NETWORK AND APPLICATION
SECURITY
SOLUTION PROVIDER

新一代威胁分析专家

NSFOCUS TAC

绿盟威胁分析系统

NSFOCUS THREAT ANALYSIS CENTER

如需获取更多信息，请访问www.nsfocus.com

www.nsfocus.com

总部 地址：北京市海淀区北洼路4号益泰大厦3层
电话：010-68438880 邮编：100089

美国子公司 地址：美国加利福尼亚州圣克拉拉市2520 Mission College Blvd Suite 103 Santa Clara CA 95054 USA
电话：+1 408-907-6638 邮编：95054

日本子公司 地址：日本东京都千代田区神田须田町1-26高野大厦7层(7F，1-26，Kandasudacho，Chiyoda-ku，Tokyo 101-0041，Japan)
电话：+81-3-6206-8156 邮编：101-0041

欧洲及中东子公司 地址：#2.09 Saunders House 52-53 The Mall Greater London
电话：+44 (0)20 30786850 邮编：W5 3TA

德国子公司 地址：Hanauer Landstraße 291 B 60314 Frankfurt Germany
邮编：60314

亚太子公司 地址： 26-03 PSA Building 460 Alexandra Road Singapore 119963
电话：+65 6809-3128 邮编：119963

香港子公司 地址：15/B Building 15 Cheuk Nang Plaza No.250 Hennessy Road Hong Kong

中央业务部 地址：北京市海淀区车道沟1号青东商务区A座西6层
电话：010 68438880 邮编：100089

华北区

北京 地址：北京市海淀区花园东路11号泰兴大厦11层1101室
电话：010-59610688 邮编：100191

石家庄 地址：河北省石家庄市长安区中山东路598号融通·财金大厦14层1401、1405室
电话：0311-68019861/62/63/64 邮编：050011

