执行摘要

随着 Web 应用程序和 API 安全市场的发展和演变，买家面临艰难的选择

Gartner 在其 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection 中将 Akamai 评为领导者

随着 Web 应用程序攻击、分布式拒绝服务 (DDoS) 攻击以及勒索软件的激增，网络安全专业人员面临着巨大的压力。近年来，随着定向攻击的增加，Web 应用程序和 API 安全性变得越来越重要。这种情况的发生让安全团队不堪重负，而 Web 应用程序又依赖于多云环境，这让他们不得不面对日益复杂的应用程序生态系统。

要想了解 Web 应用程序和 API 攻击会造成怎样的危害，金融服务业就是一个很好的例子。2022 年 11 月，Akamai 研究团队发现，攻击者在过去 12 个月中持续利用零日漏洞针对金融服务公司发起的 Web 和 API 攻击数量增加了 257%。

攻击的激增可能与本地文件包含和跨站点脚本等多种攻击媒介密不可分，攻击者利用这些攻击媒介在网络中获得立足点。这使得保护 Web 应用程序和 API 比以往任何时候都更加重要，因为一旦攻击者成功利用这些漏洞，他们便可将其用作入侵目标企业的切入点。为了防范这些攻击，越来越多的网络安全专业人员转向那些提供单一产品即可满足所有 Web 应用程序和 API 安全要求的供应商。我们认为 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection 报告在帮助安全专业人员做出购买决策方面颇具参考价值。

在评估市场中的 Web 应用程序和 API 保护 (WAAP) 技术时，各公司如今对 WAAP 的需求更全面、更复杂。买家现在需要考虑能够至少提供四项核心功能的供应商：Web 应用程序防火墙、DDoS 防护、爬虫程序管理和 API 保护。

然而，这只是基本需求。大多数企业应扩大其需求，以包含更多的功能。Gartner 在其报告中建议买家还应考虑以下功能：

- 客户端保护
- 漏洞扫描
- 移动应用程序安全性
- DNS 服务和 DNS 安全性
- 内容交付网络 (CDN)、负载均衡、访问管理和其他功能
- 防止网站篡改

市场在不断演变

虽然 WAAP 采购历来以采购设备为主，甚至现在一些企业还在购买新设备以替换旧设备，但是云端 WAAP 部署已经成为主流趋势。Gartner 预计，这种趋势还会持续下去。

Gartner 在报告中预测：“到 2024 年，在生产环境中针对 Web 应用程序实施多云战略的企业中，将有 70% 更加青睐云端 Web 应用程序和 API 保护平台 (WAAP) 服务，而非 WAAP 设备和 IaaS 原生 WAAP 服务。”

Gartner® Peer Insights™ 的评论。发布日期：2022 年 4 月 7 日：

> **“Akamai AAP 是功能齐全的 WAF 解决方案，包括 Web 攻击检测、DDoS 防护、爬虫程序管理和 API 保护。除了拥有出色的产品，他们还有相当专业的服务团队，响应速度很快。”**
>
> **——IT 服务行业的 IT 安全和风险管理专业人员**

Gartner® 在其 WAAP Magic Quadrant™ 报告中将 Akamai 评为领导者

在 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection 报告中，Gartner 根据 15 项不同标准评估了 11 家供应商，最终将 Akamai 列入领导者象限™。前几年，Gartner 发布了类似的报告：Magic Quadrant™ for Web Application Firewalls。在这两份报告中，Akamai 现已连续六次被评为领导者。

在 2022 年 Gartner 报告中，Akamai 在“执行能力”方面排名首位，并在“愿景完整性”方面排名首位。

> **“同内部自行研发相比，有 Akamai 相助，我们可以更快、并以更低成本及风险获得最新最好的技术。”**
>
> **——Finastra 客户技术及运营首席信息官 Russ Soper**

Akamai 对 WAAP 市场的认识

Akamai App & API Protector 提供了包含 Web 应用程序防火墙、爬虫程序抵御、API 安全和 DDoS 防护在内的一套完整 WAAP 产品，这些产品可紧密协作，共同帮助客户全面了解其安全态势。多年来一直如此。Akamai 在该市场有着出色的业绩，这一点在其他分析公司的报告中也能体现出来，这些报告也将 Akamai 列入领导者行列。

例如，安全团队需要对 DDoS 攻击保持警惕，而在 Akamai 产品套件中，DDoS 防护仍然是一项核心能力。在 How to Respond to the 2022 Cyberthreat Landscape 中，Gartner 告诫道，企业应该预料到攻击者会“将勒索软件与分布式拒绝服务 (DDoS) 攻击等其他技术相结合，致使面向公众的服务离线，以胁迫企业支付赎金。”

同样，我们认为 Akamai 通过高级 API 功能简化了 API 的维护，这些功能可以自动发现 Web 流量中各种已知、未知和不断变化的 API，包括它们的端点、定义和流量配置文件。

然而，Akamai 的优势远不止其核心 WAAP 产品。Akamai 凭借在该市场中的规模、悠久历史以及大量的企业客户，使其能够通过产品发布和内部专业知识快速应对新出现的威胁，因而比特定领域竞争对手更具优势。特别是，Akamai Intelligent Edge Platform 是全球大型内容交付网络。其在 134 个国家/地区的数千台边缘服务器使 Akamai 拥有卓越的监测能力，可快速发现新出现的全球威胁。借助这些资源，Akamai 每天能够分析 300 TB 的攻击数据。此外，Akamai 还拥有 330 多名负责保护客户的数据安全专家。这使 Akamai 能够在更多的位置提供服务，并将威胁转移到更靠近其源头的地方。

与此同时，为 Akamai WAF 产品提供支持的 Akamai 自适应安全引擎会自动分析环境变化、互联网流量模式和全球威胁形势。自适应安全引擎随后会计算出威胁评分，以对企业的调整参数进行修改或给出修改建议。然后，客户可以自定义规则集以满足其业务需求。

下载 Akamai 免费提供的完整报告

为了满足当下的网络安全需求，企业纷纷增加应用程序和 API，这推动着 WAAP 市场不断发展。

在这份报告中，Gartner 评估了 11 家符合其纳入标准的供应商。如果您是安全专业人员，您必定想更多地了解这些标准，查看这 11 家供应商的评估结果。如果您在寻找符合您需求的 WAAP 供应商，我们认为这份报告不失为一个颇有价值的切入点。

> **“到 2026 年，40% 的企业会将高级 API 保护和 Web 应用程序安全功能视为选择 WAAP 提供商的依据，而在 2022 年，这一比例还不到 15%。”**
>
> **——2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection**

获取报告

访问 akamai.com

扫码关注，获取最新CDN前沿资讯