Enterprise Strategy Group | 了解更重要的事实。™

ESG 白皮书

使用 WAAP 应对保护现代 Web 应用程序的挑战

作者：John Grady，ESG 分析师

2020年11月

本 ESG 白皮书受 Google 委托制作，由 ESG 特许发布。

内容

执行摘要

Web 应用程序的开发、组成和部署位置在现代企业中发生了根本性的变化。越来越多地采用 DevOps 方法来提高应用程序部署的敏捷性和速度。有助于促进向基于微服务体系结构的转变，并相对于位置创造了更大的灵活性，以确保在应用程序需要的任何地方托管资源。

然而，在为企业带来众多好处的同时，这些发展的副产品通常也带来了控制权的分散化，并将其转移到了传统 IT 组织之外，特别是相对于安全性而言。

同时，Web 应用程序面临的威胁形势比以往任何时候都更加多样化和动态。攻击者仍然试图通过代码和基于可用性的攻击来利用传统的应用程序漏洞，同时还将他们的方法扩展到针对现代 Web 应用程序相连接的组织：API。为了应对这些挑战，一种新的模型正在出现，以克服孤立的应用程序安全方法的局限性。具体而言，将 WAF、DDoS 防护、机器人程序缓解和 API 保护集成到一个整合的 Web 应用程序和 API 保护（WAAP）解决方案正在成为简化管理、简化操作和提高安全性的首选方法。

将 WAF、DDoS 防护、机器人程序缓解和 API 保护集成到整合的 Web 应用程序和 API 保护（WAAP）解决方案中，并成为简化管理、简化操作和提高安全性的首选方法。

现代 Web 应用程序引入了新的安全挑战

Web 应用程序的开发、组成和部署位置在现代企业中发生了根本性的变化。越来越多地采用 DevOps 方法来提高应用程序部署的敏捷性和速度。有助于促进向基于微服务体系结构的转变，并相对于位置创造了更大的灵活性，以确保在应用程序需要的任何地方托管资源。

然而，在为企业带来众多好处的同时，这些发展的副产品通常也带来了控制权的分散化，并将其转移到了传统 IT 组织之外，特别是相对于安全性而言。

企业环境中支持的应用程序数量持续增加。事实上，62% 的受访者表示他们的组织支持至少 250 个业务应用程序。此外，超过四分之三（78%）的人表示，这些应用程序中超过 20% 都是内部开发的。[1] 为了实现这种规模，大多数组织已开始调整其流程和支持基础设施，以提高开发和部署新应用程序的速度、敏捷性和灵活性。不幸的是，这些改进可能会以牺牲安全性为代价。

几乎所有组织都使用某种类型的云服务，但在企业环境中看到多个云平台已经变得司空见惯，这要么是随着时间的推移而自然蔓延的结果，要么是正式的业务战略。这并不是说本地基础设施已经或将要消失。许多组织希望维护本地基础架构以支持旧应用程序、确保性能要求或维护数据留存和合规性。采用基于容器的架构也促成了这种多位置趋势。具体而言，虽然 23% 的组织目前报告基于容器的应用程序部署在公共云平台和私有数据中心的组合中，但 46% 的组织预计未来将使用混合模型。[2]

与 DevOps 计划没有密切联系的安全组织可能对这些团队正在部署和运行的应用程序的控制和可见性是有限的。

此外，应用程序开发和管理越来越分散，开发人员分散在整个业务线中，许多组织都采用 DevOps 方法。事实上，57% 使用公有云服务的组织在某种程度上使用 DevOps，另外还有 16% 的受访者表示计划在未来采用这些做法。[3]

[1] 资料来源：ESG 总体调查结果，现代应用环境趋势，Trends in Modern Application Environments，2019年12月。
[2] 资料来源：ESG 总体调查结果，Leveraging DevSecOps to Secure Cloud-native Applications，2019年12月。
[3] 资料来源：ESG 总体调查结果，Leveraging DevSecOps to Secure Cloud-native Applications，2019年12月。

