安全+
SECURITY
2020/04 总第044
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

绿盟极光，用专注惊艳了时光

智能安全运营平台的进阶之路

过往20年看安全服务变迁

20

绿盟科技官方微信

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-5463
传真：(010)6872 8708
网址：www.nsfocus.com

2020/04 总第 044

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。（本刊部分图片来源于网络）

安全+ SECURITY+

目录 CONTENTS

光阴荏苒，当年水泥地里长出来的小草，经过绿盟人汗水与心血的浇灌，终于长成了如今的参天大树。

20 年风风雨雨，绿盟科技始终走在创新的路上，践行“专攻术业，成就所托”的愿景。保障客户业务顺畅运行，这也是专业安全团队始终秉持的使命。创新已然刻入绿盟科技的基因，专注更是绿盟人的品格。

安全能力持续提升是公司的立身之本，也是技术团队最重要的任务。在过去的一年里，安全研究团队在多个新领域的研究成果引人注目。在攻防相长的思路引导下，我们定期举行内部红蓝对抗，并在外部比赛中多次夺冠。充分体现了绿盟科技在攻防领域的积累。

越来越多的企业意识到，过去打补丁、串葫芦的方式无法解决问题，需要对安全进行体系化的设计。绿盟科技始终保持对最佳安全实践的关注，持续对国内外先进的安全架构进行跟踪研究，与产品团队一起将最新的研究成果相结合为客户提供服务过程中的实战经验，实现在智能安全运营平台及相关的产品上。

安全产品的稳定性直接影响客户的业务和使用体验，产品团队始终把提升产品稳定性和可维护性作为最重要的目标，并进行严格的测试。工程团队与研发团队紧密配合，实时跟踪进展情况。

2019 年我们参与了多家企业和机构的安全演练，通过演练，各单位有组织地排查，有效减少攻击面，消除隐患，并在实战中固化以监测－研判－处置构成的威胁监控体系，部分单位安全威胁处置周期降低至秒级、分钟级。在这个过程中，我们的平台和产品得到很好的考验，发挥了重要的作用。

安全运营是保障企业安全体系高效运转的重要手段，也是公司发展的战略方向。在 P2SO 战略转型中，我们一直在践行“云地人机”协同的安全运营体系。重点推进城市、行业安全运营中心、安全增值运营业务布局落地，实现安全运营服务全区域标准化交付落地。

2020 年突如其来的疫情过后，越来越多的企业数字化进程将会进一步加速，产业结构将发生深刻的变化。我们将时刻跟踪、研究、应用最新的技术，对新数字化环境下的安全问题进行研究，努力用技术和模式的创新为客户提供优质的产品和方案。

叶晓虎

大时代，弄潮儿

绿盟科技 创新中心 刘文懋 / 高级安全研究部 左磊、张云海 / 总工办 肖岩军

二十年，对于传统产业而言很短暂，而对于网络安全这个瞬息万变的朝阳产业，却显得格外漫长。网络安全早已不是简单部署防火墙、安装杀毒软件就能高枕无忧的时代了。二十年，网络攻防技术日新月异，攻击者将网络攻击武器化、军火化；防守者抛弃被动防御，转而采用事前主动诱捕，事中纵深防御，事后快速响应的积极策略；与此同时，整个 IT 产业又快速拥抱云计算、物联网和下一代网络等新型基础设施，移动办公、共享经济、普适计算、软件定义一切，让信息产业变得异构、碎片化，在自适应安全、零信任安全、软件定义安全等先进理念的指引下，安全防护正走向体系化、智慧化、敏捷化。

本文首先介绍了安全产业的变迁，然后从安全攻防的自身演化和网络安全大环境两方面回顾了网络安全技术的发展，并介绍了绿盟科技在相关领域的技术发展路线。

一、网络安全的四个五年：安全产业的变迁

2000-2005 年，网络安全消化吸收，安全产品技术获得突破

自从二十世纪末克林顿政府提出“信息高速公路”和“国家信息基础设施”后，互联网高速发展，与之对应的网络安全问题也越来越严重。国际上 ISO27001：2000 版本于 2000 年颁布，SOX 萨班斯方案于 2001 年颁布，等级保护的第一个标准在 1999 年就已颁布，但是缺乏实用的配套落地指南，总体而言，企业都在重点建设网络和信息化的同时，存在对网络安全的重视和投入不足的问题。

总体而言，这五年既是计算机网络高速发展的黄金时期，但也是恶意病毒借互联网快速传播的时期。从几个标志性事件就可以看出：CIH 病毒，首个可以破坏 BIOS 的病毒；红色代码蠕虫，促进了防病毒行业的发展，这些网络蠕虫的发展扩散，一度占据了 60% 以上的 Internet 流量，互联网安全逐步引起人们的重视。网络安全也从数据安全、通信安全概念里脱离并发展出来，成为一个单独的安全领域。

绿盟科技自 2000 年成立后，制订了自研的技术路线，推出了极光扫描器，“冰之眼”入侵检测，“黑洞”抗拒绝服务系统。这期间由于硬件性能的不足，网络安全以评估审计为核心，网络安全三大件——扫描器、入侵检测、防火墙成为主流，主要客户是金融、运营商、政府。这期间，国外的 ISS 扫描器，以色列的防火墙，占据了国内运营商和金融市场。国内安全公司主要有绿盟科技、启明星辰、天融信、安氏等，面对国外产品的竞争，国产设备厂商主要以学习借鉴为主。

2006-2010 年，网络安全转型为管理评估，从旁路审计到串联防护

随着网络安全问题的日益突出，以及金融运营商的海外上市，大家对 ISO 27001 和 SOX 逐渐重视，针对信息安全管理体系的咨询和建设开始增加。2005 年，国家电子政务外网建设启动，政府对国内厂商扶持力度增大。2007 年，等级保护管理办法开始颁布，等级保护也开始真正落地，由此带来了咨询服务的高峰。

安全产品也随之转化，“极光远程安全评估系统”转型为“极光远程安全评估管理系统”，引入 CVSS 等先进的安全积分要素和方法，不仅可以扫描出漏洞，还能评估网络安全状况。随着硬件和

用户流量的快速发展，绿盟 NIDS 网络入侵检测系统转换成 NIPS 网络入侵防御系统。从旁路审计到串联防护，NIPS 和“黑洞”首次突破了 1G 线速。国产硬件大量用在电子政务外网建设、三金工程等国家重点工程。由于与运营商合作，绿盟 NTA 网络流量分析系统成为当时国内唯一的 Netflow 安全分析系统。“黑洞”（Collapsar）抗 DDoS 能力也随着 CC(Challenge Collapsar) 攻击手法的出现而名声大噪，成为抗 DDoS 产品中的第一品牌。这 5 年间，规则升级，攻防对抗成为主流。

随着 2008 年奥运会、2010 年亚运会等大量大型公众型活动的举办，使得安保维稳压力增大，网络安保也大量增加。“美国爱因斯坦”等国家级安全项目也传递到国内，绿盟科技也开始参与大型态势感知保障预警平台的建设。

2011-2015 年，Web 应用安全成为主流，云和 APT 概念被提出

互联网开始高速发展，微信于 2011 年推出，与支付宝大战，电子政务外网建设成果突出，电子银行、网银等深入民心。互联网产业发展提速，随之而来的安全问题也越来越多，网络安全的春天到了。各级政务企业网站建设都成为主流，但网络篡改、挂马层出不穷。大家又把 Web 应用安全从网络安全概念中独立出来，成为一个单独的概念。云的概念开始被行业接受，自 Openstack 和阿里云出现，云计算市场开始扩张，云安全和 SDN 开始兴起，云计算系统也成为网络攻防的新战场，云安全转变为纯粹的网络安全。

近年来，高级持续性威胁（APT）开始成为一个热门词汇。2010 年的震网（Stuxnet）攻击向人们展示了高级持续性威胁的巨大威力，而 FireEye 等厂商发布的一系列 APT 报告使人们意识到高级持续性威胁就在身边。由于使用了 0 day 漏洞和高级漏洞利用技术，传统的安全产品难以有效地防御高级持续性威胁，对未知威胁的检测与防御是安全厂商面临的新挑战。一些新的技术，如威胁情报（Threat Intelligence）、沙箱（Sandboxing）、欺骗（Deception）和攻击模拟（BAS，Breach and Attack Simulation）技术等也应运而生。

2015-2020 年，云大物移万物融合，安全拼的是运营与响应的时效，国家对抗加剧

最近五年，云计算已经成为标准的基础设施，移动互联网、物联网也得到了极大发展，网络安全已经不只是传统的计算机网络，而是囊括了各类复杂、异构、动态和融合的网络，云计算和工业互联网的各类安全事件也层出不穷，甚至上升到国家层面的对抗，单一的解决方案已经无法满足这类应用场景的需求，各类新型的产品和解决方案也在推陈出新。

此外，攻击者借助精良武器库和自动化的技术，攻陷时间越来越短，这就要求防守者在合规性的底线要求基础上，不断打磨己方检测和响应流程，缩短闭环时间。业界也基于自动化编排的技术，推出了如 EDR/NDR 检测响应和 SOAR 自动化编排的产品，以及 MDR 可管理检测响应的服务，目的就是提供自动化、运营化的安全能力，缩短安全检测和处置的时间。

最后，网络空间已经成为国家之间博弈的战场，中美等国都组

建了自己的网络安全部队，保护本国网络空间的安全。事实上，每当国际形势紧张时，都会在网络空间中出现定向的攻击，如乌克兰停电[1]、沙特石油设施遭袭后，国家之间的网络空间对抗加剧[2]，都是另一个形态的战争。在这一大背景下，安全可控成为我国网络安全产业发展的大方向，关键基础设施防护会成为我国未来几年网络安全发展的强驱动力。

二、网络安全的本质：始终是攻与防的博弈

2000 年，主流的漏洞类型是缓冲区溢出（Buffer Overflow）。Elias Levy（A.K.A. Aleph One）在 1996 年发表的《Smashing The Stack For Fun and Profit》和 Christien Rioux（A.K.A. Dil-Dog）在 1998 年发表的《The Tao of Windows Buffer Overflow》使得缓冲区溢出漏洞的利用技术广为人知，因此，攻击者发现缓冲区溢出漏洞之后可以很容易地实现对漏洞的利用。常见的网络服务程序中一旦被发现存在缓冲区溢出漏洞，可以被远程、无交互地进行攻击，往往会形成影响重大的蠕虫事件。2001 年的红色代码蠕虫、2003 年的冲击波蠕虫、2004 年的震荡波蠕虫等都造成了非常巨大的伤害与损失。

为了应对这类威胁，微软等厂商开始在操作系统中引入缓解措施来进行对抗。保护栈数据的 Guard Stack、Safe SEH、SEHOP 等缓解措施使得栈缓冲区漏洞的利用逐渐趋于绝迹；保护堆数据的 Safe Unlink、堆随机化（Heap randomization）、堆元数据保护（Heap metadata protection）等缓解措施也极大地减少了堆缓冲区漏洞的利用。更重要的是数据执行保护（DEP）与地址空间布局随机化（ASLR）的引入使得之前的通用漏洞利用技术不再有效，缓解措施的绕过成为漏洞利用过程中必不可少的重要环节。

到了 2010 年，缓冲区溢出漏洞逐渐减少，主流的漏洞类型开始转向释放后重用（UAF）。缓解措施的引入提高了漏洞利用的门槛，漏洞利用技术不再是人人可用，然而可以绕过缓解措施的高级漏洞技术依然存在。为了绕过缓解措施，攻击者往往需要进行一系列复杂的操作，从控制内存布局到获得任意地址读写能力，最终实现任意代码执行。因此，攻击的目标也由网络服务程序转向客户端程序（比如浏览器、PDF 文档阅读器、办公软件 Office 等），以便通过脚本语言等来获得所需的控制能力。

2015 年，微软发布了新的操作系统 Windows 10，同时开始执行新的更新策略：每年两次大版本更新，每次更新都有新的缓解措施与安全特性。延迟释放（MemGC）与隔离堆（IsoHeap）通过破坏漏洞利用的条件基本上消灭了释放后重用漏洞，使得主流的漏洞类型转为类型混淆（Type Confusion）与越界读写（OOB）。控制流防护（CFG）、返回流防护（RFG）、任意代码防护（ACG）、代码完整性防护（CIG）共同构建了一个完整的防御体系，可以有效地防止在漏洞利用中实现任意代码执行。此外，基于沙箱与虚拟化的防御技术的引入，进一步拓展了纵深防御体系的深度，增加了攻击的复杂度与难度。

无论安全产业如何发展，技术栈如何更新，安全的本质始终是矛与盾的对抗。虽然微软等厂商在缓解措施等防御技术上做了很

多努力，也还是无法避免新颖的高级漏洞利用技术绕过所有缓解措施实现任意代码执行。因此，微软在 2013 年启动了 Microsoft 缓解绕过赏金和防御赏金计划（Microsoft Mitigation Bypass Bounty and Bounty for Defense Program），向全球的安全研究者征集针对最新 Windows 平台的新缓解绕过以及防御方法，以便阻止当前绕过最新平台缓解措施的利用技术。绿盟科技天机实验室每年都会向微软提交多项新颖的缓解绕过技术，并成为全球唯一一家连续六年获得微软该项奖励的网络安全企业。

三、网络战争的新武器：数据科学、知识图谱

自 APT 兴起后，网络空间安全已经朝着网络战争的方向发展，攻击武器化、攻击组织体系化、军队化趋势明显。此外，网络安全已经成为越来越多机构、企业标准的 IT 投入，传统防护虽然单兵能力很强，但已经无法应对攻击者各类新型、未知武器的攻击，也无法大规模服务于客户，所以作为工作在大数据基础上、有规模化能力的人工智能和数据科学技术已经越来越广泛地被应用于网络安全领域，此外如知识图谱等新技术也与数据科学融合，为安全防护提供了新的支撑能力。

一方面，人工智能可以提升传统安全检测引擎的准确率，识别未知威胁。如通过深度学习技术，可以对恶意软件进行静态或动态分析，将具有相同基因的样本划分为同一家族，从而可预测新的未知恶意软件。又如，我们通过 DNN 深度学习技术学习大量通过规则确认的恶意 Webshell 请求，产生的模型就可以识别未知的攻击请求模式，一定程度上缓解已知规则绕过的问题，同时也能提升规则编写的效率。

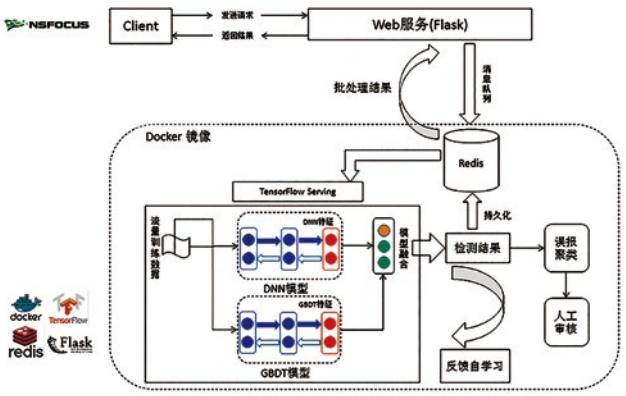


图1 Webshell异常流量检测引擎

进一步借助可解释性人工智能（XAI）技术，能够解决深度学习无法解释预测结果的问题，从而给运营团队可解释的结果，如下图可以解释上例中某个请求为什么是恶意的 Webshell（因为存在某些单词 z1、eval 等）。

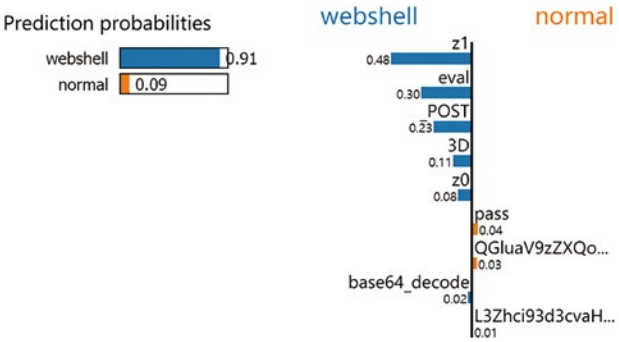


图 2 Webshell 异常流量解释

人工智能等数据科学的技术可以提供额外的检测引擎，还可应用于 DDoS、Web 安全、入侵检测、加密流量识别等单独的细分领域，也都取得了不错的效果。

另一方面，在企业场景中，安全运营（XDR、SOAR 等）和威胁狩猎（Threat Hunting）也都是应对 APT 的重要手段。数据科学和知识图谱成为辅助运营团队找到威胁，并作出处置的重要技术手段，如图 3 所示。

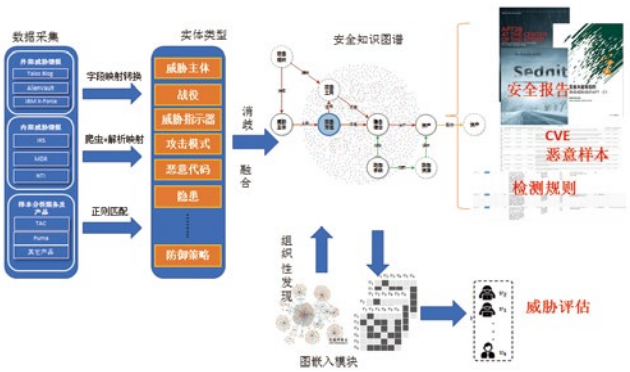


图 3 基于数据科学和知识图谱的内网威胁运营

首先，可梳理内部人员、资产等主体及其属性，与外部情报共同组建彼此连接的知识图谱，形成语义层面的联系；其次，在运行时通过各类检测技术，找到终端、网络侧的异常，此时通过知识图谱沿着节点和边寻找被攻击者感染的资产，回溯其用过的攻击手法，并分析当前系统所受影响，对态势做出研判。随着 SOAR 逐渐成熟和各类安全设备的处置功能逐渐完善，安全引擎将不仅包括检测和研判功能，还会提供决策能力。如可学习运营团队的手动处置步骤，在后续类似的场景下给运营团队提供若干处置选择，一旦运营团队确认某个处置策略，就能自动化地完成隔离、阻断、恢复等操作。

总之，数据科学和知识图谱等新技术可以配合传统的安全攻防技术，成为网络安全战争指挥部中的智囊团，让我们的安全运营更简单、更智能、更敏捷。

四、网络安全的战场迁移：云计算安全、物联网安全、下一代网络的安全

除攻防双方在不断打磨各自的矛与盾外，整个战场的环境也在发生变化，传统网络在不断与新的场景融合，例如云计算、物联网、5G、SDWAN 等，这些新环境下的安全问题值得重视。

在亚马逊推出 AWS 服务后，云计算经过了十多年的发展，已经成为企业不可或缺的计算和存储基础设施。在美国，大部分企业都使用了云端服务，而在中国，越来越多的企业也开始拥抱云计算。可以说，云计算变成了人们习以为常的资源和服务，云计算安全将变成纯安全，一方面，企业或多或少都存在云平台或云应用，企业安全建设必须将云安全纳入其中；另一方面，云计算会承载越来越多的企业业务，多云、混合云安全方案适用于普通的企业安全。

当然，需要看到的是，中美的云计算产业轨迹是不同的，美国最早发展的是应用即服务 SaaS，中小企业上云优先选择如 Salesforce、Office 365 这样的应用，所以国外前几年云安全多指云访问安全代理（Cloud Access Security Broker，CASB）；这两年越来越多的企业将传统业务迁移到云中，所以公有 IaaS 的业务占比增加，对应的云安全技术是云工作载荷防护（Cloud Workload Protection Platform，CWPP），总体而言都是面向公有云的。而中

国云计算起步较晚，且是从虚拟化发展而来的，所以前几年大型企业主要在部署私有云，不过赶上了 SDN 的浪潮，云安全则以云安全资源池为支撑技术，具有弹性、灵活的特点；这两年比较明显的趋势是政府和各行业上云趋势明显，借助私有 IaaS 的技术积累，各地都在部署各类政务云和行业云，所以对应的云安全在云安全资源池的基础上，为租户提供了按需服务 Sec-aaS。安全总是后于业务、伴于业务，洞察了行业变迁，才能把握安全之道。绿盟科技星云实验室早在 2013 年就开始研究软件定义网络和网络功能虚拟化，设计软件定义的安全体系，并在 2015 年和 2016 年率先发布了两版《软件定义安全报告》，在行业内产生了良好的反响，创新孵化的云安全资源池 NCSS，也成为业界云安全的标杆产品。

很有意思的是，尽管中美前几年云安全发展路线不同，但去年的发展趋势却惊人地一致，几乎所有的行业都在提容器安全。开发团队拥抱敏捷开发和云原生，普遍使用容器技术和编排平台，倒逼运营和安全团队了解、分析并探索这一新兴技术的安全防护之道。星云实验室也在 2018 年发布了《容器安全技术报告》，详细阐述了容器环境中如何进行静态检测和运行时防护。

另一个改变行业的基础设施是万物互联的各类物联网：工业互联网、车联网、智能家居等，一方面，物联网技术将网络延伸到了嵌入式终端，性能受限的物联网设备接入云端，具备了无穷的计算和存储能力，催生了大量以往不可想象的行业应用，推动了社会文明的前进；另一方面，我们需要看到物联网设备的弱性能，以及物联网厂商缺乏安全意识和能力，造成物联网设备的安全性极其低下。绿盟科技发布的 2018 年和 2019 年的《物联网安全年报》列出的物联网安全事件表明，攻击者正在有组织地利用互联网上的物联网设备发动各类网络攻击，同时也有针对性地对敌对势力的关键基础设施上的物联网设备或工业设备发动攻击，造成极其严重的影响。自 2017 年起，绿盟科技格物实验室关注互联网上的暴露物联网资产，历年来发布了暴露设备分布、变化情况，以及 IPv6 资产态势等一系列研究成果，并通过威胁捕获系统持续发现了攻击者对 WSD、UPnP 等物联网协议的利用和攻击。研究团队孵化的物联网安全解决方案经过产品化，提供了包含物联网安全 SDK、物联网安全网关和物联网云端安全服务完整的物联网安全解决方案。绿盟科技的物联网卡异常分析系统也在若干省和国家的运营商、主管机构得到应用，有力打击了滥用物联网卡的欺诈行为。

