AKAMAI 解决方案简介

借助 Akamai Guardicore Segmentation 监测并保护 Kubernetes

凭借前所未有的速度和灵活性，Kubernetes (K8s) 仍是在云原生数据中心内部署和管理应用程序时采用最广泛的技术之一。根据 Gartner 的数据，到 2026 年，90% 的全球组织将在生产中运行容器化应用程序，而 2021 年这一比例仅为 40%。此外，到 2026 年，20% 的企业应用程序将运行在容器中，而 2020 年这一比例还不到 10%。[1] 然而，这一日渐流行的平台不只吸引了用户，也让攻击者闻风而至，这迫使安全团队不得不应对他们本未准备好应对的挑战。

新技术带来新安全挑战

K8s 集群提供了一个完整的生态系统，其中包含 DNS 服务、负载平衡、网络、自动扩缩，以及运行应用程序所需的任何其他功能。K8s 使企业能够实现快速创新并节约成本，因此获得如此广泛的采用并不奇怪。然而，K8s 的特有属性在为其带来竞争力的同时，也带来了更多安全挑战。

它本质上是一个扁平网络，也就是说，每个 Pod 都可以与集群内的任何其他 Pod 通信。在初始入侵得手后，攻击者便可以横向移动并访问所有连接的数据中心。这是一种典型的勒索软件攻击过程，但同样的攻击策略很容易被另一种攻击媒介所利用。

《Red Hat 2022 年度 Kubernetes 安全状况报告》分析了对于 300 多名 DevOps、工程和安全专家的调查结果，其中 93% 的受访者表示，在过去 12 个月内，他们的 K8s 环境中至少出现过一次安全事件，而这些事件有时会导致收入损失或客户流失。

解决方案：微分段

K8s 的应用程序部署概念本身是不同的，因此需要不同的安全方法。安全团队不能原样照搬现有的安全解决方案，并期望它能够适应 K8s 的全新技术。要保证 K8s 集群的安全，必须采用 K8s 原生的安全方法。

正因如此，Akamai 打造了一个基于软件的分段解决方案，专门用于保护 K8s 集群。该解决方案与您工作环境中的其他工作负载（比如传统系统、云、本地工作负载和容器）的行为方式类似。通过该解决方案，您可以通过单一管理平台，对您公司内的各类资产进行监测、保护和管理。

优势

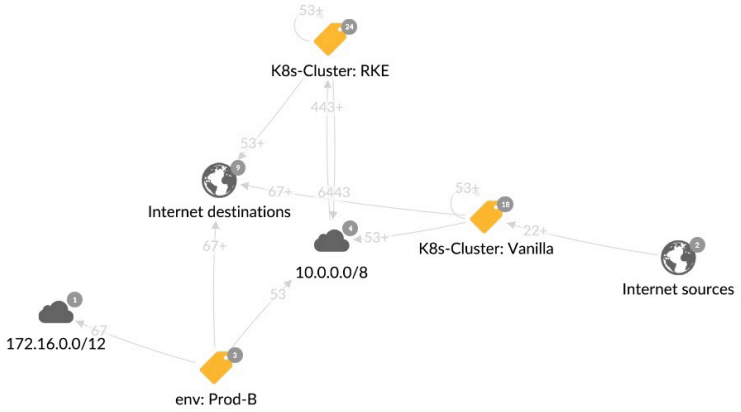
- 通过一个管理平台，实现 K8s 集群的监测、策略强制实施和监控，并处理任何其他资产
- 轻松抵御利用 K8s 漏洞的高级攻击
- 显示 Pod、服务、主机或域名空间之间的各种实时和历史连接
- 提供开箱即用的模板，可轻松为 K8s 集群创建安全围栏
- 覆盖 K8s、端点、本地工作负载和云工作负载的统一控制台和策略管理
- 接收已部署集群上的运营数据，包括监视这些集群的代理程序数量以及 Kubernetes 编排状态

