

白皮书

事半功倍

具有成本效益的应用安全防护和性能提升策略——
七家公司的成功案例。



目录

- 3 内容摘要
 - 4 当安全和 IT 团队需要用更少的资源完成更多工作时
 - 5 削减应用程序安全实践成本的方法
 - 6 通过整合安全供应商降低成本
 - 7 通过自动证书管理优化劳动力和基础设施成本
 - 8 阻止推高流量成本的攻击
 - 9 消除意外费用和成本, 例如带宽、云和出口费用
 - 10 使用 Cloudflare 优化应用安全并降低成本
- 

内容摘要

大多数 IT 架构要么过于复杂, 要么已经过时, 无法对所有 Web 应用实施一致的安全保护。安全团队被迫手动将孤立的工具拼凑起来, 因而对云、混合和本地环境的可见性和精确控制有限, 拖慢业务的速度。

所有这些复杂性导致团队不堪重负, 漏洞不断扩大, 攻击更具破坏性, 而且仅仅为跟上昨天的威胁而投入的资源水平就已经难以为继。

保护 Web 应用和 API 免受恶意机器人、DDoS 攻击、代码注入和其他漏洞的威胁是组织的一项关键任务。然而, 实施强大的安全策略并非易事, 尤其是在预算有限和团队增长受制的情况下。

本文分享了一些公司成功在其安全策略中创造效益并降低成本的真实案例。通过这些成功案例中学习, 企业可以获得有关如何使用应用程序安全实践来优化开支的宝贵见解。

当安全和 IT 团队需要用更少的资源完成更多工作时

当组织面临预算限制时，没有任何团队能完全免受影响。无论是由于普遍的经济不确定性、销售下滑、企业重组还是其他各种原因，安全和 IT 团队经常被迫在没有期望预算增长的情况下改进运营，甚至更糟的是——在削减成本的同时这样做。

但是，应用安全和性能不是允许结果下降的领域。在安全方面，保护应用的工作越来越复杂。[攻击变得比以往任何时候更大、更复杂](#)，而且随着组织规模扩大，其攻击受面也变得更大。例如，2022-2023 年披露的 CVE 漏洞数量[增加了 15%](#)。尽管在[2023 年披露了超过 5000 个关键漏洞](#)，针对高危 Web 应用漏洞发布补丁的平均时间仍然保持在[35 天](#)左右，这意味着应用在此期间得不到保护。

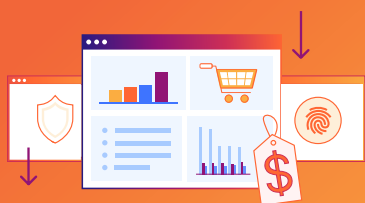
在性能方面，消费者希望每一次数字体验都是快速、可靠和个性化的。即使速度略有减慢，都有可能对用户参与度和转化率产生重大影响，如果公司无法满足客户的期望，就会陷入困境。

当面临预算限制和期望不断上升的双重压力时，安全和 IT 团队需要找到用更少的资源实现更多成果的方法。本文介绍的案例中，一些公司成功建立了具有成本效益的安全和性能实践，而且不牺牲结果。



削减应用安全和性能 实践成本的方法

就保护 Web 应用和 API 免受现代威胁而言，最佳的策略不仅提供分层安全服务，还允许组织裁减不必要的开支。为了实现这一目标，组织可以采用几种关键策略，包括供应商整合、优化证书管理、专门防护推高流量成本的攻击以及降低出口流量费用。



通过整合安全供应商降低成本



通过自动证书管理优化劳动力和
基础设施成本



阻止推高流量成本的攻击



消除意外费用和成本，例如带宽、
云和出口费用

通过整合安全供应商降低成本

[Gartner](#)最近进行的一项调查显示,有75%的公司正在探索整合其安全实践中的供应商。通过[减少所依赖的供应商数量](#),组织可以优化供应链流程并实现更高效益,从而降低成本。

Chrono24 是一个领先的奢侈手表在线市场,通过[使用 Cloudflare 整合](#)减少了对多个供应商的依赖。

在转换之前,Chrono24 使用 EdgeCast 的 CDN 解决方案以及来自另外几家供应商的 DDoS 缓解和 WAF。这些拼凑在一起的解决方案表现不佳,导致严重延迟和糟糕的性能,并浪费了供应商支出。

在整合到 Cloudflare 的解决方案(包括 CDN、WAF 和 DDoS 缓解)后,Chrono24 的网站安全和性能成本降低了 67%。

技术总监 Sven Ferber 表示:“将性能和安全整合到一家供应商后,我们的基础成本现在已大幅减少。我估计现在的开支只有原来的三分之一。”

对于企业优化采购和管理开支,供应商整合是一种高度有效的策略。如下在寻求整合供应商时可以使用的三个快速问题:

1. 您的供应商是否提供威胁保护并改善应用性能?
2. 您能否从一个控制台管理您的应用和 API?
3. 贵组织的多个团队是否可以利用同一供应商以实现预算效益?

