AKAMAI 解决方案简介

混合云环境的分段

通过对云基础架构实施分段来遏制攻击

随着应用程序和工作负载不断向云端迁移，安全和云团队面临着越来越多的挑战，其中之一就是将分段技术和 Zero Trust 原则扩展到云环境中的应用程序和工作负载。借助 Akamai Guardicore Segmentation，企业无需安装代理即可减少攻击面，并遏制针对公有云环境中应用程序和工作负载的攻击。这是因为该解决方案能支持自动应用程序发现、云数据流全面监测、精确的分段策略和网络安全告警，而且所有这些都能在单一管理平台上实现。

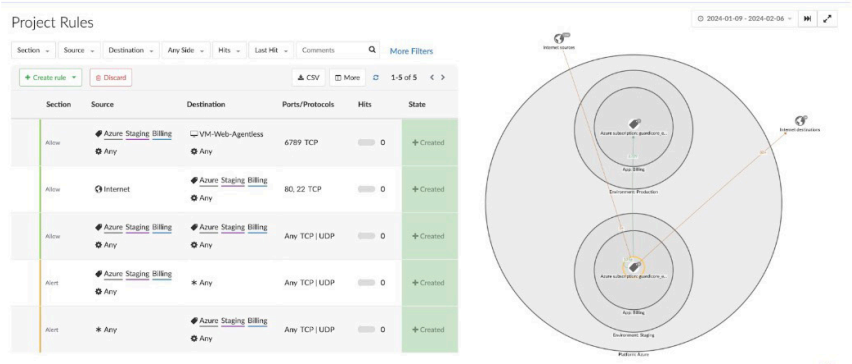
独特的云挑战

现代企业越来越依赖云服务来管理关键系统并存储有价值的数据。

根据 IBM 2023 年《数据泄漏的代价》报告，82% 的泄露事件涉及存储在云环境中的数据，包括公有云、私有云以及混合云环境。攻击者通常能够成功入侵多个云平台，其中 39% 的泄露覆盖多种环境，造成的损失达到 475 万美元，超过平均水平。

云环境的独特性和动态性质意味着云工作负载相比本地资源而言面临的外部威胁更大。安全团队需要应对几个独特的挑战：

- 监测能力不足 — 云提供商依靠不同工作负载之间数据流的原始日志来进行监测。如果不能清楚了解云环境中不同工作负载和应用程序之间的关系，就不可能创建有效的安全策略。
- 没有统一的策略 — 单纯使用原生云安全工具很难为混合云环境创建一致的策略。这是因为每个云实例都有自己的对象和规则，因此也有自己的策略，从而导致策略分散化。
- 缺乏统一的治理 — 并非所有云服务都将安全放在首位。这会导致安全团队与应用程序所有者之间产生摩擦，后者在增加工作负载时并不总是将安全性考虑在内。



利用自动策略建议对 Azure 应用程序进行隔离

对于企业的优势

使用单一界面直观查看云数据流
使用动态的网络依赖关系图深入了解云工作负载与应用程序的交互，并轻松实施安全控制策略。

运用一致的分段策略
部署能在混合云环境中发挥统一作用的单个分段解决方案，从而避免因供应商特定解决方案而产生安全孤岛。

阻止数据泄露
调整安全策略来适应云环境中的任何变化，为团队减轻手动更新的负担。

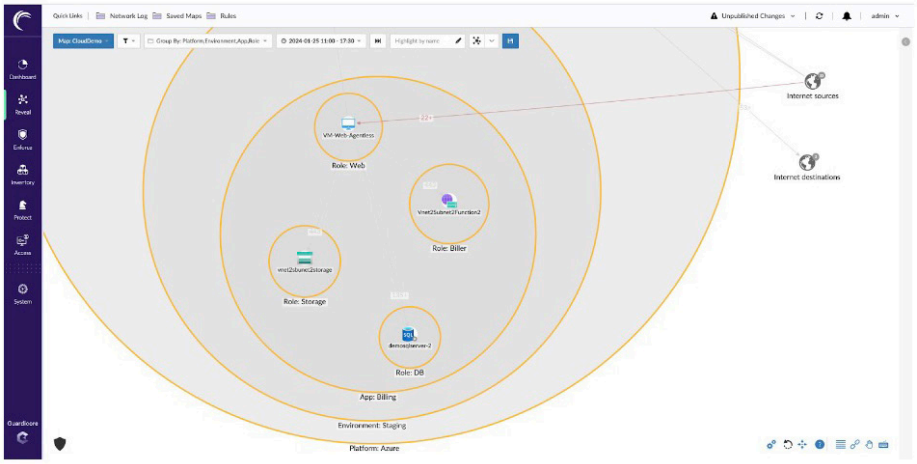
Akamai

抵御云安全威胁

Akamai Guardicore Segmentation 将业内知名的分段技术扩展到了云环境中的应用程序和工作负载。通过将分段策略扩展到云资产，可以自动阻止任何未经授权的连接，从而限制横向移动，并避免数据泄露或勒索软件事件造成损害。

主要功能

- 凭借全面、无代理的云原生监测和执行能力，管理员可以借助近乎实时的真实网络数据流交互图，直观地查看云端工作负载，同时还能了解应用程序的依赖关系，并在云端网络安全治理中统合 DevOps 和 SecOps 团队。
- 利用多个执行点的混合执行引擎，这让企业能够简单地定义网络策略的意图，并将其余工作交由 Akamai Guardicore Segmentation 策略引擎处理，由该引擎动态确定使用数据中心内的哪些基于代理和无代理的执行点。
- 集成的信誉分析和威胁情报防火墙，这些功能专为在发生违规时缩短检测和事件响应时间而设计。
- 可扩展、安全的解决方案，这能确保数据不会离开您的云环境，同时确保解决方案架构可在云环境内自动扩展。



本地和混合云环境共享的单一分布图

请访问 akamai.com/guardicore 以了解更多信息。

支持 | 发布时间：2024 年 2 月