

360 网站云监测系统

——产品白皮书



■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，所有版权均属 **360 企业安全集团** 所有，受到有关产权及版权法保护。任何个人、机构未经 **360 企业安全集团** 的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录

1	前言	5
2	为什么需要网站监控	5
2.1	攻与防的博弈	5
2.2	安全思路的转变	6
3	传统网站安全监控的弊端	6
3.1	单一的探测源头	7
3.2	钓鱼网站探测盲区	7
3.3	漏洞探测技术陈旧	7
3.4	违规资产难以发现	7
4	360 网站云监测系统介绍	8
4.1	产品概述	8
4.2	产品架构	8
4.3	产品原理	9
4.3.1	多引擎扫描技术	9
4.3.2	沙箱检测技术	9
4.3.3	特有搜索检测技术	10
4.3.4	最新漏洞舆情推送手段	10
4.3.5	可用性监控技术	11
4.3.6	DDOS 攻击检测技术	11
4.4	产品主要功能	12
4.4.1	安全趋势监控	12
4.4.2	有效跟踪通报处理进度	12
4.4.3	报表管理	12
4.4.4	资产管理	13
4.4.5	用户管理	13
5	产品优势	14
5.1	产品优势	14
5.1.1	立体多维，监控服务更周到	14
5.1.2	持续监测，反复跟踪无死角	15
5.1.3	威胁情报，助安全一臂之力	15

5.1.4	集中力量，造网站安全护甲.....	15
-------	-------------------	----

1 前言

近年来，我国互联网市场规模和用户数量高速增长，随着云计算技术迅速兴起、信息化的普及，越来越多的企业走进“互联网+”，大量的金融、游戏、电子商务、电子政务等网站业务陆续上线。与此同时，我国的网站仍然存在较多的安全风险，Web 服务日益成为网络攻击的重点目标，DNS 攻击、暴力破解、零日漏洞利用、APT 攻击依然让网站弱不禁风。数据泄露、网页篡改、网页挂马、钓鱼攻击、拒绝服务等安全事件频繁出现。

据统计，2015 年全年，360 网站安全检测平台共扫描各类网站 231.2 万个，扫出存在漏洞的网站 101.5 万个，占比为 43.9%。被篡改的网站 8.4 万个，平均每天拦截漏洞攻击 512.2 万次，扫描发现约 4097 台服务器存在后门。面对频发的各类 WEB 安全事件，如何做到有效监测、快速响应、高效处置，已经成为各行各业必须面对的问题。

2 为什么需要网站监控

2.1 攻与防的博弈

攻击与防御是信息安全的核心，现在的安全防御体系完全是建立在深度了解攻击行为的基础上的。随着攻击手段的变化，防御体系也随之升级，知名安全研究员于旻的演讲——《未知攻，焉知防》更是印证了这一观点，在 Web 安全领域同样如此。

在早期的 Web 攻防阶段，黑客的主要攻击行为是利用网站的安全漏洞进行攻击。安全研究员通过对漏洞的分析，可以确认在漏洞攻击时攻击报文中一定会含有的触发漏洞的数据段，这就是漏洞的利用特征，通过对特征进行签名技术，将特征融入到 WAF、FW、IPS 等产品中，在攻击行为触发时，依靠网络设备的签名匹配进行检测和拦截，签名检测技术对已知漏洞可以进行有效防御。

HTTP 是一个开放而且复杂的协议，漏洞攻击只是 Web 攻击的一部分，随着黑客对 HTTP 研究的深入，发现了更多攻击种类：CSRF、盗链、Webshell、CC

攻击、Cookie 盗用等等，这些攻击行为完全基于会话，没有明确的特征，传统的签名匹配技术对这种攻击无能为力。研究员在分析了这些会话攻击后，通过在会话层中增加 token，报文重定向的方式进行定位与区分，这种会话识别技术主要应用在 WAF 产品上。

如今，Web 攻击方式呈现多样化，针对 DNS 服务器的攻击、高压力 DDOS 攻击、慢速攻击、撞库攻击、零日漏洞攻击等攻击手段层出不穷，依靠签名技术、会话分析的技术已经无法承担“防”的职责，传统的安全防御体系越来越难以支撑新型的攻击方式。

