白皮书

借助 Akamai 安全解决方案将合规性转化为竞争优势

聚焦四大支柱，提升安全性并做好审计准备

聚焦四大安全支柱，为合规铺平道路

如今，世界各地的企业都发现合规变得越来越难，自己已深陷充斥着各类法规的迷宫之中——既需要应对 GDPR、HIPAA 和 PCI DSS，又需要应对越来越多的区域性法令。但证明已做好合规准备不仅是为了满足监管机构的要求，也是为了保持与客户和内部利益相关者（例如高层领导和董事会）的信任关系。

事实上，未能实现合规的影响远不止直接的监管处罚。不合规需要付出巨大代价，包括调查和补救阶段的业务中断、声誉受损以及更大的法律风险。如果企业违反了合规要求，不仅会由于客户流失而蒙受收入损失，还会导致资源被转移到补救工作而不是创新上，从而产生巨大的运营成本。根据 Forrester 的数据，2024 年全球 35 起最大规模的违规事件招致总计 30 亿美元的罚款，其中 23 起事件的违规原因与欧盟《通用数据保护条例》(GDPR) 的规定有关。

过去，安全团队通常是随着法规的出台而解决合规问题。但随着现今技术的快速发展以及攻击规模日益扩大、强度越来越高，合规已成为安全团队在评估工具和成熟度模型时必须纳入讨论的重要议题。安全团队需要问自己一个问题：“我们今天选择的安全防护措施能否帮助我们满足现在和未来的合规要求？”

Akamai 将与客户对话的重点放在安全最佳实践的四大支柱上，这些支柱能够自然而然地推动客户在做好合规准备的关键领域取得进展，从而帮助他们回答这一问题。这四大支柱包括：

- 实现对整个 IT 环境的监测能力
- 阻止跨网络、应用程序和 API 的横向移动
- 防止未经授权的访问
- 保护敏感的客户数据和帐户信息

做到这几点后将为客户树立明显的竞争优势。企业不仅可以提升安全防护水平，还能够为扫清监管障碍做好准备。在提升安全性和合规性的同时，他们也能够更好地赢得客户和内部领导层的信任。

支柱 1

实现对整个 IT 环境的监测能力

做好合规准备必须奠定坚实的基础，首先便是实现对所有数字资产的全面监测能力。企业无法保护他们看不到的东西，而监管机构也越来越多地要求企业证明他们能够提供完整的资产清单、实施持续监控并具备威胁感知能力。

做到这些并不是那么容易。Forrester 最近开展的一项研究发现，超过一半 (52%) 的金融公司认同或非常认同他们缺乏对 IT 资产的全面监测能力。遗憾的是，不合规对任何行业来说都是巨大的风险。从 2023 年到 2024 年，支付超过 10 万美元监管罚款的企业数量飙升了将近 20%。

对于许多企业来说，监测能力方面的挑战在于监控网络流量和 API。以下是一些要求企业对风险有清楚了解的法规和标准：

- 《支付卡行业数据安全标准》(PCI DSS)，提供了相关指导，以确保企业的软件能够安全地使用外部组件功能，例如将支付数据从移动应用程序传输到银行系统的 API。
- 国际标准化组织 (ISO) IEC 27001 等标准，要求在有攻击者入侵网络时对数据和数据处理设施进行隔离。
- 《中华人民共和国数据安全法》，要求实施强有力的安全控制措施，以确保在采用跨不同 IT 系统交换敏感数据的技术时，能够安全地访问客户的个人信息。

许多公司都部署了能够满足其中部分要求的工具或流程。然而，随着他们扩展到混合计算环境并开展跨地域运营，监控工作变得更加困难。对于 API 来说，更是如此。Akamai 的研究表明，拥有完整 API 清单的安全专业人员中只有 27%的人真正知道哪些 API 会返回敏感数据，这一比例低于 2023 年本就令人担忧的 40%。

最后，企业需要知道他们的敏感数据在哪里以及有哪些系统或用户正在访问这些数据，以便确定将安全工作的重心放在何处。这就需要具备以下方面的监测能力：

- 哪些资产正在跨混合云环境和本地环境与网络进行通信（具有实时视图和历史视图），包括第 7 层进程和边缘流量
- 包括影子和僵尸 API 在内的 API 清单，并显示它们在何处与流量来源和代码进行集成
- 客户端 JavaScript，这对满足最新的 PCI DSS 要求来说极为重要

