混合云世界中的 DDoS 防御

目录

DDoS 不断发展进化

分布式拒绝服务 (DDoS) 网络威胁已出现多年，它至今依然在不断发展进化，并已成为网络犯罪分子和意识形态动机黑客掌握的一种高度复杂的攻击利器。实际上，DDoS 攻击不仅给大型和小型企业带来安全风险，医疗保健、能源和公共事业及教育等领域的关键公共基础设施也深受其害。

各种公私机构越来越多地采用云计算资源导致这种充满变数的局面进一步复杂化。当这些企业将云技术与其既有的本地资源相结合时，所产生的混合环境变得更加复杂。如今，应用程序、应用程序编程接口 (API)、数据、微服务和工作负载都必须通过分散的环境交换信息。这些环境所使用的不同架构产生了新的漏洞和裂纹遍布的攻击面，为网络犯罪分子发动日益复杂的破坏性 DDoS 攻击带来可乘之机。

企业都在匆忙地保护自己的数字基础架构。他们不仅需要集成的混合 DDoS 防护平台来保护本地（私有云）基础架构免受时间短但强烈的闪电战型 DDoS 攻击，还需要利用云端清洗的规模和容量来抵御大规模容量耗尽型 DDoS 攻击。

多种趋势表明，DDoS 攻击的火力会越来越强，频率会越来越高。2023 年 2 月，Akamai 帮助 Akamai Prolexic 在亚太地区 (APAC) 的一家客户成功抵御了当时规模最大的一次 DDoS 攻击，这次攻击的流量峰值达到每秒 900.1 Gb，每秒 1.582 亿个数据包 (158.2 Mpps)。而几个月前，一家位于欧洲的 Akamai Prolexic 客户刚刚遭受过一场超大规模 DDoS 攻击。在此次攻击中，流量突然飙升至 704.8 Mpps，攻击者来势汹汹地妄图中断该企业的业务运营。Akamai 还曾成功抵御一次持续近两小时，流量高达每秒 1.44 Tb (Tbps)、385 Mpps 的全球分布式攻击，这也是 Akamai 迄今为止抵御的最大规模 DDoS 攻击。事实上，根据我们对流量和攻击模式的深入了解，Akamai 判断在整个 2023 年，DDoS 攻击变得更加频繁、持续时间更长、手段非常复杂（使用了多种攻击媒介），而且集中于横向目标（在同一攻击事件中攻击多个 IP 目标）。

日益加剧的威胁

如今的大多数 DDoS 攻击都是多媒介攻击，通常会采用 10 种以上的攻击媒介压垮基本的 DDoS 防护系统和平台。实际上，根据 Akamai 的内部威胁情报，从 2022 年到 2023 年，多目标或横向 DDoS 攻击的数量翻了一番。与此同时，2023 年容量耗尽型 DDoS 攻击的整体程度、规模和持续时间都创下了历史新高。

攻击者还会花样翻新地将各种不同的攻击手段与传统容量耗尽型攻击结合使用，导致企业的安全规划进一步复杂化。

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

DNS 基础架构

针对企业 DNS 基础架构的 DDoS 攻击已变得越来越常见，尤其是 NXDOMAIN 攻击（也称为伪随机子域攻击、DNS Water Torture 攻击或 DNS 资源耗尽型攻击）。2023 年，在 Akamai 抵御的所有 DDoS 攻击中，超过 60% 的攻击都涉及到 DNS 组件，其中 NXDOMAIN 攻击约占这些 DNS DDoS 攻击的一半。这些攻击对公司的利益和声誉构成了重大风险，因为一旦公司的 DNS 出现故障，在线业务就会陷入瘫痪。

应用层攻击

由于攻击者正在不断进化其攻击手段以利用看似无害的逻辑和工作流程，应用层（第 7 层）DDoS 攻击变得更加复杂。2023 年发现的 HTTP/2 漏洞导致发生规模创历史纪录的第 7 层 DDoS 攻击。

DDoS 即服务

Anonymous Sudan 和 Killnet 等有组织的网络犯罪分子团伙现在开始提供“DDoS 即服务”。在这种情况下，这些团伙有偿提供 DDoS 服务（通常是僵尸网络）并代表客户实施攻击。对于动机明确的团伙来说，这些 DDoS 出租服务利润极其丰厚。

