NSFOCUS

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于网络安全技术的研究，
为政府、运营商、金融、能源等行业提供优质的安全产品与服务。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com.cn

智慧安全 2.0

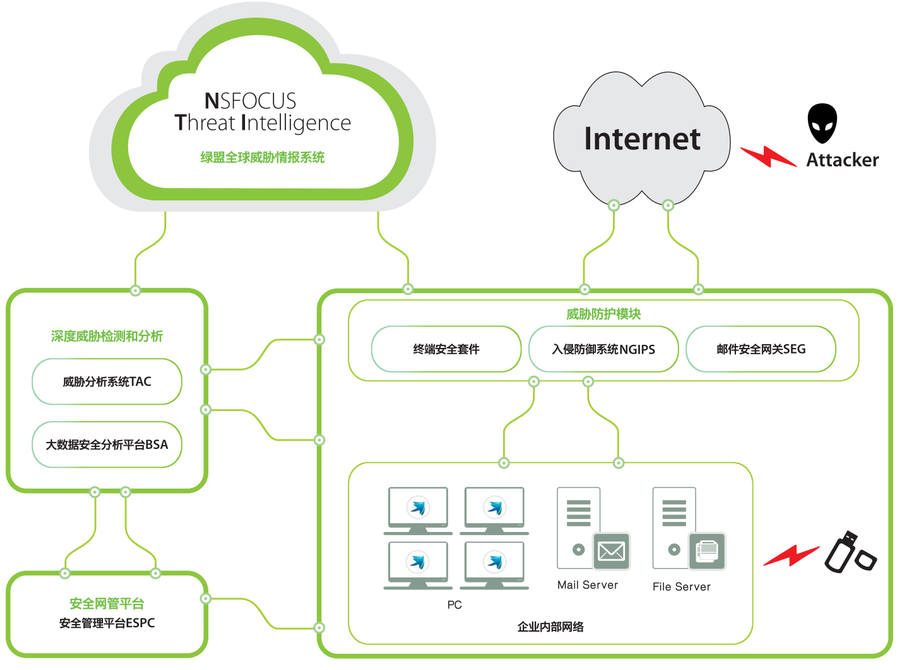
绿盟科技
下一代威胁防御
解决方案

NSFOCUS

NEXT-GENERATION THREAT PROTECTION SOLUTION

NSFOCUS

智慧安全2.0



下一代威胁防御解决方案

方案概述
OVERVIEW

网络安全威胁与互联网发展如影相随。高级持续性威胁（APT）备受关注，APT威胁持续时间长，攻击的范围广，造成的影响大。APT攻击针对政府、金融、电信、能源、高科技等行业，具有高度隐秘、攻击技术高超、攻击团队专业等特点。有些APT攻击以长期潜伏在受害者系统，持续获取敏感信息，有些APT攻击破坏电力能源等基础设施，给企业和政府部门造成严重危害。然而，传统安全产品，如防病毒，入侵检测系统等，基于“特征码”的检测技术，不能有效识别和防护APT威胁。

绿盟下一代威胁防御解决方案（简称NGTP）可以有效的对包括APT攻击在内的威胁进行检测和防御。NGTP方案通过绿盟全球威胁情报系统（NTI）实现威胁信息的共享与实时推送，在具体防护方法上，以检测未知威胁为核心，通过智能网管和大数据分析技术，对来自终端、安全网关、操作系统的告警信息进行综合分析、可视化呈现和管控，在降低安全运维成本的基础上，极大的提升了企业安全防护能力。

方案功能
FUNCTIONS

☆ NGTP解决方案组件

NGTP解决方案集成多个安全模块来实现全面威胁防护。这些模块包含：

- 未知威胁检测模块
- 威胁防护模块
- 大数据安全分析模块
- 全球威胁情报系统
- 安全管理平台

NGTP解决方案，包含了威胁分析系统TAC，入侵防御系统IPS，邮件安全网关SEG，终端安全产品，以及综合安全管理平台，绿盟威胁情报系统。

通过模块间的关联协作，检测和防御进入企业的全部威胁，对网络、邮件、终端等传统安全威胁进行检测防御，也对APT高级威胁进行检测和防御。

未知威胁检测模块

TAC产品作为NGTP解决方案的未知威胁检测模块，负责对APT威胁的分析和检测，是方案的核心模块。首先TAC对网络流量进行文件还原，对恶意软件进行识别；另外通过开放API接口，TAC还对邮件网关和终端的可疑文件进行检测，并把检测的结果进行反馈，实现对威胁的阻断关联。

