Akamai

白皮书

2023 年分段现状

事实证明，克服部署过程中的障碍意义非凡

目录

前言

IT 安全部门的工作从来都不轻松。而如今的攻击者也变得越来越狡诈，他们花样翻新地发起更大规模、更频繁的攻击，使得安全团队处于巨大的压力阴影下。任何一家企业的运营都离不开网络，但只要攻击者有一次入侵得逞，就可能对企业声誉和收入造成严重甚至无可挽回的损失。

本报告的调查结果显示，这些攻击的影响日益深重，迫使安全负责人必须选择正确的解决方案，确保整个环境安全无虞，并且还不能对总体性能或创新能力造成不利影响。

自 2021 年以来，我们一直在更新本报告的调查结果，希望借此来探索分段技术是不是企业的首选解决方案，并确定其是否有效。在 1,200 名受访者中，绝大多数人都认为分段能够有效且持续地保护资产，但在围绕其关键业务应用程序和资产进行部署的整体进度方面，分段解决方案的表现却又不尽如人意。在各个地理区域，企业面临的最大障碍一直是缺乏部署分段解决方案方面的专业知识，这也导致团队可能会担心对性能造成破坏，因而犹豫是否应该启动这样一个项目，特别是在 IT 环境日益复杂的情况下，他们愈发谨慎。

好消息？坚持不懈终有回报。事实证明，对于已经对大多数的关键资产进行了分段的企业来说，这一举措在抵御威胁方面具有重要意义。与仅有一项资产实现分段的企业相比，他们抵御和控制勒索软件威胁的时间缩短了 11 个小时。想像一下，这 11 个小时的时间对您的团队、客户、品牌声誉和收入会产生何等影响。

勒索软件攻击日益猖獗，影响也越来越严重

过去两年内，勒索软件攻击（包括得逞和未得逞的攻击）数量增加了一倍，从 2021 年的平均 43 起增加到 2023 年的 86 起。我们从被近 90 个不同勒索软件团伙入侵的网站收集了数据，这些数据显示，2023 年第 1 季度的勒索软件攻击数量相比 2022 年第 1 季度呈现出更明显的上升趋势。2023 年 8 月发布的《勒索软件异常活跃：漏洞利用技术花样翻新，零日漏洞深受黑客青睐》指出，对零日漏洞和一日漏洞的利用已导致全球勒索软件受害者总数增加了 143%。

毫不意外的是，美国公司受到的勒索软件威胁次数仍然最多（图 1）：据该国的 IT 安全团队和决策者报告，过去 12 个月内受到的勒索软件攻击平均达到了 115 次，在各个国家/地区中高居首位。

不同国家/地区在过去 12 个月内遭受的勒索软件攻击平均次数

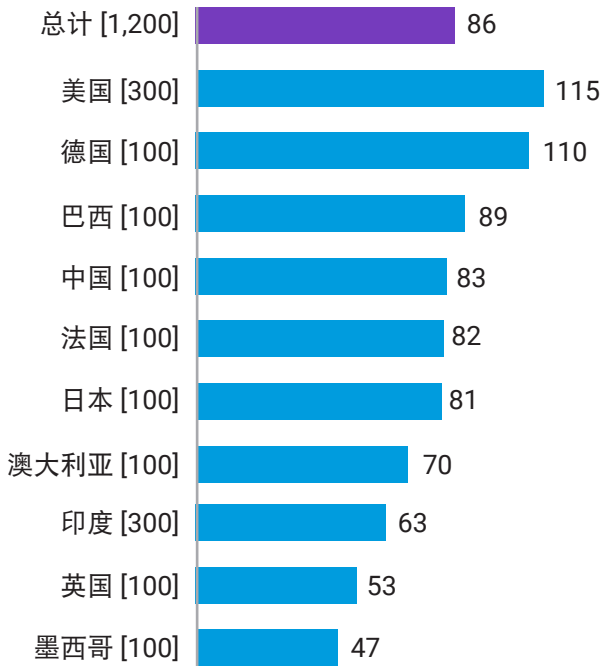

图 1：过去 12 个月内，贵企业有多少次成为了勒索软件攻击的目标（无论攻击是否得逞）？[1,200]，此处仅显示了各个国家/地区在过去 12 个月内遭受攻击的平均次数。

全球有两个国家/地区在两个以上关键业务领域实施分段的可能性较低，美国便是其中之一（图 2）。由此可见，它在遭受勒索软件攻击次数方面的排名最高与在分段部署方面的排名较低不无关联。

