

简译版

如何保护企业物联网

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	Will Enterprise IoT Become BYOD on Steroids?		
原文作者	Anand Srinivas	原文发布日期	2019 年 5 月 2 日
作者简介	Anand Srinivas 是 Nyansa 公司的联合创始人兼首席技术官。 https://www.networkcomputing.com/author/anand-srinivas		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/network-security/will-enterprise-iot-become-byod-steroids		
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.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 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共方式，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。 		

如何保护企业物联网

Anand Srinivas

2019 年 5 月 2 日

相比于传统的 BYOD 基础设施管理，IoT 设备性能和安全的管理需要一种更全面的方法。

如果你认为保护“自带设备”（BYOD）对网络安全人员来说是一项痛苦的任务，那就太孤陋寡闻了。

现代物联网（IoT）设备具有独特的、不同于其他联网设备的威胁态势和行为，会带来新的风险，使传统工具不再有效。

企业需要进行更深入的行为分析，以确定这些 IoT 设备如何在企业网络中运行。该方法与以往在笔记本电脑和智能手机等设备上使用的方法大相径庭。

如果企业对 IoT 设备保护不当，攻击者就可以利用这些设备访问企业系统，窃取大量数据。数据的完整性遭破坏会导致灾难性的后果，对企业的战略业务产生不利影响。

网络安全、端点保护、移动设备管理（MDM）、活跃漏洞扫描程序和日志分析无法应用于具有锁定操作系统或嵌入式控制系统的设备。因此，大多数 IoT 设备都达不到预期的安全状态。

面向企业边缘的新兴 AIOps 平台可以通过自动分析大量数据、识别异常以及查找威胁设备性能和安全的漏洞，来解决这一难题。

IoT 安全并没那么简单

对于供应商和客户来说，IoT 安全问题非常复杂、成本高昂，而且他们对该问题不够重视。因此，在这方面他们经常做“事后诸葛”。

大多数 IoT 设备具有有限的硬件功能和联网功能，以及不支持传统网络安全方法的专有操作系统，这使保护此类设备更加复杂。

大多数 IoT 设备都是使用专用协议开发的。相比于传统笔记本电脑或智能设备的应用和网络服务，这些协议的行为方式有所不同。此外，IoT 设备不具备安装传统软件代理的能力。

因此，IT 人员很难实现对此类设备的可见性并加以控制。

此外，IoT 管理任务可能分散在 IT 或网络运营等不同部门。如果这些部门都可以使用的 IoT 设备的性能和安全性不一致，那么 IT 人员之间就会有分歧，导致对直接影响业务成果的关键事件修复延迟。

需要更广泛的视角

应对 IoT 攻击需要更广泛的管理和安全方法。如果 IoT 设备无法正确连接到网络或在网络中运行，那么“安全”就是一项没有实际意义的讨论。

企业正在构建新兴的 AIOps 平台，通过更全面地了解 IoT 设备如何与网络的其他部分、网络服务和应用进行交互来提供“运营保障”。

对于 IT 领导者而言，IoT 运营保障的基本组成部分包括：自动识别 IoT 设备并进行分类、基线 IoT 行为、检测异常、在 IoT 设备（或一组 IoT 设备）偏离可接受行为时主动执行安全策略。

这些平台整合了基础设施的各种数据源，例如原始网络数据包、客户端数据、SYSLOG 消息、应用程序响应、无线指标和 WAN 路由器数据流。

然后，这些平台使用先进的人工智能（AI）和机器学习（ML）技术测量、分析和关联数据，以发现趋势，预测潜在事件并解决人类无法解决的复杂问题。

为何某个区域的用户在访问给定应用时会遇到问题？是 Wi-Fi 问题？DNS 响应太慢？DHCP 地址已分配尽？WAN 链路过度使用？这是一起孤立的事件还是全系统的网络问题？

目前，查明这些问题成本高昂、步骤繁琐，并且通常涉及不同的工程师团队。随着 IoT 设备的出现，这些问题只会进一步加剧。

传统基础设施管理工具不会分析整个堆栈中每个设备的网络事务。如果设备无法获得 IP 地址、无法访问应用，或连接到了不利的 Wi-Fi 接入点，企业就会受到影响，IT 人员必须查找原因并予以解决。新的 AIOps 边缘平台有效地解决了这些问题。

通过分析每个设备的网络事务，就可以建立正常行为的基线。通过与现有安全系统的直接交互，任何与此行为的偏差都会触发补救措施，例如对 IoT 设备进行分段或微分段。

现在，网络工作人员可以了解和控制 IoT 设备如何在网络的各个部分运行，并识别潜在威胁，例如输液泵与可疑主机通信或执行某种恶意行为。

最后，网络管理员需要重新审视如何最好地管理 IoT 设备的性能并确保其运行。否则，他们就无法获得在该领域投资的价值。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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>