威胁防护模块

NGIPS/NGFW，邮件网关，终端安全产品，是NGTP解决方案防护模块。这些产品既发挥传统安全产品的功能，又与TAC产品关联协同，组成安全防护体系。在NGTP解决方案中，提交不能识别的可疑文件，由TAC进行分析，并根据TAC的分析结果进行阻断。

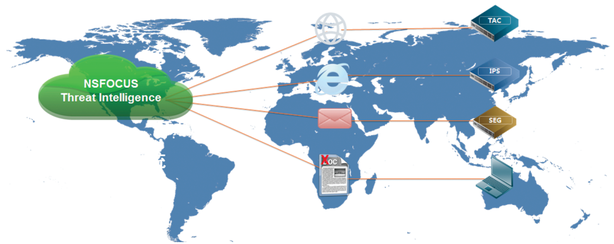
大数据安全分析模块

通过收集未知威胁检测模块和威胁防护模块的告警信息，包括网络、上网、邮件、终端等多个数据源，综合网络和主机的日志，进行收据索引和分析，抽丝剥茧，进行攻击的蛛丝马迹的洞察。

02
下一代威胁防御解决方案
NEXT-GENERATION THREAT PROTECTION SOLUTION
方案功能
绿盟科技下一代威胁防御解决方案

全球威胁情报系统

NTI（NSFocus Threat Intelligence）作为云端的信誉情报系统，为NGTP解决方案中的模块提供信誉情报，极大提高整个系统对威胁的识别的准确性和效率。



安全管理平台

安全管理平台负责管理NGTP方案中的各个模块，下发检测和防护策略，采集设备的状态信息存储告警日志，进行报表呈现等。

☆ NGTP检测和防护流程

从NGTP解决方案中各个模块的介绍可以看到，整体方案中包含了网络IPS，邮件安全网关和终端安全套件，从网络、邮件和终端层面抵御安全威胁的侵入；TAC承担了本地沙箱的功能，对高级威胁，尤其是防护模块不能识别的威胁，由TAC进行深入检测分析；再把分析结果进行反馈，防护模块根据TAC的反馈采取阻断动作，实现对高级威胁的阻断。

预警检测

NGTP解决方案防护模块中的产品，通过及时升级自身的攻击签名、病毒特征码及时发现各种威胁，而且，这些产品还会从云端情报系统更新最新的信誉信息，进行威胁检测和预警；TAC产品接受来自不同渠道的高级可疑文件，通过静态Shellcode检测和虚拟执行分析，进行预警检测。

攻击拦截

防护模块拦截已知攻击威胁，并通过与TAC的关联，对未知高级威胁也进行拦截。

可视化分析

威胁告警事件上报到安管平台ESPC或者BSA后，结合网络环境和资产，对安全事件进行汇聚关联，通过安全建模，形成威胁可视化分析。

应急响应

发生安全事件后， 尤其是比较严重的APT攻击事件，需要企业启动应急响应机制，快速评估威胁的原因，范围和影响，清除恶意软件，把危害降到最低。

绿盟提供基于线上和线下的恶意软件清除服务，能够帮助客户更好的分析事件造成的影响，并提供恶意软件清除服务 。

02
下一代威胁防御解决方案
NEXT-GENERATION THREAT PROTECTION SOLUTION
方案功能
绿盟科技下一代威胁防御解决方案

☆ NGTP解决方案优势

威胁检测和防御的全面性

绿盟下一代威胁解决方案，能够全面有效的对APT威胁检测和防御。网络，Web还是邮件，终端等，都是APT威胁可能利用的通道，NGTP解决方案，不仅在网络边界进检测和防御，还在企业内网，邮件服务器，终端等多个层面进行检测和防御。既能够实时进行检测和阻断，还利用大数据分析平台，进行事后的分析和调查。

