

## 问题挑战

近些年来，国际黑客势力对于国内政企用户的网站每年都有进行大量攻击，直接或者间接导致网站机密信息被窃取、网站被植入木马、网站页面内容被篡改、DNS 被投毒或劫持等等，这些都极大地困扰着网站所有者，给企业形象、信息网络甚至核心业务造成了严重的破坏。

虽然可以通过部署入侵防御系统、高性能防火墙等相关防护类产品来起到一定的防护效果，但是，用户难以更早的发现风险隐患，预防这些安全事件发生。另外，网站管理员需要维护大量的安全设备，分析众多日志信息，承担更多额外的工作量。

有没有这样一种解决方案？它既可以主动提前发现网站存在哪些安全漏洞，通知网站管理人员及时修补；又可以实时发现网站运营过程中出现的安全事件，第一时间通知网站管理人员采取措施消除不良影响；为此，绿盟科技推出了网站安全监测服务，可以通过不间断的远程监测，为客户网站提供安全检查、安全事件监测、实时响应和安全趋势分析服务，使其成为用户网站安全体系的最好补充。

## 产品概述

绿盟网站安全监测服务，是一款托管式 SaaS 服务。您只需将网站域名等信息告知绿盟科技工作人员，获得授权后即可享受 7×24 小时的远程网站安全监测服务。一旦发现您的网站存在风险状况，绿盟安全专家团队会第一时间通知您，并提供专业的安全解决建议。除此之外，经验丰富的绿盟安全专家团队会定期为您出具周期性的综合评估报告，让您整体掌握网站的风险状况及安全趋势。

绿盟科技已先后为金融、运营商、政府、能源、企业、互联网等行业的 2500 多家客户、12000 多个网站提供安全监测服务，帮助客户降低了网站安全运营风险。



## 客户价值

- 第一时间知晓并处理网站安全事件，降低网站运营风险隐患，减少业务损失
- 周期性专家级安全报告，网站安全状况一目了然
- 服务完全托管给第三方，网站安全管理轻松省心
- 获得一支专业安全服务团队的技术支持，网站安全水平以及品牌形象得到提升

## 核心优势

- 提供针对给定 IP 段的 IP 资产、端口监测，如有变化通告用户
- 提供专家级高中危漏洞验证，准确率可达 100%
- 提供漏洞生命周期闭环管理，让漏洞无处藏身
- 提供漏洞风险、灾害事故的可视化展示，能够让用户一目了然的洞悉全单位风险及灾害分布
- 提供网站安全事件的分级监测，能够针对不同的资产，不同的事件类型可以以不同的通知方式通知到不同的用户

## 优势特点

### 四“快”

- 应用快
  - 7\*24小时全天候服务，按需购买，即买即用，无需安装部署
- 检测快
  - 平台每15分钟监测一次，高密度发现网站异常情况
- 响应快
  - 安全专家30分钟内分析报告，及时响应告警事件
- 定位问题快
  - 风险、事故通过可视化图表一目了然

### 四“广”

- IP资产覆盖广
  - 支持给定IP段的全IP资产探测
- 漏洞扫描广
  - 支持扫描网站系统漏洞
  - 支持扫描 WASC 25 种 Web应用漏洞
  - 全面覆盖 OWASP Top 10 Web应用风险
- 事件覆盖广
  - 支持监测挂马、黑链、篡改、敏感内容、平稳度等事件
- 监测点分布广
  - 支持多点、多线路监测

### 四“免”

- 免物流
  - 直接远程交付服务，无需走物流发货流程
- 免安装
  - 纯SaaS服务，无需安装任何软硬件，成本低
- 免部署
  - 无需改变网络结构
  - 无需占用机房或办公空间
- 免维护
  - 无需处理故障、升级等问题
  - 完全托管，无需亲自运维

