Ruijie 锐捷 Networks

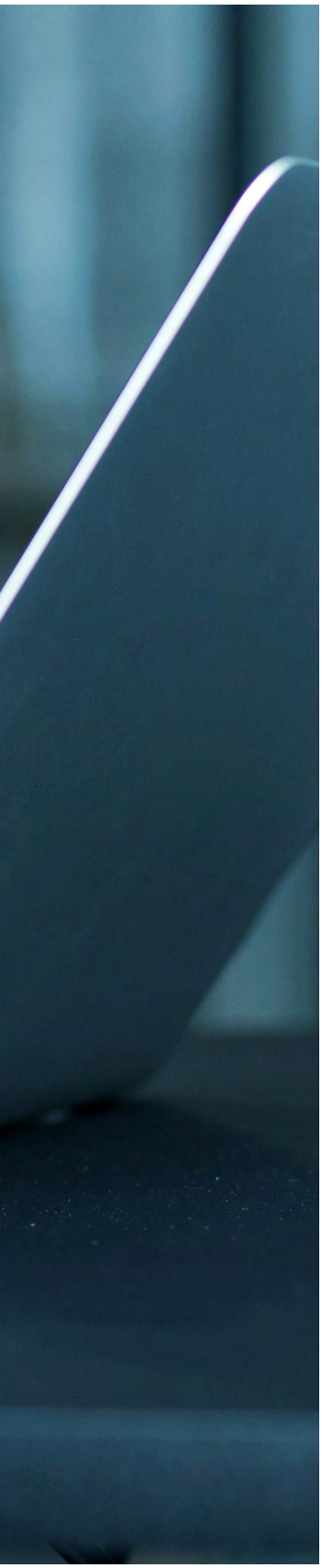
安全牛 AQNIU.COM

“网络+安全”整网安全解决方案
应用白皮书

前言

在一般定义中，网络设备被定义为连接到网络中的物理实体，对其性能测试通常也偏重于网络性能。“网络 + 安全”这一理念则是让网络设备将能够承担更多的数据输出职责，这些数据成为网络安全分析的重要补充。

随着网络信息安全与信息化同步规划同步建设的加强，网络设备与安全设备将同步采购部署，这为“网络 + 安全”理念的落地提供了便捷。



目 录 Contents

概述

1.1 背景

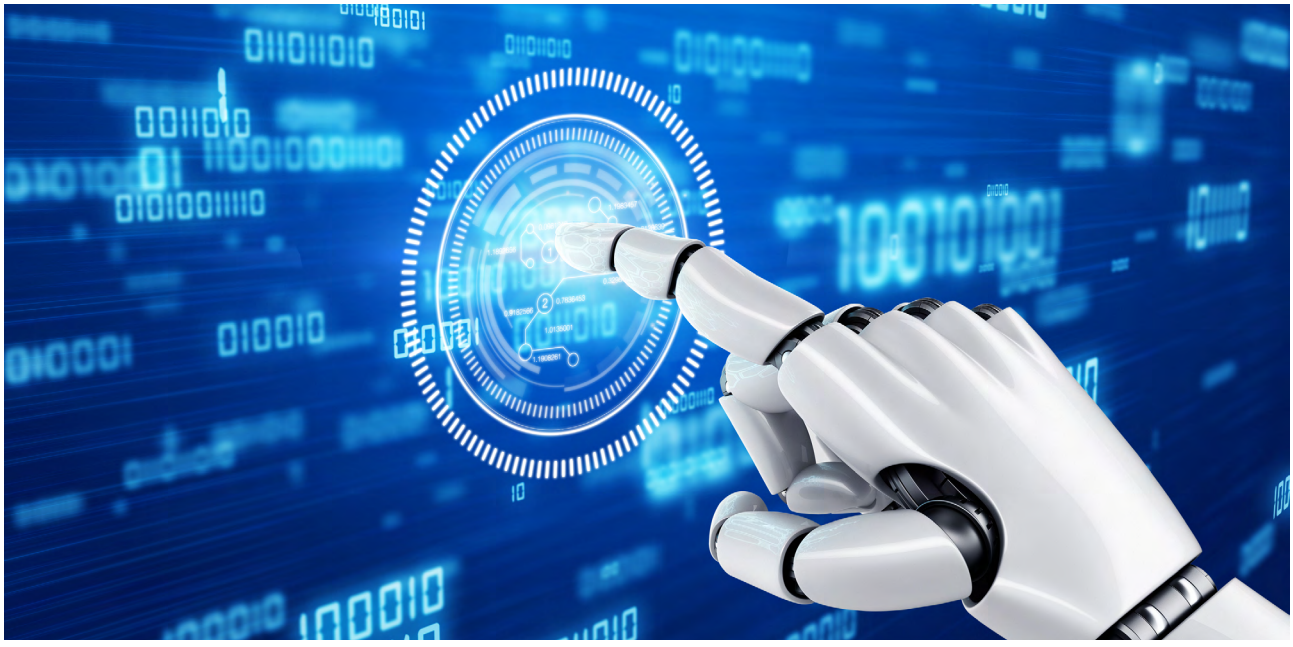
2020 年的新冠病毒疫情的到来给网络安全带来了巨大的影响。一方面，疫情提升了新兴网络接入场景的应用，远程办公、互联网医疗等新兴网络应用场景不断增加，极大加速了数据化转型的脚步。与此同时，传统的互联网业务也在逐步云化，越来越多的业务均以服务的方式提供，这也让网络越来越开放，网络安全的边界越来越模糊。

2020 年，中国网络安全整体态势不容乐观，以信息窃取、内存驻留、DDoS 等相关的恶意样本数量较 2019 年有了大幅度提升。仅 2020 年上半年，我国国内感染计算机恶意程序的主机数量达到了 304 万台，同比增长 25.7%。针对移动智能设备的恶意程序种类大幅提升，其中信息窃取和资费消耗占据主流。

随着人工智能、大数据技术的发展，攻击者的攻击方式也将向智能化发展。攻击门槛的降低就导致网络攻击的频次、网络攻击的种类进一步增加。同时，以 CobaltStrike 为代表的的商业化攻击平台出现，也提升了网络攻击的复杂度。在面对不定时、不定目标的网络攻击时，如何及时处置成为关注的重点。

虽然面临着大量的安全风险，但我国政企机构安全预算却普遍不高。通过对甲方进行访谈了解到，一般的甲方用户其安全预算通常为 100 万上下，主要用于合规建设上。而其中，安全服务和安全建设部分并未进行划分，在实际工作中，用于安全建设部分的预算存在被压缩的情况。

在这一背景下，越来越多的甲方用户考虑将信息安全和网络建设深度融合。优化网络安全投入结构，构建“网络 + 安全”整网安全解决方案、提升网络安全利用效率成为网络安全建设中的首要任务。



1.2 当前网络安全建设现状探究

党的十九大制定了面向新时代的发展蓝图，提出要建设网络强国这一发展要求。随着数字经济的蓬勃发展，网络安全防护的需求也在持续增加，网络安全防护建设永远是数字化转型的重要支撑。当前网络安全建设也存在一定的挑战。

1.2.1 网络建设与安全风险并存

网络信息化建设与安全风险并存，随着网络规模的不断扩大，或将引入网络内生安全问题、接入安全问题等不同维度的风险。

首先，信息系统软硬件的漏洞是不可避免的。漏洞存在于软件系统、硬件设备等任何地方，无论是已知漏洞还是未知 0day，都随时可能成为攻击者利用的手段。这些漏洞往往难以预知和处理。

其次，内部威胁与外部风险并存。在网络安全建设时，我们往往把目光放在来自外部的攻击行为，而忽略了大部分网络威胁是来自于系统内部的。往往外部威胁进入体系内部只需要感染某一个点，进入到系统内部，迅速转化为系统内部威胁，横向移动攻击就可以快速大面积感染整个系统。

最后，人为因素的不可靠性是系统最大的风险。我们在关注系统安全可靠性时，往往会忽略人员脆弱性也会带来安全风险。总体来看，人员脆弱性的被动因素包括安全意识的薄弱、管理体系的不完备、事后追责难以定位到人等造成的脆弱性风险。人员脆弱性的主动因素包括被策反、恶意破坏等行为。特别是特权人员，例如系统管理员、运维人员带来的安全风险尤甚。

因此，网络安全建设必须要与网络建设同步进行，必须依靠联动的防护手段进行风险阻断。

1.2.2 网络设备与安全设备联动能力构建

数字时代背景下，网络设备的种类和数量都有了爆发式增长。探究网络产品的安全属性，将网络产品与安全产品深度融合将为用户构建全方位的网络安全体系提供有力帮助。

首先，网络产品安全属性的有效利用能够提升网络安全的部署效率。与安全产品相比，网络设备的平铺速率更快。在对甲方用户调研时，我们了解到，往往网络建设与安全建设是不同步的，采用以安全设备追随网络业务的方式构建网络安全体系，对新的网络业务规划时，安全规划往往是落后于网络规划的，这一时间差可能存在一定的安全风险。利用网络设备中的网络流量数据，和网络设备中的安全属性正好可以用来降低这种异步建设时差带来的安全风险。

其次，挖掘网络产品中的安全能力和数据价值，能够节约安全建设成本。网络产品的部分功能能够为安全产品提供基础的数据采集、溯源定位和风险处置的能力，通过硬件功能复用、合理利用这些能力能够减少网络安全建设费用。例如，利用交换机中的采样流量数据进行安全分析可以减少部分节点对探针的需求。

最后，利用网络产品与安全产品联动，能够实现对网络各个层级和边界的应急处置。当前的安全产品通常部署在数据中心和出口区域，所以处置点基本也处于该区域，对内部的处置响应比较有限，特别在传统三层网络架构下，很多病毒在汇聚交换机以下扩散传播，安全设备难以进行有效的处置。通过网络产品与安全产品联动，能够实现在网络各个层级对于突发应急处置。

网络安全建设是信息化建设的重要组成部分，是网络业务大范围普及的重要保障，网络和安全也是不可分割的整体，网络设备与安全设备的充分联动，将提升网络安全建设的效率和效益。

在实际网络建设当中，网络安全厂商通常也会考虑网络架构和网络设备的实际情况，提供具有针对某一方面的解决方案如防网络攻击、数据库加密、客户端管理等，但缺乏整体解决方案。在对甲方用户调研后了解到，当前甲方最需要的产品为网络设备、业务系统、安全能力融合的全方位、多层面、一体化的立体解决方案。

1.2.3 网络安全合规建设思考

在对甲方访谈中我们了解到，合规建设开销依旧是当前进行网络安全建设预算的主要组成部分，这从侧面反映出，网络合规建设依旧是重要的驱动。《中华人民共和国网络安全法》中明确写到我国“国家实行网络安全等级保护制度。”《网络安全等级保护》制度提供了一套易于推广的安全基线，也是企业网络安全建设的工程指引。

根据等保 2.0 的要求，需要加强计算机信息系统业务建设和安全建设同步进行。这就要求同步规划，但安全合规只是对系统网络安全性的基本要求。做好网络安全防护，需要以合规为基础，在做好等保合规测评后，还需进一步进行设备使用、维护和升级，提升网络安全防护能力。

根据访谈，当前主流的安全合规解决思路是以采购服务的方式，打包完成咨询及建设。这就要求在做厂商选型时，需要考虑其安全产品线的完备性、与网络设备的兼容性，以及运维的易用性。

“网络 + 安全”应用实现

一套基于网络与安全融合的整网建设方案，能够充分调动网络设备与安全设备的功能，提高网络防御能力，并且提高预算的利用效率。

2.1“网络 + 安全”理念及价值

" 网络 + 安全”理念是指充分利用网络设备的安全特性和数据价值，实现网络设备、安全设备和安全平台联动，告别安全孤岛，构建整网联动的安全保障体系，实现检测、分析、响应、防护的自动化安全处置全流程闭环。

“网络 + 安全”理念的本质是通过网络设备和安全设备的合力，更加高效的达到用户的安全需求，即让网络更安全。作为系统管理人员，将网络设备与安全设备联动，对系统的安全性和可用性做统筹管理，在简化工作内容的同时，提升处置能力。

