



# 高影响分段服务

Akamai 助力降低网络安全的复杂性和风险

## 前言

---

对于企业来说，保护本地数据中心和公有云环境中的关键资产比以往任何时候都更加重要。面对快速演变的威胁形势，要想与新的应用程序部署模式保持同步，越来越需要专业知识和技能的支持。Akamai 服务专家将助您一臂之力，帮助您将对安全产品组合的投资转化为切实可见的业务成果。

Akamai 微分段服务团队的安全专家具有丰富的实战经验，并接受过广泛的培训，曾在私营企业和军事情报部门任职。我们提供一系列灵活的服务，让企业内部的 IT 和安全团队可以轻松获得这些专家的支持，确保从数据中心到云皆实现卓越安全性。





## 客户旅程

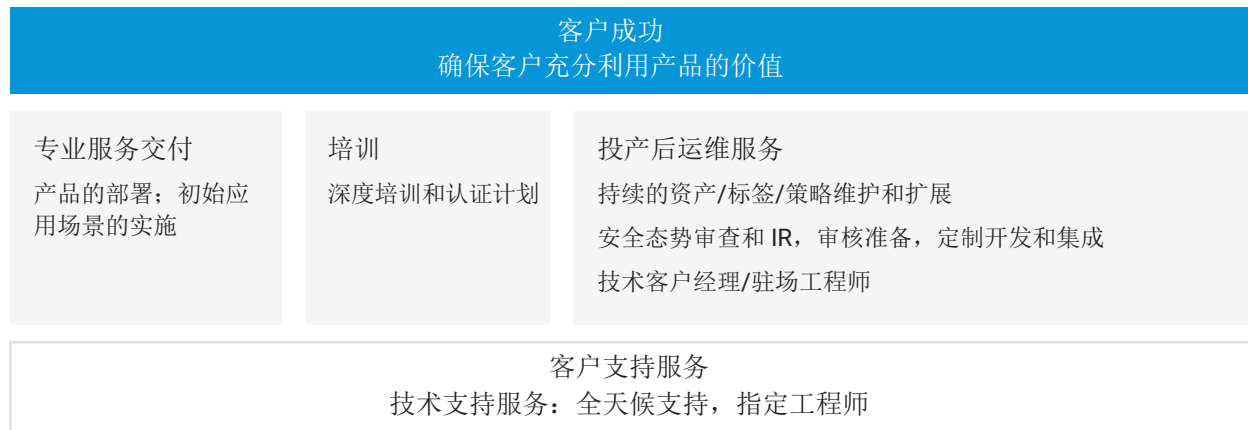
客户购买 Akamai 产品后，即可享受我们的专业服务交付支持，从而轻松完成初始部署和配置。我们会帮助客户设置环境、定义资产和标签，并针对最初的几个应用场景实施相关策略。

然后，我们会对具体使用这些解决方案的部分团队成员提供管理和工程方面的培训。

此外，我们还会提供投产后运维服务，帮助客户继续完善更多部署（定义更多资产和标签，以及针对更多应用场景实施相关策略），处理安全事件和改善安全态势，提供必要的控制和报告以供审核，并提供定制开发以促进与客户基础架构的集成。

在解决方案的整个生命周期中，我们广泛的支持服务将帮助客户解决可能发生的任何问题，而且我们的客户成功团队将确保客户充分发掘产品的价值。

### Akamai 微分段服务的客户旅程



## 专业服务交付

由安全架构师、项目经理和开发人员组成的综合团队将与客户的团队合作，共同实施 Akamai Guardicore Segmentation 平台。根据您的需求，Akamai 将提供一整套的可交付产品/服务，或指定一名固定服务期限的实施工程师。无论选择哪种方案，我们都会提供量身定制的服务，确保客户的关键资产受到保护。