与 DevOps 计划的安全集成级别可能因组织而异。与 DevOps 计划没有密切联系的安全组织可能对这些团队正在部署和运行的应用程序的控制和可见性是有限的。再加上许多应用程序安全工具不是为云构建的，而是基于以设备为中心的在线架构，这使得在所有 Web 应用程序中应用一致的安全性变得更加困难。

最后，现代应用程序组件的组成和相互作用进一步加剧了这些问题。向基于微服务的体系结构的转变导致 API 使用率急剧上升，以支持更快、更敏捷的应用程序开发。不幸的是，这些端点的蔓延可能会使维护适当的安全控制变得困难。配置错误、身份控制不佳和有限的可见性可能被攻击者所利用，并不恰当地提升权限、访问敏感数据或通过不安全的 API 对用户发起欺诈性帐户接管攻击。

传统的应用程序安全功能仍然很重要，但存在严重差距

这并不意味着传统的应用程序安全功能已经变得无关紧要。实际上，随着攻击者确定要利用的新方法和向量，威胁形势会发生变化，应用程序安全性也不例外。组织可能会遇到一系列与 Web 应用程序相关的攻击，从针对软件漏洞的攻击、针对应用程序本身或支持 API 的可用性攻击，以及针对用户凭据的欺诈。因此，虽然组织应确保对主要应用程序威胁向量的保护，但必须了解其中一些工具的运行限制。

虽然组织应确保对主要应用程序威胁向量提供保护，但他们必须了解其中一些工具的运行限制。

Web 应用程序防火墙

Web 应用程序防火墙仍然广泛部署，并且是大多数应用程序安全策略的核心组件。开放式 Web 应用程序安全项目 (OWASP) 每 2-3 年发布一次关于前 10 大应用程序安全漏洞列表和相应的修复指南。虽然目标应该是在开发和部署期间缓解这些问题，但现实情况是错误确实会发生，并且 Web 应用程序在部署时通常存在漏洞。许多 WAF 专门针对 OWASP Top 10 提供基线保护，以抵御最常见的应用程序威胁。合规性也是广泛采用 WAF 的一个因素，尤其是相对于面向公众的应用程序而言。但是，人们对 WAF 作为提高应用程序安全性的途径的兴趣日益浓厚，而不仅仅是一个复选框项。不幸的是，许多传统 WAF 的体系结构使得实现这一点变得困难，特别是由于部署和检测。