“网络 + 安全”理念的关键是网络设备成为安全体系的一个环节，为安全分析和处置等运维工作提供支撑。这一理念在建设和运营两方面均有价值。首先，安全建设和网络建设不再是割裂开的两个工作，在做规划建设时，充分考虑到网络产品的安全作用，成为策略执行、数据采集的一部分。其次，通过让网络设备承担更多的安全设备责任，从而提升整体信息化和安全的投资效益。最后，相较于传统做法只是让安全设备更多的是在边界发挥作用，转化为将网络设备安全能力发挥，可以实现对整网各个环节网络状态的直接控制。

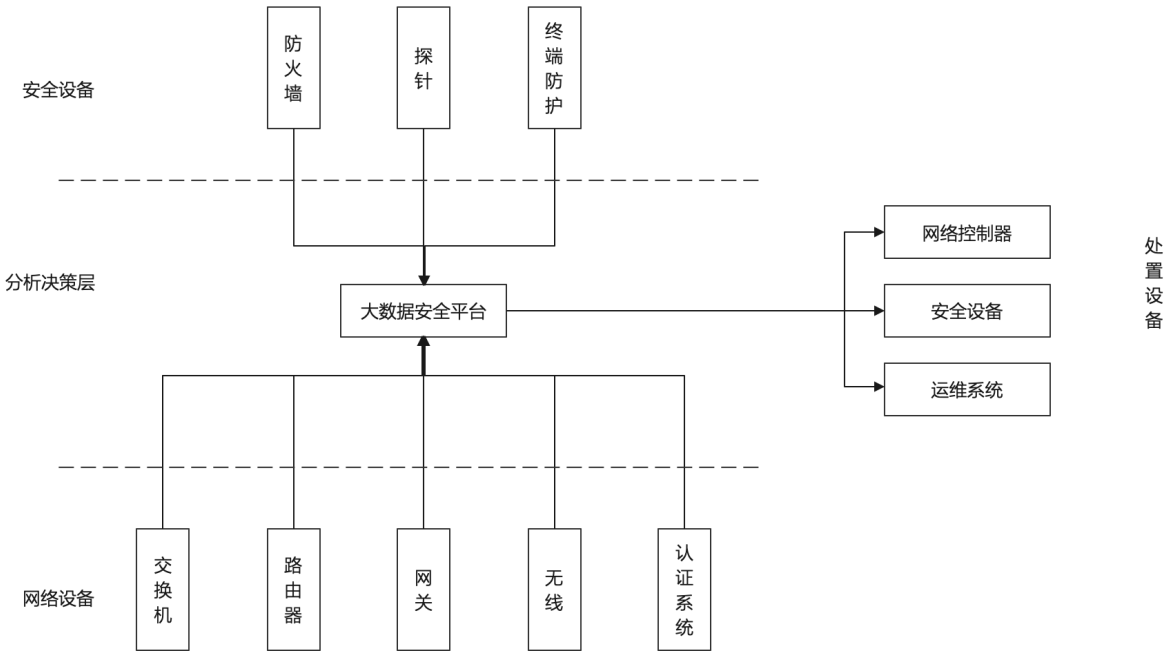
由于“网络 + 安全”这一架构需要对网络设备的充分理解和纳管，因此目前具备这种理念实现能力的厂商多以网络通讯设备起家的网络和安全综合厂商为主。通过市场调研，这些设备厂商均有相关的理念和实践，在其为用户提供解决方案时，如自身的安全产品与网络产品联动，对数据汇聚、指令控制等均能实现更佳的联动效果，能发挥更大的价值。

2.2“网络 + 安全”技术架构剖析

构建“网络 + 安全”体系的关键在于网络设备、安全设备的联动体系，实现网络与安全设备数据采集、态势分析和应急处置的一体化防护。

“网络 + 安全”的核心为数据汇聚分析系统，即将网络设备的数据和安全设备的数据进行统分析处置。通过这样一个大数据安全平台，对散落在网络各个节点的数据进行采集处理，通过内部分析引擎综合研判，并形成最终的处置决策。以大数据安全平台向下层联动网络设备、安全设备，向上联动处置设备。

在具体落地层面上，“网络 + 安全”本质是充分调用网络设备的数据采集能力、网络控制能力，从而弥补安全产品在这些方面的局限性。作为核心的大数据安全平台承担着汇聚数据和综合分析的角色。通过“网络 + 安全”，大数据安全平台所需要的数据不再局限于网络层面的信息，而是能具体定位到每个终端；同时，大数据安全平台的决策也不再成为辅助工具，该决策能够直接用于事件处置。



2.2.1 网络数据汇聚与采集

在数据采集与汇聚上，“网络 + 安全”理念是充分调动网络设备的采集能力，并在大数据安全平台进行数据汇聚。在具体落地上，依托交换机、路由器的数据采集、存储能力，获取全网的流量、日志数据。

2.2.1.1 交换机数据采集

在交换机的使用上，交换机可以承担部分网络探针数据采集的工作，为大数据安全平台提供流量数据，旨在在低开销的情况下快速发现网络内部的攻击行为。由于交换机分布在网络的各个节点，具备天然的全网数据采集优势，近几年业界的交换机大多支持 sFlow 等流量采样标准协议，大数据安全平台和接入交换机联动，可以对东西向威胁扩散进行整网覆盖检测，在大数据安全平台的分析能力加持下，让每一台接入层交换机复用为“安全微探针”，保障内网横向安全检测的有效落地。

交换机大都依靠硬件来进行报文转发，其采样需要的 CPU 能力日常的开销通常不足 10%，因此可以让接入交换机承担更多如 sFlow 等数据采样的工作辅助安全分析。交换联动需要启动接入交换机的 sFlow 功能，并将采集到的数据传输到大数据安全平台当中，以支撑大数据安全平台的分析。虽然在交换机上开启 sFlow 只能做到按比例采样数据，但是由于一般病毒横向扩散所产生的数据量都较大，实际测试可以发现绝大部分的横向移动攻击行为。

将接入交换机作为探针的优点包括：

· 东西向安全监控更全面：一般企业仅将探针以旁路部署在核心交换机，这就忽视了内网的数据流动，一旦内网一台机器被入侵，无法快速探知横向移动攻击。

· 降低开销：不需要额外部署探针或终端安全产品，即可获取网络中的流量数据，减少探针和终端安全产品部署的预算成本和管理成本。

将接入交换机作为探针的缺点包括：

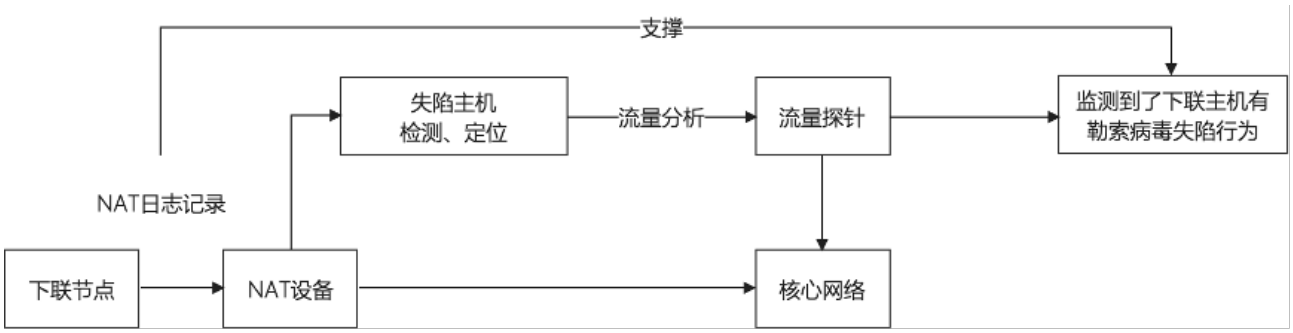
· sFlow 功能造成交换机额外开销。

· sFlow 采用抽样的流量采集方式，且缺失应用层数据，对于横向扩散相关威胁有效，配合威胁情报也有部分南北向安全检测能力，虽检测覆盖范围天然比探针强，但检测的深度和检出率会与探针会有差距。

因此，以交换机作为探针建议部署在接入或汇聚交换机，核心交换机还需以探针旁路部署的方式进行流量采集。同时，交换机产生的数据只能起到威胁发现，因缺失应用层数据无法做到对安全事件的深度研判。因此要做到威胁的全面分析，还需要结合核心交换机旁路的全流量探针，共同支撑系统的安全事件分析。

2.2.1.2 路由器数据采集

路由器可以为安全分析设备提供 NAT 数据，用于实现精准定位。传统网络溯源只能确定到网络出口，通过查找路由 NAT 数据，能够在如纵向网、多级 NAT 等场景下做到安全问题的精准溯源。大数据安全平台联动路由，根据路由器 NAT 数据进行纵向网安全溯源，准确定位源失陷主机。



这一场景特别适用于具备上下级关系总分网络架构。路由器具备 NAT 地址转化数据，当监管层大数据安全平台系统发现有恶意行为时，能够协助定位到 NAT 前哪台终端发生了恶意行为，实现纵向网络安全溯源，解决了溯源中的“最后一公里”定位。

2.2.1.3 网关数据采集

此处网关特指网络出口设备，对具体设备类型不需要进行限制，但是需要能够提供 URL 访问日志、NAT 日志、行为日志等。利用出口网关自身的 NAT、URL 日志，以及上网行为、Mail、IM 等应用日志，配合大数据安全平台的威胁情报、机器学习等分析引擎，实现出口全流量的安全分析。

· 大数据安全平台威胁情报引擎与网关 NAT、URL 日志关联分析，准确定位主机失陷。

· 大数据安全平台机器学习分析引擎与网关邮件日志关联分析，通过经验曲线与实时曲线的对比分析来识别邮箱失陷。

· 大数据安全平台违规访问引擎与网关 NAT、URL 和上网行为日志关联分析，定位是否有高危端口被访问、异常行为等。

2.2.1.4 认证数据采集

仅以网络中的IP、MAC等网络数据无法提供追踪到人的信息。网络当中的认证系统，不仅能够实现准入控制，也能够协助网络数据定位到人。

认证系统中大都会记录用户的上下线信息，包含为 IP、用户名、时间等基本字段，将这些数据实时同步给大数据安全平台，并通过定时发送总在线用户表进行复核效验，形成实时用户与 IP 映射表，通过该表与大数据安全平台中的安全设备、网络设备数据联动匹配，形成实名制的安全事件溯源。

2.2.2 网络管理与处置

在网络管理与处置上，大数据安全平台可以直接下发处置策略到具备管理或处置能力的设备或系统上，从而提高应急响应速率和管理效率。

2.2.2.1 网络控制设备

大数据安全平台联动网络控制设备，根据产生的决策，自动向控制端下发处置策略。在实际运作中，需要设置自动操控基线，或采用自动和半自动相结合的方式应对不同使用场景。

对于以 SDN 为架构的网络，通过大数据安全平台产品向 SDN 控制器发送控制指令，阻断威胁的横向扩散，实现对应急事件的快速处置。

2.2.2.2 运维体系联动

大数据安全平台与 IT 运维监控系统关联，实现安全运维与网络运维的一体化。将大数据安全平台与 IT 运维平台“合二为一”，不管是安全问题，还是运维问题，只需通过一个平台就可快速定位故障并及时排除，实现安全数据和运维数据的统一展示和管理，大大提升管理工作效率。

业务出现异常的原因有很多，可能是服务器、网络设备等硬件异常导致，也有可能是安全问题引起的，传统的做法是在多套管理平台上一一查证，效率较低。当前的大数据安全平台产品数据源通常包含网络流量数据、主机安全产品数据和威胁情报数据。而运维系统能够深入到服务器内部，调取服务器的运行数据，形成综合的研判和故障溯源。