Akamai 的产品组合能够帮助安全团队获得他们所需的监测能力。

Akamai Guardicore Segmentation 可以识别并监测整个 IT 环境内在网络中进行通信的资产，包括第 7 层进程、哈希和命令行详细信息。它还为合规审计期间的认证提供了历史监测能力，以证明审计范围内的资产并未遭到入侵。南北向和东西向流量监测还能显示访问在何处发生。

API Security 提供了企业合规所需的 API 实时清单，并可以帮助确定未加密数据可能在何时何处流经 API。

App & API Protector 提供了应用程序级的监测能力，包括 API 清单、敏感数据泄露检测和实时流量分析。

Client-Side Protection and Compliance 提供了 PCI DSS v4 所要求的客户端脚本监测能力。

一家医疗保健企业实施了 Akamai Guardicore Segmentation，以满足 HIPAA 和 SOC 2 合规要求。它提供了有关不同应用程序之间流量流向的宝贵视图。安全团队可以检查第 4 层日志以外的详细信息：用户 ID、命令行输入，甚至是服务相关性。

支柱 2
防止横向移动

与安全团队本身一样，许多监管机构也承认，即使具备强大的安全态势也有可能发生违规行为，因此他们要求企业确保在出现此类事件时能够减轻事件所造成的损害。例如：

- GDPR 第 32 条要求“有能力确保处理系统及服务持续保持机密性、完整性、可用性及恢复能力”，并且“在遭遇物理或技术事故时能够及时恢复个人数据的可用性和访问权”。
- 同样，PCI DSS v4 也要求企业“部署防火墙以保护信用卡持卡人的数据，并确保防火墙经过正确配置，能够限制可信网络和不可信网络之间的连接”。
- **国际标准化组织/国际电工委员会 (ISO/IEC) 27001** 要求对信息和数据处理设施进行隔离，以保障信息的机密性、完整性和可用性。

虽然大多数企业都部署了某种形式的防火墙，但要想在恶意攻击者入侵网络后限制其横向移动，还需要实施更高级别的控制措施。这使得微分段（最好是软件定义的微分段）成为实现合规的关键工具。Akamai 具有得天独厚的优势，能够解决审计人员所担心的横向移动问题。

Akamai Guardicore Segmentation 可以有效限制横向移动，从而帮助企业保持合规。开箱即用的策略模板有助于通过精细的第 7 层控制措施，快速实施与合规相关的举措。并且由于它是软件定义的，因此无论资产位于何处，它都可以实现相同级别的精细防护。此外，它还能够识别在网络内通信的应用程序以及分段区域之间的通信尝试，让审计人员对您抵御威胁的能力更有信心。

借助 API 的激增，攻击者正在不断寻找实现横向移动的新机会，尤其是容易遭受“失效的对象级授权 (BOLA)”攻击的 API 端点。攻击者可以操纵 API 请求中的对象 ID，在网络内实现横向移动。一旦入侵成功，他们就能绕过授权、升级权限，并获得客户数据的访问权限。

Akamai API Security 可以标记那些在未进行适当身份验证的情况下暴露敏感数据的 API，并识别访问控制措施薄弱或错误配置的 API，它们可能会导致未经授权的数据访问和横向移动。与 Akamai Web Application Firewall (WAF) 集成之后，API Security 还能够实时阻止恶意威胁。

Akamai 的一位客户是一家全球性的金融服务企业，其环境中的未知 API 让他们深受困扰，因此他们实施了 API Security 解决方案。Akamai API Security 可对敏感数据进行分类以帮助满足 GDPR、HIPAA 等法规的要求，因而显著减少了 API 蔓延并提升了合规性。在监管审计期间，这些解决方案的实施直接证明了该公司已采取适当的技术措施。

今天的 AI 威胁是明天的监管障碍

如今，任何针对企业网络安全防御措施的审查，都必须解决 AI 带来的新型威胁。AI 赋能的应用程序、大语言模型 (LLM) 以及与生成式 AI 关联的 API 的快速激增带来了许多企业尚未意识到的新漏洞。这些应用程序种类繁多，包括 AI 赋能的聊天机器人、零售产品推荐引擎、健康诊断工具和风险决策引擎。与此同时，攻击者正在利用 AI 发动更为复杂的攻击。

只要出现了影响业务运营和公众安全的威胁，监管措施便会随之而来。

希望保护其在 AI、数据和客户方面的投资的企业正在向 Akamai 寻求帮助。作为一家安全服务提供商，Akamai 在满足当今企业对监测能力、横向移动限制和访问控制要求方面取得了出色的成绩，并且已进行主动投资来满足未来的 AI 要求。Akamai 开发了先进的 AI 功能以增强其安全解决方案，现在又推出了一种解决方案来帮助企业保护自己的 AI 投资。