当然，美国之所以遭受的勒索软件攻击次数最多，可能还有其他诸多原因，其中之一在于重大攻击事件具有颇高的新闻价值，例如俄罗斯网络犯罪团伙于 2023 年针对美国联邦机构发动了攻击。另外一大原因就是美国的物联网设备激增（比排名第二的中国多出 20 亿台）。针对物联网的勒索软件 (R4IoT) 会利用易受攻击的物联网设备（如 IP 摄像头）实现初步入侵，然后在 IT 网络内进行横向移动，并利用不完善的安全实践来劫持关键任务型进程。

与 2021 年相比，2023 年的全球勒索软件攻击不仅变得更加频繁，其影响也愈发严重（图 3）。我们的受访者纷纷表示，其内部的网络中断、数据丢失和声誉受损都呈上升趋势，这些无一不让安全团队所面临的风险大大提升。这一压力同时也体现在了战略层面上：持续更新网络安全战略或策略的企业数量从 2021 年的 5% 增加到了 2023 年的 13%，这不仅是为了抵御勒索软件攻击，也是为了应对不断变化的攻击面。工作团队和应用程序越来越分散，数据也在逐渐迁移到云端，而这只不过是日常影响安全策略的其中两个因素。

已对两项以上的资产/业务领域实施分段的国家/地区

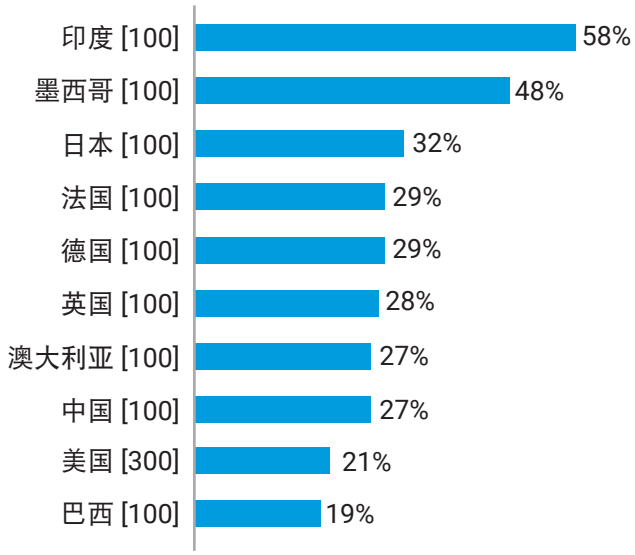

图 2：以下每项 IT 安全措施分别覆盖了哪些资产（如果有）？[1,200]，仅显示针对分段安全措施的回答以及使用分段来保护关键资产的百分比，按国家/地区划分。

勒索软件/网络攻击的影响

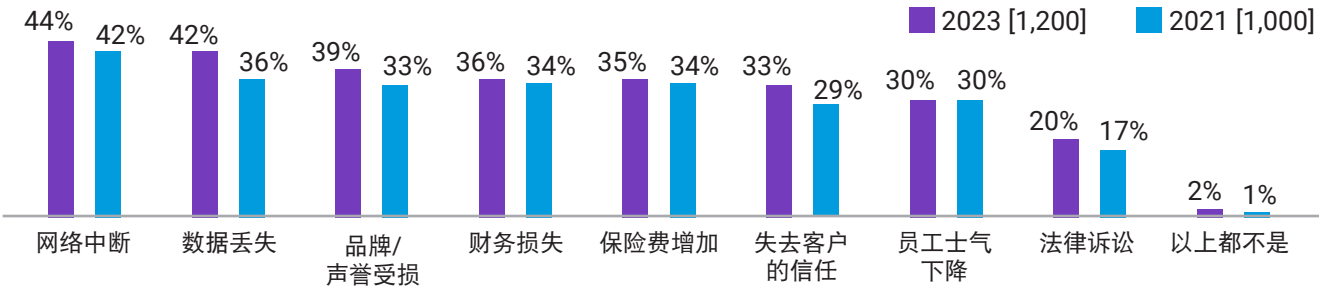

图 3：如果贵企业之前曾检测到勒索软件或其他形式的网络攻击，它对贵企业造成了以下哪些影响？[图中所示为基本规模]，未显示所有回答选项，按历史数据划分。

区域要点

网络攻击者更有可能以美洲企业作为目标：美洲遭受勒索软件攻击的总次数最多，过去 12 个月内平均达到 96 次，而欧洲、中东和非洲地区及亚太地区分别只有 83 次和 75 次。

相比欧洲、中东和非洲地区，亚太地区和美洲对分段和微分段的重视程度更高：亚太地区和美洲的 IT 安全团队和决策者更有可能认为网络分段对确保其企业安全极为重要，比例分别达到了 62% 和 60%，而欧洲、中东和非洲地区的这一比例只有 53%。