在工控安全和工业互联网安全方面，格物实验室分别于 2014 年和 2019 年发布了《工业控制系统的安全研究与实践》和《2019 工业控制系统信息安全保障框架》两份报告，阐述了工业安全的思路和防护方法。相关的产品团队也发布了如工控漏扫、工控防火墙等一系列工控安全产品。

传统的云 - 管 - 端体系下，云计算侧和终端侧已经产生了巨大

的变革，而管道侧的革命刚刚开始，5G、SDWAN，甚至刚刚启动的卫星互联网（空天一体化），都是试图重构我们所在的接入、传输和骨干网，将云端的计算能力通过边缘计算分布在管道段，使得算力无处不在，必将催生无数新型的应用和产业，这无疑是未来十年信息产业发生变革的最大基础。可以说，管道侧的新技术迭代，左右对接云和端，下可达新型计算设施，上可催生新应用，使得我们所处的各类环境不断融合，不断演化，合中有分，分中有合。

SDWAN 在国外发展得如火如荼，多分支机构互联、随时随地办公、灵活一致的安全策略等需求直接引爆了零信任相关细分领域，也直接改变了中小企业边界安全产品的形态；5G 推进方面中国毫不落后，但 5G 能否成为有力推动下一次工业革命、产业革命的前提，必须先保证其安全性，特别是在边缘计算数据中心中，其模式与公有云类似，那么如何保证多方参与的基础设施、平台和应用安全性，以及云端和边缘侧应用的安全策略一致性，仍需要做很多研究工作。

如果说云计算是计算侧的革命，物联网和各类新型网络是网络侧的革命，那么区块链则是存储侧的革命。2019 年 10 月，习总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术重要突破口，加快推动区块链技术和产业创新发展。区块链技术层面早已成熟，而应用方面很可能因此进入快车道。在金融、物流、供应链等领域，以联盟链为代表的区块链技术会支撑各自业务的应用。当然，该技术虽然可以达到无信任达成共识、防篡改、存证回朔等目的，但也引入了如有风险的智能合约不易更新、隐私泄露、不易监管等问题。绿盟研究团队将于 2020 年上半年和兄弟单位联合发布面向企业应用的区块链安全报告，敬请期待。此外，我们也利用区块链不可篡改的特性，于 2017 年完成了一个分布式 Web 防篡改的原型系统，可用于下一代 Web 3.0 站点。

总之，在万物互联、普适计算的大环境下，传统安全的技术实现遇到了很大的挑战，需要在现代化的安全理论指引下，先解决新型基础设施的安全问题，然后探索通过这些新型基础设施赋能，帮助我们更好地完善、提升安全防护能力。

五、结语

安全的本质是对抗，有人，就存在江湖恩怨和利益冲突，有漏洞（无论是技术的还是管理的），就存在攻防。

这是一个最坏的时代，传统网络的蠕虫病毒、勒索软件、零日攻击不会停止，相反还会受利益驱使，蔓延到新型网络中，产生更严重的后果：转移到车联网危害人身安全，转移到工业互联网破坏企业生产安全，转移到电网影响社会稳定和国家安全。

但这又是一个最好的时代，国家层面的网络空间安全立法步伐加快，网络安全产业迅速扩大，各种应对威胁的技术手段帮助我们识别已知威胁，发现未知威胁，云计算、软件定义网络、人工智能和生物技术等使能技术使得我们的安全防护更加敏捷和智能。

在这波澜壮阔的大时代，攻防双方纵横捭阖，网络安全方兴未艾。在每次风起浪涌时，绿盟人就会审其时，顺其势，勇可做大时代的弄潮儿，睿可当巨人背后的专家。

[1] http://blog.nsfocus.net/ukraine-power-plant-attack-analysis-protection-programs/.

[2] https://tech.sina.com.cn/i/2019-10-17/doc-iicezuev2860274.shtml.

网络威胁攻守博弈纵横二十年

绿盟科技 威胁情报与网络安全实验室 范敦球、李东宏、李文瑾 / 系统架构部 叶建伟

绿盟科技成立之初，国内信息技术刚刚起步，各大高校还没有设立安全专业，2001 年的中美黑客大战如火如荼，白宫网站上飘扬的红色旗帜使“网络攻击”这个名词进入国内大众视野。随后，2003 年出现的冲击波（Worm.Blaster）病毒通过一个最新的 RPC 漏洞进行传播，病毒席卷全球，让无数电脑反复重启，其同时对微软一个升级网站进行拒绝服务攻击，导致网站堵塞，用户无发通过该网站升级系统。此次网络攻击让正在进行信息化建设的企业和个人用户真正意识到网络安全防御的重要性。

“威胁”这个概念可以追溯到 20 世纪 80 年代，Adenrson 用了“威胁”这一概念术语，其定义与入侵相同，将入侵企图或威胁定义为未经授权蓄意尝试访问信息、篡改信息、使系统不可靠或不能使用。Heady 给出另外的入侵定义，入侵是指有关试图破坏资源的完整性、机密性及可用性的活动集合。Smaba 从分类角度指出入侵包括尝试性闯入、伪装攻击、安全控制系统渗透、泄露、拒绝服务、恶意使用 6 种类型。早期网络黑客与安全专家正是围绕这些入侵的方法及使用的技术手段进行攻守博弈。

防火墙、入侵检测系统向入侵防御系统的转变

最早的网络安全防御系统是防火墙，其在本地网络与外界网络之间执行控制策略，对网络间传输的数据包依照制定的安全策略进行检测，以决定通信是否被允许。防火墙存在局限性和不足，其通常作用于已知协议的访问控制，如攻击者将恶意代码或攻击指令进行协议隐藏就可能逃逸防御。

同期出现的网络威胁检测系统是入侵检测系统，它通常位于防火墙之后，被认为是第二道安全闸门。入侵检测技术主要分为两大类：异常入侵检测和误用入侵检测，其提供了对内、外部攻击的实时检测，包含在网络受到威胁之初的拦截和响应入侵。入侵检测系统的不足在于，它只能检测攻击，而不能阻止攻击。

随着技术的发展，结合上述两种系统的联动技术应运而生，防火墙可以通过入侵检测系统及时发现策略之外的攻击行为，入侵检测也可以通过防火墙对来自外部网络的攻击行为进行阻断。

而完成这两种系统的融合、实现 1+1>2 的是迅速崭露头角的网络入侵防护系统。作为国内首家企业级网络入侵防护系统的发布厂商，绿盟科技推出的“冰之眼”网络入侵防护系统，能提供从网络层、应用层到内容层的深度安全防护，具备实时、主动的防护能力，能精确识别各种黑客攻击，并有效阻断攻击而不影响正常业务流量。

漏洞挖掘技术促进安全防御

安全专家在博弈过程中尝试主动出击，去挖掘存在的威胁隐患，鼓励发布、共享这些威胁隐患的信息，促使从业人员能更好地保护用户。漏洞挖掘是一个多种漏洞挖掘分析技术相结合、共同使用和优势互补的过程。常用的漏洞挖掘技术包括手工测试技术、Fuzzing 技术、对比和二进制对比技术、静态分析技术、动态分析技术等。

随着越来越多的专家投入其中，为大众所知的漏洞数据逐年增加，从 2000 年的 1243 条增长到 2019 年的 20827 条，为网络防御技术提供了坚实的知识储备。

漏洞库

早期做网络安全产品，安全研究员发现漏洞后对其进行命名，随着漏洞研究的深入，一些漏洞已经很难依靠名称区分，早期的安全研究机构和大型厂商开始使用漏洞库管理众多漏洞。漏洞库是进行网络安全隐患分析的基础，建设漏洞库有十分重要的意义。绿盟科技早在 2000 年就推出了漏洞库，是国内首家推出商用漏洞库的厂商，历经 20 年的岁月，仍持续维护着漏洞库的更新，至今已收录 45689 条漏洞，包含主流漏洞信息以及公司研究员自主发现的漏洞信息。

漏洞库对安全防护产品也非常重要，在各个厂商的安全防护产品展示自身防护能力的时候，使用同一漏洞库的描述将直观地让用户了解防护效果。绿盟科技漏洞库兼容国家信息安全漏洞库（China National Vulnerability Database of Information Security，简称 CNNVD）以及国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD），此外还兼容国外的通用漏洞披露 CVE(Common Vulnerabilities &Exposures)，为国内外用户使用提供了便利。

Web 安全的兴起

随着 Internet 技术的兴起，便捷的跨区域事务处理显得尤为重要，为了实现用户脱离程序的复杂安装而使用 WWW 浏览器进行跨地域的应用操作，相关的应用开发逐步从 Client/Server 架构转向了 Browser/Server 架构，用户端仅需要实现少量的事务逻辑，而主要的事务逻辑在服务器端进行实现。Browser/Server 架构可以大大简化客户端电脑负载，减轻系统维护和升级的成本和工作量，从而降低总成本。解释型语言的不安全使用（对用户输入的内容没有做严格检查）催生了基于 Web 的攻击技术，例如 SQL 注入、跨站脚本攻击（XSS）、远程命令注入、跨站点请求伪造（CSRF）、CC 攻击等，这些攻击导致企业或者个人敏感数据泄漏、服务器拒绝服务或者业务被接管，甚至有可能由于受到的攻击而背上法律责任。为了解决各类组织所面临的众多复杂 Web 应用安全问题以及由此衍生的维护、管理问题。

针对 Web 攻击技术对网站安全威胁越来越严重，安全公司相应推出了 WAF 网站安全防护工具和 Web 安全评估工具。

随着 B/S 架构越来越主流，浏览器成为最主要的网络入口。同时，浏览器也成为网络攻击的焦点，漏洞军火商 ZDI 公司举办的 PWN2OWN 比赛，攻陷浏览器也是重要得分点。

工控安全引起大家关注

2010 年的震网蠕虫病毒（又名 Stuxnet 病毒），一个席卷全球工业界的病毒，是一种精心构造的恶意代码，其中包含了多个可利用的漏洞，通过一套完美的入侵和传播流程，突破工业专用局域网的物理限制，针对现实世界中的工业基础设施展开攻击。通过周期性修改 PLC 的工作频率，造成 PLC 控制的离心机转速突然升高和降低，导致离心机发生异常震动和应力畸变，最终破坏离心机。

针对关键基础设施的攻击造成的损失给整个工业界敲响了警钟，各国开始明确指出工业控制系统信息安全面临着严峻的形势，并要求切实加强工业控制系统的信息安全管理。安全公司纷纷主动肩负起守卫之责，将工控安全定位为战略发展方向，利用传统攻防优势，立足“未知攻、焉知防”的思维，调研历史事件，分析网络攻击方式，以脆弱性为入口点，纷纷发布了针对工业控制系统的远程安全评估系统，先于攻击者发现工控业务系统存在的脆弱性，并提供缓解方案，其中绿盟工控漏洞扫描系统 ICSScan 是亚太地区第一个进入 Gartner 视野的工控安全专用检测产品。在已知威胁的基础上，为了更好地实现系统防护，切实保障工控业务的顺畅运行，安全防护产品如雨后春笋般浮现于工控业务市场，例如工业防火墙、工业安全网关、工业安全隔离装置以及纵向加密装置等。

随着攻击日益多样化、复杂化和攻击目标明确化，安全公司需要构建从平台到设备的分层安全架构，覆盖评估、防护、检测、相应的安全体系，提供全生命周期的安全防护。

工控安全防御体系的建设需要消除 IT、OT、工程、财务、管理和执行领导的界限，联合多方力量才可以完成，绿盟科技作为发起单位，率先加入工业控制系统信息安全产业联盟，希望能聚集多家之长，共同抵御针对工业控制环境的网络攻击，为工业网络安全保驾护航。

物联网

当今社会物联网设备已经逐步渗透到人们生产生活的方方面面，为人们及时了解自己周围环境以及辅助日常工作带来便利。但随着互联紧密度的增高，物联网设备的安全性问题也逐渐影响到人们的正常生活，甚至生命安全，物联网设备安全不容小觑。

当前物联网中存在的威胁是显而易见的，从 2014 年趋势科技曝光的 Netcore 路由器后门到 2016 年大规模爆发的 Mirai 恶意代码事件，从 2017 年的无人机多次入侵机场到 2019 年酒店偷拍摄像头引发全民恐慌，不但“物联网成为网络攻击中重要环节”从预言变现实，而且物联网安全事件数量呈现出迅猛的增长趋势。超过百 Gbps 源于物联网的攻击已经成为现实，物联网场景下的安全对抗已经出现在这次变革的浪潮中，影响着千万企业或者普通个人。无论我们是否意识到，这场战役已经打响。

物联网应用中涉及多个参与方：物联网设备提供商、物联网平台提供商、物联网网络提供商、物联网应用提供商、普通用户、物联网安全提供商，每个参与方在考虑安全问题时侧重点也会有所不同，一个设计合理的物联网安全防护方案需抓住各需求点，才能切实将物联网安全落实到位。

随着环境和威胁的变化，安全防护思路也在逐渐变化。物联网的碎片化、动态性特点，造成单纯的依靠安全厂商进行常规的防护已然不够，只有融合多方力量，才能真正解决物联网安全问题，防护数以百亿计的物联网设备安全，保护广大人民群众的人身财产安全。

APT 攻击

2009 年高级可持续威胁（APT：Advanced Persistent Threat）进入人们的视野，特别是“极光（Aurora）”攻击、“震网（Stuxnet）”病毒、“夜龙”攻击，让 APT 高级持续性威胁成为信息安全行业瞩

目的焦点。APT 作为一种精准、高效的新型网络攻击方式，被频繁用于各种重要网络攻击事件之中，在政治安全、国防安全、企业安全等多个重要领域被高度关注，并迅速成为信息安全最大的威胁之一。由于黑客普遍使用 0Day、未知木马进行远程控制，木马攻击行为特征难以提取，给传统的入侵检测技术带来了巨大的挑战。如何准确地检测面向未知木马的 APT 攻击，提高 APT 的检测能力，及时发现网络中可能存在的 APT 攻击威胁，是网络安全公司维护网络秩序，保障社会安全的使命所在。对 APT 的研究分析发现，APT 攻击主要体现在三个方面：

- 以“时间换空间”。以长期潜伏的攻击过程为代价，隐匿攻击行为的异常，同时不断擦除攻击痕迹，使得攻击效果显著提升。一些 APT 攻击潜伏期长达 3 个月之久，在此期间，攻击者有足够的时间窃取重要价值情报。

- 攻击方案精心定制，绝不雷同。从多个 APT 案例中获知，APT 攻击和普通攻击表现迥异，即使各个 APT 攻击之间选择的攻击技术手段都具有独特性，即便攻击的整体阶段或思路上存在相似性，但在具体的攻击行为或数据中差异巨大。

- 先入为主，掌握攻击主导权。掌握攻防博弈先机，通过长期的前期准备，使用多种手段收集信息，拉开攻击和防御的信息不对称性，获得主导权。攻击者往往拥有较强的黑客能力和网络攻击技术，掌握着高超的漏洞挖掘和利用技术，了解攻防心理，运用社会工程学获得有效信息。

APT 攻击目的非常明确——窃取特定目标核心机密资料。攻击者通常会综合利用钓鱼邮件（被 90%的活跃 APT 组在初始访问阶段使用）、水坑站点、社会工程学，利用文档型漏洞制作诱饵文档，隐蔽隧道等多种技术手段绕过目标网络的层层防线，从外围到核心区域逐步攻克目标。在攻击工具和攻击技术上着重实用性，有的利用合法工具（大约一半的 APT 组织使用合法的管理工具和商业渗透测试软件）逃避检测，也有的自研发程序且实现攻击工具的语言多样，程序实现不讲究复用性。

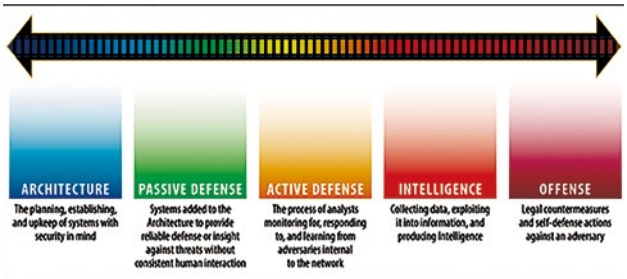
随着安全公司对 APT 攻击的总结和深入分析，APT 检测系统也随之进入市场。预计 APT 保护解决方案的全球市场收入将从 2019 年的超过 43 亿美元增长到 2023 年的超过 94 亿美元。现有 APT 检测系统建设还处于初级阶段。APT 防护解决方案是一套集成的解决方案，用于检测、预防、对抗持久性恶意攻击。它可能包括但不限于：沙箱、EDR、CASB（Cloud Access Security Broker）、信誉网络，威胁情报管理和报告、取证分析等。因此，对于安全产品供应商来说，至关重要的是提供能够智能地识别和关联跨多个来源和渠道的潜在攻击信息的解决方案。

应急响应体系和威胁情报的出现

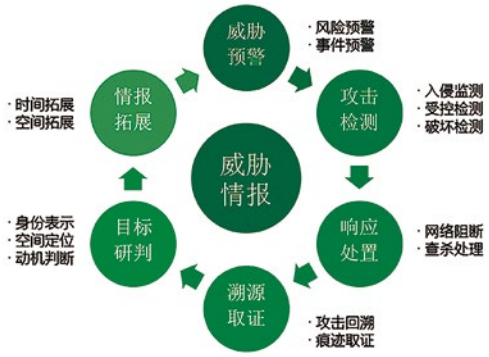
威胁情报的诞生源于攻防的不对等。随着黑客攻击的规模化、自动化、多样化、灵活化，传统的基于签名和规则的攻击检测和防御体系显得捉襟见肘。由于无法提前获取签名和规则信息，传统的基于“已知”规则的检测在遇到 0Day、APT 等“未知”威胁时，完全无法感知和防御。

2013 年, Gartner 发布《Definition: Threat Intelligence》，其中给出了威胁情报的定义：威胁情报是关于资产所面临的现有或潜在威胁的循证知识，包括情境（上下文）、机制、指标、推论与可行性建议，这些知识可为威胁响应提供决策依据。

随后, 2015 年, SANS 提出“网络安全的滑动标尺模型”（The Sliding Scale of Cyber Security），为企业安全建设提供了宏观上的指导和建议。滑动标尺模型从左到右，是企业逐步应对更高级网络威胁的过程，其中情报是继架构安全、被动防御、主动防御之后的进阶阶段。



威胁情报的出现驱动了应急响应体系甚至是网络安全防御体系的转型，即从静态的、基于规则被动防御，转变为动态的、自适应的主动防护体系，为下一代安全奠定了基础。孙子曰“知己知彼，百战不殆”，威胁情报正是网络攻防战场上“知己知彼”的关键。威胁情报最大的价值在于帮助防守方了解他们的对手（攻击者），包括攻击者的背景、思维方式、能力、动机、使用的攻击工具、攻击手法、攻击模式等。对攻击者了解越多，就能越好地识别威胁以便快速地做出响应。准确全面的威胁情报能够极大地扩展威胁防御的时空边界，是实施主动防御策略的关键。基于对“对手”的了解，威胁情报构建了威胁预警、攻击检测、响应处置、溯源取证、目标研判、情报拓展的防御方“生环”。在应急响应中，威胁情报通过为安全防御设备进行赋能，可以大大缩短安全设备对最新威胁的响应和处置时间，达到“单点感知，全网防御”的效果。



绿盟科技于 2015 年组建了威胁情报中心，并推出了绿盟威胁情报分析与共享平台（NTI）。依托绿盟在安全领域的长期积累，绿盟的情报来源不仅包含原创漏洞库、样本库、安全分析数据、产品运营反馈数据等绿盟特有的数据源，同时也涵盖了全面的互联网情报采集和广泛的第三方情报合作机构。基于绿盟大数据分析平台，结合安全情报专家对情报数据进行深度挖掘分析，获得高质量的多维度威胁情报，覆盖网络资产基础信息、指纹、漏洞、TTP、高级威胁分析结果等不同层面；通过 NTI portal 界面、API 接口、订阅推送等不同输出方式将威胁情报与安全设备、客户和安全厂商进行共享，有效保护了客户的安全。

绿盟科技“黑洞”ADS

——— 二十年风雨兼程，十八载筑梦前行

绿盟科技 SPG研发部 何坤

联合作者

吴铁军、陈景妹、樊宇、苗宇、郑彬、李凯、王秀慧、汤湘君、潘文欣、钟施仪、李宇博、姜艳杰、汤旭

2002 年 10 月 25 日，历经两年的技术研究和产品开发，绿盟“黑洞”正式面世。

在 2005 年之前，网络安全的相关法律还未出台，很多稍大一些的网站经常会受到黑产的勒索威胁，动不动就被 DDoS，服务器瘫痪。正所谓“乱世出英雄”，危难时刻方显英雄身手。绿盟科技在这时出现，它研发出针对当时主流 DDoS 攻击的防护产品——“黑洞”(Collapsar)。黑洞是中国第一款抗 D 产品，是这个细分品类的创造者和先行者，在黑洞之后才出现了思科、Arbor 等友商的同类产品。天文学上说，“黑洞的质量是如此之大，它产生的引力场是如此之强，以至于任何物质都无法逃逸，哪怕是光”。

2020 年是绿盟科技 20 岁生日，也是黑洞的 18 岁生日。当小编问到黑洞是如何成为一款得到全球市场检验和认可的产品时，笔者脑海里不禁出现了一部放映机，回放着一个个”黑洞”故事。