勒索软件 + DDoS = RDDoS

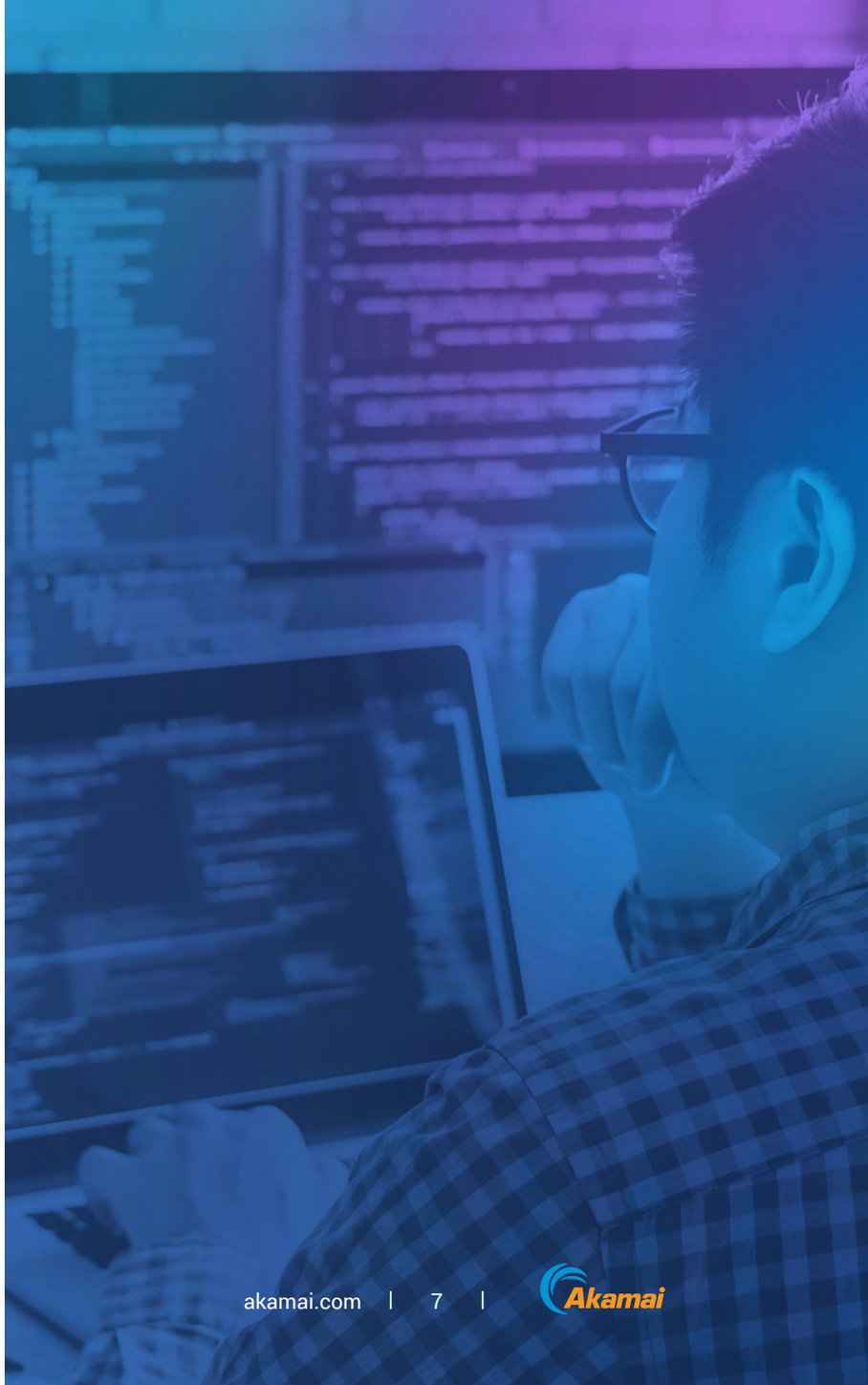
此外，“DDoS 即服务”等手段的出现也让攻击者更容易将 DDoS 攻击作为分散安全团队注意力的烟幕弹。与此同时，他们会发动勒索软件攻击或三重勒索攻击。这些攻击都称为勒索软件 DDoS (RDDoS) 攻击。