在美洲企业中，更有可能表示实施微分段是最高优先事项的比例为 41%，而在亚太地区及欧洲、中东和非洲地区，该比例分别为 35% 和 23%。

欧洲、中东和非洲地区更有可能完全不实施分段的企业：在欧洲、中东和非洲地区，有可能表示完全不对关键业务资产实施分段的企业比例达到了 10%，而亚太地区和美洲的这一比例则低得多，分别只有 4% 和 1%。

部署速度最慢，也就是未对任何领域实施分段的企业在英国的比例最高 (23%)，其中认为传统设备是主要障碍的企业比例为 46%。

亚太地区实施分段的企业比例最高：亚太地区更有可能已对两项以上的关键业务资产实施分段的企业达到 36%，而欧洲、中东和非洲地区和美洲的该比例分别为 29% 和 26%。

所有地区的企业都遇到了各种挑战：97% 的美洲企业表示，他们在对自己的网络实施分段时遇到了问题。欧洲、中东和非洲地区及亚太地区的情况也与其类似，该比例分别为 94% 和 97%。

欧洲、中东和非洲地区及亚太地区的许多企业均表示，他们实施分段的最大障碍在于缺乏相关技能/专业知识（该部分比例分别为 38% 和 43%）。而美洲的企业则认为，最大障碍来自性能瓶颈的增加 (41%)。

更多的美洲企业认为自己的 Zero Trust 安全框架已经比较成熟：在美洲企业中，更有可能表示自己的 Zero Trust 部署已非常完善且清晰的比例为 49%，而在亚太地区及欧洲、中东和非洲地区，该比例分别为 35% 和 33%。

分段是 Zero Trust 中公认的重要组成部分

我们的受访者普遍认同分段是一种确保企业安全的重要策略，特别是在抵御恶意软件方面。在各个行业中，有 93% 的企业相信这是帮助抵御破坏性攻击的关键。而在生产制造业中，这一比例更是高达 99%。这种情况有因可循，这些行业高度依赖于其供应链中的大量第三方，一旦遭受破坏，很可能会对整个企业产生巨大的级联效应。

在 Zero-Trust 框架中，分段也发挥着重大的作用。在解释为什么会启动分段项目时，排名第三的最常见回答是为了推动实施 Zero Trust：在已完全实施分段的所有企业中，大多数都正在或已经部署了 Zero Trust 安全框架 (99%)，但只有五分之二 (40%) 的受访者表示其 Zero Trust 框架已完全清晰且完善。

在全球范围内，大多数受访者都希望更进一步实施微分段，从而对应用程序工作负载实现精细的保护：89% 的受访者表示微分段至少是一项高优先级事项，其中 34% 的受访者认为这是他们的最高优先事项。此外，有 97% 的 IT 安全团队和决策者表示，其所在行业中至少已有少部分企业采用了微分段。而在公共部门（包括医疗保健行业），这一比例只有 80%。之所以存在这种差异，其中一个原因可能在于预算紧张，并且传统基础架构也对部署微分段的工作负载级保护造成了更大障碍。

微分段

的 IT 安全团队和决策者表示，其所在行业中至少已有少部分企业采用了微分段。

但是，实施微分段这样的先进安全技术同样能让公共部门大为受益。该行业中的系统在设计时不一定考虑了彼此之间的交互，因此会缺乏互操作性，这也造成人为失误和网络攻击得逞的可能性增加。

在分段方面，15% 的公共部门受访者表示其所在部门没有实施分段，但其中 93% 的受访者都认可这项技术的重要性。这意味着公共部门的部署程度最低，而其最大的障碍在于合规要求 (52%)。

分段是一项不错的技术，微分段则更为有用。

分段这种架构级方法可以将网络划分为较小的区段，其目的在于增强性能和安全性。

微分段则是在单个工作负载级别将网络划分为区段，从而能够为每个不同的区段制定安全控制措施和服务交付方法。

部署虽然缓慢，但坚持就是胜利

遗憾的是，尽管分段已被公认为阻止攻击的关键，但分段的部署仍然很缓慢，至少没有预期的那么快。2023 年，只有 30% 的企业在两个以上的关键业务领域进行了分段（相较而言，2021 年为 25%），而 44% 的企业在两年前或更早便开始了网络分段项目，这表明此项工作已处于停滞状态。

