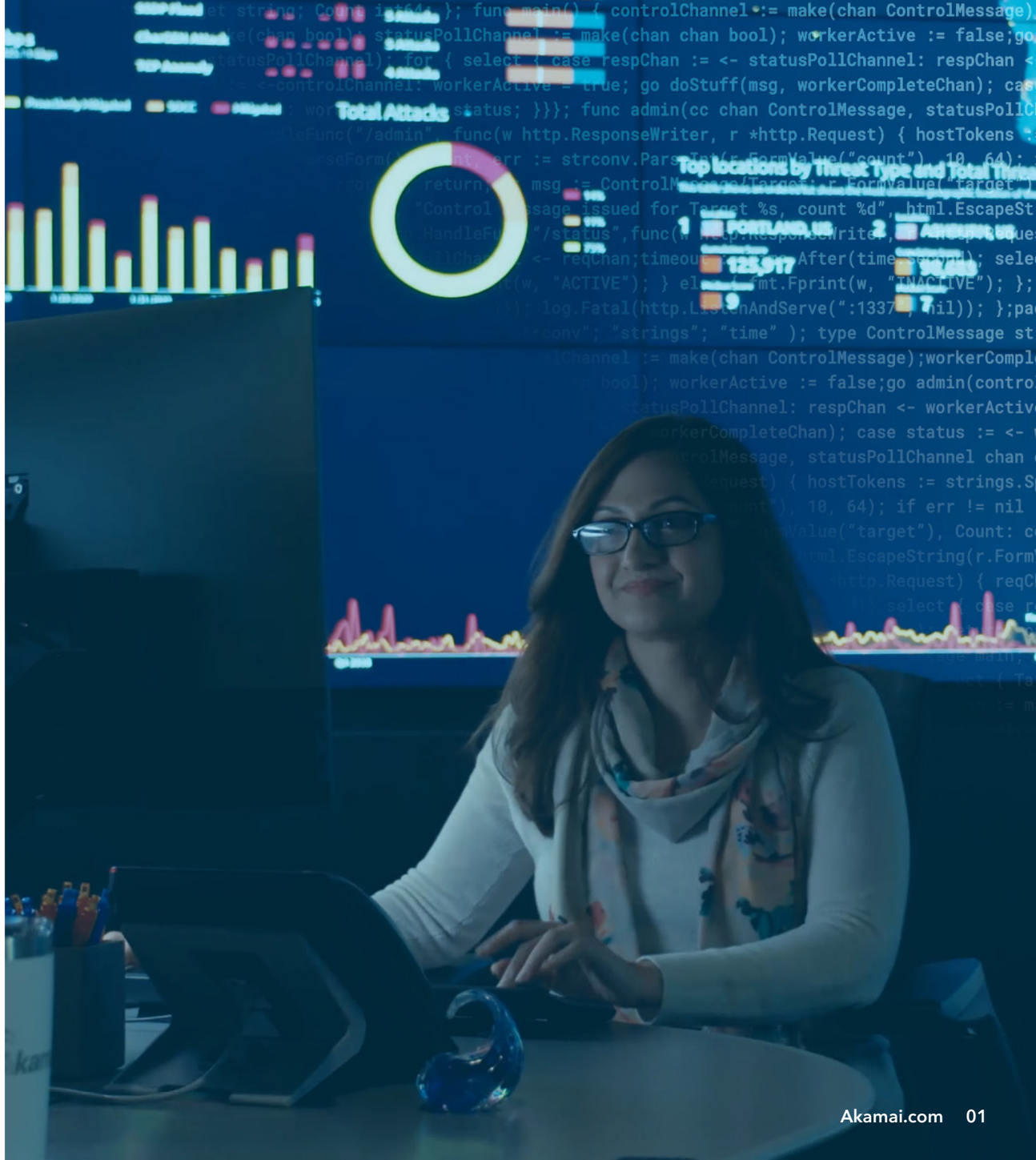
混合云世界中的 DDoS 防御

电子书

混合云世界中的DDoS 防御

分布式拒绝服务 (DDoS) 是最古老的网络威胁之一，它仍然是实施大规模破坏的热门手段，几乎对各种类型的企业（无论大小）都构成了安全隐患。实际上，根据 IDC 的数据，到 2023 年，DDoS 攻击预计将以 18% 的复合年增长率增长，这清楚地表明，企业是时候增加对强大缓解控制措施的投资了。尽管有些企业可能认为他们是 DDoS 攻击的低风险目标，但如果基础架构得不到保护，在企业越来越依赖互联网连接来为关键业务服务和应用程序提供支持的情况下，每个人都会面临停机和性能下降风险。



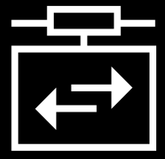
不断演变的威胁

DDoS 攻击的规模每两年翻一番，它在攻击媒介的数量和组合方面具备前所未有的复杂性。由于应用程序和网络可用性对业务连续性至关重要，恶意攻击者希望发起容量耗尽攻击、协议攻击和应用程序层 DDoS 攻击，以破坏任何潜在的故障点，使最终用户无法使用面向互联网的资源和资产。

DDoS 攻击者会以任何潜在的故障点为目标，例如：

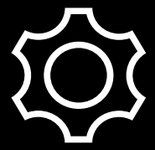
网站

Web 应用程序和
其他企业服务



VPN 集中器
（用于远程访问公司资源）

SD-WAN 控制器



应用程序编程接口 (API)

域名系统 (DNS)
和源站服务器

数据中心和网络基础架构

通过对这些受害环境、应用程序和 IP 空间进行侦查，攻击者可以确定哪些 DDoS 媒介将对面向互联网的服务和源站托管基础架构造成最大的潜在损害。由于进入门槛很低，这些恶意攻击者可以借助大量攻击技术和工具（例如引导程序、DDoS 租用等）来帮助发现企业防御中的弱点或漏洞。

