白皮书

从 WAF 到 WAAP：Akamai 一路打造全面的应用程序和 API 安全解决方案

目录

前言

当下，企业的攻击面日益扩大且呈现多样化的趋势，运营摩擦和成本不断攀升，并且面临持续演变的多维度威胁。在这种形势下，安全团队亟需超越传统 Web 应用程序防火墙 (WAF) 的监测能力。具体而言，他们需要更多自动化工具来提高效率，并在应用程序和应用程序编程接口 (API) 生态系统中提供更深层次的保护措施。对于这些保护措施来说，更现代的术语是 Web 应用程序和 API 保护 (WAAP)。独具慧眼的企业会将其业务安全和客户安全放在首位，他们需要在其整个数字资产中针对多种威胁提供全面防护。除了保护应用程序免受已知、未知和零日攻击的影响之外，这些保护措施还包括：

- 自适应威胁检测
- 自动策略更新
- 强大的 DDoS 攻击防御措施
- API 发现和保护
- 爬虫程序监测和抵御
- 在开发生命周期内轻松集成

本白皮书探讨了传统 WAF 技术、从 WAF 向 WAAP 的转变，以及推动 WAAP 解决方案不断发展的持续市场需求。作为安全领域的佼佼者，Akamai 专注于安全技术创新方法，以支持并保护最终用户的网络生活。

WAF 的传统定义

传统的 WAF 位于最终用户与 Web 应用程序之间的流量路径上。WAF 会检查流过它的未加密或加密 HTTP 流量，以确定是否存在一系列规则所定义的任何攻击。

大多数 WAF 依赖于预定义的一系列规则来识别混杂在合法 HTTP 流量中的恶意 HTTP 请求，以防范数以千计的潜在已知漏洞。此外，新的攻击媒介或现有攻击媒介的其他排列组合不断发展，并被攻击者所利用。在这种情况下，传统的 WAF 需要不断更新其规则并根据合法流量特征进行调整，这些特征会因应用程序而异并随时间推移而变化。

随着最终用户在保护和性能方面的要求越来越高，WAF 的范围也不断扩大，以纳入相关的安全技术和服务，如分布式拒绝服务 (DDoS) 攻击抵御、API 安全和爬虫程序抵御功能。这种持续的发展变化需要新的定义和新的术语。

传统 WAF 面临的挑战

使用 WAF 的企业经常声称，WAF 在有效性、易管理性以及对受保护应用程序和 API 的影响方面无法满足最初的期望。由于检查数十亿的 Web 和 API 请求是否存在恶意代码经常会造成 Web 性能问题，因此 WAF 往往成为了企业内部摩擦、性能降级以及因安全协议导致的部署障碍的根源。

传统 WAF 所面临的一些最严峻的部署挑战源自于以下方面：

- 检测不准确和高误报率会导致告警疲劳和其他风险
- WAF 依赖于人工审查、调整和维护
- 缺乏精细控制会导致过于严厉的拒绝政策，从而中断最终用户体验和业务流程
- 过时的威胁情报会导致漏洞增加
- 由于存在限制和缺乏灵活性，出现性能下降和覆盖范围减小
- 限制太多，无法保护数字扩展

传统 WAF 是一种功能强大的安全工具。但是，它们往往会给企业带来运营痛点和无法缓解的风险，本白皮书将对这些问题进行探讨。

寻求通过 WAAP 解决方案来更新其 WAF 技术的企业应确保该解决方案既能提供商业价值，又能提供强大的安全防护。从 WAF 转向 WAAP 可以将这种强大的防护能力与功能、效率和易用性相结合，以满足企业对安全团队和其他团队的需求。

设计原则——从 WAF 到 WAAP

由于传统 WAF 产品专注于最终用户规则创建，因此任何供应商都可以构建一个 WAF 解决方案，并相对轻松地将其推向市场，围绕开源开放全球应用程序安全项目 ModSecurity 核心规则集 (OWASP CRS) 构建的商业产品的普及就证明了这一点。

但是，提供商难以设计出一个具备以下特性的全面 WAAP 解决方案：

- 可进行内联部署，以便在新漏洞出现时保护应用程序和 API
- 能够紧跟现代应用程序开发实践
- 提供同样强大的 DDoS 攻击防御、爬虫程序抵御、API 保护和客户端 Web 应用程序保护层

在着手设计 WAAP 解决方案时，Akamai 认为它应该远超“足够好”的范畴。App & API Protector 的设计初衷是解决安全风险，同时让我们的客户企业专注于主要业务目标。作为我们的设计蓝图，我们认为理想的 WAAP 解决方案应该提供：

有效的安全防护
应用程序在业务的方方面面都发挥着重要作用。保护应用程序免受恶意攻击是企业安全团队的基本目标。安全团队面临的挑战是找到一个能够提供最佳检测功能的 WAAP 解决方案。理想的安全工具会将检测功效放在首位，因为它是 WAAP 解决方案中最重要的方面，并且在零日、漏洞利用以及常见漏洞和风险 (CVE) 防御方面具有出色的记录，以及令人印象深刻的可用性历史记录。

准确性
安全团队需要在抵御风险与促进业务快速发展之间取得平衡。理想的解决方案将具备自主调整机制，可帮助减少误报，同时不影响最终用户体验和业务流程。

现代保护措施

各企业必须不断（并且常常需要手动）将保护措施更新为最新规则，以解决发现的新漏洞。为此，他们需要两项关键能力：获取攻击媒介的最新情报，以及能够调整防御策略以应对可修改攻击的专业安全资源。理想的解决方案将成为威胁情报社区中的佼佼者，并提供用于在整个资产保护范围内简化安全运营的功能。

适应性

威胁形势在不断快速发展变化。随着依托 AI 技术的攻击即将出现，安全团队需要比以往更加高效地开展安全运营。理想的 WAAP 解决方案会将高级自动化、机器学习和深度全球情报相结合，以自动提供更新并提供能够一键实施的自定义规则修改建议。

监测能力

传统的 WAF 解决方案通常会源源不断地发出告警，并依靠安全从业人员仔细分析每个告警，从而导致内部资源消耗殆尽。更有效的 WAAP 解决方案可通过告知企业攻击发生的时间、位置和方式来提供多解决方案监测能力以及主动提供攻击的背景信息，从而减轻资源负担。

可扩展性

如果一个解决方案没有足够的规模来处理传入流量，那么它很容易就会遇到瓶颈，不仅会导致网络延迟增加，而且可能会在负载加重时崩溃。有效的 WAAP 策略能够自动进行无缝扩展以应对随时间变化的流量需求和攻击，并且可以在不中断或降低性能的情况下提供持续防护。

