AKAMAI 产品简介

App & API Protector

在当今互联的世界中，保护网络应用程序和 API 免受各种新兴和不断演变的威胁对企业的成功至关重要。但是，云之旅、现代 DevOps 实践以及不断变化的应用程序给保护数字化互动带来了新的复杂性和挑战。

通过部署全面的 Web 应用程序和 API 保护 (WAAP) 解决方案，可以自适应地更新保护措施，主动提供有关目标漏洞的深入洞见，从而强化安全态势。

Akamai App & API Protector 在单一解决方案中汇集多种安全技术，包括 Web 应用程序防火墙 (WAF)、爬虫程序抵御、API 保护和分布式拒绝服务 (DDoS) 防护。App & API Protector 是备受认可的卓越 WAAP 解决方案，其能力超越传统 WAF，可快速发现并抵御威胁，保护整个数字资产免受多维攻击。该平台易于实施和使用，能够提供全方位的监测能力，并可通过 Akamai 自适应安全引擎自动实施定制化的新式保护机制。

发挥自适应安全防护的优势

在自适应安全引擎的助力下，App & API Protector 的功能已远超规则集。借助这一创新技术，持续、自动地更新安全保护机制，让您一键实施自定义策略建议。自适应安全引擎可结合机器学习、实时安全情报、高级自动化以及来自 400 多名安全专业人士和威胁研究人员的见解，提供现代化的保护措施。自适应安全引擎的独特之处在于：

- 在边缘实时分析每一个请求的特征，从而加快检测速度
- 使用本地和全球数据学习攻击模式，根据客户的具体情况调整保护机制
- 适应未来威胁，确保不断更新保护机制，即使攻击方式不断发展演进，也能跟上脚步

自适应安全引擎提供零接触更新，可减轻耗时的手动调优的负担，实现接近于无需人为干预的体验。该项技术一经发布，便被证实可将检测效果提升为原有的 2 倍、误报减少为原来的 1/5。利用近期对机器学习算法的更新，现在可将误报再减少为之前的 1/4。安全专业人员能够再度成为中坚力量，而且有更多时间去专心致志地实现安全、客户友好的数字化业务运营。

对企业的好处

值得信赖的攻击检测能力
跟上威胁形势的演进步调，抵御既有和新兴威胁，包括 DDoS、僵尸网络、注入、应用程序和 API 攻击等

一款产品，广泛的保护
利用包括 WAAP、爬虫程序监测和抵御、DDoS 防护、安全信息和事件管理 (SIEM) 连接器、Web 优化、云计算、API Acceleration 等功能的解决方案，充分发挥安全投资的价值

省心省力的安全机制
利用由 Akamai 自适应安全引擎提供支持的自动更新和主动式自主调优建议，减少耗时的手动维护工作

易于使用
使用经过改进的 UI 设计来简化初始配置和综合安全运营，更有设置和问题排查指南可助您一臂之力

统一监测能力
通过 Akamai 安全解决方案的共享遥测数据，可以分析单个仪表板或主动发现报告中的各项安全指标

新资讯：DDoS 行为模式分析引擎

全新 DDoS 行为模式分析可增强应用层 DDoS 防御和简化相应的防御过程，并通过机器学习增强支持。DDoS 行为模式分析引擎通过基于行为和异常的检测算法，分析各种流量维度，如国家 / 地区来源、网络指纹和其他 HTTPS 请求属性，以量身打造保护措施，并提供针对应用层 DDoS 攻击的自动化防御方法。

DDoS 行为模式分析引擎利用机器学习，提升了流量维度的效率和决策能力，可用于创建流量的特征档案或基线。不同敏感度级别的评分机制兼顾了您的企业在检测攻击和减少误报方面的风险偏好。

Akamai App & API Protector 由自适应安全引擎提供支持，功能远超规则集。

卓越的攻击检测能力——作为 Akamai 客户，您的保护解决方案的深度与广度能够随着数字环境的发展而增加。除了自适应安全引擎提供的自动更新和自适应自主调优之外，App & API Protector 还拥有获得分析机构认可的卓越检测机制，可检测 DDoS、爬虫程序、恶意软件及更多攻击媒介。利用我们的威胁研究工具，确认您的 Akamai 防护措施可以抵御新出现和不断升级的 CVE。

应用程序安全性——App & API Protector 提供全套防御措施和定制化功能，可根据您企业的需求量身打造安全机制。Client Reputation、网络列表、新型攻击检测等有效功能为您对抗攻击者提供优势，同时简化了安全操作。Akamai WAAP 解决方案的高级应用层防御措施可抵御 DDoS、SQL 注入、跨站点脚本、本地文件包含、服务器端请求伪造和其他攻击媒介。

DDoS 防护和精细的速率控制——App & API Protector 是公认的卓越 DDoS 解决方案，可在多个方面提供 DDoS 防护。首先，它会在边缘即时拦截网络层的 DDoS 攻击，以抵御风险并节省资源。然后，它会在边缘自动检测并抵御复杂的第 7 层 DDoS 攻击，提供无须人工干预的实时保护，以应对不断演变的 DDoS 威胁环境。精细的速率控制会专门针对您的流量和攻击特征来定制 DDoS 防御机制。