> 恶意攻击者有着不同的动机，包括勒索和财务操纵。Akamai 观察到，勒索活动正在扩展到金融领域以外，开始针对商业服务、游戏、旅游和酒店、高科技、物流以及零售行业。
>
> - Akamai 全球安全运营副总裁
> Roger Barranco

随着企业尝试扩展和保护远程访问功能，以确保员工的工作效率和企业的正常经营，DDoS 攻击的影响在加剧。

DDoS攻击的后果

在网络（第 3 层）和传输（第 4 层）层攻击中，基于容量耗尽和协议的攻击试图填满互联网管道，让服务器不堪重负并耗尽状态表条目，以使网络和服务不可用。借助基于应用程序的攻击（第 7 层），恶意攻击者旨在通过低速攻击和慢速攻击以及 HTTP 泛洪攻击等媒介来产生影响正常运营的停机，从而破坏 Web 性能和用户体验。

但停机造成的不良后果影响到的不仅仅是因遭受攻击而变为不可用的服务和应用程序的成本。*根据 Ponemon Institute 的数据，企业遭受的 DDoS 攻击的平均年度成本为 170 万美元*，这一成本来源于技术支持增加、事件响应资源消耗、内部上报流程、法律成本、运营中断和员工生产力损失。

显然，风险越来越高，并且随着向混合云基础架构迁移的增加，这种风险还会进一步增长。

云的采用继续使安全状况变得复杂

随着企业停用传统数据中心并将应用程序移至云托管环境，安全架构变得更加复杂。许多企业都难以采用与数据中心内相同的 DDoS 防御水平来保护面向互联网的资产。更复杂的是，许多云托管 IP 不在企业的直接控制范围之内，如果没有适当的保护，它们很容易遭受成功的 DDoS 攻击。

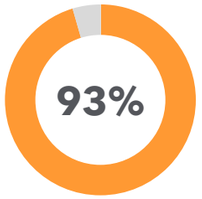
恶意攻击者非常清楚这种向主机代管设备和公共云加速迁移的过程。不一致的安全策略和要求导致企业安全架构和态势存在缺陷，企业在分散且碎片化的云托管基础架构中进行故障排除时也面临众多困难，因此攻击者希望利用这些弱点。