2.3 应用场景及特点

2.3.1 高校应用场景

高校的业务特点是网络人员流动性大，无法进行集中管控，因此高校的信息部门对于接入设备是否安全，设备之间是否会出现横向移动攻击存在担忧。

高校场景特点包括：

- 接入终端多，且不可控；
- 接入方式多，且难管理；
- 网络拓扑环境复杂，安全投入成本高；

· 注重事件到人员的追溯。

“网络 + 安全”方案的优势在于：

· 与认证联动，实现到人员的追溯；
· 利用交换机采样数据高效率实现校内病毒扩散问题监控；
· 自动化安全事件处置，网络与安全的统一运维管理。

“网络 + 安全”方案采用对接入交换机的监控，在不接入终端设备的前提下，发现网络当中的安全问题，解决了需要统一纳管终端才能发现安全风险的问题。虽然可以在每个接入交换机旁路部署探针系统，但这种部署方式将极大提高安全费用，一般高校甲方很难接受如此高的成本代价。

通过对甲方高校调研访谈了解到，高校信息部门较为注重安全事件到对于具体人员的追溯，而这对于学校是比较难的。高校信息部门认为学生终端多为不可控，无法强制要求终端设备部署数据采集体系或终端防护软件。在这一场景下，与认证系统的联动将提升对人员网络安全行为的控制。高校学生网大部分为 DHCP 动态 IP 地址环境，且一般具备认证系统，通过认证系统与大数据安全平台分析引擎的联动，可有效地解决虚假失陷、安全问题难以定责到人等问题。

2.3.2 医疗应用场景

医疗系统大都为传统的内外网物理隔离架构，但随着疫情影响，远程问诊、预约挂号等对外业务不断增加，内外网之间的界限也越来越模糊，安全风险大幅提升。医疗业务系统越来越复杂，接入人员多、需求复杂，医疗行业通常多科室、多业务，数据安全性要求较高。特别是孤立、单点的信息安全产品已不足以解决。

医疗场景的特点：

· 接入终端不可控；

· 以物理隔离为主要防护手段；

· 内网数据安全需求较高。

“网络 + 安全”方案的优势在于：

· 利用交换机数据实现东西向病毒扩散的监控，将安全事件带来的损失降到最低；

· 提升防护预算的使用效率。

“网络 + 安全”方案能够进行人员认证，人员身份与人员行为联动，对业务访问客体行为进行分析，从而实现有效监管。

医疗场景在网络安全上的需求源于信息化带来的业务安全需求和合规安全需求。“互联网 + 医疗”、“医疗大数据”的建立离不开对网络安全的依赖。与业务扩大对应的是，我国医院的网络安全防护水平还存在一定的不足，堡垒机、漏扫产品等网络安全设备采用率甚至小于 50%。这就要求一方面持续网络安全投入，另一方面是充分调动网络设备的能力。

医疗场景下，将大数据安全平台和身份认证网关做对接，可以在发现恶意行为时，及时定位到具体人员，实现有效的追踪溯源。

2.3.3 政府应用场景

政府应用场景在实际应用中可以分为两种，一种是作为上级主管机构，需要对下属子系统进行全方位的纳管、监管；另一种是作为基层政府机构，需要在上级指引下完成自身的网络安全建设。“网络 + 安全”的高性价比和定位到人员的溯源能力，能够满足这两种政府应用场景的不同需求。

政府场景的特点：

· 从上到下进行监管；
· 对安全需求较高；
· 内外网隔离基础较好。

“网络 + 安全”方案的优势在于：

· 实现上层对下层的到 IP 定位；
· 提升防护预算的使用效率。

对于监管型网络政府机构，通过大数据安全平台和路由联动，能实现监管的细化。上级主管机构所部属的全局型大数据安全平台产品，能够对子机构进行整体监管。特别是通过 NAT 日志的溯源，让这种监管定位到子系统中的最终用户。

基层政府机构在网络安全上的预算讲究效费比，其预算一般优先。“网络 + 安全”的方案，充分利用网络设备的能力，能够提升网络产品的利用效率，在满足等保合规的前提下，进一步提升网络安全防护能力。

整体上，政府行业数据敏感度高、安全要求严格，特别在安全问题处置时效上要求高时效将安全问题损失降低到最低，安全即是时间仗，没有 100% 的安全，在病毒扩散前检测和预警，将大幅度降低损失，通过 sFlow 交换机联动检测全网扩散行为，并联动 SDN 进行安全问题半自动或自动化处理价值较大。

2.3.4 常规化运维应用场景

“网络 + 安全”理念能够同时提供网络运维服务和安全服务，解决泛安全问题。

一般运维场景的需求：

· 能够快速定位失陷主机；
· 能够提供失陷主机失陷原因。

“网络 + 安全”方案的优势在于：

· 能够获取安全事件导致的主机失陷信息；
· 能够结合运维信息与安全信息，形成对事件原因定位和影响的综合研判。

在对甲方用户调研后，对于中小型机构，其信息化部门和安全部门通常为同一拨人，信息化人员即作为安全人员，安全运维融为一体。

大数据安全平台与运维系统关联，可以从系统运行层面对主机运行状态进行监控，对于挖矿病毒、DDoS 能够实现主机层面的预警发现和应急处置。

2.4 系统建设及难点

“网络 + 安全”的建设以充分利用现有网络设备的功能和数据为理念，通过以大数据安全平台产品为中心，联动网络产品的日志、数据进行联动性分析。在建设时，需要对自己的需求进行梳理，对自己的网络架构进行梳理，明确自身的网路产品可以实现的性能指标，提供针对大数据安全平台的支撑行为。

在实际建设时，还需以大数据安全平台为核心，围绕大数据安全平台对网络产品和安全产品进行配置。针对网络设备，需要将其采集的数据传送至大数据安全平台，并进行分析。需要配置控制设备，在何种情况下接受大数据安全平台的控制等。

在“网络 + 安全”联动建设中，有如下难点：

1、不同厂商产品联动：不同厂商产品日志、数据会存在一定的不同，在对这些产品联动时，可能存在兼容性问题。

2、产品性能：由于系统需要联动，对产品的实时吞吐有要求。另一方面，由于大数据安全平台产品需要直接下达处置指令，需要提升大数据安全平台的准确性和可靠性。

3、安全设备与网络设备的联动：大部分安全设备与网络设备是由不同类型的厂商研发的，在研发当中对联动性考虑不足，因此需要较多的联调适配。

锐捷“网络 + 安全”整网安全解决方案

基于在实践中遇到的建设难点，锐捷推出“网络 + 安全”整网安全解决方案。锐捷“网络 + 安全”整网安全解决方案是一套成熟、可落地的解决方案。该方案具备网络和安全综合厂商的特点，能够满足用户在网络技术层面的安全管理和维护需求。

3.1 方案特色

锐捷“网络 + 安全”整网安全解决方案依托于其在网络层面的设备布局，充分利用了锐捷网络设备的技术优势和覆盖优势，让交换、路由、网关、无线等网络设备都作为大数据安全平台的安全微探针，同时发挥 SDN 智能协防、网络准入实名日志、网络安全一体化运维的优势，实现整网设备联动，充分满足了用户对等保 2.0、网络安全法的合规需求，让网络更安全。

锐捷“网络 + 安全”整网安全解决方案的核心为安全大数据安全平台。系统集流量分析和日志分析技术于一体，由网络设备提供日志和采样流量数据，由安全产品提供流量分析和安全数据。锐捷大数据安全平台将“日志维度 + 流量维度”有效融合，同时结合威胁情报、智能分析等构建全网安全检测和防护体系。此模式可以很好地发挥日志分析全面性、异构性、合规性优势，同时配合流量分析维度，解决威胁深度分析、回溯支持、快速部署等问题。

锐捷“网络 + 安全”整网安全解决方案特色包括：

· 大数据安全平台与交换机联动：通过开启换交换机 sFlow 协议采样汇聚层和接入层流量发送日志给大数据安全平台 RG-BDS，有效发现网络内部横向移动攻击。

· 大数据安全平台与统一上网行为管理与审计系统 RG-UAC 或新一代高性能综合网关 RG-EG 系列联动：将风险分析下沉到人员，实现对在业务层面的数据外泄等安全分析，有效发现浏览不良网站、回连黑域名的情况。

· 大数据安全平台与 IT 业务综合管理平台 RIIL 联动：通过二者联动，形成业务与安全统一运维平台，一个平台不仅能发现安全问题，也能发现业务运行问题，从泛安全的角度解决威胁发现问题。

· 大数据安全平台与 SDN 控制器联动：通过大数据安全平台与 SDN 控制器联动，发现问题智能阻断，及时下发安全策略、打赢安全时间战。

3.2 方案优势

锐捷“网络 + 安全”整网安全解决方案在日常建设中有如下优势：

· 成本优势：锐捷“网络 + 安全”整网安全解决方案将部分安全建设功能融入到网络建设当中，有效整合网络设备，减少预算开销。

· 处置优势：锐捷“网络 + 安全”整网安全解决方案融合了安全处置能力，让网络安全不再是孤立的研判行为，或只能跟安全设备一起联动处置，而是与 SDN、运维系统联动，一旦发生危险及时处置。

· 智能运维：将大数据安全平台的分析能力赋予运维系统之上，提升自动化运维效率。同时运维系统提供更多的数据，提升大数据安全平台的分析能力和准确性。

· 易于落地：锐捷“网络 + 安全”整网安全解决方案可以以模块化方式交付，以大数据安全平台与交换机联动为例，用户仅需开启交换机的 sFlow 协议并将数据配置到大数据安全平台即可，该联动支持任何品牌交换机，无需额外采购设备。

3.3 用户评价

在了解锐捷“网络 + 安全”整网安全解决方案后，安全牛将该方案介绍给不同类型的甲方用户，邀请其根据自身的业务特点对该方案进行客观评价。在整理甲方的评价疑问后，安全牛将其向锐捷进行了反馈，锐捷就相关问题进行了解答。

3.3.1 某医药用品集采平台甲方评价

某医药用品集采平台用户的主要业务是为医疗设备供应商和医院之间提供对接服务，并能够进行物流追踪。该公司的业务专业性较高，接入平台进行浏览、采购的均需进行实名认证。其业务系统并未完全暴露在公网，通过采用云 waf 的方式，只允许访问部分业务，有较严格的权限校验。系统部署有防火墙、大数据安全平台、云 waf、堡垒机、终端安全产品。

在了解锐捷“网络 + 安全”整网安全解决方案后，该用户认为该方案对于传统 IDC 有部署必要，由于该用户目前只在核心交换机部署探针，对于绕过防火墙的造成终端感染的病毒，无法发现其在网络内部的行为。由于该用户安全预算每年不足百万，无法在每个交换节点部署探针产品。这种方案对其关注的横向移动攻击有一定的解决能力。

在具体部署上，如果落实锐捷“网络 + 安全”整网安全解决方案，在以下方面有所担心：

· 目前接入交换机本身配置不高，性能压力比较大，在应用中不会开启 sFlow 功能。如果部署该方案，是否会对网络使用上影响。

· 大数据安全平台本身的误报率比较高，依靠大数据安全平台自动发现风险，一方面可能存在发现不了的情况，另一方面自动处置可能影响正常业务运转。

对此，锐捷给出反馈：

· 常规情况交换机的 CPU 利用率一般都很低在 30% 以下，经过测试 sFlow 实际使用对 CPU 的影响只有 1%-5%，所以对于交换机的性能影响可以忽略不计。

· 采用大数据安全平台 +SDN 方式部署，用户可选择半自动化阻断，如针对分析后的问题人工研判后点击一键处置，也可以设置发现问题后自动化处置。自动化处置也可以设置仅对高风险、威胁扩散的端口进行精细化阻断。

3.3.2 某高校甲方评价

某高校是一所管理人员、教员、学生均较多的综合性大学。该校的教学业务网和学生宿舍区网络分开，有独立网络系统，总体接入终端超过 10 万，其中有线网络节点超过 7 万。该学校有自己的数据中心用于教务、计费等工作。对学生资产是否安装终端安全产品不作要求，只形成建议。该校网络安全预算较为充足，网络安全产品均有多套同时部署。该校计划弱化信息安全的独立性，将安全回归到正常业务中，形成整体的智能运维体系。

