简译版

IT 安全的未来：条条大路通云中

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 future of IT security: All roads lead to the cloud		
原文作者	达伦·菲尔德斯（Darren Fields）	**原文发布日期**	2021 年 3 月 18 日
作者简介	达伦·菲尔德斯是 Citrix 欧洲、中东和非洲（EMEA）区域云网络副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/03/18/cloud-based-security-strategy/		
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		
摘要	Gartner 预测，IT 安全措施也将迁移到云中。Gartner 将此称为“安全访问服务边缘”（SASE）。这意味着，用于保护分布式资源的功能将与用于加速远程访问的功能合并，以创建统一的云服务。Gartner 的分析师指出，到 2024 年，将有 40% 的大型企业采用 SASE 策略。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

IT 安全的未来：条条大路通云中

达伦·菲尔德斯

2021 年 3 月 18 日

越来越多的应用程序（以及工作流和整个业务流程）被迁移到云中。分析师预测，IT 安全措施也会进行云迁移，这会引发一系列问题。

疫情期间，公司必须有能力向员工赋能，使其能够在任何地方（当前是在家中）工作。否则，公司就会面临业务中断的风险——不仅“禁足令”会导致业务中断，火灾、洪灾或公司总部附近发生的一些重大事件也会导致业务中断。

长期以来，公司并未将弹性恢复能力作为远程工作的重点。公司允许员工进行远程工作，是因为这样可以加快工作流程，提高生产率，同时使员工更好地协调工作和生活。在疫情爆发之前，越来越多的员工就已经开始从家中、酒店、机场或火车上远程访问公司资源，这就是原因所在。

越来越多的资源和数字工作场所开始迁移到云中。最近，我们对英国警队采用云技术的情况进行了调查。结果显示，云迁移不仅发生在私有部门，也发生在公共部门。2020 年末的数据显示，自 2019 年以来，使用混合云环境的英国警队已翻了一番——目前，近一半的警队（47%）都采用了这种模式。

Gartner：安全措施将迁移到云中

Gartner 预测，IT 安全措施也将迁移到云中。Gartner 将此称为“安全访问服务边缘”（SASE）。这意味着，用于保护分布式资源的功能将与用于加速远程访问的功能合并，以创建统一的云服务。Gartner 的分析师指出，到 2024 年，将有 40%的大型企业采用 SASE 策略。

但是，我们不能将 Gartner 的预测直接应用于每个地区，因为有些地区更倾向于所谓的“过度谨慎”。此外，Gartner 的客户群是大型企业，而非中型公司。有些公司花了很长时间才进行了云迁移，所以可以肯定地说，云安全服务的广泛接受也将需要很长时间。毕竟，对数据安全和数据主权的担忧减慢了云产品的接受度。

根据 Gartner 的说法，通过 SASE 进行的云安全措施，包括保护云访问和连续监控终端设备以识别与安全性有关的异常等，这些措施直接影响业务运营。Gartner 的预测在逻辑上颇具说服力，很清楚地描绘了云迁移的路径：鉴于云具有敏捷性、扩展性和高服务可用性等优势，随着越来越多的业务应用迁移到云中，借助云来管理安全基础设架构是完全合理的。

因此，云将不可避免地受到关注。数字化最终意味着：工作将会迁移到云中、不再与地理位置相关，对工作的保护措施也会迁移到云中——这不仅是出于弹性恢复能力的考量，也是为了提高生产力。因此，企业应尽早设计一个面向云未来的，包括所有必要安全功能的远程工作策略。

重要的是 ,远程工作场所和安全构建块都能够按照公司的数字化策略所设想的方式和步调迁移到云中——这需要逐步进行，无法一步到位。

在古代，人们曾说过“条条大路通罗马”；而如今，条条大路通云中（安全基础架构的道路也是如此）。不过，这些道路不再是崎岖的罗马道路，而是多车道的数据高速公路。因此，只要公司精心规划了路线（深思熟虑的分布式工作概念和匹配的安全策略），就可以以自己想要的速度在自己的车道上实现其数字化目标。

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