Akamai

白皮书

精简 Web 应用程序安全策略

Web 应用程序攻击数量

现代 Web 应用程序变得日益复杂，特别是企业越来越多地采用基于微服务的架构，更是加剧了这一趋势。几乎每一次在线互动都严重依赖 API，这不但造成了当下的这种复杂局面，还可能为黑客提供新的切入点。与此同时，已知的 Web 漏洞仍然存在，并且反复被新一代的编码人员重新引入到应用程序中。为此，如今的攻击者也改变了攻击手段，他们使用爬虫程序、分布式拒绝服务 (DDoS) 租用和多媒介攻击，向 Web 应用程序、API 甚至客户端漏洞发起攻击。

然而，投机型攻击仍然是最常见的 Web 攻击形式 — 它们不会先把哪个企业当成攻击目标，而是先找到漏洞，然后对存在相关漏洞的企业发起攻击。扫描程序使用自动化的爬虫程序随机爬网，在数千个漏洞中寻找攻击的机会。一旦发现了一个漏洞，攻击者就可能使数据库泄密，将恶意文件加载到 Web 服务器上，或者通过海量突发流量攻击网站。

Web 攻击带来了哪些相关风险?

风险承受能力低的企业需要保持高度的安全防护，才能在内部（在系统、供应链、运营等之间）和外部（与合作伙伴、客户、管理机构等）建立起信任链。尤其是要注意保障 API 的安全，包括从微服务应用程序各部分之间的简单内部流动，到大型 B2B 交易，因为它们是连接各种系统和合作伙伴生态系统的数字化粘合剂，并为数字化和全渠道客户体验提供支持。

不幸的是，网络犯罪分子的 Web 攻击手段似乎用之不竭，这给企业造成了极大的损害。一次成功的黑客攻击可能导致敏感数据外泄，一次 DDoS 攻击可能让您的网站无法使用，这些攻击都会打破来之不易的信任，并造成客户忠诚度下降、监管罚款、法律诉讼和品牌声誉下降等重大损害。

Web 应用程序安全方面的挑战

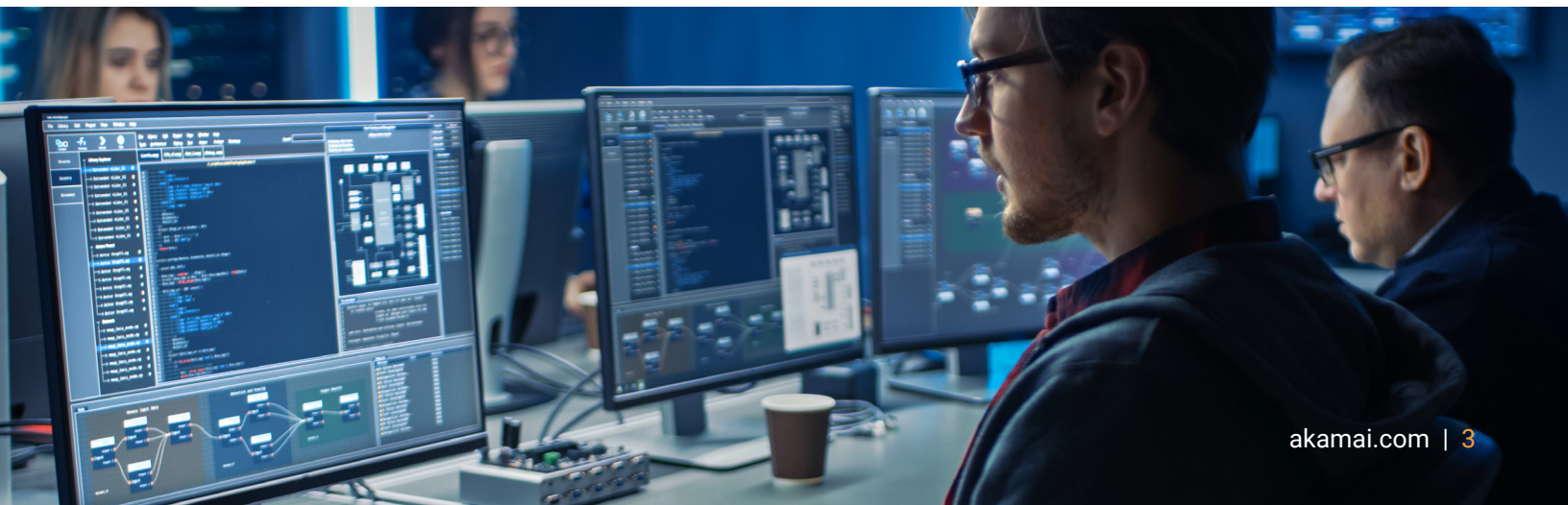
基于云的 Web 应用程序和 API 保护 (WAAP) 解决方案旨在抵御多种形式的 Web 应用程序攻击、DDoS 攻击和基于 API 的攻击。然而，防火墙面临一个主要的挑战：随着应用程序的变化以及各种更新的推出，威胁也在发展演进，因此应用程序安全团队必须不断分析和调整安全规则。配备经验丰富的安全专业人员仍是一项挑战，因为技术人员通常每两年调整一次职位。这通常是一个非常耗时的人工流程，需要熟练的操作人员，并且由于人员流动、学习生命周期和专门的技术集成架构，该流程对大多数企业而言无法扩展。

