
Akamai
破除有关微分段的
7 个误区

在扩大规模时，却又从小处考虑（即进行微分段），这似乎有悖常理，但在现代微分段解决方案方面，存在很多误解。

您是否认为，您会遇到网络停机或者在实施软件定义的部署时遇到操作上的困难？再好好想想。当涉及到细化控制时，您需要了解以下重要内容。

误区 1

我的 EDR 解决方案足以阻止勒索软件攻击

端点检测和响应（EDR）以及分段功能都是为了应对勒索软件攻击，但两者处于击杀链的不同阶段，并且采用了不同的方式。EDR 解决方案目的在于检测受监测的设备或端点中是否存在运行或执行的勒索软件。一旦检测到勒索软件，EDR 将退出程序并隔离设备，有时还可回滚任何已发生的加密操作。EDR 和分段是互补的：如果 EDR 没有检测到勒索软件，分段解决方案会将网络分段成孤立的分区，以限制攻击发生横向（东西向）移动。使用勒索软件时，必须发生横向移动，攻击者才能取得成功。分段将确保，设法从端点进行横向移动的攻击最终会遇到一个阻碍，这限制了初始感染的爆发区域。详细了解 EDR 和分段之间的区别。

1 小时 42 分钟：

这是攻击者在网络中获得最初立足点后开始横向移动的时间中位数

《2022 年 Microsoft 数字防御报告》

Akamai

误区 2

我已经在采用分段功能

分段并不是一个新概念，它只是变得更加复杂。几十年来，企业一直在使用由 VLAN、内部防火墙、ACL 和安全组拼凑而成的解决方案来对其环境进行分段。但是，这些传统方法还没有发展到可以满足现代混合和多云基础架构的复杂需求，因此，由于分段不够完善，造成了防御漏洞和盲点。

例如：传统防火墙没有绘制或评估工作流程依赖关系，因此，企业难以为应用程序、工作负载或用户确定分段。因此，企业被迫实施广泛的分段策略，这些策略过于宽松，很容易（*而且会很快*）导致危险的错误配置，而对这些错误配置进行故障排除的过程又十分困难，非常麻烦。

借助微分段，企业可以分段和执行的层级可达到第 7 层，这种覆盖范围远远超越了传统分段工具。

三年内可避免

200 万美元

的防火墙升级费用

(Forrester TEI)

Akamai

误区 3

微分段的实施和操作难度太大

现在是企业采用现代微分段技术的最佳时机，当下比以往任何时候都更需要这种技术。

在 Akamai Guardicore Segmentation 帮助下，通过使用基于软件的单一解决方案，在所有环境中（从数据中心和云，到基于容器的资产）实现分段，提供监测能力，并创建和执行策略，从而尽可能地提高运营效率。部署后，Akamai Guardicore Segmentation 会创建整个 IT 基础架构的动态可视化示意图，使安全团队能够实时查看活动现状以及活动的历史记录（细分至单个流程级别）。

利用这些针对应用程序行为的详细见解，随后可以通过直观的可视化界面快速创建细化的微分段策略。全局拒绝规则、关键应用程序安全围栏以及立即对大型环境进行分段的能力意味着，企业能够快速实现价值，并降低风险。

使用传统分段方法时，您缺乏监测能力，甚至不知道从哪里开始着手。

SecOps 生产率提高

↑95%

(Forrester TEI)

误区 4

微分段意味着应用程序和网络会出现停机

使用传统分段方法时，应用程序经常在子网或 VLAN 之间移动，导致出现停机，并破坏业务连续性。网络工程师和防火墙管理员不得不计划预定的停机、变更控制或维护窗口期，这增加了部署新服务或应用程序更新所需的时间。更糟糕的是，这些延迟可能导致资产暴露在威胁之下并出现漏洞，进而导致风险增加。

另一方面，软件定义的分段会将安全措施与底层基础架构和操作系统分离，因此可以独立执行分段，而不影响网络或应用程序。当有事件发生时，微分段方法只会阻止攻击媒介，而不是完全隔离受影响的机器，这可以减少对业务造成的负面影响。

