IDC MarketScape

IDC MarketScape：全球 Web 应用和 API 保护企业平台 2024 年厂商评估

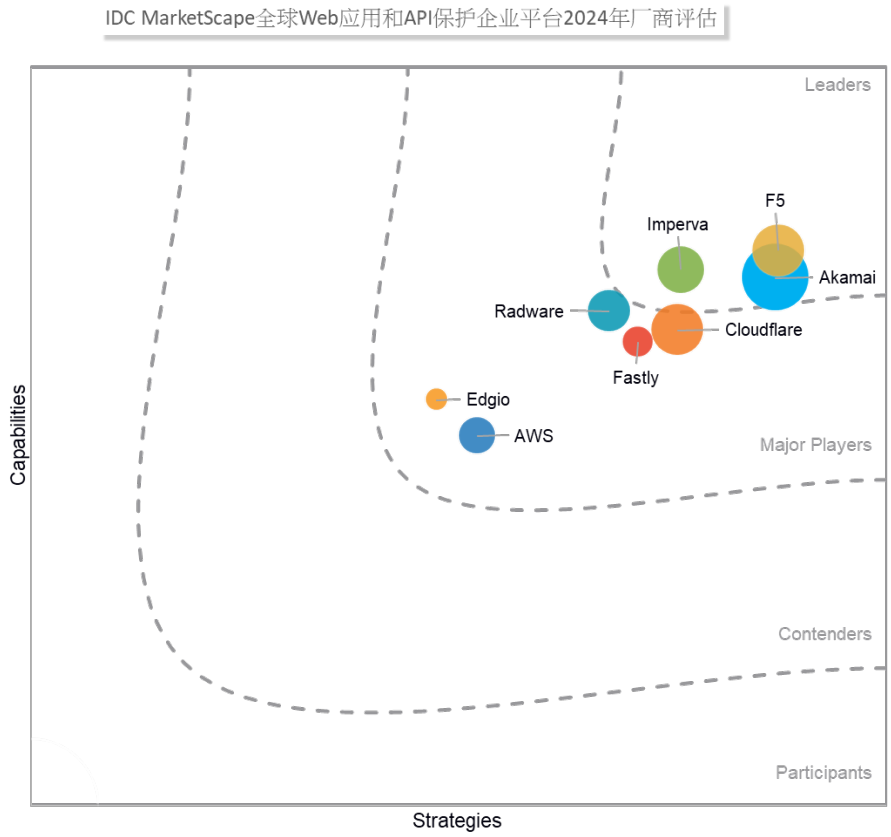
Christopher Rodriguez

本 IDC MARKETSCAPE 报告摘录重点介绍 AKAMAI 的解决方案

IDC MARKETSCAPE 图

图 1

IDC MarketScape：全球 Web 应用和 API 保护企业平台厂商评估



来源：IDC，2024 年

September 2024，IDC #US51795524e

要了解研究方法、市场定义和评分标准等详细信息，请参阅“附录”。

本摘录内容

本摘录内容直接摘自于以下报告：IDC MarketScape:Worldwide Web Application and API Protection Enterprise Platforms 2024 Vendor Assessment (Doc # US51795524)。本摘录包含以下全部或部分内容：IDC 观点、IDC MarketScape 厂商入选标准、基本指南、厂商综合概况、附录和进一步研究。另外还收录了图 1 和图 2。

IDC 观点

Web 应用是现代数字业务的基础组件，为企业与客户和潜在客户、合作伙伴和访客、员工和派遣员工的交互提供所需功能。攻击者屡屡探测这些应用和相关的应用程序编程接口（API），伺机窃取数据、获得非法访问权限或欺诈企业以获取个人非法利益。针对 Web 应用和 API 的攻击导致了备受媒体关注的数据泄露事件、代价高昂的停机时间以及包括盗窃在内的实际损失。最终用户和客户往往首当其冲遭受经济损失。最终可能会导致失去客户信任，在线开展业务的意愿降低。

