Gartner：“安全访问服务边缘”（SASE）将改变网络安全

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	Gartner: SASE Poised to Transform Cybersecurity		
原文作者	Frank Ohlhorst	原文发布日期	2019 年 10 月 8 日
作者简介	Frank Ohlhorst 是一位屡获殊荣的技术新闻记者和 IT 行业分析师。 https://securityboulevard.com/author/frank-ohlhorst/		
原文发布单位	Security Boulevard		
原文出处	https://securityboulevard.com/2019/10/gartner-sase-poised-to-transform-cybersecurity/		
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。		

Gartner：“安全访问服务边缘”（SASE）将改变网络安全

Frank Ohlhorst

2019 年 10 月 8 日

研究公司 Gartner 对一种有前景的技术“安全访问服务边缘”（SASE）给予了高度评价。SASE 是一种新兴的颠覆性技术，旨在创建完全集成到网络中的安全云环境。Gartner《2019 年企业网络炒作周期》报告显示，SASE 具有战略意义，被认为是“转型性”技术。

SASE 解决了将传统网络集成到云环境中的问题。在云环境中，网络安全变得日益僵化、不灵活。简而言之，当企业寻求迁移到云时，他们面临的问题是：网络变得僵化；物理、虚拟和云资源的安全彼此孤立——这些问题有悖于云的初衷。

鉴于云的敏捷性、弹性和普遍性，越来越多的企业开始采用云技术。通过云技术，企业能够更快地对变化做出响应，同时保留应对关键市场的能力。但是，数字转型和云迁移受到网络设计方式之先入之见的阻碍。很多企业试图通过将 SD-WAN 设备、防火墙、IPS 设备和许多其他解决方案结合在一起来构建云迁移流程，但最终形成了无法管理的、混乱的技术，这些技术带来的麻烦超过其实际价值。

SASE 云架构使这种动态变化易于管理和保护。SASE 将云从一系列孤立技术的强行集成转变为单个网络，该网络可以连接和保护任何企业资源，包括物理、云和移动资源——无论资源在什么位置。

Gartner 在 SASE 报告中将 Cato Networks 称为“典型供应商”，该公司阐述了 SASE 云的含义。基于此，Gartner 总结了 SASE 云的四个主要特征。

- **身份驱动**：用户和资源身份，而不仅仅是 IP 地址，决定了网络体验和访问权限级别。服务质量、路由选择、应用风险驱动的安全控制，所有这些都由与每个网络关联的身份驱动。无论设备是什么或在什么位置，通过该方法，公司可以为用户开发一套网络和安全策略，从而减少运营成本。
- **云原生架构**：SASE 架构利用关键的云功能（包括弹性、适应性、自我修复和自我维护）提供一个平台，可分摊客户成本以实现效率最大化，轻松适应新兴业务需求，并且可以在任何地方使用。

- **支持所有边缘**：SASE 为所有公司资源（数据中心、分支机构、云资源和移动用户）创建一个网络。例如，SD-WAN 设备支持物理边缘，而移动客户端和无客户端浏览器则可以方便地连接用户。

- **遍布全球**：为了确保全面的网络和安全功能随处可用，并向所有边缘提供最佳体验，SASE 云必须遍布全球。因此，Gartner 指出，SASE 云必须扩展其分布范围，才能向企业边缘提供低延迟的服务。

这些特征能够很好地定义 SASE。除此之外，CATO 还分析了 SASE 不应考虑的方面：电信公司托管的网络服务。虽然电信公司托管的服务看起来像是统一、安全的云网络，但实际上是由点服务集成的。电信公司擅于向最终客户隐藏所提供网络解决方案的复杂性；但是，延迟、管理成本和潜在中断问题仍然存在。此外，这些间接费用已计入托管服务费用中，这使得电信公司托管的网络服务比 SASE 云服务更昂贵。

根据 Cato 的说法，SASE 提供了一种使用流量处理引擎的、基于云的单通道架构。该引擎能够处理来自任何边缘站点、云和移动用户的流量。在将流量转发到目的地之前，SASE 能够根据丰富的背景信息，应用所有网络优化、安全检查和策略。由于所有功能都融合在一起，因此 SASE 云更加精简。与其他网络和安全方法相比，它能够更快地处理流量，且具有低延迟和更多背景信息。

Cato 希望站在这一趋势的最前沿，并进一步重新定义市场。“自 Cato 成立以来，我们一直致力于将网络和安全融合到云中，创建一个全球性的云原生架构，以连接并保护所有位置、云资源和遍布全球的移动用户。” Cato Networks 首席执行官兼联合创始人什洛莫·克莱默（Shlomo Kramer）说。

Cato 不是唯一一家追求 SASE 概念的供应商。其他网络安全和网络供应商对此也颇有兴趣。Barracuda Networks 和 Zscaler 就是另外两家认可 SASE 价值的公司。

在公布其 CloudGen 防火墙最新功能的公告中，Barracuda 肯定了 SASE 的价值。该公司很快认可了 Gartner 的观点：“客户对简单性、可扩展性、灵活性、低延迟和全面安全性的需求迫使 WAN 边缘和网络安全市场融合，从而创建了安全访问服务边缘（SASE），主要采用基于云、‘即服务’的交付模式。”

在第 8 版 CloudGen 防火墙中，Barracuda 增加了自动化功能，以简化部署并提供可视性

和可控性，便于成功实施。“SD-WAN 管理可能会很复杂。许多 SD-WAN 产品需要数天的时间进行部署；如果配置不当，就会引入漏洞。”Barracuda Networks 安全副总裁克劳斯·格里(Klaus Gheri)表示。他指出，CloudGen 防火墙是与公共云基础架构集成的一体化 SD-WAN 解决方案。

基于 SASE 思想，Zscaler 实现了在云中集成网络和安全的飞跃。该公司在 9 月 10 日的盈收电话会议上讨论了 SASE 的重要性。Zscaler 董事长兼首席执行官杰伊·乔杜里（Jay Chaudhry）说：“SASE 远远优于采用 SD-WAN 的‘多协议标签交换’（MPLS），或采用云技术或零信任原则的硬件设备。”乔杜里补充说，企业正在认识到 SASE 的重要性。“随着世界朝着 SASE 模式迈进，传统网络安全供应商多年的犹豫之后，正在接受 Zscaler 对云安全的愿景。”

很明显，在上述三家供应商达成一致的情况下，Gartner 的预言即将实现——SASE 可能是云中网络和安全的未来。它的研究信号表明，网络和云服务提供商应准备好迎接该技术。

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，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、超过十五亿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