JUMING 聚铭
让安全更简单

聚铭安全产品

EASIER WAY FOR SECURITY

累计服务10000+政企客户

# 聚铭恶意外连监测及治理系统

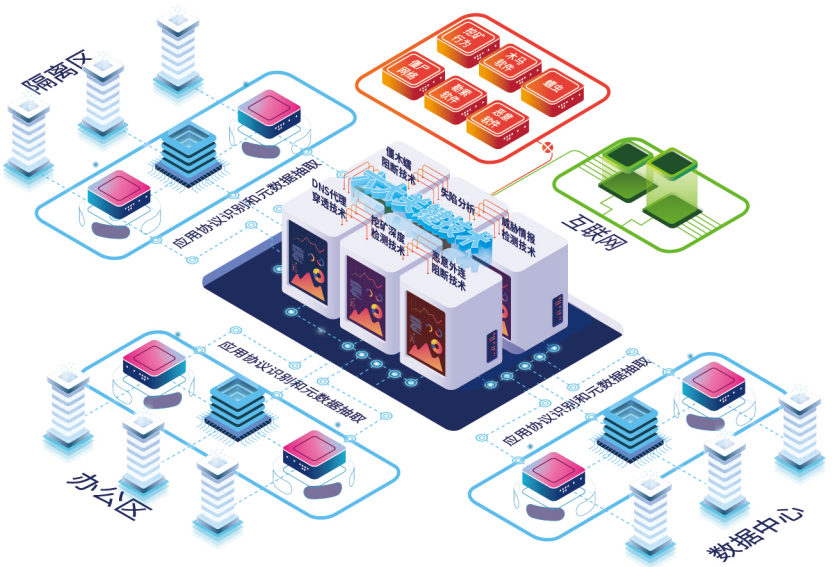
# (IMPS)

聚铭网络
www.juminfo.com

# 聚铭恶意外连监测及治理系统

数字化信息时代，以高危漏洞、病毒木马、勒索软件、挖矿行为等为主的各类恶意网络攻击事件频发，网络安全隐患呈现复杂化和组合化的趋势。对此，聚铭网络推出了新一代网络“扫黑除恶”专项工具——聚铭恶意外连监测及治理系统，用以检测全网安全管理漏洞，识别阻断恶意外连行为。

客户所有的内部网络流量通过聚铭恶意外连监测及治理系统设备出网，经过混合情报引擎和安全规则库及 AI 智能模型检测，能够将所有的恶意程序行为、恶意访问行为、不良信息进行 100% 拦截，保证出网流量是绿色安全的。阻断的方式包括 IP、DNS、数通设备联动、防火墙联动等。同时可对安全事件进行溯源分析，定位具体设备和责任人，解决被通报难题。




## 1 行业现状

**恶意网络行为持续活跃：**违规外连使原本封闭的系统环境暴露在互联网之中，内部网络将面临病毒、木马、非授权访问、数据泄密、数据篡改等多种安全威胁，给企业经营和管理带来极大影响。

**实名定位溯源难：**传统的网络安全设备缺乏未知威胁防护能力，无法快速发现未知威胁，追溯威胁来源。

**政策监管压力大：**国家信息安全监管体系向下辐射，专线、IDC、CDN、DNS 等流量会被监管通报。

## 2 系统架构


## 3 核心功能

- 实时流量解析
- 多源情报分析
- 多样化恶意行为检测
- 多场景智能阻断策略
- 网络威胁态势感知
- 威胁猎捕溯源研判

## 产品优势

### 混合精准情报

融合多家情报，提升情报的精准度。

### 全面的威胁检测

支持挖矿行为阻断，支持包括漏洞利用、WEB攻击、SQL 注入等入侵威胁检测，支持僵尸网络、木马、勒索软件、钓鱼站点等在内的恶意软件请求攻击检测。

### 灵活的部署方式

旁路 SPAN 及 TAP 部署方式，不改变用户现有网络架构和网络配置。

### 联动响应智能阻断

阻断、取证等联动手段多样，支持旁路高速阻断；支持 DNS 在线阻断；支持安恒、山石、深信服、飞塔等防火墙联动封禁；支持华为、华三、锐捷等交换机 ACL 策略联动响应。提升处置效率，降低人工投入。