DDoS 攻击的后果

在网络（第 3 层）和传输（第 4 层）层 DDoS 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，从而使网络和服务陷入瘫痪。在第 7 层攻击中，攻击者意图通过低速缓慢攻击和 HTTP 泛洪攻击等媒介来干扰 Web 性能和客户体验，从而造成影响公司盈利的停机时间。针对 DNS 的 DDoS 攻击可能更为复杂一些——根据攻击类型，它可能会影响企业的不同网络层。例如，DNS 反射攻击和 DDoS 放大攻击可能会在公司网络的第 3 层和第 4 层产生流量，而 NXDOMAIN 或 DNS 泛洪类型的 DDoS 攻击往往会攻击网络的应用层。

除了受攻击的服务蒙受损失以及应用程序不可用导致的损失外，停机还会造成一系列长期影响。根据 Ponemon Institute 的数据，企业遭受 DDoS 带来的年平均损失为 170 万美元，其中包括了技术支持成本增加、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。此外，对于金融服务机构、游戏和媒体公司等面向消费者的企业以及电商企业来说，离线不仅会带来经济损失，更重要的是还会导致无法挽回的声誉受损。

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。

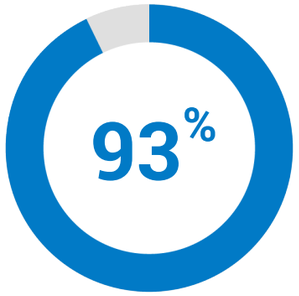


混合和多云环境在继续加大安全防护的复杂性

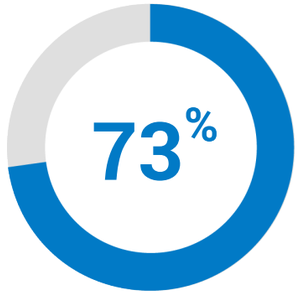
由于企业会在本地数据中心或私有云中保留一部分工作负载，并将其他应用程序迁移到公有云托管的环境中，而这种混合基础架构方法让企业更加难以构建稳健的安全防护措施。同样地，企业往往还会使用混合式 DNS 基础架构——权威 DNS 区域在云端管理，而其余的区域由本地名称服务器和全球服务器负载均衡器 (GSLB) 管理。企业可能会继续保留一些本地 DNS 基础架构的原因有很多。例如，为了满足合规要求，他们可能投入了大量资金来建立本地基础架构。将所有 DNS 迁移到云端的复杂性可能导致在经济上不可行。

攻击者非常清楚这种分散环境可能带来的漏洞。他们会想方设法地利用企业安全架构和安全态势中因不一致的安全策略和要求而产生的薄弱环节。此外，分散的云托管基础架构会加大故障排除的复杂性，这也会被攻击者所利用。

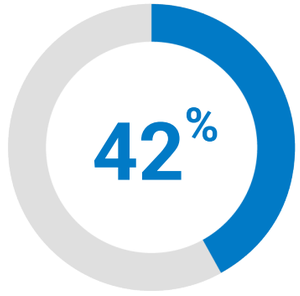
遗憾的是，公有云环境中的安全责任具体由谁负责可能因提供商而异，很多企业会做出错误的假设，导致自身面临风险。例如，IBM 的一份调查表明，73% 的企业受访者认为公有云服务提供商 (CSP) 是保护软件即服务 (SaaS) 的主要责任方，而 42% 的受访者认为 CSP 主要负责保护云基础架构即服务 (IaaS)。缺乏对安全控制责任方的了解会导致出现漏洞——这是任何企业都不愿接受的风险。



的受访者采用多云策略



的受访者认为公共 CSP 应负责保护 SaaS



的受访者认为 CSP 应负责保护云 IaaS

企业正在转而选择 DDoS 安全提供商，这些安全提供商能够提供集成且高度可扩展的综合性 DDoS 防护平台来保护企业的应用程序、API、DNS 以及为其提供支持的底层基础架构。

并非所有 DDoS 抵御措施的效果都一样

随着各公司继续在云基础架构上进行投资，确保跨混合环境的一致控制将成为安全团队面临的一项挑战。由于保护跨多个后端云基础架构部署的应用程序变得越来越困难，因此很多企业都在寻找单一控制点来编排防御措施。