在了解锐捷“网络 + 安全”整网安全解决方案后，该用户认为该方案对大多数企业有较强的应用价值，能够在合理的预算前提下，实现对东西向流量的采集。

在具体部署上，如果落实锐捷“网络 + 安全”整网安全解决方案，在以下方面有所担心：

· sFlow 协议采用的流量取样，而一些病毒爆发时流量并不高，有可能通过取样的分析无法发现恶意行为。

对此，锐捷给出反馈：

· 通过实网数据分析发现，病毒爆发时南北向回连数据相对较少，但大部分横向移动扩散的行为均具有高频数据的特性，根据对多种恶意行为的实验分析，流量抽样采集已基本能够识别大部分的横向移动攻击。

3.3.3 某政府机构甲方评价

某政府机构是一个财政机构，连接财政机构、银行等业务需求。其业务系统纵向连接县 - 市 - 省 - 中央，横向连接银行的省级汇聚信息接入。该机构的网络结构有：互联网、政务外网以及涉密网。其中涉密网有专网进行传输，内外网之间以网闸进行隔离。该机构不同系统有不同的等保测评需求，根据情况多为二级和三级。该机构的网络安全预算一般，多通过采购服务的方式完成等保测评。随着“政务云”建设需求的增加，越来越多的政务需求要向云转移，这就对了政务云本身的可靠性、稳定性形成了一定的考验。

在了解锐捷“网络 + 安全”整网安全解决方案后，该甲方认为解决方案是一个低成本实现网络安全的方案。对于大数据安全平台来说，数据是一项重要的支撑，因此通过提供更多的交换机数据，能够进行分析。

在具体部署上，如果落实锐捷“网络 + 安全”整网安全解决方案，在以下方面有问题：

· 很多企业并没有采用 SDN 的网络架构，即便采取了假如没有用锐捷的产品，锐捷“网络 + 安全”整网安全解决方案如何落地。

· 在设计网络架构时并没有使用锐捷的交换机，这个体系适配性有待验证。

对此，锐捷给出反馈：

· 从分析层面交换机 sFlow 数据、路由器、运维系统等联动不受厂商和 SDN 技术限制，所以大部分分析层面的”网络 + 安全”特性均可以使用，只是在处置阶段如果没有采用 SDN 网络架构可以使用其他联动处置方案，如大数据安全平台直接与交换机 / 认证系统 / 探针等联动处置。

· 以交换机作为探针，仅需要交换机支持标准的 sFlow 功能即可，并不需要完全采用锐捷的交换机。这一功能绝大部分交换机已经具备。

3.3.4 某高校甲方评价

某高校是一所具有四五万名师生的综合性大学，每年网络安全服务预算在 50 万元左右。目前学校部署了行为审计产品、堡垒机、APT 分析产品、防火墙产品、大数据安全平台等网络安全产品。目前该甲方用户最关注的安全行为之一是学生终端行为不可控，以及由于私搭 Wi-Fi 等行为，造成 IP 地址与人员无法对应，无法进行行为审计。

在了解锐捷“网络 + 安全”整网安全解决方案后，该甲方用户对大数据安全平台与路由联动非常感兴趣。通过大数据安全平台和路由器联动，可以对发现的恶意域名直接阻断。同时，甲方用户也提出了自己的问题。

· 大数据安全平台联动运维系统，对运维系统要求较高。如果运维系统能监管到每台交换机，能够实现智能运维。但这对运维系统要求较高，实际上很难控制到交换机。

对此，锐捷给出反馈：

· 统一监控层面，大数据安全平台与运维系统的联动主要是将分析后的告警信息同步给运维系统统一监控，这部分为标准数据对接相对难度不大。分析层面大数据安全平台是直接与交换机联动进行数据采集与分析，处置层面大数据安全平台主要联动 SDN 控制来实现处置下发，与运维系统关联度不大。

3.3.5 安全牛评

锐捷“网络 + 安全”整网安全解决方案具有网络和安全综合厂商的特点，是网络产品与安全产品的协同联动，共同构建整网安全体系。这是一套网络安全高投入产出比的解决方案，对于系统初建的机构，能够同时实现网络建设和安全建设，将为以后进一步安全建设打下坚实基础，对于老系统的改造，也能做到对原有网络和安全充分的利用，提升安全投入效益。

当前的网络安全已不仅仅是安全性，随着泛安全理念的普及，安全终究要归于业务当中，安全产品也将是网络产品重要的组成部分。当前甲方用户关注的重点已不再是单一的安全技术，而是从网络到安全再到业务的体系化解决方案。

网络安全建设是否有产出？这个问题的答案只有在实践当中才能验证。如何将安全建设融入到网络建设中，是安全甲方用户在实践中一直在思考的问题，也是安全厂商需要提供的解决方案。锐捷的“网络 + 安全”整网安全解决方案正是提供了这样一个方案，即在建设上，依照等保合规要求构建网络安全体系；在安全检测上，让交换、路由、网关、无线等网络设备都作为安全大数据安全平台的安全探针；在安全处置上，充分发挥 SDN、运维管理系统智能协防优势，实现安全一体化运维。

锐捷“网络 + 安全”整网安全解决方案为接入主机多且难以管理的用户提供了解决思路，是一种重视主机安全的解决方案。当前主流网络安全防护方案更注重边界安全或者边缘安全，而忽视内网的扩散问题。锐捷这一方案能够在预算范围内，针对内网安全提供安全防护。

锐捷“网络 + 安全”整网安全解决方案不仅是一种防护手段，也提供了应急处置，这体现了锐捷在网络端的优势。虽然网络风险的发现、取证、溯源均是重要的防护行为，但是不可忽视的是网络安全风险处置才是第一要务。锐捷的方案能提供 7*24 小时的应急处置，将风险造成的影响降到更低。

锐捷“网络 + 安全”整网安全解决方案还是一种安全投入产出比较高的解决方案，而这也是很多甲方用户在网络安全建设中必须考虑的问题。方案充分利用网络设备的功能和数据，在满足等保合规前提下，能够提升系统的安全性能。

“网络 + 安全”落地实践

4.1 某高校案例

4.1.1 用户背景及需求

某大学是一所领域特色的高校，除特色领域外，还有工学、管理学、经济学、法学、文学、理学和艺术学等 7 个学科门类。该大学共有三个校区，不仅承担着高等教育的职责，还承担着继续教育、中职教育的职责。

该校网络特点是接入交换机数量较多，汇聚交换机相对较少。在网络内部部署有防火墙，可以对服务器区、内网、IDC 机房进行防护。

该大学的诉求是以低成本实现全网动态监测，实现第一时间发现校园网内的恶意行为。学校之前出现过教室内的上课终端被感染病毒并扩散到十几个教室，导致上课终端同时蓝屏无法上课，影响较为恶劣，东西向的威胁扩散很多不经过核心，部署在核心区域的安全设备无法感知，同时由于学生流动性等原因，也无法在每个终端节点部署统一防护软件。在高人员密度、高人员流动、高接入需求的背景下，如何有效对网络的安全状态进行监控，成为该用户的主要需求。

4.1.2 方案设计及实施

该大学部署了“网络 + 安全”整网安全解决方案，将超过 200 台接入交换机作为流量采集点，并通过开启交换机的 sFlow，向大数据安全平台增强版 RG-BDS-A 输入监测数据，通过大数安全平台的分析模型库，全面监控东西向威胁扩散风险。SDN 纳管核心与接入，大数据安全平台 RG-BDS 发现网络上存在安全问题，通过联动 SDN 实现一键 / 自动阻断。

该大学的策略是：在核心交换机旁路部署万兆探针，以流量镜像的方式，在保证不造成额外网络开销的同时，获取网络全流量，提供到 RG-BDS-A 当中，用于南北向和校园网到数据中心的流量安全分析。同时，接入交换机交换机联动实施“网络 + 安全”方案，通过配置 sFlow 的数据输出目的地址，将 sFlow 数据输出到大数据安全平台当中，用于校园网内对横向移动攻击的发现。

1、交换机配置 sFlow，指定地址到大数据安全平台：

```
                                #show run | in sf
                                #show run | in sflow
                                #show run | in sflow
sflow agent address
sflow collector 1 destination
 sflow flow collector 1
 sflow enable
 sflow flow collector 1
 sflow enable
 sflow flow collector 1
 sflow enable
```

2、在大数据安全平台中接收 sFlow 信息，在设备日志中可查看标准化后的 sFlow 日志，并进入横向扩散分析引擎库进行安全分析：

在实际监测中，交换机开启 sFlow 后对其 CPU 利用率影响较小，CPU 利用率仍保持在 20% 以下，对网络正常访问无影响。

下图展示了在实际开启 sFlow 后，交换机 CPU 利用率情况：

```
?-h¥¥ę-S2910#show cpu
==============================================
[Slot 0: S2910-48GT4XS-E]
CPU Using Rate Information
CPU utilization in five seconds:  9.20%
CPU utilization in one minute:  8.80%
CPU utilization in five minutes:  8.70%
```

```
?¥--202-2VSU-201_234-S2910#show cpu
==============================================
[Slot 2/0: S2910-48GT4XS-E, Cpu 0]
CPU Using Rate Information
CPU utilization in five seconds:13.9%
CPU utilization in one minute:13.2%
CPU utilization in five minutes:13.4%

==============================================
[Slot 1/0: S2910-48GT4XS-E]
CPU Using Rate Information
CPU utilization in five seconds: 18.80%
CPU utilization in one minute: 15.90%
CPU utilization in five minutes: 15.80%
```

4.1.3 实施效果及反馈

·目前，“网络 + 安全”体系已经在该大学现网上部署，并发现了真实的网络攻击行为。上线最初的一个月时间内，通过交换机 sFlow 和安全探针的综合分析，共发现 14 个涉及 445 扫描的中毒终端 IP、40 余个矿机终端 IP、100 多个 Ramnit 木马病毒终端 IP，其中包含两台业务服务器，通过联动 SDN 进行一键下线，主机修复杀毒后均已恢复正常状态。

在“网络 + 安全”体系实施后，系统具备发现内网的横向移动攻击的能力，并基于大数据安全平台结合探针东西向流量数据进行安全分析，获取整个安全事件的行为信息、系统影响、证据链信息等。

1、通过 sFlow 发现内网横向流量安全问题

2、通过大数据安全平台分析整体安全事件溯源

3、通过 sFlow 数据溯源被扩散的终端主机

4、定位到失陷地址进行处置并记录

上下文分析 查询条件

触发前 触发后

序号	事件名称	源IP	目的IP	发现时间	目的端口	类别	子类	级别
1	内网可疑445端口扫描	[redacted]	[redacted]	2021-05-14 15:55:00	445	网络攻击	漏洞攻击	高级
2	FLOW日志	[redacted]	[redacted]	2021-05-14 15:54:26	445	连接	连接跟踪	信息
3	FLOW日志	[redacted]	[redacted]	2021-05-14 15:53:15	445	连接	连接跟踪	信息
4	FLOW日志	[redacted]	[redacted]	2021-05-14 15:53:08	445	连接	连接跟踪	信息
5	FLOW日志	[redacted]	[redacted]	2021-05-14 15:52:01	445	连接	连接跟踪	信息