合作

有效的安全解决方案需要能够与您当前的产品组合集成、可编程、简单易用，并且能够提供流畅的使用体验。理想的解决方案可以促进安全团队与开发团队之间的沟通和协作。

支持

在发生严重的安全事件时，企业往往会因技能和资源储备不足而难以迅速采取有效措施。理想的解决方案将提供常规的托管服务方案以及按需服务方案，这些方案可提供用于常见场景（包括主动攻击、服务问题、人员流动、内部技能组合差距等）的专业知识和抵御措施。

考虑到这些设计原则，我们从核心技术开始，了解 Akamai 如何着手构建我们出色的 WAAP 解决方案 App & API Protector。我们的解决方案将多款安全产品合而为一，以全面解决保护应用程序、抵御容量耗尽型 DDoS 攻击、保护整个资产中的 API 以及控制爬虫程序流量方面的挑战。

Akamai 的 WAAP 策略

摆脱传统规则

随着市场从传统 WAF 设计原则转向有效的现代 WAAP 安全解决方案，有效检测和抵御技术仍然是重点。

Akamai 于 2009 年首次推出了我们的 WAF，也是全球首款基于边缘的 WAF。当时的安全供应商都在提供基于静态规则集的 WAF 作为其检测基础。而 Akamai 通过构建基于规则的专有引擎（称为 Kona 规则集）实现了差异化，该引擎采用了少量灵活规则（而非静态规则），并结合异常评分模型来更好地解决攻击的准确性和监测能力问题。

随后在 2017 年，Akamai 推出了自动攻击组。借助 Akamai 托管的保护措施，各企业无需持续配置和更新规则。自动攻击组的出现带来了一场变革，它迅速在数以千计的 Akamai 客户主动 WAF 策略中得以启用，使客户能够利用这一全新方法。

Akamai 继续发展我们的应用程序安全方法，优先考虑组合的应用程序和 API 保护（包括爬虫程序防御功能），并于 2021 年推出了 App & API Protector，此 WAAP 解决方案旨在取代 Kona Site Defender，为企业和不断发展的全球业务提供保护。App & API Protector 将 Kona 规则集技术升级改造为 Adaptive Security Engine，改变了 Akamai 实现安全运营的方式。

超越速率限制，打造现代化的应用层 DDoS 攻击防御措施

就 DDoS 攻击而言，速率限制是一个经过验证的有效工具。但是，复杂的第 7 层 DDoS 攻击、多媒介攻击以及 API 利用的兴起，使传统的 DDoS 攻击防御措施变得力不从心。依赖于固定阈值和预定义特征的静态防御措施是被动的，容易出现误报，尤其是当攻击者越来越多地将恶意流量与合法请求混在一起时。而这正是 Akamai 改变了 DDoS 防御方法并推出了 URL 保护和 Behavioral DDoS Engine 等全新创新技术的高明之处。

Behavioral DDoS Engine 是 Akamai App & API Protector 的一项先进附加功能，与 Adaptive Security Engine 一起成为该产品的核心技术之一。这些引擎共同提供针对现代威胁的出色防护能力，使 Akamai 成为 WAAP 领域的佼佼者。此双引擎方法可以提供自动更新、自主调整功能和情景感知检测来实现无需人为干预的体验，从而让 Akamai 在市场中脱颖而出。

利用单一解决方案提供全面保护

如今，随着无服务器边缘计算、基于微服务的架构、单页应用程序以及塑造应用程序安全性的 SaaS/IaaS/PaaS/FaaS 方法的应用，现代开发实践在不断变化，应用程序安全也在不断被重新定义。

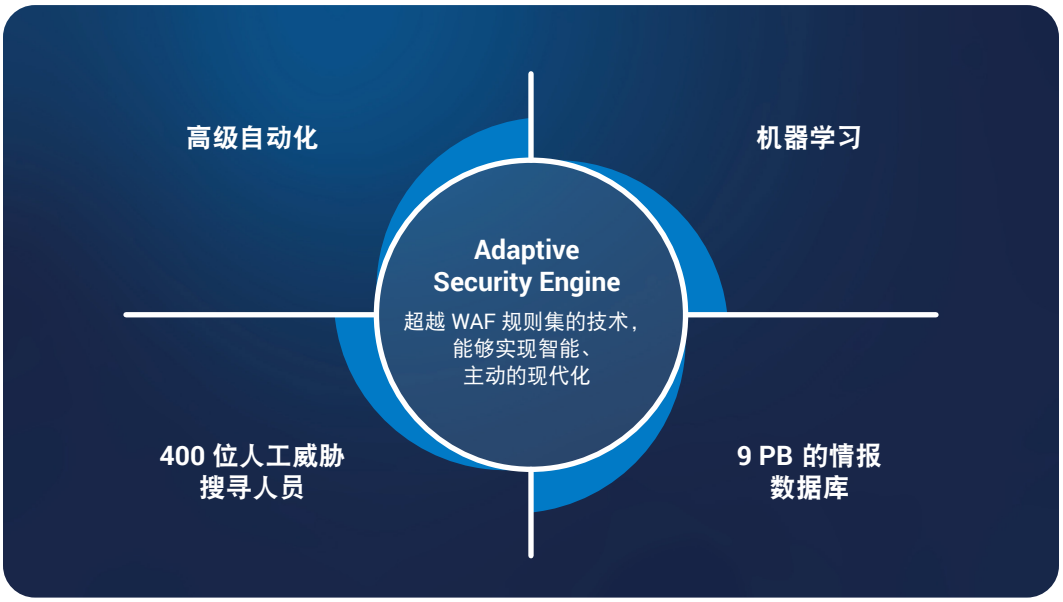
为了保护复杂 IT 环境中的现代应用程序和 API，Akamai 采用适应性更强、更灵活且更全面的方法重新构建了我们的应用程序安全技术。随着 Akamai 的 WAAP 解决方案从 Web Application Protector 和 Kona Site Defender 迁移到 App & API Protector，更多的安全功能和特色工具集被纳入其中。

App & API Protector 现在提供了很多额外的安全增强功能，所有这些功能都可以通过单一界面进行查看和控制。Akamai 的 WAAP 解决方案融合了以下功能：