2.2 安全思路的转变

在传统的防御思路中，事前发现、事中拦截、事后响应是最常见的方式。但是在 Web 安全走过了这么多年的结果中看到，在攻与防的博弈中，越来越多的行业开始意识到攻方始终占据会占据领先优势。而在传统的拦截手段逐步失去效果的情况下，如何快速的对威胁进行预测、检测、发现将成为安全的重点发展趋势。

在 Web 安全中，由于网站是开放给所有用户的，它在开放业务给用户的时候，也把自己暴露给了黑客，对网站的入侵相比其他的安全领域降低了门槛，那么在防御体系终究会被打破的预估下，如何快速、精确的发现安全影响将成为所有安全厂商面临的安全问题。

基于 Web 安全发展趋势、企业用户对网站安全风险快速响应需求，网站监控应运而生。

3 传统网站安全监控的弊端

传统厂商在做安全监控的时候基于 Web 漏洞扫描器的探测技术，通过对网站的漏洞进行爬取和探测进行安全感知，这种技术有很多局限性：

3.1 单一的探测源头

传统安全厂商由于能力的局限，在对企业网站进行可用性监控时，往往只能通过单一节点进行安全监控。网站业务是面向全国用户的，单一节点的安全监控无法掌控全国区域的用户对企业站点的访问情况，监测体系存在盲点，除此之外，也无法了解当前站点的全局访问情况。

3.2 钓鱼网站探测盲区

传统安全厂商在钓鱼、仿冒网站的发现上很困难，由于主动扫描技术的前提是知道需要扫描的站点域名或者 IP 地址，从而进行漏洞探测，而仿冒、钓鱼网站的域名和 IP 对于扫描器来说是未知的，无法进行针对性的扫描和比对，成为探测盲区。

3.3 漏洞探测技术陈旧

传统安全厂商在漏洞探测时，主要通过系统规则探测，探测效果完全依赖规则的更新与准确性，一方面规则更新存在时间差，在漏洞曝光的时候如果没有及时升级规则库，则会出现扫描空窗期，另一方面对于零日漏洞的探测上，传统扫描器没有源头支撑，无法有效支撑零日漏洞的探测。

3.4 违规资产难以发现

传统安全厂商在扫描过程中，完全依赖于对已知域名以及 IP 的探测，但是在企业中存在私搭烂建的网站，这些网站没有经过报备，扫描器无法进行探测。但是这些站点会开放 Web 业务，提供对外的访问权限，存在安全漏洞，大大增加了企业的安全风险，

4 360 网站云监测系统介绍

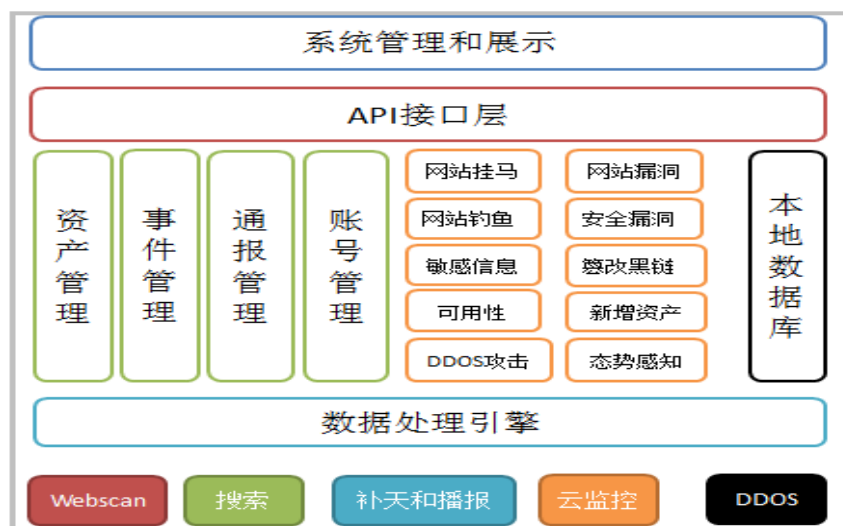
4.1 产品概述

360 网站云监测系统旨在通过云端发现企业本地网站的安全问题，是一款基于云的安全服务产品，依靠 360 强大的云端资源，为用户提供网站可用性监控、网站挂马、钓鱼网站、网页篡改、暗链发现、漏洞扫描、漏洞舆情等安全服务。