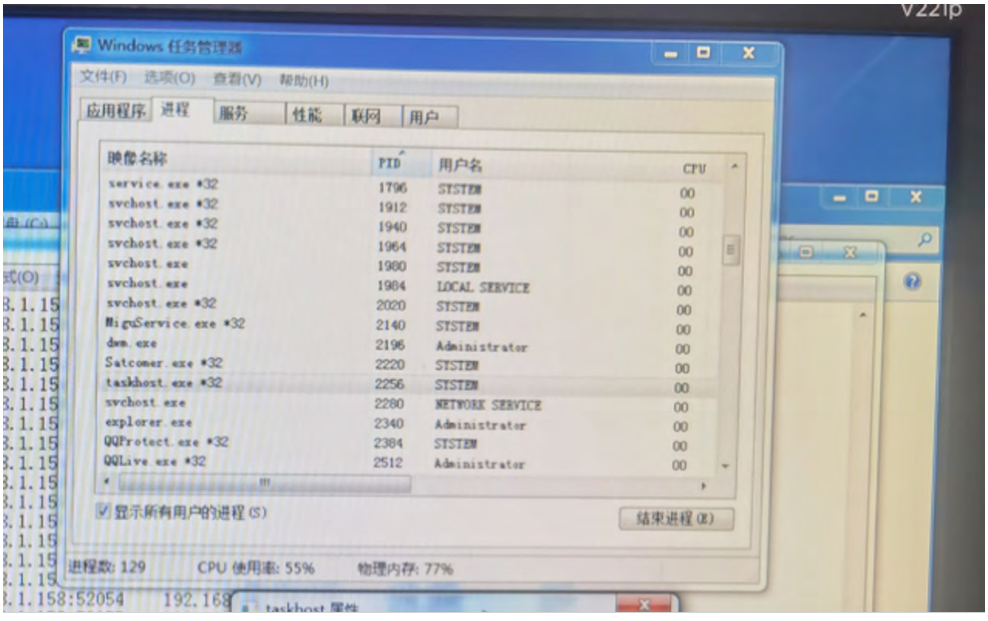
5、失陷主机处置

在发生安全时间时，安全管理人员可以在大数据安全平台上针对失陷主机进行一键下线后，通过资产列表确定该失陷主机在哪栋楼哪个办公室，并到现场进行验证。安全人员到场后，确认该主机已经失陷，表现为该主机使用过程中非常卡顿，并且正在对外不断地横向扩散。

实际监测中具体可能监测的问题有：

1）主机没有安全杀毒软件

2）已经中各种木马、蠕虫病毒，比如永恒之蓝、特洛伊等



用户对方案的实施效果较为认可，通过“网络 + 安全”，特别是交换机的联动已经发现不少病毒东西向扩散的问题，因此用户进一步扩大了实施范围，将在网出口设备、防火墙、内网 IDS 等网络设备和安全设备的日

志接入到大数据安全平台进行综合分析。后续使用期间发现了一次非法入侵行为已渗透入内网。起初用户在防火墙上已经封了某个高频 SSH 爆破攻击自己的黑 IP，相关攻击日志也实时同步到大数据安全平台，平台关联出口设备日志分析发现还是这个黑 IP，跟内部多台服务器有 SSH 链接，说明该 IP 采用了防火墙未识别的攻击方法已经进入内网，只是还没开始产生破坏所以内部无感知，通过关联 NAT 和 FW 日志分析可以发现、并提前告警。类似这种攻击与连接日志隐藏在每小时几十万条出口日志中，单一的看某一条记录无法发现风险。但通过大数据日志分析，能够综合研判出现的问题，并定位这种隐藏的安全问题。

4.2 某医院案例

4.2.1 用户背景及需求

某医院是市卫健委管理的全民事业单位，其建设发展目标是建成集医疗、教学、科研、预防保健为一体的国内一流、省内领先的三级甲等专科医院，并努力提供安全、有效、方便、价廉的医疗卫生服务。

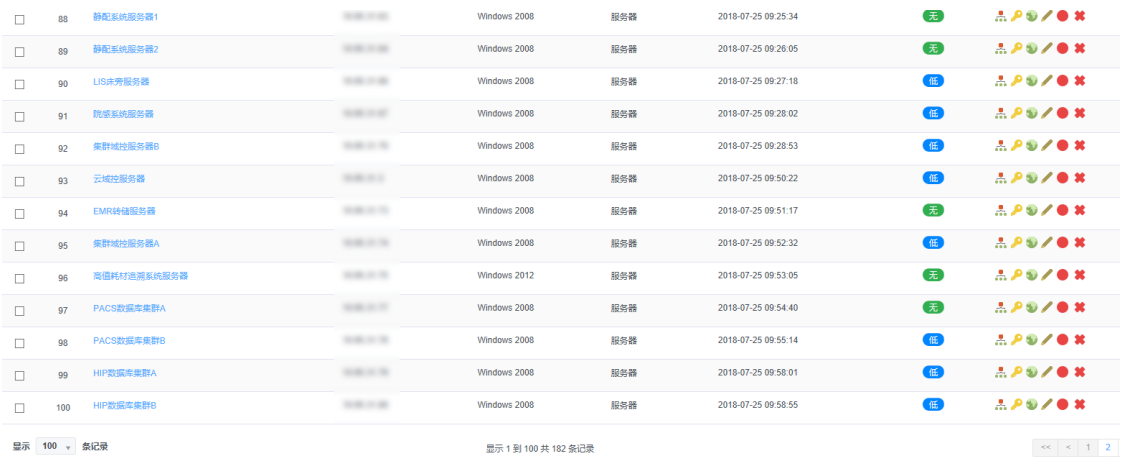
该医院主要由内网、运维网和外网三块组成，所有的安全设备部署情况都是在内网。用户需求可以分为三个阶段。初期需求为医院内网日志留存 180 天和综合安全管理；中期需求为日志和流量分析定位安全问题以及对横向病毒扩散的监控；后期需求为为对网络和安全统一监控，提升运维效率。

4.2.2 方案设计及实施

针对用户需求，锐捷设计了如下方案：

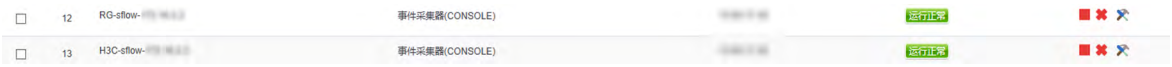
1、医院内网部署大数据安全平台增强版 RG-BDS-A 和流量态势感知 RG-BDS-TSP 系列。针对内网的资产进行日志接入，流量镜像到探针分析后同步给 RG-BDS-A； IT 业务综合管理平台 RG-RIIL 网络和业务健康度监控与 RG-BDS-A 中的安全态势分析与监控结合，形成大数据安全平台加网络运维系统的综合运维。

网络资产日志接入：



日志分析和流量分析结合：

2、将大数据安全平台和交换机联动，将部署的 H3C 接入交换机和锐捷接入交换机的 sFlow 信息导入 RG-BDS-A。

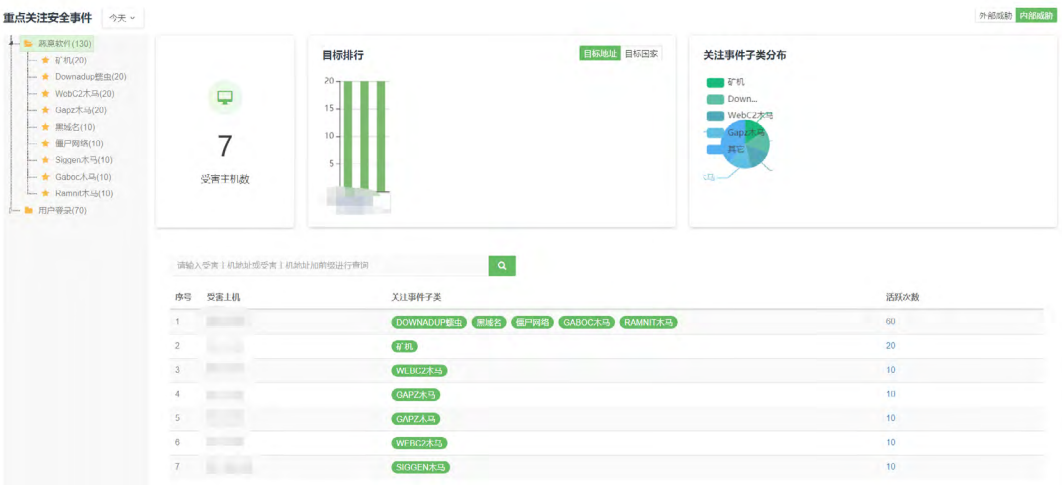


4.2.3 实施效果及反馈

1、全面提升院内日常安全事件运维成绩

该医院采用“日志 + 流量”模式进行分析，利用大数据安全平台增强版 RG-BDS-A 和流量态势感知 RG-BDS-TSP 系列及交换机 sFlow 数据，实现对网络数据的安全分析。日常运维人员也可以通过自定义查询重点关注的安全事件内容。

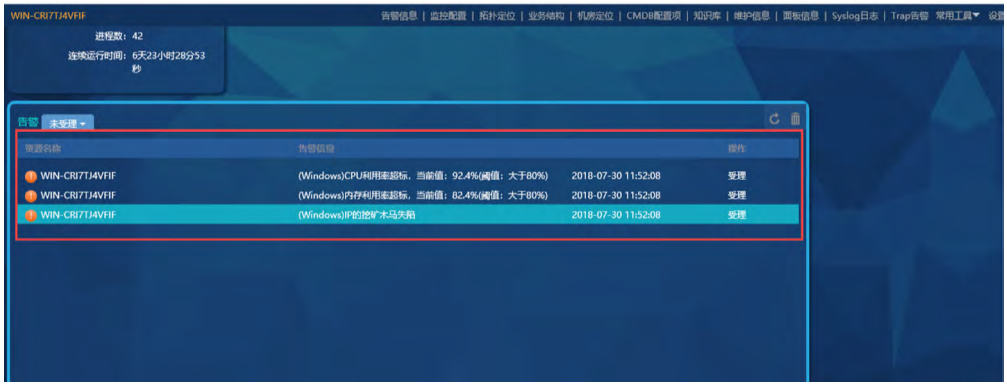
RG-BDS-A 上线之初，每日安全告警达 20-50 个之多，其中一部分由误报和医院内业务软件 SQL 语句不规范导致。经过运维人员和锐捷安服人员对内网失陷主机处置，现平均每日发现安全事件 5-10 起，有效地协助安全人员进行全网安全事件监控，提升了安全运维工作的效率。



