用例

保护您的分支机构直接互联网访问 （DIA） 连接

执行摘要

在当今永不停歇的数字世界中，许多企业在全球各地设有分支机构和办事处。

这意味着，这些企业用户并非单纯地连接到企业网络。相反，无论流量目的地、用户类型和设备如何，企业流量通常通过昂贵的 WAN 服务发送到中央位置。最后，被访问的企业应用程序从数据中心转移到混合云环境，这使得经过中央位置的流量迂回传输功能变得更加低效。

几乎

80%

的企业分散劳动力会从分支机构访问网络。[1]

因此，具有分支办事处的企业越来越多地依靠直接互联网访问 (DIA) 连接到公共互联网，以开展日常和业务关键活动。作为传统 WAN 链路和 MPLS 的替代方案，DIA 可以满足由云优先和 SaaS 密集环境所导致的、不断提高的带宽需求，同时降低复杂性和成本。

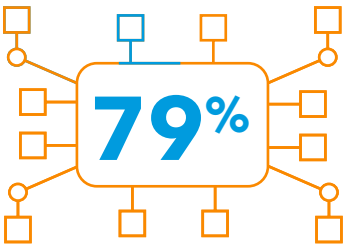
紧迫事项

保护您的 DIA 连接

虽然 DIA 连接有助于增强互联网性能并改善用户体验，但它需要一种新方法来保护 Web 流量。通常，通过使用本地硬件设备（如企业防火墙或安全 Web 网关 (SWG)）将流量回传到中心点以进行检查和控制，从而确保分支机构的企业 Web 流量安全。但是，在使用 DIA 时，依赖于这些中央控制和检查技术的传统安全解决方案已经过时。相反，企业现在经常跨地域在每个分支机构组合使用防火墙、端点防病毒以及重复架设的硬件和设备堆栈。这些很快就为 IT 管理带来了挑战。它们的性能通常不一致，维护成本也很高。最终，这种拼凑在一起的防御手段可能会使分支机构及其用户面临高风险。

当然，幕后永远存在一个越来越危险的网络威胁环境，在这种环境下，安全漏洞风险每天都在增加。

那么，如何轻松保护您的分支机构 DIA 连接，防止破坏性的漏洞?



的业务负责人报告称，他们的企业采用全新和新兴技术的速度超过了解决相关安全问题的速度。[2]

70%

经历重大事故的企业无法重新开业，或会在三年内倒闭。[3]

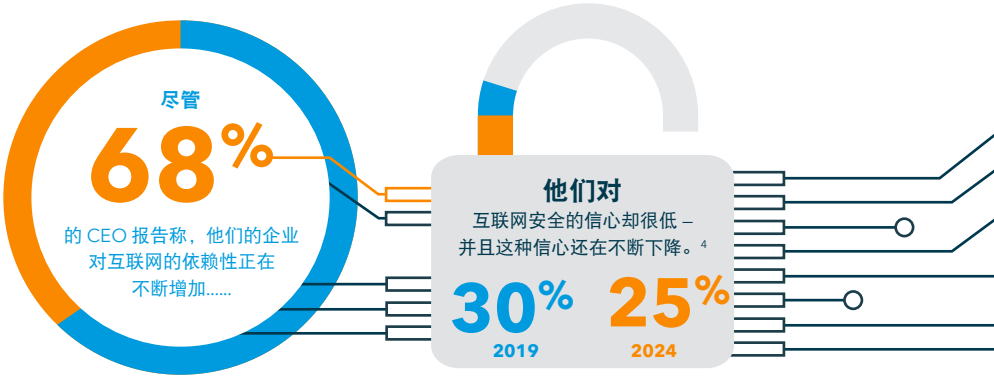
解决方案

使用云技术来实现安全的 DIA 连接

基于云的安全互联网网关 (SIG) 就是答案。通过使用这样的解决方案，安全团队能够确保所有用户和设备安全连接到互联网 — 防止恶意软件、勒索软件、网络钓鱼、DNS 数据泄漏和高级零日攻击 — 而不考虑其隶属关系、类型或位置。此 SIG 平台将使用实时威胁情报并利用域名系统来全面监控互联网活动，从而阻止所有端口和协议上的威胁 — 无论用户是在公司网络内还是在公司网络之外。

作为云交付解决方案，SIG 通过轻松即时的部署、配置和可扩展性进一步提升了分支机构的安全性。通过统一管理门户，可在几分钟内完成全球范围内企业级更新和策略更改，并保证 100% 合规。由于没有要安装的硬件或软件，后续管理工作可以忽略不计。

最后，与 SWG（通过代理检查合法和恶意流量）不同，SIG 使用 DNS 作为其初始安全控制点，仅将有风险的流量发送到代理进行检查。安全流量直接发送到互联网。这种方法可以提高性能，消除延迟，并减少因代理所有流量而导致的受破坏的网站和应用程序数量。基于云的 SIG 还可以减少安全事件和误报，从而最大限度减少帮助台请求，并释放 IT 资源以满足其他更具战略性的业务需求。



访问 **akamai.com/etp**，详细了解 Akamai 基于云的简单托管解决方案，该解决方案可保护您的分支机构 DIA 连接。

资料来源

1) https://www.riverbed.com/document/fpo/Key-Requirements-for-SD-WAN-RVBD-WP.Final.pdf
2) Accenture《2019 战略报告： 保护数字经济，重塑互联网信任》
3) https://dataconomy.com/2018/03/12-scenarios-of-data-breaches/
4) Accenture《2019 战略报告： 保护数字经济，重塑互联网信任》