1. Adaptive Security Engine
2. 可实施精细控制的应用程序安全
3. DDoS 攻击防御措施，包括高级第 7 层 DDoS 攻击防护措施
4. API 保护措施，包括发现和 PII 保护功能
5. 爬虫程序监测和抵御功能
6. 一个遍布全球、提供威胁情报并具备恢复能力的平台

Adaptive Security Engine

Adaptive Security Engine 融合了机器学习 (ML)、实时安全情报、网络安全专家的见解以及高级自动化技术，提供下一代安全防护。作为 Akamai 的核心检测和防御技术，Adaptive Security Engine 无需人工干预，即可确保所有 Web 应用程序和 API 资产的安全。它还进一步推动了 Akamai 从 WAF 到 WAAP 的转变，该转变整合了包括 Bot Manager、DDoS 攻击防护和 DevOps 集成等相关的安全解决方案。



Adaptive Security Engine 的独特之处在于它能够学习每个客户独有的流量模式和遭受攻击的模式，实时分析每个请求的特征，并利用这些知识来拦截并应对未来的威胁。它使用相同的平台见解和情报，通过调整建议来减少误报。此自主调整功能以主动更新的形式提供自适应威胁防护，为安全和开发团队带来了便捷的使用体验。

自适应威胁检测

该引擎采用了一个多维威胁评分模型，可以将这些平台情报与每个请求的数据/元数据相结合。这些数据会通过决策逻辑进行处理，以准确识别真正的攻击。

自适应检测在识别高针对性、规避性和隐蔽性的攻击方面特别有效，因为老练的攻击者会在其方法上投入更多的时间和精力。当攻击者扫描漏洞和错误配置时，Adaptive Security Engine 会收集并关联与其攻击手段相关的证据，从而使攻击者的历史指纹更容易识别。

除了实际有效负载及其在请求中的位置外，它为每个客户评估的其他攻击维度示例包括：

- 侦察和/或攻击的历史记录（例如，频率、规模、严重性）
- 任何恶意自动化和攻击工具的迹象
- 与已知攻击流量来源的关联性

此外，利用两项专有技术对 Adaptive Security Engine 进行了改进：Smart Detect：可以将输入内容标记为指纹，以实现高度准确的检测；Smart Sniff：可以检测请求正文的正确内容类型，以防止内容篡改和绕过。Akamai 威胁研究人员利用 Akamai 广泛的基础架构和系统，在所有生产流量中被动运行新的检测，然后使用 ML 模型分析这些结果。

自动更新

现在，很多企业都缺乏足够的资源或安全专业知识，无法持续跟踪不断发展的威胁、更新配置以及对其 Web 流量进行重新测试以优化策略。为此，Akamai 持续使用 AI/ML 自动测试框架来更新 Adaptive Security Engine，以便在保持高准确性的同时应对不断变化的威胁。这些更新往往在零日攻击被披露之前就已提供相应的防护。

测试框架以确保准确性

测试 WAAP 解决方案依赖于一个简单的前提：测试不同的攻击媒介并阻止 Web 攻击。但是，需要考虑以下因素：

- 真实环境比测试环境复杂得多，往往会导致误报和漏报。
- 设计一个考虑到准确性的测试框架需要额外的验证——不仅仅是进行攻击检测，还要在检测时避免无意中触发误报或漏报。
- 测试需要使用真实的 Web 流量，包括合法流量和攻击流量。

Adaptive Security Engine 更新由多个阶段组成，可确保合法流量不会受到不利影响：

- 所有检测都使用合成流量进行了实验室测试，以确保它们能够正确捕获攻击，而不会引入误报。然后，会针对实时生产流量测试更新，以确保样本对当前平台流量有效。此过程涉及针对真实客户流量以影子模式运行更新。
- 以影子模式运行可确保不会对客户流量产生任何影响，同时仍然可以运行测试检测准确性。
- 在更新完成第二阶段后，ML 会识别出人类分析可能遗漏的模式或触发因素，随后威胁研究团队会对结果进行人工审查。
- 只有在这些检查完成每个阶段后，更改才能进入下一阶段，并部署到更大的网络分段。在完成 100% 部署后，自主调整功能将消除特定于客户流量模式的所有剩余误报。

自动自主调整

人工调整可能会导致策略过时和人为错误，而自动自主调整可以减轻人工调整的负担，实现近乎于无需人为干预的体验。Adaptive Security Engine 可以对每个安全策略的所有触发条件应用 ML、统计模型和启发法，以准确区分真正的攻击和被误认为是攻击的最终用户流量。它不是仅在初始配置期间应用的通用全平台检查，而是一个全天候执行的持续调整过程，无需最终用户进行配置或干预。

自主调整非常流畅并且很简单。安全管理员只需点击一下，即可通过用户界面轻松查看和接受相关建议，他们也可以使用 AppSec API、命令行界面 (CLI) 或 Terraform 自动执行相关操作。为了提高透明度，一个预先过滤的 Web 安全分析链接显示了所有被认为是误报的请求，并对每项调整建议提供了理由。

配置和自动化灵活性

当 WAAP 解决方案供应商不再依赖传统的规则集技术时，配置和自动化将变得更加灵活。Adaptive Security Engine 会赋予用户以下能力：

- 针对不同的应用程序及其关联的风险偏好采用不同类型的 WAF 更新（自动与手动）
- 如果应用程序/流量行为不符合标准，则控制每个攻击组的操作以及定制所需的贡献规则
- 针对不同的请求特征（例如，IP、地理位置、标头、有效负载等）设置简单和复杂的条件
- 利用“受罚区”功能，主动抵御已检测到对您自己的应用程序进行可疑 WAF 攻击/扫描的威胁来源
- 修改调试标头
- 修改请求有效负载检查大小或攻击有效负载日志记录设置
- 对检测逻辑的变化进行模拟，以便放心地将这些更改推送到生产环境中

在现实世界中验证

评估模式让 Akamai 客户能够灵活、精细地配置特定的 Adaptive Security Engine 版本并测试更新或新规则/策略。客户可以先查看新的更新或更改，然后再酌情或者根据其具体的 Web 应用程序环境的需要选择启用这些更新或更改。为了实现有效的安全现代化，Akamai 认为，对实时流量进行测试比对过去的流量进行测试更能提高安全成果。评估模式类似于应用影子规则，您可以看到实时结果，就像执行了策略一样，但不会对当前的最终用户造成任何影响。企业可以选择这种手动/评估操作模式，以最大限度地减少对误报和漏报的意外影响。

