对比指南

Akamai Guardicore Segmentation 与传统微分段解决方案的对比

出色的监测能力

要了解您的环境中发生了什么，必须具备对工作负载间通信情况的监测能力。真正有效的监测能力意味着，企业在任何时候都能够结合全面的背景信息了解各工作负载的当前状况。此外，要快速、有效地制定策略，资产和规则的分组及筛选功能是必不可少的组件。

Akamai	传统微分段
轻松监测整个网络环境 Akamai Guardicore Segmentation 代理是一种基于主机的防火墙，可在现代操作系统和传统操作系统上运行，能够对 Windows 和 Linux 操作系统的网络流进行全面的进程级和服务级监测，监测范围还可以覆盖 MacOS 端点。	**对于旧有操作系统，仅能提供部分监测能力** 无法监测 Windows 2002 之前的 Microsoft Windows 系统。这是因为传统微分段解决方案代理依赖于 Windows 防火墙，而该防火墙功能是从 Windows 2002 版之后的系统才开始提供。对于 Linux 系统，适用的代理仅支持 L4 监测能力。
无比丰富的背景信息 谈到监测能力，拥有正确的背景信息和详情至关重要。我们的解决方案不但收集流数据，还会收集进程信息、文件、所安装的补丁程序版本等重要背景信息。	**背景信息极其有限** 仅收集有关通信流和机器的信息，缺少进程和文件等重要背景详情。因此，了解应用程序依赖关系的过程要更耗时费力。
不受限制的标签类型或数量 我们不限制您可以使用的标签类型或数量，因而可以实现灵活性并支持更多的应用场景。这样，您不必转换配置管理数据库 (CMDB) 和其他数据源中的现有标签。	**死板的标记功能** 传统解决方案使用固定的预定义添加标签层次结构，在您为应用程序添加标签时，不论环境要求和业务需求如何，都只能使用这些解决方案定义的一组标签。
由 AI 提供支持的添加标签功能 如果没有可靠的 CMDB，由 AI 提供支持的应用程序检测和添加标签功能会帮助您识别相应的应用程序，并自动为它们分配正确的标签。	**没有 CMDB？那谁都无计可施…** 由于采用手动添加标签功能和预配置的标签层次结构，在企业没有可依赖的 CMDB 时，添加标签过程会变得极其复杂。

Akamai

行业领先的覆盖范围

优秀微分段解决方案的核心要素之一是能够保护关键资产，与它们部署在传统还是现代机器上、Windows 还是 Linux 上无关，与它们部署在本地还是虚拟机或容器上无关，而且与从何处对它们进行访问也无关。

Akamai	传统微分段
全面支持 Windows 和 Linux Akamai Guardicore Segmentation 代理在所有 Windows 和 Linux 操作系统（无论新版系统还是旧版系统）上都受支持，因为我们的解决方案与底层基础架构无关。	**有限的 Windows 和 Linux 支持** 策略实施依赖于 Windows 防火墙（对于 Windows 环境）和 iptables（对于 Linux 环境）。这必然意味着对一些旧版 Windows 操作系统只能提供有限保护或无法提供任何保护，并且对于 Linux 环境无法提供 L7 进程级规则。
全面的容器支持 提供对容器化环境的全面监测能力，同时能够利用容器网络接口 (CNI) 控制进行实施。	**有限的容器支持** 实施依赖于 iptables 和来回策略计算，并且在容器环境内不具备扩展能力，因而会造成延迟和停机。

迅速制定简单易用的策略

优秀的策略引擎允许您以极少数量的规则清晰表达意图，并且不会对策略所用语言进行强制限制。它还会提供自动化机制和向导功能，从而最大限度地减少策略的管理工作量。

Akamai	传统微分段
允许和拒绝 我们支持将规则加入允许列表和拒绝列表，也支持除这两种做法以外的任何做法。这让安全与 IR 团队可以迅速响应任何安全情景，而无需先将每个合法的通信流加入允许列表。	**提供允许列表功能，但对拒绝规则的支持有限** 由于采用安全但耗时的允许列表模式，传统分段解决方案无法自动响应需要快速拦截的已知威胁。
适合各种使用场景的策略模板 提供多种开箱即用的模板和策略构建工作流程，可用于各种常见场景，例如抵御勒索软件、为应用程序设置安全围栏、执行环境分段等。模板有助于节省时间并减少人为错误。	**有限的模板** 所支持的分段模板大多适用于 Microsoft 环境。不支持适用于常见分段应用场景（例如，安全围栏设置以及勒索软件抵御与修复）的模板。
丰富的策略条件 策略条件可包含来源、目标、端口、协议、进程、服务（例如，勒索软件常用的任务计划程序）、用户以及完全限定域名 (FQDN)。	**有限的条件** 对于 Linux 操作系统不提供 L7 进程级策略，而且不具备任何基于各项 Microsoft Windows 服务构建策略的能力。

安全至上

抵御勒索软件等高度复杂的安全威胁需要全面的安全方法。在美国国家标准语技术研究院 (NIST) 和白宫给出的指示中，分段属于基本响应措施，但必须有集成化安全和入侵检测方法，才能保证您的企业安全无虞。

Akamai	传统微分段
勒索软件防范与抵御 Akamai Guardicore Segmentation 针对攻击杀伤链的所有阶段（防范、遏制直至抵御）提供了开箱即用的模板。	**无勒索软件模板** 在使用开箱即用的模板拦截勒索软件攻击方面，传统解决方案的能力有限。
查询端点以实现威胁检测并确保合规性 通过我们基于 osquery 的工具 Insight，您可以实时查询服务器和端点，以确保合规性并检测恶意软件。	**无实时检测能力** 传统解决方案无法检测数据中心内的实时恶意活动。
欺骗功能 Akamai Guardicore Segmentation 代理依托一项享有专利的技术，可将被拦截、失败的会话重定向到动态欺骗引擎，以完成进一步的分析和隔离。	**无隔离能力** 传统解决方案不具备欺骗功能，也不具备使用已知入侵指标 (IOC) 检测或隔离机器的能力。
托管式威胁搜寻团队 Akamai 提供托管式威胁搜寻服务，可为您的安全团队提供有效助力，让您的企业抢先一步抵御最新威胁。	**无威胁搜寻服务** 传统供应商无法提供基于其解决方案构建的威胁搜寻服务，而这项服务在面对勒索软件和恶意软件升级时会成为一项关键的差异化优势。
威胁情报防火墙 为了防范已知恶意行为，Akamai Guardicore Segmentation 可利用自动防火墙规则拦截恶意 IP、文件和哈希。	**无威胁数据源** 传统解决方案不具备类似的功能，无法拦截来自已知恶意 IP 和 URL 的访问，也不能阻止访问此类 IP 和 URL 的企图。

运营或性能与延迟

为了保证分段项目的成功，低延迟至关重要。因此您需要能扩展策略，也就是说添加更多规则、按资产添加标签或是添加其他策略对象，同时不能造成额外的延迟。

Akamai

延迟优化型引擎

我们的分段引擎专为大规模情景而打造。这是通过经优化的过滤机制实现的，其设计可确保延迟时间受策略大小的影响相对较小。

传统微分段

规则数量的增加会造成延迟增加

随着规则数量和大小的增加，代理的延迟会增加。Linux iptables 并非为企业级东西向流量规模扩展而打造。因此，会产生随策略大小增加而增加的显著延迟。

如需详细了解 Akamai Guardicore Segmentation，或者申请个性化产品演示，请访问 akamai.com/guardicore。