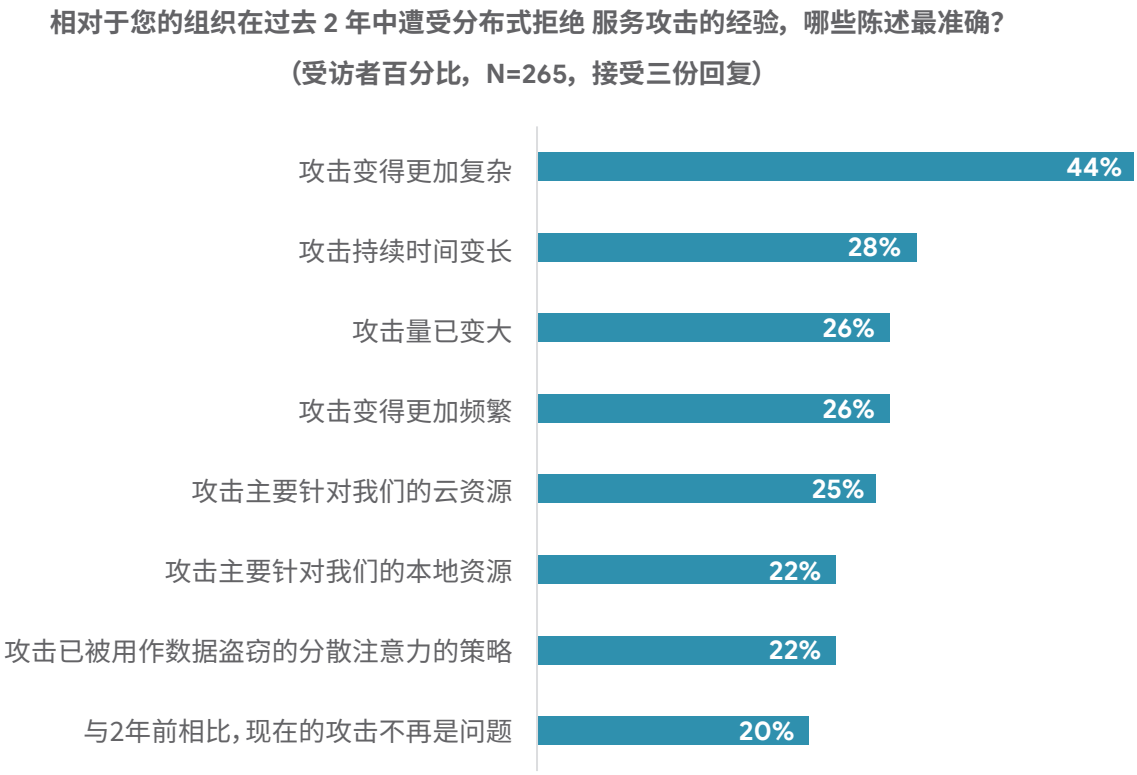
旧版 WAF 面临的最大问题是，许多 WAF 是为保护本地整体式应用程序而构建的，这使得它们难以扩展以满足更动态的应用程序部署实践。这些解决方案可以在虚拟化形式中提供，以解决云应用程序的问题，但云原生流程中的可扩展性、灵活性和集成性可能无法满足以云为中心的组织的需求。这种情况已经开始改变，但在许多情况下仍然是一项正在进行的工作。

最后，从采购和运营的角度来看，WAF 历来都是昂贵的。以设备为中心的方法需要大量的前期资本投资。此外，对基于特征码的检测模型的依赖使部署、调整和维护成为一个劳动密集且成本高昂的过程。这并不是说签名是无关紧要的。然而，更先进的 WAF 解决方案正朝着使用机器学习功能增强签名的方向发展，以减少误报和以自适应的方式调整防御。这有助于组织降低与 WAF 相关的间接成本，同时提高安全性。

分布式拒绝服务预防

DDoS 攻击相对容易发起，并可能导致重大的业务中断，导致品牌声誉影响和收入损失。这些攻击可能会起伏不定，但对于拥有面向公众的 Web 应用程序的所有类型的组织来说，这些攻击仍然是最重要的安全问题，并且越来越难以防御。事实上，44% 的组织报告说，DDoS 攻击在过去两年中变得更加复杂，尽管持续时间更长，数量更大，频率增加也很常见，这些攻击的趋势也是如此(见图 1)。[4]

图 1. DDoS 攻击趋势



资料来源：Enterprise Strategy Group

因此，许多组织已转向基于云的 DdoS 防护服务，主要是为了防御大型攻击，同时也是为了简化操作并节省成本。由于攻击通常达到 100Gbps 范围，在极少数情况下甚至超过 1Tbps，基于设备的方法无法扩展到所需的缓解能力水平。DDoS 解决方案通常专注于针对第 3 层和第 4 层的以网络为中心的容量攻击，或第 7 层应用程序攻击。但是,需要覆盖跨两个向量的攻击，更重要的是，必须包含来自应用程序的遥测数据，以确保提供足够的保护。

[4] 资料来源:ESG 总体调查结果,Network Security Trends ,2020年3月。

API 保护

在过去几年中，对支持现代 Web 应用程序的 API 的保护越来越受到关注。事实上，34% 的受访者表示，API 安全将是他们的组织在未来 12 到 18 个月内为保护云原生应用程序而进行最重大投资的领域。[5] 然而，这种投资如何转化为工具，却存在很大的差异。许多 WAF 具有一定的 API 安全性功能，但在大多数情况下，这些功能仍然受到一定限制，并且是解决方案的次要重点。此外，此模型通常不提供发现功能来标识尚未清点的 API，因此需要与单独的 API 网关或管理工具集成以提供更完整的解决方案。最后，部署在边缘的 WAF 无法查看其后方流动的应用程序内部 API 流量。