集成现代化保护措施

安全和 DevOps 团队还可以使用 CLI、Akamai Terraform 或其 CI/CD 自动化管道中的脚本来集成对 Akamai API 的调用，从而有效运行安全功能。配置和自动化灵活性可确保兼顾强大的安全性和开发速度。这些集成可以：

- 实现快速的应用程序初始配置
- 为大型应用程序组合提供统一的安全策略管理
- 跨混合云和多云基础架构集中实施安全措施
- 在一个 GitOps 工作流程中改善 DevOps 与安全团队之间的协作，以实现最佳覆盖范围

此外，借助安全信息与事件管理 (SIEM)，您可以收集 Akamai 平台上发生的安全事件。相应地，我们的 SIEM Integration 解决方案提供了一种方法，可以将 SIEM 事件传输到本地和基于云的 SIEM 分析工具（如 Splunk 和 QRadar），从而使您能够通过四个基本步骤将 Akamai 安全事件整合到您的整体事件和安全基础架构中。

您可通过以下功能保护和控制您的数据馈送：

- **事件过滤**
  使用安全配置和安全策略来帮助您专注于应对真正的威胁。
- **数据保留**
  收集器会将数据存储 12 个小时，以便您捕获错过的事件。
- **SIEM 过载保护**
  在您的 SIEM 连接器中，您可以定义每次请求中获取的最大安全事件数。这将帮助您避免 SIEM 应用程序过载。
- **获取间隔**
  您可以定义 SIEM 连接器对 SIEM API 发出调用以获取安全事件数据的频率。

应用程序安全防护与 DDoS 防御

应用程序安全防护是现代网络安全的一个关键方面，可确保应用程序在面对各种威胁和漏洞时保持恢复能力。其重要性体现在多个关键领域。数据完整性和保密性至关重要，因为应用程序安全可确保敏感数据免受未经授权的访问和篡改。它还在业务连续性方面发挥着重要作用，可保护应用程序不会因安全事件而中断，从而确保服务的持续可用性。此外，应用程序安全对于声誉管理至关重要，可防止出现损害企业声誉和削弱客户信任的违规行为。最后，它可以帮助企业遵守法规要求，从而避免法律和经济处罚。

从功能上来说，WAAP 解决方案可以过滤并监控 Web 应用程序与互联网之间的 HTTP 流量。这可以防范基于 Web 的攻击，如 XSS、SQL 注入和 DDoS 攻击。

App & API Protector 因其卓越 DDoS 防护能力而备受认可，它专为应对旨在让资源不堪重负的容量耗尽型攻击而设计。该解决方案可以通过下列方式抵御 DDoS 攻击：

- **基于边缘的 DDoS 攻击抵御**
  利用 Akamai 的全球分布式边缘平台，App & API Protector 可以在 DDoS 攻击到达应用程序源站之前即时阻止它们。此边缘优先的方法可确保最大限度地降低延迟并提供最大程度的保护，同时不会影响应用程序的性能。

- **速率限制**
  App & API Protector 提供自适应速率限制功能，以抵御分布式应用层 DDoS 攻击。可以对这些控制措施进行配置，以根据各种条件（包括但不限于 IP、地理位置、IP 声誉控制、各种 HTTP 标头以及匹配条件）限制传入请求的速率。

- **使用智能减载技术进行 URL 防护**
  采取不同方法来实施速率限制。借助 URL 防护，您可以根据可接受的请求速率（最大 RPS，具体取决于源站容量）保护自己的源站免受过多请求的影响。它专门用于保护计算量大的 URL、API 端点等免受高度分布式应用层 DDoS 攻击。

- **Behavioral DDoS Engine**
  App & API Protector 的新增功能 Behavioral DDoS Engine 是一个功能强大的工具，可用于打造纵深防御策略。通过使用 ML 建立流量基准并识别违反规范的异常情况，它引入了一种无需人工干预即可管理和抵御 DDoS 事件的方法。该引擎通过了解不断变化的流量模式来工作，允许用户定义系统如何响应不同的异常情况，而无需设置明确的阈值，从而减轻了管理和调整系统的操作负担。

- **自动更新和自适应自主优化**
  通过使用 Akamai 的双引擎策略（即 Adaptive Security Engine 和 Behavioral DDoS Engine），App & API Protector 可以通过自动更新和 ML 驱动的自主调整来不断适应新的威胁，从而减轻操作负担。

Behavioral DDoS Engine：工作原理

Behavioral DDoS Engine 的核心是一种先进的 ML 模型，该模型可以持续监控实时流量，为正常行为建立基准并即时检测表明遭受攻击的偏差。通过分析多个动态维度（例如，国家/地区来源、TLS 模式、IP 和 TLS 指纹）的流量模式，此引擎可以快速识别出异常情况并采取措施。

Behavioral DDoS Engine 的关键组成部分包括：

- **实时行为监控**
  该引擎会持续分析流量，以便为正常活动建立基准并即时检测表明遭受潜在 DDoS 攻击的偏差。

- **利用机器学习精准抵御攻击**
  先进的 ML 模型可增强该引擎识别流量模式中细微异常情况的能力，同时确保实施准确的抵御措施而不妨碍合法用户。

- **主动抵御**
  利用 Akamai 的全球网络洞察（每天的流量达 1,056 TB），该引擎可以预测并化解攻击，避免对企业造成影响。

- **多维分析**
  该引擎可从多个维度（例如，IP、国家/地区以及 TLS 模式）分析流量，进而根据每个应用程序的需求提供强有力的保护

先进架构，实现卓越防御
Behavioral DDoS Engine 通过一个复杂的架构运行，其中包括多个关键组件：

- **检测引擎**
  使用动态维度和历史攻击数据来实时识别 DDoS 攻击。
- **抵御引擎**
  使用来自基准生成器和威胁信号的情报来自动应对攻击，从而减少安全团队的运营开销。
- **误报减少**
  ML 模型可以过滤掉不相关的数据，从而确保使用干净的流量进行分析和抵御。
- **基准生成器**
  通过处理两周内的清理数据来不断完善流量分析，让引擎能够随时利用最新的攻击策略进行更新。
- **基准验证器**
  在 AI 的帮助下，这个至关重要的组件每个月都会评估数以百计的 DDoS 攻击以对解决方案进行微调。

此自动化框架可确保安全团队能够依靠该引擎动态调整防御措施，而无需人工干预。此解决方案会检测异常流量活动（例如，爬虫程序生成的流量或 DDoS 攻击尝试），并将其过滤掉以有效保护应用程序。