受访者明确指出，造成部署缓慢的主要障碍包括：缺乏分段方面的技能/专业知识 (39%)、性能瓶颈增加 (39%) 以及合规要求（38%；见图 4）。无论受访者所属的部门、行业或国家/地区如何，几乎所有受访者都报告了相同的障碍，只是程度略有差异而已。值得注意的是，缺乏相关技能/专业知识是造成分段项目延迟的第一大原因，整个网络安全行业都面临着人才短缺的现状，而这一领域的变化实在太快，存在技能缺口几乎成了必然结果。

尽管进展缓慢，但整体的分段实施速度仍在逐渐提升。从 2021 年到 2023 年，对关键业务应用程序/数据实施分段的企业比例上升了 12%，对服务器实施分段的企业比例上升了 8%。

实施网络分段时遇到的障碍

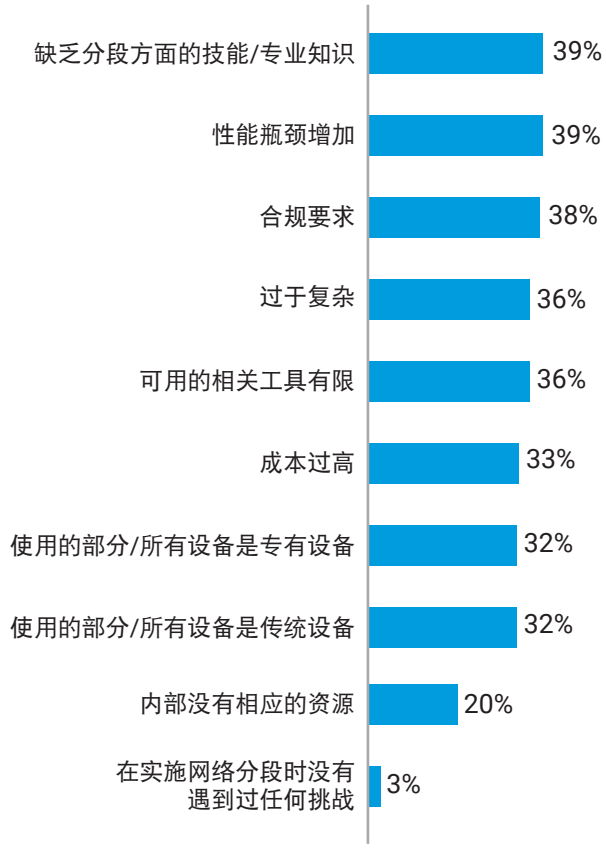

图 4：贵企业在实施网络分段时遇到过/预计会遇到什么样的问题（如果有）？[1,187]，仅显示已实施网络分段的企业的数据，未显示所有回答选项。

要点总结：对六个关键业务领域实施分段可显著降低风险

对更多资产实施保护和分段可立竿见影地提高企业的安全性。安全团队能够更容易地识别攻击，并且更有效地作出响应。如果实施的分段策略不够成熟或明确，只会增加企业的风险。但只要方法得当，为克服障碍并实施分段所付出的一切努力就会有所回报。

我们的调查结果显示，在实施分段的情况下，遭受入侵后恢复的时间缩短了 11 个小时。来做一道数学题：企业在所有六个关键业务领域实施分段之后，平均只需要 4 个小时就能完全阻止勒索软件攻击；但如果只是对一项资产实施了分段，则需要 15 个小时。

同样，实施分段后，限制横向移动所用的时间也缩短了 11 个小时。企业在所有六个关键业务领域实施分段之后，平均只需要 3 个小时就能明显遏制勒索软件攻击的横向移动。如果只是对一项资产实施了分段，则平均需要 14 个小时。

想像一下，不论在哪种情况下，这 11 个小时对您的团队有何意义，对控制成本和品牌损失又有何帮助。

阻止攻击

4 小时

已对所有六项业务资产实施分段的企业完全阻止勒索软件攻击平均所用的时间

仅对一项资产实施分段的企业：**15 小时**

限制移动

3 小时

已对所有六项业务资产实施分段的企业明显限制勒索软件攻击横向移动平均所用的时间

仅对一项资产实施分段的企业：**14 小时**

基于软件的微分段解决方案如何帮助应对挑战

微分段不仅能够实现更先进、更精细的分段，其实施也更为容易。

在部署 Akamai Guardicore Segmentation 这样基于软件的解决方案时，无需对网络进行任何物理更改即可迅速完成。您不需要为新的区段重新分配 IP，也不用担心服务器和设备的物理位置在何处。与防火墙和 VLAN 等基于基础架构的方法相比，这一优势可以大大加快和简化该解决方案的部署。由于该解决方案使用自己的专有驱动程序来推动策略实施，因此可以跨不同机器和操作系统无缝地发挥作用，包括从裸机服务器到多云部署，从 Windows Server 2003 之类的传统技术到最新的物联网/OT 设备和容器化技术。这意味着您只需要在一个界面上管理一个解决方案，就能监测和控制整个环境中由不同操作系统和设备建立的连接，而不必考虑它们的物理位置在何处。

