WAF 评估终极检查清单

一款可根据您的应用程序和 API 安全需求找到正确解决方案的工具

让您更轻松地找到合适的 Web 应用程序防火墙 (WAF) 或 Web 应用程序和 API 保护 (WAAP) 供应商。使用这份全面的检查清单来评估 WAF 和 WAAP 提供商，确保解决方案满足您的安全、性能、财务和运营需求。

安全功能

应用程序安全

- 确保**覆盖 OWASP 十大漏洞**，例如 SQL 注入、XSS、LFI 和 SSRF。确认是否可以自定义以及自动部署保护措施。
- 评估您的解决方案是否会主动控制来自**劣迹 IP** 的流量，并在发现先前的**例外情况遭到滥用**时向您发出警告。
- 评估**允许列表和拦截列表的灵活性**，确定您能否通过关联 IP、地理位置、ASN 和 TLS 指纹等属性来创建有效策略。

DDoS 防护

- 验证供应商是否为应用程序和 API 提供**多层 DDoS 防护**，包括针对 DNS、第 3 层/第 4 层和第 7 层的攻击防护。
- 确认解决方案是否提供**行为 DDoS 检测**来确保应用程序安全。
- 确定**速率限制**控制措施的精细程度。这些控制措施是自动还是手动配置的？这些措施能否防范容量耗尽型和慢速 POST 攻击？
- 审查是否具备在 DDoS 攻击期间**降低负载**以及提高性能的能力。
- 了解 DDoS 事件期间流量增加所带来的潜在**额外成本**。
- 确保**第 7 层 DDoS 攻击防护可以自动实施**，以节省团队的时间并减少所需的专业知识。**这些保护措施是否适应**您的特定流量概况或风险承受能力？

零日漏洞保护

- 确认 WAF 是否提供**针对已知 CVE 的保护措施**，及其能否快速调整以抵御新的零日漏洞。调查该解决方案的**零日防御跟踪记录**和响应时间。
- 确定您作为客户是否有**针对特定 CVE 的保护措施**。

API 防护

- 确保该解决方案能够**保护 API 端点**免受注入攻击、DoS 攻击的影响并防范违反规范的行为。
- 检查 **API 发现**功能，确认它能否自动检测到新的和已修改的 API，以及对这些 API 实施保护的难易程度如何。
- 确认 **PII 检测和告警**，以保护敏感数据并防止数据泄露。

爬虫程序防护

- 确认 WAF 能否使用爬虫程序目录和定义来**检测并抵御自动威胁**。爬虫程序目录的全面性如何？它多长时间会针对新的和已修改的爬虫程序更新一次？
- 确定该工具中提供的**爬虫程序定义**。您能否**创建自己的**爬虫程序定义？
- 检查该解决方案是否包含不会中断用户体验的 **CAPTCHA 或人工验证机制**。CAPTCHA/验证是否要求最终用户在继续操作前与其进行交互？

威胁情报和自动化

威胁情报

- 确保提供商将**第一方数据**用于威胁情报，以避免出现第三方延迟和潜在的数据篡改。
- 验证提供商的**威胁搜寻团队**的规模以及负责监控新兴风险的安全专家的全球网络。
- 评估由情报数据库处理的**数据量和数据相关性**。它是否包含来自与您类似的行业或者经常遭受网络攻击的企业的数据？

自动化

- 检查 WAF 是否依赖**过时的规则集技术**。它是否使用先进的现代技术，例如通过先进的启发式方法和机器学习进行自动更新？
- 确保规则集会进行自动更新，**而无需人工干预**。自动更新是否在全球范围内应用？您可以通过哪些选项来移除先前应用的更新或**在实时流量上测试该更新**？
- 确定该解决方案是否无需干预即可根据您的环境自定义保护措施。该解决方案是否可以根据贵企业的实时流量概况来不断**自我调整**安全策略？
- 评估该解决方案如何控制**误报**。它如何在减少误报与最大限度减少**有效流量中断**之间取得平衡？

