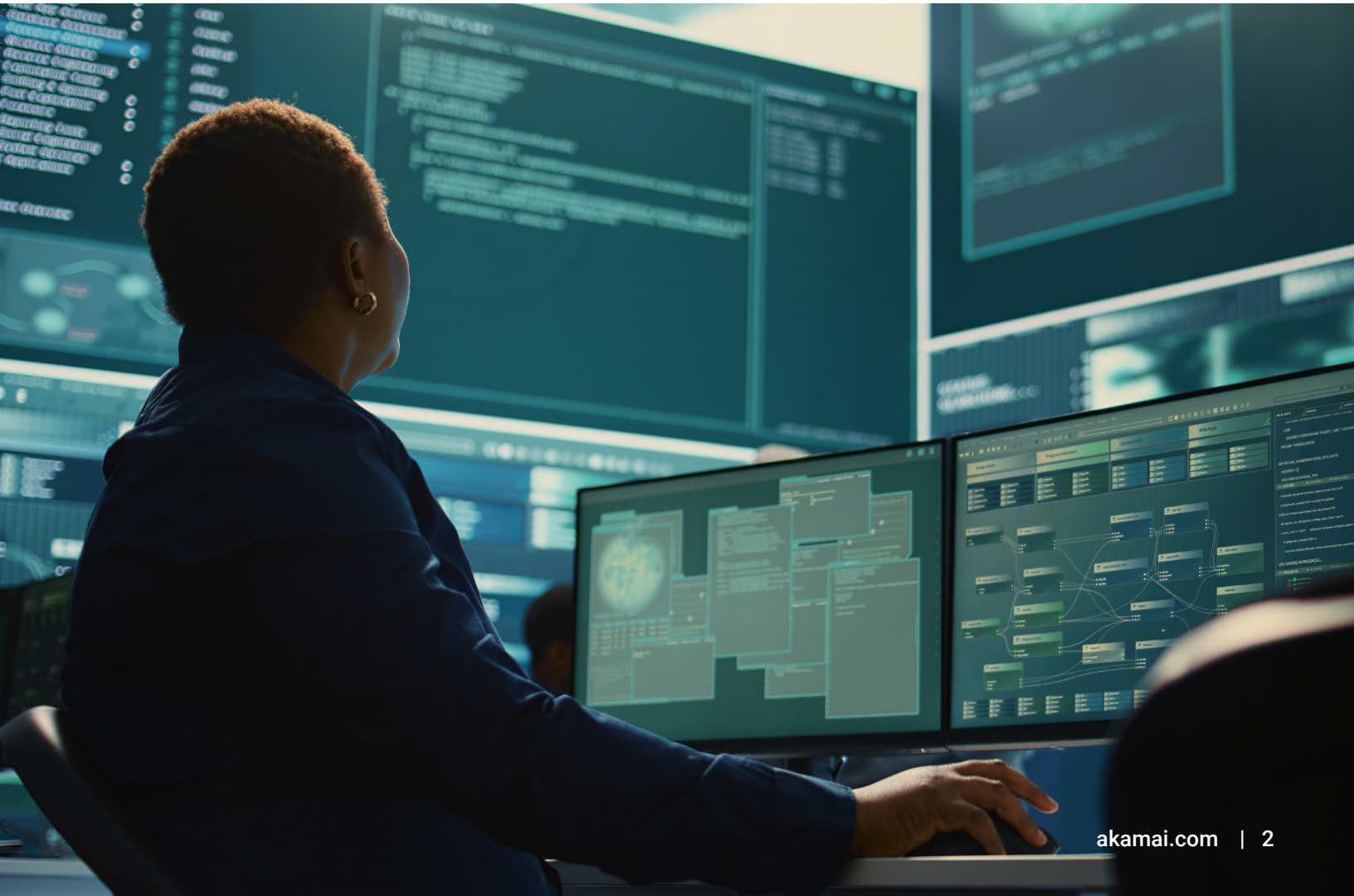
Akamai

白皮书

API 安全与合规性

数据保护的隐式和显式要求

报告内容



前言

从传统上来说，企业要证明遵守数据保护法规，通常意味着耗费大量的精力和资源去跟进一些众所周知的风险。但这种情况正在发生改变。当今企业的攻击面正在快速演变，有许多威胁超出了大多数企业合规计划的考虑范围。部分原因在于监管机构自身无法保持与时俱进，也无法全面地阐明防止泄露所需的各种保护。