网络犯罪不仅仅是一种滋扰。它甚至可能会削弱和破坏业务成果。多年来，企业采用了多种安全工具来应对源源不断的新威胁手段和不断扩大的攻击面。Web 应用防火墙（WAF）提供基本级别的防护，可抵御已知和新出现的应用层攻击。企业在此基础上，部署了诸多专门解决方案，例如 DDoS 缓解和机器人（bot）管理，以及最近的 API 安全防护解决方案。

Web 应用和 API 保护（WAAP）将这些基本安全技术整合到一个集成的统一平台中，确保可靠防御大量在线威胁。这样的一体化集成平台有助于减少安全漏洞、降低管理难度、简化检查。IDC 研究表明，77%的企业将安全解决方案之间的集成评为“重要”或“至关重要”。应用每天都面临一系列威胁，攻击者有目的地利用多种手段寻找防御措施中的薄弱环节。因此，为防止功亏一篑，旨在解决专业安全孤岛问题的应用安全战略应运而生。要加强安全态势，无论是通过提高检测准确性、减少误报率，还是通过可靠检测高级威胁和零日威胁来实现，都需要安全融合与整合，这是至关重要的一步。

除此之外，融合还能带来许多业务收益，如减少部署和管理所需的时间和资源、改善用户体验、改进分析等。此外，通过一个服务执行所有安全功能可减少因将流量路由到多个安全检查点产生的延迟。

同时，企业必须采取审慎方法，根据需要或在时间和资源允许的情况下逐步采用各种应用保护技术。对于客户来说，模块化的集成平台至关重要，因为它可以让客户轻松地逐步实施 WAAP。对于厂商来说，挑战在于如何从可能包含在不同产品层级中的各个核心安全功能区块中精准找出各种集成功能。

WAF 是基础组件，而要实现现代化的应用保护，还需要统一的 API 战略。API 如今在现代化的数字业务时代发挥着重要作用，它可以简单高效地集成应用，将应用强大的新功能发挥出来。不过，API 给攻击面带来了新威胁。API 容易发生配置错误，泄露敏感数据和遭受拒绝服务攻击。重要的是，API 容易受到许多以用户界面为目标的攻击，同时，它们还会招致 API 特有的威胁，例如对象级授权失效（BOLA）。API 还提供了一种应用间通信方法，这些通信可能不再经由边界保护解决方案（如 WAF）。这可能导致安全盲点，而攻击者可能利用该盲点进行横向移动，而不被基于网络的防御措施发现。

将 WAF 安全防护与 API 安全防护相结合，对于确保全面保护所有接口和攻击面上的 Web 应用至关重要。WAAP 的价值主张还需要辅以专为应对特定威胁类型（如 DDoS 攻击和恶意 bot 活动）而设计的技术才算完整。这些威胁在检测难度、缓解难度、发生频率和影响严重度等方面各不相同。总而言之，完整的应用保护堆栈需要兼具 WAF 和 API 安全、DDoS 缓解和 bot 管理。然而，API 的独特技术要求以及 DDoS 攻击和 bot 活动的特殊要求意味着向 WAAP 的演进是一个漫长而曲折的过程。

IDC MARKETSCAPE 厂商入选标准

WAAP 是以 WAF 为核心的综合化主动应用保护安全解决方案。本节将讨论 IDC 认为有资格纳入本 WAAP 企业平台 IDC MarketScape 分析的解决方案必须具备的关键特性。

厂商必须提供综合化 WAAP 解决方案，在统一的安全平台中再加入以下其中两项功能：

- API 安全防护
- bot 管理
- DDoS 缓解
- Web 应用防火墙 (WAF)

请注意，WAF 在本研究中属于基础功能，必须包含此功能才被视为 WAAP。此外，作为独立解决方案一次性销售的 WAAP 组件将不算作 WAAP。

此外，本 IDC MarketScape 分析还包括以下市场参与度和市场份额要求：

- **市场参与度：**厂商在 2023 年就开始或继续以统一解决方案的形式提供关键 WAAP 功能。某些核心或扩展功能可以作为其他捆绑包或平台的一部分提供，也可以作为独立解决方案提供，但不得仅作为独立产品提供。有关必备和可选功能的完整详细说明，请参阅"市场定义"部分。
- **市场收入份额：**经 IDC Security Products Tracker 查证，厂商在 2023 年 WAAP 竞争市场中达到规定的最低收入份额。
- **全球收入份额：**经 IDC Security Products Tracker 查证，截至 2024 年，厂商在全球各个主要地区（包括北美；拉丁美洲；欧洲、中东和非洲地区以及亚太地区）的收入都已达到最低要求。

