# 绿盟统一威胁探针

## 1. 产品概述

随着 5G、物联网和人工智能等新技术的全面普及，黑客的攻击手段层出不穷，为了应对大量不同类型的攻击，传统威胁检测方案面临诸多挑战，NSFOCUS 推出了绿盟统一威胁探针（简称 UTS）。UTS 是一款集 IDS、WAF、威胁情报和全流量行为日志于一身,支持对接第三方大数据平台的多功能融合探针。

UTS 通过搭载 IDS 和 WAF 双检测引擎系统，结合威胁情报、恶意文件检测、DDOS 检测、WEBshell 检测和异常行为检测等手段能快速检测传统威胁和高级威胁，同时配合自身的阻断策略对威胁进行快速旁路阻断，缩短用户响应处置时间，此外还可通过输出标准化日志对接态势平台进行统一威胁呈现和回溯分析。

## 2. 客户价值


- **降低采购成本**

  UTS 不仅融合绿盟 IDS、WAF、威胁情报和恶意文件等系统的检测能力，还能对接第三方 SIEM 平台，满足用户多期建设需求，无需多次购买单检测类型硬件设备。此外 UTS 不仅拥有硬件版本还支持软件部署，用户可自配硬件资源，这极大的提高了用户安全建设的能力。

- **提高威胁发现能力**

  UTS 融合多款检测产品，拥有多种检测手段，支持传统威胁检测(覆盖入侵行为检测和 WEB 攻击检测)和高级威胁检测（覆盖恶意代码检测和 APT 事件）。

- **提升威胁回溯分析和取证能力**

  UTS 支持全流量采集和存储，用户在发现威胁后可对威胁相关的元数据进行检索获取攻击的上下文信息，同时支持对相关 pcap 进行提取作为物证。

- **缩短威胁响应处置时间**

  UTS 支持旁路阻断，在发现威胁后可根据策略自动阻断攻击者，同时对外提供一键封堵接口，在平台上也能立即响应处置。

## 3.产品优势

- 检测能力强

UTS 搭载 IDS 和 WAF 双引擎检测系统，能对入侵行为和 WEB 攻击进行精准检测和研判，快准狠。

- 可对接第三方 SIEM 平台

UTS 支持标准化日志输出（syslog/sftp），不仅可对接我司平台也可对接第三方平台，投标灵活。

- 旁路部署，易交付

  UTS 拥有硬件版本和软件版本能快速部署满足不同环境需求，旁路接入到网络中，上电即用，省时省心。

## 4.关键技术

- 全流量采集和存储技术

  UTS 使用自定义的高性能内核和驱动程序，能对实时采集的流量进行元数据提取和存储，支持最高 2Gbps 网络流量全量 pcap 包留存。

- 多检测引擎融合技术

UTS 采用虚拟化技术，融合 IDS、WAF、威胁情报、DDOS、WEBshell 和恶意文件多个检测引擎，极大提高了单产品检测能力

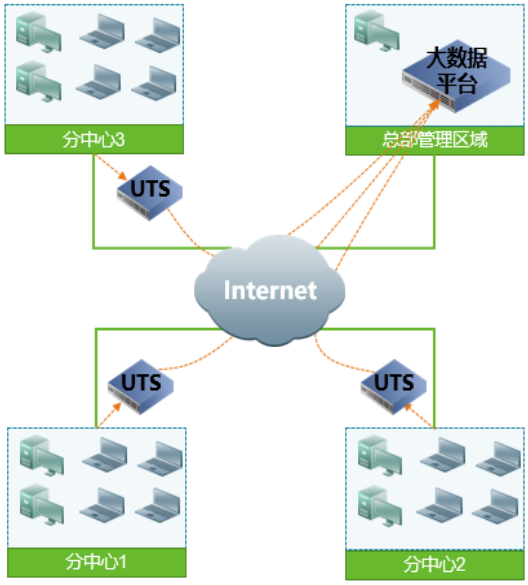
- 机器学习检测引擎

  UTS 内置基于文件特征检测模型和基于流量行为特征检测模型能对文件进行检测和分析，发现未知威胁。

## 5. 典型应用场景

### 场景 1：威胁态势感知

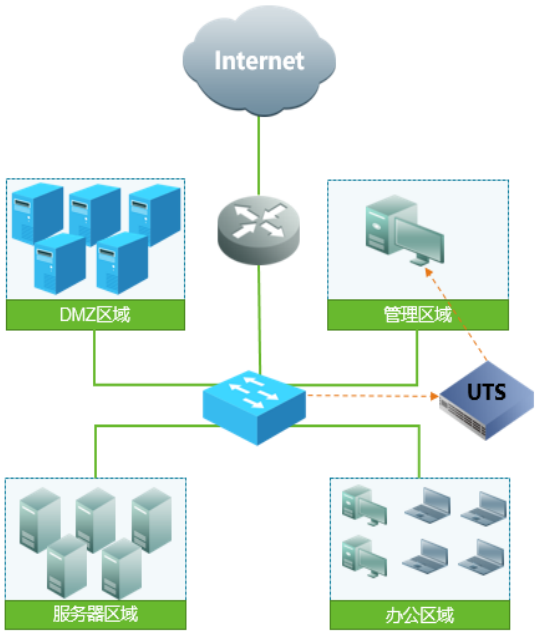
需求：用户组建分布式的态势感知平台，对多个区域的流量进行威胁检测、汇总分析。




| 部署：UTS+大数据平台（含第三方平台） |
| --- |
| 1.全流量采集 |
| 2.全流量存储 |
| 3.多维度检测：入侵行为检测、WEB应用检测、威胁情报检测、恶意文件检测、webshell检测、DDOS检测、异常行为检测 |
| 4.整体回溯分析，可对元数据、pcap进行追溯分析 |
| 5.旁路阻断，对攻击IP、恶意域名流量进行阻断 |
| 6.取证，可提取原始数据包作为证物 |
| 7.整体威胁态势展示、关联分析 |

### 场景 2：未知威胁检测

需求：用户在核心资产处部署探针对其访问流量进行实时监测，结合实时的威胁情报和领先的机器学习检测模型快速发现 APT 事件定位失陷资产，缩短响应时间，将重大事件影响降到最低（同时满足等保 2.0 需求：抗 APT 攻击系统、网络回溯系统和威胁情报检测系统）。




| 部署：UTS |
| --- |
| 1.全流量采集 |
| 2.全流量存储 |
| 3.多维度检测：入侵行为检测、WEB应用检测、威胁情报检测、恶意文件检测、webshell检测、DDOS检测、异常行为检测 |
| 4.回溯分析，可对元数据、pcap进行追溯分析 |
| 5.旁路阻断，对攻击IP、恶意域名流量进行阻断 |
| 6.取证，可提取原始数据包作为证物 |