## Jumpstart

---

如果客户需要加快部署 Akamai Guardicore Segmentation，但更愿意在专家的指导下自行实施和管理后续策略，可以选择 Jumpstart 方案。无论是对网络进行分段、隔离应用程序还是限制对服务器的访问，我们的工程师都将为客户设计并实现首个策略目标，并且随时提供指导，协助客户团队顺利实施后续的策略。

我们的团队还会与客户团队一起规划安全架构，理清任何应用程序的设计注意事项。这其中包括定义和记录标签策略、在平台中标记客户资产，以及正式创建和微调策略，为客户的应用场景提供支持。

Akamai 完成首次策略实施后，将来客户团队实施任何策略时，我们的工程师都将继续提供直接的帮助，并继续充当客户团队的外援成员，直到客户的部署目标得以实现。

## Extended Jumpstart

---

对于想要实现多重分段目标的企业来说，Extend Jumpstart 方案是理想的选择。Akamai 专家将与客户团队合作实施多种分段策略，加强对客户关键资产和珍贵资产的保护。

我们的团队将与客户团队一起规划安全架构，理清任何应用程序的设计注意事项。这其中包括定义和记录标签策略、在平台中标记客户资产，以及正式创建和微调策略，为多种安全措施提供支持。





## 常见的策略目标

无论是对网络进行分段、隔离应用程序还是限制对服务器的访问，我们的工程师都将与客户的团队合作，完成整个客户旅程中的每一步，确保客户资产得到可靠的保护。

在这项服务中，客户可以选择多个策略目标，或专注于特定的高优先级目标。我们的工程师将实施构成策略所需要的标签和规则，直到客户资产得到保护并达成客户预先确定的目标。

一些示例包括：

- 环境分段——除非明确允许，否则位于不同环境中的服务器将不能进行通信。
- 应用程序隔离——关键应用程序只能与明确允许的相关方通信。此外，允许内部应用程序之间进行通信。
- 应用程序微分段——仅在明确批准的情况下，才允许关键应用程序接收内部和外部流量（Zero Trust 策略）。
- “企业外”端点分段——处于企业网络保护之外的端点的攻击面将受到限制。Akamai Guardicore Segmentation 支持对企业网络内外使用不同的规则集。
- 服务器特殊访问权限——可实施服务器访问控制策略来实现相关目标，例如，将管理端口限制为仅跳板机可连接，或者根据来源的用户身份阻止对特定服务器的访问等等。
- 安全最佳实践的执行——通过实施阻止列表规则来执行网络安全最佳实践。

## 实施工程师

---

如果企业要实现大量的策略目标，通常更好的做法是与指定的工程师合作一段时间。我们的工程师可以帮助创建数量不受限制的策略，确保解决方案的成功实施。在企业网络需要完整的端到端分段时，理想的选择是让 Akamai 来为您的实施过程提供支持，以帮助您成功达成目标。

	Jumpstart	Extended Jumpstart	实施工程师
安装	✓	✓	✓
标签架构的安装	✓ 有限	✓ ✓ ✓	在固定期限内提供全面的实施资源，对应用场景无限制，可确保成功实现目标
关于整体安全态势的指导	✓ 有限	✓ ✓ ✓	
关于策略创建的指导	✓ 有限	✓ ✓ ✓	
实施策略应用场景	单一策略	多种策略	
终端用户培训	✓	✓	✓
通常持续时间	6 个月	12 个月	6-18 个月
根据需求选择合适的方案	客户或合作伙伴更愿意以内部实施为主；Akamai 仅实施初始应用场景	Akamai 实施多个应用场景和多种策略，并提供广泛的指导	客户或合作伙伴希望全面实施（多个应用场景），他们更喜欢在整个过程中探索和定义具体内容和方式