IDC 指出，某些提供 WAAP 组件的云和安全提供商没有被纳入分析，原因是他们主要关注单点产品，而不是整体的 WAAP 解决方案。同样，有些提供 WAAP 的厂商因为没有达到最低市场收入份额或全球收入份额要求而没有入选。

给技术买家的建议

重点考虑的厂商能力

IDC MarketScape WAAP 企业平台分析考虑了 IT 买家共同要求和期望的保护级别，还有集成程度、易用性、相邻的专业和托管服务以及总拥有成本。在企业层面，WAAP 必须提供出色的保护，减少对安全性能的影响，尽可能降低对最终用户体验的影响。该分析还着重分析了 WAAP 的主要目标，即将多种基本安全技术整合到一个集成的统一平台中。WAAP 解决方案还必须具备可扩展性并提供多种定价模式，只有这样，才能完美契合持续抵御大量在线威胁这类需求，以及客户对业务价值的要求。

用户的期望不断攀升，企业则不断采用新兴技术，以提供创新的、令人满意的用户体验。应用对复杂的分布式基础设施的依赖只会越来越严重。DevOps 团队正在以更快、更智能的方式竞相推出新功能。企业可能要额外考虑特种产品和功能特有的专业能力，这些能力可以是厂商原生提供，也可以不是；可能是解决方案默认提供，也可能以其他方式（如第一方附加功能或单独产品）提供，或由第三方 OEM 或技术集成提供。具体来说包括：

- **客户端 WAF**：客户端 WAF 也称为客户端保护，是一种新兴的安全技术，旨在解决一种特殊的威胁向量——在最终用户设备上运行的 Web 应用代码。此代码包括在设备上而不是在 Web 服务器上执行各种功能的浏览器脚本。
- <g id="1">防欺诈/防滥用：</g>防在线欺诈和滥用能力通常依赖于 bot 管理能力，这些能力经过专门调整，可以识别表示特定欺诈活动（如账户接管或新账户欺诈[也称为虚假账户欺诈]）的独特模式。要全面检测欺诈行为和其他表明应用和 API 被滥用的行为，需要深入了解用户身份、客户端和设备级遥测数据以及用户行为。所以，在欺诈检测功能以及如何将这些功能包装并推广给买家方面，不同的 WAAP 解决方案之间存在巨大差异。
- **住宅代理**：WAAP 解决方案在检测隐藏在住宅代理后面的攻击者或其他混淆方法（如 IP 轮换）的能力各有不同。
- **WebSocket**：涉及是否支持使用 WebSocket 协议的应用。WebSocket 是一种通过全双工连接实现实时通信的协议。随着在线用户越来越期望使用交互式实时应用程序，支持 WebSocket 变得越来越重要。
- **WebAssembly（WASM）**：一种提供可移植二进制代码格式的低级语言。迄今为止，WASM 的主要优势是能够轻松支持各种开发语言。随着采用率的增加，WAAP 能不能支持 WASM 成为越来越重要的考虑指标。
- **运行时应用自我保护（RASP）**：一种高级安全功能，保护应用运行时环境并监控数据输入以识别、检测和阻止攻击。RASP 对于实现深度应用安全可能是一个正确选择，但前提是要对其可能带来的部署复杂性及性能影响有合理的认识。
- **私有访问令牌（PAT）**：苹果和其他科技公司加大了对最终用户隐私的关注，提供了在不暴露个人身份详细信息的前提下证明访问请求设备真实性和可信度的方法。WAAP 支持苹果的 PAT 可能有助于减少对 CAPTCHA（全自动区分计算机和人类的图灵测试）或其他 bot 检测技术的依赖，这些技术会给用户体验造成摩擦或不确定性。苹果 PAT 是整个行业向隐私保护技术迈进的一个缩影，这一技术可实现在不泄露敏感个人身份信息（PII）的前提下与特定方共享或共同处理用户数据。
- **自动化**：自动实施更新可提高易用性并增加业务价值。
- **仿真测试**：允许先测试更新后的规则，然后再将其用于生产环境。。如果在实际流量上执行仿真测试，得到的仿真结果会更有效。
- **eBPF**：扩展的伯克利包过滤器（eBPF，Extended Berkeley Packet Filter）是 Linux 的一项功能，它允许沙盒程序在操作系统内核中运行，这对提高安全可观测性具有重要意义，尤其是在云原生环境中。