2、RG-RIIL 与 RG-BDS-A 结合，通过运维数据和安全数据有效融合互动，在发生安全事件时，可以直接定位故障位置，并发现故障原因。

以发现挖矿主机为例，运维人员在查看统一运维平台时，发现一台主机产生性能告警，进一步查看到告警内容是 CPU 和内存利用率超标。

在拓扑上查看主机，显示该主机的告警有一条挖矿木马失陷的告警，该主机疑似中了挖矿木马。

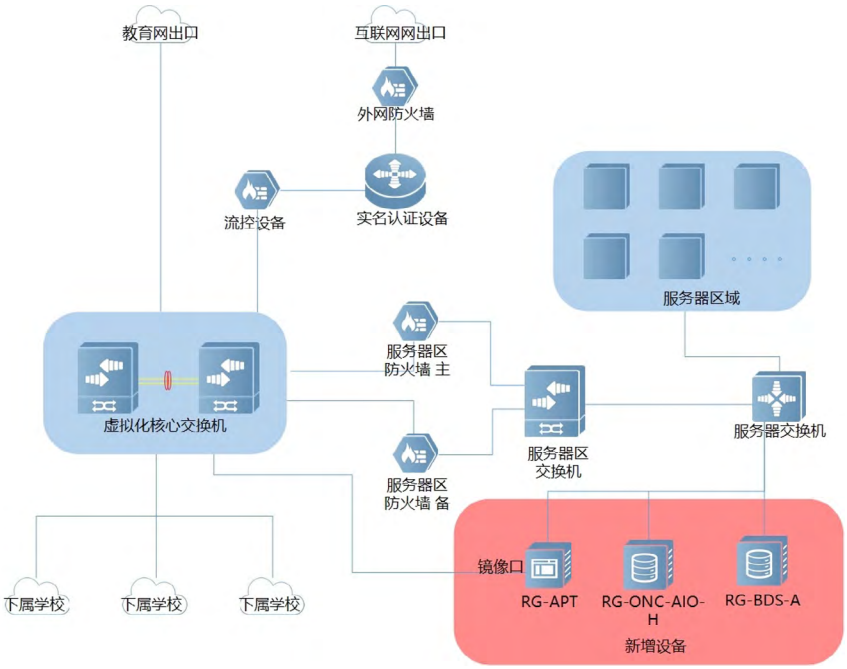


通过 RG-BDS-A 查看该主机黑客的攻击路径和时间轴路径，发现该主机有明显的被木马植入并且有相应的流量和异常行为，进行杀毒处置后服务器状态恢复正常。

4.3 某教育局案例

4.3.1 用户背景及需求

该教育局下属 120 余所学校，需要对学校的安全状况进行监督，并对整体安全状况把控。下属学校的网络设备主要为普通师生上网终端，服务器集中部署在区教育局机房。

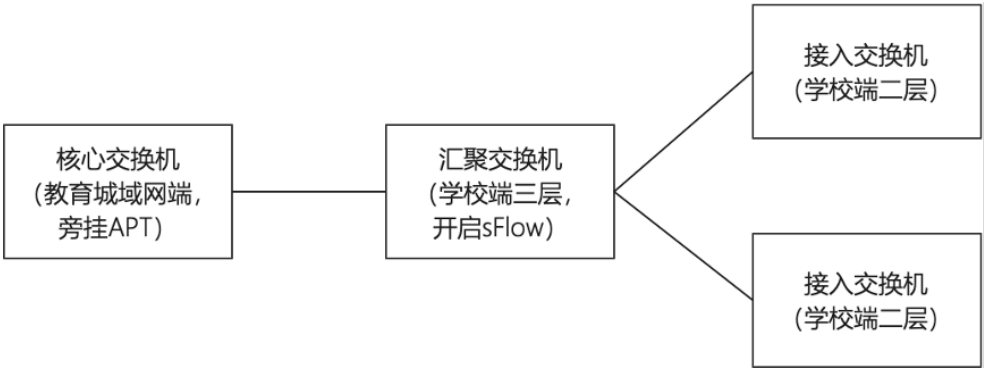


用户的核心诉求为能够及时发现辖区下属学校的安全事件，并且可以实现阻断处理。当前由于各学校防护能力较弱，一旦发生安全事件向上可感染区节点和市中心网络，横向扩散可感染辖区任意学校。目前教育局无法及时发现这种东西向威胁扩散。例如失陷的师生终端，在各个下属学校之间扩散病毒时，由于安全设备存在于教育局边界、核心、服务器区等，无法对学校间和学校内的此类威胁做出反应。另一方面，区教育局无法管控学校端的安全风险，因此无法满足上级单位和监管单位提出的协助完成教育体系整体安全防护要求。

4.3.2 方案设计

针对用户的需求，锐捷设计的方案为：部署高级威胁检测系统 RG-APT 分析核心交换机的镜像流量，用于感知所有下属学校的经过核心交换机的南北向流量，并将管辖范围内的学校上联交换机开启 sFlow 数据采集，用于东西向流量检测。所有数据同步给大数据安全平台。实现学校间的扩散行为发现；并且部署 SDN 控制器，纳入管理所有下属学校的交换机，通过大数据安全平台增强版 RG-BDS-A 与 SDN 控制器联动，下发指令在下属学校交换机层面封堵失陷终端，避免了失陷终端对其他下属学校带来安全威胁。

在数据采集部署上，核心交换机通过高级威胁检测系统 RG-APT 流量文件综合检测、学校端汇聚交换机开启 sFlow 数据采样。



4.3.3 实施效果及反馈

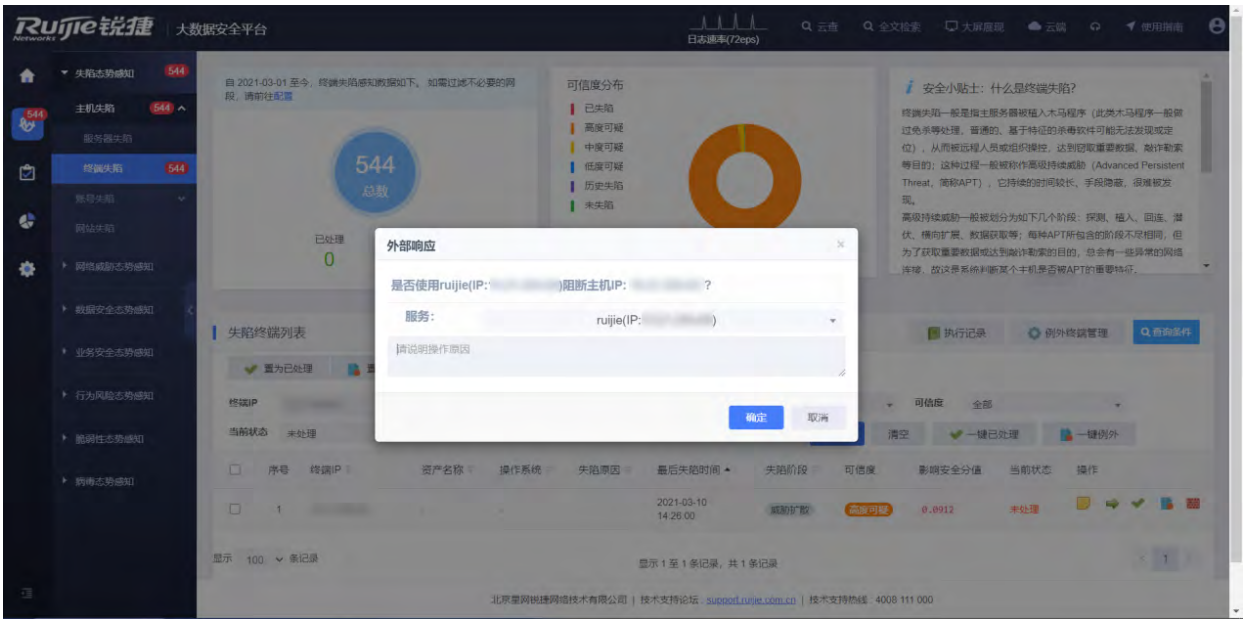
该用户通过“网络 + 安全”整网安全解决方案，实现了对下属机构的网络安全状态监管。教育局下属的中学、小学很难自身部署一套大数据安全平台，因此通过教育局纳管实现安全赋能。在综合分析下属学校的流量后，教育局多次及时发现和处置下属学校的异常攻击行为。

教育局高度评价了该系统，表示该系统非常适用于教育城域网这种环境，特别是交换机组网架构下，能够利用交换机联动及时发现下属机构的安全问题，并快速响应。

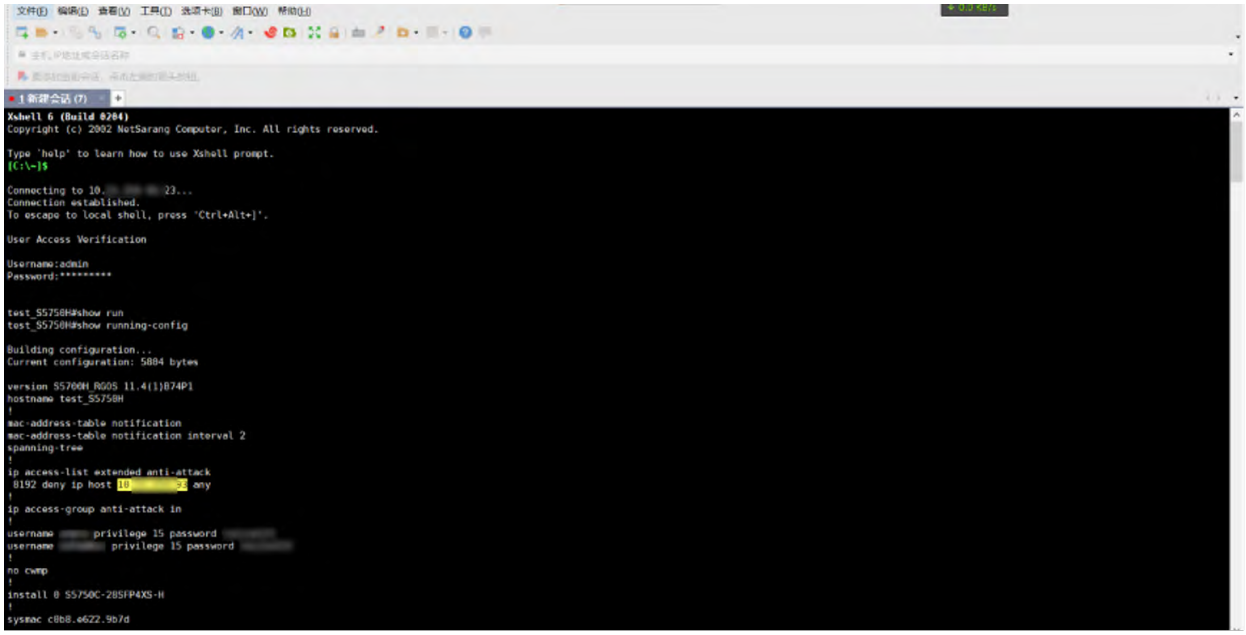
在用户处理流程上，大数据安全平台 RG-BDS 联合高级威胁检测系统 RG-APT 和交换机发现安全问题，联动 SDN 控制器下发阻断策略一键封堵失陷主机，防止威胁大规模扩散。

1、大数据安全平台对 SDN 控制器进行联动，在出现问题时，能够下发指令并执行，在交换机层面实时封堵，避免失陷终端出现威胁扩散行为。

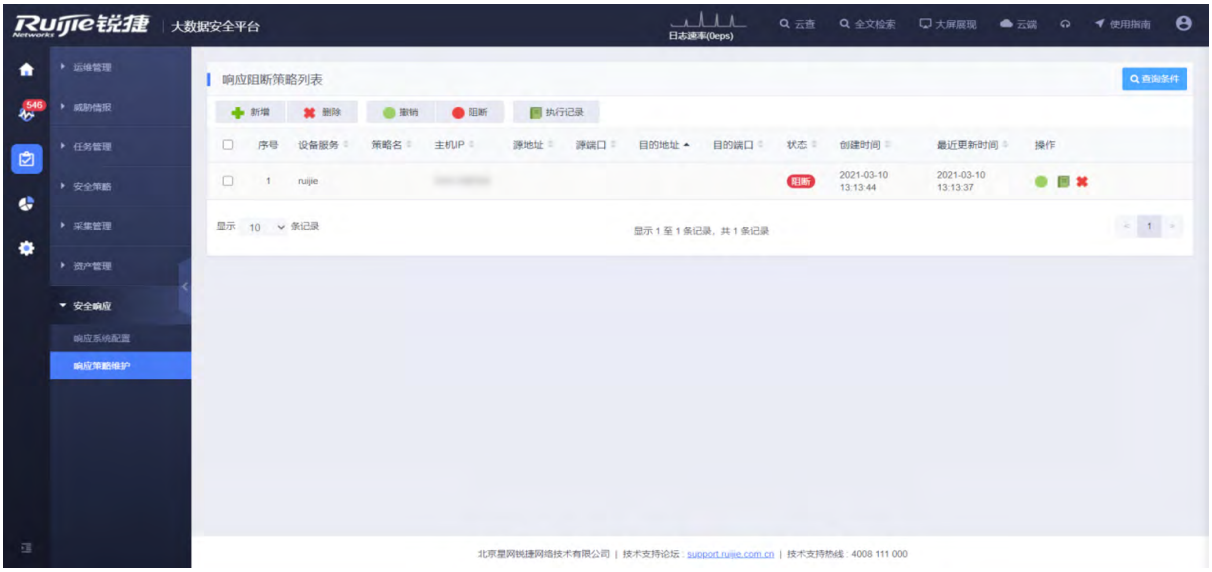
大数据安全平台阻断失陷主机：



SDN 控制器下发阻断命令到交换机：



大数据安全平台联动 SDN 控制器实现阻断：



目前用户处有驻场工程师在做日常运维，大数据安全平台每周平均发现 30 台失陷主机。当发现失陷问题时，工程师结合到安全管理平台 RG-SMP 系统搜索认证记录，找到对应实名老师后给该老师打电话，建议老师全盘杀毒或重装系统。若多次通知后无整改的行动，工程师就会通过 SDN 控制器直接下发阻断策略，防止病毒的扩散。针对下属学校安全的强管控，也带动了整体教育城域网使用者安全意识的提升。