此文篇幅较长，这是因为，黑洞的发展史，就是当今 DDoS 攻击与防护的对抗史。

路，从那一天开始。

抵御“洪水”，“黑洞”降世

时间拖回到 2002 年，那个时候国内大部分人还是拨号上网，人们对网络安全的认知最多停留在杀软的层面，如今人们耳熟能详的各类硬件安全设备在当时还是个新鲜玩意儿，至于“黑洞”这种抗 D 专业设备，在当时就是个传说级的东西，只有安全专家才能搞清楚。

那时市面上没有黑洞的同类产品，很多时候，客户遭遇了 DDoS 攻击就会直接电话找到绿盟科技，希望借一台黑洞临时顶一下。当时的绿盟科技黑洞产品线经理，黑洞之父，更为准确的说是抗 D 之父叶晓虎博士，回忆起当时的情形：一开始黑洞组就几个人，欧怀谷、吴铁军、刘添怡、徐祖军等（现如今都已是大神）经常是一边做着开发，一边做着技术支持，叶博士就有时亲自扛着黑洞到用户机房，将设备安装上线、调试好。“很多服务器被 DDoS 攻击缠上后，7*24 小时，没完没了地打，服务器要么关机，要么在那里“半死不活”，那些维护工程师非常头痛”，“只要黑洞一上线，服务器就活了，效果非常明显”，“就因为我们帮忙解决攻击，以前都是用户请我吃饭的”。

早期的黑洞最多只能处理 10Mbps 大小的流量，现在看来很低，但在当时 Modem 拨号速率只有 14kbps-56kbps 的年代，黑洞的处理能力已是海量，而如今的黑洞 ADS 已经具备单机 240G、单集群上 T 的清洗能力。

图 1 早期黑洞的照片

黑洞上市后很长一段时期里，“黑洞”就是抗 D 产品代名词，甚至在一些主管机构文章中，就直接把抗 D 产品称为“黑洞”。那时，黑洞就等同于抗 DDoS 技术。

很多网友会在网站上发表自己对黑洞、对抗 D 算法的理解。例如，有人讨论黑洞的反向探测技术，写到：“黑洞不断向流量来的方向发送大量的反向数据，将攻击报文包围消灭掉……”文中描述的黑洞，给人感觉不像是一台网络安全设备，更像是一台正负粒子对撞机，制造正负质子的对撞和湮灭。事实上，黑洞确是有反向探测技术的（现已经是公开的技术），但是无法像论坛帖子上所述，可通过反向的数据包消灭发送过来的 DDoS 报文，黑洞只是通过反向探测技术来区分正常或恶意流量。

除去这些轶闻趣事，网络上还是会有很多对黑洞的研究。当时一些论坛上，有人公布自己的发现，宣称找到了黑洞的弱点，比如，有人反推黑洞的抗 D 算法，然后研讨在黑洞防护下的绕过方式。面对这些挑战，黑洞组的同事们大多一笑而过，但也有个别，让大家感受到真正的威胁。

这其中，最著名的应该就是 CC 攻击了。

Challenge Collapsar，黑洞迎接 CC 挑战

CC 攻击的全名—Challenge Collapsar，翻译过来就是挑战黑洞。

挑战的起因是一次未如约进行的面试，叶博士当时因一些突发原因没能面试 Qaker，于是 Qaker 含怒埋头苦研，发布了专门针对黑洞 Collapsar 的 CC（Challenge Collapsar）攻击。谁都不曾想到，此后 CC 攻击（以及后来的 CC 变种）给中国乃至世界互联网安全带来长期困扰。

棋逢高手甚欢喜，面对突如其来的新型 DDoS 攻击，黑洞组的同事们泛起缕缕喜悦，丝丝紧迫。在叶博士带领下，黑洞组开启自虐模式，潜心分析 CC 攻击表象及原理，并结合用户环境不断推演方案，力求防护的同时对业务的影响降到最低。设定方案、推演方案、驳斥方案、确立方案，理论逐渐完备，最终，黑洞对 CC 攻击的清洗能力得到广泛认可。

或许是不打不相识，抑或是相互欣赏，后来叶博士和 Qaker 成为朋友，经常一起探讨新型攻击的原理和对抗方式。保持旺盛的激情，形成清晰科学解决问题的逻辑体系，了解黑客所思所为，夯实关键技术实力，是成就全球知名安全产品的先决条件。魔高一尺，道高一丈。虽然 CC 攻击的发展危害了互联网安全，但它也激发了我们网络安全人员应对各种攻击的斗志。

DDoS 的发展史就是黑洞演进史

算法是黑洞的宝贵资本，是产品的核心竞争力之一，它主要来源于技术研究和实战积累。

对客户而言，攻击是否能防住，业务是否受影响是衡量一款抗 D 产品的重要指标。如果攻击来了业务却掉线了，界面再好看的产品也是不合格。有时候，防护算法一个字节的不同，就可以使整个防护效果差之千里。攻防算法的提升没有太多的套路可循，如果没有时间和大量的客户积累，相信黑洞也无法达到其现在的防护能力。

从这点来说，黑洞的成长应该真心感谢那些使用它的用户。

DDoS 的发展史，就是黑洞的演进史，我们结合 DDoS 技术演进时间线，将 DDoS 攻击大致分为几个阶段：

第一阶段，虚假源 DDoS 攻击

早期的 DDoS 以虚假源攻击为主，简单粗暴但极为有效，聊天室聊着聊着可能就“死了”。这类攻击一般由工具或者仪表构造产生，因为其源 IP 虚假而无法响应黑洞探测报文的属性，一般传统的 TCP-Flood 防护算法就能够很好的清洗此类攻击，这块已经没有太多的技术门槛。

再后来，ISP 也开始在网络接入层面启用 URPF 策略（注，URPF 是一种单播反向路由查找技术，用于防止基于源地址欺骗的网络攻击行为，主要在网络接入层面启用），以期从大网架构层面直接过滤虚假源攻击。从我们的统计数据来看，URPF 起到了一定效果，但仍有漏网之鱼，近几年虚假源 Flood 依然是 DDoS 攻击重要组成（参见绿盟科技历年 DDoS 威胁报告）。

实际上，虚假源 DDoS 攻击也并不是大家想象的那么“简单”。攻击者也在不断思考、改进和实践虚假源攻击的实战效果，因为这种攻击的”开销”实在是太低了，如果能以低成本的方式打垮对方，又何必去兴师动众发动更复杂、更高成本的攻击（攻击 ROI）？以至于在 DDoS 攻防对抗史中，出现了一些增强型虚假源 DDoS，也可以简单理解为第一代 DDoS 的 Plus 版本。

举个例子，大概在 2010 年，我们发现攻击者打出的虚假源攻击不再全随机源了，而是将攻击源 IP 伪造为真实服务器的地址段，比如伪装为某省某服务商的地址段，当黑洞去探测这些源 IP 真实性的时候，就很可能误认这些 IP 是真实存在的，从而探测算法失效，服务器崩溃，同时，这些服务商还被流量反射了，攻击者可谓一箭双雕，从另外一个角度讲，这也算最早期的 DDoS 反射攻击，更早于名震四方的的 NTP 反射。

当看到这些增强版攻击的时候，黑洞组的同事们都会异常兴奋，彻夜研究对策，提升黑洞防御能力。

第二阶段，针对知名协议，DDoS 真实源攻击

CC 攻击的重大改变在于，它不再简单利用虚假源发起攻击，而是利用真实源（比如网上的代理服务器），对 Web 服务器发起攻击（HTTP），以耗尽服务器资源。现如今，CC 攻击（最早期的 CC 攻击是 HTTP Flood）已有非常成熟的算法应对，比如，黑洞现已经内置 9 种 CC 防护算法。

广义上的 CC 攻击，应该还包括 HTTPS 攻击、慢速攻击、连接耗尽、空连接攻击等，万变不离其宗，它们都有一个共同点，就是利用真实源发起攻击，攻击者利用真实源可跟随协议栈行为的特点，使得防御难度加大。

但知名协议（如 HTTP、DNS）有一个好处，就是大家可以通过研究公开的 RFC 文档去了解协议的每一个细节（黑洞组员癖好之一：喜读 RFC。我们发明的不少抗 D 算法，就是在业余时间读 RFC 产生的灵感），而 DDoS 攻击和防御的平衡点往往就在毫厘之

间，一点就破，不点破就会觉得很高深，我们也有多种算法被友商通过各种途径验证、学习并吸收。

为持续保持攻 / 防之间的这一点差距，一方面我们潜心进行理论研究，保持算法先进性，比如在 2012 年，黑洞就已完全内置 IPv6 多种 DDoS 防护算法，提供 v4/v6 双栈防御能力，又比如近期火热的 5G DDoS，我们也做了大量技术储备；另一方面，我们也会保持与前线（绿盟工程线 / 业务线同事、客户等）信息、实战的关注，紧跟攻击变化趋势。知己知彼，方能立于不败之地。

除了 CC，还是有一些攻击，是曾让我们不安的。

第三阶段，针对私有协议，DDoS 真实源攻击，SDK 防护算法的诞生

对于 DDoS 防护设备，任何无法解码的流量都可以认为是私有协议流量，极难防御。知名协议大家还可以通过查看分析 RFC，寻找蛛丝马迹，但当面对私有协议流量的时候，大家两眼一抹黑，除了限速不知道怎么办了，出现了攻守不平衡的局面。

大概在 2012 年，黑洞为腾讯当时最火爆的某款游戏（那时候还没有王者荣耀）提供抗 D 防御——吸金的业务往往都会招来复杂且有针对性 DDoS 攻击。那段时间，黑洞组和腾讯安全中心的专家们（creativeLiu、jerrybai、cchen、junjunluo，现在都已是大佬）苦不堪言，但同时又很亢奋，经常探讨到深夜。攻击者的思路、手法都非常高明，很多高阶攻击手段都被用上，这样的对手难得一见，一度让我们怀疑攻击是“内行团伙”发起——我们也把这类攻击叫做游戏 CC。

那段时间，我们先后发明了业务自学习 Self-learning、XX-Retrans 等新算法，成功应对了攻击。

但是俗话说，不怕贼敲门，就怕贼惦记。几个月后，算法被突破，游戏又开始出现掉线的情况。

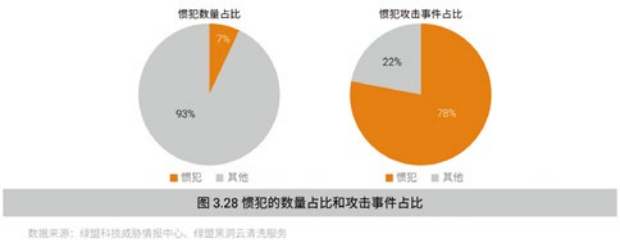


图 2 2019 年绿盟科技 DDoS 威胁报告——攻击惯犯的数量占比

游戏 CC，是否还有更好的应对方案？那段时间大家激情碰撞，彻夜讨论，终于，我们共同发明了私有协议 DDoS 防护的终极解决办法 (之一)——SDK 防护算法，黑洞上面叫水印算法。水印算法，顾名思义，也就是客户端在发送业务流量之前，根据黑洞提供的 SDK，将水印嵌入到业务流量中，当流量经过黑洞时，黑洞根据水印进行识别，达到精准清洗的效果。这一技术的问世，解决了很多无状态敏感业务（如，游戏、金融等）要求零误杀、低时延的业界难题。

第四阶段，超大反射攻击的出现，出现攻守资源不平衡的局面

2014 年，一起峰值达到 400Gbps 的 NTP 反射攻击震惊全球网络，它使得原本小众的 DDoS 攻击进入平常人们的视野，超大反

射攻击的出现，从根本上改变了 DDoS 对抗格局。

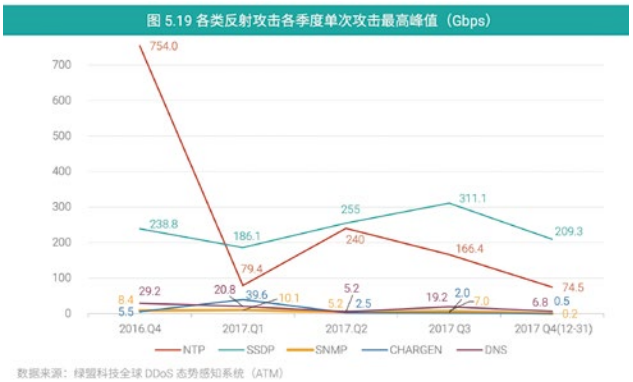


图 3 2017 绿盟科技 DDoS 威胁报告—反射攻击流量趋势图

2016 年，可谓热闹非凡。这一年的 9 月 19 日，OVH 声称遭受了一起来自 145607 个网络视频监控设备发起的峰值最高 800Gbps 的 DDoS 攻击。

紧接着 9 月 20 日，KrebsonSecurity 遭受峰值达 620Gbps 的 DDoS 攻击。

10 月，黑洞组联合绿盟威胁情报中心（NTI）和绿盟威胁响应中心，对外正式发布《网络视频监控系统安全报告》，对此类 DDoS 攻击源头进行了深度剖析。

我们认为，这几起攻击均来源于名叫 Mirai 的僵尸网络，据我们的统计，当时全球感染 Mirai 的物联网设备数量累计超过 200 万，遍布全球 90 多个国家和地区。我们推算了一下，光这一僵尸网络就具备发动峰值超过 1.5Tbps 的攻击能力。后 2016 年 10 月发生的“北美大面积网络瘫痪”事件和 11 月发生的“德国大范围用户断网”事件也相继印证了我们当时的这一观点。

当攻击者可以较低成本的利用网上资源，将攻击规模提升到百 G 甚至上 T 的级别，这是极为可怕的，物联网等设备带来的安全问题给全球的网络安全防护都带来巨大挑战。

图 4 2016 年绿盟科技网络视频监控安全报告

安全生态合作

2015年开始，绿盟科技陆续与电信云堤、腾讯云、阿里云、华为云、浪潮云等云服务商展开合作，实现各安全领域的优势能力互补，强强联合打造抗 D 混合清洗等安全方案，为企业客户提供最佳防护方案。既可帮助用户应对复杂应用层混合 DDoS 攻击，也可自动化应对突发的超大流量攻击。同时，黑洞也为各大云厂商的私有云客户提供强大的本地 DDoS 防护能力，成为私有云整体解决方案的一部分。

打通天地，造就“云 - 地 - 人 - 机”的立体防护体系

安全事件的偶发性，注定了产品不可能时刻都在客户面前秀肌肉、显实力，只在关键时刻一显身手。但是，安全专家不是时时有、处处有；超大流量云端防御费用高，也有流量绕道产生延时、第三方安全顾虑等问题；安全设备不是谁都精通，这些都是客观存在的问题。

如何在关键时刻一显身手？绿盟科技在很多年前，就已开始思考并践行解决这一难题，也就是业界熟知的 P2SO 战略。其中，黑

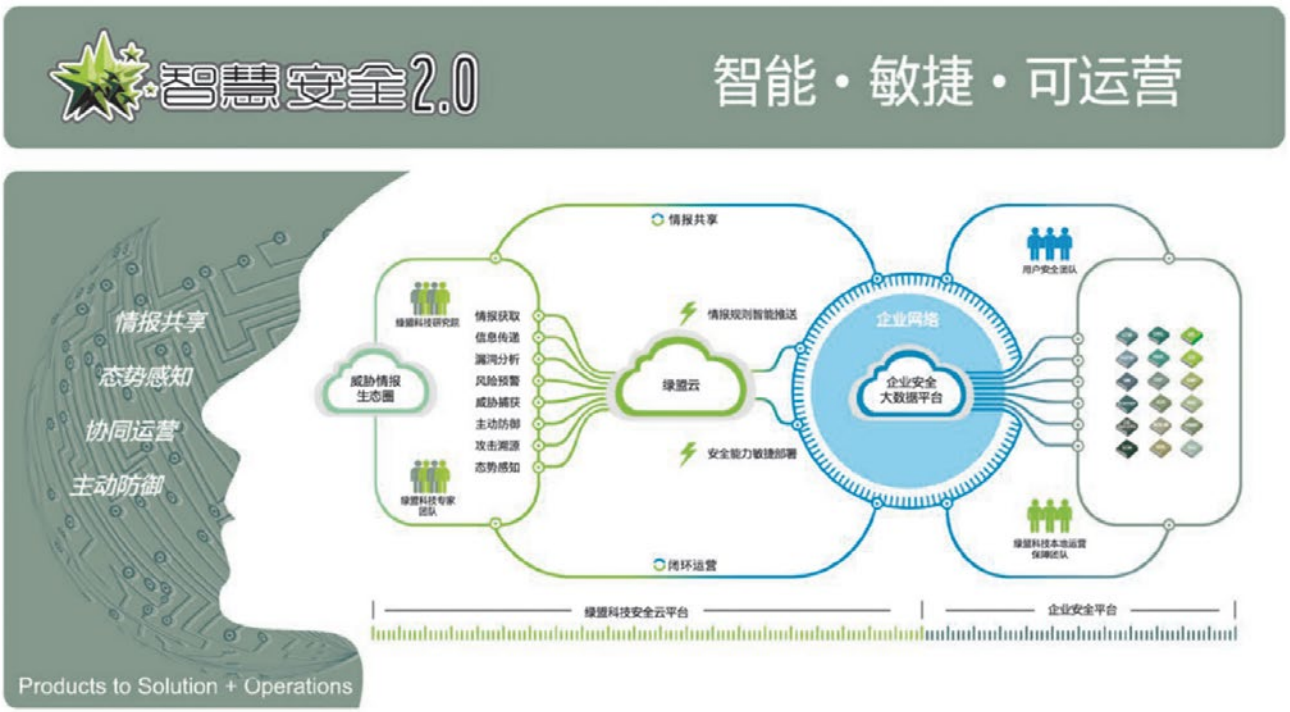


图 5 绿盟科技智慧 2.0

洞系列产品就是该战略的践行者之一。

2015 年，绿盟科技发布了以智能、敏捷、可运营为核心理念的智慧安全 2.0 战略，绿盟抗 D 的整体解决方案的发展建设，也是围绕这个理念展开。

看得见的能力——绿盟科技全球 DDoS 态势感知系统（ATM）

2016 年，黑洞组主导的绿盟科技全球 DDoS 态势感知系统（ATM）开发完成。

基于该系统，我们可以实时清晰地观测到网络中实时发生的海量 DDoS 攻击事件，能够第一时间知道：谁被打了？被谁打了？怎么打的？打了多久？等等多维信息，此系统也是“由被动响应变主动响应，由非实时变成实时，由无数据变成有数据”战略的一个有效实践。

现如今，绿盟科技威胁情报中心 NTI 每年发布的《DDoS 威胁报告》，其中就有 ATM 的贡献。记得有一年，我司情报与国际友商 PK 情报质量，其中有一个测试项就是 PK 恶意 IP 数据质量，最终的结果是，绿盟科技的情报质量在数量、准确性、新鲜度等方面具备明显优势。

智能、敏捷、可运营

这个场景可能很多运营人员会有体会：深夜，某 VIP 客户遭受国外黑客组织的大流量 DDoS 攻击，业务受到影响，客户紧急报障后经过一系列工单流程，最终在攻击发生后 20 分钟找到对应后端运维部门，运维部门人员打开电脑—登陆 4A 系统—登陆设备—最终发起流量清洗指令。最后虽然黑洞成功防御住攻击，但操作过程还是偏长，客户的业务也已受损。同时，当客户业务正常的时候，客户也没有渠道看到自己的业务安全数据和态势情况。

为帮助运营商做好安全增值运营能力建设，在运营商专家和绿盟运营商事业部的指导帮助下，黑洞组集中精英研发力量，一鼓作气迅速研发出绿盟流量清洗业务运营系统 ADBOS（Anti-DDoS Business Operation System），解决了若干过去抗 D 增值运营的痛点，极大提升运营效率和客户感知，打通抗 D 增值运营最后一公里。

黑洞 AI 出世

除了 ADBOS 系统，实际上我们还做了很多有意思有价值的事情，篇幅的原因就不具体一一展开描述。

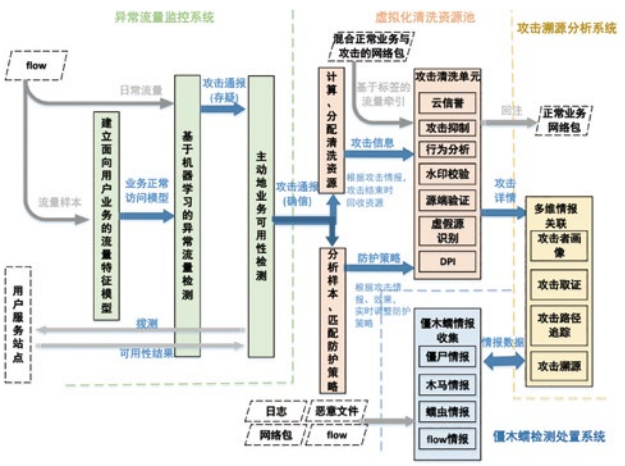


图 6 黑洞某平台架构图

如前所述，我们将 DDoS 攻击发展分为 4 个阶段，每一个阶段都有鲜明的特点，以及对应的最佳的防护策略，但很多策略都是需要人为配置干预的，黑洞是否可以自己去生成 DDoS 算法、调整策略应对攻击呢？答案是，可以，而且我们的实践效果还不错。

2016 年，在叶博士以及绿盟系统架构部的帮助指导下，我们发明了一种新的抗 D 方法 / 模型，叫做自适应拟态遗传 DDoS 防护算法，时髦一点的叫法就是 AI 抗 D。

该算法主要使用黑洞防护过程数据进行训练，生成动态攻击防护模型库，在防护过程中根据流量模式自动计算最佳防护策略和参数，由机器自己去判断哪些流量大概率是攻击，哪些是业务，实现攻击流量高速精准识别和清洗。同时，云端可在线更新攻击样本库和信誉数据库，同步到清洗平台和设备，实现“一处被打，多处联动”的云化预警和防护机制，大大提高 DDoS 攻击的检测和清洗效率。