它是如何简化部署的

微分段首先会生成一个互动视图，其中包含在您的环境中建立的所有连接，这是克服主要部署障碍的一个关键组成部分。此外，针对性能瓶颈和合规要求，Akamai 还在我们的解决方案中融入了各种主动应对方法。

性能瓶颈的起源并不一定是由于分段解决方案而对系统造成的技术性压力，也可能来自员工队伍所存在的瓶颈，他们也许要手动对业务领域实施分段，还需在出现问题时手动进行故障排除。Akamai 减少了对手动分段的要求，并且提供了出色的技术支持和专业服务，从而有效解决这一问题，同时消除了最大的部署障碍：缺乏专业知识。我们的分段技术专家将在整个部署过程中与您通力合作，确保在您在自身特有的 IT 环境中成功实现分段目标。

该解决方案本身也提供了部署支持：它附带了由 AI 驱动的策略建议以及适合常见用例的开箱即用策略模板，可以节省时间和精力、简化工作流程、缩短实施策略的整体时间，同时防止由于人为失误而造成的错误配置。以我们的一家客户为例，我们仅仅用了一位工程师和六周的时间，就完成了一项预计需要花费两年时间、总成本超过 100 万美元的精细化分段项目，使项目总成本降低了 85%。这证明精细化分段的部署同样可以快速、轻松地完成，并且不会造成任何瓶颈问题。

它是如何简化合规的

许多客户在部署我们的解决方案时，都希望能够确保并证明符合国内外的各种合规要求，例如 PCI-DSS、SWIFT、Sarbanes-Oxley、HIPAA、GDPR 等等。这些规定通常要求在您的环境中将保护范围内的数据与其他系统隔离开来。虽然使用防火墙和 VLAN 也可以达到类似的效果，但我们基于软件的解决方案却允许您专门为保护范围内的数据创建区段，并制定关于可以和不可以访问此类数据和通信规则。我们的可视化示意图中包含近乎实时视图和历史视图，使您可以实际展示保护范围内的数据并未受到未经授权用户和机器的访问，从而证明符合这些规定。

利用正确的解决方案和支持转变企业安全态势

分段的实施可能会非常困难。但正如本报告所述，一旦实施成功，就能有效降低网络风险。实施正确的分段策略之后，将能够限制威胁的横向移动，并允许您在遭受入侵时更迅速地作出响应。而在入侵事件过后，也能明显减少恢复工作所需的精力和时间。

只要选择一种能够克服分段部署常见挑战的解决方案，并在整个实施过程中与经验丰富的专家开展合作，必将能够顺利地彻底转变您的安全态势。此外，分段的业务领域越多，就越能降低当下风险，同时确保针对未来的威胁媒介构筑第一道防线，从而推动您的 Zero Trust 架构发展。

我们的调查团队

我们对 10 个国家/地区的 1,200 名 IT 和安全领域的决策者进行了采访，旨在评估企业在保护自身环境方面的进步，并重点关注分段技术在其中的作用。

受访者回答了各种问题，涉及其 IT 安全方法、分段策略以及他们的企业在 2023 年可能面临的威胁。这些发现使我们得以洞察自 2021 年以来安全策略的演变，以及仍需努力改进的领域。

接受我们调查的安全人员和决策者来自美国、墨西哥、巴西、英国、法国、德国、中国、印度、日本和澳大利亚。他们为拥有超过 1,000 名员工的企业工作，来自不同的行业和部门，使得调查结果更具普遍性。

注意：本次调查的样本与 2021 年略有不同。样本规模——2023 年：完成量 1,200 份，2021 年：完成量 1,000 份。2023 年，来自澳大利亚、日本和中国的受访者也接受了访问。调查的行业与 2021 年略有不同。2023 年，我们有意将数字商务作为一个单独的行业予以关注。

了解有关 Akamai Guardicore Segmentation 的更多信息

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、保护应用程序和 API 并保护您的基础架构，让您信心十足地不断创新、发展和转型。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，或者扫描右侧二维码，关注我们的微信公众号。发布时间：2023 年 10 月。

扫码关注，获取最新CDN前沿资讯

Vanson Bourne 是一家面向科技行业的独立市场研究专业机构。他们以稳健、可靠的研究型分析而闻名于世，其成果源于严格的研究原则，及其在所有商业领域和所有主要市场中寻求技术和商业职能部门高级决策者意见的能力。有关更多信息，请访问 www.vansonbourne.com。