4.4 某医院案例

4.4.1 用户背景及需求

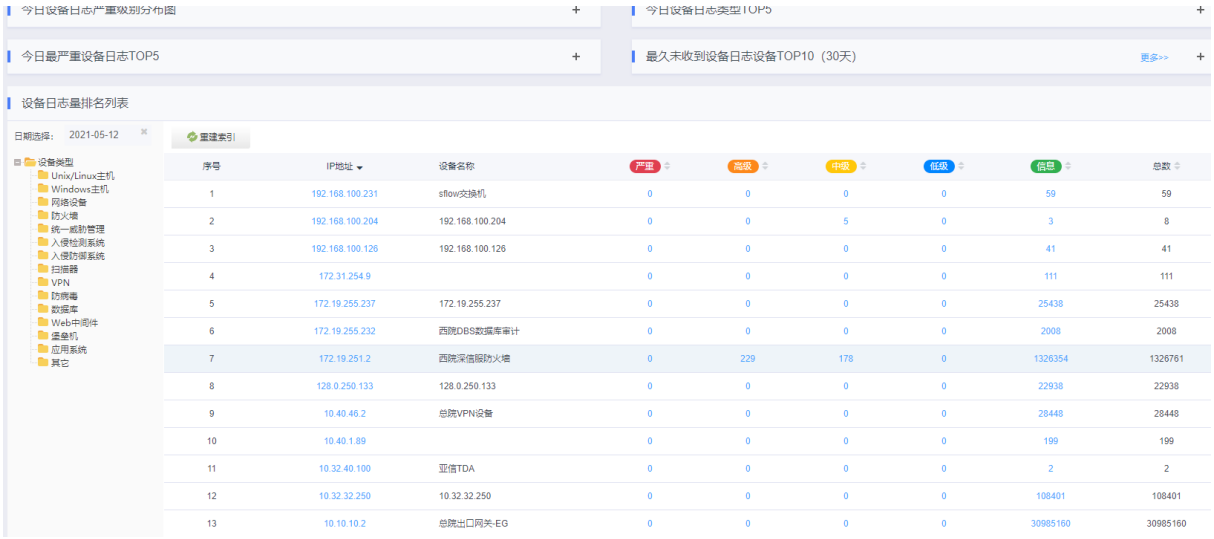
某医院是国内三甲医院，是国内最著名、最具国际化特色的医教研中心之一。该医院现有多个园区，有临床医技科室 40 个，核定床位 2092 张。

该用户安全设备较多，但由于联动体系做的不好，安全设备各自形成孤岛，告警量大误报多，安全运维难以全量监控，无法对整网安全事件有统一的运维入口。且目前安全设备均部署于数据中心和网络核心，针对主机东西向流量的安全监控有空缺。该医院曾考察和测试了业界多种方案，试图失陷安全设备的统一纳管，但由于终端数量较多，所以无法在每个接入节点均部署探针。

4.4.2 方案设计

目前，该医院在西院区部署了大数据安全平台 RG-BDS-A，防火墙、网关、堡垒机、数据库审计、入侵防御等安全设备日志均已接入 RG-BDS-A 进行范式化和安全分析，并结合接入交换机 sFlow 流量数据进行东西向流量监控，实现对全网安全的实时监测与分析。

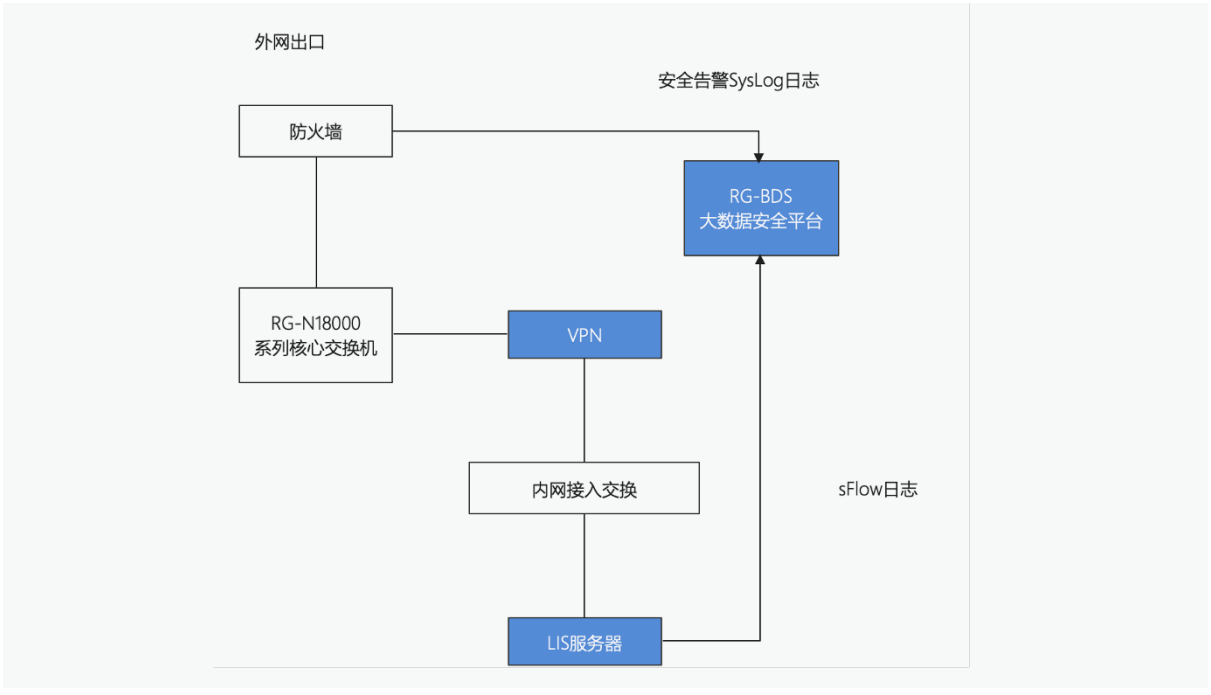
西院区“网络 + 安全”部署上线，交换机开启 sFlow 接入大数据安全平台 RG-BDS-A，监测整网横向流量；



用户现网安全设备告警日志接入，利用大数据安全平台 RG-BDS-A 针对各设备安全日志进行分析与研判。

4.4.3 实施效果及反馈

以某一次跳板攻击为例，通过内网 sFlow 数据分析发现多次 VPN 地址与 LIS 服务器的通信记录，而正常 LIS 业务的访问源中并不应该有 VPN 过来的访问。安全管理员通过防火墙日志配合威胁情报综合研判发现，外网非法 IP 地址多次探测 VPN 地址。经过防火墙和交换机日志关联分析后，定位发现有恶意人员通过 VPN 设备进入内网扫描探测，此行为具备较大风险。用户排查后发现 VPN 对内网开放的权限太大，VPN 作为内外网的桥梁，自身的安全防护较薄弱，很容易成为跳板，因此用户紧急封堵了非法 IP 并及时进行权限修订。



同时，用户对勒索病毒的横向扩散监控问题一直比较困惑，很多病毒扩散传染的流量不经过核心核心交换，而是直接在接入的二层传播，即内网传播。核心上面的探针、IDS 等安全设备无法感知到横向扩散，等发现问题后已经是大片感染的状态了。采用锐捷 RG-BDS-A+ 交换机的联动方案，由于在中毒扩散时，该主机会大量地对内部高危端口进行扩散扫描。这些异常数据流量被记录下来，通过交换机 sFlow 协议采样汇聚层和接入层流量发送日志给 RG-BDS-A，安全人员可以通过分析引擎直接定位具体的病毒扩散源。整体方案直接利用交换机的 sFlow 特性零成本实现对勒索病毒扩散的监控以便及时止损，受到用户的高度认可。用户早期有顾虑是否会影响交换机的正常转发，其实二层网络的转发一般靠硬件转发，常规情况交换机的 CPU 利用率一般都很低，在 30% 以下，经测试 sFlow 实际使用对 CPU 的影响只有 1%-5%，对交换机的性能影响可以忽略不计。

看到初期效果后，院方较为认可方案价值，将总院运维层交换机替换为新型号支持 sFlow 的交换机，并扩大实施范围，这将实现全网的交换机 sFlow 数据和南北向安全设备数据的综合分析与安全态势感知。

4.5 某高校案例

4.5.1 用户背景及需求

某大学是一家综合性的大学，学生较多，接入需求较大。该大学人员众多，师生上网需要有上网行为实名记录，且需要满足 180 天日志留存需求。除了合规，也希望将这些数据利用起来，一方面对出口安全进行分析和监控，另一方面需要对不良的访问行为和可疑的连接行为实时监控进行舆情预警。

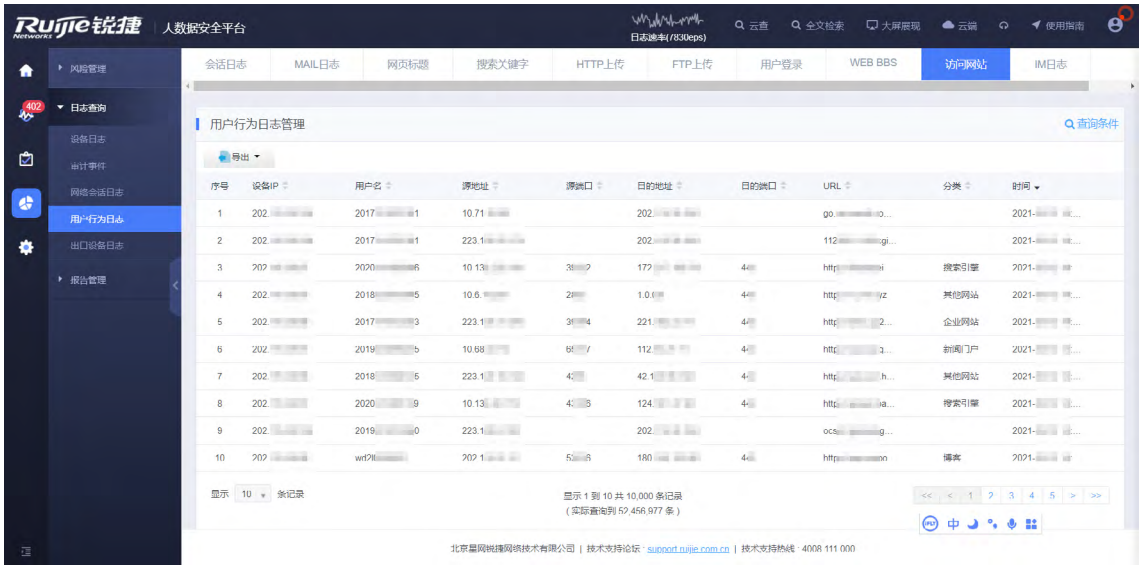
4.5.2 方案设计及实施

根据用户需求，锐捷给出的方案设计如下：

设计使用大数据安全平台增强版 RG-BDS-A 用于存储统一上网行为管理与审计系统 RG-UAC6000 系列上的日志，同时 RG-BDS-A 联动认证计费管理平台 RG-SAM+，通过用户上下线信息来获得实名信息，RG-BDS-A 整合上网行为记录日志与实名信息后，一次性关联显示上网行为记录与实名信息，RG-BDS-A 提供大存储空间和秒级日志溯源满足合规要求。