API 保护就是这种情况。每当有客户、合作伙伴或供应商与企业进行数字互动时，后台都会有相应的 API 来帮助实现信息的快速交换，这些信息通常包含敏感数据。现在，攻击者发现可以简化策略，直接以 API 为目标即可窃取这些数据。

您可能已经发现法规中有了新的措辞，指出企业需要清查、评估或保护 API。但是，即使未包含有关 API 的具体措辞，也改变不了它们已成为确凿无疑的攻击媒介这一事实，因此对 API 进行充分的保护也*势在必行*。

API 成为主要的合规问题并不让人感到意外。暴露或配置错误的 API 非常普遍，很容易遭到入侵，而且往往缺乏必要的安全保护。仅仅是一个遭到入侵的 API 就会导致数百万条记录被窃取。数字本身就说明了问题：

- 78% 的企业遇到过 API 安全事件。[1]
- 44% 的企业曾因 API 安全事件被监管机构处以罚款。[2]

这对您的合规性计划有何影响？监管机构需要看到您的企业正在采取措施来保护敏感数据的所有访问点。这意味着您需要证明自己的企业能够：

- 全盘考虑每个 API，包括难以发现的影子 API
- 发现并修复任何 API 漏洞
- 应用量身定制的控制措施来避免发生以 API 为中心的数据泄露

本白皮书探讨了日益增长的 API 风险的本质，重点介绍了（明示或暗示）要求实施 API 保护的六个法规示例，并提供了关于如何通过 API 安全最佳实践满足合规要求的建议。

1. 和 2. 的来源：Akamai Technologies，2023 年发布的《对 API 安全存在认知脱节》

了解 API 风险

API 是企业数字产品、服务和云环境的核心。由于 API 会持续访问数据和关键系统，它在帮助企业提升收入的同时，也会带来运营风险。但问题在于，大多数企业都不会像注重其他威胁（如网络钓鱼或勒索软件）那样优先考虑与 API 相关的威胁，即使是拥有成熟的安全计划的企业也是如此。

部分企业依赖 API 网关和 Web 应用程序防火墙实施基本的 API 保护，但这些工具并未经过专门设计，无法提供专业 API 安全解决方案所提供的监测能力、实时保护和持续测试。以下是这些工具无法完全满足要求的原因：

- API 网关和 WAF 只能监测流过它们的*受管* API 流量。
- 它们无法保护非受管 API，而分析人员预测，到 2025 年这些 API 差不多会在典型企业的 API 生态系统中占据半壁江山。
- 因此，安全团队并未做好充分准备来保护攻击面中增长速度最快的部分，并且对 API 的传送位置、配置方式、它们交换的敏感数据的类型以及带来的风险都知之甚少。

监管机构认为保护用户信息是企业的首要任务，并会对未能合理保护客户数据免受未经授权访问的公司处以高额罚款。考虑到只有四成的安全专业人员掌握完整的 API 清单并知道哪些 API 会返回敏感数据[3]，并且很多 API 调用都由攻击者发出以测试是否存在漏洞，因此通过 API 进行的数据泄露只会越来越多，更遑论现在实施 API 攻击非常容易。