34% 的受访者表示，API 安全将是他们的组织在未来 12-18 个月内为保护云原生应用程序而进行最重大投资的领域。

机器人缓解

使用机器人来促进应用程序攻击只会随着时间的推移而增加。然而，由于不同类型的机器人和机器人流量的性质，恶意机器人流量很难防御。由于并非所有机器人都是恶意的，所以区分坏机器人和良性网络爬虫机器人至关重要。此外，只有当机器人的规模达到临界质量或者机器人导致不良了结果时，例如帐户接管、自动帐户创建或类似情况。机器人攻击才可能成为恶意的，在此之前，机器人只是在模仿人类行为，但规模更大。

机器人不断发展，使检测更加困难。早期一代的机器人可以通过 cookie 或 JavaScript 挑战轻松识别。现在高级机器人使用合法的浏览器，更准确地模拟人类活动的细节，在不影响用户体验或产生误报的情况下进行大规模检测变得更加困难。虽然存在强大的机器人管理解决方案，但是相对于整体应用程序安全方法的有效性来说，机器人用于针对应用程序和 API 的程度限制了这些解决方案。

孤立的工具无法充分保护现代 Web 应用程序环境

将所有这些安全功能整合到现代 Web 应用程序环境中会显着增加安全复杂性和成本，因为这些工具是孤立的并相互独立管理。只有当应用程序环境分布在本地和云环境的混合环境中时，管理复杂性才会变得更加复杂。事实上，ESG 研究发现，43% 的组织表示，在部署云原生应用程序的数据中心和公有云环境中保持安全一致性是最大的应用程序安全挑战之一。[6] 从采购和供应商管理的角度来看，按照这些思路，让提供这些工具的供应商参与进来会增加成本并降低效率。

这种复杂性可以通过专门配备熟练的安全人员在一定程度上得到补偿，但对于大多数组织来说，这不是一个现实的选择。不幸的是，正如 33% 的受访者所指出的那样，应用程序安全是技能短缺最严重的网络安全领域。[7] 前面讨论的应用程序的分散化和企业支持的应用程序数量不断增加，只会加剧这种情况。最终，这也会影响效率，无论解决方案本身不共享有关应用程序攻击的信息以改进保护，还是由于跨多个工具集的潜在配置错误。因此，一致性和易用性变得至关重要。

[5] 资料来源:ESG 总体调查结果，Leveraging DevSecOps to Secure Cloud-native Applications，2019年12月。
[6] 资料来源:ESG 总体调查结果，Leveraging DevSecOps to Secure Cloud-native Applications，2019年12月。
[7] 资料来源:ESG/ISSA 研究报告，The Life and Times of Cybersecurity Professionals 2020，2020年7月。

最后，随着组织优先级的转移，安全预算显然在不断变化，以确保远程工作人员得到所需的支持与安全性。应用程序安全工具可能是在企业中部署和维护的更昂贵的解决方案之一，部分原因在于完全保护应用程序免受攻击者所需的广泛覆盖范围。毫无疑问，保护 Web 应用程序将继续在安全预算中占据相当大的份额。然而，许多组织将尽可能地寻找减少支出的方法。

现代 Web 应用程序安全解决方案的关键属性

为了解决这些成本、复杂性和效率问题，结合 WAF、DDoS 预防、机器人程序缓解和 API 保护的安全解决方案已经开始出现。这些解决方案有时称为 Web 应用程序和 API 保护或 WAAP，代表了从孤立应用程序保护到统一应用程序保护的转变（请参见图 2）。与任何安全整合方法一样， 用户希望改进威胁防御，提高运营效率，在以前不同的控制之间更紧密的集成以及改进的供应商关系。相对于 WAAP，这种转变仍在进行中，解决方案才刚刚开始进入市场，导致供应商之间的架构和功能存在显着差异。然而，即使出现这种情况，组织在考虑 WAAP 解决方案时仍应注意一些关键属性。

