AKAMAI 产品简介

Akamai Guardicore Segmentation

通过高精度监测能力和微分段控制，阻止横向移动

企业的 IT 基础架构在不断从传统的本地数据中心转型为集成了多样化平台和应用程序部署模型的云端和混合云架构。尽管数字化转型使许多企业提高了业务敏捷性、降低了基础架构成本并支持远程工作，但同时也形成了一个更大、更复杂且边界不明的攻击面。如今，每台独立的服务器、虚拟机、云实例以及端点都可能成为安全漏洞。随着勒索软件和零日漏洞等威胁的日益猖獗，攻击者在找到入侵途径后，向高价值目标进行横向移动的技巧变得越来越熟练，这已成为既定事实。

Akamai Guardicore Segmentation 可助您在网络中以非常简单、快速和直观的方法实施 Zero Trust 原则。它旨在通过监测您 IT 环境中的活动、实施精准微分段策略，以及快速检测可能的入侵行为，从而有效阻止横向移动。

解决方案的主要功能

AI 技术加持的精细分段

借助 AI 建议，用于补救勒索软件和其他常见用例的模板，以及准确的工作负载属性（如流程、用户和域名），只需几次点击即可轻松实施策略

实时和历史监测

基于实时或历史数据，绘制细化到用户和流程级别的应用程序依赖关系及流动情况

广泛的平台支持

涵盖裸机服务器、虚拟机、容器、物联网和云实例中的现代和传统操作系统

灵活的资产标签

通过可自定义的标签层次结构添加丰富的上下文，以助力监测和执行，并与编排工具和配置管理数据库集成，以实现标签自动化

多种保护方法

集成威胁情报、防御和入侵检测功能，以缩短事件响应时间

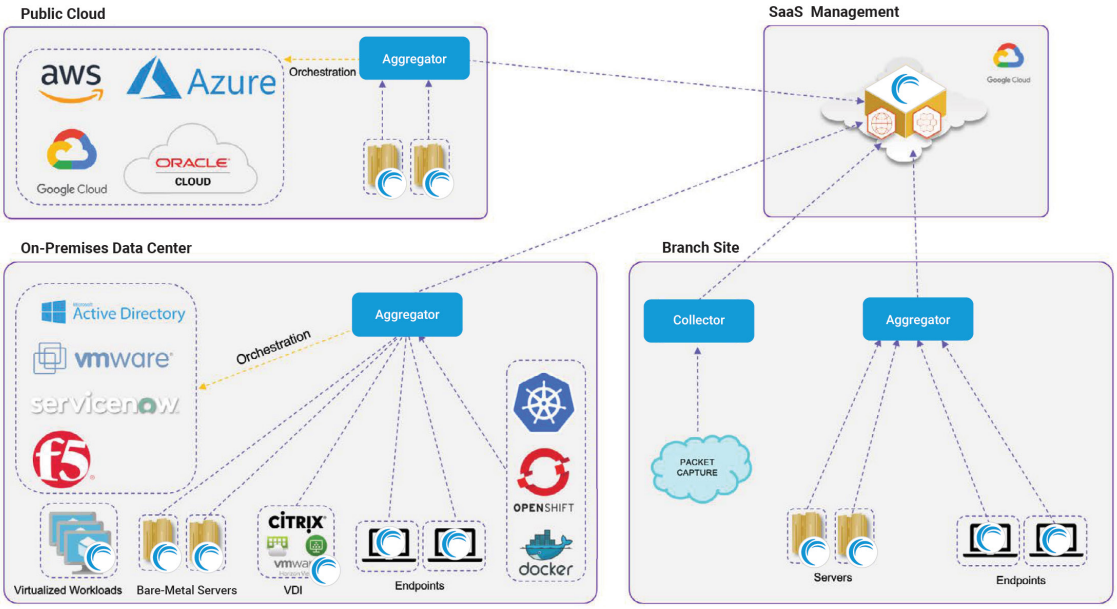
对企业的好处

- 抵御勒索软件
- 实现 Zero Trust 目标
- 加快实现合规
- 隔离关键应用程序
- 确保云迁移的安全
- 保护远程员工
- 保护端点
- 超越内部防火墙