关注厂商的战略

此外，鉴于 Web 应用和 API 技术的快速发展、业务实践日新月异以及威胁攻击者无休止的应变和创新能力，安全解决方案的买家应特别注意解决方案能否满足他们未来三到五年的需求。具体来说，这些能力包括：

- **检测混淆：**网络犯罪分子窃取数据和产品，实施欺诈、骚扰或勒索公司的行为越来越肆无忌惮。对于能挣大钱的目标，他们总是使用复杂的工具和精明的手段。如果安全公司发现并阻止了攻击，他们就会开始调整变化。所以，WAAP 提供商应大量投资相关技术以隐藏检测手段，让攻击者花费更长的时间来找到破解办法。此外，最得力的战略还可以防止攻击者知道自己何时被检测到，以此来消耗他们的资源。已知的先进 bot 和欺诈缓解措施包括使用欺骗技术阻止攻击者的网络武器开发循环实现闭环。
- **平台化：致力于简化**复杂性的平台正在重塑各行各业，只需简单的用户界面即可提供专业功能，不再需要从头开发技术。以 Shopify 为例，这个商业平台可以简化建设新在线业务的过程。客户信息、库存和支付处理等功能通过完整的全包式 SaaS 提供。包括基本 WAF 和 DDoS 防护在内的安全功能均作为内置功能包含在平台内。这将改变买方对 WAAP 解决方案的需求和期待，因此，厂商需要进行战略上的调整。
- **"左移"战略：**在软件开发生命周期的早期实施安全测试和实践的理念已提出多年。先检测软件漏洞然后再将软件发布至生产环境，可防止攻击者发现和利用漏洞。尽早发现和纠正也更有效、更具成本效益。然而，近年来，出现了左移的概念，它通过将传统的后期生产工具集成到开发人员工具和工作流程中来实现这些理想结果。例如，使用 API 调用动态应用安全测试（DAST）可以让 DevOps 快速轻松地发现和纠正威胁。此外，随着 DevOps 团队工作速度的加快并利用微服务、可组合代码、基础设施即代码（IaC）和其他手段来缩短开发周期，支持"左移"战略已变成不可避免的需求。
- **角色变化：**平台化趋势、"左移"战略以及安全意识文化（每个人都对安全负责）的普遍提高正在推动买家和决策者发生转变。开发人员、云和网络团队，甚至业务部门买家都会参与 WAAP 的采购过程。WAAP 厂商必须在简化、自动化、强大的开箱即用保护和市场培训方面加大投资，以更好地支持广大买家和决策者。
- **GenAI**：GenAI 的出现引发了人们对该技术可能给企业环境带来的潜在新风险的担忧。因此，根据 IDC 的买家研究，企业正在考虑为应用安全防护领域增加预算的必要性。不同 WAAP 厂商对 GenAI 相关潜在风险的关注和预案也存在较大差异，这表现在多个方面，例如：
  - 以 GenAI 为武器更有效地躲避防御措施的潜在新威胁
  - 可能应用新兴技术（例如，利用 GenAI 减缓机器人活动、阻碍、减缓或破坏 bot 操作）
  - 企业在应用战略中构建 LLM 能力或利用第三方 LLM 时，可能需要部署专门的功能或产品，或者可能依赖现有的防御措施
  - GenAI 在提高安全运营效率和生产力方面的潜在应用
  - AI 在改善安全检测方面的潜在应用

