简译版

本地安全工具在云端效果不佳

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	On-Premise Security Tools Struggle to Survive in the Cloud		
原文作者	Kelly Sheridan	原文发布日期	2018 年 4 月 10 日
作者简介	Kelly Sheridan 是 Dark Reading 的编辑。https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/on-premise-security-tools-struggle-to-survive-in-the-cloud/d/d-id/1331501		
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。		

本地安全工具在云端效果不佳

Kelly Sheridan

2018 年 4 月 10 日

企业称，他们目前的安全工具在云中并不奏效，但他们却不愿意采用云安全系统。

云使用的增长速度超过企业保护云的能力。尽管 IT 专家很快指出了“软件即服务”（Software as a Service，SaaS）应用程序的好处，但他们对采用云中特定的安全工具却犹豫不决。与此同时，他们现有的安全系统将云端数据置于危险之中。

iboss 在其《2018 年企业云趋势》报告中指出，大多数（64%）大型企业表示，SaaS 的采用速度已经超过云安全措施。平均而言，约有 20%的企业应用程序是 SaaS，预计在未来两到三年内，这一比例将达到 36%。

iboss 的所有受访者均表示，相较于物理软件，使用 SaaS 应用程序至少有一个好处。这些好处包括速度（71%）、人性化（58%）、数据存储容量（49%）、提高生产率（43%）和数据可访问性（40%）。他们最常将 SaaS 用于电子邮件（63%）、数据丢失防护（59%）和文件共享（59%）。

员工希望在工作场所使用 SaaS，而且他们将会继续这样做。然而，91%的受访者表示，如果要在云环境中运营，企业的安全策略就需要改进。10%的受访者表示需要“彻底检修”。

当前工具在云中效果不佳

Sumo Logic 公司在一项名为“2018 年全球云安全趋势”的调查中指出，97%的受访者认为云安全是一项挑战。大多数受访者报告称缺乏工具、跨职能协作和资源来深入了解企业安全。

几乎所有的（93%）受访者都表示面临在云中使用安全工具的问题。约一半（49%）受访者认为现有工具在其云环境中效果不佳，指出太多的工具使得他们很难确定优先级。45%的受访者表示，由于整合不佳，他们无法及时调查威胁。受访者还表示，不同的工具会给出相互矛盾的信息，云中特定的工具既昂贵又难以学习。

“传统的本地安全工具根本不是为大多数大型企业今天使用的无边界网络设计的，”

iboss 联合创始人兼首席执行官保罗·马蒂尼（Paul Martini）说，“本地解决方案需要通过总部的物理安全设备路由所有网络流量，这是一个非常昂贵且效率低下的过程。”

Sumo Logic 发现 87%的企业出于若干原因费力地在云中使用本地安全信息和事件管理（SIEM）解决方案。超过一半（51%）的受访者表示无法有效吸收云数据和威胁（51%），34%的受访者表示在云中使用本地工具太过昂贵，33%的受访者表示部署和使用很困难。只有 17%的受访者表示他们不愿意在云端使用本地 SIEM。

Sumo Logic 首席安全官乔治·格尔乔（George Gerchow）表示，SIEM 最初创建的目的是用于安全数据，主要由安全团队使用。现在，这些系统需要更加透明，以便开发人员和运营人员可以访问数据。随着企业日益依赖 Office 365，Salesforce 和 Workday 等云服务，他们意识到需要进行改变。

格尔乔解释说：“他们终于开始学习他们需要的东西，这些东西将具有可扩展性，弹性和在现代应用程序中的可见性。”

他补充说，在云中使用本地工具成本高昂。从云环境中收集数据，导入数据进行分析，然后将数据推回到云端，这些过程的效率低下且成本高昂。

云安全需求也给安全团队的结构施加了压力。Sumo Logic 的受访者中超过 60%认为云安全需要更广泛的技术专长，54%的受访者表示需要更大规模的跨团队协作，51%的受访者表示他们的员工超负荷工作。总体而言，97%的企业面临着云安全方面的挑战。

切换到 SaaS 安全：为何要等？

尽管对 SaaS 应用程序充满热情，但约一半（49%）的 iboss 受访者表示他们对采用基于 SaaS 的安全工具犹豫不决。

“因为他们认为每个 SaaS 解决方案都需要他们利用多租户共享云架构，所以公司通常会因数据隐私问题而不愿意采用 SaaS 安全工具。”马蒂尼说。他补充说，金融服务和医疗等行业的人士也担心监管控制。

但是，如果不切换到云安全，企业就得放弃 SaaS 应用程序提供的诸多好处。越来越多的员工要求灵活地使用云应用程序进行远程工作；使用本地安全工具会妨碍他们安全地做到这一点。

“使用云安全工具的风险在于知识和教育，”格尔乔说，“我们在这方面有欠缺。如果移到云端，（企业）根本没有技能来了解这些工具是如何工作的。”

采用云安全工具可能需要一条学习曲线，但格尔乔警告称，那些在转移到云端时坚持使用本地工具的公司是很危险的。

“在我看来，最大的风险是，你只能看到环境的一部分，”他解释说，“你无法对发生的事情进行全面的 360 度审视。”

随着公司收集大量数据，他们转向 SaaS 安全的压力将会增加，格尔乔继续说道。基于云的解决方案可以扩展以处理更大的数据存储。例如，如果你在 AWS 中管理工作负载，并且从 10 TB 的数据扩展到 40 TB 再到 100 TB，那么你就无法使用本地安全系统来保护所有的数据了。

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，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，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，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。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，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“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*