# Akamai 培训

---

Akamai 微分段认证培训为管理员 (GCSA) 和运维工程师 (GCSE) 提供成功完成相关维护和管理任务所需的必要技能和信息。

培训方法丰富多样，从基本的在线培训到讲师指导的认证培训，甚至私人专门培训（虚拟或面对面），都能满足客户和合作伙伴的需求。



## Guardicore 认证分段管理员 (GCSA)

我们为五个半天的培训计划为 Akamai Guardicore Segmentation 平台的用户提供必要的专业知识和技能，让他们能够熟练地执行平台上的各种操作。完成 GCSA 认证的学员将获得独立使用该平台的自信，能够实施并维护企业所需要的各类安全策略。

该课程涵盖 Akamai Guardicore Segmentation 的核心功能集，包括监测、标记、微分段和入侵检测。课程重点讲解该平台的功能行为和使用方法，指导学员掌握从平台初始配置到日常操作的各种技能。



## Guardicore 认证分段工程师 (GCSE)

我们为三个半天的计划为系统运维负责人提供必要的专业知识和技能，让他们能够熟练地执行与平台相关的管理任务和维护任务。

完成 GCSE 认证的学员将能够管理 Akamai Guardicore Segmentation 平台的整体运维。该课程涵盖的主题包括：平台和组件配置、与第三方工具的集成、平台运行状况检查、故障排除和常见的维护任务。

这两门课程都附带线上实操实验室，所有学员在课程有效期内都可以使用该实验室。每门课程结束时都会有认证考试。



## 企业支持与客户成功

Akamai 的企业支持计划旨在协助客户处理使用 Akamai Guardicore Microsegmentation 的过程中可能产生的各种问题。我们的支持部门将全年全天候提供服务，解决客户遇到的各种问题，并协助进行升级和修复。

我们的客户成功计划可帮助客户实现短期和长期的安全目标，同时充分利用平台的价值，尽可能提高投资回报。

## Elite 支持

Akamai 的 Elite 支持计划可以让企业优先获得专门指定、经验丰富的顶尖专家的支持。我们将指定一名熟悉客户数据中心和内部流程的高技能专家作为单点联系人，帮助客户团队加快响应和解决各类问题，让客户在软件分段解决方案中的投资充分发挥其价值。

	Premium	Elite
提供支持的时间段	全年全天候	全年全天候
不限制案例	✓	✓
升级和修复	✓	✓
电话、电子邮件、Slack 和门户	✓	✓
根本原因分析（按需提供）	严重级别 1	严重级别 1 和 2
由专门指定、经验丰富的工程师优先处理案例		✓ 指定的工程师在工作时间内提供服务
主动、持续的系统运行状况监控		✓
定制优化		✓ 每季度优化一次
定期提供问题总结和支持报告		✓ 每周提供问题总结； 每月提供支持报告
咨询天数		✓ 每年 2、4 或 6 个咨询日，具体取决于规模 (SKU)
根据需求选择合适的方案	部署规模较小；以需求支持为主	部署规模较大；需要对持续性问题进行更严格的控制



## 投产后运维服务

---

在完成针对最初几个应用场景的部署后，Akamai Guardicore Segmentation 产品便可为客户创造价值。

但是，产品需要持续维护和更新，才能充分发挥其潜在价值。这些工作包括：

- 更新部署（资产、标签、策略），以体现企业发生的变化
- 实施初始部署阶段未处理的其他应用场景（使用产品后发现的新应用场景、要处理的附加服务和/或应用程序等）
- 在企业内其他部门实施 Akamai Guardicore Segmentation，例如云网络和云应用程序。（新环境或留待第二阶段部署的环境）
- 部署到其他端点、物联网设备、虚拟桌面基础架构环境等
- 使用 Akamai Guardicore Segmentation 识别和管控安全事件（即，阻止网络中的横向移动）；可将系统连接到 Akamai 安全运营指挥中心，获取全年全天候监控和实时告警以及阻断支持
- 借助 Akamai Hunt、Akamai Edge DNS（用于保护 DNS 并防止分布式拒绝服务）和 Akamai Enterprise Application Access（用于访问控制和身份管理）获得增强的主动式安全防护
- 使用 Akamai Guardicore Segmentation 协助进行认证审核