应用程序安全防护的准确性

如果应用程序安全解决方案（WAF 或 WAAP）无法做到准确防御，就需要投入更多内部资源来管理日益增加的每日告警。一旦出现偏差，还可能会带来大量误报（非恶意请求被标记为恶意请求的情况）和漏报（恶意请求被标记为非恶意请求的情况），使得企业不得不浪费宝贵的安全技能资源和时间来研究和分析这些类型的告警。

企业经常会面临告警疲劳的挑战，但由于控制措施过于宽泛，或者处理能力存在过度校正或校正不足的问题，导致他们始终无法找到相应的解决方案。这往往会导致企业无奈之下停用 WAF，更甚者，直接无视告警和版本更新。虽然这减轻了许多企业对意外拦截合法用户的担忧，但也相应地减少了能够抵御的 Web 攻击和 API 攻击。此外，很多企业还缺少精细的控制措施，无法在访问合法流量与精确地阻止恶意流量之间取得平衡。

有效 WAAP 解决方案的好处在于，它可以利用一组全面的 WAAP 控制措施和功能来同时减少误报与漏报，从而提高准确率并最大限度地减少对合法用户的影响。

了解准确性

准确性衡量的是 WAF 或 WAAP 在有效阻止攻击的同时，避免误拦截合法用户的能力。它会考虑以下四个变量：

- **真正例 (TP)：**被正确识别为存在恶意的真实攻击
- **假正例 (FP)：**被错误地识别为存在恶意的合法请求
- **真负例 (TN)：**传递给应用程序的合法请求
- **假负例 (FN)：**错误地传递给应用程序的真实攻击

Client Reputation 评分

Client Reputation 使用复杂的风险分析引擎，为尝试访问您网站的每个 IP 地址计算一组“风险评分”。它会分析传入 IP 地址并利用各种因素（例如攻击者持久性、目标应用程序的数量、攻击严重性、规模、行业以及先前针对客户应用程序的攻击）来确定一个分数，该分数说明了此 IP 地址参与 Web 攻击的可能性，包括：

- **DOSATCK**
  它使用僵尸网络来发动拒绝服务 (DoS) 攻击。DoS 攻击的目标是利用大量虚假请求对网站进行泛洪攻击，使网站变得异常缓慢，甚至发生崩溃。在分布式拒绝服务 (DDoS) 攻击中，这些请求来自于数千个位置（通常是被恶意软件感染的计算机或手机），因此无法仅通过拦截给定的 IP 地址来阻止该攻击。

- **SCANTL**
  扫描工具可以识别潜在的安全风险，例如 SQL 注入、跨站点请求伪造 (CSRF)、无效的重定向及其他漏洞。对您自己的网站运行 Web 扫描工具是一种良好做法。让犯罪分子对您的网站运行扫描工具并不是什么好事。

- **WEBATCK**
  使用 SQL 注入、远程文件包含或跨站点脚本编制等手段来执行安装恶意软件或窃取用户数据等操作。黑客或许能够检索您的所有用户数据，包括密码、信用卡号、社会保障号以及您可能已存储在用户数据库中的任何其他信息。

- **WEBSCRP**
  使用自动化工具下载网页的副本，然后“抓取”（即，复制）该页面上的所有内容。这些内容可能会被转用于非法或不道德的用途。

借助 Client Reputation，您可以根据来自 Akamai Connected Cloud 的累积威胁信息，主动保护自己的企业免受可疑威胁来源的侵扰。

恶意软件防护

攻击者会使用恶意软件作为一种常用的攻击手段。为了全面保护应用程序，Akamai 提供了抵御恶意软件的解决方案。所有规模的企业都允许上传文件以提高内部和外部的效率，包括以下常见用途：

- 求职简历
- 雇佣协议、入职培训、电子验证、直接存款设置等
- 申请，包括贷款、帐户设置和信贷申请
- 汽车、房屋等保险或维修估价
- 用于保险或患者帐户设置的医疗记录
- 包含图片的客户产品或体验评论

应用程序和 API 安全内的恶意软件防护用于在边缘检测和隔离恶意软件威胁，防止它们进入目标企业系统。通过为应用程序和 API 提供恶意软件防护，企业可以保护时间、预算和生产力，以及内部数据和客户数据：

- **在边缘检测并阻止恶意软件**
  避免在服务器上进行扫描所带来的风险，因为扫描时恶意软件可能早已传播开来。
- **避免复杂性并腾出时间**
  只扫描一次文件，而不是像使用 ICAP 和基于代理的扫描程序那样在每个系统中分别设置保护措施。
- **使安全态势满足发展需求**
  通过选择一种具有预防性的分层式方法，企业可以随着业务的增长扩展其保护范围，同时在边缘提供额外的保护并提供在源站进行再次扫描的选项。
- **为您的应用程序提供一致性**
  企业无需配置或更改应用程序代码。恶意软件防护完全托管在 Akamai Connected Cloud 上。

应用程序安全分析

App & API Protector 中包含 Akamai 备受客户青睐（以及使用最多）的产品：Web 安全分析。借助此 Akamai WAAP 解决方案，您可以在 Akamai 平台上捕获与您的 Web 应用程序和 API 发生相关的安全事件，并在所提供的安全分析工具中将其可视化。

Web 安全分析是现代网络安全的重要组成部分，让用户可以全面了解 Web 流量和潜在危险。通过分析大量数据点（包括流量模式、用户行为和安全事件），它可以让用户详细了解 Web 应用程序的安全态势。利用这种主动方法，企业可以更有效地检测和应对威胁，从而在风险造成重大损害之前消除风险。Web 安全分析不仅可以帮助识别恶意活动（例如，爬虫程序攻击、SQL 注入和跨站点脚本攻击），还可以帮助了解和解决 Web 应用程序中的漏洞。此外，它还可以通过生成报告来证明遵守安全策略和法规要求，从而为合规工作提供支持。

API 发现和分析

API 使企业能够创建强大的网络和移动体验，这通常是通过公开后端数据和逻辑来开发新产品及创新产品实现的。API 也会扩大攻击面。企业需要了解在其环境中有哪些 API 端点、API 的功能及其流量概况。Akama 的 API 发现和分析功能可以自动、持续地完成上述操作，还具备其他功能。

API 发现功能可发现企业中不同业务部门连接的新应用程序和 API（往往未受保护），并向安全团队发出告警。此自动化检测技术是 Akamai WAAP 解决方案的新功能，可以使开发团队、业务线负责人及安全团队保持一致。