3. Akamai Technologies，2023 年发布的《对 API 安全存在认知脱节》

影响合规性的四种 API 攻击

API 漏洞如何影响公司的合规状况？下面举几个例子：

- 某个攻击者利用 API 端点缺少身份验证控制措施的漏洞入侵了常用的项目管理应用程序。该攻击者入侵了此 API，未经授权便访问了数百万用户的信息，并且几个月后在互联网上泄露了超过 21 GB 的数据，包括电子邮件地址和董事会成员信息。
- 据报道，一家大型电信公司超过 1100 万条客户记录遭到泄露，起因是在不知情的情况下某个 API 被暴露在互联网上并且不需要身份验证。攻击者入侵了该 API，看到它缺少唯一标识符，因此猜出了它的 ID 编号，从而轻松获取了敏感数据。
- 据报道，一家社交媒体公司近年来两次遭到攻击者通过非法利用 API 实施抓取策略进行的攻击。在第一个示例中，攻击者从 5 亿份用户资料中抓取了隐私数据并进行出售。在第二个示例中，攻击者创建了一个数据库，其中包含所抓取的 7 亿名用户的电话号码和薪水数据。
- 该技术还被用于攻击另一家社交媒体公司，并导致数百万用户的数据泄露。该公司被处以 50 亿美元的罚款，因为第三方供应商使用了该公司的 API 来收集敏感数据。供应商滥用 API 并不是该公司受到重罚的主要原因；未能合理地监控自己的应用程序才是该公司*自身*受到处罚的原因。

涉及 API 安全的六个法规和框架示例

在很多法规和框架中，并不一定会特别地提到 API，但这些要求很清楚地强调了要保护运行 API 的应用程序和基础架构。例如：

- 支付卡行业数据安全标准 (PCI DSS) v4.0 提供了如何确认某个企业的软件是否安全地使用了外部组件功能的相关指导。这包括用于将支付数据从移动应用程序传输到银行系统的 API。
- 《NIST 安全软件开发框架》提供了相关指导，让您可以了解如何开发受到良好保护的软件、如何为其提供持续保护以及如何应对漏洞。API 是软件开发的核心。

在很多情况下，法规都对数据保护目标提出了宽泛的定义，例如《通用数据保护条例》(GDPR) 对“适当的安全措施”的要求。您的 API 每天可能会收到来自客户*和*攻击者的数百万次调用并请求提供此类数据。您需要确定哪些安全控制措施是必需的，然后展示它们是如何运作的。

我们来深入了解一下直接影响您的 API 生态系统的法规和框架。

1. PCI DSS v4.0

由支付卡行业安全标准委员会制定的 PCI DSS 已成为保护支付数据的全球标准。如果贵企业允许顾客使用主流信用卡进行支付，并以电子方式处理、存储或传输持卡人数据，那么您就必须遵守这些要求。

原始版本的要求涵盖了安全领域中至关重要的核心要素，这些要素现在仍然与 2006 年 PCI DSS 发布时一样重要，例如根据拥有知情权的原则授予对系统和持卡人数据的访问权限，并按角色制定访问权限要求。

但是，随着 PCI DSS v4.0 的生效，企业需要修改他们的合规计划，以应对频繁攻击与支付技术息息相关的成千上万个 API 的攻击者。整体而言，PCI DSS v4.0 具有四个关键目标：

1. 持续满足支付行业的安全需求
2. 倡导将安全防护视为一个持续的过程
3. 帮助企业灵活满足合规性要求（例如，提供新工具、新的控制措施）
4. 增强验证方法和验证流程

PCI DSS v4.0 要求 6.2.3 的核心是企业需要审查其定制和自定义的应用程序代码（即，由第三方供应商开发的代码，但并非标准的现成商用应用程序），以确保不会将漏洞发布到生产环境中。此要求针对 API 提供了指导，以确认企业软件能够安全地使用外部组件的功能（库、框架、API 等）。此类要求强调了 API 在更广泛的软件供应链中发挥的关键作用，以及需要采取什么措施来保护它。

API 现已成为现代化应用程序环境中连接和数据交换的默认方法。考虑到这一点，从生产前（左移）和生产后（右移）的角度来保护 API，对于确保数字化业务能够弹性应对攻击至关重要。此处介绍了遵守要求 6.2.3 应遵守的一些 API 安全最佳实践：

- 确认所用的基于 API 的组件以及安全态势（例如，查找有无错误配置导致出现漏洞，包括使用弱加密密码）。
- 验证 API 使用过程中正常的预期行为，并实施控制措施来阻止可疑行为者滥用系统（例如，检查应用程序的行为来检测逻辑漏洞）。
- 检测用于支持 API 的第三方框架，确定是否有任何过时和易受攻击的地方。
- 建立所有 API 的完整清单，包括您在运行的不同版本；这可以让您深入了解需要管理的后门和潜在的未记录功能。
- 验证 API 代码的安全性，避免将任何与 API 相关的漏洞引入到生产环境中。
- 实施针对 API 的安全编码最佳实践，让您可以采取程序性的方法来持续地安全交付代码。