此外，为提升运营效率，我们将动态相似性聚类算法和自动协同防护模型引入到日常运维工作中，基于动态聚类的流量检测及牵引联动模型，在传统的正常流量建模基础上，引入攻击数据进行建模，使得海量用户可进行自动聚类分组，并结合“流量监控 + 受保护服务”多维检测机制，配合智能研判实现数据流的自动牵引与复原，当有主机受到攻击时，具备流量相似性及受攻击相似性的同聚类组其它主机也可预先进入防护准备状态。通过这一系列方法和手段，每一台黑洞的清洗精度和准确度，就可以在实战中不断得到增强，无需人工介入。

2016 年，基于绿盟黑洞 ADS、ADBOS 平台以及多项专利防护算法等成果，我们和广东电信客户联合申报并获得了广东省科学进步三等奖。2018 年，基于 ADBOS 平台的北京移动清洗项目成为工信部的电信和互联网行业网络安全试点示范项目，以及 2019 年工信部试点示范项目推介会的特邀项目。

实际上，不仅是在运营商行业，黑洞在金融、游戏、政企、教育等行业均有最广泛的部署和应用，得到客户广泛认可。根据第三方分析机构 Frost&Sullivan 在 2019 年最新发布的《DDoS China Market Ranking Statement,CY2018》 和《DDoS Greater China Market Ranking Statement，CY2018》两份市场报告：绿盟抗拒绝服务系统 ADS（黑洞）以市场占有率 21.2% 和 15.5% 的份额，名列大中华区及中国地区双第一。这也是黑洞在该报告中连续五年排名第一。

图 7 黑洞若干获奖图

在海外市场，绿盟科技黑洞也收获不断。2017 年 3 月，英国伦敦智能混合 DDoS 防御解决方案提供商 NSFOCUS 被授予“2017 年欧洲 IT ＆软件（www.iteawards.com）年度最佳安全解决方案奖。”与此同时，绿盟科技也是“年度公共部门与公用事业解决方案”和“年度安全供应商”两项大奖的决赛入围者，这是绿盟科技第一次同时入围三个国际安全奖项。

经过海内外绿盟人的不断努力，现如今绿盟科技黑洞的国际客户

图 8 部分绿盟科技黑洞海外客户

名单中，已经不乏 Telefonica、TM、AIS 等国际大牌运营商，收获满满。

十八年，作为绿盟科技产品中的一员，黑洞从当时只有 10M 清洗能力的单机产品，发展到今天分布式机框和云化的黑洞，黑洞能力已全球无处不在，黑洞每分每秒都在为全球用户抵御攻击，保障用户业务安全。我们相信，过硬的技术和服务是终极的营销手段，正如叶博士所说，过去打补丁、串葫芦的方式无法解决用户安全问题，需要对安全进行体系化的设计和落地。绿盟科技始终保持对最佳安全实践的关注，持续对国内外先进的安全架构进行跟踪研究，将最新的研究成果和实战经验，实现在智能安全运营平台及相关的产品上，为客户提供优质的产品和方案。

最后，祝绿盟科技 20 岁生日快乐！黑洞 18 岁生日快乐！

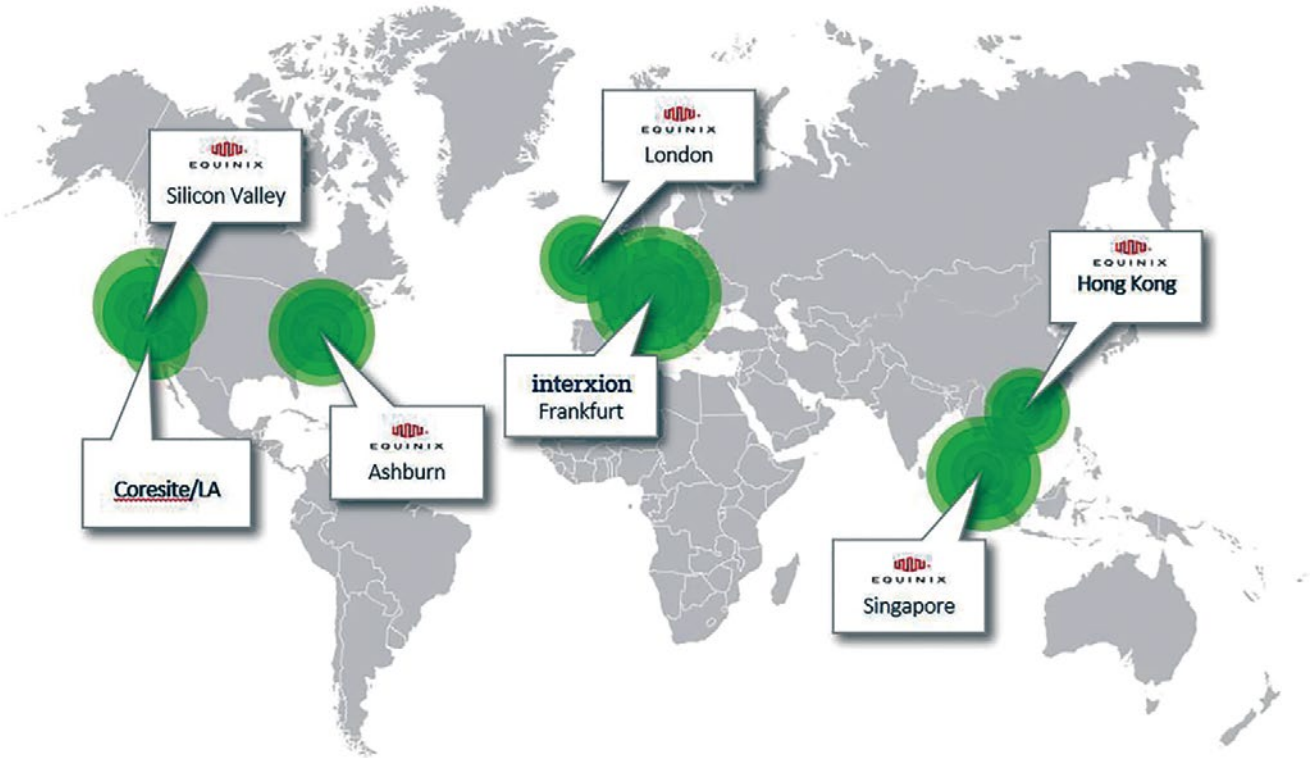


图 9 绿盟科技黑洞云清洗 (DPS) 节点分布示意图

绿盟极光，用专注惊艳了时光

绿盟科技 RCM产品部 尹航

联合作者
张云海、李晨、向智、李晔磊、陈庆、彭艳亭、樊志甲、刘晓霞、符春辉、谭福超

在安全圈久了，一定听说过绿盟极光漏洞扫描器——一款知名度很高的产品。在近 20 年的发展中，它曾被赋予了一系列标签——技术强、好用、团队强大、更新快等，它的市场认可度极高，用现在的话说这是一个爆款产品，IDC 资料显示已经在国内连续 8 年市场占有率第一，后来，极光漏洞扫描器更名为 RSAS 绿盟远程安全评估系统，简称 RSAS。

缘起

绿盟科技是国内最早推出企业级商用扫描器产品的厂商之一。2000 年的绿盟科技以技术起家，一些有技术梦想的安全研究人员开始折腾一款国内自己的扫描器产品。那时候圈里流行为自己起一个网络 ID，绿盟扫描器团队有着日后可能会被记录在安全发展史的知名 ID——deepin、watercloud、scz、jbtzhm、zhangyunhai……

极光扫描器的起步并没有因为众多大咖的加入而变得顺利，从技术梦想到产品诞生是一个艰苦的过程，企业级应用产品对产品品质、功能和可靠性的要求极高，与平日安全研究人员们的个人工具差别很大。最早折腾扫描器的是 deepin 和 ipxodi。到 2001 年，极光扫描器还在实现产品化的路上。后来，随着 watercloud、hip 的陆续加入，才最终完成了第一个版本：极光 V1.54，一个值得纪念的版本。

从个人工具软件到企业级产品的发展，有三个重要特性作为一个整体贯穿产品发展的全过程，直至今天这三个重要特性依然在绿盟漏扫产品中沿用。首先，是 B/S 架构，现在已经是企业级软件的基础特性了，但在当年 C/S 还是 B/S 一直存在理念之争；其次，地址簿是企业级产品化的重要特性，让产品从根本上摆脱了个人工具的思维，为后续绿盟漏扫产品的资产、风险、闭环管理等概念奠定了基础；最后，电子盘让绿盟漏扫产品顺应了国内客户易部署、可靠性高的硬件需求，并在市场上越走越远。值得关注的是，为绿盟漏扫产品奠定这三个特性的人，网络 ID 叫“眼圈”，可以说绿盟人都认识。

2003 年极光项目组

专注与沉淀

一个技术型的公司，对产品的要求也必然是技术至上。在绿盟科技漏扫产品的第一个版本发布后的很长一段时间里，团队都在专注于把技术做到极致，专注于产品技术优化：代码自动化编译和安装优化、引擎稳定性优化、插件的质量优化、插件数量添加、性能优化。

这是一个痛苦的自我磨砺过程，代码不断地被重构和修改，进行最严格的语法检查，保证编译警告不出现，还得自己定制测试检测程序，做最严格的测试。在这场旷日持久的艰苦战役中，产品团队养成了互相质疑、互相骚扰、监督提升的习惯，最终也使得产品的插件无论是数量还是质量都大幅领先，产品得到用户认可，绿盟科技极光的名气也越来越大。

2007 年年底，在漏洞扫描产品取得了一定成绩后，团队开始不满足于现状，既然已经做到了国内最好，就要再跟国际厂商掰掰腕子，团队发狠要挑战当时信息安全类产品最高认证——国际厂商都望而却步的英国西海岸实验室的 Checkmark VA 认证。Checkmark VA 认证极度严格，要求 Critical 级别的安全漏洞检测率为 100%，全球只有北美的五家顶级安全厂商的漏洞扫描产品通过此认证。

当意识到跟国际顶尖水平认证要求的差距后，团队不仅没有气馁，反而像是打了鸡血，开始不分昼夜地加班。有人疯狂写插件到

拿到西海岸证书后美滋滋的极光漏扫团队

凌晨，有人用蹩脚的英语跟西海岸实验室沟通，有人用电驴下载游戏——是的，认证测试项包含欧洲比较火的几款游戏，需要搭建测试环境，团队整个冬天就在这样火热的氛围中度过。专注和激情终将获得回报，在 2008 年春天，绿盟极光跻身全球顶尖厂商产品行列，成为北美之外唯一获得英国西海岸实验室认证的产品，也是绿盟科技产品取得的第一个国际认证。

成功就是不断地超越

跟大多数公司的产品团队一样，极光漏扫产品团队这些年不断

有新鲜血液加入，也不断有人离开，去撑起另外一片天空。但是专注于技术，专注做最优秀产品的精神一直被传承下来，在极光扫描器产品一代代发展的过程中，不断地超越自我也成为产品团队的传统。

极光团队在 V3 版本中对漏洞信息做了重要的概念重定义，把漏洞本身信息与确认漏洞存在的各类指纹和常见信息进行分离，重新定义了各类信息的格式，为最终的详细分析和灵活展示提供基础。V4 版本中团队提出了一个期望，期望扫描器不仅能发现问题，而且能够真正贴合企业流程发现和确认最终问题是否解决，团队提出了 OpenVM

不断超越的漏扫 V5 产品团队

开放漏洞管理流程的概念。V5 版本开始正式融入了 Web 应用扫描能力，并在 2008 年为解决安全运维人员面临的问题和挑战，推出了业内首款安全配置核查系统，形成了完整的脆弱性综合检查能力。

从 2008 年开始，极光更名 RSAS，Cheney 加入漏扫团队。随着新的配置核查产品发布，绿盟漏扫进入一个新的时代。2010 年产品销售额过亿，之后的 8 年时间，在 IDC 每年的国内市场调查报告中，绿盟漏扫连续市场占有率第一，并且多次进入 Garter 市场报告和技术报告，漏扫产品作为绿盟科技的支柱产品之一，也被公司寄予了极高的期望。

公司总裁与产品线代表签署产品团队任务书

变局已至 砥砺前行

绿盟极光漏洞扫描产品上市近 20 年的时间，一直致力于帮助客户在日常网络管理中发现网络安全漏洞和解决漏洞问题，在各类重大安全保障场景中也发挥着重要作用。

近年来网络环境不断变化，新技术不断涌现，云、大数据、IPv6 的应用，均是对漏洞扫描产品新的技术挑战。信息安全攻防也在持续升级，业界安全运营管理体系的设计也在不断进步，产品的应用场景也在变化，相应的对漏洞扫描和管理的要求也越来越高。

变化的是新环境新设计对产品的需求，不变的是绿盟科技漏扫产品团队一直传承的不断超越自我的精神。在最新的绿盟漏扫产品中，漏扫团队已经针对新技术要求，增加了云、大数据、物联网等场景的扫描能力；针对新攻防要求的漏洞安全管理工作，提出了漏洞 TVM 管理概念，并结合平台产品形成了整体解决方案。

随着 5G、物联网的兴起，更多变化将会接踵而至，产品也会面临更多的挑战，产品团队将继承专注技术的一贯传统，做极致的产品，持续为客户提供发现和解决安全漏洞问题的好产品，不忘初心，砥砺前行。

二十年风沙洗礼，终成参天大树

——“冰之眼”NIDS/NIPS 技术创新之路

绿盟科技 ESD产品部 焦玉峰

联合作者
魏向杰、孙月梅、徐兴华、赵阳、肖丰佳、钟岳林、张英、谢正明、
孙建坡、杨三杨、李文瑾、范敦球

随着互联网的迅猛发展，越来越多的商业活动从线下发展到了线上，新模式在带来便利的同时也增加了被攻击的风险。攻击手段与防御技术此消彼长，作为安全防护体系重要组件的入侵检测与防御系统（简称 IDPS）起着举足轻重的作用，回顾国内 IDS/IPS 市场的发展，唯有保持核心技术和持续创新的厂商，才能获得长期稳定的市场地位。

“冰之眼”IDPS 见证了行业的风起云涌及客户不断变化的安全需求，并及时做出自身的调整来适应这种变化。蓦然回首，随着绿盟科技的快速发展，“冰之眼”IDPS 已经从一株小树苗长成了一棵参天大树。在它的成长过程中，不同时期的产品团队为其持续注入生命力。

国内首家通过 NSS Labs 专业测试

NSS Labs 的 IDPS 评测标准，已经成为业界公认的“试金石”。2010 年 4 月，“冰之眼”IPS 1200 顺利通过测试，荣获 NSS Labs Approved 认证，并且被 NSS Labs 认定为最高级别—— “Recommended”，成为截至目前国内唯一获得该认证的产品。

在测试报告中，NSS Labs 对“冰之眼”IPS 做了如下评价：“管理非常简单，直观得让人惊讶，加载有效的预定义防护策略后，它能够被快速部署到企业网络之中”“对已知逃避检测技术的抵御非常完美，在所有相关测试中，均获得 100% 的通过率”“基于优秀的应用安全防护能力，卓越的千兆处理性能，以及杰出的总体拥有成本，这款产品非常值得用户考虑”。

据当时的项目组成员李文瑾和范敦球回忆：“这个（项目）印象太深刻了，为了冲击 NSS Labs 测试，团队投入了很多资源，对整个引擎的架构和攻击检测方式做了质的提升，到最后设备入场了，我们还安排每天倒班支撑，那段时间很艰难，压力很大，但结果很美好。”NSS Labs 测试通过，也为产品顺利进入 Gartner 魔力象限做好了铺垫，一年后，“冰之眼”IPS 成功进入该报告。

从千兆、万兆到百 G，单机性能持续突破

作为直路部署的产品，性能是 IPS 的生命线和基石，在行业集采中，严格的性能测试项已经成为标配。在“冰之眼”的性能演进中，有两个关键里程碑：

首家万兆 IPS

2008 年 12 月，“冰之眼”IPS 产品 4000P 通过中国软件评测中心（CSTC）的测试，成为业界首款通过第三方权威评测的 10G IPS。本次测试对吞吐、时延、背景流量、并发、新建、攻击检测与拦截率等进行了严格的测试。其中，网络层性能测试从 64 字节到 1518 字节等多种包长的测试流量下，“冰之眼”4000P 吞吐率

均达到 100%，达到了双向线速转发，并且对混杂在背景流量中的攻击行为实现 100% 拦截。应用层性能测试项目，“冰之眼”4000P 在使用 Avalanche/Reflector 混合模拟的 HTTP 流量中，能够同时维持处理超过 350 万的并发连接。

据当时研发经理回忆：“对于万兆 IPS 产品，是我进团队领的第一个大任务，时间紧、任务重，硬件平台计算能力有限，我和团队几乎每天都加班加点，在引擎架构和流程优化以及仪表使用中摸爬滚打 .....”

首家 120G IPS

2016 年某客户 IPS 集采首次招标 80G 产品，这对长于安全攻防检测能力的单体盒式设备为主的绿盟科技来说是极大的挑战，需要面对长于大容量网络数通处理的友商硬件战。整个项目的时间非常紧张，而且遇到的挑战和困难也是前所未有的。比如，机框硬件平台方案、软件分布式方案、百 G 性测试仪表等都不具备，为了在短期内提升产品性能，产品组、规则组和架构部组成联合攻关团队，测试中前后场紧密配合，如期交付样机参加集采，在入场测试中，后端研发彻夜加班支持现场测试。最终，IPS 12000A 通过测试并获得较好的集采份额，产品的性能也实现了质的飞跃，TCP 并发 12000 万、TCP 新建 180 万、2544 大包近 200G。

据负责机框产品的研发经理回忆：“高性能机框产品是我接受过的最具挑战性的任务。分布式架构团队从未接触过，很多工作都是从零开始、摸着石头过河，一边学习一边设计。仪表也是临时向友商借用，并且只能在对方下班后用使用。那段时间大家都是夜猫子，团队采取轮班倒策略。百 G 性能的攻克充分体现了我们是一支能打硬仗的队伍，单机大容量处理能力为产品拓宽了部署场景，除满足集采外，也为城域网僵木蠕监测市场单机 100G 方案做好了技术储备，在高性能第一个版本之后，团队也集中资源，在提升产品的稳定性、管理端的易用性等多点发力，力争在更广阔的国际市场上有所收获”。

成都团队研发经理表示：“我们 IPS 引擎有了较大的性能提升，但挖掘的潜力还很大，后续我们还将继续在性能优化上投入研发资源，每个版本都把性能提升和稳定性列入必备项，除保证产品在高端市场持续有竞争力外，在同档位的中低端型号上性能也要高出友商一截。”

“硬核”的安全防护能力

“冰之眼”IDPS 在发展演进中，充分体现了绿盟科技优秀的技术基因，作为安全技术的集大成者，“冰之眼”IDPS 积极吸收各安全研究团队的成果，形成了以威胁检测技术为核心，同时兼顾上网行为管控、流量管理等几大功能的产品。

流式引擎和并行架构设计

并行加管道混合式引擎架构，可以充分利用硬件平台的多核计算优势。与其他实现技术相比，流式状态解码技术使得引擎的实时性更强、更高效。

攻击描述语言与签名库

灵活的攻击描述语言，加上安全研究实验室支撑，目前“冰之眼”IDPS 支持近万条签名库，实现紧急漏洞防护签名 24 小时内发布，例行签名一周内发布。

APT 检测与防护

对于高级可持续性威胁（APT），传统的单一检测方法无法有效应对，“冰之眼”IDPS 与 APT 检测系统（TAC 设备或者云沙箱）协同，通过行为分析和虚拟执行技术，发现隐藏在流量中的高级恶意代码和恶意回连，并动态调整 IDPS 的防护策略，拦截恶意流量。

高级恶意代码检测

在恶意代码发现能力上，不同于传统基于签名的技术，“冰之眼”IDPS 采用启发式技术、静态模拟技术以及虚拟执行等技术，对隐藏在流量中的恶意代码识别，能精确拦截。

威胁情报

不同于通过例行签名分发获得防护能力，“冰之眼”IDPS 通过与威胁情报系统（NTI）联动，可以实时获得对恶意 IP 访问、僵尸网络、恶意 URL 以及高级样本的检测防护能力。

机器学习技术

对于无明显特征或者特征难以提取的攻击，如 SQL 注入 /XSS 攻击，绿盟科技安全研究团队通过在云端对 WEB 正常和异常的访问流量进行学习训练，形成基于行为的向量模型，训练后的模型随着例行签名更新发布，使得设备不依赖于特征即可识别此类攻击。

上网行为管理

应用管理 & 流量控制：采用了 DFI/DPI 技术，除支持签名识别技术外，还可以通过流量行为来精准识别应用 / 协议，为攻击检测和基于应用的流量控制、上网行为管理等提供准确的依据。

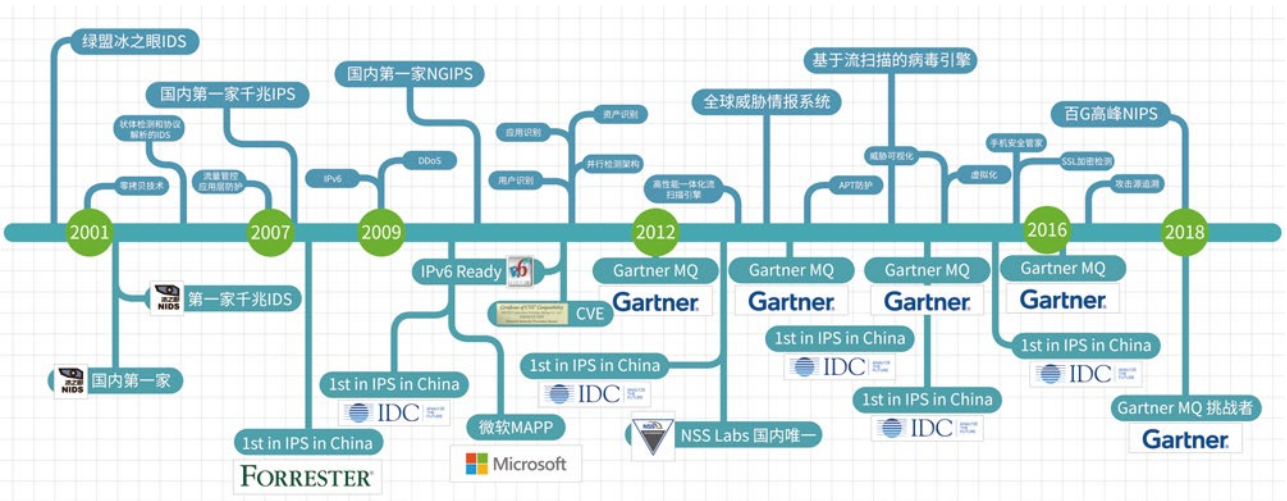
URL 分类过滤：采用设备本地 + 云端双层过滤技术，实现对未知分类的识别以及实时更新。

