

绿盟网络入侵防护系统

产品概述

面对新一代威胁的挑战，绿盟科技根据多年攻防研究积累、以及产品研发经验，推出了新一代网络入侵防护系统（NSFOCUS NIPS）。NSFOCUS NIPS 具备国际领先的攻击特征库，8000 多条规则可对网络攻击类、信息破坏类、有害程序类和漏洞类攻击一网打尽；为应对高级威胁，集成了沙箱检测能力，实现了对已知和未知威胁的立体防护；协同绿盟威胁情报系统，利用其上千万的文件库、IP 库、URL 库和 C&C 库等，在云端实时检测恶意文件、恶意 IP、恶意 URL 和 C&C 通信；采用流式和启发式病毒检测技术，捕获热点病毒，极大地增强防病毒能力；集成手机安全管家，实现安全咨询推送和安全态势即时监控，将运维人员从繁重的工作中解放出来；虚拟化 IPS 具备网络流量牵引，集中授权的能力，绿盟 NIPS 为用户提供了一套“看得见、检得出、防得住”的全新入侵防护解决方案。

技术优势



1、高级威胁防御

集成沙箱检测功能，有效应对日益增加的 APT 攻击，发现 0day 漏洞攻击和未知恶意软件，实现对已知攻击和未知攻击防护的融合。

2、流式扫描病毒技术

采用业界领先的流式病毒扫描技术+启发式防病毒技术，实时跟踪热点病毒，实现小时级别的热点病毒更新服务。在性能和检测率方面均有优异表现。

3、敏感数据保护

能够识别并阻断特定格式文件的外发，同时能够检测出文件中包含的敏感数据，进行告警和阻断，保护企业敏感数据，防止敏感数据泄露造成的损失。

4、客户端防护

增加了针对主流客户端应用程序的攻击签名规则，如 Word、Excel、PDF、Firefox 等，增强了客户终端应用程序的安全防护能力。

5、僵尸网络防护

基于准实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意 URL、僵尸网络、恶意文件，第一时间拦截 Web 威胁，及时发现网络中僵尸网络和 C&C 连接，保护用户在访问含有恶意代码的网站时不受侵害。

6、手机安全管家

通过手机安全管家 APP 提供的服务，安全管理员可以获取最新的安全漏洞以及重大安全事件等资讯。另外，APP 可以监控安全设备健康状态，同时可以实现企业安全态势的统计、查询以及趋势分析。

7、全球威胁情报系统（NTI）

NIPS 集成了绿盟全球威胁情报系统，实现威胁情报的实时推送。同时，绿盟与部分友商（金山、腾讯、bitdefender 等）实现了情报交换，使得 NIPS 在第一时间具备最新威胁检测能力。

8、虚拟化

绿盟虚拟化 IPS 实现流量牵引（路由），支持一虚多的技术，实现客户资源有效利用。

10、云端沙箱检测

IPS 可以直接和部署在绿盟云端的 TAC 联动，减少实施部署的复杂度，减少客户运维成本，实现和本地沙箱相同的 APT 防护效果。

11、100G+高性能 NIPS 系统

100G+高性能 NIPS 系统，采用模块化、硬件加速和电信级边缘计算架构可扩展平台，兼顾高密度计算性能和网络扩展能力，为用户提供不间断的交付服务，适合运营核心网络、云计算数据中心、大型企业以及 IDC 出口等高端应用场景。

Magic Quadrant Network Intrusion Prevention Systems



Source: Gartner (January 2018)