## 技术优势

### 恶意加密流量检测技术

利用机器学习能力和TLS/SSL特征，结合DNS请求综合研判恶意软件的活动，明显提升加密流量检测能力，通过千万级的恶意样本验证，将恶意加密流量的检测准确率提升至99.8%。

### DNS 代理穿透技术

基于全流量中的DNS代理服务器上下文行为以及终端上下文行为，结合机器学习、关联分析等分析方法，精准定位真实失陷主机，彻底解决DNS代理误报导致的用户溯源定位难问题，提升取证溯源效率。

### 恶意外连阻断技术

动态阻断策略，仅阻断与挖矿相关的请求，在不影响正常业务的前提下，对挖矿应用流量实现阻断，阻断成功率可达100%，并且在客户内网即可实现阻断，真正做到挖矿流量不出网。

### 恶意软件定向抓捕技术

通过深度分析失陷主机的异常流量行为，无需安装agent，使用绿色版抓捕工具，即可在失陷主机上对挖矿、木马软件、病毒程序进行精准抓捕，让恶意软件无处遁形。

## 产品价值

### NO.1

基于恶意外连检测及治理方案有效发现已知及未知威胁，如勒索软件、挖矿等僵木蠕及未知加密恶意通讯，全面提升安全监测能力。

### NO.2

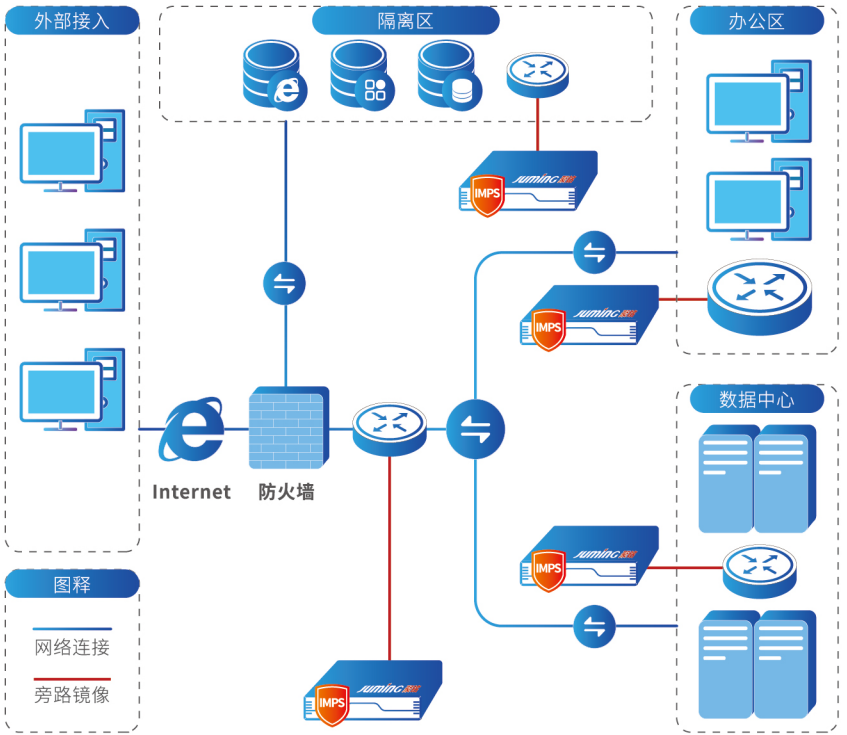
采用应急响应处置流程，先抑制，后治理。依托聚铭威胁情报平台及其他多种恶意程序监测技术，更全面、精准的识别安全隐患，提前阻断恶意通讯，降低被监管单位通报的概率。

### NO.3

面对检测到的恶意外连行为，以及被监管单位通报的安全事件，可以快速精准地定位到具体设备，具体人员，积极响应整改。

# 部署方式

聚铭恶意外连监测及治理系统采用旁路 SPAN 部署方式和 TAP 部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响。设备部署的示意图如下：



聚铭 Juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】
【ISO14001环境管理体系认证】【ISO45001职业健康安全管理体系认证】
【CCRC信息安全风险评估服务资质认证】【CCRC信息安全应急处理服务资质认证】

公司地址：江苏省南京市雨花台区软件大道180号南京大数据产业基地7栋4层
电话：025-52205520　　传真：025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com