结论：

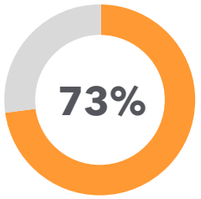
现代企业需要采取自适应防御机制，以保护各种面向 Web 的资产和服务（无论它们位于何处）。随着超过 93% 的企业（<1,000 名员工）采用多云战略，现在是时候修复由基础架构复杂性导致的防御漏洞了。[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

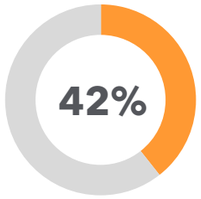
各家提供商对于公共云环境中的安全性的责任可能并不一致，使得许多做出错误假设的企业可能会使自身面临风险。例如，在 IBM 的一份调查中，有 73% 的企业受访者认为公共云服务提供商 (CSP) 是负责保护软件即服务 (SaaS) 的主要责任方，而 42% 的受访者认为，CSP 主要负责保障云基础架构即服务 (IaaS) 的安全。安全控制责任归属的缺乏会导致出现漏洞 - 这是任何企业都不愿接受的风险。



的企业采用多云战略



的调查受访者认为公共 CSP 负责保障 SaaS 安全



的受访者认为 CSP 负责保障云 IaaS 安全

Forrester 在最近的一篇文章中指出，大多数企业正在选择一种混合策略方法，该方法利用了多个公共云提供商并托管本地工作负载。因此，该分析公司建议选择可跨混合架构实现保护的 DDoS 缓解提供商。

恶意攻击者只需做对一次即可。
公司需要响应迅速的缓解控制
措施来进行反击。

并非所有 DDoS 缓解措施都具有同等的效力

随着企业继续对云基础架构进行投资，安全团队在确保跨混合环境的一致控制方面仍然面临挑战。为跨多个后端云基础架构部署的应用程序提供保护变得越来越困难，因此，许多企业都希望通过单一控制点来编排防御措施。随着安全技术堆栈变得越来越复杂，许多企业也希望拥有这种单一的控制面板 - 不仅是为了优化可见性，也为了通过 API 将优化的报告馈送到事件数据关联系统中。

*为了解决此问题，企业正在转投基于云的 DDoS 安全提供商，这些提供商可以支持（而不是阻止）他们的混合云迁移策略。他们希望获得可扩展且响应迅速的防御 - 无论企业服务位于何处。*这是为了直接应对在 CSP 的独特环境中集成、部署和管理 DDoS 防御措施所需增加的操作复杂性。由于存在跨多个云的众多面向互联网的资产，复杂性迅速增加。

使得压力加剧的是，许多 CSP 内部 DDoS 缓解解决方案在关键领域都缺乏足够的能力：可见性、SLA 和报告，这些因素对于增强当今企业防御能力至关重要。

对于安全团队而言，关键在于可见性，以及获得可行的见解来优化事件响应和准备。某些 CSP DDoS 解决方案在报告、可见性和攻击后分析方面几乎没有公开任何信息 - 难怪许多人将 CSP 称为分析和报告的黑匣子。

此外，某些 CSP 不提供缓解时间 SLA，而是向受影响的企业提供服务积分。当时间至关重要时，企业需要确信，他们的提供商能够全力维持正常运行和可用性，而不会影响性能。

