AKAMAI 客户案例

大型医疗系统选择与 Akamai 合作，以提高合规性并实现上云

全面的网络监测能力

跨 IT 基础架构的分段

安全地采用新技术

客户概况

作为大型医疗系统，这家 Akamai 客户承担着重任，需要保护其 6,000 多项资产和患者数据避开潜在威胁的侵扰。

业务挑战/要求

尽管该公司计划将其数项关键工作负载迁移到 Microsoft Azure，但其 IT 利益相关者发现，有许多因素阻碍着他们成功采用云技术。

他们目前的环境存在一些安全风险，其一是网络相对扁平化，医疗物联网设备可以在不受监控的情况下访问数据中心；其二是应用广泛的“自带设备”政策。这意味着一旦发生入侵，就会导致严重的横向扩散，从而危及其他关键业务应用程序中的患者和支付数据。由于几乎不存在隔离，他们必须人工地梳理详尽的安全日志，以向审计人员证明合规性。

同样令人沮丧的是，由于缺乏对流量和应用程序依赖关系的监测能力，他们将工作负载迁移到 Azure 的工作也是举步维艰。

为什么选择 Akamai?

如果使用 VLAN 或防火墙来解决该公司当前面临的监测和安全挑战，那么就需要在几支已经不堪重负的团队之间开展协调，还需要付出巨大的努力来执行必要的网络变更。

Akamai 团队展示了一种软件定义式分段方法，能够精细映射其不同环境，并为其本地和云端工作负载一致地应用分段策略，这促使该公司的利益相关者争取到了预算，也促使 IT 领导层做出了购买决策。

Large Healthcare Systen

行业
医疗保健

解决方案
Akamai Guardicore Segmentation

重要影响
- 阻止未经授权的横向移动
- 保护关键应用程序
- 简化并更快地实现合规性
- 支持安全迁移到云端

Akamai

Akamai Guardicore Segmentation 的结果

简化和加速微分段

Akamai Guardicore Segmentation 采用独立于底层基础架构的软件叠加式方法，这让该客户的安全团队能够独立加速分段项目，同时尽可能控制对 IT 部门其他团队的影响。

借助新平台，该组织能够快速为关键应用程序创建安全围栏，并严格限制设备对数据中心的访问，而且不需要停机，也不需要更改任何应用程序或网络。利用全新的实时和历史数据监测功能，该公司现在还可以轻松地向审计人员证明，所有受监管资产都得到了有效隔离。如今，该公司只需要安排两名员工专门负责管理数据中心的安全性。

最后，通过映射应用程序依赖关系、创建必要的策略，该医疗系统成功地实现了采用云技术的目标，同时也确保未来的任何工作负载都能安然无忧地迁移到云。

请访问 akamai.com/guardicore 以了解更多信息。

> 每一个潜在的医疗保健客户都应该了解一下 [Akamai] 解决方案，这样他们就可以从一个视图中看到整个数据中心流量，同时轻松地在混合云环境中创建和应用安全策略。
>
> - 大型医疗系统 IT 安全负责人