网络可见性的问题

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The Problem With Network Visibility		
原文作者	伯纳德·布罗德（Bernard Brode）	**原文发布日期**	2020年1月11日
作者简介	约翰·爱德华兹是一位科技记者。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/networking/problem-network-visibility		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

网络可见性的问题

伯纳德·布罗德

2020 年 1 月 11 日

近几年来，“网络可见性”一直是一个热门词，吸引着众多追捧者。浏览一下自 2020 年到现在的行业新闻，我们会得到这样一个印象：网络可见性是解决所有网络安全弊病的灵丹妙药。

我并不是要唱反调。我也认为，正如“在保护网络免受新型威胁方面，检测很重要”一样，要想对网络设备的运行生成高质量的反馈，可见性也很重要。但是，我们需要认识到，可见性不应成为寻求保护其系统的网络管理员的唯一手段。相反，他们还应重视控制。

换句话说，未来几年，企业应从追求可见性转向追求洞察力，这一点很关键。相比于能够了解详细的网络攻击细节，我们更应该知道如何阻止攻击。

网络可见性是什么

为了了解网络可见性的局限性，我们首先要理解这个术语的含义。近年来，网络可见性已成为一个笼统的术语，类似于“多个防火墙”。但是实际上，可见性的概念是在非常特殊的场景中（工业物联网[IIoT]）产生的。

众所周知，IIoT 正在迅速发展。据统计，联网设备的数量以每秒 127 台的速度增长，到 2025 年联网设备的总数将超过 750 亿台，而工业设备在其中占了很大的比例。实际上，IIoT 的迅速发展使一些人认为我们正处于第四次工业革命中。

但是，对工业生产有利的联网设备，对网络安全可能并不那么有利。在 IIoT 基础设施发展的早期，人们就认识到这将带来巨大的安全挑战。这些挑战并非源于联网设备数量过多（当然联网设备的大量安装也会带来问题），而是源于它们互联的方式。

可见性和安全性

传统上，网络安全范式基于一个简单的理论——如果企业能够阻止黑客（或恶意软件、工业间谍机器人等）进入其网络，那么企业就是安全的。因此，只要为外部端点配备了入侵检测、防火墙和适当的身份鉴别解决方案，企业的网络就会相当安全。

上述理论有两个问题。其一，许多 IIoT 系统有大量的外部端点，难以进行管理。其二，这些 IIoT 网络的规模非常庞大，其内外部端点的边界正在迅速消失。例如，在一个高度网络化的工厂中，每个员工的笔记本电脑都可以访问工业控制系统的某些部分，这些笔记本电脑可能会成为黑客进入其网络的入口点。

除了当代 IIoT 系统中的端点数量呈指数增长之外，还有另外一个问题。那就是，许多为 IIoT 网络提供感知功能的小型设备相互连接，而这种连接不受控制和监测系统的管理。

正是这个问题导致我们关注网络可见性这一概念。我们担心，如果无法监控所有端点连接到哪些目标，以及它们之间相互发送的内容，就无法阻止恶意软件通过横向移动和凭证升级迅速在 IIoT 网络中传播。

可见性与控制

这种担心当然是合理的。不幸的是，我们为解决这一问题而创建的系统（通常）无法完成任务。实际上，在许多方面，“实现可见性”这一想法已经掩盖了网络安全工程师真正想要的能力——控制。随便看一下当今主要网络安全提供商的产品和服务，你就能明白我的意思。这些提供商通常提供“可见性”、“监控”和“检测”类产品和服务，而非诸如“清除恶意软件”等更有用的功能。

对可见性的过度关注，导致我们对风险和责任的认识出现错误。通常，企业将网络安全看做昂贵且复杂的“打地鼠”游戏——系统检测到在两个网络节点之间移动的威胁并将其清除。但是，许多企业缺乏专业知识或资源，来执行那种未能发现威胁源的取证分析，甚至无法找到可见性工具发现的威胁在何处。

最终，企业就悲剧了：除非其网络可见性是完整的，否则就几乎是无用的。鉴于分包软件系统、混合云和专有 IIoT 系统非常复杂，几乎没有什么公司能够真正实现对其网络的全面监管。

聊胜于无？

你可能会认为我在说胡话。对网络有可见性（即使是一点点）总比没有好吧？我同意这一观点。问题在于，有时对可见性的追求会掩盖更重要的东西——执行有效的网络取证并锁定外部端点的能力。

我知道，我的观点不太可能对市场上的防入侵软件的功效或类型产生什么影响。我们知道，内容分发网络（CDN）时代需要新的网络可见性标准，但是大部分企业并未实现这一点。网络安全供应商更有可能向企业鼓吹“需要更好的可见性”的原因，而非向其提供能够阻止入侵者的工具。

但是，企业自己应意识到，在提高网络可见性的同时，提升防护和控制能力同样重要。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）
安天企业安全公司更多信息请访问： http://www.antiy.cn
安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com