Akamai

白皮书

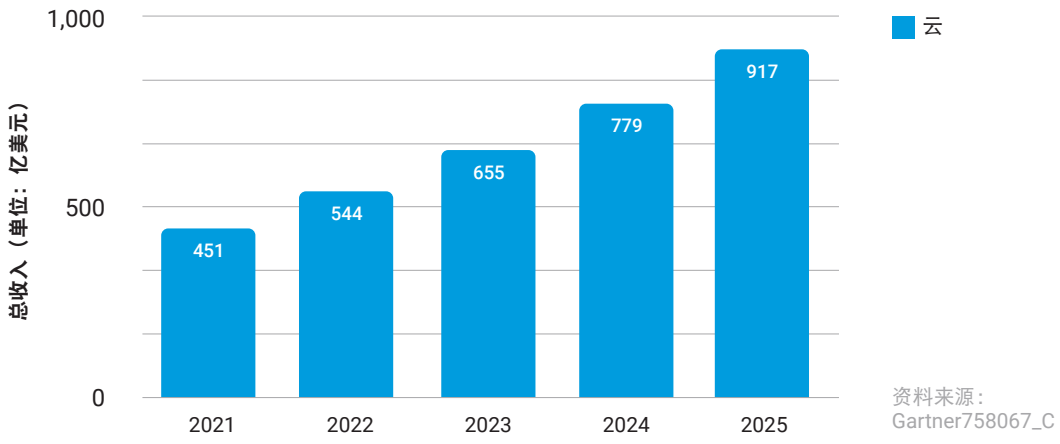
为微分段铺平道路：

在混合云中实施微分段的策略指南

云技术预计会进一步发展

在过去十年间，企业计算领域最大的变革或许就是海量数据和数据处理迁移到云端，更准确地说，是迁移到多种云平台。越来越多的企业正在迁移到公有云，而且所采用的通常是公有云与私有云混合式数据中心架构。与此同时，他们还在利用基础架构即服务 (IaaS)，以求进一步提高敏捷性。科技分析机构 Gartner 预计，到 2025 年，潜在细分市场中将有一半稍过的 IT 支出从传统解决方案转移到公有云。而在 2022 年，这一比例为 41%，到 2025 年，收入中投入到公有云的总开销预计将超过 9000 亿美元。[1]

“云”与“多云”之间的区别并非微不足道。企业越来越多地采用多云平台和服务提供商。有一点确切无疑：“企业数据中心是一个安全的物理空间”，这种想法即将被彻底淘汰。现代数据中心越来越多地采用异构环境和技术，结合运用本地设施、私有云和公有云 IaaS 提供商环境内的物理服务器、虚拟机和容器。这种异构安装也并非一成不变——企业会根据流量水平和处理需求，不断在各种本地和云环境之间转移数据和工作负载。



全球公有云服务收入预测（单位：亿美元）

更高的复杂性引发新的漏洞，造成攻击面扩大

云客户无疑可以受益于 IaaS 更高的灵活性、弹性和可扩展性——这些优势也是云技术如此吸引人的主要原因。但这些优势也伴随着代价：管理复杂性大幅度增加、无法监测多个环境中的工作负载，进而造成企业无法清晰了解网络安全环境。由于与多家云提供商合作，安全团队必须应对多种不同的安全标准和能力。专为本地服务器和端点设计的传统安全工具根本无法驾驭云的庞大规模和复杂性。IaaS 供应商提供的较新工具在其自己的环境中或许比较有效，但在多供应商基础架构中，其价值并不高。

此外，即使在这个虚拟化和“软件定义一切”的时代，安全理念（以及大部分相关投资）的基础依然是在入口点拦截攻击。这绝非贬低外围防御机制，在 IT 安全堆栈中，外围防御依然有着举足轻重的意义，只是在外围不断变化的今天，其效果大打折扣。数据和工作负载在公有云、私有云和本地数据中心之间来回移动，访问这些数据和工作负载的用户越来越多地在远程地点办公，而且其所在地点不一定具备适当的安全控制措施。