济南 地址：山东省济南市历下区浪漫大街68号济南玉泉森信大酒店B座16层1606室
电话：0531-85108806 邮编：250063

太原 地址：山西省太原市高新区长治路306号火炬创业大厦C座2510、2511室
电话：0351-7555987 邮编：030012

呼和浩特 地址：内蒙古自治区呼和浩特市赛罕区呼伦南路119号东达城市广场商务楼706室
电话：0471-5255518 邮编：010020

天津 地址：天津市南开区黄河道与广开四马路交口34号格调大厦4层406、407室
电话：022-83192366 邮编：300102

青岛 地址：山东省青岛市市南区宁夏路288号青岛软件园2号楼16层
电话：0532-85733520 邮编：266071

华东区

上海 地址：上海市黄浦区蒙自路763号丰盛创建大厦2005室
电话：021-62179591 邮编：200023

杭州 地址：浙江省杭州市下城区体育场路229号粮油大厦1106室
电话：0571-85778560 邮编：310003

南京 地址：江苏省南京市白下区汉中路1号国际金融中心46层E座
电话：025-83247712 邮编：210029

南昌 地址：江西省南昌市北京东路448号恒茂梦时代广场7号办公楼1208室
电话：0791-86662623 邮编：330029

苏州 地址：江苏省苏州市工业园区苏月路华盛苑10栋306室
电话：0512-62935332 邮编：215021

温州 地址：浙江省温州市鹿城区车站大道诚信商厦2幢2301室
电话：0577-86790571 邮编：325088

宁波 地址：浙江省宁波市江东区东胜路11号凌江名庭45楼4501室
电话：0574-87736971 邮编：315040

华南区

广州 地址：广东省广州市荔湾区康王中路486号和业广场15楼1501-1503室
电话：020-81301251 邮编：510145

深圳 地址：广东省深圳市深南大道竹子林中国经贸大厦21楼FGH室
电话：0755-88316319 邮编：518048

福州 地址：福建省福州市鼓楼区东街96号东方大厦18层C区
电话：0591-83300623 邮编：350001

南宁 地址：广西壮族自治区南宁市青秀区金湖路59号地王国际商业中心12G
电话：0771-5605255 邮编：530021

海口 地址：海南省海口市龙华区玉沙路11-8号玉沙国际4楼401室
电话：0898-66596097 邮编：570125

厦门 地址：福建省厦门市思明区莲前西路2号莲富大厦18G
电话：0592-5821591 邮编：361000

泉州 地址：福建省泉州市丰泽区刺桐明珠裕兴苑D栋801单元
电话：0595-22899787 邮编：362000

漳州 地址：福建省漳州市芗城区延安北路29号钱隆首府10栋1302室
电话：0596-2038832 邮编：363000

三亚 地址：海南省三亚市河东区迎宾路聚鑫园C栋7C04号
电话：0898-66596097 邮编：570206

西南区

成都 地址：四川省成都市武侯区人民南路三段2号汇日央扩大厦1栋25楼5号
电话：028-86632080 邮编：610041

成都研发中心 地址：成都市高新区科园二路10号航利中心一期工程2栋2单元14楼1号及2号
电话：028-66330466 邮编：610000

重庆 地址：重庆市北部新区青枫北路高新园拓展区双子座A座18-3
电话：023-67997503 邮编：401122

昆明 地址：云南省昆明市盘龙区白塔路131号云南汇都国际B座B8015室
电话：0871-63130419 邮编：650011

贵阳 地址：贵州省贵阳市南明区花果园大街1号花果园项目C区贵阳国际中心2号楼8层13号
电话：0851-88508965 邮编：550003

拉萨 地址：西藏自治区拉萨市当热西路52号天路康卓小区12栋2号
电话：0891-6846788 邮编：854000

华中区

武汉 地址：湖北省武汉市江汉区建设大道568号新世界国贸大厦2906室
电话：027-85267921/7925/7901/7910/8096 邮编：430022

武汉研发中心 地址：湖北省武汉市东湖开发区光谷软件园A9座1楼
电话：027-87611190 邮编：430074

合肥 地址：安徽省合肥市包河区马鞍山路130号万达广场7号楼2202室
电话：0551-65114777 邮编：230011

郑州 地址：河南省郑州市金水区农业路71号中州国际饭店2410室
电话：0371-63581386 邮编：450002

长沙 地址：湖南省长沙市开福区中山路589号开福万达广场A座写字楼44002室
电话：0731-84447448 邮编：410000

西北区

西安 地址：陕西省西安市高新区科技路48号创业广场B座2506
电话：029-88327733、88322383、88321292 邮编：710075

西安研发中心 地址：陕西省西安市高新区科创路168号西电科技园C座5层509
电话：029-89195565 邮编：710065

兰州 地址：甘肃省兰州市城关区雁南路天庆大厦588号天庆国际商务大厦8层816室
电话：0931-8888422 邮编：730010

乌鲁木齐 地址：新疆维吾尔自治区乌鲁木齐市新市区北京南路358号大成国际18层1805室
电话：0991-2323233 邮编：830000

银川 地址：宁夏回族自治区银川市金凤区北京中路瑞银财富中心C座12-4室
电话：0951-6088774、0931-8888422 邮编：750002

西宁 地址：青海省西宁市冷湖路10号2号楼4单元461室
电话：0971-6280673 邮编：810008

东北区

沈阳 地址：辽宁省沈阳市沈河区惠工街10号卓越大厦2910室
电话：024-22511115 邮编：110013

哈尔滨 地址：黑龙江省哈尔滨市开发区长江路398号会展总部大厦603室
电话：0451-82892102 邮编：150090

长春 地址：吉林省长春市南关区人民大街4848号华贸国际大厦1103室
电话：0431-81912151 邮编：130022

NSFOCUS

NSFOCUS PRODUCT PORTFOLIO

绿盟科技安全产品系列

TAC

nsfocus.com

NSFOCUS

TAC

绿盟威胁分析系统

NSFOCUS

THREAT ANALYSIS CENTER

THE EXPERT BEHIND GIANTS

产品概述

绿盟威胁分析系统（简称TAC）可以精确检测通过网页、电子邮件等方式试图进入内部网络的恶意软件，包括零日攻击及具有抗检测能力的高级恶意软件。当前的恶意软件大多具备强大的抗逃避能力，而APT攻击还可能使用零日攻击的方式，传统的防病毒引擎很难发现它们。TAC通过新型的虚拟执行检测技术可以有效发现这些攻击行为，帮助客户有效的遏制由此带来的风险，如敏感信息泄露、业务中断等。

