WEB 应用程序和 API 保护功能：

金融机构检查清单

应用程序编程接口 (API) 有着巨大的潜力和能力，能够支持各类设备、应用程序和数据之间的互连，是不断增长的内部和外部银行策略及活动的技术基础。它们带来了提高开放性、增强竞争力的承诺，可让客户从中受益。但金融服务业对 API 的快速采用也扩大了攻击面，并带来了新的安全风险。

在规划、实施或优化信息安全策略的同时嵌入 Web 应用程序和 API 安全解决方案，您的企业就能获得理解独有风险、识别安全漏洞和检测威胁的强大能力。为了保持竞争力，金融机构需要的是这样一种 Web 应用程序和 API 保护 (WAAP) 解决方案——能够提供持续的监测能力和综合全面的见解，还具有识别和阻止大部分复杂攻击的全面能力。

这份检查清单可用于评估供应商能力，也可以用作一份需求核查列表，用来确定实施有效的 WAAP 解决方案时需要满足的要求。

01. 平台要求

02. 自适应 Web 应用程序和 DDoS 防护

03. API 监测能力、保护和控制

04. 灵活管理

01 平台要求

- 具备与流量需求匹配的可扩展性，提供持续保护并且不会导致性能下降
- 架构能够应对跨地域分布式应用程序带来的挑战
- 具备审核日志功能，以确保合理使用
- 保护本地、私有云或公共云（包括多云或混合云）源站
- 能够抵御网络层 [L3/4] 分布式拒绝服务 (DDoS) 攻击，并且提供零秒服务等级协议
- 在整个平台中融入通过众包模式获得的攻击情报，支持发现攻击者、攻击频率和攻击严重程度
- 通过端口 80 和 443 提供 Web 流量反向代理功能
- 利用 SSL/TLS 加密保护网络隐私
- 根据公正的第三方的评估结果，在至少 5 年内是相应解决方案类别中经过证实的领导者
- 能够自动发现在何时何处发生了个人身份信息 (PII) 传递行为，并发出警报，以防范数据泄露

金融机构有责任保护敏感的客户数据和金融数据，避开快速发展变化的安全威胁。为此，您的 Web 应用程序安全解决方案应该灵活、可扩展，并且易于管理。

自适应 WEB 应用程序和 DDoS 防护

02

Web 应用程序安全机制必须超越基于签名的传统检测，采用更高级的自适应 Web 应用程序和 DDoS 防护，以实现最为精准和可靠的安全效果。

- 提供基于异常和风险的评分功能，而不仅限于基于签名的攻击检测
- 完全托管式 WAF 规则，无需持续配置和更新
- 提供针对个人和共享 IP 地址的客户端声誉评分和情报
- 具备机器学习、数据挖掘和启发法驱动的检测能力，从而识别快速不断变化的威胁
- 自动 Web 应用程序防火墙 (WAF) 规则能够根据安全研究人员持续发布的实时威胁情报更新
- 支持测试新的或更新的 WAF 规则在处理实时流量方面的效果，然后再将这些规则部署到生产环境
- （至少）抵御 SQL 注入、XSS、文件包含、命令注入、SSRF、SSI 和 XXE 攻击
- 提供可全面自定义的预定义规则，以满足特定客户需求
- 能够抵御应用程序层 [L7] 容量耗尽 DoS 攻击，这种类型的攻击会通过递归式应用程序活动造成 Web 服务器不堪重负
- 提供能快速抵御特定流量模式的自定义规则（虚拟修补）
- 具备请求速率限制功能，能够抵御自动化或过多的爬虫程序流量
- 能够抵御指向源站的攻击
- 通过多个网络列表实施 IP/地域控制，阻止或允许来自特定 IP、子网或地理区域的流量
- 抵御自动化客户端（例如漏洞扫描和 Web 攻击工具）发起的攻击

03

API 监测能力、保护和控制

- 自动发现和分析未知和/或不断变化的 API（包括 API 端点、特征和定义）
- 支持自动检查 XML 和 JSON 请求，从而检测基于 API 的攻击
- 提供基于 API 密钥的 API 端点速率控制（节流功能）
- 支持基于 IP/地域的 API 网络列表（允许列表/拦截列表）
- 带有版本控制的 API 生命周期管理
- 支持自定义 API 检查规则，以满足特定用户需求
- 通过 JSON Web 令牌 (JWT) 验证来保护身份验证和授权
- 能够预定义可接受的 XML 和 JSON 对象格式，以限制 API 请求的大小、类型和深度
- 为 API 后端基础架构提供防护机制，抵御专为耗尽资源而发起的低速缓慢攻击（例如慢速 Post、慢速 Get）
- 支持按密钥（每个独立定义的密钥具有相应配额）定义允许的 API 请求，从而全面掌控用量
- 使用标准 API 定义（Swagger/OAS 和 RAML）进行 API 初始配置
- 可在 API 级别生成实时警报、报告和仪表板

API 防护已经成为 Web 应用程序安全的关键部分。您需要具备稳健的 API 发现、防护和控制能力的 WAAP 解决方案，它应该能消除 API 漏洞，减少您面对风险时受到的攻击面。

灵活管理

04

- 支持开放式 API 和 CLI，可将安全配置任务集成到 CI/CD 流程中
- 包含实时仪表板、报告和启发法驱动的警报功能
- 集成本地和基于云的安全信息以及事件管理 (SIEM) 应用程序
- 具备能访问详细攻击遥测数据并分析安全事件的集中式用户界面 (UI)
- 提供完整的暂存环境和实施变更控制的能力
- 具备能自动适应流量的自行调整式安全防护
- 提供涵盖安全管理、监控和威胁抵御的全托管式安全服务，以减轻您的负担或增强安全性

您需要简单且自动化的工作流程来尽可能提升投资价值并提高运营效率。无论是保护全新应用程序、更改应用程序、采用新的 WAF 规则，还是将保护延伸到 API，所采用的流程都必须无缝且直观。

Akamai 为全球领先的金融机构提供 Web 应用程序和 API 保护。我们的全球安全研究团队每天从数百万次 Web 应用程序攻击、数十亿次爬虫程序请求和多达数万亿次的 API 请求中获取见解。这种程度的见解辅以先进的机器学习和威胁研究，让我们可以不断提升能力、捕获新型威胁，并开发创新功能。

Akamai 的 Web 应用程序和 API 安全解决方案为您的金融机构提供安心保护，帮助抵御更高级的 Web 应用程序攻击、DDoS 攻击和基于 API 的攻击。敬请访问我们的安全中心，随时了解我们的最新研究资讯。

Akamai

Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。我们横跨云端和边缘的计算平台在全球广泛分布，不仅能让客户轻松开发和运行应用程序，而且还能让体验更贴近用户，帮助用户远离威胁。如需详细了解 Akamai 的安全、计算及交付解决方案，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。

扫码关注，获取最新CDN前沿资讯