每年报告的数据泄露事件数量惊人，这足以让我们认识到，狡诈的攻击者几乎可以随心所欲地突破外围防御。在攻破外围防御后，他们看到的是相对扁平化的网络环境，内部资产几乎不设防。多云基础架构确实给企业提供了充分的灵活性优势，但伴随而来的是更高的管理和保护复杂性，以及呈指数级增加的攻击面；由于服务器之间的通信几乎不受控或者仅受到很少的控制，每一台服务器本身都是一个攻击面。因此，攻击者可以潜藏更久，借助东西向流量工作负载实现横向移动，从而找到您最关键的资产。

网络分段是一种广为人知的成熟安全实践，但考虑到当今动态多变的 IT 基础架构、体量庞大的云环境，其执行难度极大，因为工作负载会在不同分段之间通信和迁移。企业云客户已经认识到，他们需要进一步对应用程序和工作负载进行分段，以便实时地严格管控通信流，并及时检测和阻挠数据中心内的威胁，避免其造成任何破坏。我们需要找到一种解决方案，它应该能跨基础架构边界一致地工作，降低安全复杂性，缩小整体攻击面，让安全团队能够更快地检测到更多威胁，并限制其扩散。

这就是微分段的意义所在。

微分段定义

Gartner 对微分段的定义是：“在虚拟数据中心内为保证安全性而实施隔离和分段的过程”。此外，微分段可以“降低高级攻击在企业数据中心内横向扩散的风险，助力企业在本地和云端工作负载中执行一致的分段策略”。[2]

微分段的典型工作方式是围绕个别应用程序或应用程序分组建立安全策略，而不考虑它们驻留在混合数据中心内的什么位置。这些策略规定了哪些应用程序和组件可以相互通信，哪些不可以。因此，任何未经授权的通信尝试都是威胁的即时信号。在理想情况下，微分段技术不受基础架构限制，这样当应用程序在云环境中移动时，安全策略就可以继续保护其对应的应用程序。

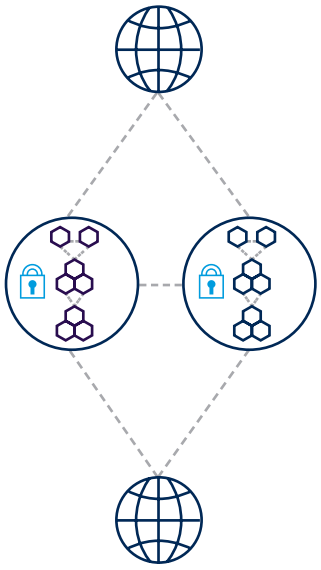
分段解决方案的领域

基础架构分段

保护特定基础架构内的应用程序流量。

应用程序分段

保护应用程序与外部网络之间的流量。



微分段

制定相关规则，利用更多的上下文信息（例如进程级归因）保护应用程序内部的流量。

2 Gartner，《微分段技术洞察》(Technology Insight for Microsegmentation)，2017 年 3 月；“2017 年云安全流行周期”(Hype Cycle for Cloud Security 2017)，2017 年 7 月

实施微分段的理由

当今的数据中心有着动态多变的特点，这就要求企业将注意力从入侵防御和访问管理转移到工作负载和应用程序本身。而这样的转移似乎正在加速。早在 2017 年，Gartner 就已经注意到一种趋势：“越来越重视服务器工作负载的保护，防范高级针对性威胁绕过传统安全边界和基于签名的防护措施。这些攻击通常有着牟取经济利益的动机，采用入侵服务器和应用程序工作负载的手段，设法获取敏感数据或交易信息”。[3]

微分段的一个主要推动因素就是保护关键任务应用程序和工作负载的需求。其初衷似乎只是维护自身利益或保证业务正常运转，但在许多情况下，这也是为了遵守安全政策和监管要求。

安全团队需要设法减少数据中心内不断扩大的攻击面，也就是要减少运行应用程序的服务器的漏洞。对于老练的攻击者而言，基于签名的拦截或应用程序允许列表等传统验证技术不堪一击。微分段让团队能够设置并执行严格、精细的访问和通信策略。它还能加强应用程序流的监测能力，支持团队更好地评估其安全态势。

您是否需要微分段?

