

中小型企业网络安全 服务提供商发展的新机遇



前言

中小型企业 (SMB) 需要并希望获得网络安全防护。Hiscox 在其《2021 年网络就绪状况报告》中提到：“遭受攻击的企业比例从 2020 年的 38% 增加到 2021 年的 43%。许多企业都是多次受到攻击。”安全是一个全球性问题：英国政府于 2021 年开展的一次[网络安全漏洞调查](#)发现，37% 的微型企业（1-9 名员工）、39% 的小型企业（10-49 名员工）和 65% 的中型企业（50-249 名员工）在过去 12 个月内发现过入侵或攻击。鉴于调查回复的相似性，我们可以合理地得出这样的结论：不论经营地点如何，只要小型企业拥有攻击者认为有价值的资产，就会成为攻击目标。本白皮书将探索：

- 中小型企业在互联网上的安全风险，及其在应对安全威胁时的特有挑战
- ISP 如何帮助中小型企业应对其安全风险
- 中小型企业安全市场发展机遇，以及提供商如何构建业务案例

小型企业面临的网络安全挑战

中小型企业每一天都面临着安全威胁。他们的整体经济价值可观，而且往往不具备充分的安全专业资源，因此成为攻击者觊觎的目标。中小型企业面临的网络安全风险类型众多：恶意软件可能窃取或移除财务信息、客户数据或宝贵的知识产权资料；网络钓鱼攻击利用精心筹划的社会工程伎俩，哄骗用户下载恶意软件，或是交出用于访问可变现资产的凭据；智能设备的广泛使用（即物联网）造成了企业所有者可能尚未考虑到的额外风险。如需了解更多深入信息，请阅读相关 Akamai 白皮书：[《中小企业威胁态势》](#)。

本文在此简单汇总一下小型企业受到的影响：

- 2021 年发布的一份 Hiscox 报告指出：“攻击造成的代价各有不同。在遭受过攻击的企业中，有六分之一表示这类事件已经危及企业生存。”
- 2021 年英国政府发布的报告也指出：“在发现过入侵或攻击的 39% 的企业中，五分之一 (21%) 的企业最终蒙受了资金、数据或其他资产损失。三分之一 (35%) 的企业表示受到了负面影响。”（注：在原报告基础上节略部分内容以突出重点）

要点总结

大多中小型企业都没有形成大型企业那种“安全肌肉记忆”，因此更难充分保护自身安全。

中小型企业面临着严峻的风险，但英国调查表明，就企业领域而言，仅有 38% 的企业具有正式的安全策略，仅有 14% 的企业为员工安排了网络安全培训。77% 的企业表示，网络安全是其高管层高度重视的优先事项。要点总结：大多数中小型企业都没有形成大型企业那种“安全肌肉记忆”，因此更难充分保护自身安全。

中小型企业安全服务市场机遇

在帮助中小型企业解决安全隐患方面，ISP 具有得天独厚的优势。ISP 已经与中小型企业建立了长期 IT 服务关系，拥有现成的联系渠道和结算关系，是中小型企业心目中可信的顾问，因此中小型企业极有可能欣然接纳其指导建议。一些现成的安全解决方案可帮助提供商把握这样的市场机遇，同时满足中小型企业对于易用性、设备覆盖广泛性，以及价位适合紧张预算的需求。提供商可以打造愉悦的用户体验，同时推动自身收入节节攀升，提高其网络接入服务的亲和力。

TeleGeography 是一家跟踪全球 ISP 业务情况的领先市场分析机构，根据其发布的数据，以及有关各提供商以中小型企业为重心的业务部门的调查，Akamai 预估，全球大约有 6500 万中小型企业在使用互联网接入服务。全球互联网接入服务的费用在每月 50 美元到 125 美元之间，在此类服务中内置基本安全机制时的加价幅度是 10% 到 20%（每个月 5 美元到 25 美元），取中间值计算（最高和最低预估值的平均值），整体市场商机的价值接近于每年 120 亿美元。

Akamai Secure Internet Access SMB 推动中小型企业安全转型

Akamai 赋能提供商把握中小型企业安全服务市场机遇。Akamai Secure Internet Access SMB 是一种全新的网络安全解决方案，可提供基于 DNS 的安全防护，具有轻量级、可扩缩的优势。它使 ISP 能全面覆盖固网、移动网络和融合网络，为中小型企业打造基本防护层。Secure Internet Access SMB 的开发初衷就是由 ISP 运营，既可作为提供商托管的网内许可软件，也可作为 Akamai 托管的“即服务”。基于 DNS 的安全防护能够覆盖中小型企业设施内的所有设备，并且能高度灵活地应对当今的动态威胁。