工作原理

Akamai Guardicore Segmentation 通过一系列基于代理的传感器、基于网络的数据收集器、来自云服务提供商的虚拟私有云流量日志，以及支持无代理功能的集成，收集有关企业 IT 基础架构的详细信息。相关上下文通过一个灵活且高度自动化的标签流程添加到此类信息中，该流程包括与现有数据源（如编排系统和配置管理数据库）的集成。

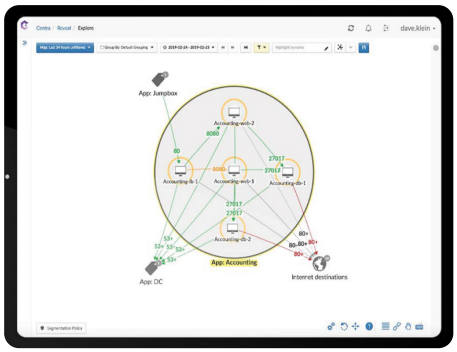
基础架构拓扑



大多数客户使用 SaaS 管理，但本地管理选项同样可供使用。

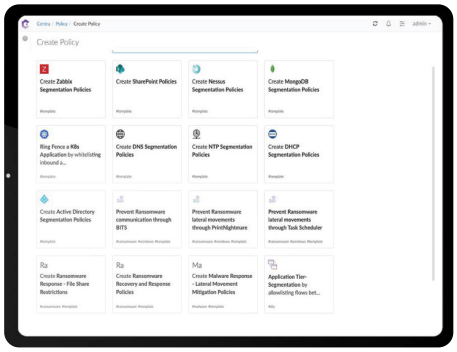
网络图

输出的是一个展示整个 IT 基础架构的动态图，安全团队能够在图中查看细化到用户级别和流程级别的实时活动和历史活动。这些细致的见解与 AI 驱动的策略工作流相结合，有助于快速、直观地创建基于真实工作负载上下文的分段策略。



模板

对于大多数常见用例来说，使用预构建的模板可以简化策略创建。策略实施与底层基础架构完全独立，因此无需进行复杂的网络更改或停机，即可创建或修改安全策略。此外，不论工作负载位于何处（本地数据中心或公有云环境），策略都会遵循工作负载的要求。得益于与一系列精密的威胁防御和漏洞检测功能，以及与托管威胁搜寻服务 Akamai Hunt 的默契配合，我们的分段功能将如虎添翼。