您只要回答几个简单的问题，就能确定是否需要微分段。

- 您所在的行业是否受监管，或者您是否需要遵守有关数据和交易安全的法规?
- 您是否拥有工作负载跨越多个云平台的混合式基础架构?
- 您是否在虚拟机或容器中运行应用程序?
- 您是否感觉无法了解并掌控工作负载?
- 您能否随时判断数据中心是否存在威胁或是否正遭受攻击?
- 您能否通过单一管理平台掌控整个基础架构的安全性?

微分段之路上的四大障碍

针对当今动态多变的数据中心，安全专家普遍认为微分段势在必行，但高效、成功地实施微分段为何如此困难？尝试使用传统工具实施微分段的企业通常会遇到四大障碍：

1. **缺乏进程级监测能力**
   这可能是您遇到的第一个障碍——无法监测，就无从保护。微分段的要义在于保护单个应用程序、应用程序分组及工作流进程。安全团队需要监测实际的东西向流量，并在相应上下文中加以了解。大多数工具都无法实现这样的深度。

2. **缺乏混合多云支持**
   微分段安全策略必须能够在本地环境和公有云环境中轻松扩展，并跟踪来回移动的工作负载。专门针对特定环境设计的工具在混合环境中效果不佳。

3. **不够灵活的策略引擎**
   如前所述，当今的数据中心并非一成不变。安全措施也是一样——“只需设置一次”的思路已经不再适合当今世界。遗憾的是，云提供商的现有工具不具备必要的灵活性，无法持续为规则调整范围、执行测试并加以优化。在需要多种策略工具的混合式基础架构中，这种挑战要更加复杂。

4. **未集成能力互补的控制措施**
   如果实施得当，微分段不仅能保护进程，还能侦测到攻击。但功能单一的微分段工具通常不包括入侵检测功能，这迫使用户集成多种工具，并设法确保其有效协作。这种东拼西凑的方法很可能失败。

项目不成功并非例外，而是常态

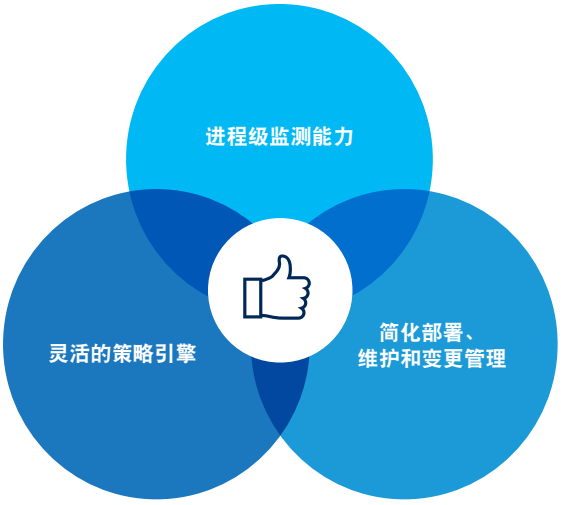
大多数微分段项目往往会经历漫长的实施周期，成本居高不下，还要耗用大量的资源，最终也无法达成目标，考虑到这些障碍的存在，这种结果并不令人意外。由于缺乏监测能力，企业往往难以确定需要分段的目标和分段的程度。他们可能要花费好几个月的时间制作电子表格，为进程级通信制定错综复杂的规则，根本无法发现进行应用程序分组并简化策略的机会。他们往往会出现“过度分段”的错误，即设置过于分散的策略，导致安全机制的复杂性过高，违背了降低这方面复杂性的初衷。正如 Gartner 所指出的那样：“……超过 70% 的分段项目会因为过度分段而对初始设计进行返工”。[4]