系统为用户提供统一的云平台管理账号，用户处无需部署任何软硬件产品，可以随时通过互联网终端对监控对象进行 7x24 小时的监控、查看与管理。解决用户处因硬件资源申请流程长，设备资源利用率不高，开发及运维人员成本迅速升高等问题。

4.2 产品架构

360 网站云监测系统由基础数据支撑系统，数据处理引擎，本地数据处理模块、系统管理与展示模块 4 部分组成：



- 爬虫引擎是监测平台重要的基础组件，完成对监测域名的内容爬取，以供各类分析引擎使用。
- 流量抓包引擎，按照比例针对互联网流量进行抽样，将抽样流量进行汇总分析。得出网站是否存在安全威胁的结论。
- 大数据平台存储爬取的页面数据，检测的数据等。可用于后续做大数据

分析和数据挖掘。

- 内容监测 API 和运维平台主要针对已有数据进行分析, 为平台提供监测结果。
- 监测平台 API 和运维平台主要是将群监测的功能界面化, 方便用户的日常监控及运维管理。

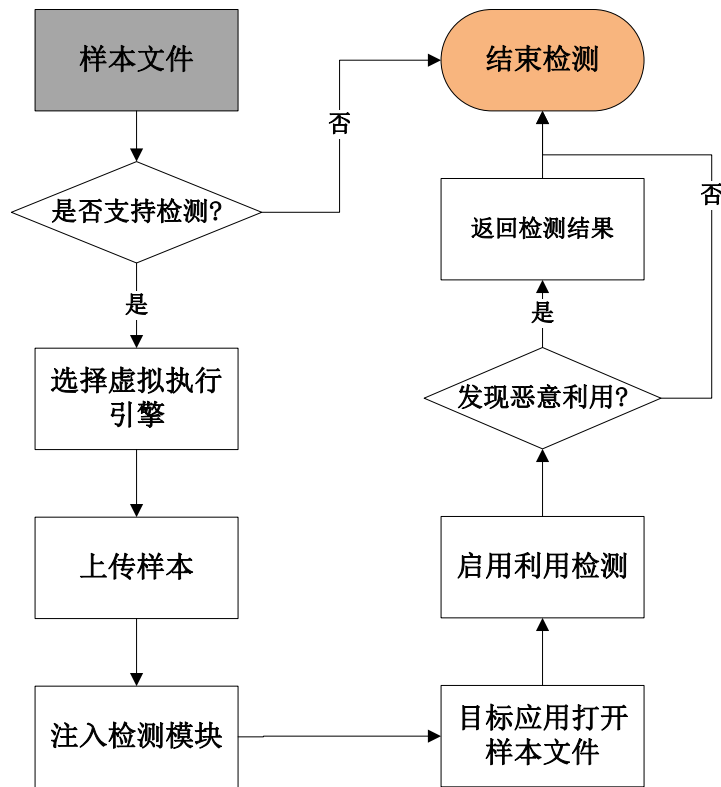
4.3 产品原理

4.3.1 多引擎扫描技术

Webscan 扫描引擎以多年免费网站防护经验为基础研发的一款扫描产品, 周期性的提供安全漏洞检测服务, 自动更新补天及运营团队每日编写的检测规则。全面、快捷识别网站存在的最新漏洞。根据爬取的信息, 通过分析模型及海量样本库加权判断网站是否被仿冒, 网页是否被挂马, 检测网页被篡改位置及内容, 及时告警使其得到快速处理。同时可以搜取更具有价值的相似页面, 通过内容比对, 上下文分析等技术为网站钓鱼提供判断依据。

4.3.2 沙箱检测技术

沙箱检测技术主要针对网页挂马行为的相关技术进行检测, 判断样本文件是否存在恶意利用代码。本检测技术包含动态检测引擎和半动态检测引擎。动态引擎依赖于漏洞利用环境重现, 虚拟机执行引擎运行 Windows 操作系统以及相关应用程序, 注入检测模块, 对恶意文件利用行为特征进行检测。使用 Hook、指令流分析、模拟执行等检测手段对 shellcode 执行生命周期的各个阶段的特定行为进行检查, 检测流程如下所示:



4.3.3 特有搜索检测技术

搜索引擎技术是 360 好搜的核心技术，目前已经占据 20% 以上的搜索份额。系统利用 360 强大的搜索功能及过亿级别的用户数据，有效识别、收集、定位敏感关键词，形成告警，提醒出现涉黄、暴力、诈骗、政治等敏感信息的网站及时整改，以免遭受不良影响。同时结合互联网数据的支撑和搜索运营团队的人工判断，准确高效。

4.3.4 最新漏洞舆情推送手段

“补天平台”，原名为“库带计划”，于 2014 年 12 月 1 日 10 点更名为“补天漏洞响应平台”，简称“补天平台”。该平台是 360 互联网安全中心推出的国内首个现金奖励漏洞平台，旨在建立企业与白帽子之间的桥梁，帮助企业建立 SRC（安全应急响应中心），让企业安全，让白帽子获益。

该平台于 2013 年 3 月份推出时，是一项针对开源建站系统漏洞的有奖征集项目。该项目通过现金奖励的方式征集开源建站系统漏洞，用以帮助软件公司

和开发者及时推出漏洞补丁，加强国内数百万家网站对黑客攻击的防范能力，并加强 360 网站安全产品的漏洞检测能力和攻击防御能力。

从 2014 年 06 月开始，除了通用型漏洞外，补天平台也开始收集事件型漏洞。事件型漏洞主要是指网站或应用的一个具体漏洞，只对该网站自身有影响。如某政府网站后台存在弱口令可进后台 GETSHELL，某著名企业门户网站存在重要信息泄露等。

同时，360 利用专有的爬虫技术，快捷全面的获取主流漏洞平台发布的漏洞信息如：补天、乌云、漏洞盒子等。监控业内影响比较大的安全人员的社交动态如：新浪微博、twitter 等。综合分析安全现状，有效预测安全态势。

4.3.5 可用性监控技术

使用全国 40 个探测点定时对网站的访问性、DNS 解析失败率、连接失败率等基本访问情况进行探测。目前云服务监控拥有全国 31 个省市的 40 余个监测点，同时监测频率最小能到 1 分钟。能 7x24 小时实时监测用户的网站的可用性，并结合 360 的大数据分析平台，对网站的性能指标进行详细分析，为网站的运维和优化提供数据支撑。



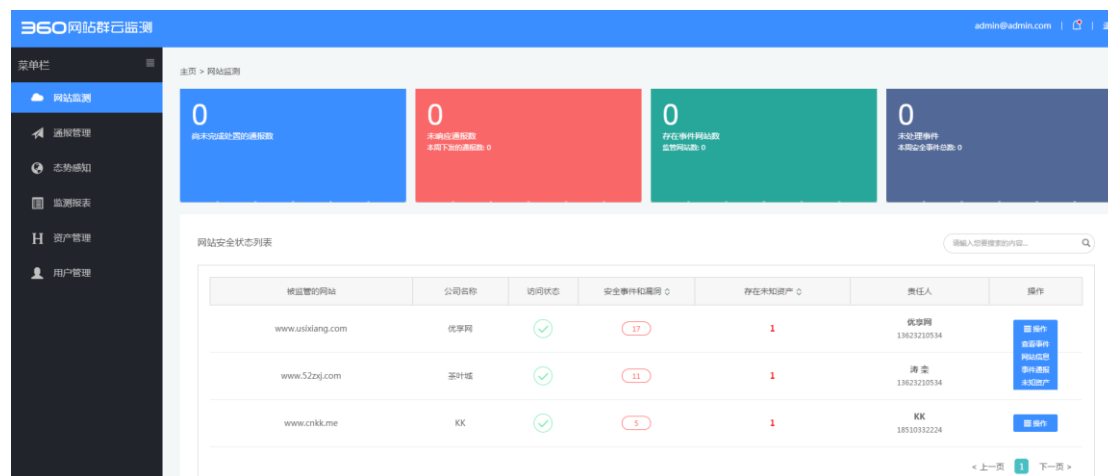
4.3.6 DDOS 攻击检测技术

DDOS 分析系统，聚焦于全球 DDOS 攻击现状及趋势的分析功能。结合海量网络数据进行分析建模，有效发现异常访问流量。系统检测到被监管资产出现故障后，能有效分析网站是否遭受 DDOS 攻击，攻击类型，开始时间等重要信息供参考解决客户问题。