Adaptive Security Engine 会基于考虑了响应内容类型、路径特征和流量模式的评分机制，每 24 小时自动执行一次 API 发现。这些发现数据包括所观察到的 API 规范的相关信息，其详细信息如下：

- 主机名
- 基本路径
- 资源路径
- 参数及其数据类型
- 方法
- API 的格式

基本路径和资源路径是根据算法确定的，该算法考虑了从具有 API 流量的特定主机名上观察到的流量的路径深度、子代数量以及同级项。在资源路径中，如果观察到某个特定方法的某个参数，则标记该参数并识别该参数的数据类型。

API 端点的流量概况包含的信息有助于了解 API 的用途和当前威胁级别。包含的一些数据点为：

- 自 API 首次被发现以来的总请求数，包括过去 24 小时内的请求数和随时间变化的趋势
- API 首次被发现和最后一次出现的日期
- 采用不同方法（如 GET、PUT、POST、DELETE 和 OPTIONS）的请求的数量
- 生成 2xx、3xx、4xx 和 5xx 响应的请求的数量
- 基于用户代理的终端客户端识别
- 响应错误数，例如导致客户端错误和服务器端错误的流量的百分比
- 来自已知攻击者的点击量（包括已知恶意攻击者向 Akamai 平台发起的流量占总流量的百分比），按网络攻击者、Web 扫描程序、内容抓取程序和 DoS 攻击者分类

当缺乏监测能力时，将很难为 API 提供保护。企业如何保护不在监测范围内的资产？在 Akamai 帮助下，企业可以自动、持续地发现和分析 API，包括它们的端点、定义以及资源和流量特征。一旦 API 被识别，Akamai 就会提供全面的保护，以便抵御 DoS 攻击、恶意注入、撞库攻击并防范违反 API 规范的行为。借助 Akamai 的云无关和源无关方法，可以轻松发现整个应用程序资产中的 API，而无需最终用户进行任何额外配置。有了这种监测能力，开发人员、应用程序所有者和安全团队便能抢先一步识别新的、未知的或不断变化的 API，并能轻松地将它们注册为防范对象。

爬虫程序监测和抵御

由于在网站流量中爬虫程序的占比超过五成，因此很难知道哪些爬虫程序在帮助贵企业实现目标、哪些爬虫程序有破坏企图。良性爬虫程序可以自动完成评估、对话或提供建议，从而提高企业的效率。恶意爬虫程序会堵塞流量路径，影响客户和操作体验，进而影响收入。在 App & API Protector 中，爬虫程序监测和抵御功能提供了强大的检测能力，能够发现良性爬虫程序并让它们通过，同时拦截恶意爬虫程序。这让企业能够：

- **发现爬虫程序并了解其影响**
  由于爬虫程序广泛用于搜索、检查网站性能以及与业务伙伴交互等操作，因此对于现代数字业务来说，爬虫程序流量监测能力至关重要。
- **提高运营控制能力**
  拦截恶意爬虫程序可以提高效率、降低业务和财务风险，并且可以更好地控制 IT 支出。
- **制定由数据驱动的、更好的决策**
  详尽的分析和报告可以帮助您对客户旅程、安全态势、风险承受能力和 IT 运营做出有创造性、有效的选择。

App & API Protector 固有的爬虫程序监测和抵御功能

对于可能会对网络资产的性能和安全产生不利影响的爬虫程序流量，App & API Protector 可以进行爬虫程序检测和控制。它提供监测能力，以主动监控随时间推移而出现的与爬虫程序相关的异常情况和威胁。

通过使用 App & API Protector 中提供的 Akamai 爬虫程序解决方案，您可以：

- 获取 Akamai 已知的 1,700 多个已定义爬虫程序的信息
- 对爬虫程序流量进行实时监测
- 创建自定义的爬虫程序定义
- 允许良性爬虫程序并拒绝恶意爬虫程序
- 查看爬虫程序监测和趋势报告

对于存在高级爬虫程序问题的网站，Akamai 提供了 Bot Manager，该产品具备高级爬虫程序防护功能，可增强电子商务和数字安全性。Bot Manager 针对持续的对抗性爬虫程序提供更精细的操作，例如用于以下攻击的爬虫程序：

- 撞库攻击
- 囤积库存
- 内容和价格抓取
- 业务逻辑滥用

主要的爬虫程序功能

Akamai 认识到通过 WAAP 进行爬虫程序管理的需求在不断变化，并改进了我们的爬虫程序监测和抵御工具，以包括新纳入的功能，例如：

- **浏览器仿冒检测**
  Akamai Bot Manager 中这项备受客户青睐的功能使用动态评分模型和 ML 来辨别和应对浏览器内的爬虫程序活动，并且该功能也在 App & API Protector 中提供。
- **条件响应操作**
  客户现在可以更好地了解浏览器内的爬虫程序活动，并且可通过条件操作做出响应，以对恶意爬虫程序应用不同的响应策略。
- **质询操作**
  通过各种不同的质询操作来应对爬虫程序，包括在未能解决时可以阻止爬虫程序访问相关内容的间隙质询。

超越 WAF：Akamai 解决方案带给您更多优势

Akamai 的 WAAP 策略带来了 App & API Protector 解决方案。但是，让我们的 WAAP 客户受益的产品不止一种。Akamai Connected Cloud 是在全球分布广泛的平台上构建的一款解决方案，并由数百位人类威胁研究专家提供支持。它可以提供出色的性能、可用性、情报、专业知识和切实有效的安全成果。

威胁情报与检测

完善的内部威胁情报功能可改善 WAAP 供应商应对不断变化威胁的能力。但是，所提供的情报的质量、时效性和可操作性将决定对应用程序安全防护效果的影响程度。Akamai 持续分析通过 Akamai Connected Cloud 获取的数据，以此识别威胁形势的当前趋势、首次发现的新攻击媒介以及当前活跃的攻击者。然后，Akamai 会通过多种方式将这些情报融入到我们的 WAAP 解决方案中。

本白皮书中先前介绍的 Akamai Adaptive Security Engine 会将两个层级的深度威胁情报相结合，以创建一个功能强大的专有引擎，为我们的客户自动管理最新的保护措施。除了 ML 和自动规则采用之外，Adaptive Security Engine 还可以提供来自 Akamai 全球化平台和庞大的威胁研究专家团队的威胁情报。

Akamai 平台情报

凭借全球领先的平台规模，Akamai 能够及时分析并防御针对所有客户的全球性攻击。我们的情报数据库平均每天提供 1,056 TB 的攻击数据。依托于 Akamai 对海量网络流量的监测能力，它能够从成千上万家大规模、高流量、且频繁遭受攻击的在线企业获取相关的高质量数据，供 Akamai 威胁研究团队进行分析：

