AKAMAI 解决方案简介

通过 Akamai Guardicore Segmentation 保护 AWS 中的工作负载

现在，众多企业在继续使用 Amazon Web 服务 (AWS) 中的 PaaS 资源，有很多企业正在将关键工作负载迁移至公共云。虽然迁移至公共云会给这些企业带来诸如成本降低、可扩展性和性能提升以及业务敏捷性提高等好处，但在向云端迁移过程中，伴随而来的安全问题也越来越严峻，例如：

新的工具集

在云环境中运营需要一整套全新的安全控制措施。这些控制措施需要支持云中的 AWS 以及通过 AWS Outposts 在本地部署的资源，同时还要支持混合云工作负载。现有的云安全组可能足以保护 AWS 云中的资产和资源，但这些控制措施无法保护其他环境中的相关资产或资源。这意味着您的团队必须管理多个安全工具，而这可能导致潜在的安全漏洞。

新的安全运营模式

按照 AWS 责任分担模式，在云端或本地使用 AWS 资源意味着 Amazon 仅负责保护其所有 AWS 云服务的基础架构。但在这些实例上安装的任何应用程序软件或实用程序，以及安全组配置，完全由用户负责。不仅如此，客户还要负责保护和监控流量（包括南北向和东西向流量），以及部署控制措施以检测、预防和应对入侵。

基础架构监测与控制能力降低

AWS 环境的一些优势在提升其运营吸引力的同时，可能导致企业无法充分地控制和监测其分布在多个 AWS 帐户、虚拟私有云 (VPC) 和网络安全组，以及更广泛的企业混合生态系统中的资产。

关键优势

- 一款端到端的解决方案能够保护 AWS 中的工作负载（包括 PaaS 资源），帮助 DevOps 和安全团队将有限的资源集中于核心任务，而非数据中心安全管理
- 管理和实施严格的微分段策略，这些策略不仅覆盖 AWS，还覆盖本地资产甚至跨公共云的资产
- 可靠检测策略违反情况并实时对其做出响应
- 通过使用声誉分析和实时动态欺骗等多种入侵检测和防御方法，保护环境免受潜在的入侵威胁

面向 AWS 安全的 Akamai Guardicore Segmentation

Akamai Guardicore Segmentation 可针对 AWS 云环境、本地 Outposts 和混合环境中运行的工作负载和 PaaS 资源，提供统一的监测和策略实施解决方案。该产品可提供微分段和应用程序级监测功能，以及漏洞检测和响应功能。

自动发现和监测能力

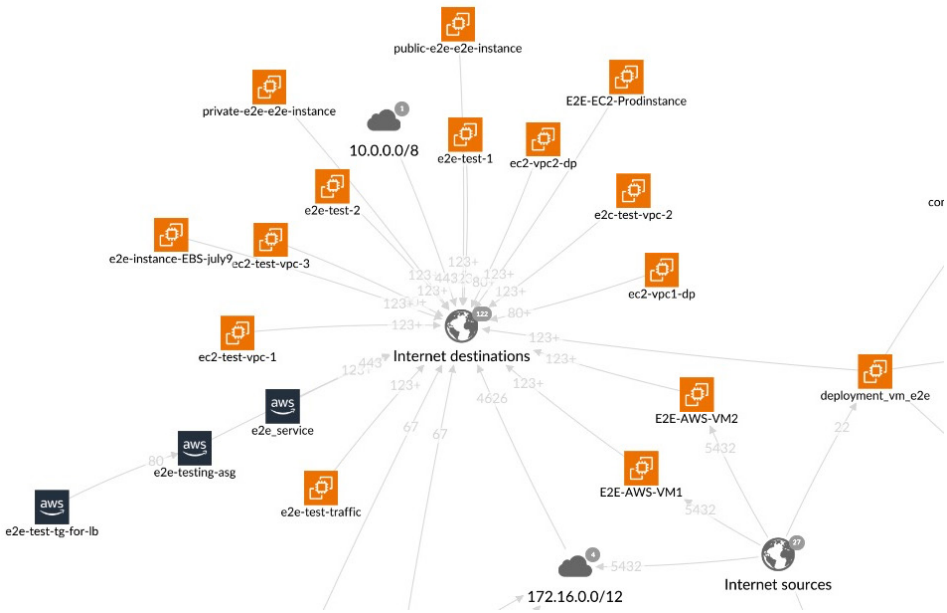
- 自动直观显示应用程序、资源及其通信流量
- 快速了解应用程序行为并为其设定基线
- 生成应用程序依赖关系映射，实现细化至进程级别（第 7 层）的监测能力

强大的分段与实施能力

- 仅需几分钟即可定义分段策略
- 自动提供策略建议
- 智能标记和分组，便于在复杂环境中轻松导航

威胁检测与事件响应

- 无需配置；从第一天起即能体验到价值
- 多种检测方法，覆盖各种类型的威胁
- 动态欺骗提供全方位网络覆盖



使用 Akamai Guardicore Segmentation 监测和保护 AWS 中的应用程序和资源

> 通过选择 Akamai Guardicore Segmentation，我们能够填补微分段和应用程序级可见性以及漏洞检测和响应的关键安全缺口，将 AWS 和本地服务器纳入覆盖范围。
>
> **— DevOps 团队负责人**
> **生物技术公司**

无缝保护 AWS 中的工作负载和 PaaS 资源。要了解更多信息，请访问 akamai.com/guardicore。