过时的安全策略可能变成企业挫败的来源，因为告警疲劳效应大大降低了准确区分误报和真实攻击的能力。如果安全团队无法有效调整规则，还可能会导致保护不力，并因担心影响合法用户和破坏业务而有意接受更高的风险态势。

为什么选择 Akamai WAAP?

Akamai App & API Protector 是一款基于云的 WAAP 解决方案，包含爬虫程序监测和抵御功能，可在减少工作量和开销的同时，保护您的大规模应用程序和 API 免受各种网络层和应用层的威胁。Akamai 的自助式初始配置向导减少了对先验知识的需求，为快速、轻松地保护您的资产提供了指导和见解。我们的自动设置过程将分析安全触发条件并学习应用程序的行为以自主调整保护措施，从而节省更多资源。App & API Protector 解决了当下许多防火墙问题，这些问题是导致企业内部矛盾、运营负担以及部署障碍的根源。

由 Akamai 完全托管的自动防护机制实施在我们全球分布广泛的平台上，使您能够采取免干预的方法来保护应用程序和 API 的安全。提供广泛的防御范围，自动抵御 SQL 注入、跨站点脚本攻击和本地文件包含等 Web 攻击，而且几乎不需要持续维护。通过应用机器学习和启发法，我们可以在逐个策略的基础上（而不是在整个网络范围内进行一般检查）提高对流量误报模式的识别，进而获得最相关和可行的结果。



通过使用我们的 CVE 查找工具，验证您的安全态势，该工具提供每个 CVE 的详细信息，包括威胁级别和有关 Akamai 当前保护措施的见解，可为您的内部安全和开发策略提供指导。此外，通过 Akamai 预构建的 SecDevOps 集成（包括 Akamai 代码、API、CLI、Terraform 和集成），可提高内部一致性并加快产品上市速度。

通过自适应保护措施，提高安全水平

那么，Akamai App & API Protector 是如何做到既简单又准确的呢？首先，App & API Protector 核心技术 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。该技术通过分析所有异常或可疑数据点并为每个请求分配一个威胁评分，简化了安全运营。威胁得分越高，保护措施就越有力。之后，我们可以根据检测到的威胁水平动态修改保护措施，利用此举甚至可以发现那些规避性很强的攻击，同时保持尽可能低的误报率。

应用程序攻击通常涉及某种形式的侦察，但在攻击者对漏洞进行扫描时，Akamai 也可以搜集到与其技术和战术有关的证据。这不仅使快速识别这些攻击者成为可能，而且当攻击者再次出现时，您还能有迹可循。攻击者尝试的次数越多，您的保护措施就越强。

Akamai 可分析并了解：

超过 7.8 亿次
的每日 Web 应用程序攻击告警

260 多亿次
爬虫程序请求

932+ TB
每日数据查询量

众包的威胁情报

互联网上许多遭受大量攻击的网站后来都成了 Akamai 的客户，包括前 10 大零售公司中的 9 家、前 10 大银行，前 10 大医疗保健公司中的 9 家，以及美国所有的 6 个军种等。我们可以监测每天超过 7.8 亿次 Web 应用程序攻击以及 260 亿次爬虫程序请求。Akamai 有数百名专业威胁研究人员和数据科学家，他们每天会查询超过 932 TB 的新数据，从中寻找可能的威胁。这种水平的全球洞察力，加上高级机器学习和人工分析，使我们能够主动和预测性地阻止常见和高度复杂的攻击。

十多年来，Akamai 致力于抵御应用程序攻击，即使客户面临一些大规模的攻击，也能出色保护其安全，并确保基础架构的正常运行。我们一直坚持调查和报告不断涌现的新兴威胁，随着攻击模式的发展演变以及攻击规模和复杂程度的提升，我们会继续创新和调整我们的解决方案，以在面对恶意攻击者时保持领先优势。由于 App & API Protector 建立在 Akamai 平台上，并内置了可提升性能的功能，可确保您的网站、Web 应用程序和 API 高效运行。

通过使用此免费试用版，了解您的 Web 应用程序和 API 保护需求，并体验 App & API Protector 的优势。