图 2. Web 应用程序和 API 保护

资料来源：rise Strategy Group

以云为中心，但与位置无关

随着越来越多的应用程序迁移到云中,接下来应该从以保持与资源的距离这个角度进行相应保护。不幸的是,许多企业支持的现代多云环境可能会使这变得困难。此外,对于大多数组织来说,支持本地应用程序仍然是现实。为了实现更少产品,更少的供应商和更低的复杂性的承诺,可以跨混合、多云环境保护应用程序的 WAAP 解决方案至关重要。也许同样重要的是,组织应该考虑插入 CI/CD 工作流并与用于应用程序开发、配置、供应、监控和修复的 DevOps 自动化工具集成的 WAAP 解决方案。

集成

虽然 WAAP 承诺采用集成的运行时应用程序安全方法,但现实情况是,大多数解决方案才刚刚开始向这一概念过渡。这为从业者在评估 WAAP 解决方案时留下了一个相当大的灰色地带,这也使得达到正确的平衡变得更加困难。解决方案可以包括由集中式管理界面连接的离散产品。但是,即使是此管理组件也可以从单个仪表板(提供对所有向量的攻击流量和应用程序响应的可见性)到跨 WAF、DDoS、机器人和 API 保护的完全统一的策略管理。

某些解决方案确实通过单个产品提供跨 WAF、DDoS、机器人和 API 保护的集成功能,在其中进行一次流量扫描,即可检测所有四个向量中的恶意活动。然而,在许多情况下,主要关注点是一个或两个功能,其余功能存在重大限制。通常,强调 WAF 和 DDoS,只有有限的机器人和 API 保护。对于大多数组织而言,在考虑安全解决方案时,效率仍然是最重要的因素。事实上,ESG 发现,虽然人们对整合企业环境中使用的供应商和产品数量非常感兴趣,但 68% 的受访者表示,他们的组织继续购买同类最佳的产品,这表明平台方法的门槛很高。[8]

遥测和风险

任何 WAAP 解决方案的一个主要组成部分都应该是能够跨其面前的所有应用程序、跨所有载体收集遥测数据,并且您可以获取该信息以实时评估风险并改进防御。例如,当潜在的机器人流量源自于一组特定的 IP 地址时被识别,该信息应与 DDoS 缓解组件共享,以便与这些 IP 地址相关的流量不被允许超过指定的阈值,来确保应用程序的可用性。

任何 WAAP 解决方案的一个主要组成部分都应该是能够收集它跨其面前所有应用程序、跨所有载体收集遥测数据,并使用该信息实时评估风险和改进防御。

此外,通过了解基于威胁和应用程序的攻击可能带来的风险,可以实施缓解措施,从而减少误报,改善客户体验,并允许在阻止之前收集额外的遥测数据。换句话说,如果可疑的流量被简单地阻止,就会收集有限的情报。通过采取有限的措施(如要求多重身份验证),安全团队可以确保有效用户的可用性,同时更好地了解针对其应用程序的攻击类型和策略,并使用该信息来改善组织的安全状况。理想情况下,这些功能是 WAAP 解决方案的本机功能。但是,至少需要与 SIEM,日志记录和监视工具的强大集成才能整理收集的情报。

易用性

最后,对于大多数组织来说,要意识到 WAAP 可以提供的好处,必须强调可用性。管理 Web 应用程序防火墙的难度是一个老生常谈的话题,但有充分的理由。管理员必须管理数千条规则,并且通常必须在学习模式(这需要时间)和监视模式(不防止攻击)和阻止模式之间进行选择; 但是会存在误报影响合法用户体验的风险。DDoS、机器人程序,尤其是 API 保护同样复杂。