过度分段可能造成应用程序运行速度缓慢，最终拖慢业务的发展步伐。但如果矫枉过正，也可能出现“分段不足”的问题，最终损害企业的安全态势。

实现成功微分段之旅的策略

微分段的实施之路并非一片坦途，在您发现、了解和控制环境中的应用程序通信流时，一定会遇到许多曲折。安全团队在制定安全策略时需要保证灵活性，以确保在不破坏应用程序的情况下可以持续整合新的更改或新增内容。许多解决方案提供的策略创建引擎都不够灵活，迫使安全团队在未做好充分准备的情况下实施不完善或无效的规则。

简单地说，为确保成功实施，企业需要克服或避开四大主要障碍，避免过高的复杂性，并通过阶段式方法降低分段不足或分段过度的风险。这就要求找到一种能满足这些要求的解决方案：



- **进程级监测能力：**团队需要具备揭示、收集和规范所有东西向和南北向流量的能力；需要能自动发现应用程序并了解其通信要求的工具；需要具备对多个应用程序属性进行过滤的能力，以促进对可共享策略的资产进行标记和分组的过程。

- **灵活的策略引擎：**您应该能为大型分段设计高层次的最佳实践和合规规则，并为微分段设计更精细的规则。理想的解决方案应允许您从提醒开始，逐步过渡到强制实施。此外，它还应能让您制定适用于所有平台、设备和云环境的策略。

- **简化部署、维护和变更管理：**理想的系统应支持轻松部署、维护和按需修改规则。它应包含内置的入侵检测和事件响应功能。最终，您的策略应该足够完善，确保可以集成到自动部署 (CI/CD) 工具之中，从而为每个新推出的应用程序实施。

理想的解决方案功能

市面上固然有许多微分段工具，但并非所有工具都能帮您轻松完成这段旅程。为确保实施更顺畅、更成功，一定要确保您选择的解决方案具备这些功能：

- **自动化应用程序发现**，提供覆盖裸机服务器、虚拟机和容器的完整进程级监测能力
- 定义**强大且广泛的查询**的功能，以创建上下文相关的标签和对象组
- 具有智能规则设计的**灵活策略引擎**，可助您优化、加强和维护策略
- 集成的多方法**入侵检测能力**，支持更快地发现更多威胁，并限制其扩散
- **混合基础架构支持**——可配合各类基础架构（数据中心、公有云和私有云等）工作的平台

一款具备这些核心功能的解决方案可伴您走上实施微分段的成功旅程，帮您克服已知的障碍和复杂问题，也能帮您做好充分准备，从而在不牺牲安全性的情况下获享灵活混合云基础架构的所有业务优势。

相较于“封闭式”本地数据中心，混合式数据中心、多云平台和 IaaS 给企业提供了更高的灵活性、可扩展性和敏捷性。但它们也给应用程序和工作负载（网络攻击者实际针对的资产）造成了更高的风险和更多的漏洞。微分段被广泛视为保护云端工作负载的最佳实践，但企业很难正确实施微分段。好消息是，您不必一次到位。当今的先进解决方案与分阶段、分步骤的方法相结合，能帮您更轻松地实施微分段。这就意味着企业最重要的资产将获得更出色的安全保护。

如需进一步了解如何成功实施微分段，请访问 akamai.com/guardicore

1 “Gartner 表示，到 2025 年，关键细分市场的企业会将半数以上的 IT 开销转而投入云计算”(Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025)。Gartner，2022 年 2 月 9 日。

2 Heiser, Jay，“2017 年云安全流行周期”(Hype Cycle for Cloud Security, 2017)。Gartner，2017 年 7 月 17 日。

3 MacDonald, Neil，《云工作负载保护平台市场指南》(Market Guide for Cloud Workload Protection Platforms)。Gartner，2017 年 3 月 22 日。

4 Young, Greg，《以安全性为目标的网络分段的最佳实践》(Best Practices in Network Segmentation for Security)。Gartner，2016 年 7 月 28 日。

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、发展和转型。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2023 年 5 月。

扫码关注・获取最新CDN前沿资讯