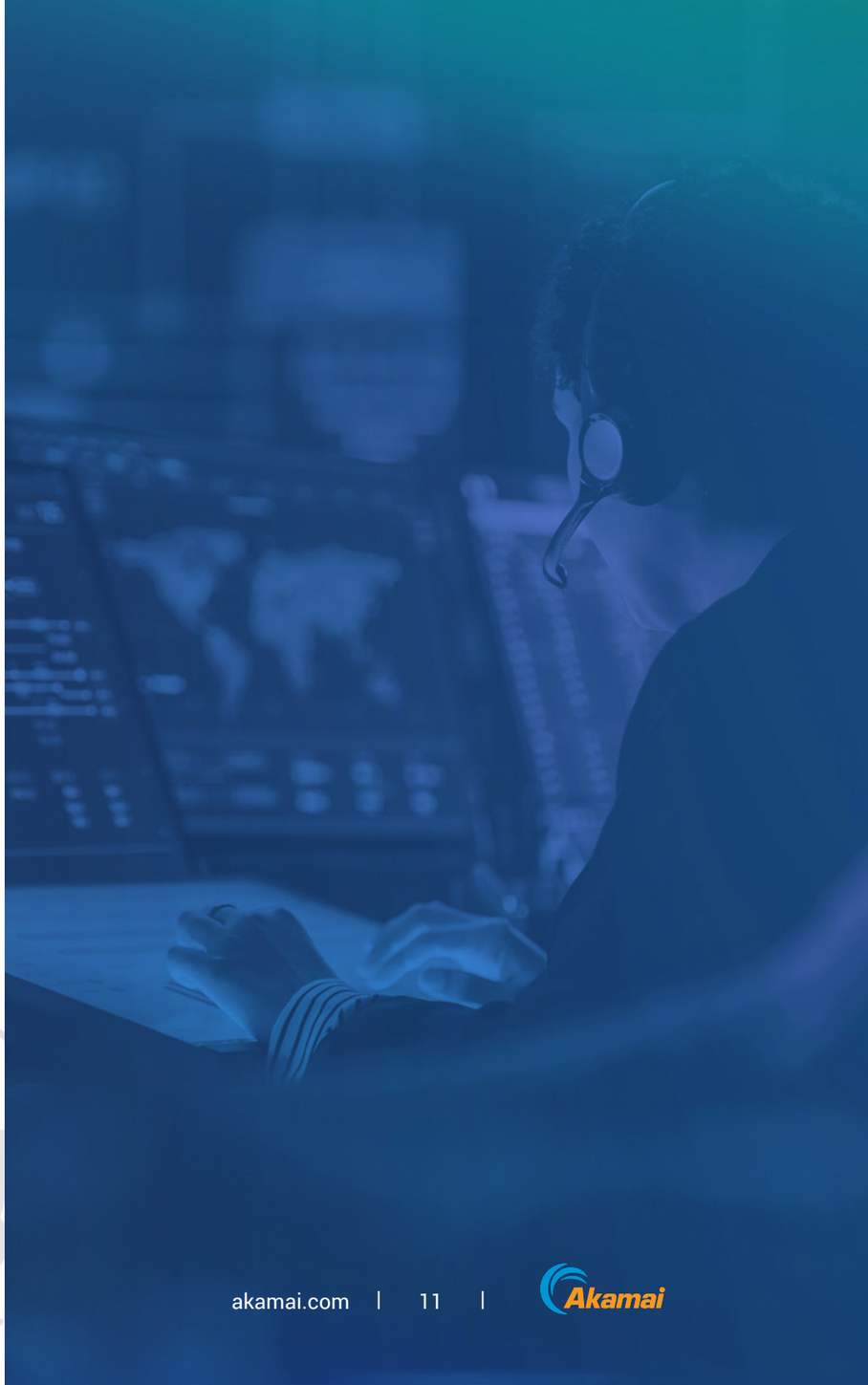
随着安全技术堆栈变得越来越复杂，很多企业希望能获得可以一览整个环境的综合视图——不仅是为了优化监测能力，也为了简化报告功能，以通过 API 直接将报告发送给事件数据关联系统。

为了解决此问题，企业正在转向 DDoS 安全提供商，这些安全提供商能够提供集成且高度可扩展的综合性 DDoS 防护平台来保护企业的应用程序、API、DNS 以及为其提供支持的底层基础架构。无论企业服务位于本地、云端还是混合环境中，他们都希望获得可扩展且响应迅速的防御措施。这有助于直接解决在 CSP 的独特环境中集成、部署和管理 DDoS 防御措施时，可能造成的操作复杂性增加的难题。不仅如此，由于很多面向互联网的资产都位于多个私有云和公有云中，导致复杂性迅速升高。