通过遵循上述整合提示,组织可以降低成本,简化供应链管理,并加强与重要供应商的关系。



要点

75% 的公司正在探索
供应商整合

与 Cloudflare 整合后,
Chrono24 将网站安全和
IT 成本降低了 67%

通过减少供应商数量和整合
服务,公司可以**降低成本**
并简化供应链管理



通过自动证书管理优化劳动力和基础设施成本

对于 IT 团队来说，跨多个域和地区部署安全配置可能是一个昂贵且耗时的过程。而且隐藏成本会为他们支持的组织带来额外的麻烦，特别是那些面临预算限制的组织。

通常，这些隐藏成本会被证书管理所掩盖。SSL/TLS 证书构成一个网络的数字身份。平均而言，一个企业的 Web 服务可能需要数百甚至数千张证书。但是，管理这些证书所需的劳动力和基础设施开支加起来可能非常高昂，更不用提由于意外证书中断可能导致的收入损失了。

电子商务平台 SHOPYY 使用 [Cloudflare 自动化 SSL 证书的管理](#)，包括私钥创建、保护、域验证、颁发、更新和重新颁发。

最初，SHOPYY 使用一个免费的证书管理工具，该工具提供的证书不可靠且有效期短。因此，SHOPYY 不得不雇佣额外的员工来监督证书管理和更新过程。

通过 Cloudflare SSL for SaaS，SHOPYY 将证书管理流程委托给 Cloudflare，只需要一位内部员工来维护整个过程。

创始人兼首席技术官 Yuanming Chen 表示：“**仅在运营和维护方面，使用 Cloudflare 产品就已经削减了 60% 的成本。**”

低效的证书管理实践也会因证书过期而影响收入。在线借贷市场平台 LendingTree 使用 [Cloudflare 的 TLS 证书来节省成本并防止停机。](#)

应用安全负责人 John Turner 说：“我们有数千个不同的资产。在这种规模下，我们错过更新证书只是时间问题。使用 Cloudflare 可自动更新的 TLS 证书，我们每年节省大约 5 万美元，包括行政成本和因证书过期所致停机带来的收入损失。”

建立有效的证书管理系统还有助于适当地重新分配资源。成立于德国的 [自动化云应用部署平台](#) mogenius 使用 Cloudflare 自动化其证书管理实践，使该公司有更多时间开发核心业务。

联合创始人兼 CPO Jan Lepsky 表示：“如果 Cloudflare 为我们所做的一切都在内部管理，将占用我们至少 20% 的时间。**借助 Cloudflare，我们可以专注于为客户优化云开发和部署流水线。**”

对于想要避免隐藏成本并确保业务顺畅运作的企业来说，外包证书管理至关重要。低效、手工或拼凑的证书管理实践会导致高昂的人力和基础设施费用、证书过期造成的收入损失和浪费的资源配置。

通过实施具备 SSL for SaaS 或 TLS 证书等功能的证书管理，企业可以节省大量成本并改善其收入。



要点

采用 Cloudflare SSL for SaaS 后，SHOPYY 将运营和维护成本降低了 60%

Cloudflare TLS 帮助 LendingTree 每年节省行政成本和挽回收入损失 5 万美元

Cloudflare 使 mogenius 能够自动化其证书管理工作，释放出 20% 的时间来专注于核心业务

阻止推高流量成本的攻击

API 使用增长的同时，攻击面随之扩大。恶意机器人、DDoS 攻击和其他威胁会危及应用程序和 API，高管和技术领导者特别清楚这些攻击对其业务可能产生的重大影响。

据估计，API 安全问题给企业造成**每年高达 750 亿美元**的损失。

这些攻击会导致凭据填充和 DDoS 攻击，不仅会中断对合法用户的服务，还会迫使组织承担攻击所致流量激增的成本。

LendingTree 曾经合作的一家安全供应商在 DDoS 攻击期间收取激增费用，LendingTree 为此花费了大量金钱。这种模式不仅产生了庞大的超额成本，而且最终还会阻塞合法流量。

应用安全负责人 John Turner 回忆说：“每当我们推出新的电视广告或社交媒体广告活动时，请求量就会超过供应商要我们指定的任意限制，这意味着供应商会将其解释为 DDoS 攻击并阻止合法流量。我们不仅失去了那些潜在客户，还浪费了将他们引导到我们网站所花费的成本，而且供应商会向我们开具‘DDoS 保护’账单。”

为了解决这些低效问题，LendingTree 转用了 Cloudflare 的机器人管理和速率限制功能。在 48 个小时内，对特定 API 端点的攻击减少了 70%，不到五个月的时间里，LendingTree 通过阻止 API 端点滥用节省了 25 万美元。

