
Akamai
浏览器内保护的
7 个误区

互联网使得面向 Web 的应用程序和资产暴露在各种复杂的网络攻击之下，这已经不是什么秘密了。企业明显侧重于保护他们的关键任务应用程序免受服务器端攻击，但是，许多企业低估了浏览器或网页本身存在的客户端威胁可能造成的损害。这种盲点使网站容易受到危险的客户端漏洞影响，可能导致出现欺诈、敏感数据渗漏，以及对客户信任造成破坏。

我们来详细分析与浏览器内保护有关的一些常见误解，以便更清楚地了解真正面临的风险。

误区 1

内容安全策略 (CSP) 是非常有效的客户端防御措施

内容安全策略是一项安全标准，它允许网站运营商细化控制可以在浏览器中执行的资产（包括脚本）。内容安全策略响应标头用于维护一个许可的域列表，其中包含的域被视为合法和安全的可执行代码来源。它们可以成为您的防御措施的关键组成部分，以帮助您抵御 JavaScript 威胁，但它们需要大量的资源来进行维护。而且，大多数客户端攻击都是在使用受信任的来源时发生的。所以，您必须要了解您的网站上运行的所有脚本的行为，即使是受信任的脚本，也是如此。Akamai Page Integrity Manager 利用行为技术来监测网页上的所有脚本执行行为，从而收集情报，帮助您了解脚本操作及其与其他脚本的关系。然后，它通过多层检测方法（包括启发法、风险评分、人工智能，等等）来分析这些数据，以立即识别可疑活动。

目前，94%
的网站至少使用了一个
第三方脚本

资料来源：第三方，2021 年 11 月

误区 2

WAF 保护我的企业免受 Web 数据窃取攻击

Web 应用程序防火墙（WAF）是一种安全解决方案，它通过监控和过滤流量，阻止恶意流量进入 Web 应用程序或阻止未经授权的数据离开应用程序，从而保护 Web 应用程序免受常见攻击。WAF 侧重于保护您的服务器和最终用户之间的连接，但并非设计为可在浏览器层面保护您的 Web 应用程序。由于是在最终用户的浏览器中通过执行恶意代码来开展 Web 数据窃取攻击，因此，WAF 既无法检测这种攻击，也无法抵御。

误区 3

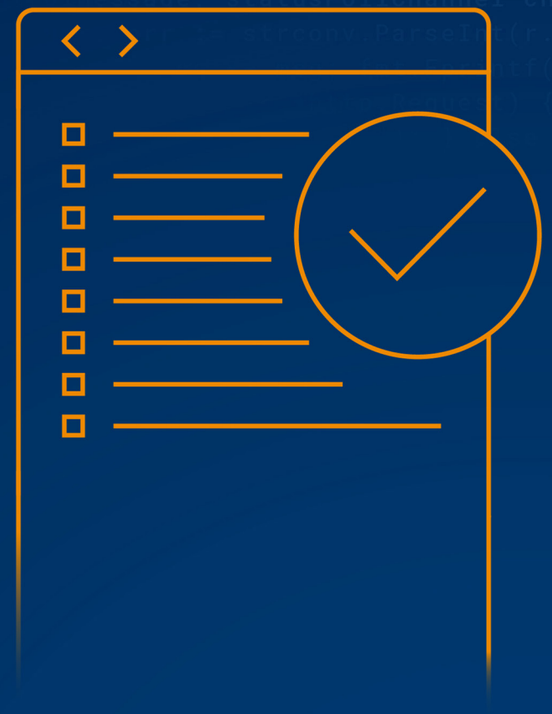
如今的 Magecart 攻击并不像过去那样频繁发生

Magecart 攻击比以往任何时候都更加活跃，而且人们越来越难对其进行检测。最近，我们的 Akamai 威胁研究团队发现了一项针对多个电子商务网站开展的全球 Magecart 攻击活动。该活动采用了复杂的技术，比如冒充 Google Tag Manager 等知名第三方供应商，或使用 Base64 编码来对恶意代码进行伪装。这是一场猫捉老鼠的游戏，攻击者试图绕过安全措施，在执行 Web 数据窃取攻击时采取更加聪明的做法，以便规避检测。Akamai Page Integrity Manager 可监测脚本的所有行为（包括它们与其他脚本交互的方式），以揭示任何可疑的活动，并迅速抵御高级攻击。在我们最近的博文中了解更多信息。