2.《通用数据保护条例》(GDPR)

GDPR 是一项欧盟 (EU) 立法，旨在加强欧盟内部的个人数据保护，确保采取一致的方法。而且 GDPR 不仅适用于欧盟公司；在欧盟提供消费品或服务的所有企业也必须遵守此条例。

该法规规定，个人数据是指可以与个人相关联的信息。受 GDPR 监管的数据可能包括个人的姓名、联系信息、银行和财务数据以及医疗信息。从技术角度来说，受保护的数据还包括 IP 地址和网络 Cookie 等地理位置数据。

这对 API 安全意味着什么？无论您要开发应用程序、微服务还是物联网 (IoT) 设备，作为这些技术的核心的 API 都可能交换受 GDPR 监管的数据。因此，开发可以访问互联网的 API 的企业必须从一开始就将数据保护纳入 API 设计中，而不是事后再考虑数据保护。

考虑最低权限原则，这要求确保用户仅拥有执行其作业所需的最低权限。

GDPR 第 25 条*基于*最低权限原则，要求所有公司实施“技术和企业级措施，以确保默认情况下，仅处理每个具体目的所需的个人数据...”反过来，API 开发人员应实施用户身份验证和授权控制措施，以保护通过其 API 传输的敏感数据。API 开发团队也必须使用安全通信协议对客户端与服务器之间的信息交换进行加密，以确保数据在传输过程中保持机密。

但是，企业在过去几年甚至几十年以来构建的现有 API 生态系统怎么办？有相当一部分企业 API 都未受到管理、被遗忘或在没有制衡机制的情况下永久运行。在这些情况下，要遵守 GDPR，就需要：

- 发现 IT 环境中的每个 API
- 评估其风险因素（例如，它们已交换的数据的类型以及可以访问这些数据的用户或对象）
- 修复所有漏洞，例如错误配置或弱身份验证机制
- 针对传统和新出现的漏洞及攻击方法对 API 的恢复能力进行持续测试

3.《数字运营弹性法案》(DORA)

鉴于欧盟金融行业担负着重要基础设施运营者的角色，DORA 的要求旨在帮助欧盟成员国中的企业抵御网络攻击并从这些攻击中恢复。有了 DORA，该行业将拥有一个有约束力、全面的信息和通信技术 (ICT) 风险管理框架。该方案的目的是协调并加强对欧盟金融公司的要求，因为当前的形势牵涉大量法规和标准。

在欧盟，总共有超过 22,000 家金融机构和 IT 服务提供商受到 DORA 的影响。值得注意的是，这些企业中包含为欧盟金融公司提供 ICT 系统和服务的第三方，包括云服务提供商。该法案要求金融机构制定 ICT 第三方风险策略并进行尽责调查以审查提供商的适合性。

DORA 提出了多项与 API 安全相关的要求，包括数字运营稳定性，这要求企业实施定期测试计划，以识别数字运营稳定性中的潜在不足、漏洞和/或缺陷。例如，网络安全测试、渗透测试、Web 应用程序测试等。必须根据威胁主导的渗透测试 (TLPT) 进行强制性审查，具体取决于金融企业的规模、风险和业务状况。同样重要的是定期测试您的 API 是否存在漏洞。

DORA 概述了一些安全测试示例，这些示例包含基于 Web 的应用程序和 API 测试。这包括利用面向公众的资源，例如开放全球应用程序安全项目 (OWASP)。尤其是 OWASP 十大 API 安全风险，它可帮助企业识别让攻击者能够获取访问权限、操纵或控制企业资源的配置错误、弱点、逻辑缺陷和代码问题。

4.《健康保险流通与责任法案》(HIPAA)

