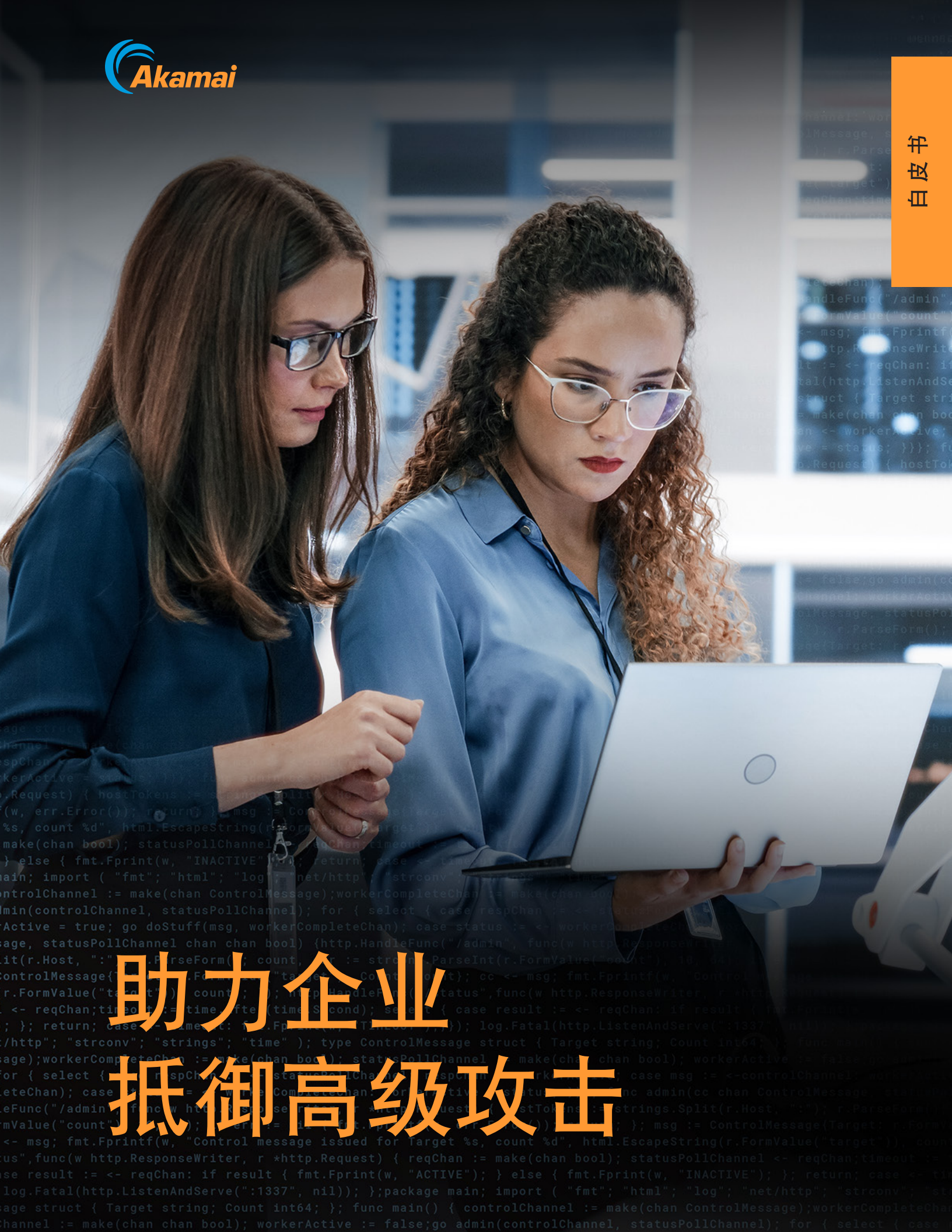
Akamai

白皮书



助力企业抵御高级攻击

随着 IT 环境日趋复杂，网络攻击也顺势而起，花样翻新地利用各种新的可乘之机。与此同时，应用程序、API、微服务和网络组件的阵容正在不断壮大，并改变着企业的在线运营模式。遗憾的是，这些先进技术在发展的同时也带来了新的漏洞和威胁面，让攻击者有机可乘。因此，网络安全解决方案不但要应对内部存在的威胁（保护自身数据安全），还要抵御来自外部的攻击（阻止勒索软件、DDoS、资源耗尽及其他类型的攻击）。