总体而言，尽管按照定义，WAAP 包含和涉及的功能非常广泛，但 IDC 从本 IDC MarketScape 所分析的解决方案中发现了一系列高级功能。鉴于新兴技术不断涌现，威胁不断变化，WAAP 的定义预计也会不断变化。某些功能领域仍有改进的余地，且各家厂商已经制定了详尽的路线图。虽然在某些场景或特殊要求下可能需要专门的单点产品，但 WAAP 厂商在打造完整、强大的平台的道路上取得了长足的进步，这些平台拥有了确保强大的应用保护和性能所需的深度功能。

厂商综合概况

本部分将简要介绍 IDC 对各厂商的重要评估，这些评估结果决定了厂商在 IDC MarketScape 中的定位。有关厂商的评估标准，请参见“附录”，此处将概述厂商的优势与挑战。

Akamai

Akamai 在“全球 WAAP 企业平台 2024 年 IDC MarketScape”中属于领导者类别。

Akamai 是一家全球网络和安全提供商，通过其分布式边缘和云平台 Akamai Connected Cloud 提供网络和安全服务，该平台具有让应用和体验更贴近用户，让威胁远离用户的特点。Akamai 专注于企业市场，在财富 500 强企业中有较高的渗透率。Akamai 安全产品组合包括一款名为 App & API Protector（AAP）的集成式 WAAP 解决方案，以及 API 安全、DDoS 缓解、bot 管理、账户保护、WAF、客户端保护和合规性、DNS 和品牌保护等类别的专用解决方案。Akamai 已凭借 ZTNA、微隔离、DNS 防火墙、威胁捕获和 MFA 等解决方案进入了企业安全防护领域。

优势

能力

- Adaptive Security Engine（ASE）提供自我调优功能，以可靠地应用开箱即用的规则。ASE 的零日保护更优越，检测能力更强（根据 Akamai 的说法，提升了 2 倍），误报更少（根据 Akamai 的说法，最高减少 80%），还支持自动更新，实现了长期易用性。ASE 由 Akamai 安全情报提供支持。
- ASE 提供了误报标记功能，可以更轻松/更快地修正误报。Akamai 声称在一天后的修正率超过 50%，一周内超过 75%。
- 全面的 WAAP 套装一站式实现既简单又全面的安全防护。配有单个 WAAP SKU，并提供可实现高级或专业功能的附加组件。
- 丰富的附加组件和专用解决方案可满足特定场景的要求，例如账号接管（ATO）、品牌保护和爬虫程序（炒作活动）保护。
- Akamai 提供了超大规模的边缘/内容分发网络（CDN）基础设施。靠近用户提供保护可确保性能。
- 支持 DevOps 工作流以支持企业客户的左移战略。支持通过 API、命令行界面（CLI）和 Terraform 进行管理和部署，可在不减开发人员速度的情况下改善安全态势。

- 与相关安全工具的现有集成简化了与更广泛的安全架构的集成，实现了更好的安全成果。该解决方案包括用于 Splunk、Qradar 和 ArcSight 的预置连接器。
- 提供了多模态 API 安全方法。这种方法可开箱即用地保护已知的平台内 API 流量，并在以后根据需要提供完整的 API 保护。
- 还伴随 WAAP 提供了广泛的其他相关功能，确保安全功能不妨碍性能。该产品组合包括 SiteShield、mPulse Lite、EdgeWorkers、Image & Video Manager 和 API Acceleration 等解决方案。
- Akamai 最近推出了用于应用层 DDoS 缓解的新功能，包括短时突发检测和基于精细上下文线索的可自定义速率限制。这些方法可解决各种 DDoS 攻击，包括满足应用层攻击的特殊需求。
- 内含安全遥测统一视图，可提供广泛的安全分析和可视化，具备向下钻取功能。所有应用安全产品都包含 Web 安全分析。
- 利用评估模式，可以在实施规则更改前，在实时流量上评估规则更改的效果。利用这一功能，可以在实施新规则时避免对生产流量产生未知影响。