这些服务应该由 GcSP 认证合作伙伴提供





## 技术客户经理和驻场工程师

Akamai 技术客户经理和驻场工程师是我们为企业指定的高级技术顾问，致力于满足企业各种潜在的复杂分段需求。我们的工程师在融入客户团队后，很快会成为客户 IT 环境的专家，帮助客户利用 Akamai Guardicore Segmentation 取得卓越成效。

专门指定的驻场工程师\*将融入客户团队，主动为客户的所有运维工作提供支持，帮助客户充分发掘 Akamai Guardicore Segmentation 的价值。

驻场工程师可以提供策略决策的指导，介绍产品中即将推出的新功能，规划（并协助执行）升级，以及实施管理业务审查，确保客户成功实现目标。

技术客户经理或驻场工程师还可以为客户监督和执行投产后运维服务。

*\*驻场工程师可以远程工作*

## Akamai Hunt: 托管威胁搜寻服务

Akamai Hunt 是 Akamai Guardicore Segmentation 的扩展，也是我们提供的托管威胁搜寻服务，可以帮助企业抵御隐蔽的威胁，更好地保护企业资产安全。

即使最先进的安全解决方案，也可能会漏掉某些异常攻击行为和高级威胁，Akamai Hunt 团队会持续搜寻这些攻击行为和威胁。有了 Akamai Hunt，一旦网络中检测到任何严重事件，客户团队会立即收到通知，并且我们的专家会与客户团队密切合作，修复任何遭到入侵的资产，快速解决出现的问题。

无论是着重检测并预防勒索软件、阻断高级持续性威胁、防范零日漏洞，还是改善常规 IT 安全状况，Akamai Hunt 都可以帮助客户充分利用 Akamai Guardicore Segmentation 带来的安全价值，而无需任何其他软件、代理部署或升级。



## Akamai Hunt 包含：

全天候专家人工分析——我们的网络安全专业人员来自广泛的领域，包括安全研究、进攻性安全、军事情报、红蓝对抗、事件响应和数据科学等领域。

真实威胁告警——为了避免疲于应对各种告警，Akamai Hunt 团队只会就真正的威胁向客户发出告警，从而完全避免误报。

专有搜寻工具——Akamai Hunt 专家定期开发高级威胁搜寻算法（比如用户和网络活动异常、可执行文件分析、日志分析等），以构建强大的工具集，实现快速检测和响应。Akamai Guardicore Insight 是一个基于 Qsquery 的强大工具，用于实时查询端点和服务器。该工具已包含在此项服务中，不需要额外付费。

具备丰富背景信息的威胁情报——我们的搜寻团队利用 Akamai Guardicore Segmentation 和 Akamai 的海量全球威胁情报，收集从 IP 和域到进程、用户和服务的各种入侵指标。

网络、云和端点监测——通过对 Akamai Guardicore Segmentation 部署点和 Akamai 全球传感器的数据（包括每天发送到 Akamai DNS 云的 7 万亿条 DNS 请求）进行整合分析，我们的团队能够全面监测企业网络环境中的活动。

即时通知和主动洞察——

- 检测到威胁后立即发送电子邮件通知
- 定期提供高管级威胁报告，其中包括分析统计数据和指标，让企业高管或董事会能够了解关注度高的攻击活动
- 与 Akamai Guardicore Segmentation 控制台集成，轻松管理事件

如需进一步了解 Akamai Guardicore Segmentation，  
请访问 [akamai.com](https://akamai.com)



Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。Akamai Connected Cloud 是一种大规模分布式边缘和云平台，可使应用程序和体验更靠近用户，帮助用户远离威胁。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 [akamai.com](https://akamai.com) 和 [akamai.com/blog](https://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 9 月。



扫码关注 · 获取最新 CDN 前沿资讯