Akamai 研究人员平均每天都会分析 788 TB 的数据，因此我们能够掌握第一手的信息，同时利用所获得的分析洞见推进产品创新，无论攻击格局如何变化，都能保护您和您的用户免遭高度危险的攻击和高级攻击活动。

您的公司可能会面临哪些高度危险的攻击？您又该如何做好准备以应对它们？

勒索软件更加猖獗

无法访问自身数据和客户数据是企业面临的一个重大威胁。Akamai 在《勒索软件异常活跃》报告中指出，在 2022 年第一季度到 2023 年第一季度期间，全球的勒索软件攻击数量增加了 143%，并且攻击者主要是利用零日漏洞和一日漏洞发起的此类攻击。若想降低遭受高级攻击的风险及其带来的影响，您可以使用分段技术。

分段是一种将网络划分为较小区段的架构级方法，其目的是增强性能和安全性。而微分段是一种安全防护技术，让您可以从逻辑上将网络划分为不同的安全区段，并细化到工作负载级别。然后，您就可以为每个不同的区段采取适当的安全控制措施和服务交付方法。

Akamai Guardicore Segmentation，在 Akamai Guardicore 平台中用于提供 Zero Trust 保护，它旨在有效遏制对您所有关键系统的攻击，并阻止它们在您的资产内部传播（即“东西向移动”），为应对攻击事件和实施恢复措施提供强有力的支持。最终，您将能够成功避免攻击带来的声誉受损、数据损失和收入损失。

作为一种无代理的微分段解决方案，Akamai Guardicore 平台部署简单快捷，而且无需对您的网络进行任何物理更改，也不必为服务器和设备的位置而担心。它将以交互式的方式直观地展示您网络中的所有连接，进而帮助您解决部署过程中遇到的一个核心难题，即缺乏监测能力。不仅如此，Akamai 还开发了一系列高效实用的方法，用以解决潜在的性能瓶颈和合规性要求问题。同时，我们也实施了相应的策略，以满足不同基础架构的各类需求。所以，我们可以在单一平台上对各种环境实施广泛监测和精细控制。

Akamai 可以出色地监测我们庞大的全球分布式网络中的在线流量。得益于此，Akamai Guardicore 平台可帮助您深度监测您的企业环境、资产、访问情况和网络流量。有了这些实时信息，您就可以安心确保业务不会中断。

攻击阴影下的应用程序和 API

您公司正在使用的应用程序有多少？肯定比您知道的要多。每家公司使用的应用程序平均超过 1,000 个。企业严重依赖 API，几乎在所有线上交易中都会用到它们，而且越来越多地采用基于微服务的架构，这也意味着应用程序变得更加错综复杂。遗憾的是，面对以创新促增长的压力，企业往往急于发布应用程序而忽略了严格的测试环节，这种做法不仅增加了潜在的安全问题，而且也给整个应用程序生态系统带来了更大的风险。

Akamai 在最近一期的《互联网现状》报告中指出，全球 29% 的攻击都是针对应用程序编程接口 (API) 发起的，因为 API 是大多数数字化转型的核心。在欧洲、中东和非洲地区，这一比例略高于 47%。对于传统的攻击手段以及针对 API 设计的特定攻击手段，API 都已成为网络犯罪分子常用的攻击媒介。另外，务必将爬虫程序、分布式拒绝服务 (DDoS) 攻击以及多媒介攻击全都考虑在内。

使用 Akamai App & API Protector 保护您的 Web 应用程序，让您的工作流程、用户和业务免遭恶意活动和欺诈侵袭。该解决方案提供了可配置的防火墙保护机制，可吸收针对应用程序层发起的攻击（包括通过 API 发起的攻击）。通过实时监测爬虫程序流量，您可以调查存在偏差的 Web 分析，防止源站超载，并自定义权限来顺利访问第三方及合作伙伴的爬虫程序。

但我们回到最开始的问题，如果您并不知道自己到底使用了哪些应用程序和 API，该怎么办？这再一次印证了监测能力的重要性，Akamai API Security 将帮助您识别所有 API，评估其风险级别并采取措施应对攻击。这将有效防止攻击者访问您的数据、将恶意文件加载到服务器上，或利用突发流量让服务器不堪重负。