战略

- Akamai 提到，计划将 WAAP 与相邻的安全工具（如微分段）相集成。这将使得各个安全工具之间相辅相成，并实现纵深防御。
- 面对 LLM 使用量的增加，Akamai 正在制定相关的保护战略。将现有工具用于新的安全实践可提高客户价值；但面向 GenAI 的专用保护措施仍可能是更专业的方法。
- 该公司正计划积极进军边缘计算领域。保护边缘事务的方案可能有助于防止威胁攻入源服务器。
- 该公司提到了战略执行证据，特别是 API 安全战略的执行证据。在完成对 Noname Security 和 Neosec 的收购之后，API 安全战略即将形成。
- 这些战略收购取得了非常好的效果，将 Cyberfend、Neosec、Noname Security 和 Prolexic 等单点产品融合成了一个统一平台。这些投资显示出公司全力为客户安全着想的精神。
- Akamai 利用遥测技术跟踪战略进度，例如政策的使用/接受程度、自动模式和缓解状态。这保证了开发战略始终贴合客户实际情况。
- 即将发布的源 WAAP 将打破 CDN 安全的局限性，保护东西流量、非 CDN 流量和多云环境。这种功能即将推出，且有迹象表明正在稳步推进。
- 为客户互动提供了多种途径，例如客户会议、定期咨询委员会会议、临时活动等。

挑战

能力

- 客户要调优 AI/ML 引擎并不容易（即不能更改规则顺序）。这可能会在响应误报时造成延迟，需要与 Akamai 合作解决。允许临时的例外情况和变通方法可能是处理规则顺序复杂性的选项之一。

- 容器和无服务器等有限的形态限制了对希望控制安全基础设施的客户的支持。目前，对 Terraform 和基于 API 的控制措施的支持是 Akamai 部署和自动化的重点。
- Akamai 的 WAAP 按高端产品定价，这样的价格可能会让业务决策者望而却步。不过，Akamai 还提供了其他定价方案，包括零开销固定费用（ZOFF）保护、按请求定价和 DDoS 保护费用（包括不对 DDoS 攻击导致的流量激增加收超额费用）。
- 不支持 Google 远程过程调用（gRPC），但 gRPC 在专业场景或特定行业中可能是首选。

战略

- 专业可选功能和附加组件可能会额外收取费用，这会增加总拥有成本（TCO）并有碍全面部署。CDN 之外的流量（例如，API 网关流量）也要额外付费。
- Akamai 的 WAAP 产品开发战略中目前包括在在名义上与 Akamai Enterprise Application Access（EAA）零信任解决方案进行跨领域集成。Web 应用提供了一种支持工作场所转型的方法，而提高产品线之间的集成力度是支持各种安全访问场景的关键。
- 多个解决方案（例如，Account Protector、Brand Protector 和 Content Protector）会导致防欺诈战略略显零散，而这可能会增加消息传递的复杂性。

在以下情况下考虑选择 Akamai

Akamai 提供了一套强大的交付、性能和安全功能，这些功能集成在一起，作为一整套服务实施。Akamai 将各种高级和专业功能作为可选附加组件分别提供许可证。这种做法便于企业投资定制化解决方案，更好地满足其安全和交付需求。总而言之，Akamai WAAP 解决方案可满足大型现代数字企业的各种安全、可用性、完整性和合规要求。

附录

解读 IDC MarketScape 图

基于该分析的目的，IDC 将成功的潜在关键因素分为两大类：能力和战略。

Y 轴反应了厂商目前的能力、服务菜单以及该厂商与客户需求的匹配程度。能力范畴集中讨论企业和产品此时此刻的能力。在该范畴中，IDC 的分析师将着眼于使厂商能够实现其在该市场中已确定的发展战略的发展/交付能力。

X 轴或战略轴分析了厂商未来的战略与客户未来 3 到 5 年的需求的匹配程度。战略范畴集中讨论基于未来 3 到 5 年的产品、细分用户、业务和市场推广的高层决策和基本假设。

