

2.2. 产品适用行业及场景

网宿内容安全产品面向的行业主要包括：

1、 政企行业

门户网站作为政府、企业提供给用户获取内容服务的重要渠道，一旦发生安全事件，如被篡改植入黄色、非法内容，将严重影响形象和公信力。

2、 金融行业

金融行业(证券、基金、股票等)向来是黑客觊觎的“钱袋子”，黑客通常会通过盗用用户账号密码、网银、信用卡、股票账号密码等用户敏感信息进行金融犯罪和诈骗，不仅危及了用户资金财产安全，而且严重影响企业的形象并承受经济损失。

3、 电商行业

电商行业频繁遭受黑客攻击，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。

4、 UGC 行业

UGC 行业（如：社交平台、照片分享平台、社区论坛等），用户既是网络内容的浏览者，也是网络内容的创造者。随着 UGC 产生的内容越来越丰富，安全问题也日益突出，大量色情、暴力等低俗内容在各 UGC 类平台等平台涌现，大大增加了企业人工鉴黄的成本。

5、 版权保护场景

随着图片、音视频、软件等资源的正版化推进，盗链现象也日益猖狂，网络黑产利用技术漏洞盗取正版资源，严重占用网站带宽和服务器资源的同时，侵害正版内容的权益。

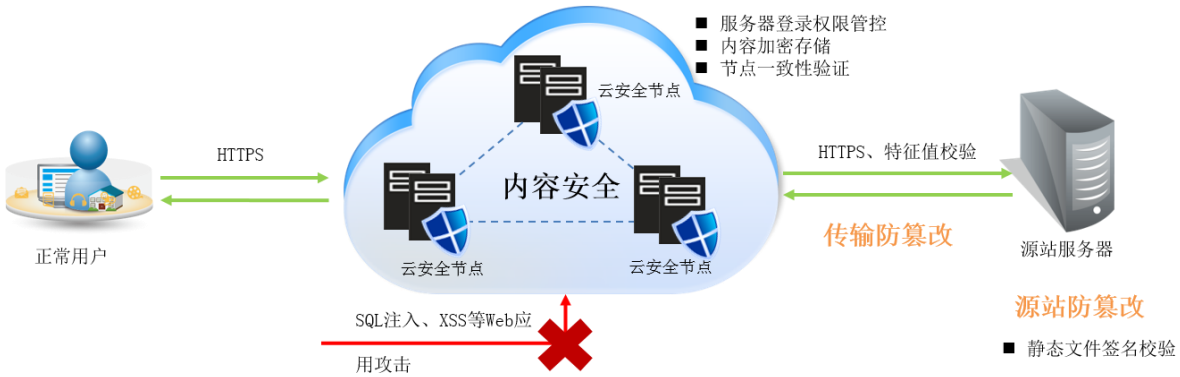
3.产品功能

网宿“内容安全产品”提供全链路防篡改、防敏感信息泄露、防资源盗链、清除广告植入、智能图片鉴黄等功能，为企业提供全方位的内容安全保护。

3.1. 全链路防篡改

非法者可能通过多种途径对源站内容进行篡改，从而使最终呈现给用户的内容与源站真实发布内容不相符，譬如：通过 SQL 注入、XSS 等 Web 应用攻击获取服务器管理员权限并对源站发布内容进行篡改或者在网络传输过程中非法截取数据包并恶意篡改包中内容。

网宿“内容安全产品”提供全链路防篡改方案，包括云端阻断篡改行为、传输防篡改和源站防篡改服务，避免内容被篡改而带来不良影响。



云端阻断可能导致篡改的行为

- 云端阻断篡改行为

网宿内容安全平台可实时阻断 SQL 注入、XSS 等请求，避免攻击者通过 Web 应用攻击的方式获取管理员帐号和密码，进而避免对网站内容进行篡改。

- 传输防篡改

对节点网络内部采用严格的服务器登录权限管控和内容加密存储方式，并在节点间进行内容一致性验证工作，保障网站内容在节点网络之间传输过程中不被篡改；同时针对网站到节点网络的传输可能存在的篡改问题，可以采用 HTTPS 传输或特征值校验。

- 源站防篡改

对于源站发布的图片、文章等内容，网宿内容安全产品采用自研算法进行签名，并在云端服务节点上对源站的响应内容进行校验，如发现校验结果不一致，则报警并将节点上一次缓存的页面内容响应给访问者，避免用户获取到被篡改的页面。