## 功能特性

### ■ 远程网页篡改监测服务

远程实时监测目标站点页面状况，发现页面被篡改情况，第一时间通知用户。用户可参考绿盟科技提供的安全建议及时修复被篡改页面，避免篡改事件影响扩散，给自身带来声誉和法律风险。

### ■ 远程网页敏感内容监测服务

远程实时监测目标站点页面状况，发现页面出现敏感关键词，第一时间通知用户。用户可参考绿盟科技提供的安全建议及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。用户也可以自定义所关心的敏感关键词。

### ■ 远程网页挂马及黑链监测服务

绿盟科技基于安全云，采用业内领先的智能挂马检测技术，可高效、准确识别网站页面中的恶意代码，以及黄赌毒广告类黑链，使网站管理员能够第一时间得知自己网站的安全状态，及时清除网页木马，清除黑链，避免给访问者带来安全威胁，影响网站信誉。

### ■ 远程网站漏洞扫描服务

网站的风险漏洞是站点被攻击的根源。通过远程的网站漏洞扫描服务，由绿盟安全专家定期进行网站扫描、高中危漏洞验证，用户无需采购任何 Web 应用扫描产品，即可获得网站的漏洞情况，以及修补建议。该服务支持远程扫描 6 种系统漏洞和按照国际权威安全机构 WASC 分类的 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险。

### ■ 远程网站可用性监测服务

从全国多省运营商网络线路远程实时监测目标站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问，第一时间通知用户。用户可参考绿盟科技提供的安全建议优化网站性能，避免网站业务中断或响应延迟给访问者带来不好的体验，甚至给自身造成经济损失。用户也可以视情况选择合适的网站响应时间告警阈值。

