AKAMAI 解决方案简介

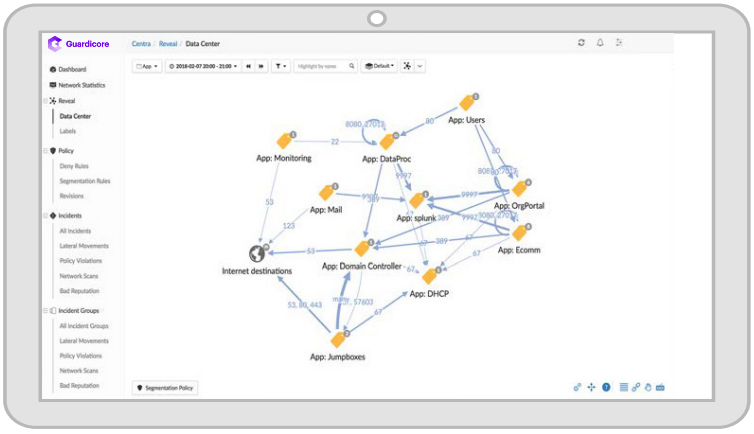
利用 Akamai Guardicore Segmentation 实现混合环境中的快速微分段

微分段的实施之旅并非一马平川；在您着手发现、了解和控制 IT 环境中的应用程序流量时，一定会遇到许多曲折。但如果没有正确的方法来应对这一切，您就会遇到一些难题。网络盲点往往会造成您无法充分地对应用程序、工作负载和底层进程进行发现和通信映射。僵硬刻板的策略引擎会强制采用一刀切的决策，造成用程序中断风险。不同操作系统之间不一致的策略表达会造成高风险安全漏洞。最后，策略违规数据与入侵监测工具之间的复杂集成（往往需要手动完成）会拖慢事件调查和响应的速度。Akamai Guardicore Segmentation 可帮助您通过简单三步实现微分段。

第 1 步：揭示

自动发现应用程序，并直观显示流量

Akamai Guardicore Segmentation 具有出类拔萃的监测能力，能够自动发现并直观显示所有应用程序、工作负载和通信流量——无论其位于何处，并提供进程级的情境信息。您可以通过同一个视图查看本地环境、云环境、多云环境及更多环境中的资产。这种可视化功能与自动导入编排元数据的功能相结合，让您的安全团队能够快速、轻松地标记和分组所有资产和应用程序，进而简化策略开发。



保护位于任何环境中的关键应用程序

不受平台制约

Akamai Guardicore Segmentation 可直观显示资产，并跨多种基础架构（本地、云和多云）执行安全策略。

快速制定策略

自动规则建议、灵活的策略引擎和直观的用户界面都能让策略的创建和执行更加省时

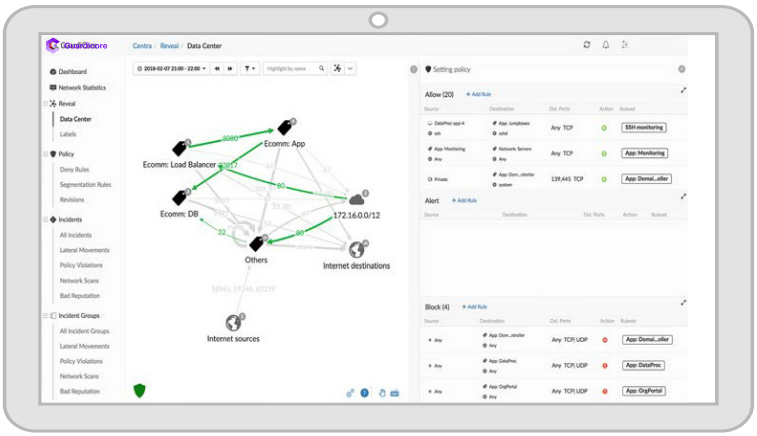
集成化入侵检测和响应

直观显示策略违规情况，快速应对主动威胁，保护您至关重要的资产—无论其位于何处

第 2 步：构建

快速设计、测试和部署策略

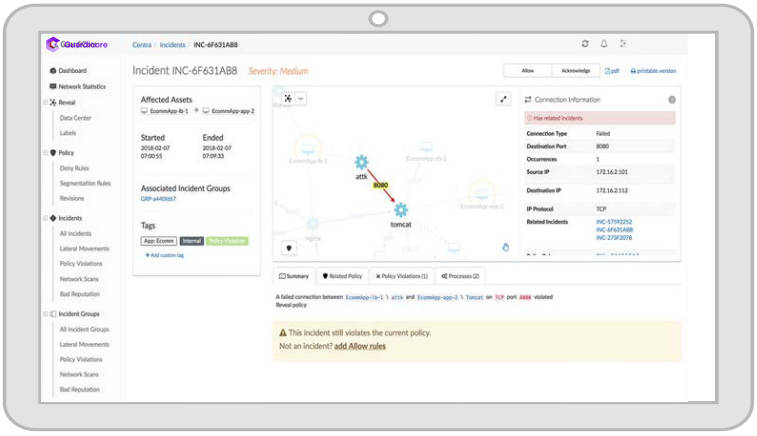
Akamai Guardicore Segmentation 简化了微分段策略的开发和管理工作。只需点击“揭示”映射中的通信流，该解决方案就能根据历史观察结果生成自动规则建议，支持您快速构建强大的策略。直观的工作流和灵活的策略引擎助您不断优化策略，减少代价高昂的错误。



第 3 步：执行

在任何环境中提供强有力的安全机制

Akamai Guardicore Segmentation 能够覆盖多种系统，在网络和进程级别执行通信策略，因此无论操作系统有怎样的执行限制，您都能维护安全性。此外，集成的入侵检测和响应功能可让您在遭遇入侵期间查看策略违规，从而快速识别攻击方法并实施补救措施。



请访问 akamai.com/guardicore 以了解更多信息。