3.2. 双向防敏感信息泄露

网宿采用双向敏感信息检测机制，一方面检测并阻断可能引起敏感信息泄露的请求，另一方面检测响应内容是否存在敏感信息，并采取相应措施，避免敏感信息泄露。

- 请求检测

实时阻断 SQL 注入、XSS 等 Web 应用攻击，避免攻击者通过 Web 应用攻击的方式获取管理员帐号和密码，进而窃取网站敏感信息。

实时阻断非法者对网站敏感文件进行下载，如：密码、配置、备份、数据库等文件。

- 响应检测

网宿内容安全平台对源站的响应内容进行检测，判断是否存在服务器敏感信息、个人隐私信息、非法敏感词汇等信息，若出现敏感信息则采取相应措施避免敏感信息泄露。

✓ 服务器敏感信息防泄露

非法者可能故意构造错误的语句使得源站返回服务器敏感信息，如 Web 应用软件、操作系统类型，版本信息等，再利用这些软件所存在的漏洞进一步攻击。

1) 服务器响应内容检测： 内容安全平台对响应内容进行检测，对存在服务器敏感信息的响应直接进行阻断，避免非法者利用服务器敏感信息进行攻击；

2) 响应码检测：一般服务器返回 4 和 5 的响应码时会携带服务器敏感信息，内容安全平台支持针对状态码进行告警或者拦截，快速阻断敏感信息泄露。

✓ 个人隐私信息检测

对响应内容进行个人隐私敏感信息检测识别，如身份证、手机号、银行卡号等，并提供告警和屏蔽敏感信息等防护方式，避免网站用户个人敏感信息泄露。

✓ 非法敏感词检测

内容安全平台通过内置的非法敏感词库，对响应内容进行检索，若出现相关词汇，提供告警和屏蔽非法关键词等防护方式。

✓ 自定义敏感词

支持客户自定义敏感关键字，如：响应中存在敏感关键字，进行告警或者拦截。

3.3. 全程防劫持

劫持主要分为两种：一种为域名劫持，用户终端向运营商发出 DNS 解析需求时，由于某种原因返回错误的源站 IP 地址给终端，将用户引导至错误的网站，导致源站域名被劫持。域名劫持后的业务现象表现为：无法正常访问业务域名，访问超时或返回错误；访问业务域名返回涉政、涉黄等敏感、违法页面；访问业务域名返回广告、导航等第三方页面。另一种为内容劫持，指传输过程中，黑客可以拆解分析出请求内容，并在请求内容中插入一些广告或恶意内容等。

网宿内容安全产品提供域名防劫持、内容防劫持、防广告植入等服务。

- 域名防劫持

使用 HTTP 协议进行域名解析，客户调用网宿提供的 HttpDNS API，将域名解析请求直接发送到网宿的 HTTPDNS 服务器，从而绕过运营商的 Local DNS，从根源上避免 Local DNS 造成的域名劫持问题和调度不精准问题。

- 内容防劫持

通过 HTTPS 或特征值校验的方式防止内容被劫持。

- 防广告植入

网宿内容安全产品实时检测客户端是否存在被恶意植入广告的行为，如存在则移除被植入的广告内容，使其对访客不可见，流程如下图所示：

3.4. 防资源盗链

有些网站抓取其他网站服务器上的内容，直接在自身网站中向最终用户展示，骗取最终用户的浏览和点击率。大量消耗被盗链网站的带宽，而真正的点击率也许会很小，严重损害了被盗链网站的利益。

网宿内容安全产品提供防盗链功能，确保网站的内容资源不会被非法者恶意引用或非法下载，确保服务的安全性以及避免不必要的带宽浪费，确保网站的利益。网宿内容安全平台提供多种防盗链方式，满足客户不同的防盗链需求。

- 请求控制防盗链

针对客户端请求过程中所携带的一些关键信息(如：请求 IP、Referer、User-Agent 等)来验证请求的合法性，适用于版权保护(禁止或允许某些地区的用户访问某些特定的资源)、企业内部员工使用系统等场景：

1) IP 访问控制，通过 IP 访问的控制来禁止网站链接被非法者访问，实现防盗链；

2) Referer 防盗链，通过 HTTP 请求头中 Referer 字段来防止网站链接被其他站点非法引用；

3) User-Agent 防盗链，只允许特定的浏览器或者带有特殊 User-Agent 标识的专属客户端访问。

- 时间戳防盗链

对防盗链可靠性有更高要求的场景，通常是一些重要的大文件下载（如正版电影、音乐等），可以采用时间戳防盗链。加密的 URL 具有时效性，无法伪造，当达到过期时间后不再被允许访问。内容