IDC MarketScape 图中的气泡的大小反映了厂商在所评估的具体细分市场内的市场份额。

针对每项具体标准，对厂商按照 1 到 5 分进行评估，其中 3 分表示平均评估基线，5 分表示最高也是极为少见的得分，1 分表示最低也是同样少见的得分。然后，根据分析师观点和分

析师对总体市场趋势的理解对标准进行加权，以便为 IT 买家决策提供最佳信息。对每项标准的评估也分为“定量”评估和“定性”评估，具体根据适用性和相关性而定。

图 1 将这几个因素以它们在每个轴上的位置的形式直观显示出来。“能力”轴重点展示了产品的现有特性和功能，但也考虑了其他因素。同样，尽管“战略”轴主要考虑厂商的未来产品开发计划，但也考虑了其他几个因素，包括整体业务的实力和产品上市计划。这些因素可能会对解决方案产生长期影响，IDC 相应调整了这些标准的权重。总体而言，每个厂商评估都涉及几个因素，建议读者结合厂商概况中提供的上下文来解读图 1。

IDC MarketScape 研究方法

IDC MarketScape 的选择标准、权重和厂商得分代表了 IDC 对市场和特定厂商的判断。IDC 的分析师通过与市场领导者、参与者和最终用户进行有组织的讨论、调查和访谈，来评估厂商，并制定了一系列标准特征。市场权重是基于用户访谈、买方调查、以及 IDC 专家审查组对各个市场的意见。IDC 分析师基于对厂商的详细调查和访谈，公开信息和最终用户反馈等对各厂商进行评分，并确定各厂商在 IDC MarketScape 中的位置，力求对各个厂商的特征、行为和能力提供精确的、一致的评估。

市场定义

WAAP 是以 WAF 为核心的综合化主动应用保护安全解决方案。WAAP 解决方案将包括 WAF、bot 管理、API 安全、DDoS 缓解和其他安全技术在内的多种功能集成到一个统一的安全平台中。不过，WAF 属于基础功能，必须包含此功能才被视为 WAAP。此外，作为独立解决方案一次性销售的 WAAP 组件将不算作 WAAP。

WAAP 基本组件

Web 应用防火墙

WAF 产品监控、过滤或阻止进出 Web 应用的通信。WAF 可以基于网络，也可以基于云，通常通过代理部署在一个或多个 Web 应用程序前面。WAF 是 WAAP 解决方案的核心组件。

API 安全

API 安全解决方案专门用于保护 API 通信免遭误用、滥用和攻击。这些解决方案提供部分或全部基本功能，例如 API 模式摄入、验证和实施；动态和自适应流量监控和模式分析；检测/预防恶意软件、漏洞利用、代码注入、bot、DDoS 攻击、欺诈和滥用等威胁。

WAAP 产品可能默认包含某些 API 保护功能，例如，在 WAF 检查点完成 API 流量检查。但是，完整的 API 安全部署可能需要额外的传感器和组件，才能确保对所有 API 端点的可视化和盘点，并最终保护所有 API 通信。

Bot 管理

bot 管理是一种确保在线通信完整性的做法，它依照受控和批准的条件，仅限真实的人类用户和所需的 bot 活动才能访问。bot 管理解决方案利用大量信号和对客户端、设备、浏览

器、用户身份和行为的洞察，并结合高级分析来检测最复杂和最难以捉摸的 bot。这些解决方案还可以根据风险概况、bot 类型或特定 bot 对整个 bot 生态系统进行精细分类和控制。

更宽泛的 bot 程序管理市场还包括旨在解决有害 bot 施加的独特安全要求的专用解决方案。不同 WAAP 解决方案，bot 解决方案的集成级别也不相同。WAAP 解决方案一般都会提供最低级别的 bot 检测和控制，高级功能作为附加功能或通过升级订阅提供。