满足客户需求，持续创新

公开数据显示，“冰之眼”IDPS 自 2009 起连续 7 年国内市场占有率第一（IDC 报告），连续 6 年入围 Gartner IDPS 魔力象限，并在 2018 年进入“挑战者”象限。安全市场复杂多变，系统漏洞和新型攻击技术层出不穷，“冰之眼”IDPS 将始终以满足客户安全需求为己任，继续为客户网络提供专业的安全防护。

附录：“冰之眼”IDPS 发展大事记

- 2019 年: 实现对申威、飞腾和兆芯等处理器千兆、万兆的全覆盖;
- 2018 年: 在连续 6 年入选 Gartner MQ 的基础上, 进入“挑战者”象限，亚太唯一一家；
- 2016 年：发布 120G 高性能机框 IPS 产品；
- 2016 年：IDS 进入运营商僵木蠕监控市场；
- 2014 年：发布 20G IDPS 产品；
- 2013 年: 首家在 IPS 中引入基于情报驱动的威胁检测和溯源技术;
- 2012 年：国内首个进入 Gartner IPS 魔力象限的产品；
- 2012 年：发布国内第一款下一代 IPS（NGIPS）；
- 2010 年：通过 NSS LABS 认证，并获得最高级 Recommended 评价，跻身全球三强；
- 2009 年：获得 Frost&Sullivan 颁发的 “2009 年中国 IDS/IPS 市场增长战略领导者” 奖；
- 2009 年：国内首家获得 EAL3 级认证的入侵防护类产品；
- 2008 年：发布 10G IDPS 产品；
- 2008 年：继续占据 IDC 定义的 2007 年中国入侵防御硬件市场领导者地位；
- 2007 年：中国第一家千兆 IPS；
- 2005 年：中国第一家 IPS。



智能安全运营平台的进阶之路

绿盟科技 安全能力中心 杨传安 / ESM产品部 吴天昊 / 总工办 陈景妹 / ESM技术部 潘登

2014 年，绿盟科技内部启动 P2SO；2015 年，绿盟科技发布智慧安全 2.0 战略。这些战略的核心，都是将绿盟科技过去以硬件产品为主导的方向升级为给客户提供完整的安全解决方案及安全运营，而平台产品作为安全运营的抓手、解决方案的核心，在战略执行过程中的地位是举足轻重的。

初步尝试——BSA

早在 2014 年，绿盟科技 P2SO 战略发布之前，产品线就在大数据能力方向做了研发投入和技术布局。在数据接入方面，使用过 Logstash、Flume、Heka、StreamSet 等组件；在数据存储方面，使用过数据仓库、MPP、搜索引擎等类型的组件。产品技术团队构建了绿盟科技的大数据平台，并且应用到内部作业系统。

随着公司 P2SO 战略的推进，以及客户市场对整体的安全解决方案和运营服务持续增长的需求，安全管理平台产品成为客户提升安全能力水平的重要抓手。由此，2015 年初，绿盟科技推出了面向企业安全管理的产品：BSA——绿盟大数据安全分析平台。

第一代安全大数据平台产品的核心价值，是把大数据技术引入网络安全管理的领域，然而当时国内的主流管理产品还停留在使用传统技术处理海量的安全告警日志，效果差强人意。国内外领先的创新厂家，纷纷开展新型技术应用的开发。在充分调研后，我们认为此阶段的大数据平台产品的产品化目标是提供足够的数据接入、处理、存储及分析支撑，提供标准开发接口，并在上层开放安全业务，由各安全厂商、客户基于大数据平台进行开发 APP，并进行 APP 售卖，形成一个开放的生态环境。这是个非常超前的产业创新尝试，确定“BSA + APP”模式后，技术组件上决定采用“Hadoop +kafka + Spark +ELK（ES+Logstash+Kibana）”体系。用 Spark 代替 Storm，主要是因为 Spark 具备流计算和批处理的能力，非常适合安全管理的时效性要求。同时也保留了 ELK，通过重用“Kibana + ES”灵活的搜索条件生成自定义可视化图表的能力，非常适合有 DIY 偏好的管理员。

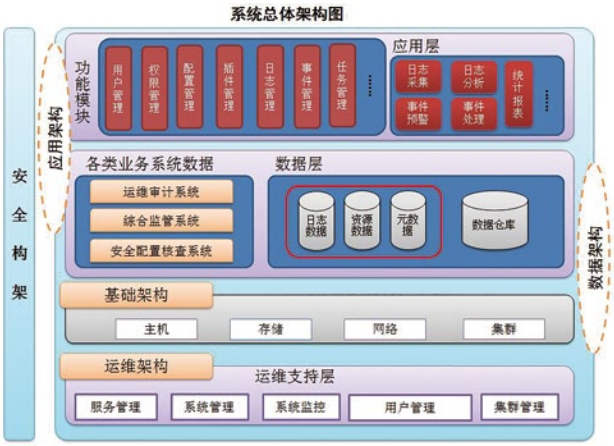


图 1.1 BSA 架构图

第一代 BSA 可以说是一种技术流导向的设计思路，基于 Hadoop 跟 Spark 提供平台底层存储及计算的横向扩展能力，“ES+Ki-

bana”的“搜索与报表”功能，提供了灵活自定义的仪表盘及可视化图表的能力；通过“告警”模块，自定义告警规则，提供了从日志生成告警事件的能力。告警模块，应该是平台最早的规则引擎。通过灵活的 APP 管理框架及封装的对外 API 接口，提供了上层业务应用开发的能力。

图 1.2 初代 BSA 首页截图

不难看出，这是把 ToC 互联网产品思维转向 ToB 企业安全产品市场的一个创新。从结果来看，这并不是一次非常成功的尝试，企业用户的使用习惯，APP 的轻量级业务定义很难满足国内产品售卖的市场需求。构建 APP 生态，基于平台进行二次开发，无疑有很大的难度，市场情况也确实不尽人意。无论如何，第一代大数据平台的实践，为解决海量的日志管理，以及流式实时告警等客户迫切需要解决的安全管理问题，提供了新的技术手段。当时，行业内广为诟病的传统数据库技术支撑的管理平台产品看到了新生。

业务落地——TSA、ESP

安全管理的问题千万重，有用且好用的产品必须找到有效的场景。综合的网络安全态势感知，日常的威胁事件处置都是客户需求度非常高的场景。

基于绿盟科技完整的产品线，尤其是威胁感知，漏洞发现，异常流量，高级攻击检测等产品能力。2015 年年底，绿盟科技推出了基于 BSA 大数据平台的态势感知方案——TSA，该解决方案覆盖了网络入侵态势、异常流量态势、僵木蠕态势、网站安全态势、系统漏洞态势等五大态势的感知能力。基于攻击链，TSA 实现了海量日志到精准事件的态势感知分析能力，绿盟安全态势感知面向的主要客户群是监管、运营商等大型网络下的安全监控业务。在多个重大会展或国家社会活动期间，态势感知平台为客户保障网络安全发挥了巨大的作用。

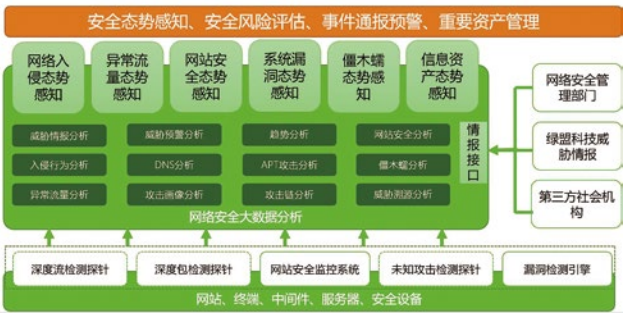


图 1.3 绿盟安全态势感知平台架构

图 1.4 绿盟安全态势感知平台首页

在企业内部，威胁事件分析、资产以及漏洞处理无疑是日常运营的重要工作。2015 年年底，绿盟科技发布了绿盟企业安全平台——ESP，ESP 以大数据框架为基础，结合威胁情报系统，通过攻防场景模型的大数据分析及可视化展示等手段，协助企业建立和完善了安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。ESP 通过独有的自适应体系架构，高效地结合情境分析，协助安全专家快速发现和分析安全问题，并能通过运维手段实现全生命周期的安全闭环处理流程。

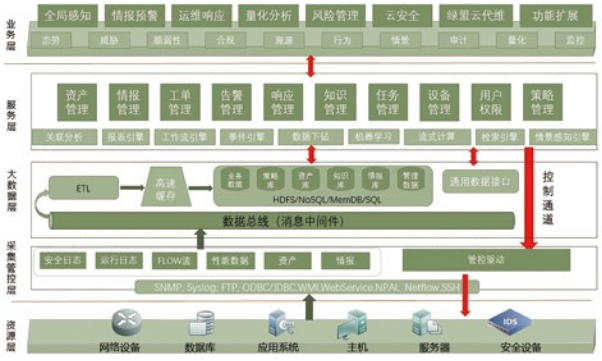


图 1.5 绿盟企业安全平台架构

图 1.6 绿盟企业安全平台首页

两大业务平台的落地，解决了高频的部分管理问题，丰富了绿盟安全管理平台的解决方案，其业务也迅速开展，市场反响不错，获得了客户的好评。

百花齐放——CIIP、TAM、TVM、TAT、ESP-H

随着客户安全管理的场景化需求落地，发展到 2019 年绿盟关键信息基础设施态势感知平台（CIIP）上市的这期间，产品线不断完善产品体系，陆续发布了多种平台型产品，针对不同的细分行业、细分领域，都有了对应的覆盖。

这其中有通过接入镜像流量，进行深度包检测，并对流量日志及告警日志进行留存及分析，针对高级威胁、重保期间进行深度威胁分析及溯源的全流量威胁分析系统——TAM；有通过对接漏洞扫描探针，实现脆弱性数据集中收集、集中分析及管理，针对企业及监管单位进行脆弱性集中监控的绿盟威胁与漏洞管理平台——TVM；有对接异常流量检测探针，实现 DDoS 攻击检测、异常流量

分析及溯源，针对运营商大网进行 C&C 主机溯源的绿盟 DDoS 溯源分析系统——TAT；有针对监管单位，实现针对被监管单位关键信息基础设施进行态势感知，以及预警通报的关键信息态势感知平台——CIIP；有针对中小企业，辅助高层安全决策，帮助中层管理落地，支持基层日常运营的轻量级安全态势感知平台——ESP-H。

图 1.7 关键信息态势感知平台

在这个过程中，绿盟科技的安全分析能力及大数据能力也有了较快的发展，开发了支持大数据平台关联分析的规则引擎。规则引擎的发布使平台从单一日志的分析，走向了多维日志的关联分析。规则数量和覆盖的场景都取得了长足进步，既支持内置规则，也可以通过自定义的方式增加规则。能力的后端，组建了专职的平台规则建模团队。从此，平台规则的能力化进入了可运营阶段，在一次次客户应急保障活动中，体系化运营支撑快速地帮助客户解决了问题，得到了客户的认可。

图 1.8 基于大数据与情报的安全分析

随着大数据使用的深入，机器学习和 AI 技术越来越受重视。随着攻击溯源业务的发布，诺亚引擎作为开放式、可配置的安全类机器学习引擎在 2017 年应运而生。客户或内部的研究成果可以快速地在绿盟大数据平台落地实现，降低了安全分析人员进行研究机器学习的门槛，提升了绿盟科技在安全大数据分析领域的竞争力，缩短了机器学习和数据分析类研究性课题产品化的时间周期，节约了项目成本。从客户运营实践来看，基于诺亚引擎的数据算法为解决 Netflow、Webshell 和 DNS 日志指示的安全问题提供了有力的技术保障。

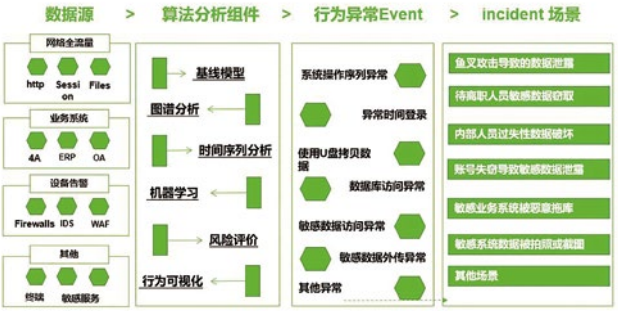


图 1.9 异常行为分析场景

随着产品的不断研发，业务的不断开展，绿盟科技平台的产品在各行各业的客户那开花结果。在这个过程中，细分产品越来越多，一些问题也逐渐浮现出来，给我们的团队效率、产品版本管理带来了一些困扰。

内敛，归一——ISOP

2018 年年底，在各行业、各领域的平台产品积累了一定的经验后，为更好地适应客户统一运营的需求落地，需要整合成松耦合、模块化的大平台产品，ISOP 应运而生。ISOP，是遵循了绿盟科技智慧安全 2.0 理念，以运营为中心，智能化、全场景的统一安全管理平台。ISOP 以大数据框架为基础，结合威胁情报系统，通过对攻防场景的机器学习、威胁建模、场景关联分析、异常行为分析、安全编排自动化以及可视化呈现等技术，帮助客户建立和完善了安全态势全面监控、安全威胁实时预警、资产及漏洞全生命周期管理、安全事故紧急响应的能力。通过独有的自适应的体系架构，为安全运营提供了可靠的信息数据支撑，协助客户快速发现和分析安全问题，并通过运维手段实现安全闭环管理。

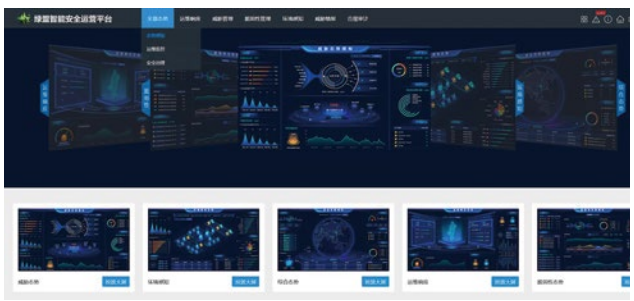


图 1.10 ISOP 智能安全运营平台首页

在这个过程中，我们对历史平台能力及架构也进行了有机融合，实现了平台统一、模块化、组件化。ISOP 技术架构的特点是分层组件化，强调系统的可扩展性，注重性能优化。技术架构上保留原有的“BSA+APP”（或组件）模式，组件可以单独升级，启动停止，对外视图体现，以统一的综合平台形式提供，整体分为基础平台层、能力引擎层、业务应用层的三层打包。分层的原则是越底层的通用性越强，越上层的业务性越强，设计理念上符合 Gartner 的 CARTA 安全模型，具备很强的开放性和完整性。

图 1.11 智能安全运营平台架构

2019 年，随着 ISOP 的发布，分析引擎做了升级更新，发布谛听引擎。谛听引擎融合国标、行标的需求输入，对到平台的日志进行了分类，并实现了按接入设备进行分类，支持融合绿盟科技的设备日志和第三方厂商日志。其次，对平台数据进行了分层，定义了 Log、Event、Alarm、Incident 等四个层次。每个层次都可以根据规则和场景进行数据量级的降低和数据价值的提升。在不同层次中可以利用攻击链模型和 ATT&CK 模型进行 Hunting 和分析，做到了一套体系、一套规则、一套流程，解决了安全检测的全部问题。

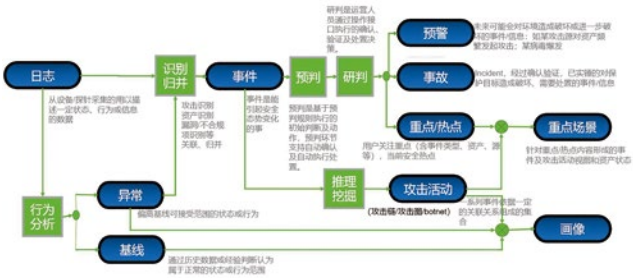


图 1.12 智能安全运营平台分析流程

在分析及响应体系上，我们也开始尝试用“ATT&CK+SOAR”的方式，将分析过程及分析结果，映射到 ATT&CK 体系下。ATT&CK 将攻击者的行为更有效地映射到防御中，对每种攻击技术都给出了非常详细的描述，有部分甚至还存在详细的代码片段。当攻击者利用这些攻击技术时，根据其留下的数据源信息，可以制定各种机器可读的检测或处置剧本，包括定义剧本的输入、输出接口以及内部执行逻辑。对于需要人工研判的情形，可适当留出合适的参数接口，基于大量的攻击技术，可构建原子剧本集合。这样就能将“ATT&CK+SOAR”进行有效结合，既可以快速评估攻击危害及防御能力，又能够有效地进行自动化响应。

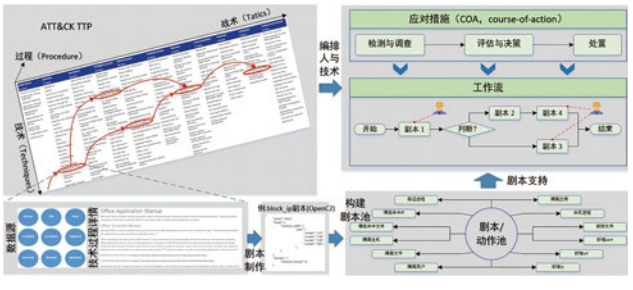


图 1.13 ATT&CK+SOAR 的分析及响应理念

最后，我们将运营体系与产品体系进行结合，形成了以 ISOP 平台为核心的安全运营体系，发布 MDR 服务，提供以资产为基础，实现威胁、脆弱性管理闭环，并通过服务工具提升检测及防护效果一体化的安全运营解决方案。

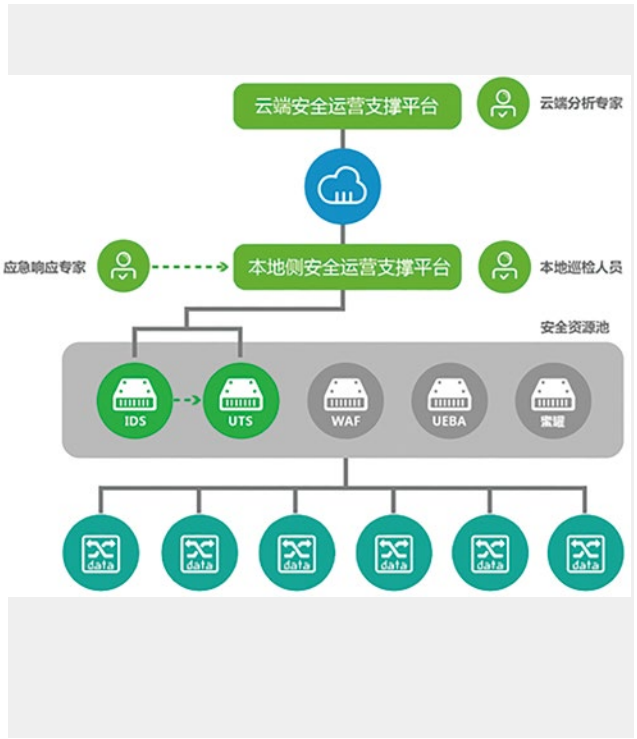


图 1.14 安全运营服务体系架构

为践行绿盟科技 P2SO 战略，支撑因客户数字化变革带来的网络安全挑战，以及体系化的安全运营服务需求，ISOP 还会继续在自动化、智能化之路前行，担当 AISecOps 的先锋。

智慧城市安全运营体系建设及展望

绿盟科技 业务拓展部 向智 金力 柴森 安宏亮 / 总工办 李国云

信息安全保障建设在智慧城市建设中至关重要，成功的智慧城市实践离不开安全运营的保驾护航。本文首先介绍了智慧城市发展中面临的安全威胁，进而论述了运营对安全的重要意义，并分析了驱动安全运营发展的主要因素。文章进一步阐述了“安全运营 +”体系的提出对智慧城市安全运营体系系统性、完整性、有效性建设的促进作用，并对安全运营今后的发展方向做了展望。

关键词 智慧城市；安全运营

一、智慧城市面临的安全威胁

近 10 年来，智慧城市已成为我国城市发展的新理念和新模式，以新一代信息通信技术在城市经济社会发展各领域的运用为主线，实现城市管理的精细化、公共服务的便捷化、生活环境的宜居化，满足城市发展转型和管理方式转变的需求，但它在给人们生活带来更好的生活体验和极大便利的同时也带来了不少信息安全威胁和隐患（如个人信息泄密、公共信息泄密、恶意网络攻击，等等）。国际信息系统审计协会（ISACA）在其报告中指出，有 71% 和 70% 的能源、通信基础设施遭到过网络攻击，其中有 67% 的攻击来源于国家级别的黑客组织。

二、成功的“安全”在于“运营”