爬虫程序监测能力和抵御——通过访问由 Akamai 提供的爬虫程序目录（包含超 1,750 个已知爬虫程序），实时监测爬虫程序流量。调查存在扭曲的 Web 分析、防止源站超载，并创建自己的爬虫程序定义，以允许不受阻碍地访问第三方和合作伙伴爬虫程序。App & API Protector 现在包含更多的爬虫程序控制措施，例如浏览器仿冒检测、条件操作和加密质询。

OWASP 十大风险清单

Akamai 可抵御 “OWASP 十大风险清单” 与 “OWASP 十大 API 安全风险清单” 列出的全部风险。进一步了解 App & API Protector 和 Akamai 安全产品如何保护客户，帮助客户抵御大型、常见或新型威胁。

如需了解 Akamai 针对 “OWASP 十大风险清单” 提供的防护机制，请下载白皮书。

API 防护——Akamai 业界卓越的 API 防护机制能够全面监测您的数字资产的流量，主动发现漏洞、识别环境变化并抵御隐蔽的攻击，从而助力您提升安全级别。利用 App & API Protector 的 API 功能，您可以：

- 自动发现 Web 流量中的各种已知、未知和不断变化的 API，包括其端点、定义和流量特征
- 只需点击几下鼠标，就能轻松登记新发现的 API
- 确保 API 能够抵御 DDoS 攻击、恶意注入、撞库攻击并防范违反 API 规范的行为
- 使用 App & API Protector 的个人识别信息报告功能控制敏感数据的处理，从而确保合规性

来自全球大型网络的性能及更多优势——Akamai 平台无与伦比的全球规模，为客户提供了竞争优势，同时支持客户实时监测大部分互联网流量。凭借这些海量数据，Akamai 能够提供切实可行的威胁情报，帮助企业提前应对不断变化的安全威胁，并支持在各种不同环境中更快地检测和抵御攻击。该平台还提供经验证的性能提升以及保证 100% 可用性的 SLA。

Malware Protector——此附加模块可在边缘处的文件上传之前对文件执行扫描，检测其中的恶意软件，阻止其进入企业系统，并防范恶意文件上传。由于不需要额外的应用程序或 API 配置，您可以省下分别在各系统内设置保护机制的时间。

Simple Start Onboarding——无论安全工具有多么出色，只有付诸使用才能发挥效力。Akamai 致力于打造一个方便易用的平台，助您提高工作效率、加强安全防护。您可以借助简便初始配置功能快速上手，或者只需点击几下鼠标，就能向新应用程序应用保护措施。

仪表板、警报和报告工具——Web Security Analytics 是 Akamai 的详细攻击遥测仪表板。您可以在此处分析安全事件、使用静态筛选器和阈值创建实时电子邮件告警，并使用可定制报告工具持续监控和评估 Akamai 平台上保护措施的有效性。

DevOps 集成——通过 GitOps 将安全措施无缝集成到 DevOps 工作流，确保始终在快节奏的开发过程中提供安全保障。Akamai 的 API 通过 CLI 或 Terraform 提供，支持通过代码全面管理 App & API Protector，并与用户界面中提供的每个操作配合使用。

SIEM 集成——App & API Protector 还提供了 SIEM API，并且自带连接 Splunk、QRadar、ArcSight 等平台的预建连接器。

随附功能——App & API Protector 如今整合了倍受 Akamai 客户青睐的多种产品，可提高监测能力和性能，其中包括：

- Site Shield：防止攻击者绕过基于云的防护而瞄准您的源站基础架构
- mPulse Lite：深入了解用户行为、解决实时性能问题，以及衡量数字变革对收入产生的影响
- EdgeWorkers：探索无服务器计算的优势，包括缩短上市时间，以及在靠近最终用户的位置执行逻辑
- Image & Video Manager：智能优化图像和视频，选择理想的质量、格式与大小组合
- API Acceleration：轻松管理访问权限、按需扩展以应对高峰并增强 API 安全性，从而提升 API 性能

免费层级的产品在使用时可能存在一定限制。如需了解详情，请联系 Akamai。

高级安全管理

对于那些应用程序环境更复杂且有着高级安全需求的客户，可以通过选配的高级安全性管理模块获得自动化机制与配置灵活性。高级安全性管理选项包括附加安全配置、速率策略、安全策略、应用层 DDoS 控制措施、自定义 WAF 规则、正向 API 安全性，并且支持访问现成的 IP 声誉威胁情报 (Client Reputation)。

Managed Security Service

Akamai 为所有客户提供全天候标准支持服务。除了按需提供咨询或单项目作业方面的专业服务之外，Akamai 还提供三种层级的托管服务——全托管式 WAAP 服务、托管式攻击支持，以及专门的安全运营中心支持。

要了解 App & API Protector 并注册使用免费试用版，请访问 akamai.com/aap

扫码关注，获取最新云计算、云安全与CDN前沿资讯