简译版

边缘安全问题

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	Addressing the Challenges of Moving Security to the Edge		
原文作者	John Maddison	**原文发布日期**	2019 年 4 月 4 日
作者简介	John Maddison 是 Fortinet 公司产品和解决方案高级副总裁。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/addressing-challenges-moving-security-edge		
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。		

边缘安全问题

John Maddison

2019 年 4 月 4 日

对于许多企业而言，网络边界已被各种新的网络边缘所取代。这带来了一些独特的挑战，使企业难以维持一致且可管理的安全基础设施。这些挑战包括两个方面。

第一个挑战是：在独特的网络、平台配置或功能的前提下，在网络边缘实施有效且一致的策略。第二个挑战是：在各个边缘之间实施一致的安全策略，这不仅仅是为了实现可见性，还是为了在所有边缘环境中有效地协调策略更改和威胁响应。

对任何安全策略来说，保持一致的可见性和控制措施都非常重要，但是实现这一点越来越难了。数字化转型以及新的计算和联网环境的发展，不断将安全团队引向新的方向，使他们分散精力，无法为特定环境提供充分的保护。

我们看到，在过去的几年中，利用已知漏洞的成功攻击数量激增——这些漏洞的补丁已发布了数周甚至数月，但是安全团队未来得及打补丁。许多安全团队分身乏术，甚至无法在其系统上实施基本的安全措施，更不用说评估和满足新联网环境的需求了。要想应对这些新的边缘环境，企业不仅要了解它们面临的挑战（包括在它们之间实施一致的安全策略），还要考虑如何以及在何处建立先进的自动化技术来简化整个安全流程（从初始部署到威胁检测和协调响应）。

保护网络的扩展边缘

接下来，本文将介绍企业需要保护和管理的网络边缘环境、这些环境面临的安全挑战，以及应对这些挑战需要注意的问题。

云和“多重云”

每个云平台都有独特的控制措施和管理界面。但是，大多数安全设备被部署为覆盖解决方案，因此无法使用其中的许多控制措施和管理界面。虽说通过“多重云”（multi-cloud）方法，企业可以在各种云平台上轻松部署同样的工具，但是这些工具可能会丧失某些功能，这使得企业难以建立一致的安全策略。此外，由于这些工具不是云原生工具，它们的性能也

会受到严重的影响。

云原生安全解决方案则要好得多，因为它们不存在覆盖解决方案的功能和性能问题。但是，在多重云部署中，企业可能需要与在另一平台上运行的设备进行互操作。幸运的是，通过添加连接器，可以解决这一问题。这些连接器不仅可以将云原生安全工具一键部署到云环境中，还可以充当已部署解决方案之间的转换器，确保平台内和平台之间的安全策略一致性。

最终用户和物联网

物联网（IoT）和最终用户端点设备的激增是企业面临的另一个挑战。这些设备越来越智能，运行速度越来越快，而且具有很高的移动性——一位用户同时将多台设备连接到网络的情况并不罕见。此外，由于用户经常将个人与企业数据、应用和配置文件混合到同一台端点设备上，加之端点设备的安全措施过于松懈，因此企业面临着严重的风险，如数据丢失、被盗，恶意应用下载，无意中连接到被感染的公共接入点等。

IoT 设备会带来各种风险——它们以前所未有的速度连接到网络，而且大多具有内在的不安全性，甚至无法更新或修复。因此，IoT 设备沦为网络犯罪分子的首选目标。

要想保护端点边缘，企业需确保通信已加密且安全设备能以“网络速度”（network speed）检查加密数据，确保自动识别设备，并在没有人为干预的情况下应用适当的策略和分割规则。此外，企业还需持续监控这些设备，将其访问策略自动分发到扩展网络的安全设备上。

广域网边缘

新的“软件定义分支”（SD-Branch）需要与其他远程位置和数据中心连接，这意味着它们需要网状 VPN 连接。这样一来，SD-Branch 不仅能与远程位置和数据中心连接，还能支持“性能密集”（performance-heavy）和“延迟敏感”（latency-sensitive）业务应用，如网络电话（VoIP）和视频会议。此外，它们有自己的局域网（由固定和移动设备、IoT 设备、IaaS 和 SaaS 连接以及多个公共互联网链接组成），因此需要一整套安全工具。

有效和安全的“软件定义广域网”（SD-WAN）解决方案不仅需要高级路由功能和性能增强功能（例如 VPN 连接之间的负载均衡应用），还需要一套完全集成的安全工具，以便与其他地方部署的安全解决方案进行互操作，无缝地将安全功能、性能和策略扩展到本地分支局域网。这不仅能够确保对 WAN 边缘的一致可见性，而且无需构建特殊的 SD-WAN 安全

解决方案。

5G

5G 将带来前所未有的速度和互联性，进一步改变我们共享关键信息、提供/接收丰富的媒体、运行大规模应用和做出实时决策的方式。设备之间的互联也有可能创建一个新的开放边缘云。鉴于数据需要在网络的最边缘使用，且功能以微秒为单位进行测量，应用往往无法承受往返数据中心的负荷。

为了应对上述问题，数据和决策（以及安全性）也需要走向边缘——它们需要嵌入边缘网络和 IoT 设备中。此外，为了满足性能需求，企业不仅要实现大多数安全协议的自动化，还要利用机器学习和“人工智能”（AI）技术以“数字速度”（digital speed）做出自主决策。要想做到这一点，企业不可再将有限的资源分散化，而是将新边缘的安全策略与其他边缘环境中的策略无缝集成。

结论

企业需要意识到，这些新的边缘环境不是独立存在的。它们都属于同一个安全环境，最好的办法是开发一个全面且适应性强的安全策略。该策略可以轻松扩展到新的网络环境，不会影响其他地方部署的安全设备的功能和互操作性，也不会影响可见性和集中式编排和控制，易于管理且具有成本效益。

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*