HIPAA 侧重于数据隐私和安全规则，用于保护电子健康记录 (EHR)、计算机化医嘱录入平台和其他医疗保健 IT 系统中的受保护健康信息 (PHI)。任何以电子方式存储或传输 PHI 的美国医疗保健提供商、计划管理机构或票据交换所都必须遵守 HIPAA。这包括确保 PHI 的机密性、完整性和可用性，并保护其免遭未经授权的披露和不当使用。

即使 HIPAA 并未在要求中明确提到 API，它也是一项对 API 具有重大影响的法规。

假设一家技术供应商需要为全天候医疗诊所构建病患门户。这些门户的底层功能是能够让患者高效、安全地访问与就诊、检查结果、支付等相关的数据。API 能够促进该数据交换的进行。诊所和供应商都必须遵守 HIPAA 要求。

HIPAA 的隐私规则规定，所涵盖的实体“必须制定和实施政策和程序，根据其员工的具体角色，限制对受保护健康信息的访问和使用”。因此，企业的 API 开发人员必须嵌入技术性保护措施（例如身份验证、唯一用户 ID 和基于角色的访问控制），以确保遵循了最低权限原则。

对于受 HIPAA 管辖的企业——无论是 IT 团队创建定制 API 的提供商，还是为提供商开发 API 的供应商，具备监测能力都至关重要。企业需要有关每个 API 的风险状况的实时评估和报告，包括它们传输的 PHI 的类型。这与合规性相关，也与满足 HIPAA 的要求（即，企业需要对请求了解其 PHI 在何时、何地、为何以及向何人披露的信息的个人进行回应）相关。

5.《网络和信息安全指令》(NIS2)

欧盟于 2023 年 1 月采用 NIS 指令的 2.0 版，该指令在原始版本准则的基础上进行了更新，说明如何保护 IT 基础架构和报告事件。虽然 v2.0 未明确提到 API，但它的要求对 API 的保护和管理具有重大影响，因为 API 是受该指令约束的企业中很多数字服务运作时不可或缺的一部分。值得注意的是，NIS2 涉及：

- 更广泛的行业——例如，云服务提供商和社交媒体公司加入了现有名单中，其中包括关键基础设施运营商。对于这些行业，API 广泛用于集成和服务交付，因此确保 API 安全成为了首要任务。
- 首次强调了保护供应链安全的重要性——企业必须对其 IT 供应链和第三方供应商关系进行评估并提供保护。由于 API 通常用于集成外部服务，因此确保其安全是实现合规的关键。
- 要求构建用于评估人员、策略和技术的信息安全管理系统，以保护敏感资源并确保运营弹性。由于 API 是快速增长的攻击媒介，因此必须将它们纳入风险管理策略中。
- 报告重要的网络安全事件，包括 API 漏洞。因此，企业需要采取相应的机制来监控、检测和报告与 API 相关的事件。

6. 适用于美国金融服务监管机构的指导原则

美国联邦金融机构检查委员会 (FFIEC) 为联邦监管机构制定了监管美国金融行业的指导原则和标准。这些机构包括美联储、FDIC、OCC 和 NCUA。该委员会的使命是保护消费者和投资者免遭欺诈、滥用和不当行为的侵害。虽然它不是一项法规，但 FFIEC 的指导原则对于确保金融公司知道如何遵守所建议的安全措施具有关键意义。

这是一份非常有代表性的文件，包含了关于如何保护 API 并反过来保护消费者免遭欺诈和身份盗用影响的具体指导内容。下面概述了相关信息：

- **清单：**FFIEC 建议建立一份清单以包含所有需要身份验证和访问控制的信息系统（包括 API）。这不仅适用于金融机构，也适用于其第三方，例如云服务提供商。
- **身份验证：**API 应该仅允许授权用户进行访问。确定需要进行访问控制的所有用户（例如，客户）至关重要。此外，还必须确定需要采取增强控制措施（例如，多重身份验证）的用户。
- **授权：**API 应该仅允许授权用户访问特定资源。也就是说，FFIEC 建议实施分层安全性——例如，对活动进行监控、日志记录和报告，以识别和跟踪未经授权的访问。
- **风险管理：**FFIEC 在其最新的指导原则中提供了很多有效的风险管理做法。但是，这些做法在“信息系统清单”类别下明确提到了 API，这意味着您需要建立 API 的准确清单。