4.4 产品主要功能

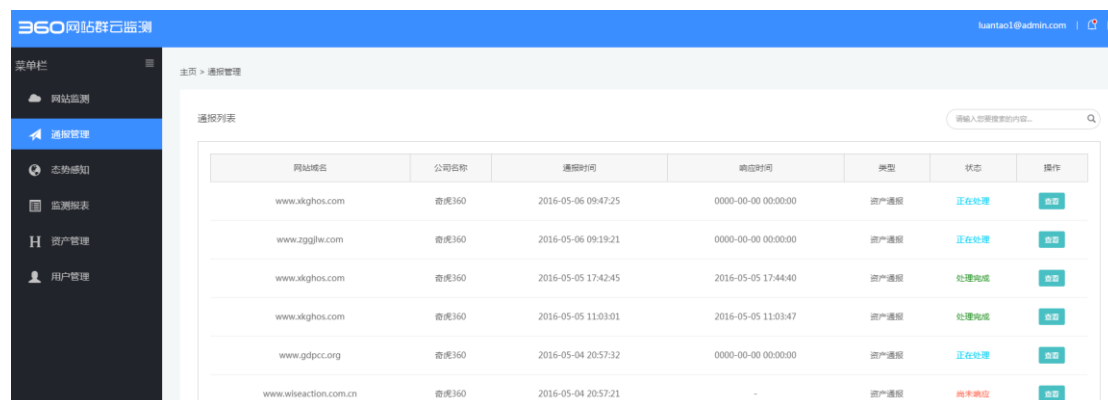
4.4.1 安全趋势监控

有效聚焦关注问题，直观定位被监管网站的安全概况，简单易用，为用户提供一个快捷处理通报的入口，快捷下发未知资产确认的接口。



4.4.2 有效跟踪通报处理进度

详细记录通报下发时间，响应时间，标注通报处理状态，提供通报跟踪轨迹，了解通报处理过程，被监管单位处理意见实现有效沟通、高效处理。



4.4.3 报表管理

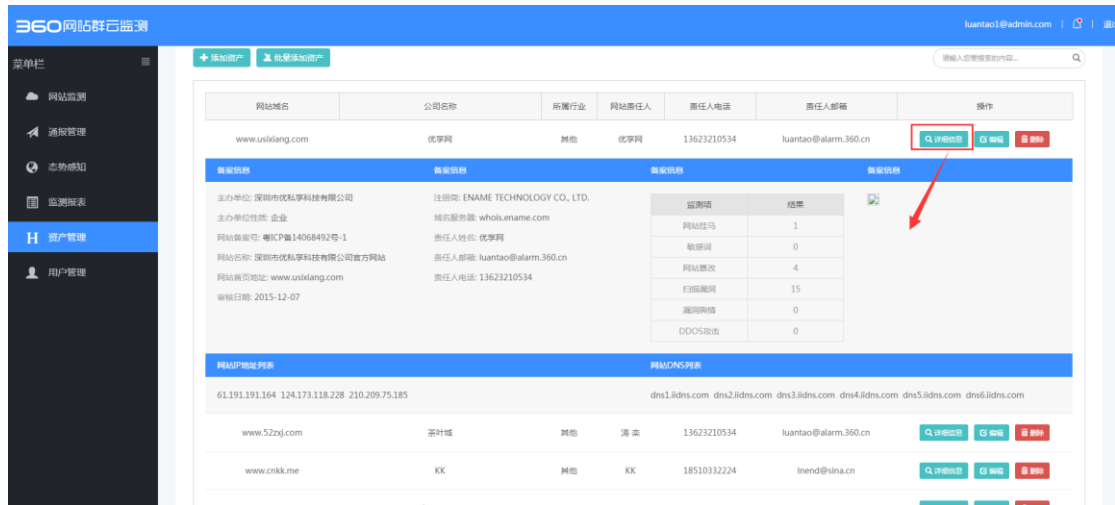
支持生成日报、周报、月报及预览功能。多维度图表展示被监管网站的安全态势，深度分析资产新增情况，安全事件发生比例，被监管网站受影响的严