更让人头痛的是，很多 CSP 内部 DDoS 抵御解决方案在监测能力、服务等级协议 (SLA) 和报告功能等关键领域存在短板，而这些都是当今企业安全防御人员所需的重要功能。

对于安全团队而言，只有具备监测能力和获得可行的见解才能优化事件应对方案和做足防御准备。一些 CSP DDoS 解决方案在报告、监测能力和攻击后分析方面几乎没有透明性可言，难怪许多团队将 CSP 称为分析和报告的黑匣子。虽然一些 CSP 允许企业安全团队设置控制措施并保持对客户特定环境的主权，但他们通常会拒绝对 DDoS 流量承担任何责任，并且无论 DDoS 攻击是应用层攻击、网络层攻击还是 DNS DDoS 攻击，他们最终都会向客户收取这些攻击带来的海量恶意流量所产生的费用。

此外，一些 CSP 和安全供应商没有提供明确的抵御时间 (TTM) SLA，而是向受影响的企业提供服务补偿。了解 TTM 条款是否包括识别攻击的时间很重要。如果某个平台需要数分钟甚至数小时识别 DDoS 攻击，然后才开始计算抵御时间，那么受害企业可能会长时间处于离线状态。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。



此外，同样（甚至更加）重要的是，安全团队或买方企业必须确定 DDoS 安全供应商和 CSP 是否提供**专用 DDoS 防御容量**或者防御容量是否与其 CDN 网络共享。专用 DDoS 防御措施就像一支特警队，专注于对抗 DDoS 攻击并且不会与业务中的其他部分（如内容交付）共享资源或基础架构，从而确保即使发生创纪录的 DDoS 攻击时，也能将影响降至最低。在评估 DDoS 防护解决方案时，企业还要明白一点：供应商自身有时也会遭受 DDoS 攻击，因此应该重点考虑供应商是否提供正常运行时间/可用性 SLA。

最后，除了缺乏攻击前、攻击中和攻击后援助之外，很多 CSP 和安全供应商还不提供在需要时可以随时联系的全天候全球安全运营中心 (SOC) 支持服务。即使他们提供此服务，也会采用额外收费的形式，并且通常该费用比一家优秀提供商提供的专业混合 DDoS 抵御解决方案更加昂贵。借助全托管式混合 DDoS 防护解决方案，服务提供商会成为企业事件响应团队的扩充力量，并提供专业知识以快速响应 DDoS 事件。

在当今的威胁形势下，现代企业显然需要选择能够在混合环境中提供优化安全体验并降低攻击面复杂性的 DDoS 抵御合作伙伴。您的 DDoS 防护合作伙伴应该推动（而不是阻碍）您的混合或多云策略向前发展，并与您的业务目标保持一致。