某个企业或许跟得上网络钓鱼或勒索软件等已知威胁的步伐，但 FFIEC 要求识别*任何*“有可能影响金融机构信息系统”及其数据的网络威胁。正如前言中所述，78% 的企业都遇到过 API 安全事件，因此随着金融监管机构要求的不断发展变化，API 保护将成为实现合规的必要条件。

通过 API 保护最佳实践应对合规挑战

如今的威胁形势需要一个能够提供 API 发现、态势管理、运行时保护和 API 安全测试的全面 API 安全解决方案。这种全面的方法可作为对已实施的任何 WAF 或 API 网关的补充。

1. API 发现

企业存在未被发现的 API 这种情况很常见。大多数企业几乎不具备对大部分 API 流量进行监测的能力，往往是因为他们认为其所有 API 都会通过 API 网关路由。但事实并非如此。如果没有完整、准确的清单，您的企业将会面临各种风险。所需的核心功能：

- 无论配置或类型如何，找到您的所有 API 并将其加入清单中
- 检测休眠、遗留和僵尸 API
- 识别被遗忘、被忽视或未知的影子域名
- 消除监控盲点，发现潜在攻击路径

2. API 态势管理

在有完整 API 清单的情况下，了解哪些类型的数据会流经您的 API 以及这会如何影响您遵从监管要求的能力至关重要。API 态势管理让您可以全面了解流量、代码和配置以评估贵企业的 API 安全态势。所需的核心功能：

- 自动扫描基础架构，从而发现配置错误和隐藏的风险
- 创建自定义工作流，从而通知主要利益相关者有关漏洞的情况
- 确定哪些 API 和内部用户能够访问敏感数据
- 为检测到的问题分配严重程度评级，从而确定补救工作的优先级

3. API 运行时安全

毫无疑问，您熟悉“假设入侵”的概念。专门针对 API 的入侵和攻击同样不可避免。对于生产环境中存在的所有 API 来说，您需要能够实时检测和阻止攻击。所需的核心功能：

- 监控数据篡改和泄露、策略违反情况、可疑行为以及 API 攻击
- 无需进行额外的网络调整或安装难以部署的代理，即可轻松分析 API 流量
- 与现有工作流（工单、SIEM 等）进行集成，以便向安全/运营团队发出告警
- 通过部分或全自动化补救，实时防止各类攻击和滥用行为

4. API 安全测试

API 开发团队压力重重，需要尽可能快地完成工作。速度对于所开发的每个应用程序都至关重要，这更容易导致漏洞或设计缺陷发生且随后无法被检测到。将 API 发布到生产环境中之前在开发阶段对其进行测试，可以显著降低风险并减少修复易受攻击 API 的成本。所需的核心功能：

- 运行模拟恶意流量的各种自动化测试
- 在 API 进入生产环境之前发现漏洞，从而降低攻击得逞的风险
- 依据已确立的管理策略和规则，对 API 规范进行检查
- 根据实际需求或在 CI/CD 管道中运行以 API 为重点的安全测试

Akamai API Security 如何简化 API 合规复杂性

API 是造成漏洞的主要原因，而如今的法规正是为了防止出现这些漏洞。在 API 及其风险成倍增加的情况下，需要采取什么措施来保护您的企业？很多企业用于实施基本 API 保护的现有工具只能提供一部分保护，但这远远不够。如果您在寻找更好的方法来保护贵企业的 API 并证明符合法规要求，我们很乐意为您提供帮助。

对于本白皮书提到的每项要求和指导原则，Akamai API Security 都可以帮助企业增强所需保护——不仅能遵从相关法规，还能保护客户的数据和信任。

Akamai 的全面解决方案可以从初始开发阶段一直到生产后阶段，全程为 API 保驾护航，使您能够遵守核心最佳实践：

- API 发现
- API 态势管理
- API 运行时保护
- API 安全测试

详细了解 API 以及如何保护它们免受攻击。

了解 Akamai API Security 如何为您的企业提供帮助。

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，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。
发布时间：2024 年 9 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