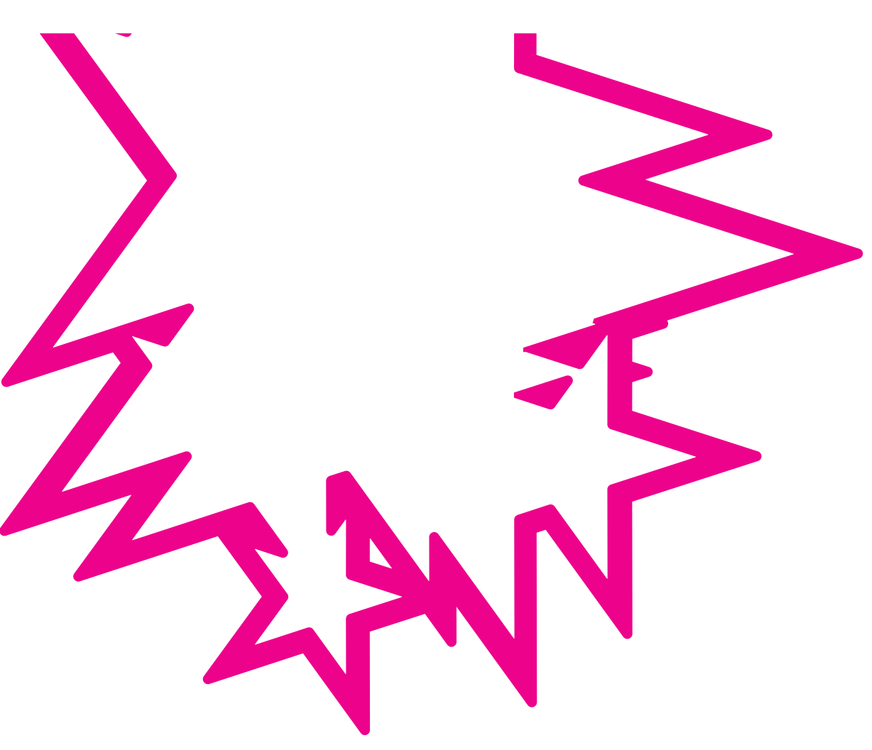


荣誉资质

- 国家信息安全测评信息安全服务资质（最高级）
- 国家级网络安全应急服务支撑单位（最高级）
- 中国网络安全产业联盟理事长单位
- 国家信息安全漏洞库（CNNVD）一级技术支撑单位
- CSA云安全联盟中国分会创始人单位
- 《基于大数据的安全态势感知分析和溯源系统》入选2017年工信部网络安全试点示范项目

合作伙伴

NSFOCUS
总部：北京市海淀区北洼路4号益泰大厦
绿盟科技（股票代码300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：webadmin@nsfocus.com

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具
有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

绿盟科技
全流量高级威胁分析系统

THREAT ANALYSIS AND EMERGENCY DISPOSAL SOLUTION

THE EXPERT BEHIND GIANTS

NSFOCUS

NETWORK AND APPLICATION
SECURITY
SOLUTION PROVIDER

安全挑战

☆ 随着国家对安全的重视，业务应用对安全需求的持续提升，用户对安全认识的不断深入，安全能力需要实现关联和整合。

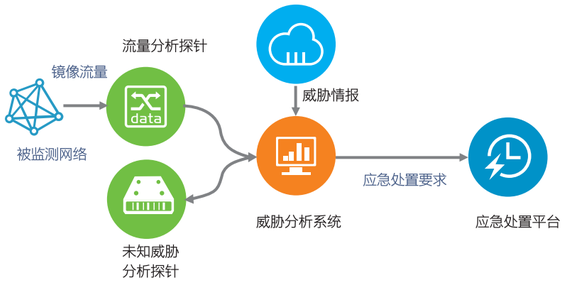
☆ 传统基于规则检测、功能单一的安全设备和系统已经无法有效应对日益严重的安全威胁，尤其是面对0day、APT等，更加难以应对。

☆ 亟需能够对安全威胁、安全事件进行更加全面、更为深入的分析、告警、溯源、取证和处置，把安全工作做到实处。

漏洞应急处置	事件回溯分析	日志多维关联	快速应急处置
漏洞应急滞后 企业风险陡增	历史数据不全 难以回溯分析	传统告警日志 分析维度受限	重大活动安保 无法快速处置

方案介绍

绿盟全流量高级威胁分析系统针对原始流量进行采集和监控，对流量信息进行深度还原、存储、查询和分析，并对用户关注的重要安全事件进行快速处置，可以及时掌握潜在的网络安全风险，及时检测漏洞、病毒木马、网络攻击状况，及时通报预警重大网络安全威胁，快速处置影响业务应用的安全威胁事件，保障重要信息系统的安全稳定运行。



全流量安全解决方案

检测 威胁检测 无所遁形

- 规则检测：丰富的安全规则库，提升检测准确率
- 威胁情报：关联威胁情报，提升分析准确率
- 沙箱监测：文件还原检测，发现恶意文件
- 机器学习：多种安全场景建模，使用机器学习模型完善安全分析结果

处置 一键处置 安全可控

安全事件快速处置

网页篡改事件 | 短彩信系统被控事件 | DDoS攻击事件 | 域名劫持事件 CDN劫持事件 | 违规网站事件

特点和优势

- 传统检测方法和创新机器学习模型，对已知、未知威胁进行全方位检测。
- 分析结果支撑运营能力提升，明确运营目标，取证确认攻击行为，提升运营效果。
- 安全事件闭环处置，秒级响应，极速关停异常服务，有力支撑重大活动的安全保障工作。

攻击能检测 | 流量能看见 | 结果能运营 | 事后能追溯 | 问题能处置

- 直观查看流量构成、端口开放情况，监控流量状态，及时发现异常情况。
- 事后回溯分析，发现潜在威胁，主动威胁狩猎，加强主动防御能力。

客户价值

- 深度威胁检测 发现潜在威胁
- 拒绝海量告警 提高运维效率
- 攻击有证可查 协助确认攻击
- 分析场景定制 快速满足需求
- 事件主动响应 及时分析处置