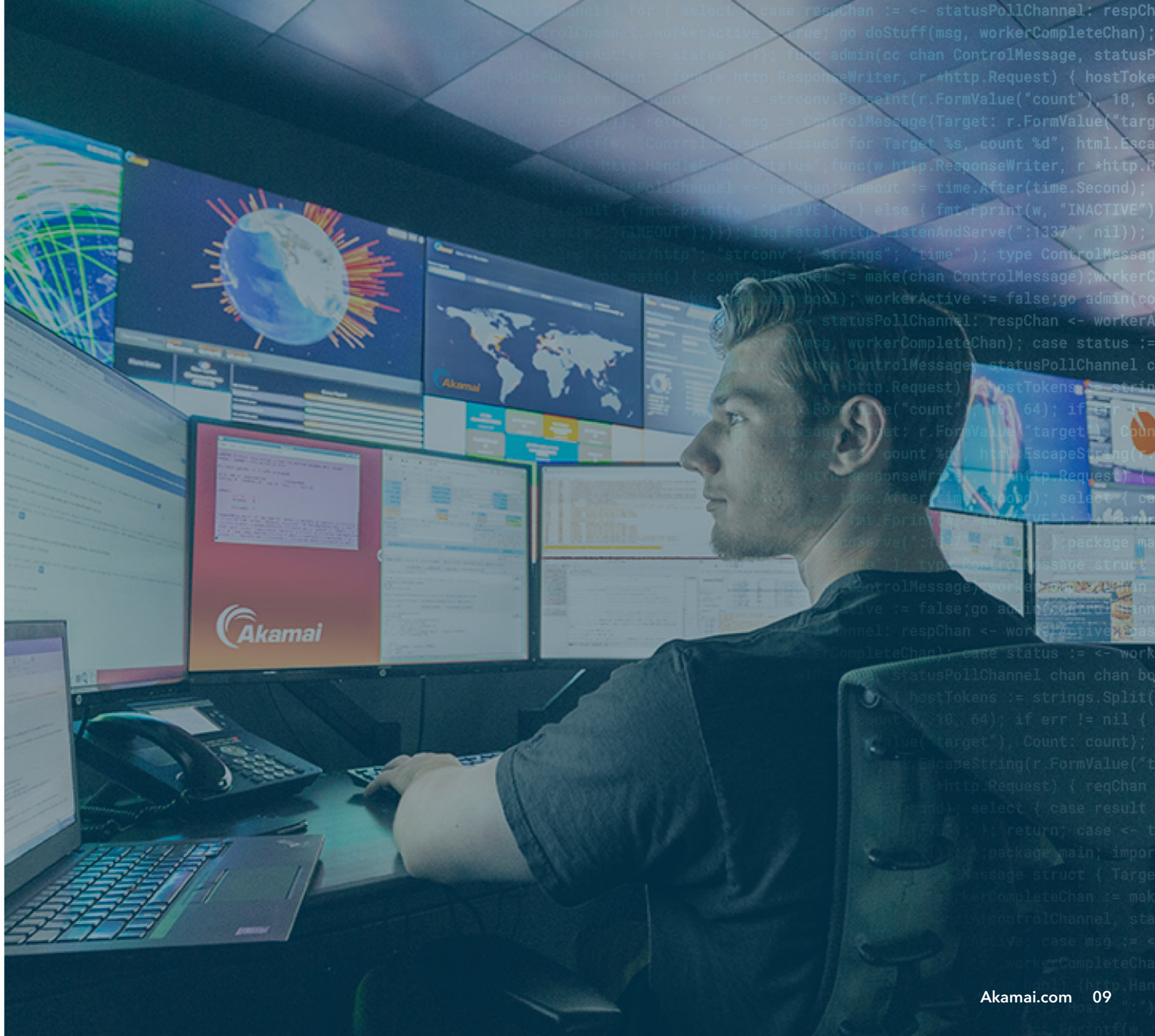
最后，许多 CSP 都不提供按需访问的全天候全球安全运营中心 SOC 支持服务，以及攻击前、攻击中和攻击后的协助，而优秀的基于云的 DDoS 缓解提供商会标配此服务。如果提供此服务，则采用增值付费的形式，并且通常比一家优秀提供商提供的专业 DDoS 缓解解决方案更加昂贵。借助完全托管的 DDoS 防护解决方案，服务提供商可以充当企业事件响应团队的扩展资源，并提供专业知识以快速响应 DDoS 事件。