从提供商的角度来看，Secure Internet Access SMB 旨在为提供商提供全面控制权。提供商可以根据自身的企业形象和目标，对该服务进行品牌定制。除了通过 API 定义用户体验，并指定服务级别之外，供应商还可确定业务模式（付费服务、套餐、分层式服务等），并设定适合相应地区状况的价格。Akamai 精心打造了一套“产品上市”资料包（包含指南和示例），帮助提供商迅速启动营销工作。



Secure Internet Access SMB 为中小型企业而设计，其用户体验的设计充分考虑了专业能力、时间和资源有限的客户的需求。它不要求安装任何软件，而且能够妥善保护企业内常见的各种设备。企业管理者可以畅享“设后即忘”的便捷体验，该服务能识别并拦截恶意活动或不当内容，无需人工干预。所有这些特点都是相当突出的优势。相比之下，传统中小型企业安全解决方案只是重新打包并重新定价的产品，其中的许多功能往往不适用于大多数中小型企业，因此他们无法从中受益。

在下面的几个例子中，您可以看到，提供商在积极探索使用 Secure Internet Access SMB 的多种业务模式。他们也在研究补充性的付费服务，比如防病毒工具，以满足希望进一步加强安全防护的客户的需要。

业务案例 1

某大型北美提供商拥有大约 250 万中小型企业用户，该提供商制定了两种安全服务级别，通过套餐的形式为网络接入服务提供补充：基本套餐提供恶意软件和网络钓鱼活动拦截服务，每月收费 9.95 美元，高级套餐（每月收费 29.95 美元）在基本套餐的基础上提供了简单的过滤机制，可供企业主自行配置，以拦截不希望出现在其工作场所内的内容（此功能称为可接受使用策略 [AUP]）。该提供商使用 Secure Internet Access SMB 缩短产品上市时间，并将内部运营开销控制在最低限度。在初步推广中，他们将目标锁定在新客户身上，并且计划在将来将这服务推广给所有中小型企业客户。用户如果注册高级套餐三年，则可以享受一定的折扣。他们预计该服务将在第二年盈利。

业务案例 2

另外一家大型北美提供商拥有 50 万中小型企业客户，他们制定了可作为网络接入服务补充的两个服务级别——入门级产品每月收费 19 美元，高级产品每月收费 29 美元。他们后续将推出一项基于 SD-WAN 技术的服务，目标受众是区域性连锁餐厅和零售连锁店。这些附加服务的关注点结合在一起，将使安全成为网络接入服务本身的关键要素，也让 Secure Internet Access SMB 成为其服务组合中的核心元素。这样的创新之所以能够实现，依靠的正是 Secure Internet Access SMB 完全独立于网络、可扩缩的特点。

结语

激烈的同行竞争促使 ISP 积极探索网络接入服务以外的业务领域，并提供更多增值服务来保持收入增长。安全服务显然是理想的选择，因为当今客户已经充分意识到了安全防护的必要性。凭借在中小型企业细分市场的业务触角以及深受中小型企业信任的地位，ISP 有着提供基本网络防护层以帮助其客户降低风险的独到优势。中小型企业细分市场在很多领域都没能得到充分的关注，而中小型企业自身的资源限制往往使其倾向于外包安全防护等服务。

Akamai Secure Internet Access SMB 采用可部署为 ISP 服务的形式，专为中小型企业而开发。这项服务有着“上手即用”的特点，不会给企业管理者增加配置或管理负担。

图形化门户便于了解威胁状态，还支持配置可选的网络内容过滤器，以实施 AUP。部署选项（许可式和“即服务”）帮助提供商协调业务与运营需求。

Secure Internet Access SMB 让提供商可以控制定价策略和业务模式，并实现符合地区要求和习惯的品牌定制和用户体验。为了激发兴趣，提供商可与中小型企业用户分享威胁态势信息，甚至是有关当地状况的深入见解。Akamai“产品上市”资料包可帮助提供商迅速启动营销工作。

如需详细了解中小型企业网络安全的话题，请访问 akamai.com。



Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。我们横跨云端和边缘的计算平台在全球广泛分布，不仅能让客户轻松开发和运行应用程序，而且还能让体验更贴近用户，帮助用户远离威胁。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2022 年 6 月。



扫码关注 · 获取最新CDN前沿资讯