

AKAMAI 产品简介

Secure Internet Access SMB

面向宽带 ISP 的中小型企业安全服务

中小型企业 (SMB) 通常缺乏 IT 资源和安全专业技术，在这些公司中，近四分之三 (77%)¹ 的高级经理将网络安全列为高优先事项，并正在寻求降低风险的方法。勒索软件攻击持续受到媒体的广泛关注，对此类恶意软件的报道量明显高于预期，甚至超过了同期的其他互联网威胁。对于有能力保护中小型企业免受各种威胁侵扰且简单易用的高级网络安全解决方案，市场需求从未如此强烈。中小型企业常因资金紧张而限制支出，但月费适中的订阅模式则可解决这些预算难题。

Akamai Secure Internet Access SMB 不仅可实施内容策略和先进的威胁防范功能，而且简单易用。该产品可作为提供商互联网服务的一部分无缝实施，除了能让订阅者对其轻松管理之外，还可对所有连接互联网的设备进行全方位的监测、控制和保护。它的服务选项很多，订阅者既可轻松实现内容过滤和家长控制，也可获得多层次的深度防御功能，从而防范一系列最新的恶意互联网威胁，包括勒索软件、僵尸网络、网络钓鱼和零日恶意软件攻击。

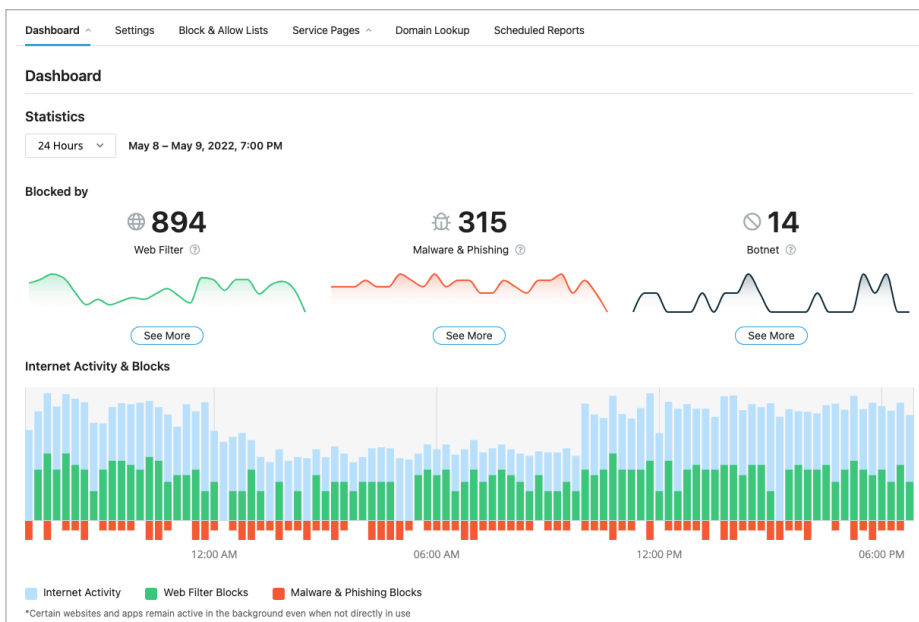
让公司享有企业级的保护

Akamai Data Science 运用先进技术，每天分析 1000 多亿个 DNS 查询，进而识别恶意活动并向我们的威胁数据源每天添加数百万个新条目。与此同时，允许正常流量通过。这样便可全天候确保公司及其员工的在线访问安全、可靠，而且无需复杂的配置并节省 IT 资源。

主要特色

-  防范恶意软件、勒索软件和网络钓鱼等威胁
-  有 Akamai Data Science 团队作后盾，该团队每天能够分析 1000 亿个 DNS 查询，足以抵御各种网络威胁
-  快速启动且简单易用
-  可针对不同的员工角色量身定制访问权限
-  管理控制台操作简单，公司可随时更改配置文件和访问权限
-  依靠实时数据库更新，轻松拦截不当内容和恶意内容
-  为视频和文件共享等高带宽消耗服务提供“流量控制”
-  既可部署在云端，也可无缝集成到您的核心网络服务中





一个可钻取查看摘要或详情的仪表板，即可显示所有已拦截的恶意软件。借助此“可随时随地访问”的启动台，企业主可随时添加设备，创建配置文件并调整设置。

公司客户可以根据员工需要、位置和角色拦截或允许内容，只需一次点击便可开启恶意软件和网络钓鱼防护。通过只允许用户访问适当的站点和类别，该产品可使员工免受不当的内容的影响。

产品	混合	全托管	运营商云 (本地部署)
CacheServe	本地部署	X	Akamai 云
Secure Internet Access SMB	Akamai 云	X	本地部署



运营商云



混合



Akamai 云

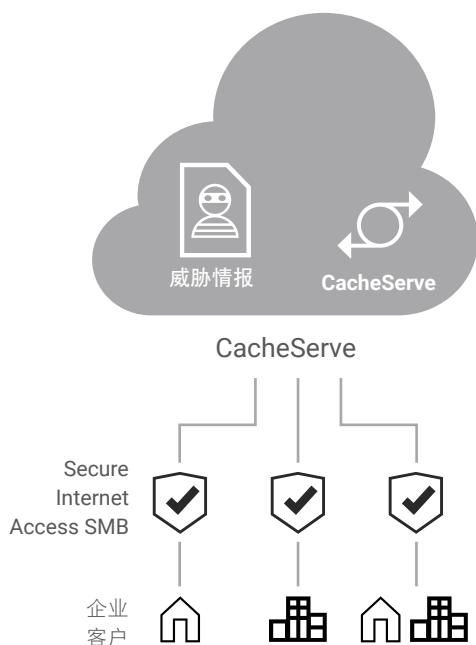
多种云部署选项使上市时间缩短

借助 Secure Internet Access SMB，提供商能够利用其现有网络基础设施为中小型企业提供云保护，或在 Akamai 云中托管解决方案。由于是白标解决方案，因此提供商可控制品牌运作并拥有数据，进而与其公司客户培养更深厚、更有利的关系，并提供非常有效且颇具成本效益的网络威胁防御。

让企业主轻松调整互联网内容设置

通过易于使用的控制面板，公司能够拦截预先设定的内容类别，如社交媒体、游戏、色情内容和流媒体服务。轻度、中度或严格的内容过滤设置自动包括内容类别过滤。对于希望拥有更精细控制功能的企业主，则可指定要拦截或允许的特定网站和 URL。

在过滤方面，Akamai 使用的是全球非常精确、博大的 URL 数据库，其中包含数百万个分门另类的 URL。Akamai 会持续更新这些预先设定的类别，进而确保对新出现的网站进行适当分类和自动拦截。通过控制面板，公司可轻松建立员工配置文件，并在配置文件中预先设定内容限制。



一个可钻取查看摘要或详情的仪表板，即可显示所有已拦截的恶意软件。借助此“可随时随地访问”的启动台，企业主可随时添加设备，创建配置文件并调整设置。

要了解 Secure Internet Access 的更多信息，请访问 akamai.com

1 《2021 年网络安全漏洞调查》，<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021>



扫码关注，获取最新 CDN 前沿资讯