抵御 DDoS 攻击和资源耗尽型攻击

在所有攻击中，广为人知的规模最大的在线威胁是分布式拒绝服务攻击。只要互联网存在，DDoS 攻击就难以根绝，其影响已经渗透到互联网的各个领域。近年来，DDoS 攻击呈现出规模更庞大、持续时间更长的特点，同时多样化的攻击媒介和攻击目标也使得此类攻击异常复杂。2021 年到 2023 年期间，大规模 DDoS 攻击的数量增加了 50%。2023 年，超过 60% 的 DDoS 攻击都涉及到 DNS 组件。

即便是许多大型公司也被这些恶意僵尸网络拖垮，导致他们无法为数百万客户提供正常服务，甚至使业务陷入停滞状态。一些资源丰富的网络犯罪分子、民族国家攻击者和出于地缘政治动机的黑客不遗余力地利用大型分布式僵尸网络，他们不但攻击大型公司，而且也向学校、医院、机场和公用事业提供商等重要公共机构伸出罪恶之手。一些破坏性的 DDoS 攻击和资源耗尽型攻击瞄准了所有层、端口和协议，甚至包括企业和公共机构的 DNS。

您知道吗？

2021 年到 2023 年期间，DDoS 攻击量增加了 50%

2023 年，超过 60% 的 DDoS 攻击都涉及到 DNS 组件

要想保护您的基础架构免受 DDoS 攻击，需要掌握实时威胁情报。Prolexic 是我们的一款 DDoS 攻击防护和抵御解决方案，可利用我们收集的数据为您提供强大助力。它能够保护支撑公司数字应用程序和体验的底层数字基础架构，及时拦截对云端、本地或混合部署中所有端口和协议发起的攻击，从而确保您的业务免受任何影响。

近年来，企业 DNS 基础架构遭遇的资源耗尽型攻击呈现显著回升趋势。DNS 是公司在线业务的基础元素。如果 DNS 系统瘫痪，企业的在线业务就会停顿。Akamai Edge DNS 和 Shield NS53 在边缘拦截 DNS 资源耗尽型流量，仅允许合法 DNS 查询到达客户源站。

长期以来，虽然攻击规模每两年就会翻一番，攻击的复杂性也随之增长，但 DDoS 防护始终是保护在线业务的有力筹码。为了免受收入损失和客户信任崩塌的风险，企业迫切需要加强所有潜在故障点的安全防护。

如果发生攻击该怎么办?

可以肯定的是，只要您有数字业务，就有可能在某个时刻成为攻击的目标。而我们的安全策略是防患于未然，通过保护您的重要资产，为您提供网络监测能力，让您能够实时了解网络状况，以及在攻击初露端倪时立即进行检测，减少您成为攻击目标的风险。

但如果确实遭到了攻击（比如零日攻击），又该怎么办？这就是 Akamai App & API Protector 等解决方案的核心所在——行为分析。

Akamai 利用高度自动化的解决方案和机器智能，结合来自全球安全运营指挥中心 (SOCC) 超过 225 名一线响应人员的人工情报，帮助客户保护数据、基础架构及其最终用户的数字体验。

Akamai 每天都会分析超过 13 万亿条域名系统 (DNS) 查询，每季度可抵御超过 120 亿次 Web 应用程序防火墙 (WAF) 攻击。我们始终与客户并肩作战，将我们对攻击的分析洞见转化为坚实的防护力量。Akamai 利用这些威胁情报不断优化我们的解决方案，以提升其响应性能和效率。

即便您没有使用 Akamai 的安全解决方案，但一旦遭遇攻击，也欢迎您通过我们的网络威胁热线联系我们。我们的安全专家将会与您联系，告诉您如何抵御所遇到的攻击。

让您全球各地的业务都安全无虞

如同死亡和交税一样，网络攻击也是这个世界上无法逃脱的定数。但是，您可以利用安全解决方案来保护您的企业和客户。这些解决方案使用最新的威胁情报，可帮助您密切监测应用程序和网络，并会随着威胁形势的变化而不断完善。

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。我们广泛的解决方案组合立足于 Akamai 全球平台的出色威胁监测能力，可为企业提供高度的可靠性，让您抢先一步防范威胁，并迅速适应不断变化的安全形势。

更多资源

了解如何通过 5 个步骤打破勒索软件杀伤链

为混合云策略提供支持，同时免遭 DDoS 攻击

使用强大的 API 安全策略保护企业的基础组件

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，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：2024 年 6 月。

扫码关注 · 获取最新CDN前沿资讯