AKAMAI 产品简介

Akamai Guardicore Access
统一的 ZTNA 和微分段

由单个控制台进行监测和控制，简化并加速 Zero Trust 实施

企业正在迅速采用 Zero Trust 安全策略，以阻止勒索软件攻击、满足合规性要求，并为混合工作团队和云基础架构提供安全防护。Zero Trust Network Access (ZTNA) 和微分段是企业向 Zero Trust 架构转型的两大关键解决方案。这两个解决方案强强联合，助力减少攻击面、防止漏洞攻击，并提供更好的访问控制和改善用户体验。

统一的力量

Akamai Guardicore Access 将微分段和 ZTNA 相结合，通过单个代理进行部署，并由单个控制台进行管理。这项创新方法可确保从用户到工作负载（南北向）以及从端点到端点或工作负载（东西向）的全面可监测性，进而实现基于身份的应用程序访问控制和端点分段。通过结合这些技术，企业可以从强大的安全框架中受益，该框架可增强网络防御、降低风险，并营造安全合规的环境。

Akamai Guardicore 平台是首个将业界卓越的微分段和 ZTNA 相结合的安全平台，可帮助安全团队阻止勒索软件攻击、满足合规性要求，并为其混合工作团队和云基础架构提供安全防护。

这是企业第一次能够通过单个代理和单个控制台，在所有类型的资产和基础设施上实施分段，以最大限度地减少攻击面，同时轻松管理来自各地的混合工作团队的访问权限。

主要功能

端到端可见性

通过端到端的可见性，全面了解您的网络，显示在地图和日志中，并提供对最终用户访问模式的见解。这只有通过包含微分段和 ZTNA 的产品才能实现。查看从端点到工作负载的连接路径，并细化到进程级别。近乎实时的监测和历史监测能力使取证分析更加容易，抵御响应速度也更快。

对企业的好处

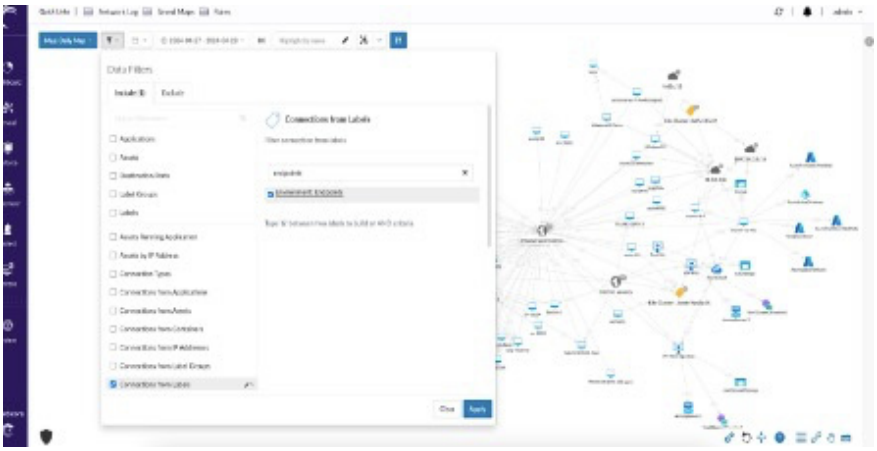
单个控制台、单个代理
通过单个代理和单个控制台实施分段，最大限度地减少攻击面，同时轻松管理来自各地的混合工作团队的访问权限

广泛覆盖
在各个地方应用访问控制措施，并确保远程员工和办公室员工的安全

统一策略
针对东西向流量和南北向访问实施策略，而无需更改语法或控制台，以极为简单、有效的方式实现 Zero Trust

应用程序发现

通过快速识别需要访问权限的应用程序，减少制定策略的时间。轻松发现您的私有应用程序，并获得有关其使用模式的宝贵见解，包括用户访问权限和频率。



轻松发现需要访问权限的应用程序

访问和分段策略同步

自动同步访问控制和分段规则，以减少跨团队依赖性，并消除人为错误的可能性。

主要应用场景

全面的勒索软件防护: 通过基于身份和机器间的策略，降低勒索软件和其他恶意软件攻击的可能性和影响。确保端点在最低权限的基础上访问资源，同时实施精细访问控制。

- 保护高价值资产：允许用户根据安全访问控制规则访问关键资产，并阻止定向 VPN 流量
- 限制特权用户：阻止 VPN 流量流向可能被利用的管理端口，为管理员提供安全访问

员工分布： 通过实施严格的访问控制，支持员工随时随地办公，确保每个设备仅连接至所需的资源。这可以最大限度减少攻击面以及网络内部的横向移动。

合规性： 实施端点分段策略，以便企业可以确保其端点符合相关行业标准和法规，从而降低因违规而遭受处罚的风险，并增强整体安全态势。

第三方访问： 通过专用的 Akamai 门户路由并验证访问，无需安装代理即可让承包商和合作伙伴连接到特定应用程序。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯

如需了解详情，请访问 Akamai Zero Trust 安全