- **WAAP 触发条件**
  直接从 Akamai 的全球 WAAP 部署中提取数据，并捕获针对每个 Akamai 安全客户的实际攻击事件。
- **CDN 日志**
  结合对来自每个 Akamai 客户（包括尚未部署 WAAP 解决方案的客户）的事件日志进行的离线分析。

Akamai 的情报数据库拥有全球最大的数据集之一 (9 PB)。对于高度重视业务和客户安全的企业而言，Akamai 凭借卓越的威胁情报成为其首选的 WAAP 解决方案提供商。

威胁研究和事件响应

为完善和扩大 WAAP 解决方案的攻击防御范围，许多威胁研究和事件响应企业都在其解决方案中提供了人工智能和分析功能。Akamai 拥有多个具有不同职责的团队，可以为我们的 WAAP 客户提供支持并识别可能需要额外保护措施的新攻击媒介。

威胁研究

Akamai 威胁研究团队会定期分析整个 Akamai 客户群所面临的 Web 攻击趋势，并按需求对各个客户提供自定义分析。该团队还负责设计和实施启发法来查询切实可行的情报，以便为核心 WAF 规则逻辑和 Client Reputation 的创建及更新提供支持。

事件响应

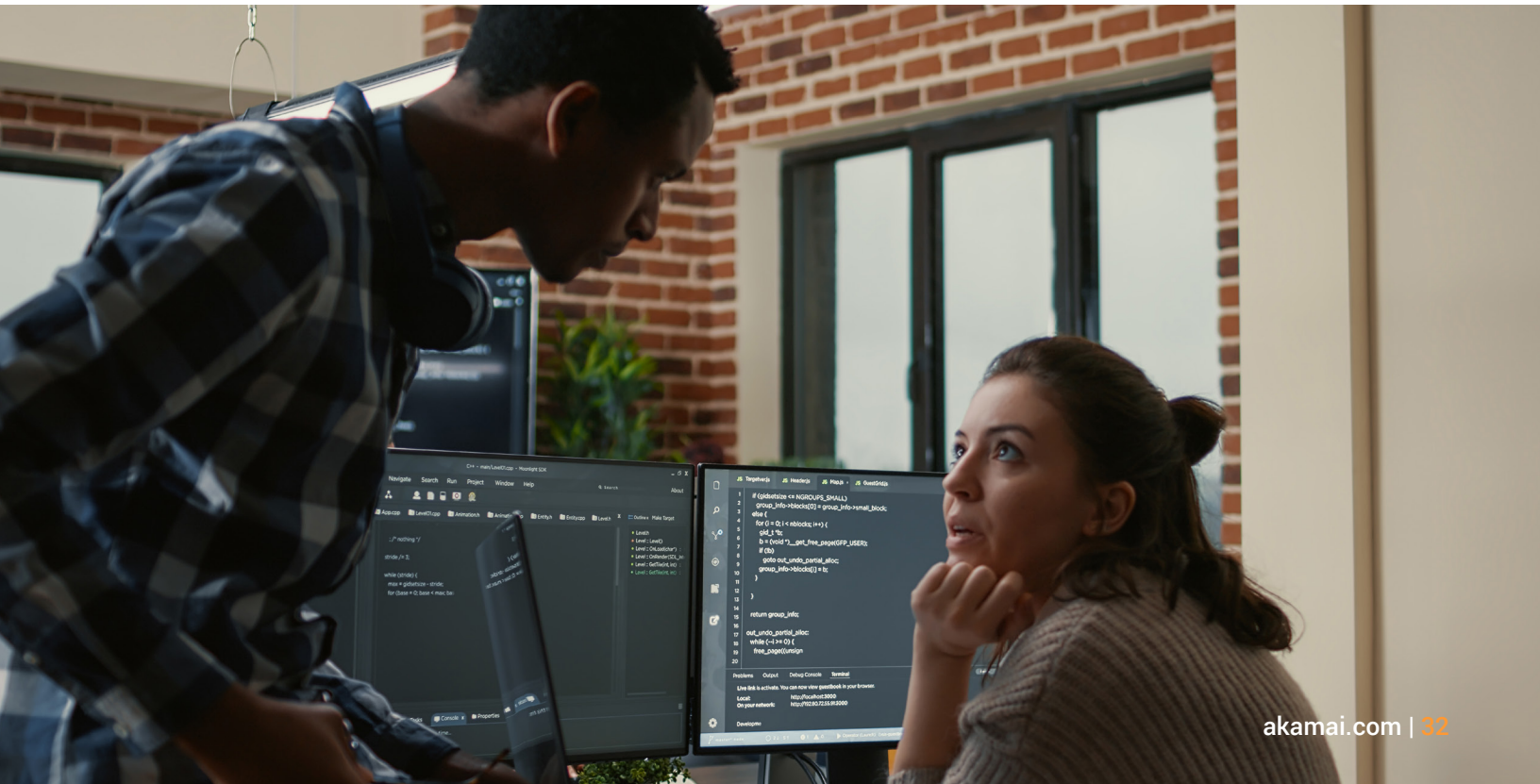
Akamai 旗下有两支事件响应团队，分别是计算机安全事件响应团队 (CSIRT) 和安全情报响应团队 (SIRT)，他们与 Akamai 全球安全运营中心 (SOC) 合作，在客户遭受攻击时向其提供分析和事件响应服务。此外，CSIRT 还主动监控经常遭受攻击的 Akamai 客户。这些客户来自各行各业，是预判新型攻击手段和趋势的“晴雨表”。

快速威胁检测

我们的新功能可以快速部署针对新兴威胁和知名 CVE 的防护措施。自动更新和“Akamai 托管”操作的方案意味着，您可以灵活地管理自己的防御措施。

CVE 保护

Akamai 威胁研究团队会持续监控常见漏洞和风险，并确保 WAAP 解决方案处于最新状态，能够保护客户应用程序并通过 Akamai CVE 查找工具提供必要的确认。此工具可通过提供有关 CVE 的详细信息（包括威胁级别和对 Akamai 当前保护措施的见解）来提供帮助。Akamai 的 CVE 防护目录为您提供监测能力，以便您可以根据 Akamai 的防护措施来确定安全工作的优先顺序，并且允许您搜索 CVE 数据库以确定 Akamai 针对漏洞采取的主动防护措施，还允许评估威胁程度并访问 CVE 详细信息。



