

# 某领先广告商实现 Zero Trust 安全防护

该广告商获得网络保险投保资格，成功抵御攻击，并且通过微分段更好地保护了知识产权



成功投保网络保险



检测威胁



抵御攻击

## 增强品牌与电视观众的联系

某全球领先联网电视广告商通过更广泛地触达高度分散的流媒体观众，帮助品牌商让广告投入发挥出最大价值。为了获得网络保险的投保资格时，该广告商部署了 [Akamai Guardicore Segmentation](#) 以加强安全措施。

## 获得网络保险投保资格

作为一家创新型企业，该公司深知保护知识产权 (IP) 的重要性。就像很多现代公司一样，一旦爬虫程序或黑客入侵内部服务器或应用程序，就很容易发生知识产权暴露。

为了减轻潜在入侵造成的经济损失，母公司敦促其购买网络保险。随着 [网络攻击](#) 的增加，保险公司会先审查公司的安全准备情况，然后才为他们提供保单。考虑到这一点，该公司决定实施内部分段。



Advertising  
Leader

位置  
美国

行业  
媒体和娱乐

解决方案  
[Akamai Guardicore  
Segmentation](#)



## 部署内部分段控制措施

该公司发现 Akamai Guardicore Segmentation 解决方案提供的基于软件微分段方法可以解决这个问题。Akamai Guardicore Segmentation 旨在阻止攻击者在整个数字环境中实现**横向移动**，是该公司 IP 保护措施中的关键一环。借助微分段，该公司可以确保包含其知识产权信息的服务器和应用程序及其工作负载完全与基础架构的其余部分隔离开来。

通过使用 Akamai Guardicore Segmentation 为关键资产建立安全围栏并限制横向移动，该公司可确保攻击者无法轻易在其 IT 环境中移动。对物理和虚拟环境中移动行为的精细监测能力能够帮助立即阻止攻击者的行动。

## 检测和抵御勒索软件攻击

为了确认 Akamai Guardicore Segmentation 就是最佳选择，该公司进行了概念验证 (PoC)。在 PoC 期间，Akamai 解决方案检测到很多攻击者，甚至还检测到一次勒索软件事件。

看到 Akamai Guardicore Segmentation 能够有力地保护公司环境，该广告商深信自己找到了理想的解决方案。该公司计划对超过 3,000 台服务器（Linux 服务器、裸机服务器和云服务器）以及大约 1,500 个容器（Docker 和 Kubernetes）进行分段。