误区 4

我可以慢慢配合遵守 PCI DSS v4.0 的新脚本要求

2022 年 3 月，最新版本的 PCI DSS (v4.0) 发布，以应对支付卡数据面临的、不断变化的威胁，以及自 2018 年发布 PCI DSS v3.2.1 以来发生的一些重要市场变化。根据新增的要求 6.4.3 和 11.6，任何在线处理支付卡的企业现在必须了解他们的网站上运行了哪些脚本、这些脚本何时发生变化以及每个脚本何时停止运行，这样才能防御浏览器内脚本攻击。尽管 PCI DSS v4.0 要到 2025 年才生效，但您必须立刻开始保护敏感的支付卡数据，以免攻击者从网站的支付页面中窃取和渗漏这些数据，此举不容推迟。Akamai Page Integrity Manager 可以立即帮助您加快实现 PCI 合规性。



误区 5

受众劫持对在线零售商来说不是一项重大挑战

“受众劫持”是一个术语，描述的是由于客户端安装了浏览器扩展程序或插件而发生的不需要的（有时是恶意的）浏览器活动。这些不需要的活动可能包括联盟欺诈、未经授权重定向到竞争对手网站或恶意网站、非有意的折扣，以及分散注意力的广告注入（可能会阻止访问者完成购买）。企业估计，其网站的总访问量中有 15%-24% 受到了受众劫持手段的影响。

这意味着什么？转化率和品牌忠诚度降低，以及数百万的潜在收入损失。借助 Akamai Audience Hijacking Protector，用户能够了解常见浏览器扩展程序如何影响网站会话，以及扩展程序运营者如何进行恶意活动。它使您能够决定允许哪些扩展程序与您的网站进行交互，同时在单个扩展程序层面使用细化的策略设置来阻止或允许活动。

企业估计，其网站的
总访问量中有

15%-24%

受到了受众劫持手段的影响

资料来源：在线零售商对于受众劫持的了解，Retail Dive，2023 年 2 月

误区 6

数字化体验平台可以监测浏览器内活动和浏览器扩展程序的影响

数字化体验平台由一组技术构成，这些技术通过协同运行来优化和交付内容驱动的体验。目前，这些平台提供的分析只针对网站会话中企业一端发生的情况提供见解，而无法针对最终用户提供见解。这意味着，虽然您可以跟踪网站访问者与您的网站的交互方式以及他们的行为，但您无法了解浏览器与最终用户的交互方式。在了解浏览器扩展程序和不必要的浏览器活动如何影响您的网站会话后，您就可以全面了解整个客户历程，并可以更好地找出客户放弃购买交易的原因。

误区 7

优惠券和价格比较扩展程序对我的业务没有损害

这很复杂，我们都明白。每个人都希望达成出色的交易，Honey、Rakuten 和 Amazon Assistant 等扩展程序可以帮助在线零售商提高转化率。但是，这些扩展程序可能具有更黑暗的一面。以优惠券扩展程序为例，它自动将专属优惠代码插入您的目标受众之外的用户的结账页面，造成大规模的折扣。Amazon Assistant 也存在类似的问题，它会在您的网站上自动注入一个广告，表明竞争对手能够以更低的价格提供与您相同的产品或服务。这些扩展程序会导致巨大的潜在收入损失，并使您最忠实的客户离您而去。Akamai Audience Hijacking Protector 支持数十个全球热门的浏览器扩展程序，我们的高级仪表板可在单个扩展程序层面提供见解，使得用户可以分析哪些扩展程序实际上对企业有利，以及哪些扩展程序不值得一用。

在 Akamai 客户的全球网站流量中，受优惠券和价格比较扩展程序影响的网站会话数量在黑色星期五和网络星期一之间增加了

25%

资料来源：Akamai 威胁研究，2022 年

Akamai 如何为您提供帮助

很明显，企业受到客户端攻击影响的风险正在加剧，要降低风险，他们就必须能够监测浏览器内的行为和不必要的活动。Akamai 的 Page Integrity Manager 可以识别有漏洞的资源，检测可疑行为以及阻止恶意活动，从而帮助网站抵御 JavaScript 威胁（例如 Web 窃取、表单劫持和 Magecart 攻击）。为了阻止不必要的浏览器内行为，Audience Hijacking Protector 提供了精细的分析和抵御选项，帮您实时监测电商网站上发生的浏览器活动

了解 Akamai 的应用程序和 API 防御措施以及浏览器内保护解决方案如何帮助您改善客户端安全状况。