当在线游戏公司 Flutter Entertainment 意识到他们的流量中几乎有 70-90% 是恶意流量时，他们需要一个解决方案来过滤和阻止恶意机器人。实施 Cloudflare 机器人管理后，Flutter Entertainment **将恶意流量降低了 90%，每年节省超过 200 万英镑**。

使用机器人管理和 DDoS 保护，组织可以预防攻击和 API 滥用，并减少攻击相关支出。在考察安全供应商时，组织应该寻找提供以下功能的供应商：

- 使用机器学习根据观察到的流量数据设置速率限制
- 超越基于地理位置和 IP 位置的速率限制，因为现代攻击可以轻松绕过 IP 限制
- 确保开发人员通过 Web 应用程序防火墙 (WAF) 和 API 网关路由所有 Web 应用程序和公共 API 流量
- 整合 DDoS、WAF 和 API 网关工具，以实现更多分层的威胁防御
- 确保在企业服务其流量的位置部署保护措施，以降低延迟
- 提供不计量的 DDoS 缓解服务，免除超额费用

实施正确的供应商/安全策略可以帮助组织每年节省成千上万，甚至数百万美元的费用。

Flutter™

要点

API 不安全性**每年给企业带来高达 750 亿美元的损失**

实施正确的供应商/安全策略可以帮助组织**每年节省成千上万，甚至数百万美元的费用**

使用 DDoS 保护后，LendingTree 在 48 小时内看到对特定 API 的攻击下降了 70%，并在不到五个月的时间里通过阻止攻击节省了 25 万美元

Cloudflare 机器人管理帮助 Flutter 将其恶意流量降低了 90%，每年节省超过 200 万英镑

消除意外费用和成本, 例如带宽、云和出口费用

许多安全服务依赖于云, 而许多云服务提供商会向企业收取存储和计算费用。此外, 这些服务提供商通常要求企业支付数据出口费用, 即从存储中传输数据的相关费用。

数据出口费用根据多种因素进行计算, 例如客户级别、订阅类型和传输的数据量。因此, 这些费用往往很难预测, 累加起来时会给组织造成不利影响。事实上, IDC [估计数据出口费用占云存储成本的至少 6%](#)。

有鉴于此, 欧洲数字目录和本地搜索服务 PagesJaunes [决定实施 Cloudflare CDN, 以帮助削减带宽费用](#)并改善其缓存和 DNS 管理。

架构、性能和安全负责人 Loïc Troquet 坚称: “我们很快注意到, 由 Cloudflare CDN 吸收的流量意味着我们的基础设施压力更小, 更具韧性。**70% 的带宽不再需要由 Solocal 的基础设施服务。**”

而且带宽节省意味着成本节约。在采用 Cloudflare 的 CDN、DNS、WAF 和 DDoS 缓解服务后, 在线学习和学习工具 Quizlet [每天节省超过 10 TB 的总带宽](#), 并将 Google Cloud Services 的网络出口账单削减了 50% 以上。

实施应用安全策略和实践可以消除意外的数据出口费用。



PagesJaunes

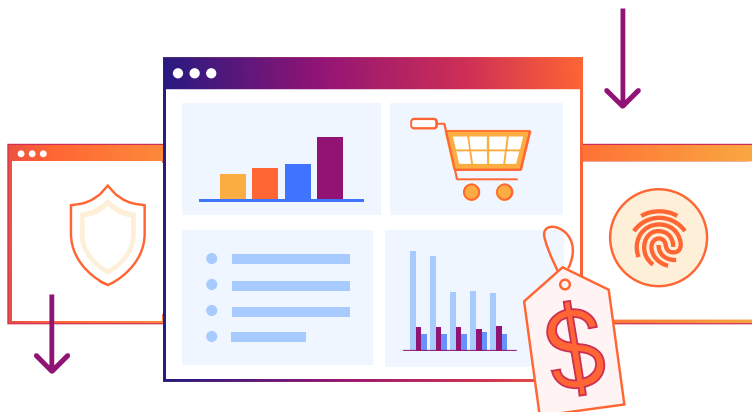
Quizlet

要点

实施应用安全策略, 例如选择正确的 CDN 供应商, 可以消除意外的数据出口费用

通过使用 Cloudflare CDN, PagesJaunes 将其带宽减少了 70%

Quizlet 使用 Cloudflare **每天节省超过 10 TB 的总带宽**, 并将 Google Cloud Services 的网络出口账单削减了 50% 以上, 每月节省数千美元



使用 Cloudflare 优化应用安全并降低成本

通过 Cloudflare, 组织可以构建应用安全策略, 以提高效益并优化开支。Cloudflare 的集成应用安全服务组合汇集了一流的不计量 DDoS 保护、可阻止最高级攻击的 Web 应用防火墙、主动 API 安全、由威胁情报驱动的机器人管理和高级客户端攻击检测。

是否感兴趣?

[立即联系 Cloudflare](#)