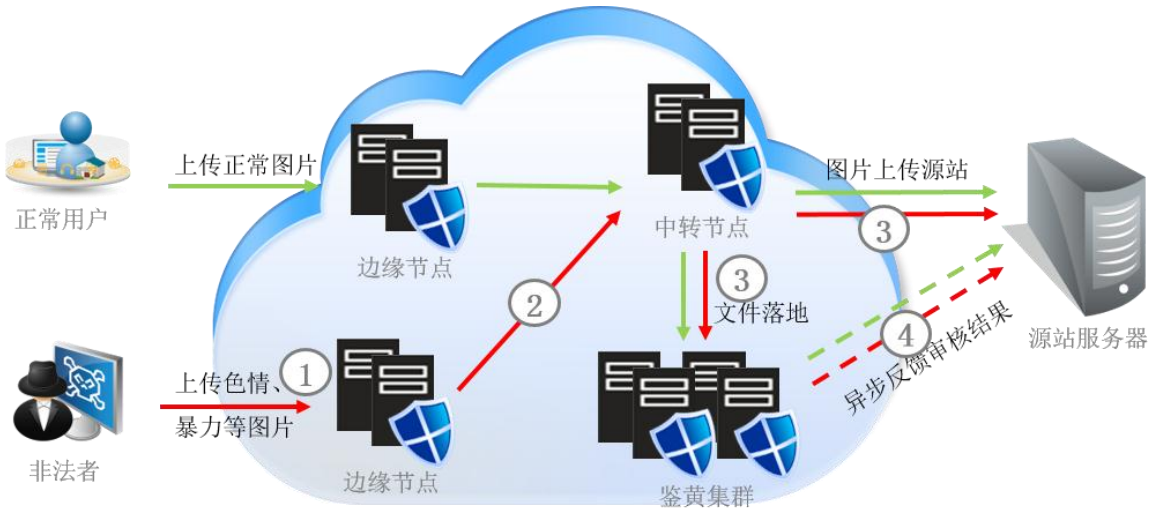
提供商负责生成加密的 URL，网宿内容安全平台根据预先设定的规则对 URL 进行合法性验证，对于验证不通过的非法请求直接阻断。

- 回源鉴权

网宿内容安全平台每次接收到的请求，都需要先回源进行验证，验证通过后才确认为合法请求，继续提供服务，适用于防盗链有很高实时性要求的场景。

3.5. 智能图片鉴黄

网宿内容安全平台基于大数据和深度学习的人工智能技术，可鉴别图片中是否存在不良内容，为网站提供高效经济的智能鉴黄服务，架构图如下所示：



网宿图片鉴黄

网站在接入网宿内容安全平台后，终端用户的上传内容将被引导到内容安全平台上，内容安全平台会对流量进行异步并行处理、计算，将流量复制转发到特定的审查集群，在不影响用户上传体验的同时起到鉴黄的作用。利用智能鉴黄服务，可以在终端用户上传到源站这一过程中对用户上传的内容进行审查和识别，对内容做一层过滤筛选，为客户大大节约人工审核成本和其他额外支出。

4.产品价值

4.1. 全链路防篡改，维护政企形象

网宿内容安全产品提供全链路防篡改功能，通过在云端阻断篡改行为、传输过程防篡改和源站防篡改避免网站被篡改、挂马，维护网站形象。

4.2. 双向防敏感信息泄露，保障企业及用户信息安全

网宿内容安全平台提供双向敏感信息检测机制，一方面检测并阻断可能引起敏感信息泄露的请求，另一方面检测响应内容是否存在敏感信息，并采取相应措施，防止敏感信息泄露，保障企业及用户信息安全。

4.3. 智能图片鉴黄，节约人力成本

相比传统的人工审核，基于人工智能的鉴黄技术具备突出的检测效率和优异的准确性，鉴黄机器可以提供 7×24 小时无间断的稳定运作，极大地降低人工审核的工作量，提高网站智能鉴黄效率。

4.4. 全方位内容安全防护，保障业务正常运行

网宿内容安全产品提供全链路防篡改、双向防敏感信息泄露、防资源盗链、全程防劫持、智能图片鉴黄等一系列内容安全防护措施，为网站提供安全健康的内容提供环境，保障业务正常运行。

4.5. 高效应急响应能力，保障业务稳定

网宿的专属服务团队提供一对一 7*24 小时的贴身服务，对于监控的网站出现突发问题能够快速响应，保障网站稳定。

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。