在当今的威胁环境中，很明显，现代企业正在寻求 DDoS 缓解合作伙伴，这些合作伙伴可在混合环境中提供优化的安全体验，同时降低攻击面复杂性。

DDoS 缓解合作伙伴应该是云战略的推动者（而不是阻碍），以帮助缓解安全压力。

Akamai 提供的专用 DDoS 缓解解决方案

正如企业需要端到端云战略一样，他们还需要考虑端到端 DDoS 防护。通过采取整体策略，Akamai 将充当第一道防线，通过专用边缘、分布式 DNS 和云缓解策略提供保护，这些策略旨在防止附带损害和单点故障。相较于其他云安全提供商的架构作为“一体化”解决方案构建，Akamai 专门构建的 DDoS 云提供了更高的恢复能力、专用的清理容量和更高的缓解质量，可以针对 Web 应用程序或基于互联网的服务的特定要求进行微调。



Akamai 的 DDoS 缓解解决方案可在 DDoS 攻击到达应用程序、数据中心和基础架构之前，立即在云中阻止攻击。

边缘防御

Akamai 边缘 (CDN) 使用 HTTP 和 HTTPS 协议交付并加快 Web 流量。每台 Akamai 边缘服务器均充当反向代理，在端口 80 和 443 上转发合法的 HTTP/S 流量，并在网络边缘丢弃所有其他流量。这意味着，每个 Akamai 客户直接可以立即缓解所有网络层 DDoS 攻击，而且此功能内置在其 Web 交付中。

DNS 防御

同一技术也适用于 Akamai 的权威 DNS 服务 - Edge DNS，该服务会立即丢弃不在端口 53 上的所有流量。与其他 DNS 解决方案不同，Akamai 专门设计了 Edge DNS，以提高可用性和抵御 DDoS 攻击的能力以及性能，并具有多个级别的架构冗余，包括名称服务器、入网点、网络，甚至包括分段 IP Anycast 云。

云清理防御

作为经过实践检验的云清理服务，Prolexic 可保护整个数据中心和面向互联网的基础架构免受 DDoS 攻击 - 跨所有端口和协议提供保护。通过 Prolexic 路由合法和恶意流量，我们能够建立正/负安全模型，从而主动并即时地以高精度缓解 DDoS 攻击。Akamai 安全运营指挥中心 (SOCC) 专家充当了客户事件响应团队的扩展资源，以在自动检测和响应与人工参与之间取得平衡。

为什么选择 Akamai

Akamai 拥有遍布全球的大规模成熟 DDoS 缓解云。无论您是要保护单个应用程序、整个数据中心还是权威 DNS，Akamai 在设计 DDoS 缓解措施时已将大容量、高恢复能力和快速缓解考虑在内。

我们已经缓解了全球范围内发起的一些大规模 DDoS 攻击。我们的主动式缓解控制可实现真正的零秒缓解，这种 SLA 十分优秀。我们可以为多个客户端提供 DDoS 防护服务，并同时应对多个 DDoS 攻击。

Akamai

由于 DDoS 攻击媒介在不断变化且攻击规模不断扩大，因此，提供商必须不断投资、开发和部署工具和规则，以检测、编排和缓解攻击。Akamai 致力于在攻击开始之前缓解攻击，从而从容应对威胁。

您的 DDoS 缓解策略应为您的云策略提供支持。Akamai Intelligent Edge Platform 提供了 DDoS 防御来实现此目标，从而帮助客户将保护范围扩展到整个核心、云和边缘，以大幅降低风险，同时为未来云战略的发展提供灵活性。

请联系我们，以了解我们如何保护您的业务

了解更多

*Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其业务获得快速、智能且安全的体验。全球顶级品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而实现竞争优势。Akamai 使决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均可由优质客户服务、分析和全天候监控提供支持。如需了解全球顶级品牌信赖 Akamai 的原因，请访问 **www.akamai.com** 或 **blogs.akamai.com**，或者扫描下方二维码，关注我们的微信公众号。您可访问 **www.akamai.com/locations**，寻找全球联系信息。发布时间：20 年 11 月。*

扫码关注・获取最新CDN前沿资讯