AKAMAI 解决方案简介

聚焦多方法入侵检测：利用分段策略检测数据中心入侵

数据中心的入侵事件毫无减少迹象，因此安全团队应该将工作重点放到数据中心的核心部分，也就是应用程序彼此通信、发挥任务关键型功能的位置。越来越多的企业将数据中心资产分散到多个虚拟化环境中，边界防御已不足以满足需求。安全管理员需要找到一种行之有效的方法，保护内部东西向流量，抵御已成功突破边界防线的攻击。

防火墙布置陷入困境

防火墙历来用于保护数据中心内外的通信。但将防火墙置于数据中心的核心位置会造成许多问题。它们无法适应大量的东西向流量，反而会成为性能瓶颈。服务器级别的防火墙要耗用大量主机计算资源，让原本已经负重前行的主机承受更多压力。此外，这种方法还要求部署多种解决方案，以适应数据中心内多种不同类型、不同品牌的操作系统，进一步增加了管理难度。

直到不久之前，在 L7 进程层面实施安全策略还是一项棘手的难题。因为这要求监测在环境中通信的所有应用程序和进程，还要求全面了解不同进程应如何在在应用程序和数据中心内协同工作。如果不具备这些重要见解，实施进程级安全策略就可能存在风险，造成中断的几率也会大大提高。

为了保护数据中心的关键资产，同时改进入侵检测和响应，安全团队需要具备以下能力的方法：

- 实时直观显示数据中心内运行的所有应用程序和进程
- 在不妨碍关键进程的情况下实施细粒度安全策略
- 检测可能指向入侵的未经授权的通信

进攻就是最好的防御：利用 Akamai Guardicore Segmentation 进行基于策略的检测

基于策略的检测可帮助安全团队更快地检测、确认并遏制威胁，从而防止破坏，并将损失控制在最低限度。这些精细的安全控制措施具有双重作用，既能防止入侵者恶意访问应用程序或进程，又能提醒管理员入侵者的存在。

Akamai Guardicore Segmentation 中的分段策略功能能够支持安全从业者：

- 生成数据中心内所有应用程序和活动的全面可视化映射图，从而全面监测所有工作负载，并充分了解应用层通信
- 对应用程序执行过滤，并划分成组、添加标签，以便设置通用安全策略—例如，与特定工作流或业务职能相关的所有应用程序
- 定义和创建管理应用程序间经授权通信的规则
- 测试并完善这些规则，确保它们不会干扰经过授权的正常流量

多种检测方法加速入侵检测

动态欺骗

在不影响数据中心性能的情况下，重定向架构和动态生成的实时环境可吸引攻击者，并识别其攻击方法

基于策略的检测

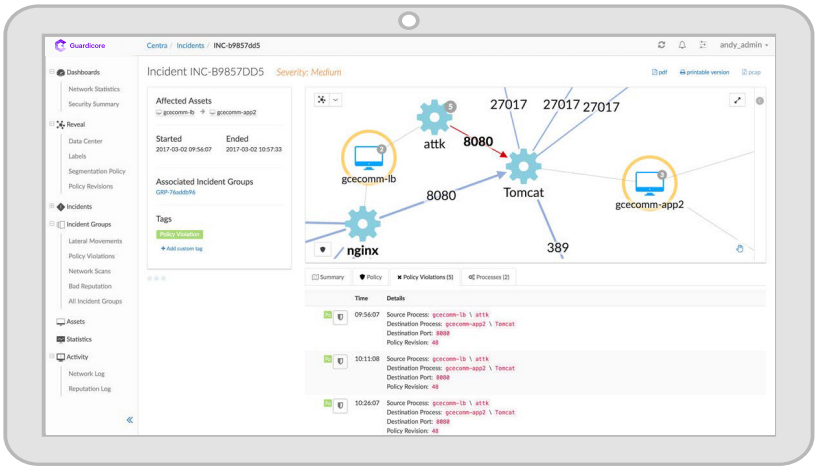
第 4 层网络和第 7 层进程级别的安全策略可立即识别未经授权的通信和不合规的流量

信誉分析

检测流量中的可疑域名、IP 地址和文件哈希值，提供全面的入侵检测功能

Akamai

任何不合规流量、未经授权的通信或其他违反策略的行为都会触发自动警报，指明可能存在入侵者。随后这会启动调查流程，以确认并遏制威胁。



Akamai Guardicore Segmentation 可检测潜在的违规行为，它能识别违反分段策略的行为，包括未经授权的进程在两个经允许的主机间的授权端口上通信的情况，并就此发出警告。

利用多种检测方法围剿攻击者

我们的解决方案通过多种方法改进实时入侵检测和响应，基于策略的检测只是其中之一。这些互为补充的方法还包括：

- **动态欺骗**，将真实的数据中心服务器、IP 地址、操作系统和服务用作诱饵，在出现最初的迹象时主动寻找可疑活动，与之互动，并将其重定向至隔离区，以便开展威胁确认和调查
- **信誉分析**，利用 Akamai 的全球威胁传感器网络和情报反馈，识别与威胁相关的有害进程和可疑 IP 地址、域名或文件哈希值

通过同时部署这三种方法，就能建立强大的安全网，从根本上确保捕获、抵御和控制数据中心的任何实时入侵，以便开展深入调查。

如需进一步了解 Akamai Guardicore Segmentation 的全面入侵检测能力，请访问 akamai.com/guardicore。