[8] 资料来源:ESG 总体调查结果,Enterprise-class Cybersecurity Vendor Sentiment ,2020年3月。

将这些功能结合到实用的 WAAP 解决方案中需要精简规则集，以简化管理员必须管理的参数数量。预配置的规则在一定程度上肯定会有所帮助，并已成为 WAF 和 WAAP 解决方案的工作重点。结合自然语言描述、将规则分组到更广泛的漏洞利用保护类别以及使用机器学习自动建议规则都可以帮助降低通常与应用程序保护相关的复杂性。

组织应考虑在所有四个 WAAP 组件中具有强大单个功能的解决方案，这些组件能够以本地共享遥测数据，以改进威胁检测并确定可用性的优先级，并可将集中式管理和功能集成作为额外的优势。

总体而言，组织应考虑在所有四个 WAAP 组件中具有强大单个功能的解决方案，这些组件能够以本机方式共享遥测数据，以改进威胁检测并确定可用性的优先级，并可将集中式管理和功能集成作为额外的优势。供应商的透明度和沟通也非常重要。用户应确保全面了解其供应商的路线图，以明确跨 WAAP 组件完全集成的优先级和时间表。

Google 的 WAAP 方法可跨混合、多云环境保护 Web 应用程序

Google 的 Web 应用程序和 API 保护解决方案基于与 Google 用于保护其面向公众的服务的相同技术，并提供针对 Web 应用程序漏洞利用、DDoS 攻击、欺诈性机器人活动和针对 API 目标威胁的保护。该解决方案包括三个组件：

- **Cloud Armor:** Cloud Armor 托管在 Google 的全球负载均衡基础架构中，提供 WAF 和 DDoS 防护功能，保护应用免受 OWASP Top 10、复杂的应用漏洞利用以及容量耗尽和应用层可用性攻击。
- **Apigee:** Google 的专用 API 平台提供整体 API 管理功能，但重点关注安全性。该解决方案验证 API 密钥、生成和验证 OAuth 访问令牌、速率限制流量、强制执行、配额，并提供 API 趋势分析。
- **reCAPTCHA Enterprise:** 近十年来，Google 的机器人程序缓解功能一直在保护数百万个网站。reCAPTCHA Enterprise 服务以该技术为基础，具有专门针对企业安全问题而设计的功能。该解决方案可防御欺诈活动，例如抓取、凭证填充和自动帐户创建。该解决方案旨在不因挑战而干扰用户体验，但可以定制以实施对策，例如基于组织的风险承受能力的两因素身份验证或电子邮件验证。

Google 通过其 Cloud Logging 和 Monitoring 仪表板提供集成的可见性和遥测功能，以简化操作和管理。作为一种云交付解决方案，Google 的 WAAP 比本地解决方案更具成本效益。除了保护托管在 Google 云中的应用程序之外，Google 的 WAAP 还可以利用 Google 的可扩展性庞大足迹来保护其他公共云或本地应用程序，从而为组织的整个 Web 应用程序库存提供保护。

更重要的事实

总体而言,技术尤其是应用程序日益相互关联的性质正在推动对跨多种 IT 工具进行更高级别集成的需求。在网络安全中尤其如此,攻击者很少专注于单一的妥协途径,而是利用不同媒介的多种策略作为更广泛活动的一部分。

应用程序安全性也不例外,这是向基于 WAAP 的方法转变的起源。

然而,集成的需求必须与控制措施的能力相结合,以充分保护环境,解决相关用例,并使从业者能够更有效地完成工作。面向公众的 Web 应 用程序代表了企业资源中一些最关键的任务。这些资产的妥协或不可用可能直接导致收入损失和客户不满。WAAP 解决方案通常可以解决组织面临的效率问题,但用户必须确保对所有应用威胁向量的强大覆盖,以使这些实施真正成功。

Enterprise Strategy Group 是一家从事 IT 分析、研究、验证和战略的公司，致力于为全球 IT 社区提供市场资讯和可行见解。

www.esg-global.com

contact@esg-global.com

508.482.0188