Akamai

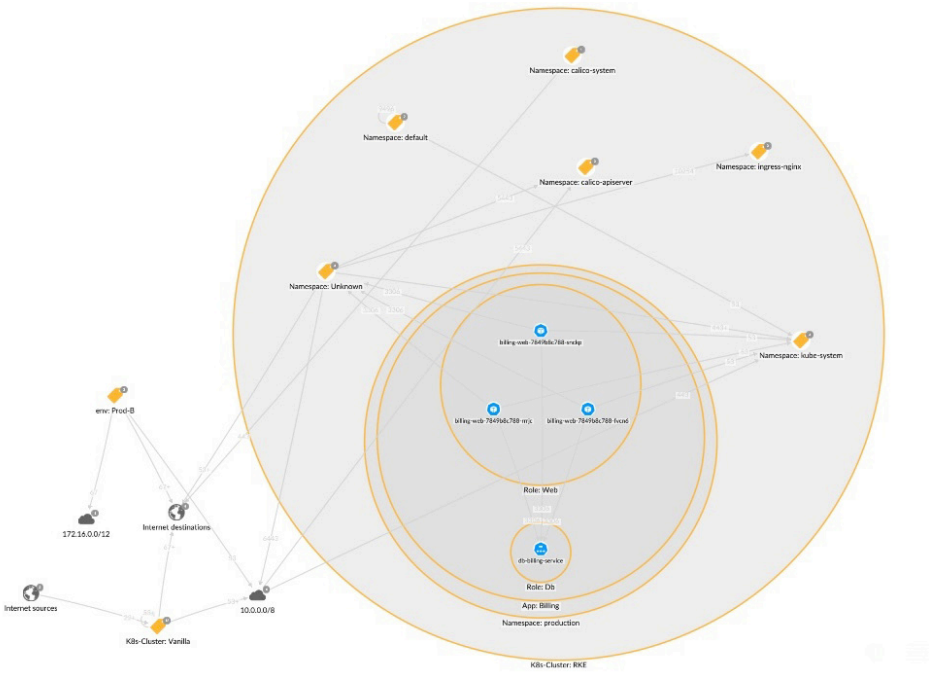
用于 Kubernetes 集群分段的主要能力

监测能力。借助 Akamai Guardicore Segmentation，您能够了解 K8s 环境中运行的内容，并确认流量仅到达您期望的目的地，而这对您成功创建策略至关重要。

- **展现依赖项关系的映射** — Akamai 提供了映射功能，可用于监测数据中心内部和多个数据中心之间的通信，并适用于虚拟机、K8s、Docker 容器等各类技术。这些映射支持监测并检测 Pod、服务、主机或域名空间之间的任何可疑连接。
- **标签** — 通过使用多层标签，映射可以准确地反映应用程序在集群中的部署方式。这一功能可以显示应用程序管理人员规划的 K8s 层次结构。这种程度的详细信息有助于 Akamai 用户准确了解集群中部署的内容，以及所部署的应用程序与基础架构其他部分之间的网络关系。



Reveal 映射中显示的集群。双击一个集群，即可显示集群内的域名空间及其相互连接。



Reveal 映射可显示 Pod 信息

> 93% 的受访者表示，在过去 12 个月内，他们的 K8s 环境中至少出现过一次安全事件，而这些事件有时会导致收入损失或客户流失。

强制实施能力。为尽可能缩小 K8s 集群的攻击面，需要使用严格的分段策略。分段强制实施解决方案应该满足两项主要标准：它应该具备非侵入性特点，并且不存在任何规模和性能限制；它应该通过灵活的方式为所有级别的 K8s 对象（包括域名空间、控制器和 K8s 标签）提供安全围栏。

Akamai 使用了原生的 Kubernetes Container Network Interface (CNI)。CNI 包含一个网络安全策略插件，该插件最初用于在 K8s 中强制实施网络分段。这是一种规模不受限制的非侵入性方法。其专用模板允许用户为 Kubernetes 业务关键型应用场景提供安全围栏，无论这种应用场景是域名空间、应用程序还是任何其他对象。

> **Ring Fence a K8s Application** by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace
>
> *Kubernetes 应用程序安全围栏模板*

高级监控能力。利用高级日志和监控系统，专门针对 K8s 网络调整网络日志，可显示每个事件的目标服务、节点 IP、源端口和目标端口以及进程。这让用户可以更便捷地调查网络中的异常活动，并将数据导出到第三方应用程序（如 SIEM）。

《Red Hat 2022 年度 Kubernetes 安全状况报告》指出，安全问题是 K8s 采用面临的最大问题之一，迄今依然导致许多应用程序迟迟未能部署到生产环境。

总结

Kubernetes 已经成为许多业务环境中不可或缺的一部分。这是一种不同于以往的方法，它实现了更高的资源利用率、更精简的开发过程，以及更强的可移植性和可扩展性。但是，这种不同以往的应用程序开发方法也需要不同的安全方法。

Akamai Guardicore Segmentation 提供了整体的解决方案，允许您通过单一映射监测不同类型部署（裸机、虚拟机、K8s）之间的通信流。它提供了一种非侵入性且可扩展的 K8s 原生方法，让您能进行监测、监控和强制实施，从而为安全和开发团队减负，使您的业务能够在不牺牲安全性的情况下快速实现创新。

要了解更多信息，请访问 akamai.com 或联系您的 Akamai 销售团队。

1. Gartner，《The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem》，Arun Chandrasekaran、Wataru Katsurashima，2021 年 8 月 18 日。

扫码关注・获取最新CDN前沿资讯

 | 支持 | 发布时间：2022 年 9 月