监测和报告

精细监测能力

- 确保 WAF 让您可以**深入了解威胁**和性能，并提供覆盖多解决方案环境的可定制仪表板和报告。
- 运行 WAF 时，安全团队的大部分时间都花费在数据控制台上。了解您可以访问的**自定义内容**、主动分析功能以及**报告的详细程度**。
- 评估该解决方案在有效**监控 API 流量**和应用程序流量、检测滥用以及提供针对 API 蔓延的详细见解方面的能力。

实时告警和主动分析

- 检查是否具有可在出现重大威胁时向您的团队发送通知的近乎**实时的告警**功能。告警应该能够根据严重性、来源或攻击类型等具体标准进行自定义，以便于理解和实现快速响应。
- 确认该解决方案是否能够提供针对攻击何时、在何处以及如何发生的**预分析见解**以减轻安全团队的负担。该解决方案还应该**提供后续步骤建议**来增强您的安全态势。

平台和架构

全球覆盖

- 确认 WAF 是否提供对全球网络边缘或 CDN 服务的访问来增强性能和安全性。研究该解决方案的**全球可用性**，以确保覆盖您和客户的主要运营地点。

云和混合支持

- 验证该解决方案是否**适用于任何云环境**以及能否支持您的多云、混合和本地环境。如果该解决方案基于 CDN，请确保它能够将保护措施扩展到 CDN 之外，以实现边缘安全。

恢复能力和故障转移

- 评估该**解决方案的恢复能力**，确定它能否在故障或中断期间进行自动故障转移以实现持续保护。
- 查看提供商的**近期服务中断情况和应对措施**。
- 确定**服务等级协议** (SLA) 是否满足您的业务需求。

支持和托管服务

所包含的支持及获得服务

- 确定 WAF 解决方案**所包含的支持级别**以及需要付费才能获得的支持级别。
- 检查**全天候事件响应**是否可用以及在攻击发生期间您是否可以直接访问安全运营中心 (SOC)。
- 确保供应商提供**全托管式安全服务**以弥补您内部资源中的潜在不足，包括用于处理攻击、配置或人员流动的专业知识。

集成和 DevSecOps 兼容性

API、CLI 和基础架构自动化

- 检查该解决方案是否提供 **API、CLI 和 Terraform** 集成，以实现安全自动化并将其融入您的开发工作流中。对于跨环境实现一致的安全措施来说，支持 GitOps 和其他基础架构即代码框架至关重要。

SIEM 集成

- 确保 WAF 能够与 Splunk 或 QRadar 等 **SIEM 工具无缝集成**，以增强监控、报告和事件响应能力。

业务成果和效率

可扩展性和性能

- 确认该解决方案能够**自动扩展**以处理大量流量，同时不会降低性能。该解决方案在什么情况下会出现延迟或在高负载下变得容易受到攻击?
- 确保有 **100% 可用性** SLA，并评估该解决方案是否还能提供缓存和流量加速等性能增强功能来改进您的应用程序。

统一管理

- 评估提供商是否提供单一管理平台界面来**管理所有环境（云、本地和混合）中的安全策略**。确保该解决方案可以与您当前的产品组合集成，并为安全和开发团队提供顺畅的体验。

经济高效

- 评估该解决方案是否有能力**统一单个供应商旗下的 WAF、DDoS、爬虫程序管理和 API 防护**解决方案以降低复杂性并减少管理成本。评估安全有效性和运营成本之间的平衡以确定总体价值。

信任和供应商可靠性

服务和稳定性历史记录

- 查看提供商过去 5 年的**故障和服务中断历史记录**。
- 验证该公司的**财务状况是否稳健**。是否有盈利？公司经营了多长时间？它为什么规模和类型的客户提供服务？

声誉和评价

- 研究经过验证的评价和客户荐言，了解您所在行业的类似企业是否**信任该供应商**。当前客户的应用场景是否与您的需求相符？
- 确定它的应用程序和 API 保护解决方案是否**得到了 Gartner 和 Forrester 等行业分析公司的认可**。
- 确保在与供应商进行讨论后，您对成为其客户后出现的问题时的响应速度和支持**充满信心**。询问完成初始配置后谁将为您的帐户提供支持。

想要了解有关 Akamai WAAP 解决方案的更多信息？
开始免费试用 App & API Protector。