全球化分布式边缘平台

可靠性和恢复能力

付费 WAAP 解决方案建立在广泛、强大的网络上，即使在最大规模的网络攻击中，这些网络也不会限制客户的正常流量。对于 WAAP 提供商的全球平台来说，经过验证的质量、容量和执行能力应与解决方案的功能同等重要。如果 WAAP 提供商未能在主动攻击期间无法提供正常流量，则客户应评估他们投资的是解决方案还是工具。

Akamai 致力于为客户提供行业领先的性能和保护。只有将服务建立在坚实的基础之上，才能完成这一使命：Akamai Connected Cloud。Akamai 构建了全球分布广泛的云平台，该平台由 130 多个国家/地区的 4,200 多个边缘入网点组成。

Akamai 的客户包括所有 10 大证券公司、所有 10 大银行、所有 10 大视频流媒体服务商和所有 10 大游戏公司。我们的客户群包括大多数顶级汽车公司、医疗保健提供商、零售商和电信运营商以及大量政府机构和军队。

这些客户相信 Akamai 能够为他们提供支持并保护他们免受每天 400 亿次爬虫程序攻击、每天 7.8 亿次应用程序攻击以及每季度 1,889 次 DDoS 攻击的威胁，避免他们的网络遭到破坏。Akamai 可以成功地提供安全保障，因为一个客户获得的威胁情报能够惠及每个客户，并为其提供保护。Akamai 全球化平台的规模可提供保护企业进入 AI 时代所需的数据量和数据质量。

覆盖全球

对于 WAF 来说，规模问题既涉及其检查所需 Web 流量（最初以及随时间推移而增加的流量）的能力，也涉及需要评估这些流量时所依据的 WAF 规则的数量。基于硬件的传统 WAF 解决方案通常存在规模性较差的问题，因为它们受限于设备内可用的 CPU 和内存资源，并且可能必须与同一设备上的其他解决方案进行竞争。

通过在整个 Akamai 云平台部署集成 WAAP 解决方案，可利用 Akamai 分布式服务器资源来检查传入 Web 流量，从而化解规模问题。用户和攻击者通过最近的 Akamai 服务器连接到受保护的网站，然后该服务器会检查流量中是否存在攻击，并阻止检测到的所有恶意请求。这使得 Akamai WAAP 解决方案能够随着 Web 应用程序流量的增长（包括流量的突然激增和长期增长）以及全球新用户位置的增加而无缝扩展。

性能

性能不佳可能会阻碍安全解决方案的部署，尤其是在应用程序之前以内联方式部署的 WAAP 解决方案。如果对业务至关重要的网站性能下降，则会导致生产力下降、用户体验不佳、上市速度放慢以及收入下降。

Akamai 云平台遍布全球，使得 WAAP 能够保护 Web 应用程序而不会降低性能。全球分布的 WAAP 会在 HTTP 流量首次进入该平台时对其进行检查，并在该平台的所有服务器上分配检查该流量所需的 CPU 和内存资源。这可以消除作为企业内部摩擦根源和部署障碍的性能问题。

边缘平台助力安全防护

Akamai 的云无关 Web 应用程序安全解决方案可在整个平台上无缝协作，以抵御各种应用程序和基于 API 的攻击。下图展示了 Akamai 的全套分层安全机制和控制措施，它能有效防御源站攻击，同时优化合法用户的访问速度和使用体验。

Akamai App & API Protector 提供自动内置的各种安全机制和控制措施（以蓝色表示），可实现开箱即用的全面防御体系，同时添加了其他 Akamai 产品和服务以提供完整的第 7 层保护

托管攻击支持

除了持续 WAAP 管理，Akamai 还向客户提供托管攻击支持，该支持服务可全天候监控受保护的网站并对检测到的任何攻击做出托管响应。

在安全事件发生时，托管攻击支持会通过 Akamai 全球 SOC 的工作人员按以下方式做出响应：

- 对 WAAP 告警和客户请求做出响应，并对问题进行进一步调查
- 确定相应的攻击特征，并部署额外的抵御措施
- 与客户应用程序团队合作，衡量已部署抵御措施的有效性和准确性，并根据需要调整抵御措施
- 在事件发生后，与客户应用程序团队一起审查整个响应过程
- 在界面中提供用于启动紧急支持请求的攻击告警按钮

安全运营指挥中心 (SOCC)

十多年来，Akamai 的 SOCC 帮助抵御了全球多次大规模的攻击，保护客户免受不断变化的全球威胁形势影响。

监控和抵御恶意攻击需要四项功能：

- 全球监测能力
- 主动监控和告警
- 灵活的攻击抵御
- 由经验丰富的安全团队提供持续的咨询服务

Akamai SOCC 凭借其全球领先的安全基础架构，为用户提供这些强大的安全功能。所有网络流量都会流过我们统一的安全平台，该平台会实时收集相关情报。例如，Akamai 收集了安全趋势，例如 SQL 注入攻击最近大量增加。

所有这些都可以帮助 Akamai 的安全团队以最有效且影响最小的方式迅速抵御客户面临的威胁。

结语

除了传统的网络层和应用层 DDoS 防护外，企业还需要采用全面的纵深防御策略，保护所有 Web 应用程序、API 端点、浏览器以及基础架构，以应对新型爬虫程序和通过 API 与客户端组件发起的定向攻击。安全负责人和从业人员需要利用 Web 应用程序安全解决方案来快速识别和抵御来自多种攻击媒介的威胁，并将传统安全防护扩展到防火墙之外，与相邻的安全技术协同工作，从而实现最佳安全防御效果。

Akamai 的 WAAP 策略具有出色的广度和有效性，为构建现代安全体系提供了一站式解决方案。我们认为，出色的安全解决方案不应该仅服务于全球知名品牌。为此，我们的应用程序和 API 防护产品组合采用分层机制，可让所有重视安全问题的企业有效确保 Web 应用程序的安全。

Akamai 依托持续演进的安全解决方案和深入全面的威胁情报，与全球企业通力合作，助力其实现安全能力现代化，并不断提升安全成效。我们致力于为您的安全团队提供强大的情报、全面的监测能力、高度的自动化以及专业的指导，助力您推动内部安全计划，并将威胁拒之企业系统之外。我们深知责任重大，并以提供全面防护为己任，也因此而备受那些为网络生活提供支持且要求严苛的品牌信赖。

Akamai 安全部门致力于为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2025 年 2 月。

扫码关注，获取最新云计算、云安全与CDN前沿资讯