4.5.3 实施效果及反馈

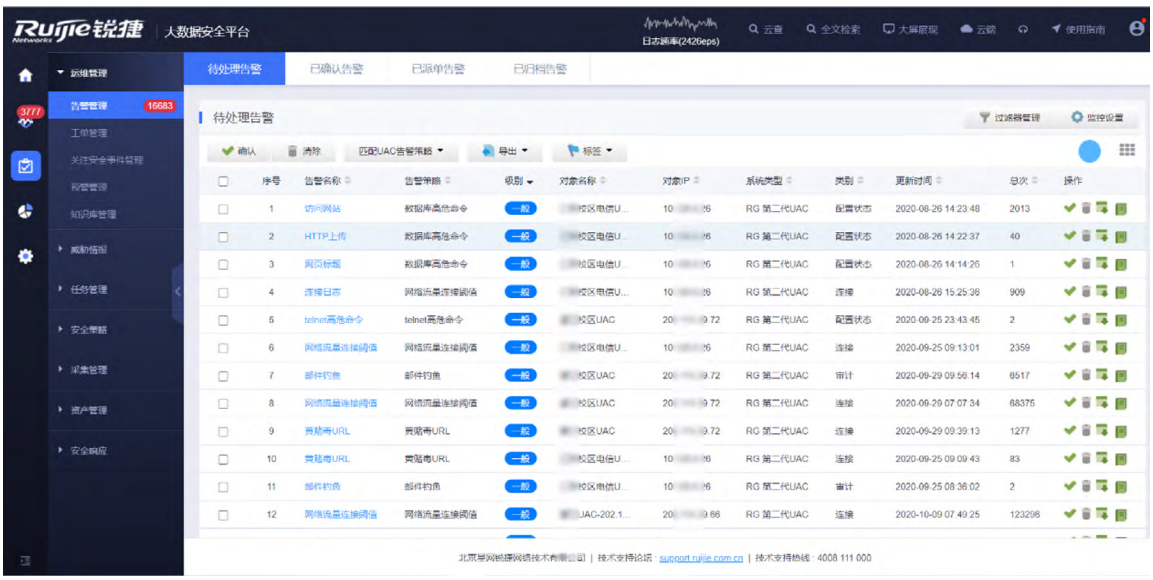
实施锐捷“网络 + 安全”整网安全解决方案后，为用户实现了对网络设备和安全设备的统一纳管，能够有效监控用户行为，并在第一时间发现风险异常。



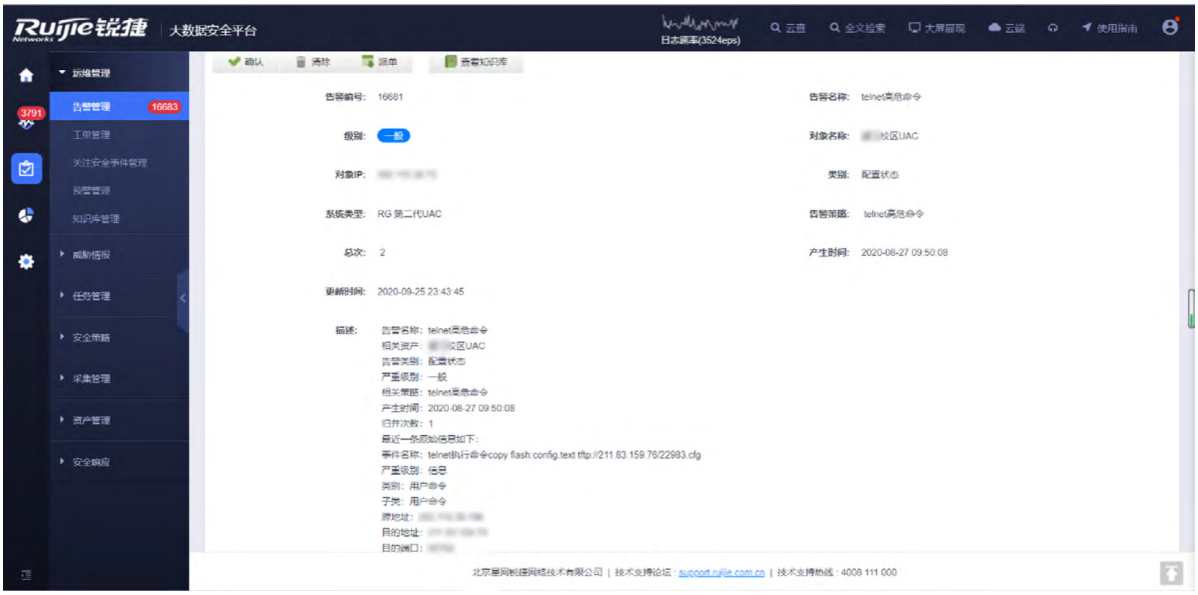
在实际使用中，通过与学校网络认证计费系统联动，结合 RG-UAC 6000 系列的日志，如上图这种非法访问能够直接定位到具体用户。学校还设置了关键词列表，一旦发现有学生搜索“自杀”、“裸贷”等关键词，能够及时进行告警，并且通过关联认证系统账户信息直接定位到具体人员，从而进行线下的沟通和教育。在与用户沟通中，该校确实曾多次通过大数据安全平台发现有消极行为的同学，并及时进行了制止。

对于人的行为的监测分析方面，RG-BDS 有很多有用的告警策略，比如黄赌毒 URL、邮件钓鱼、邮件泄密、即时通讯泄密和文件上传泄密。

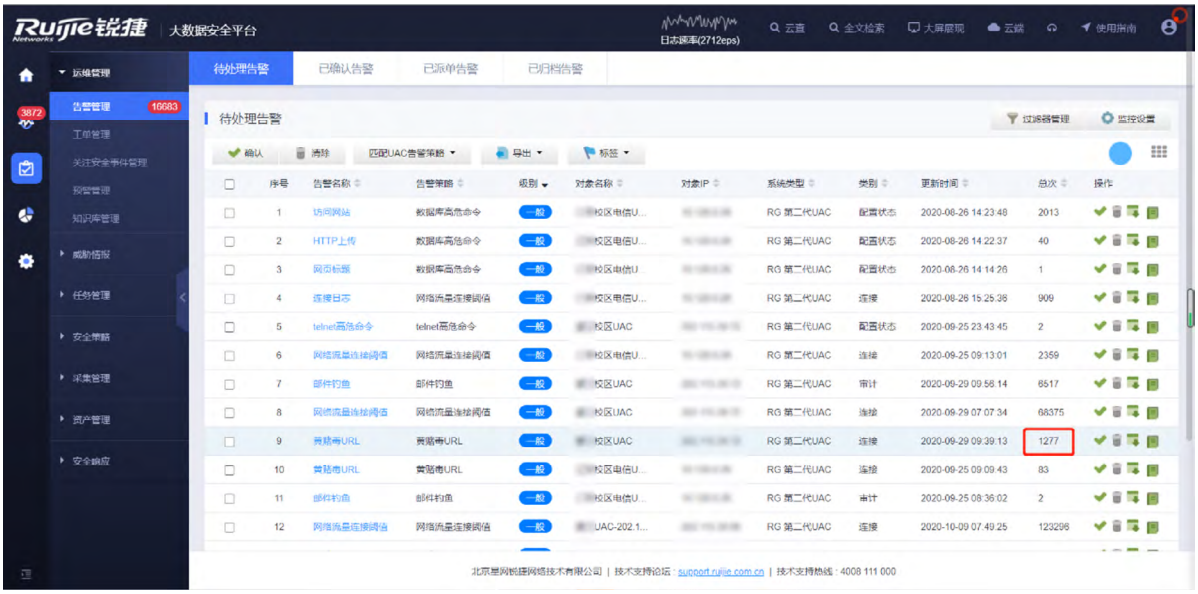
第一步，在 RG-BDS 上设置了 11 条 RG-UAC 6000 系列的安全告警策略，每天收集相关的日志信息进行分析。



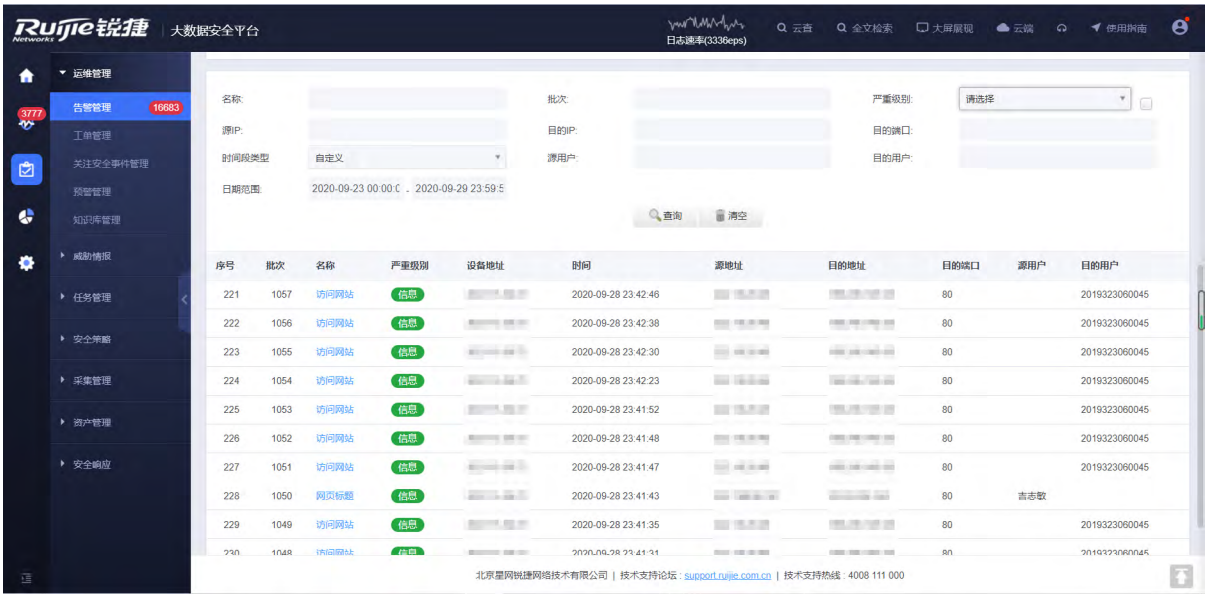
第二步，通过 RG-BDS 看到这个黄赌毒 URL，点击进来后可以看到相关信息，它会展示这条告警的来源与基本信息，



第三步，RG-BDS 通过设定的策略分析了归并信息的所有内容， 将一段时间内，按照策略和告警名称进行归并，能大大缩小告警量，减轻负担，如下图，将 RG-UAC 6000 系列的相关 1277 条黄赌毒 URL 告警归并成一条告警，直接锁定非法访问人员。



第四步，我们可以知晓触发告警的源目地址，再结合认证系统的账户信息联动，将所有告警实名化，就直接能找到该 IP 背后的用户对其进行教育。



总结来说，将统一上网行为管理与审计系统 RG-UAC6000 系列和大数据安全平台 RG-BDS 联动通过监控告警，能够协助我校规范用户的行为，避免人为因素导致学校被通报，通过内置的分析模型库还能及时发现恶意攻击、数据泄露、蠕虫扩散、钓鱼邮件和数据库拖库等，及时防范于未然。

发展与展望

“网络 + 安全”是一个方案更是一个理念。“网络 + 安全”的本质是让网络设备发挥更多的安全价值，在减少预算的同时提升网络安全防护能力。当前的主流理念是将安全融入到网络建设中，一方面是在网络布局中尽早融入安全设备，而让网络设备承担更多的安全责任则是另一种实现方式。随着性能的提升，网络设备将能承担更多的安全功能。

安全合规依旧是当前安全市场的重要导向，以等保合规为基础，在基础之上进一步提升安全能力是大多数安全甲方选择的建设方式。随着信息化业务的扩大，合规已经不能满足日常的安全防护需求。但在网络安全当中，合理的安全投入永远是网络安全绕不开的话题。

随着安全回归于网络，从独立建设变成信息化的一部分，“网络 + 安全”这一理念将获得更多的认可。诸如锐捷这样的信息化厂商，基于其本身的网络设备布局的优势，也将越来越多的将网络和安全产品联动起来，形成采集、分析、决策、处置为一体的体系化信息安全方案，这将为甲方用户提供更好的技术支撑。

“网络 + 安全”将是越来越多的厂商探索的模式，而锐捷具备本身的网络背景和安全实践经验，是将这一理念实践的理想载体。

Ruijie Networks 锐捷 | 安全牛 AQNIU.COM

零时代·安全牛

网络安全旗舰智库

合作电话:18311333376　合作微信:aqniu001