您也可以在警报模式下部署微分段，以便在实时生产环境中测试策略，而无需面临停机风险。结论：现代分段解决方案应能兼顾更出色的安全性和业务敏捷性。

误区 5

微分段并没有覆盖我的物联网或 OT 环境

您知道吗？对于无法运行基于主机的安全软件的物联网和 OT 设备，可以采取 Zero Trust 策略。

对于诸如经过物理隔离的端点等无法运行代理的设备，我们的无代理分段功能弥补其间所存在的防御不足，以消除监测上存在的盲点。这种扩展的覆盖范围对于具有许多联网（且易受攻击的）物联网设备和传统 OT 系统的医疗保健、零售和制造环境尤为关键。通过将无代理分段集成到您的网络基础架构中，您可以自动发现新设备，支持指纹识别和执行策略，以帮助抵御风险，同时在整个企业范围内加快向 Zero Trust 转型。

误区 6

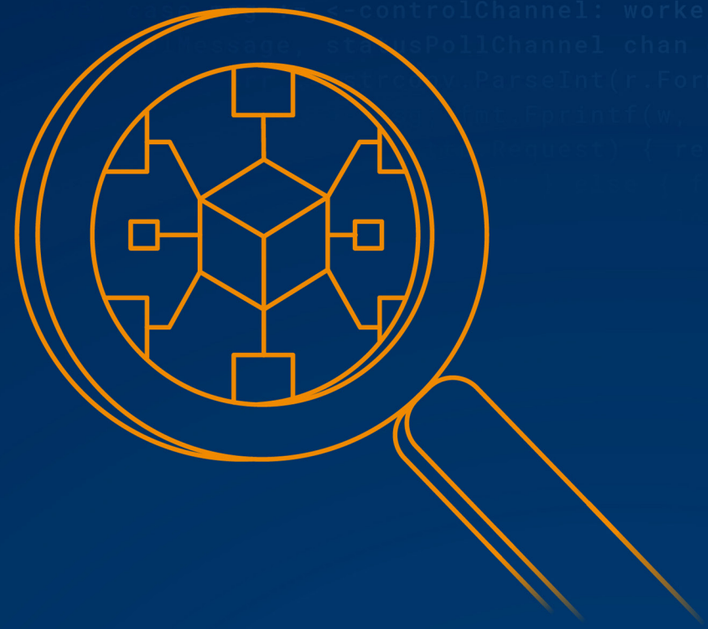
微分段代理增加了太多延迟

与微分段有关的一大误解是，它会增加延迟。

实际上，通过使用基于软件的分布式分段策略，而非强制所有流量流经特定的防火墙阻塞点，即可消除网络瓶颈。从设计的角度来看，Akamai Guardicore 代理经过高度优化，可与 Linux、Unix、Windows 操作系统和 MacOS 配合使用，并且不会消耗大量资源。

由于代理没有联机，因此它不会执行可能增加延迟的深度数据包检查。

相反，Akamai Guardicore 代理只需从数据包标头中获取最低程度的信息，即可针对客户环境提供丰富的见解。如果您希望提高速度和性能，请放心，您可以两者兼顾。



误区 7

微分段意味着，企业要聘用全职员工，而这种员工是不可能找得到的

CISO 感受到了“少花钱多办事”带来的压力，考虑到这一点，安全解决方案必须减轻防御者的负担，而不是进一步消耗稀缺的内部资源。

传统分段方法（比如管理防火墙和 VLAN）需要实施一个痛苦的多步流程，该流程涉及到许多团队，这些团队分别负责交换、路由、防火墙的实施和安全策略的创建。传统防火墙的实施平均需要 14 至 22 周。所有这些因素都增加了项目所需的时间，使企业承受了巨大的人力成本和运营开销。

相比之下，Akamai 的软件定义解决方案平均只需要两周的时间即可部署，而且只需要一名全职员工。通过添加 Akamai Hunt（我们的托管式威胁搜寻服务），我们可以监测您的环境中出现的攻击、横向移动和异常攻击行为，从而节省您的时间和资源。

如今，很难招聘到网络人才，而要挽留他们，甚至更难。现在应当让防御措施为您的企业提供助力，*而不是阻力*。

关键统计数据

106%

经证实，12 个月内的投资回报率高达 106% 左右

(Forrester TEI)

Akamai 如何为您提供帮助

Akamai Guardicore Segmentation 是一种基于软件的微分段解决方案，为实施 Zero Trust 原则提供了简单、快速和直观的方式。它使您能够通过精准的分段策略、IT 环境内活动的可视化以及网络安全警报来防止网络中的恶意横向移动。Akamai Guardicore Segmentation 可在您的数据中心、多云环境和端点之间发挥作用。它不但部署速度比基础架构分段方法更快，还能为您提供出色的网络监测和控制能力。

了解 Akamai Guardicore Segmentation 如何实现细化的保护、深入的监测能力和一致的大规模安全策略执行，以保护您的敏感数据。