APT检测的准确性

绿盟下一代威胁解决方案，利用本地沙箱和云端安全信誉，有效地对APT威胁检测和防御。本地沙箱提供了恶意软件静态检测和虚拟执行分析，检查恶意软件Shellcode，并且模拟真实的PC环境进行验证，极大提高恶意软件的准确性；同时，云端信誉提供最新的威胁情报信息，进一步提供NGTP方案对APT威胁检测的准确性。

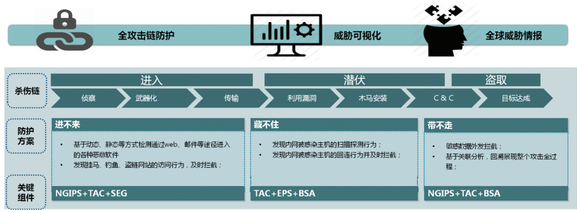
解决方案技术成熟

组成NGTP解决方案的各个模块技术成熟。TAC威胁分析系统是国内较早推向市场的APT安全监测设备，Shellcode检测技术和虚拟执行技术的应用，为APT威胁检测提供强力支撑。绿盟IPS产品久负盛誉，屡获国内外权威咨询机构的认可。绿盟安全威胁信誉系统，提供全面及时的安全信誉，让NGTP方案发挥最大效能。

☆ NGTP解决方案部署场景

APT高级持续性攻击，普遍采用“攻击链”的方式逐步渗透。总体来说，可以分为三个大的环节，即尝试进入阶段，潜伏扩散阶段，数据盗取阶段。

NGTP解决方案能够对APT威胁进行检测和防御，切断APT威胁的攻击链，在威胁尝试进入企业，在企业内部进行扩散，以及最后的信息盗取的每一个环节，都有对应的部署场景。



按照威胁进入通道进行分类，NGTP可以按照以下场景进行部署：

NGTP网络高级威胁场景（NGIPS+TAC）

APT常常利用“水坑攻击”进行渗透，入侵防护系统和威胁分析系统能够互相配合，优先检测和抵御此类攻击。网络高级威胁场景，TAC提供了更加灵活的部署方式。其一，TAC可以作为旁路设备，监控网络流量中的高级威胁，同时还能够通过REST APL，接受来自IPS的文件提交，经过动态引擎分析后，把本地信誉返回给NGIPS进行告警和防御；其二，TAC可以作为NGIPS的沙箱模块，与NGIPS一起协作，能够同时对传统威胁和未知高级威胁进行防护。

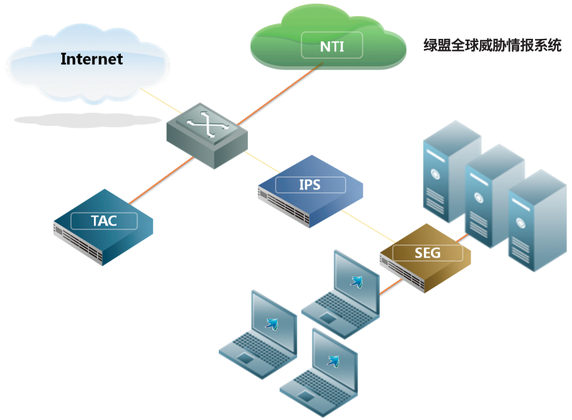
NGTP邮件高级威胁场景（SEG+TAC）

“鱼叉攻击”，是APT威胁另一种攻击方式，这种定向的钓鱼方式更隐蔽也更有诱惑力。采用SEG邮件安全网关和威胁分析系统，能有效识别通过邮件定向钓鱼的渗透尝试，把APT威胁拦截在外。

NGTP终端高级威胁场景（EPS+TAC）

终端安全套件，提供了防病毒之外的防护。终端把可疑的恶意软件提交给TAC，经过TAC对威胁的静态检测和虚拟执行后，在根据分析结果采取防护动作。

上面这些部署场景是威胁分析系统加上一种威胁防护系统的组合方案。还可以根据实际情况，防护系统两两组合，比如网络和邮件，邮件和终端等。根据防护通道的侧重来选择和组合不同的部署场景。



方案价值
VALUE

NGTP解决方案，有效检测和防御APT威胁，帮助企业建立安全防护的金钟罩。

☆ 威胁“进不来”