安全运营，是通过统筹运用多种手段，将产品的核心价值持续输出传递给用户的过程。所谓核心价值就是产品的核心竞争力，举例来说，美团的核心价值是低价，滴滴的核心价值是便捷，知乎的核心价值是优质的内容，而安全运营传递给用户的核心价值，就是发现安全问题、验证问题、分析问题、响应处置、解决问题并迭代优化，持续降低用户面临的安全风险。安全运营不是单纯的产品或服务，而是一个以安全为目标导向，统筹规划人（运营团队建设、人员能力提升等）、工具技术（安全基础设施建设、大数据集中分析、人工高级技术分析等）、运营管理（检测、预警、响应、恢复和反制，以及配套的运营流程和管理制度等），用于解决安全问题，实现最终安全目标的复杂安全保障体系。

人、数据、工具技术、流程，共同构成了安全运营的基本元素，以威胁发现为基础，以分析处置为核心，以持续优化为目标通常是现阶段安全运营的主旨。不管是基于流量、日志、资产的关联分析，还是部署各类安全设备，都只是手段，安全运营最终还是要能够清晰地了解用户自身安全情况，发现安全威胁、敌我态势，规范安全事件处置情况，提升安全团队整体能力，逐步形成适合用户自身的安全运营体系，驱动安全管理工作质量、效率的提升。

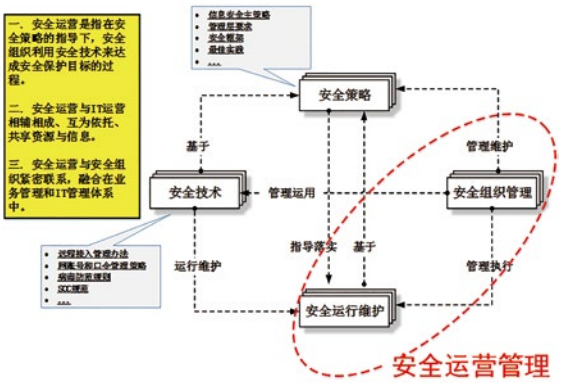


图 1 安全运营管理的定位

安全运营最主要的特点是对专业度的要求，包括安全攻击、防御、分析等技术的积累，安全发展新动态的跟踪，以及拥有高端安全人才队伍等。以上各方面对用户来说，比较难以实现且性价比不高。而安全厂商天然具备以上各方面优势，可以通过传统的产品化形式，以及安全咨询、安全服务或者安全运营中心等多种形式实现安全运营能力的输出，帮助用户实现整体安全运营。

三、安全运营发展的驱动力

当前，驱动智慧城市安全运营发展的主要因素表现为以下几点：

1. 日益严峻的国内外网络安全大环境

面对网络攻击组织化、产业化态势，我们需要不断推进安全工作的进一步迭代，需要将安全运营作为智慧城市整体运营的 IT 运行保障。

2. 政策法规推动下的合规管控要求的增强

信息安全已上升为我国国家战略，2016 年以来，我国网络安全监管环境整体趋严，强制性更高而且监管范围更大，随着《网络安全法》《等保 2.0》等政策法规落地，信息安全行业迎来空前的发展机遇。

3. 常态化对抗下安全能力不足内生出的安全管控追求

近几年，网络安全攻防演习成为各企事业单位，乃至国家层面培养网络安全人才的创新型培养模式。通过攻防演习，一方面，安全做得不好，有什么危害，在实战演练的模拟下，可以被真实地展现出来；另一方面，被点名通报整改的监管动作也动真格了，再也不像以前，买一堆安全产品应付合规就能蒙混过关了。戳破了表面安全的假象，各企事业单位发现，要做到平时具备演练同等的防御能力，很需要运营技巧，而不再满足于敷衍的应对合规。内生出对安全风险控制的追求，是安全运营发展的核心动力。**在安全法和强攻防对抗下，促使企业从“合规”到“效果”的需求升级，也回归到安全攻防的本质**。

4. 企业成长产生的安全运营的需要

从发展周期视角来看，随着企业的成长，其市值、体量、社会影响力都不断增大，安全建设工作也有了基础，对安全保障及管理有了需求，到了需要运营建设的阶段。

5. 新一代信息技术应用带来的安全运营需求

随着云计算、大数据、物联网、移动互联网、人工智能等新一代信息技术的广泛应用，产生了智能交通、智能物流、工业智能化等许多新的应用场景，同时也带来了新的安全风险与挑战。例如，工业控制系统与传统 IT 系统存在很大的差异，工控协议类型繁多、适用于不同的控制环境，相对于传统互联网安全而言，工业互联网安全领域依旧是一个盲点。供电、供水这些基础设施的核心控制器件是工控系统，如果遭遇黑客攻击，会面临更大面积的瘫痪，需要安全运营提供有效的信息安全防护保障。

四、“安全运营 +”助力智慧城市建设

“安全运营 +”体系旨在为智慧城市、云计算及政企等领域客户提供一体化的安全运营服务解决方案，原有产品与服务基础上进一步整合优势资源，以达到为客户提供安全运营整体方案及运营支撑，协助客户建设适用于自身业务的安全运营体系，并进行持续优化的战略目标。

“安全运营 +”提供从安全运营的目标出发，由安全管理支撑、安全运维及安全技术保障三方面构建的一体化解决方案，从而确保安全运营体系的系统性、完整性、有效性。由此，安全防御体系也从静态、被动、基于规则的防御，逐渐转变为主动、动态、自适应的弹性防御体系，从而真正做到“云地协同、智行合一”。

- 智慧城市安全运营

基于对智慧城市网络安全目标的深入分析，‘安全运营 +’提出了智慧城市总体安全保障框架。其包括安全规划设计体系、安全能力保障体系和安全治理运营体系，分别从规划设计、建设实施、治理运营三个方面提供重点能力支撑。

其中，在规划设计阶段，专业团队将协助地方政府从智慧城市安全顶层设计战略出发，规划提出城市安全建设具体目标和要求，

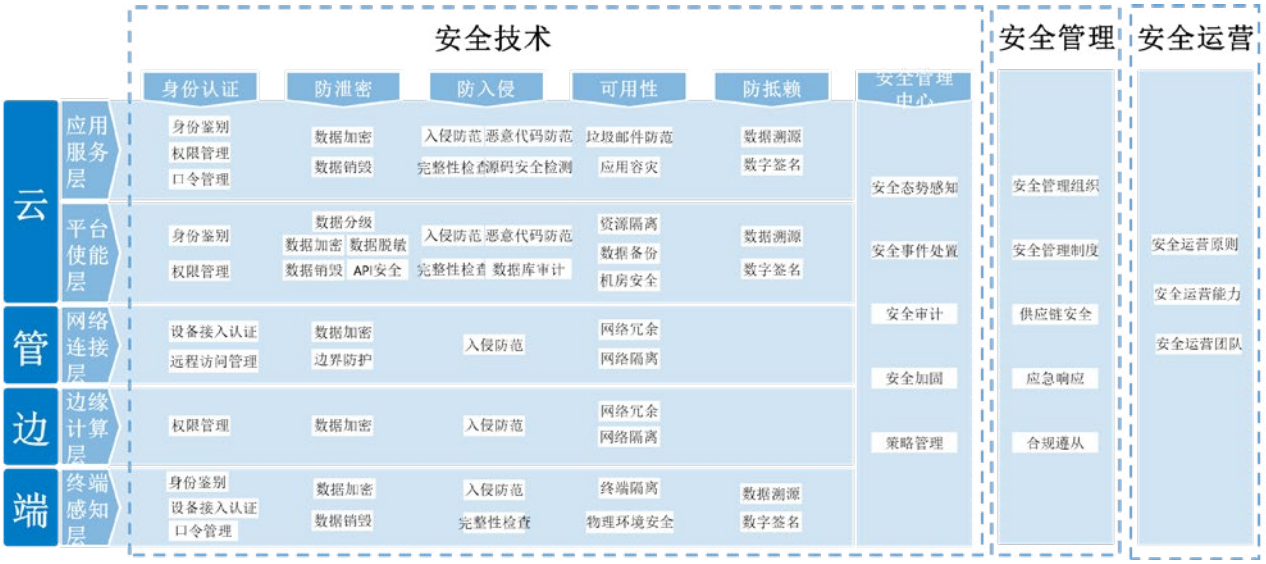


图 2 智慧城市安全架构

设计安全建设内容，包括管理体系和技术体系等；建设实施阶段，依托业内优势安全技术产品，为智慧政务大数据云中心提供专业级安全资源池基础防护能力和满足安全等保合规持续建设要求的服务能力；最后在治理运营阶段，助力建设城市级网络安全集中监控运营中心，实现对智慧城市网络安全事件的综合分析、态势感知、风险预警。

- 云计算安全运营

云安全解决方案主要是将资源池安全能力和端点防护相结合，提供丰富的云安全服务，可帮助用户从网络、主机、应用和数据等多个维度进行防护，形成安全服务闭环；利用图形化的界面帮助用户快速了解整个云平台的安全态势，及时发现未知威胁，同步到相应安全服务，协同防御；整个安全服务采用自动化的交付模式，可快速完成安全服务交付，提升业务响应速度和运维管理效率。并最终形成基于云中心外部安全及虚拟化层防护，结合线上运营、线下服务的立体防护体系。

云安全解决方案的核心优势是“云地人机”的服务理念，能够提供诸如核心数据导出、云端 7×24 小时值守团队的协助，且与地面部队支撑相结合的云端能力。如果云端无法完全解决，还可以提供地面部队及时到达客户现场，为客户排忧解难。

- 企业安全运营

在企业安全运营层面，为企业用户提供基于 MDR（可管理的检测与响应）技术的一体化安全运营服务。MDR 是一种集安全检测设备、安全分析平台、安全专家服务的一站式安全运营支撑服务。主要用于帮助企业建立威胁监控体系，帮助企业及时发现 APT 攻击。

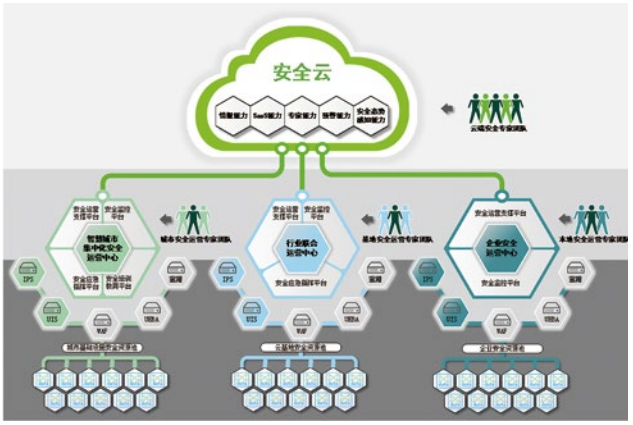


图 3 云计算安全运营体系

五、安全运营的展望

1. 运营模式创新

“安全成熟度”是一个综合的考量尺度，包括建设投入、人员数量与技能、安全的认知等。但安全运营也并不是“成熟”阶层的专属，在安全体系发展的各个阶段都可以匹配不同的安全运营模式与内容。

智慧城市安全运营建设中，对于规模较小、可经营性较强、厂商愿意积极参与的项目，可采用政府引导的方式，交由市场建设运营，根据项目运营效果，给予奖励补助。这样，一方面节约了政府财力；另一方面提高了市场参与热情，以提供更优质的服务。

图 4 企业级 MDR 一体化安全运营服务

综合性较强、投资较大、运营维护难的智慧城市项目，尤其是牵涉多个重大项目并行推进的系统性工程，可以采用政府购买服务的一揽子模式，由实力较强的厂商做总包，包括后期的运营维护，政府每年只支付购买服务的费用。这样既减轻了政府的财政压力，同时培养了企业，推动了信息产业的发展。

2. 运营标准化

运营标准化，简单地说就是建立标准化的运营体系，按体系要求系统化管理。例如，麦当劳、肯德基、星巴克的上千家门店对于产品、工艺、服务流程、品质有着统一的标准。

有的企业虽然项目做了一个又一个，但每操作一个新项目时，还是会犯同样的错误，一次次重复交学费，这就是运营缺乏统一标准的问题。出现这种问题的企业，一般会找一个专业能人来带领团队，而不是建立企业层面的标准化运营体系。专业能人凭借自己的能力，在缺乏统一指导下依旧能管理好这样的团队。但当能人离开后，组织能力一切归零。

因此，需要建立标准化运营体系。通过不断发掘并整合以往运营中积累的经验和教训。

第一，让运营操作经验教训得以总结并在新的业务上得以推广。

第二，增强企业在规模上的承载力，保证规模扩大后的风格统一。

标准化运营体系包括：运营策划、运营实施、运营监督、运营改善。其中，运营标准化需要策划的内容包括：产品标准化、流程标准化、操作规范标准化、工作成果标准化。

标准化运营可以实现科学管理、量化管理、思想和行动的统一；有利于提高产品质量和劳动效率，有助于提高服务质量，树立企业形象；企业运营模式得以复制，当专业人员流动时，不会给企业带来巨大损失。

3. 开放异构的能力

异构安全体系与非异构安全体系主要有以下几个方面的区别：

（1）策略规范异构

不同安全厂商的产品默认的安全策略规范不同，能有效地增加入侵者的破解难度。网络中异构的安全设备如果都能正确配置不同的安全设置，就能形成一个深入的具有多层防护功能的安全系统，

这意味着如果黑客想获得系统内的重要文件就要面临不同的障碍。

（2）通信协议异构

安全厂商一般都有各自的私有通信协议，一般的入侵者只能掌握一家或两家的私有通信协议。异构的安全设备增加了通信系统的复杂性，好比不同结构的防盗门黑客的攻击行为难以奏效。

（3）底层系统异构

主流安全厂商都研发了自己的安全操作系统，在该系统上开发相应的安全防护产品。原则上专业安全操作系统几乎是没有漏洞的，但是安全行为是动态变化的，像微软这样实力强大的公司都不断地打补丁，安全设备系统的升级周期一般都在半年左右，从这个方面来考虑，不同的安全系统能有效地的阻止入侵行为，提高安全体系的防御能力。

基于以上几点原因，在安全运营建设时建议考虑异构安全体系，并且在建设指导文件中规定不同安全级别的安全域互联要求部署不同厂家的安全防护设备。

4. 运营体系设计

安全运营的最终目标是逐步形成适合用户自身的安全运营体系，因此，需要做好以下几点：

（1）组织架构设计

应根据自身的组织架构、业务特点设计运营岗位、运营流程、运营制度、运营考评机制，建立完善的安全运营体系。要充分考虑现有安全组织机构情况、安全建设水平、安全保障能力等现状，为运营体系设计提供现实资料保障。根据安全防护范围，垂直管理情况，组织机构设计情况，安全保障人员情况等，确定安全监控、安全分析、安全响应等各类角色，设置安全监控员、安全分析员、安全处置员、应急响应领导小组等。

（2）事件响应流程设计

根据自身行政管理机制，责任落实机制的特点，有针对性地设计安全事件监控、分析、通告、响应、处置、复核等全周期的安全运营流程，确保安全运营工作可闭环管理。

（3）安全规则设计

能够在深入理解业务的基础上，结合业务特点，完成各类安全威胁场景的建模。通过自定义场景规则，不断优化，提升准确度，将日常威胁事件处理的数量控制在可人工处理数量级。成熟的安全运营体系一定要确保自身是可消化、可吸收的。

结束语

安全运营建设应与智慧城市建设应同步规划、同步建设、同步使用。智慧城市的安全建设也不可能一蹴而就，而是一个长期运营，不断完善的过程。围绕防泄密、防攻击的安全目标，统一规划、分步实施、长期坚持，逐步构建完善的智慧城市网络安全体系。

API崛起下的Bot管理

绿盟科技 WAS产品部 刘嘉奇 刘书浩 詹圣君 盛德祥 / 系统架构部 查文静

近几年，应用安全领域的新技术、新厂商如雨后春笋般涌现。该领域之所以会如此快速地发展，一方面，得益于 nginx 及 OpenResty 高扩展性的设计，使得技术团队可以专注于特定安全问题，并且快速开展攻防能力的研发，不必投入驱动级 HOOK、内核协议栈修改以及用户态的 HTTP 协议解析代理等这些复杂而又晦涩的底层技术领域；另一方面，应用是承载着信息交互的实际桥梁。随着信息化浪潮的来临与科技的进步，云、大、物、移作为基础设施逐渐完善，企业必然有更多的业务通过应用（web、移动、人工智能机器人）对外提供。诸多因素推动当前应用开发模式在迈向 devops 及 API 服务化。在新模式的原始阶段，安全的诉求会接踵而至，而笔者团队在 Bot 管理领域具有一定的技术积累，希望与应用开发及应用安全领域的从业者进行交流。

我们先引用一些咨询机构在应用安全领域报告中的摘要：

“到 2023 年，网络中 Bot 流量的比例将会超过‘人的请求流量’。

到 2022 年，API 滥用将转变为最常见的攻击方式，从而导致数据信息泄露，这将成为 Web 企业面临的严重问题。

到 2021 年，将有 90% 的 Web 应用程序以 API 而非 UI 的形式面对网络攻击，其占比远远高于 2019 年的 40%。”

可以看到，API 将是未来企业核心对外的业务接口，这导致了 Bot 流量占比继续大幅度上升。它一方面增加了业务与业务之间正常的交互，另一方面却催生了背后附加的黑灰产的蓬勃发展，猫池、接码、打码平台等一条龙工具随着 API 的启用，更加便捷、灵活。

1）Bot 模拟正常人操作实现下面的请求更加难以识别：

a. 信息泄露：内容爬虫、价格爬虫

b. 漏洞探测：自动化扫描

c. 账户安全：信用接管（暴力破解、撞库）、恶意注册

2）业务安全防护的难度更高：

a. 交易欺诈：虚假交易、薅羊毛

b. 恶意竞争：库存囤积、黄牛党

3）从面向 HTML 格式的 URL 攻击，变身为针对 XML/JSON 的攻击脆弱性更明显：

a. API 滥用：短信轰炸、拖库

b. 信息泄露：数据遍历、批量获取

c. 身份越权

d. 恶意访问

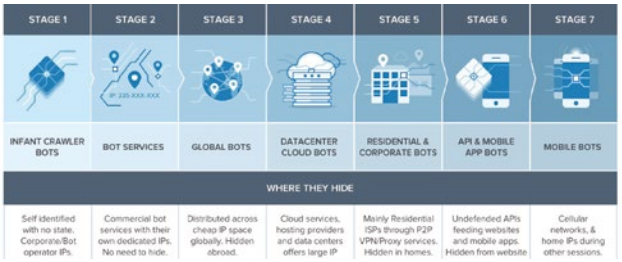


图 1 Bot 衍进路线

以前对抗这类黑灰产，Bot 识别是核心工作。一般应有几个层

级的图灵测试：

1）简单脚本 -- 爬虫、Python 脚本

一般爬虫和简易的 Python 脚本工具等都不具备 JS 脚本的执行能力，通过在流量中注入 JS，验证客户端脚本执行能力来进行识别。

2）一般工具 -- PhantomJS 扫描器等工具

PhantomJS 和主流扫描器（Appscan、AWVS、RSAS 等）都集成了 JS 解析引擎，因此都能够执行 JS 脚本，我们需要通过随机选取 W3C 规范中的浏览器属性以及各个不同浏览器的特殊属性进行组合来判断客户端是否为真实的浏览器。

3）高级工具 -- seleium + Webdriver

Webdriver 是目前使用最多的前端自动化测试工具，它能够打开一个真实的浏览器并通过脚本来进行操作。在识别这种高级工具时，我们需要通过监听操作事件来获取操作特征，比如，鼠标移动轨迹、按键频率等，判断是否为真人操作。

4）专业工具 -- seleium + Webdriver + 模拟操作特征

在黑产专业工具中，攻击者一般会通过代码来模拟真人操作触发相应的事件，这种情况下，我们建议结合 API，将收集到的操作特征数据，基于 API 进行聚类，来判断是否为真实的人工操作。

而在 API 环境下，上述通过下发 JS 来实现层层递进的自动化工具检测，有些场景却无法完成校验工作。经过研究调用，目前发现了一种技术手段可以对该类问题进行解决——将 API 调用顺序，抽象为场景模型，结合业务的理解，标识意图为 Bot 的流量：

1）基于 Bot 行为特征进行初步分类

- 利好 Bot：搜索引擎、合作伙伴、第三方服务
- 中立 Bot：爬虫、不明意图机器人
- 恶意 Bot：恶意评论、垃圾邮件、价格 / 库存爬虫、扫描器、恶意抢购

2）将 Bot 行为及业务特征进行联合分析

- 记录 Bot 行动轨迹，结合网站业务特征来分析机器人的行为特征。例如机器人访问的都是商品页面，还是频繁地提交同一个 / 一组表单，或者是无意义的访问了很多 404 页面。

同时，可视化呈现各类已识别意图的访问轨迹、行为和特征属性，帮助用户结合业务挖掘哪些业务是 Bot 最主要的目标，能够获取怎样潜在的利益。完成 API 环境下跟黑灰产的对抗及处置。

此外，WAF、API 安全与 Bot 管理三位应用安全成员未来的关系，也是困扰咨询机构和国内外 WAF 大厂的一个问题。两家咨询机构 Forrester 和 Gartner 持有的意见各有侧重，而 akamai、imperva、F5 三家曾作为 leader 象限的厂商，应对方式也不尽相同。到底会融为一体，还是组合成 WAAP 解决方案，或是独立存在，还需要随着技术和环境的演进慢慢得到统一。笔者团队也多次讨论过这个问题，我们更倾向于形成 WAAP 平台——支持 WAF、Bot

管理及 API 防护几个组件在公共资源、受限资源和内部资源间进行选择性部署，形成不同的防护等级，具备多种安全能力联合组合解决方案，为应用提供分层递进的安全体系架构。讨论的观点主要有:

1）这两种防护能力是无法进行替换的，Bot 管理虽然可以通过页面混淆使得扫描器无法扫描成功，但它仅仅是一个针对机器人的迷宫，如果后面的数据没有一道实在的‘墙’在前面检测攻击，正常人无需任何额外技巧，可以直接绕开这种防护能力。