重程度等问题。从资产、可用性、完整性、脆弱性、通报处理时长等多角度深入问题监管问题。为监管单位提供网站安全建设考核指标的参考。



4.4.4 资产管理

支持用户单个资产导入、批量资产导入等功能。



4.4.5 用户管理

管理员通过用户管理，完成平台运营人员和下级平台管理员的创建。平台管理员和平台运营人员的权限是相同的，只是管理员可以看到所有，多个运营人员之间账号信息是不可见的，运营人员也看不到管理员的账号信息。

360网站群云监测

kuantao1@admin.com

菜单

- 网站监测
- 通报管理
- 态势感知
- 监测报表
- 资产管理
- 用户管理

主页 > 用户管理

+ 添加用户

请输入您要搜索的内容...

账号	姓名	手机号码	账户类型	操作
admin@admin.com	系统超级管理员	13623210534	下级平台管理员	编辑 授权 删除
kuantao1@admin.com	测试1	13623210534	下级平台管理员	编辑
kuantao2@admin.com	测试1	13623210534	下级平台管理员	编辑 授权 删除

< 上一页 1 下一页 >

5 产品优势

5.1 产品优势

5.1.1 立体多维，监控服务更周到

未雨绸缪，安全方得稳固。360 网站云监测系统以多年积累的大数据、成熟的样本分析模型、高尖端的安全运营团队为基础。为用户实时监控网站可用性、实时分析网站完整性、周期扫描网站脆弱性、及时通告网站 oday 及舆情、自动抓取并分析仿冒网站、事实监控网站是否遭受 DDOS 攻击等服务。

监控服务分类如下图：



5.1.2 持续监测，反复跟踪无死角

7X24 小时对被监控网站进行连续的、全面的、系统的、动态的检查以评估被检测网站的可用性，完整性等安全隐患。实时发现被监管网站环境的变化，持续跟踪事件处理进度，针对已处理完事件进行自动化复测，保障系统发现的安全隐患得以充分且正确的解决。

5.1.3 威胁情报，助安全一臂之力

360 通过自主研发技术，共监控全球 30 多亿域名的流量分布。近万名从业人员及爱好者的社交言论（Twitter，微博），400 多家安全网站，安全论坛和网络安全媒体网站的安全文章。收集并整理全球 40 万漏洞信息，并能对漏洞的影响及危害进行评估。360 全线安全产品的上百亿恶意样本特征及拦截记录，为数据分析提供了庞大的数据支撑。

威胁情报是来自于系统外部的安全知识或信息，可以帮助系统管理者更好的实现系统内部安全问题的分析、发现与溯源，是系统安全防御能力的重要扩展。

目前，威胁情报在国际上已有一些商业实践，但在国内尚属于新鲜事物。有能力提供威胁情报服务的厂商屈指可数。2015 年 8 月，360 建成了国内首个威胁情报中心，并于 9 月开始正式商用，目前主要为相关政府机构和大型企业提供威胁情报的信息服务。

360 拥有充分的互联网数据做支撑、具有相对全面的专业安全技术能力、能够能力保证威胁情报提供的及时性，为监管网站提供高效的、维度丰富的、高价值的威胁情报服务。帮助企业更早的发现问题，解决问题，规避重大损失。

5.1.4 集中力量，造网站安全护甲

在互联网技术蓬勃发展的时代，任何网络安全都可以能上升至国家安全，近年来 360 不仅聚焦个人用户上网安全，同时更关注企业用户的业务安全。在 WEB 安全方面 360 陆续推出了 DDOS 防护系统，网站漏洞扫描设备，成立了第一

个威胁情报中心，建造了权威的 web 攻防实验室等多专攻 WEB 安全方向的技术团队，为网站安全检测提供了有力技术支撑和数据来源。