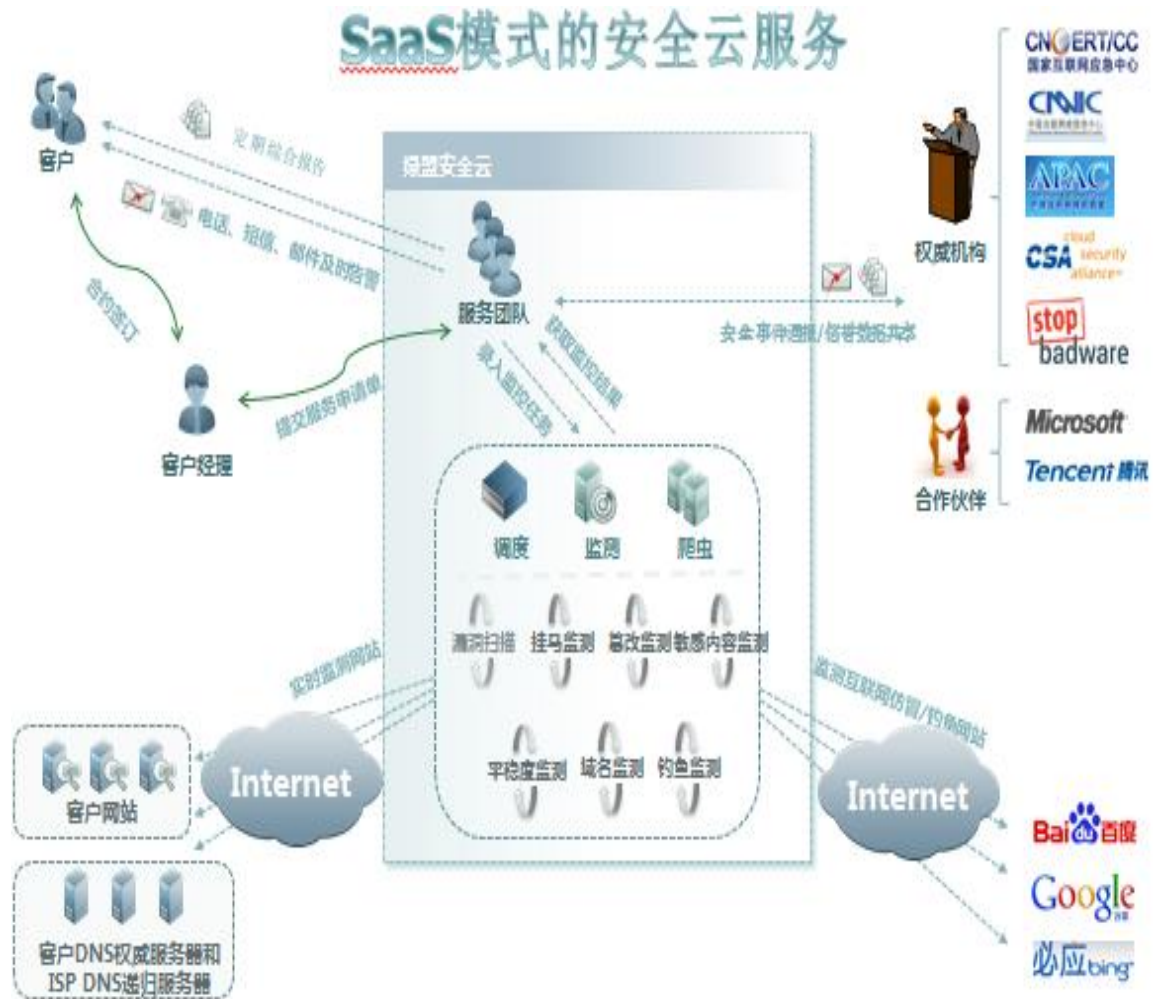
### ■ IP 资产核查服务

通过绿盟云端强大资产检测引擎为指定的 IP 网段进行资产扫描，通过与现有资产比对发现新上线的网站及变更的网站系统，并及时向用户通告。在用户确认资产变更内容后，更新现有资产列表并将变更的资产纳入到安全监测体系中，以便及时发现漏洞与安全事故。

## 实施流程

- ✓ 首先，客户和我们的客户经理签订合同后，由客户经理向服务团队提交申请单。
- ✓ 接着，服务团队评估确认后，将任务录入网站安全监控平台，平台会实时远程监控客户网站。
- ✓ 服务团队会在监控中心 7×24 小时值守，监视平台告警事件，在 30 分钟内验证完毕，通过电话、短信、邮件等方式通知到客户，使客户能够及时应对突发事件。
- ✓ 除了及时通报告警事件，服务团队还会定期给客户发送综合报告，为客户呈现网站

整体风险状况并提供整改优化建议。



## 最终交付

- ✓ 各类安全事件即时通过邮件、短信、电话方式进行交付。
- ✓ 漏洞扫描结果和各类事件监测结果以周报、月报形式进行交付
- ✓ 通过信息通报门户进行交付，用户可通过互联网浏览器进行查阅

13 危险站点数 28 恶意站点数

地域视图 组织结构

紧急 2015-10-18 CVE-2015-5477 JSC 漏洞 BIND TRILY Query 本地服务漏洞

最近1个月 今年

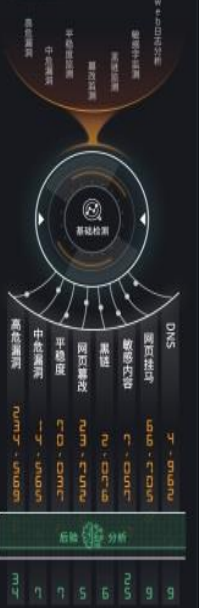
> 高风险资产TOP10

- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息
- www.portaledit.hy.com/资产信息

> 安全态势总览



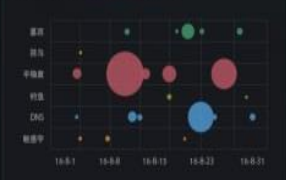
> 安全监测分析



> 高中危漏洞TOP | 高中危漏洞分布



> 高风险事件TOP5 | 高风险事件分布



> 监测结果汇总 | 漏洞类型分布TOP5

