破除有关 Web 应用程序防火墙的 5 个误解

对于需要线上开展任务关键型业务的企业，Web 应用程序防火墙 (WAF) 是阻止恶意流量侵入的第一道防线，同时确保合法流量的顺畅通过。WAF 技术已经问世多年，它的最初定义对于其后续发展和现代应用已显得过于简单。这导致许多商业领袖和安全专家仍然坚持过时的观念和误解。

这些误解可能导致企业低估和未能充分利用其技术堆栈中可能已经存在的 WAF 的功能，继而为攻击者敞开大门，增加了运营风险。对 WAF 技术的全面数字化安全需求持续增长。为了提升安全态势并充分利用新的 WAF 技术进行保护，我们首先需要澄清那些最常见的误解。

我们在 2023 年第三季度观察到 99.3 亿次 Web 应用程序攻击

在 2023 年第三季度，每日攻击数量达到峰值，大约为 3.27 亿次

资料来源：Akamai 威胁研究

误解 1

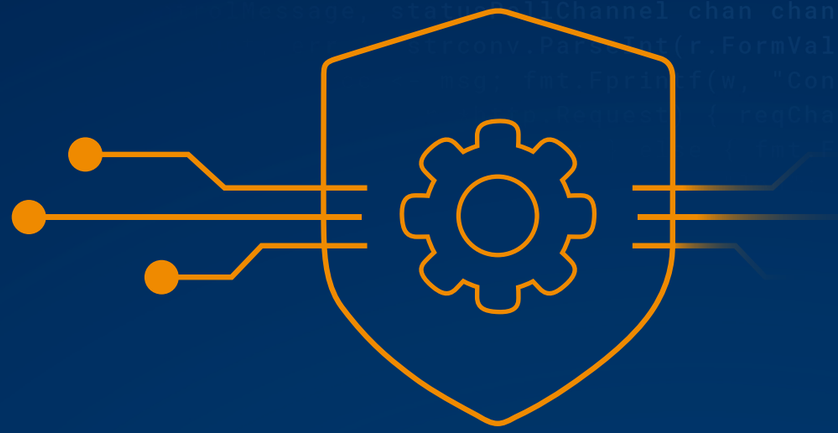
WAF 需要不断进行手动更新，才能保持有效

虽然更新到最新状态确实能够提供最新的保护措施，但围绕这一说法有一些误解需要澄清。目前，许多企业缺乏足够的资源或安全专业知识来持续更新和优化 WAF 规则。自动化和自适应更新不仅能节省时间和提高易用性，更能降低风险。通过对选择手动更新的企业的调查，我们发现超过 77% 的企业在规则集更新方面落后了 5 个或更多版本。Akamai 不断自动推送 WAF 更新，帮助您的企业节省时间、资源投入，并避免不必要的风险。

误解 2

WAF 仅仅控制流量

传统的 WAF 位于用户与 Web 应用程序之间，并根据预设的规则列表对二者之间的 HTTP 流量进行检测。Akamai 在传统 WAF 的基础上进行了快速而强有力的创新，以提供更多的功能和保护措施，其中包括 DDoS 抵御、API 安全、爬虫程序抵御、恶意软件检测、敏感数据发现以及性能加速等功能。随着 App & API Protector 的发布，您的 WAF 安全解决方案现已与 Site Shield、mPulse Lite、EdgeWorkers、Image & Video Manager、API Acceleration 等多项备受客户喜爱的技术紧密结合。Akamai 的 WAF 解决方案是一种集多种功能于一体的技术，可为安全专业人员提供完整的监测和控制能力，进而确保整个资产安全无虞。



误解 3

WAF 导致防御人员陷入告警疲劳

询问任何一线防御人员，您都将听到安全团队抱怨他们因需要处理大量告警和触发事件，特别是由 WAF 防御产生的告警和触发事件，有多么的倍感压力和不堪重负。Akamai 开发 Adaptive Security Engine 正是为了解决这个问题，它也是 Akamai WAF 解决方案的核心技术。借助 Adaptive Security Engine，结合机器学习、实时安全情报、高级自动化以及来自 400 多名 Akamai 威胁研究人员的专业见解，您的企业可以获得现代化的保护。Adaptive Security Engine 专为保护 Web 应用程序和 API 资产而构建，它的独特之处在于能够学习每个客户的流量模式和遭受攻击的模式，实时分析每个请求的特征，并利用这些知识来阻止并应对未来的威胁。通过依靠 Adaptive Security Engine，防御人员可以摆脱告警疲劳，节省宝贵的时间，并减轻保护应用程序和 API 的工作负担。

经过验证，Adaptive Security Engine 的调优建议可将误报率减少到原来的

1/5

误解 4

WAF 规则的可自定义水平越高，提供的安全性就越高

更多的规则意味着需要更多的设置、测试和分析工作。规则的数量并不总是与安全性成正比，过多或过少的规则都可能无法提升安全性。如果您是认为“更多规则”就等于“更加安全”的安全专家，请不用担心。我们的 WAF 支持数量无限制的自定义规则，无论您有多少规则，我们都能提供主动且自适应的规则更新。通过自动更新和自动自调优，您的团队能够以更有效的方式大规模高效验证 WAF 配置，确保整个数字资产的安全。想要添加新规则？借助评估模式，您可以评估新规则和修改后的规则对实时流量的影响，并在客户门户仪表板中实时查看效果。通过这种影子模式的测试方式，您能够验证新规则在部署后是否能达到预期的保护效果。

误解 5

WAF 只会阻碍开发人员

开发人员可为现代企业带来客户认可的价值。如果安全问题成为障碍，创新步伐将放缓，产品发布周期将延长，实现价值的速度也将减慢。然而，如果未经测试就发布产品，可能会导致严重的安全后果，进而导致业务中断。Akamai 致力于支持安全专家和开发人员的工作。我们坚信，使用 WAF 防御措施能够增强应用程序和 API 等的安全性，从而推动 DevSecOps 文化的发展，提升速度、敏捷性和协作能力。这就是为什么我们所有的 WAF 功能都通过开放的 AppSec API 或 Terraform 进行管理的原因，这样您的团队就可以自动载入应用程序和 API，以及轻松管理安全配置。当您需要帮助时，Akamai TechDocs 为您提供一系列专为开发人员设计的现代、直观的交互式功能。

Akamai 如何为您提供帮助

要想应对迅速扩大的攻击面、不断演变的威胁以及高活跃度的攻击者，防御人员需要具备超越传统 WAF 保护机制的监测能力。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、爬虫程序抵御、API 安全和 DDoS 防护。App & API Protector 能够持续、自动地更新安全保护机制，让您一键实施自定义策略建议。Adaptive Security Engine 是 App & API Protector 的核心，它融合了机器学习、实时安全情报、高级自动化，以及来自 400 多位威胁研究人员的深入洞见，为企业提供了现代保护机制。

开始免费试用，或了解 Akamai 如何为您面向 Web 的关键资产提供保护，帮助您的企业降低风险和操作上的阻碍。