客户价值

网络安全事件的发展显示骇客正在使用越来越精密且有效率的方式来进行攻击。通过鱼叉式钓鱼邮件或者水坑式攻击的方式，利用高级恶意软件去攻击终端主机，以进入组织的内部网络，进行偷窃或破坏。由于这种高级恶意软件的具备的特点（如：多种逃避检测技术、针对特定目标、零日攻击等）传统安全产品很难及时发现。组织不能有效的抵御这些高级恶意软件，意味有可能存在以下的风险。

- 竞争力受损：攻击者有可能盗窃商业机密、客户记录等业务资料，也有可能窃取知识产权信息，这些数据的曝光或者被竞争对手掌握，都可能严重损害竞争力。
- 声誉受损：客户和合作伙伴的信任是市场成功的关键，被曝光的安全事件、泄露客户个人资料以及成为攻击跳板都可能迅速的破坏这种信任关系。
- 业务中断：部分攻击的目的是为了中断组织的相关业务，使其无法正常运转。而安全事件爆发后的处理也会严重影响正常的运营。
- TAC产品通过及时、准确的检测高级恶意软件，在最关键的位置阻止攻击者的对内渗透，从而保障了内部关键IT资产和业务的安全，是面对当前的威胁形式，最重要的安全检测产品。

产品优势

检测已知和零日攻击，抗逃避能力强

基于不依赖已知攻击特征的虚拟执行技术，可以检测利用零日漏洞以及其它传统防病毒引擎无法检测的高级恶意软件。不同于沙箱技术仅在行为层面进行检测，可以通过内存指令级分析，在漏洞利用阶段发现攻击，对抗针对沙箱技术的逃避技术。

检测恶意软件全生命周期活动

对恶意软件在终端的整个活动进行分析，跟踪漏洞利用、软件下载、回连命令控制服务器外传数据等恶意软件各阶段的活动行为，并输出详细的入侵行为报告。

分析应用协议及文件类型全面

覆盖主要的传输协议：http、smtp、pop3、ftp等，同时可以对黑客利用的主要文件类型全面检测，包括Office文档、PDF等，并可对压缩文件进行检测。

检测精确

基于恶意软件在模拟环境下运行的真实行为做判断，误报的几率可以忽略不计，使安全专家聚焦响应真正的威胁，保障安全运维的效率和效果。

多引擎集成，提供事件响应的优先排序

集成多种传统检测引擎，可以通过报警比对等方式了解威胁的严重程度，确定事件响应的优先级。并同时面对传统恶意软件提供更高的检测能力。

提供闭环的纵深解决方案

通过二级信誉系统（企业本地信誉库、全球信誉库）联动IPS，自动化阻截恶意软件的下载及回连活动，保障防御的及时性。同时提供事件的关联分析、攻击的地理位置视图等先进的可视化能力，更直观的了解威胁态势。

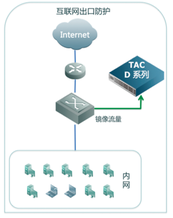
关键功能

部署方式	旁路部署	D系列产品对镜像的网络流量进行还原和检测
	邮件代理	E系列产品基于MTA检测并拦截邮件威胁
检测类型	应用协议	HTTP、SMTP、POP3、FTP、IMAP
	文件类型	Office文档、Java、PDF等，支持常见压缩格式
检测能力	虚拟执行检测	多个虚拟环境检测漏洞利用及后续的恶意行为特征，发现零日攻击及高级恶意软件
	其它检测技术	启发式检测、漏洞利用检测、AV检测
管理报表	管理方式	CLI、Web界面、集中管理软件ESPC
	实时监控	系统状态监控、24小时威胁数量统计、TOP事件监控，最近威胁事件等
	日志功能	日志的查询、导出、删除等
	常规报表	基于威胁来源地理位置、基于主机、基于用户、基于应用协议及文件类型等
	统计分析	基于受害主机、基于恶意软件类型、基于回连命令控制服务器地址；基于地图的实时统计监控

典型应用

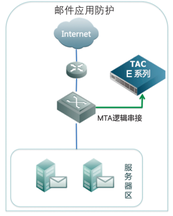
场景一：互联网出口防护

- 检测通过互联网Web浏览等方式进入的高级恶意软件



场景二：邮件高级威胁防护

- 检测并拦截通过邮件传播的高级恶意软件



场景三：文件及目录扫描

- 检测通过移动存储及服务器共享目录传播的高级恶意软件