DDoS 缓解

DDoS 缓解市场包括检测和筛选分布式拒绝服务攻击的解决方案。虽然防火墙、IPS 和其他安全产品可能具有 DDoS 防御功能，但专用的 DDoS 缓解解决方案特别设计用于处理规模最大、最复杂的攻击和新型攻击。此类产品可以位于本地，也可以部署在云端，或两者兼有之。

根据 WAAP 解决方案或部署的性质，解决方案中可以自由包含各种级别的此类保护措施。扩展的保护功能，例如加大防护容量或抵御特定类型的攻击，可能会以附加功能或升级订阅的形式提供。

WAAP 的扩展、高级和可选组件

客户端 WAF

客户端 WAF（CSWAF）将应用安全可视化和控制功能扩展到了最终用户浏览器中执行的脚本。不同 CSWAF 解决方案的功能范围也大不相同。核心能力通常包括脚本和通信的可视化、评估和盘点。高级安全功能方面，如漏洞检测、加密、代码混淆、异常和威胁检测以及政策执行等，市场更加分散。

防在线欺诈

防欺诈解决方案种类丰富，它们可以独立运行，也可以彼此协同，保护数字系统免受欺诈或其他有害活动的侵害。防在线欺诈可能涉及使用身份管理、强身份验证、身份证明解决方案、支付欺诈防护、交易欺诈识别、企业防欺诈和防在线欺诈专用解决方案等。

防在线欺诈和滥用功能与 WAAP 有关，通常依赖于 bot 管理能力，这些能力经过专门调整后，可以识别表示特定欺诈活动（如账户接管或新账户欺诈[也称为虚假账户欺诈]）的独特模式。要全面检测欺诈行为和其他表明应用和 API 被滥用的行为，需要深入了解用户身份、客户端和设备级遥测数据以及用户行为。所以，在欺诈检测功能以及如何将这些功能包装并推广给买家两方面，不同的 WAAP 解决方案之间存在巨大差异。

进一步研究

相关研究

- *Web Application and API Security Survey Presentation，2024*（IDC #US52509324，2024 年 8 月）

- *Identifying and Measuring the Costs of Cyberattacks Targeting Web Applications and API*（IDC #US52025924，2024 年 4 月）
- *Market Analysis Perspective:Worldwide Active Application Security Market， 2023*（IDC #US51332023，2023 年 11 月）
- *IDC TechBrief:Client-Side WAF*（IDC #US51199423，2023 年 9 月）
- *Worldwide Application Protection and Availability Forecast, 2023–2027:Threat Escalation and New Frontiers*（IDC #US51178423，2023 年 9 月）
- *Worldwide Application Protection and Availability Market Shares, 2022:Platforms Compete with Emerging Technologies*（IDC #US51204923，2023 年 9 月）
- *Tales of the Tape:WAF and API Protection Emerge as Security Essentials*（IDC #US51187923，2023 年 9 月）

概要

本 IDC 研究概述了现有的 WAAP 解决方案本身的优势，同时分析了多家厂商的优势、战略和技术合作伙伴关系、知识产权、并购情况、总拥有成本、客户满意度和竞争差异化因素等。WAAP 是一种集成解决方案，可实现安全、高性能地访问重要 Web 应用和相关 API。市场日新月异，只靠单点产品无法充分缓解风险。因此，安全买家还要考虑其他功能和方法。

IDC 安全与信任团队研究总监 Christopher Rodriguez 表示："WAAP 市场正处于一个关键时刻，厂商们为防御下一代在线威胁，抵御残酷的新式攻击，正在竞相角逐。与此同时，企业买家也在制定他们的 WAAP 规划，以应对快速变化的技术环境。"

关于 **IDC**

国际数据公司（IDC）是全球著名的信息技术、电信和消费科技咨询、顾问和会展服务专业提供商。IDC 在全球拥有超过 1,300 名分析师，他们针对 110 多个国家/地区的技术、IT 对标研究和采购以及行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。IDC 的分析和洞察有助于 IT 专业人士、业务主管和投资界做出基于事实的技术决策，实现他们的关键业务目标。IDC 成立于 1964 年，是国际数据集团（IDG，Inc.）的全资子公司。

全球总部

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com