2）规划防护资源的视角不同，如前文所述，Bot 管理是基于同一个域下不同业务类型进行管理的，如登录、活动、服务集等，而 WAF 则面向站点的开发语言和中间件。这会导致配置无法归一。

3）Bot 防护的核心在于管理，根据 Bot 类型和活动情况，分别、分时调整，这是一款中度使用的产品，并应具备以下管理手段：

- 限流: 最通用、也是最温和的一种方式。对于机器人操作者来说，只是网站的访问速度变慢了；但对于企业来说，是在不打草惊蛇的基础上，缓解了机器人造成的资源浪费、释放了服务器资源。限流措施适用于第三方服务机器人、不明意图的机器人等类型。哪怕是扫描器类型的机器人，有些时候限流措施都比直接封堵要更加适合。

- 欺骗：对于抱着特定目的而来的机器人，欺骗措施非常适用。例如对于价格爬虫，可以通过欺骗的方式，返回给爬虫一个错误的价格，诱导竞争对手设置错误的价格。而此时竞争对手完全意料不到自己获取到的是错误信息。

- 引流：当机器人流量太大以至于确实影响到了正常的业务流量时，可以通过引流的方式，把机器人流量都分流到空闲服务器或其他业务服务器上，从而缓解业务高峰期的压力，为优质用户提供更好的用户体验。

- 提醒原站：此方式非常适用于业务逻辑复杂的场景，避免网关类型的设备过多地介入业务逻辑带来的配置难题。此时只需要告诉源站，哪些请求可能是机器人流量，由源站结合此信息来判断响应内容。例如优惠券抢购活动，通过提醒源站，源站可以给机器人流量返回高折扣的优惠券。这样既不会减少活动热度（点击率），又不会造成业务损失，为企业热门活动节约了成本。

- 二次校验：类似于验证码机制，在有风险的情况下，增加二次验证，避免正常客户业务无法进行，又增加了黑灰产进一步获利的难度。

因此，在恰当的时机调整 WAF、API 安全及 Bot 管理产品的技术规划路线，进行 WAAP 的预研及 devops 环境的对接，应当可以在应用开发快速发展的未来，持续提供足够的安全保护能力。

过往20年看安全服务变迁

绿盟科技 专业安全服务中心 曹嘉 / 咨询设计部 赵波 / 网络安全学院 杨方宇

绿盟科技安全服务体系从无到有，可以将其分成五个阶段。

第一阶段：安全能力传递（2000 年~ 2003 年）

自绿盟科技成立伊始，安全服务就成为首批具有鲜明绿盟特色的安全业务，早期安全服务的主要客户群体是互联网企业，其企业规模和如今的互联网企业不可同日而语，服务内容也相对单一，主要是围绕服务器这一核心资产进行的技术性服务：包括渗透测试（攻防能力展示）、安全加固（缺陷修复）、应急响应（抑制和止损）、安全培训（知识能力传递）。基于自身安全能力的传递和变现成为安全服务在国内行业启动的第一源动力。

这期间，绿盟科技开始实践并孵化出了一些工程服务的业务雏形。

1. 尝试管理评估

基于英国标准化协会《信息安全管理体系》标准 BS7799，尝试在客户项目中进行目标明确的管理评估（与管理评估相对应的通常被称为技术评估），这为后来的风险评估体系化和管理咨询业务注入了关键基因。

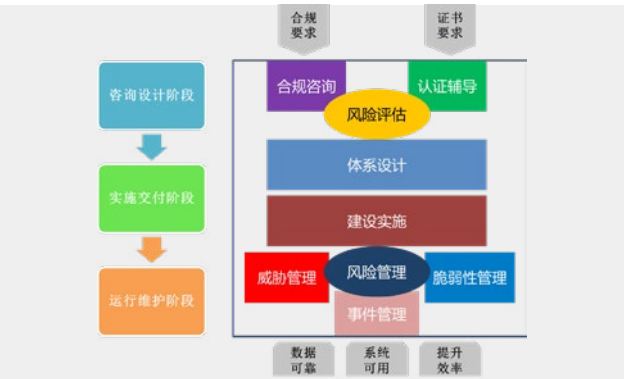
2. 标准化安全服务

随着服务项目体量的逐步加大，包括中标某运营商的全网评估，都对工程管理、文档质量和数据呈现提出了更高的要求。当时正值非典时期，疫情期间业务的暂时搁置给了技术人员大量的空窗期，他们对文档模版、工作规范开始了全面的标准制定，包括渗透测试报告等模版都开始出现了。这一标准化工作的启动，一改安全服务输出成果的文档形态，更加贴近技术文档的行业现状，成为安全服务标准化的第一步。

第二阶段：安全服务体系建立期（2003 年~ 2008 年）

在绿盟科技的“产品”和“服务”两大业务体系的构建过程中，如同行业内众多安全细分领域的创业公司一样，绿盟科技在以服务为触点接触客户的同时，为产品赋能成为安全服务的重要使命：围绕产品构建服务体系；通过产品为人员二度赋能：如基于扫描器进行评估服务，基于 IDS 流量进行一定周期内的威胁分析。这一模式很大程度上解决了“专家级”人才相对不足的问题，人员通过产品培训以及基础知识储备即可完成“程序化”服务。

这一阶段，绿盟科技安全服务的服务主张逐步形成，一个优秀的服务离不开清晰的服务主张，只有具备服务主张，服务人员才能和客户最大程度上达成一致的认知。早期绿盟提出的服务主张被概括为 5-3-9-3 模型（5 个目标、3 个阶段、9 个服务模块、3 个价值）。



5-3-9-3 模型

通过 5-3-9-3 模型可以看到，其融合了 BS7799、国际标准化委员会《信息安全管理指南》标准 ISO/IEC 13335 以及系统安全工程能力成熟度模型 SSE-CMM 的体系思想，充分识别了认证合规、风险管理以及数据和业务可靠的安全服务核心驱动力，尤其是数据可靠这一安全目标的识别，在当时是难能可贵的。在这一时期，安全合规以及与 IT 治理相关的咨询服务随着 BS7799 被采纳为 ISO27 系列标准，以及美国《萨班斯—奥克斯利法案》SOX 的出台，绿盟科技安全服务开始逐步进入客户的视野并且获得了客户的认可。越来越多的客户意识到各项安全工作推进前，安全标准需先行，安全标准的重要性被提升至了新的高度。绿盟科技也从向单一客户提供技术和管理的实践性服务，逐步过渡到参与行业安全标准乃至国家网络信息安全标准的制定，包括国家信息安全产品测评中心《网上证券交易系统安全保障要求》、公安部《信息系统等级保护评估实施指南》、国家信息中心《信息安全风险评估 / 管理指南框架》、证监会《证券期货业安全保障体系》、国家应急响应处理中心《网络安全事件处理服务规范》等一系列标准的讨论和制定，这其中均可以看到绿盟科技安全服务顾问的身影。通过对安全标准的充分理解和吸纳，并将其与绿盟科技的原生服务能力融合，绿盟科技通过 5-3-9-3 模型首次将风险管理、认证咨询与合规和可管理安全服务（MSS）整合形成统一解决方案的体系模型，这也奠定了绿盟科技安全服务体系化的发展基石。

值得一提的是，这一阶段的绿盟科技也开始尝试通过全面运营的方式助力客户安全能力的提升。2003 年正值与微软操作系统相关的各类蠕虫爆发的时期，包括冲击波在内的蠕虫爆发给大量企业造成了巨大的业务损失，绿盟科技立即启动与某国内大型券商的全面运营服务，作为安全第一责任人全面参与各项网络安全工作，将日常运维服务与系统安全管理紧密融合，迅速带动了客户安全能力的实质提升。

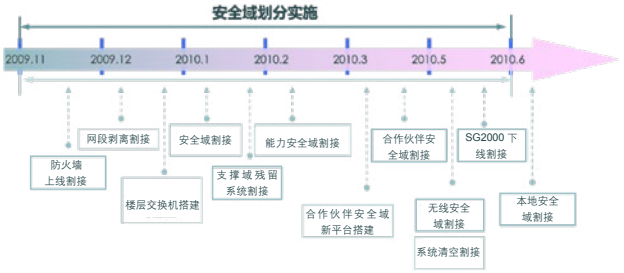
随着 2008 年北京奥运会的举办，绿盟科技也首次参与国家级重大活动的保障。经历了国家重保，绿盟科技意识到安全服务的“地面部队”需要与云端能力共同构建，从而形成立体的保障体系。通过云端能力和现场保障人员的充分连接建立“云地”两级的保障体系，这也成了绿盟科技“云地人机”思想的雏形。

第三阶段：安全服务成熟期（2008 年 ~ 2014 年）

随着行业客户的崛起和成熟，绿盟科技安全服务也进入了业务的成熟期。典型模式中开始将服务能力与行业特点和业务场景相融合，无论是针对银行业的电子银行评估，还是主要面向运营商行业的安全域划分，绿盟科技安全服务均成为行业服务的标杆，同时也进入了行业客户和通用安全的视野。善用依托通用安全服务的能力和知识体系，设计具有行业针对性的安全服务，成为绿盟科技安全服务的特色。

电子银行安全评估报告内容	权重	总分		分项值
1. 安全策略	15%	10分	1.1 安全策略制定的流程与合理性	2
			1.2 系统设计与开发的安全策略	1.5
			1.3 系统测试与验收的安全策略	1.5
			1.4 系统运行与维护的安全策略	1.5
			1.5 系统备份与应急的安全策略	1.5
			1.6 客户信息安全策略	2
2. 内控制度建设	15%	10分	2.1 内部控制体系总体建设的科学性与适宜性	3
			2.2 董事会和高级管理层在电子银行安全和风险管理体系中的职责，以及相关部门职责和责任的合理性	3
			2.3 安全监控机制的建设与运行情况	2
			2.4 内部审计制度的建设与运行情况	2
3.风险管理状态	15%	10分	3.1 电子银行风险管理架构的适应性和合理性	2
			3.2 董事会和高级管理层对电子银行安全与风险管理的认知能力与相关政策、策略的指定执行情况	2
			3.3 电子银行管理机构职责设置的合理性及对相关风险的管控能力	2
			3.4 管理人员配备与培训情况	1
			3.5 电子银行风险管理的规章制度与操作规定、程序等的执行情况	1
			3.6 电子银行业务的主要风险及管理情况	1
			3.7 业务外包管理制度建设与管理状况	1
4. 系统安全性	20%	10分	4.1 物理安全	1
			4.2 数据通讯安全	2.5
			4.3 应用系统安全	2.5
			4.4 秘钥管理	1
			4.5 客户信息认证与保密	1.5
			4.6 入侵监测机制和报告反应机制	1.5
5. 电子银行业务运行连续性计划	15%	10分	5.1 保障业务连续运营的设备和系统能力	5
			5.2 保证业务连续运营的制度安排和执行情况	5
6. 电子银行业务运行应急计划	15%	10分	6.1 电子银行应急制度建设与执行情况	2
			6.2 电子银行应急设施设备配备情况	3
			6.3 定期、持续性检测与演练情况	2
			6.4 应对意外事故或外部攻击的能力	3
7. 电子银行风险预警体系	3%	10分		10
8. 其他重要安全环节的机制的管理	2%	10分		10

典型行业服务 - 电子银行评估



典型行业服务 - 安全域划分

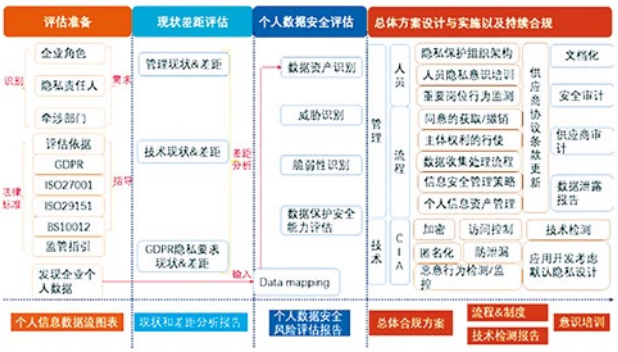
同时，这一时期的安全服务体系也将咨询设计、可管理安全服务、教育与培训、安全能力评价以及安全研究等主要的服务领域进行了更加模块化的设计，形成了更加清晰的客户服务全景。参考 IT 服务领域的成熟经验，绿盟科技安全服务也引入了“服务产品化”的概念，即基于安全服务研发和交付的同时性，快速构建创新服务的体验原型，实现安全服务能力端到端的交付与快速复制。

绿盟科技安全服务体系

第四阶段：安全服务爆发期（2014 年~ 2018 年）

随着 2014 年绿盟科技在深交所上市，在原有优势的基础上，对安全研究领域加大投入，分别在物联网、云计算与虚拟化、数据智能等前沿领域成立了独立实验室，并且发布了智慧安全 2.0 战略，正式启动基于“云地人机”的安全运营战略转型之路；服务业务也开始走向海外市场，其中具有代表性的包括在海外陆续建立的云清洗中心 Cloud DPS 等服务能力建设。

这一时期，合规与治理的外部政策环境出现了里程碑式的根本变化，随着《网络安全法》、欧盟《通用数据保护条例》（简称 GDPR）等法律的相继发布和实施，资产保护的视角从聚焦服务器资产和人员资产逐步转向关注全生命周期的数据资产。从这两年网络安全大会 RSAC 创新沙箱环节的评选就可见一斑，数据和隐私成为新的行业热点，一批相关领域初创公司（2020 年的创新沙箱得奖者 Securiti.ai 就是典型代表）开始涌现。在数据和隐私这条安全新赛道上，绿盟科技及时面向客户群体启动了针对 GDPR 以及《网络安全法》的政策解读，并第一时间面向具有跨境业务的客户提供 GDPR 咨询服务，从人员、流程、技术和隐私治理等多角度出发，督促企业尽快符合 GDPR 的要求，成为最早拥抱数据和隐私领域的国内主流安全服务商。



绿盟科技 GDPR 咨询合规服务

在对抗领域，在“震网”Stuxnet 时期初露端倪的 APT 攻击以及全球网络战逐步成为安全的新兴驱动力。在此背景下，国家也对关键信息基础设施保护提出了更高的要求，评估服务在作为不可替代的基础服务的同时，更具对抗性和协同效果的评估服务如红队 / 蓝队（RedTeam/BlueTeam）服务作为增性型服务开始出现。为应对对抗升级，绿盟科技通过建立专业的红队和蓝队，将攻防能力、设备防护与运营能力，分别从红蓝两方的视角面向企业客户提供对抗服务，从而确保关键信息基础设施在运行过程中，可以实现情报能力、事件响应能力和对抗性能力的协同运营。

第五阶段：安全服务体系 2.0（2018 年~至今）

回顾绿盟科技安全服务体系的演进过程，其核心驱动力始终是

以风险管理、合规驱动以及新技术领域或新攻击面为导向，进行全生命周期管理的服务理念，姑且称之为安全服务体系 1.0。基于这一理念，绿盟科技认为构建一个成熟的安全服务体系的基础要素包括服务主张、核心能力、体系化和标准化能力以及持续运营能力。那么，面向未来安全服务业务领域，进行 2.0 版本的服务体系升级，需要哪些变革呢？

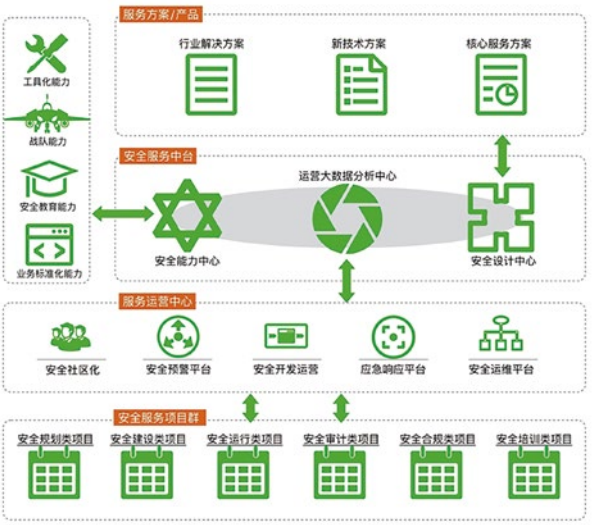
1. 逐步改变以产品和服务为触点的模式，将用户视作安全能力运营中的监测点，通过辅助用户闭环运营来驱使安全能力的提升。

2. 服务能力从依托专家和积累经验的异质性交付，变为以知识管理为前提，依托高效能平台工具，将安全能力传递给用户并构建有效的运营机制。

3. 安全人才从单一的攻防型人才强势需求，走向细分岗位横纵拉通、高效协作的复合型需求。安全服务体系 2.0 将出现能力团队、运营团队、服务方案设计团队以及专项业务纵向指导团队，实现了从需求到建设，再到运营的立体架构。

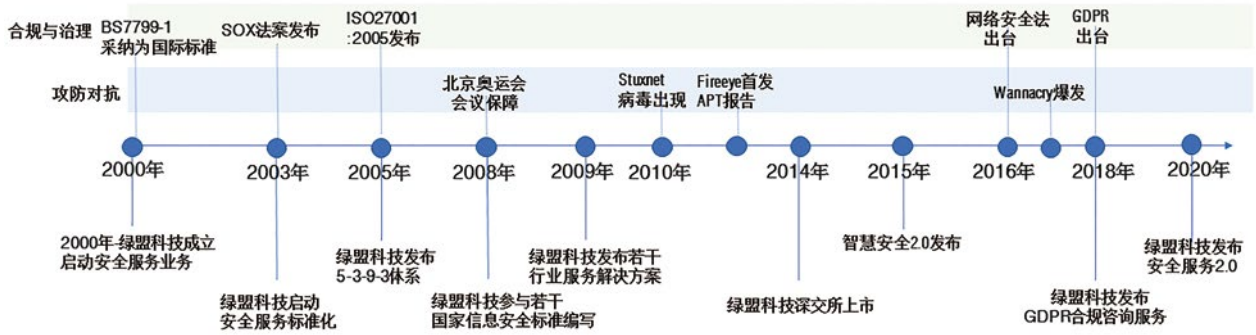
4. 安全人才与业务模式互为推力，安全人才在演进的过程中呈现出多元化的发展态势，其实是业务需求、技术变更和监管的共同驱动作用下，推动安全服务业务模式的进步。安全人才在业务模式的带动下，岗位发展逐步精细化，当专业化人才形成规模时，反过来会对安全服务业务进行正向的改进和优化。因此，需要对体系化和标准化的服务框架进行撮合，相互促进。

绿盟科技安全服务体系 2.0 立足于自身安全能力以及对行业客户的理解，以“创新、共建、价值化”作为服务理念，将服务项目、服务数据、服务人员作为触点，通过运营强化和知识管理来构建服务能力中台，最终通过“标准化 + 方案化”的服务产品来进行端到端的交付，实现面向客户的能力转移。



绿盟科技安全服务体系 2.0

可以预见，在新的安全体系下，除了风险管理、合规治理以及新增攻击面等传统驱动力，通过新的数据和知识驱动，将衍生出一系列新兴服务：



信息安全行业以及绿盟科技安全服务时间轴（2000 年~ 2020 年）

新体系下的安全体系建设咨询：随着安全思想的进步以及专业安全人员的相对稀缺，原有的安全体系难以更好地匹配安全建设、检测与响应等场景的需求。而“对抗战术、技术和常识”ATT&CK 框架、安全编排自动化与响应 SOAR 等兼具知识管理，可拓展、可落地，具备实战能力的体系模型开始成为客户安全建设时的体系参照，由此衍生出的威胁建模等服务，将客户的检测和响应体系、自动化能力以及内外部安全数据和知识更好地进行结合，使企业安全建设能力得以最大程度地发挥，实现投入和产出比的最大化。

情报与协同服务：由于安全行业存在大量的细分领域，任一安全厂商可能都无法独立完整构建满足客户需求的安全情报体系，即便客户采购多源的情报，但这些情报如何更精准地应用于客户，往往只有贴近客户的服务供应商才有最大的发言权。了解企业的资产情况和风险偏好，结合外部多情报源的输入，并发挥安全厂商原生情报和社区化能力，将使企业应对关键时刻，（如国家级演练、高危漏洞爆发时）快速响应和决策，拉通每个客户形成一定范围的情报共享社区，实现跨企业的响应闭环和情报共享。

数据分析与评价服务：随着客户运营能力的增强，服务过程中产生的大量客观数据和主观评价，均可用于持续定级和度量当前的安全运营状态。安全厂商在介入运营的过程中，也会提供更强的数据能力和决策建议能力，协助企业掌握自身的风险评级。

结束语

绿盟科技经过在安全服务领域的深耕，并与各行业客户风雨同舟二十载，深深意识到安全服务能力的长期发展将是对服务团队耐力和生命力的考验，其过程注定是持续而漫长的，若失去了耐力和延续性，安全服务能力的进步将停滞或者偏离。安全服务是一种共创价值的业务形态，持续抓住客户需求并对其精准回应，共同决策，共同积累和沉淀经验，最终共同实现安全能力的螺旋式上升。

最后，用我翻阅 2001 年绿盟科技的某一份测试报告时，无意中看到的一句话结束本文，“虽然我们可以利用各种工具来完成一些自动化的检测工作，但是更重要的是经过我们经验丰富的工程师的人工检测，撰写了这样一份易于理解和实施的专业性报告，这是任何安全工具都不能实现的目标”。