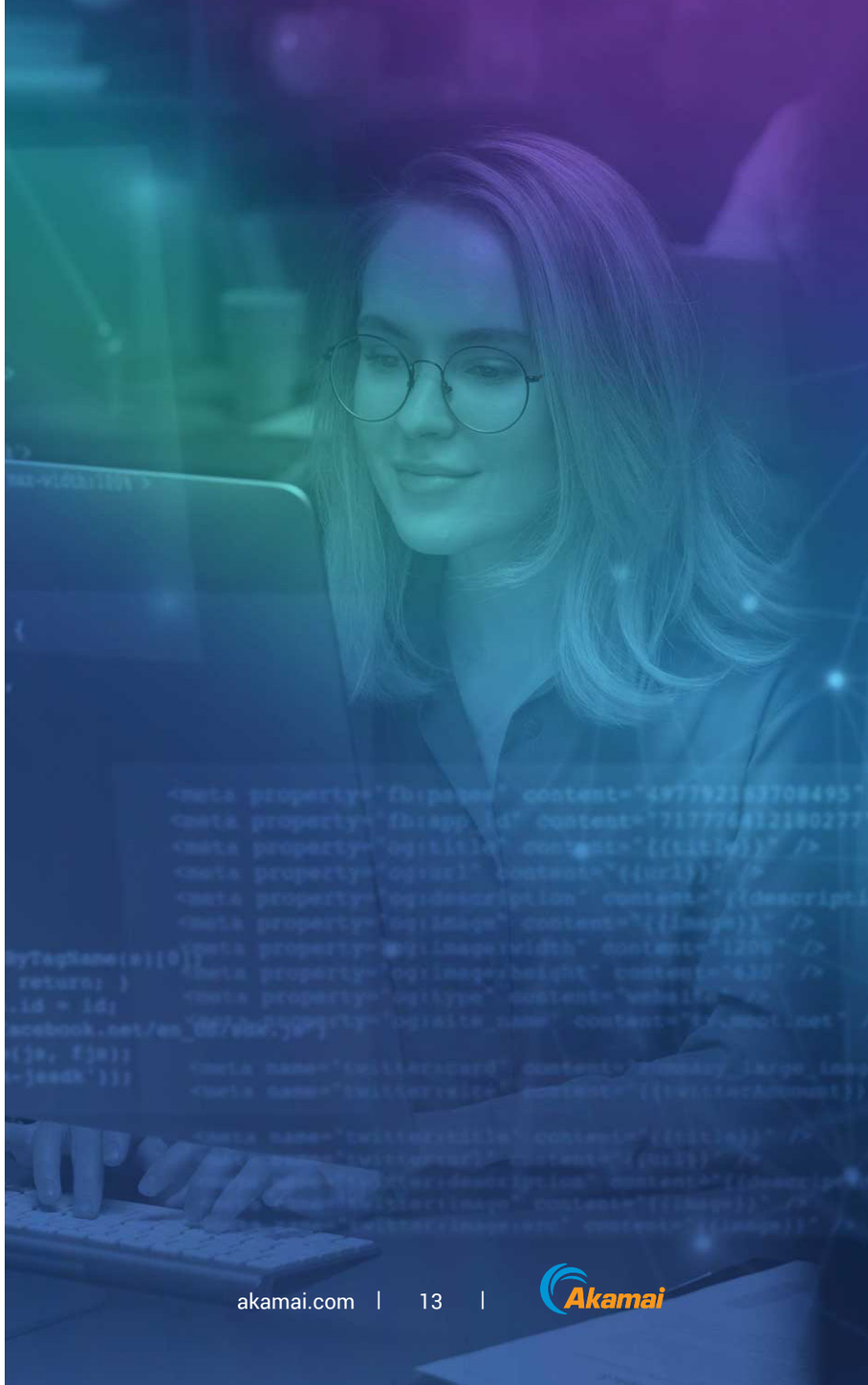
Akamai 提供的专用 DDoS 抵御措施

正如企业需要包含混合和多云环境的端到端数字基础架构战略一样，他们还需要考虑端到端 DDoS 防护。凭借全方位的防御方法，Akamai 可充当第一道防线，利用专用边缘、分布式 DNS 以及旨在防止附带损害和单点故障的混合抵御策略，为您提供保护。与其他作为一体化解决方案构建的 CSP 架构不同，Akamai 专门构建的 DDoS 解决方案提供了更高的恢复能力、专用的 DDoS 防御容量和更高质量的抵御措施，可以针对 Web 应用程序或基于互联网的服务的具体要求进行微调。Akamai 的 DDoS 防御措施能够随时随地满足客户对使用场景（本地、云端、混合）以及使用方式（不间断或按需）的需求。此全方位保护涵盖三个核心产品。

专用 DDoS 防御容量

分布式 DNS

混合抵御措施



Akamai Prolexic 是专为帮助企业实现积极主动的安全态势而量身定制的卓越 DDoS 防护产品

可扩展的现代架构

Akamai Prolexic 使用完全软件定义式架构，该架构可以适应与边缘计算、5G/6G 及网络虚拟化相关的不断变化的网络趋势。随着平台向虚拟化软件环境转变，Prolexic 彻底消除了对专用硬件的依赖。这种标准化部署使 Akamai 能够针对不断变化的客户需求更快地提供服务，方便进行模块化部署以实现容量扩展，通过低延迟链接扩大区域覆盖范围，并提高平台的冗余度。此外，该架构还有助于加快 Prolexic 高级行为学习能力的提升，使平台能够从攻击特征中学习、适应新兴威胁媒介，并提前为客户建设能抵御 DDoS 的安全环境。Prolexic 云服务**由分布在全球 32 个都市区的多个净化中心提供支持，专用防御容量总计超过 20 Tbps**。就 Prolexic 的防御容量而言，即使是已知规模最大的第 3 层和第 4 层 DDoS 攻击，也只占 Prolexic 客户可用容量的不到 10%。