大规模全面保护

任何环境

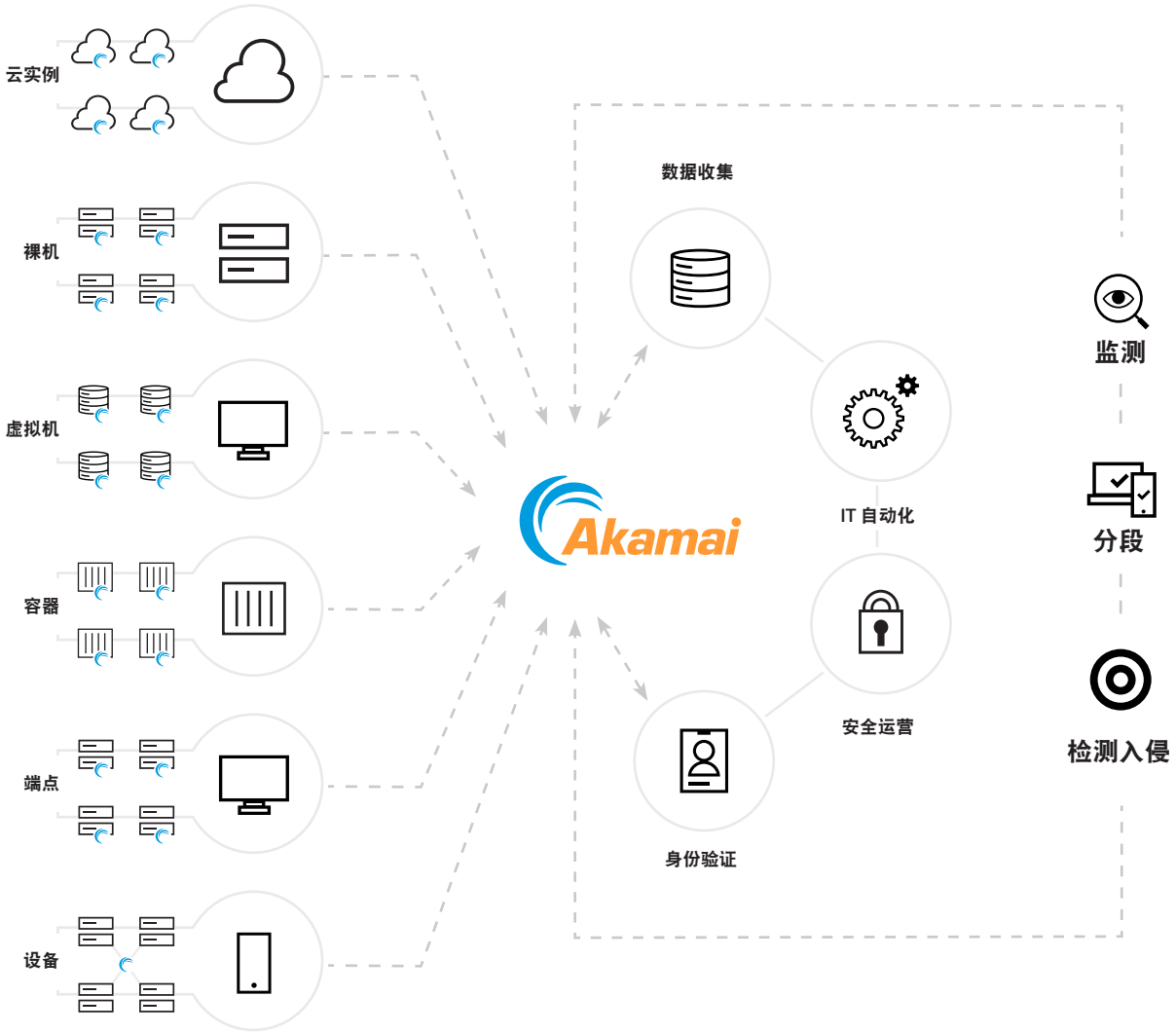
通过组合使用本地工作负载、虚拟机、传统系统、容器和编排、公有/私有云实例以及 IoT/OT，保护复杂 IT 环境中的工作负载

简化安全防护

通过使用一个平台，我们可以简化安全管理，为 Zero Trust 计划提供网络监测、分段、威胁防御、入侵检测功能和指导性策略执行

企业可扩展性和性能

首先，我们会对最重要的数字资产进行重点保护，然后再逐步扩展至整个企业的保护，避免出现复杂性问题、基础架构变更或性能瓶颈



支持的平台和技术

- Akamai Guardicore Segmentation 旨在与您现有的基础架构相集成。
- 我们的操作系统能够随着客户需求的增长而不断扩展。
- 查看我们的技术合作伙伴页面，获取我们完整的集成列表。

操作系统

Linux

SUSE, CentOS, Red Hat, debian, aws, aws 2, ORACLE LINUX, ubuntu

Apple

Microsoft

Windows Server, Windows

Unix

AIX, ORACLE SOLARIS, FreeBSD, hp UX

公有云提供商

aws, Microsoft Azure, ORACLE, Google Cloud

虚拟机管理程序

KVM, CITRIX XenServer, VMware ESXi, vSphere Hypervisor, NUTANIX, AHV, Hyper-V

虚拟化编排

vCenter Server, vSphere, NSX, apachecloudstack, openstack., MIRANTIS, nuagenetworks

安全网关

CISCO, paloalto NETWORKS, CHECK POINT

容器编排和引擎

docker, kubernetes, Red Hat OpenShift

用于 Web 控制台的浏览器

内存和系统最低要求

Management Server 32 GB RAM, 8 vCPUs, 530 GB	**Aggregator** 4 GB RAM, 4 vCPUs, 30 GB
Deception Server 32 GB RAM, 8 vCPUs, 100 GB	**ESC Collector** 2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

如需详细了解 Akamai Guardicore Segmentation，或者申请个性化产品演示，请访问 akamai.com/guardicore。