绿盟科技安全服务，将安全带到设备不可达的地方。

（感谢左磊、陈庆、付峥、王红阳、徐特、程文静对本文的意见以及提供的相关素材。）

AI时代的安全对抗，人永远是技术主宰

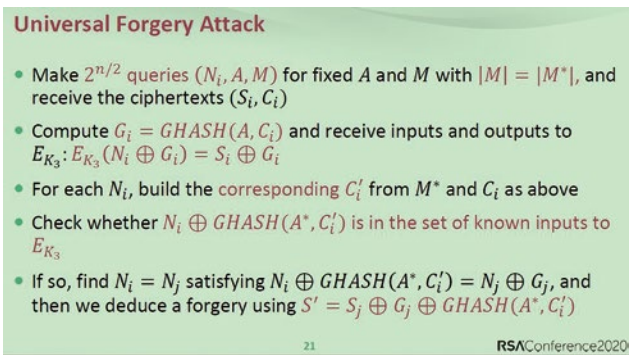
绿盟科技 总工办 顾杜娟

我们知道，AI 将在很长一段时间占据互联网技术时代的风口。但是，有代码的地方就有缺陷，随着 AI 技术在安全领域的运用，AI 对安全产业起到了极大的赋能作用，但自身安全问题也随之上升到前所未有的高度，更糟糕的是 AI 极有可能会成为攻击者的利器。

一、AI 被攻击者滥用

How AI inference threats might influence the outcome of 2020 election 报告指出：AI 算法和代码的设计都依赖编程人员的判断与选择，因此极容易被利益集团操纵。

1. **网络攻击者使用 AI 分析防御机制，模拟行为模式以绕过安全控制，利用分析和机器学习进行黑客攻击，并且制造深度伪造内容，包括视频、音频和文本记录等**。据了解，AI 已经可以通过改变社交媒体上的舆论导向来操纵选民的投票行为，破坏选民的政治情感中立性，从而影响最终的选举结果。伪造视频将一个人的动作和语言叠加到另一个人身上，造成煽动政治暴力等严重后果，而 AI 的加入使深度造假难以检测。



2. **帮助黑客更方便地绕过传统的安全工具**。例如 DeepLocker 的新型攻击工具能够绕过传统的安全工具，在设备中安装勒索软件或其他恶意软件。SCYTHE 推出了 SCYTHE Marketplace，该平台使受信任的第三方开发人员能够为公司的攻击仿真平台创建新功能。红色、蓝色和紫色团队可以使用创建的模块来模拟某些类型的攻击并测试其防御。这两年绿盟科技一直致力于构建网络安全对抗演练系统，一方面在安全培训时提供模拟演练，另一方面验证安全防御方案的有效性并进行防御方案的学习推荐。

但是我们不能因为担心而阻碍AI的发展，人永远是技术的主宰，正如大会主题“人的因素”，才是网络安全的意义所在。

AI 赋能安全自动化和智能化

人工智能和机器学习的进步正在为网络安全的技术进步提供助力，以大数据、安全分析、深度学习、人机协同为代表的 AI 与网络安全融合实践日益增多，比如威胁情报、威胁检测与分析、智能安全平台等。

在这个大数据时代，越来越多的安全企业将威胁数据作为核

心资产。FireEye 推出 FireEye Mandiant hreat Intelligence Suite，提供威胁情报订阅相关服务；Palo Alto Networks 推出 Cortex XSOAR 集成威胁情报管理与 SOAR 功能；CrowdStrike 利用威胁情报提供端点恢复服务，帮助组织在被入侵后恢复业务运营。**威胁情报是打造基于情报的安全服务和平台的关键所在，对威胁数据进行挖掘分析、深入追踪，才可能真正地解决安全问题**。

融合各种异构威胁数据，将历史性本地日志、全球威胁态势和实时发生的事件流放在一起**构建安全知识图谱，打造从感知—决策—响应提供闭环管理的安全运营平台和解决方案**。

RSA 2020 大会上，思科推出 SecureX 平台整合不同的安全产品，自动化安全分析和处置，加快威胁检测和响应速度。Fortinet 发布的 FortiAI 利用深度神经网络实现对复杂决策场景的学习，原有安全专家处理的威胁分析、事件调查和威胁溯源等一系列耗时任务转为自动化执行，因此安全专家能够聚焦到更有价值的任务中。可见，AI / ML **技术提供智能分析和决策能力，被运用在安全运营流程的自动化上**。

AI 技术在威胁情报、安全分析和智能决策等方面的优势为应对动态多变、复杂交织的网络安全问题提供新思路。安全领域已经成为 AI 应用的重要领域之一。

AI+ 网络安全

AI 赋能网络安全同时，越来越多的议题开始关注机器本身的风险，数据安全、样本污染、识别系统混乱、软件漏洞等安全问题日益显现。本次 RSA 2020 上，来自不同领域的安全专家围绕“AI 与安全”的话题展开了讨论，AI 自身存在安全问题，包括隐私数据窃取问题、学习框架和组件漏洞被利用等问题。

敏感数据的识别和防护是国内外最重要的合规性要求，安全大数据有必要处理好正常的个人数据隐私利用与个人隐私保护关系。RSA 2020 创新沙盒冠军 SECURITI.ai 戳中了数据隐私保护这一全球性的难题和挑战，推出的 Auti 机器人自动化执行隐私保护，授予用户对数据的权利，成为用户数据的负责人和保管人，同时遵守全球隐私法规并建立与客户的信任。Intel Casimir Wierzynski 指出 AI 和隐私结合不是零和博弈问题，而是对计算和存储资源都提出了更高要求。安全领域对隐私关注更多，围绕隐私保护框架和自动化实施方面也变得更具实操性。

RSA 大会于 2 月 27 日下午对抗性 AI 的报告中给出了对真实 AI 系统的真实威胁和攻击示例。攻击者试图欺骗图像识别系统，了解系统的图像识别引擎如何工作后，找出有效欺骗的对抗样本并打破数学模型。同样，攻击者通过收集和处理大量安全数据，有效实施深度伪造攻击或欺诈网络安全中使用的 AI 模型。这两年我们开发对抗实验平台研究分析对抗样本攻击的经典算法，分析生成对抗样本的效率及其对深度学习模型的误导效果，为对抗样本检测和防御算法设计提供一定的技术基础，从而提供 AI 模型的鲁棒性。

AI 在推动安全产业发展同时，也需要我们加强对潜在风险的研判和防范。AI 数据样本、算法模型、框架平台等技术自身安全亟待加强，加强 AI 安全与治理前瞻研究，确保 AI 在不同领域中深入融合的安全发展和可靠应用。

总结

AI 已经来临，安全亦在前行。面对 AI，我们需要技术和监管共同发力，用其所长、避其所短，让 AI 在发挥最大优势的同时，防止其安全威胁，将 AI 与人类的关系维持在最佳状态。

绿盟科技作为一家网络安全公司，早已在不同安全产品中融入 AI 技术，同时做好 AI 技术发展背后的安全专家，提早对 AI 安全风险和应用威胁加强安全防范，确保 AI 技术的安全发展。

为什么绿盟科技要连续十三年参展RSA大会?

绿盟科技 品牌推广部 孟祥聃 / 安全能力中心 杨传安

650 余家企业或机构参展，超过 700 位演讲者、500 场议题分享……这就是 2020 年的 RSAC。

由 RSA 主办，拥有近 30 年历史的 RSA 大会（RSAC），作为全球规模最大的网络安全行业会议，一直着眼于推动全球网络安全

界的共享、创新与进步。来自全球的领先安全公司或者安全部门高级专家齐聚 RSAC，对当下的安全趋势、挑战、解决方案和创新点进行探讨。这使得 RSAC 逐渐成为一个网络安全从业者分享、学习的圣地，更是安全企业实现快速成长的秀场。

得益于绿盟科技北美分公司的高效协同，绿盟科技本次参展活动并未受到太多疫情的影响。无论是传统活动创新沙盒，还是各种圆桌会议、业界大咖的主题分享，抑或是展区热火朝天的交流摸底，此次前方不仅收获颇丰，更是借助 RSAC 这样一个平台以及国内外多种传播渠道，向全球发出了拥有近 20 年积累，属于绿盟科技自己的观点与声音。

今年是绿盟科技连续参展 RSAC 的第十三年。作为一家总部在中国北京，企业规模逾 3 千人的安全企业，远在美国旧金山的盛会，确实离我们大部分人有些距离。今年的 RSAC 虽然已经收尾，但相信不少人近期都会心生这样一个疑问：

我们为什么要大投入地参加这样一个远在美国的安全会议？而且还是连续十三年？参展 RSAC 对中国安全企业而言，核心价值在哪里？

从中国安全企业视角谈参展 RSAC 的三大价值

可以说，每年都有大量优秀的安全厂商、业界专家和客户会来到 RSAC，在大会期间分享他们创新的技术方案、优秀的安全体系建设和运营实践，以及前沿的风险治理思路。绿盟科技作为中国的网络安全产品和服务提供商，毫无疑问可以借助 RSAC 这个舞台，向全球客户针对性地展示我们最具竞争力的产品和方案。

这是一种输出的价值和收获。但除此之外，对参展企业而言还有输入的价值。

从安全企业产品和技术发展的角度，参加 RSAC 对企业战略的指导和验证是有重大价值的，而且几乎是其他任何行业会议都无法替代的。这个输入的价值可以概括为三点。

1. 指导企业国际化战略

要阐述这点，就要先简单介绍下此次绿盟科技在 Moscone 中心南厅的展位的设计思路。

我们此次在 RSAC 的现场，主要展示了抗 DDoS 和 Web 安全两方面的产品、方案，以及与之适配的服务——威胁情报和安全研究（2019 年 DDoS 攻击态势和网络安全观察两份国际版年度报告）。其中，抗 DDoS 囊括了绿盟科技在这个领域近 20 年的积累，一套完整度极高的产品和方案。Web 安全则是以绿盟科技在国内有极

高市场占有率的 WAF 为代表。

但是，在国内也可以称得上是“全线厂商”的绿盟科技，为什么只选择了这两个技术领域在 RSAC 做展示?

主要有四方面考虑：一是这两类产品交付更简单。特别是放到国际视野下，高效的产品交付能力尤为重要。二是相较于漏扫、IDPS 等产品，抗 DDoS 和 WAF 作为互联网基础设施安全层面的防护产品，能够较好地避开一些在采购不同国籍安全供应商时所考虑的一些不成文的敏感区域，也就意味着更容易被国外客户所接受。三是绿盟科技抗 DDoS 产品和囊括多项安全服务的整体方案，能面向客户种类的多样性极强，这也是全球客户非常看重的一个点。四是做出这样的选择，也是基于绿盟科技国际业务运营和参展 RSAC 多年来的经验积累。

所以，对于参展 RSAC 的中国安全企业而言，第一个重大输入价值，就是可以指导这家安全公司，产品和方案在国际化时应有的走向，应集中发力的点。

在 RSAC 现场，有更多和潜在的国际客户甚至是国际友商间交流的机会，可以在现场收集到更多真实需求和改进建议，可以看到不同区域性客户在场景上的差异，这份正反馈，可以帮助我们更积极地去修正（国际化的战略），进而持续提升产品和服务在国际市场的竞争力。

2. 商业模式转变的验证

商业模式的转变意味着创新。创新是伴随风险的，所以坚持这份创新需要信心。而信心需要前瞻的视野，以及实践的验证。

可以说，包括绿盟科技自身在内，国内许多安全企业，都在谋求这样一种变革，那就是从之前的产品交付为主，到运营服务交付为主的转变。对企业而言，无论是内部资源的整合，还是客户已有采购思维习惯的渗透和改变，这都是非常大的挑战。

近两年绿盟科技在强调的安全有效性的实战，就是这样一种变革的体现。

以抗 DDoS 这个领域为例，绿盟科技从最开始做的本地流量过滤，到之后覆盖全球的云端的近源清洗，再到去年加入了多点拨测模块帮助用户更好地监测网络链路质量 ADBOS，再到和安全托管服务结合，在云端将抗 DDoS 能力完全服务化、可订阅化，这是绿盟科技对从安全产品到安全运营服务这样一种转变或者进化途径的理解，也是我们当前的前进方向。

反勒索、托管检测与响应等也是类似。一个安全产品和服务如

果在设计之初就能更加关注效果而不是手段和过程，把安全效果的闭环、客户测的呈现等问题考虑清楚，产品和服务的价值才能在客户测得到更充分的体现。做到这些，好的产品和服务才有可能在商业性上脱颖而出。

在 RSAC，基于大量甲方对自身实践的分享，我们对如何将这种注重安全有效性、从产品交付转变到服务交付的理念，更好地契合甲方自身的信息安全管理实践，有了更深度的思考。同时，了解那些有类似想法，甚至已经成功转型的厂商的心得，对于还在途中的我们，也是一种莫大的鼓舞，和极为有效的经验参考。

所以，参展 RSAC，对增强我们坚持进行这样一个模式转变的信心，验证目前转变的方式方向是否合理，都大有裨益。

3. 对创新的借鉴与学习

创新是企业进步的原动力，对网络安全这样一个重技术、重产品化、重方案的行业而言，更是如此。但创新不等于从零开始。对国外技术应用和方案思路中创新性的学习和理解，是国内安全企业成长的必经之路。这是所有国内安全厂商不用回避，也无法回避，必须勇于承认的事实。

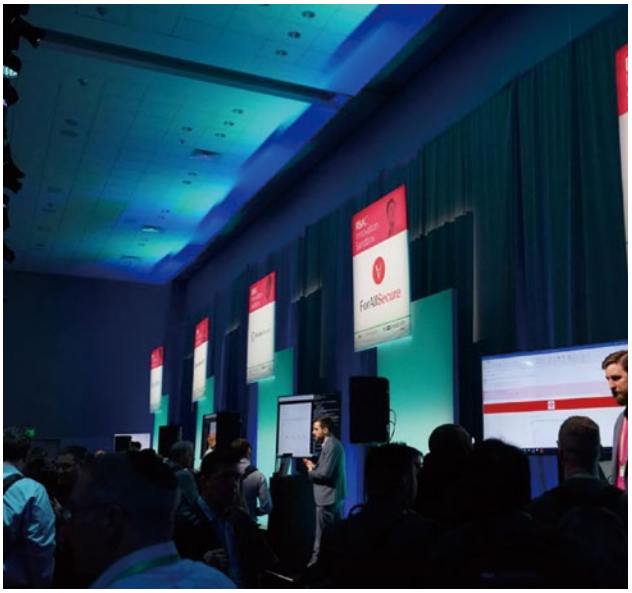
国家网络安全的整体水平可以说和人均 GDP 有着令人惊讶的正相关性。经济上越发达的国家，企业和信息化平均程度越高的国家，安全技术的创新和发展普遍也会越快，它们的网络安全整体水平也会越高。这基本已经是业界共识。

安全的本源是如何用新技术解决老问题。“新技术”，可以是新的安全技术，可以是原有安全技术的一种新的应用。要解决的“老问题”，一定是之前没有解决好的问题，所以要寻求新的“锤子”或者新的思路。闭门造车肯定是不可取的，在坚持自研的基础上，国内安全厂商还需要广泛地去交流、分享，进而借鉴、学习，甚至是投资、收购。

5 天时间，650 余家参展机构（今年受到疫情影响还比往年少了一些），500 场议题分享，2020 年的 RSAC 又是一场学习的盛宴，RSAC 能够吸引全球安全企业参与的独特魅力也正在于此。全球的领先厂商在这样一场会议中，集中展示、分享他们最新的技术应用成果。在这样一个氛围下，安全企业如何更好的对这些创新点进行借鉴学习，使其能够将全球业界最前沿的成果、趋势和自家对产品和服务进行打磨，更契合地融为一体，这是至关重要的。而且如果能够做好这点，无疑对企业加快应用新技术的速度，以及提升安全产品效能都有极大益处。

此外，RSAC 延续多年、更聚焦创业的特色活动——创新沙盒，

无论是对于追求“小而美”的安全初创，还是已有大体量但寻求更多更具有商业前景创新方向的头部厂商，都具备很高的分析和参考价值。



如果把安全行业的创新划分为两个维度：攻防技术的创新与行业的创新，那么从今年入选创新沙盒决赛 10 强公司的产品来看，我们发现，今年攻防的创新点聚焦在模糊测试、响应以及人工智能落地，而行业的创新则集中在敏捷开发、数据安全等热点领域。同时，我们还可以看到，自动化已经成为众多安全公司的产品兼具的特点，甚至贯穿安全活动始终。究其原因，是安全运营正面临更规模化、复杂化的挑战。通过自动化提升整体的安全防护效率，目前来看是一种较为行之有效的方式。

当然，无论是攻防技术创新还是行业创新，其最终目标还是解决用户面临的安全问题。今年 SECURITI.ai 之所以能够夺冠，其根本原因也在于此。有着近 20 年积累的绿盟科技，也始终秉承着以客户需求、合法合规为指引，不断更新客户化的行业安全解决方案，并通过安全产品和安全运营服务实现落地。

当今，国内网络安全行业的创新一直在前行，中国的网络安全整体水平也正稳步提升。所以，对中国安全企业而言，对 RSAC 上所谈及的创新性更多还是要抱着了解、学习的态度，而不应是模仿和搬运，真正落地自家产品和服务，落地国内的客户和场景，还需厂商结合自身的积累和客观国情，为客户提供安全、合规、友好的产品和服务，这才是我们的立足之本和发展之路。

2000年
NIDS发布

2001年
RSAS发布

2002年
ADS发布

开创千兆IDS先河

2004年
RSAS支持漏洞
说明及评分

2005年
国内首款NIPS发布

2006年
RSAS支持量化
资产风险评估

NTA发布

2007年
SAS发布

2008年
RSAS获西海岸实
验室Checkmark认证

WAF发布

2009年
IDPS获市场增
长领导者奖

BVS发布

2010年
NIPS获NSS Labs最高级别认证

国内首款OS/MS发布

2011
IDPS、WAF获
市场占有率

提出A计划，布
安全服务和运营

绿盟科技集团产品大事记

2017年

NIPS连续6年进入Gartner魔力象限，并进入挑战者象限

WAF连续4年进入Gartner魔力象限
连续8年Frost & Sullivan市场占有率第一

LAS、NCSS、TAT发布

ISOP（TSA）入选工信部案例集

ADBOS获广东省科学技术奖励

NF销售额累计破亿

WAF获ICSA Labs认证

2016年

TAC通过公安部APT产品检测

IDS-ICS、ISOP（ESP、TSA、TVM）、NTI发布

PZSO战略落地实施

2015年

RSAS连续2年入选Gartner报告

WVSS入选Gartner魔力象限

DLP、ISCS、ISTS、
ISOP（ESPC）、SEG发布

WAF销售额累计破亿元

NIPS连续7年获IDC市场占有率第一

2014年

ADS销售额累计破亿

DAS、NGTP、发布

RSAS创新发布虚拟化版本

2013年

TAC、WVSS发布

RSAS销售额累计破亿

2012年

NIPS获EAL3认证

2018年

SS、ISOP（TVM&TSA）、
BOS入选工信部试点示范

智慧安全2.0创新成果发布

M）、SAG、
发布

I究成与Palo Alto Networks、
reatQ的集成

ADS连续五年获Frost&Sullivan
市场排名第一

WAF获VERACODE VL4认证

2019年

IDPS、RSAS销售额
累计破2亿元

EDR、IDR、ISOP、NCSS-I、
SAS-ICS、UTS发布

ISOP、LAS销售额
累计破亿元

ISOP 在IDC AIRO调查中市场占有率
第一，获世界互联网先进成果

NTI支持IPv6资产测绘，获数
博会领先科技成果

DLP连续4年获赛迪销售第一

2020年

MagicFlow发布

ADBOS上线绿盟全球
云清洗服务中心

RSAS 连续8年获IDC国内市场份额第
一，作为历史代表性产品入选世界
互联网大会展区

图例说明

里程碑事件

新品发布

重大成绩

资质认证

绿盟智能安全运营平台

全场景，合规，智能

全场景覆盖，支撑企业安全运营，协助用户全面提升安全治理水平

全场景运营支撑 + 合规管理落地 + 智能运营辅助决策

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

绿盟云安全解决方案

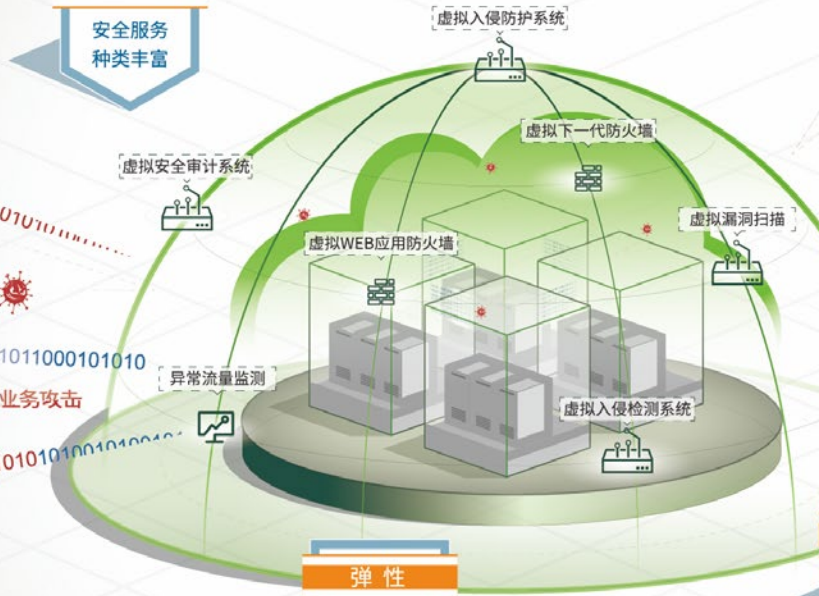
NSFOCUS CLOUD SECURITY SYSTEM

安全护“云”，随需而动

云上安全 绿盟守护
云背后的安全专家

全面
安全服务
种类丰富

灵活
满足云和传统
环境安全需求



窃取数据
恶意程序
业务攻击

弹性
按需购买
弹性可扩展

开放
第三方安全厂商、
多种云平台
及SDN控制器

方式灵活	能力丰富	形态多样	开放性
提供了多种引流方式（SDN API／策略路由等）可以适用于传统和云计算网络	提供了从预防、检测、防护，到响应等丰富的安全能力	不限于虚拟安全产品，也支持传统设备	兼容云平台、SDN控制器及第三方安全厂商产品

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技