NGTP解决方案把安全威胁阻挡在企业外网，防止威胁进入到企业。攻击初始阶段的检测和防御，是NGTP解决方案的重中之重。在攻击初始阶段，攻击者常用“水坑攻击”和“钓鱼邮件”方式，定向诱导用户上网下载软件或者打开邮件，以此感染恶意软件。NGTP解决方案，从上网，邮件，终端等不同层面对威胁进行检测和防御。

☆ 扩散“藏不住”

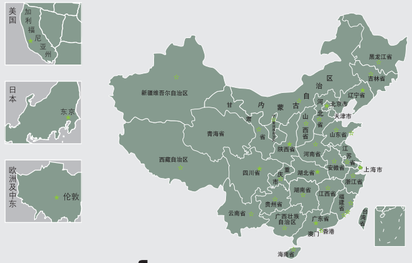
内网中已经存在的威胁，通过大数据分析引擎进行分析，检测出恶意流量和主机。对少部分进入到网络的威胁，在其尝试扩散攻击时及时检测和防护。终端安全套件既能防范已知威胁，还会和TAC进行联动，检测高级威胁，让其无所遁形。通过大数据分析网络流量、注册表等异常，分析APT威胁的蛛丝马迹。

☆ 敏感数据“带不走”

敏感数据泄露防护。 APT威胁是以窃取敏感数据为最终目的。经过APT威胁检测和防御，已经能够将绝大部分的威胁拒之门外，最后通过数据泄露防护，让APT威胁不能完成目的，有效保护敏感数据。

NGTP解决方案，为企业构建了立体的威胁防护体系。从网络边界到内网终端，既防御传统安全威胁，还特别针对APT的攻击进行检测和防御。通过对网络，邮件，终端的恶意软件进行关联分析，从云端到本地的综合防护，形成预警、检测、防护、清除的安全威胁防护闭环。

绿盟科技分支机构 NSFOCUS BRANCH OFFICES



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39号勤泰中心B座1105
电话：0311-68019861/62/63/64 邮编：050011

济南 地址：山东省济南市历下区泺源大街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：山西省太原市小店区南中环街火炬创业大厦C座2510-11室
电话：0351-7555987/88 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706A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2004-2006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：江苏省南京市秦淮区汉中路1号国际金融中心46楼E座
电话：025-83247712 邮编：215021

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：苏州市苏站路1398号喜临门商业广场4幢8005
电话：0512-62935332 邮编：215021

温州 地址：浙江省温州市鹿城区秀山路46号锦华公寓2幢306
电话：0577-86790571 邮编：325000

宁波 地址：浙江宁波鄞州区钟公庙街道风格尚品8幢602室
电话：0574-87736971 邮编：315100

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东葛路延长线118号青秀万达广场西二栋3115-3117室
电话：0771-5605255 邮编：530021

海口 地址：地址：海南省海口市龙华区国贸路2号海南时代广场17楼C座
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

西南区

成都 地址：四川省成都市武侯区人民南路四段3号成都来福士广场办公楼塔1栋第21层01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：西藏自治区拉萨市巴尔库路15号天路康卓小区25栋1−1号（1−2层）
电话：0891-6846788 邮编：850015

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：430074

武汉研发中心 地址：湖北省武汉市洪山区光谷软件园A9座3楼
电话：027-87611190 邮编：430074

合肥 地址：安徽省合肥市政务区银泰城华邦ICC-A座写字楼1902室
电话：0551-63869943 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2411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：陕西省西安市高新技术开发区丈八四路20号神州数据科技园1号楼8层
电话：029-89195565 邮编：710077

兰州 地址：甘肃省兰州市城关区张掖路一号保利大厦A座8楼801室
电话：0931-8888422 邮编：730010

乌鲁木齐 地址：新疆乌鲁木齐市水磨沟区红光山路2588号绿地中心领海101-1306
电话：0991-2323233 邮编：830000

银川 地址：宁夏回族自治区银川市兴庆区世和天玺国际中心B座10层1023、1025号
电话：0951-6088774 邮编：750000

西宁 地址：青海省西宁市城西区昆仑路四号麒麟花园一号楼1223室
电话：0931-8556697 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：黑龙江省哈尔滨市香坊区中山路93号保利科技大厦615室
电话：0451-82892102 邮编：150036

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