全面、灵活且可靠的 DDoS 防护

Akamai Prolexic 以 Prolexic Cloud、Prolexic On-Prem 和 Prolexic Hybrid 形式提供。

Prolexic Cloud 是云端 DDoS 防护服务的行业领先者，可以为客户提供零秒抵御和 100% 平台可用性 SLA。抵御控制措施可动态扩展容量，阻止以 IPv4 和 IPv6 流量的形式发起的攻击。可为需要扩展的抵御控制措施动态分配计算资源。

Prolexic On-Prem 可提供不间断的物理或逻辑层面的内联和数据路径 DDoS 防护，能够与边缘路由器进行原生集成，从而在客户网络的边缘自动阻止 98% 以上的攻击，同时无需回传流量。这是防范绝大多数短时小规模攻击的理想选择，非常适合需要超低延迟 DDoS 防护技术的企业。

Prolexic Hybrid 兼具 Prolexic On-Prem 的强大性能和自动化功能设计以及 Prolexic Cloud 出色的规模和容量，可以按需保护客户源站免受大规模容量耗尽型 DDoS 攻击。

打造超越 DDoS 防护的安全屏障

Akamai Prolexic 自带 Prolexic Network Cloud Firewall，后者是一款完全自助式且用户可配置的工具，让客户能够轻松定义、部署和管理自己的访问控制列表 (ACL) 和想要在网络最边缘执行的规则。它是一款安全防护性能更强的防火墙。该防火墙还会根据 Akamai 的威胁情报数据提供 ACL 建议，以实现更强的主动防御态势，并针对现有规则提供具有实用价值的分析。作为下一代防火墙即服务，Network Cloud Firewall 让客户能够：

- 定义主动防御规则，即时阻止恶意流量
- 将规则移到边缘，减轻本地基础架构的负担
- 通过新的用户界面快速适应网络变化

Akamai Edge DNS 和 Akamai Shield NS53 可保护并增强重要的 DNS 基础架构

Akamai Edge DNS 可为您提供全面保护，无论您使用本地、云端还是混合 DNS 基础架构，它都能够防止基础架构遭受各种 DNS 攻击。该解决方案还提供更高的 DNS 性能、恢复能力和可用性。依托于全球分布式 Anycast 网络，Edge DNS 可作为主要或辅助 DNS 服务加以实施，根据需要取代或增强现有的 DNS 基础架构。

Akamai Shield NS53 是一种双向 DNS 反向代理解决方案，可以保护本地及混合 DNS 基础架构（包括 GSLB、防火墙和名称服务器）免遭 DNS 资源耗尽型（即 NXDOMAIN）攻击。客户可以自行完成配置和管理，并且实时执行自己的动态安全策略。Akamai 可以在网络边缘拦截非法 DNS 查询和 DNS 攻击洪流，从而保护关键 DNS 基础架构免受 DNS DDoS 攻击。

Akamai App & API Protector 可保护应用程序和 API 免受 DDoS 攻击

App & API Protector 是备受认可的卓越 Web 应用程序和 API 保护 (WAAP) 解决方案，能够在边缘（为托管在 Akamai Connected Cloud 上的资产）即时抵御网络层 DDoS 攻击，并提供针对应用层 DDoS 攻击的全面防御策略。

为什么选择 Akamai?

Akamai 提供深受用户信赖的全球 DDoS 抵御解决方案。无论您是要保护单个应用程序、整个数据中心还是关键 DNS 基础架构，Akamai 在设计 DDoS 抵御措施时，都会考虑尽大的容量、尽高的恢复能力和尽快的抵御速度。

我们成功抵御多起全球范围内发起的大规模 DDoS 攻击。我们的主动抵御控制措施可实现真正的零秒抵御并提供业界卓越的 SLA。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。

由于 DDoS 攻击媒介在不断变化并且攻击规模越来越大，一家值得信赖的 DDoS 防护平台必须不断进行功能创新并提升开发和部署能力，以主动检测威胁、编排抵御策略并将影响降至最低。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 抵御策略应为您的混合和多云策略提供支持。Akamai 的下一代 DDoS 解决方案可以保护您的数字网络基础架构、应用程序及本地和/或云端 DNS，并具备机器智能与人类智慧的综合优势。

了解更多

扫码关注，获取最新云计算、云安全与CDN前沿资讯