Akamai Firewall for AI 通过识别并抵御传统安全工具无法解决且特定于 AI 的威胁和攻击，为 AI 驱动的应用程序提供全面的安全防护。Firewall for AI 专门构建的防护功能包括：

- **防御提示注入**：防止攻击者通过欺骗性输入来操纵 AI 模型
- **数据泄露防范 (DLP)**：检测并拦截 AI 生成的回答中的敏感数据泄露，同时防止在请求中接收敏感数据
- **有毒和有害内容过滤**：在内容发布之前，标记仇恨言论、错误信息和冒犯性内容
- **对抗性 AI 安全**：防范远程代码执行、模型后门以及数据中毒攻击
- **抵御拒绝服务攻击**：通过控制过多的查询使用和模型过载，抵御 AI 驱动的 DoS 攻击

此外，Firewall for AI 还可以帮助企业遵守现行的隐私、安全与保障准则。通过实施针对 AI 的安全策略，企业可以降低与数据保护法规、合乎道德的 AI 使用以及企业治理规定相关的风险。

支柱 3
防止未经授权的访问

在几乎所有的监管框架中，控制对敏感系统和数据的访问都是实现合规性的基石。企业必须了解自己的应用程序和 API 安全态势，并阻止未经授权的访问和滥用。这就要求对用户进行适当的身份验证、根据“按需知密”的原则授予访问权限，并维护所有访问活动的详细记录。

为了实现满足监管要求的完全访问控制，企业必须解决三大关键挑战。Akamai 的安全产品组合可以帮助实现纵深防御，从而解决每项挑战：

1. **全面了解应用程序和 API 安全态势**

Akamai App & API Protector 使企业能够在其运行的所有环境中实施流量策略，而 Akamai API Security 可以针对任何异常活动以及未经授权的数据访问或错误配置向企业发出告警，所有这些都是审计人员的主要考量因素。另一方面，Akamai Guardicore Segmentation 可以跟踪在网络内进行通信的所有应用程序，并建立活动基准。

2. **监控用户行为并限制对敏感信息的访问**

Akamai Guardicore Segmentation 可以根据用户身份限制其在网络内的访问权限，而 **App & API Protector** 可以利用 AI 赋能的威胁检测来实施流量策略，以防止数据泄露。最后，可以利用 **Client-Side Protection & Compliance** 来监控 JavaScript 执行行为，以抵御客户端攻击。

3. **检测并限制欺诈活动**

API Security 可以通过检测异常 API 行为和错误配置的身份验证控制来帮助阻止高风险攻击。Akamai Guardicore Segmentation 可以标记并阻止可能存在欺诈活动的可疑连接，从而保护网络。App & API Protector 可以检测并抵御 OWASP 识别的威胁，以进一步降低欺诈风险。

NIS2 和保障访问安全

更新后的《网络和信息安全指令》(NIS2) 旨在为欧盟成员国建立统一的网络安全级别。NIS2 新增的内容包括：企业必须构建用于评估人员、策略和技术的信息安全管理系统，以保护敏感数据并确保运营弹性。NIS2 还进一步强调了保护 IT 供应链及第三方供应商关系的必要性。

支柱 4
保护敏感的客户数据和帐户信息

全面法规就绪方法的最后一个支柱要求企业制定保护敏感数据的计划。在大多数以安全为重点的法规当中，保护客户、患者、合作伙伴等的数据都处于核心地位。

例如，日本的《个人信息保护法》要求执行数据保护影响评估，以针对处理大量个人数据或涉及高风险数据处理活动的技术识别并抵御风险。

针对美国金融机构，联邦金融机构检查委员会 (FFIEC) 要求实施控制措施，以确保 API 仅允许授权用户通过分层安全措施（例如，监控、记录和报告）来访问特定数据。

满足这一支柱要求需要从威胁检测开始。Akamai 的 Web 应用程序和 API 保护解决方案 **App & API Protector** 提供了第一层防御，而 **Akamai Guardicore Segmentation** 可以监控南北向和东西向流量并对其进行分段。Akamai 的**爬虫程序和滥用防护解决方案组合**针对自动化威胁和人为攻击，提供了一层额外的安全保障。

但是，企业还需要了解其网络内的基准行为，才能正确地识别威胁。以下介绍了 Akamai Security 功能如何提供此类关键见解：

- Akamai API Security 提供了对网络内进行通信的 API 和应用程序的基本了解，而 Akamai Guardicore Segmentation 可以对这些 API 和应用程序进行标记以识别任何异常行为。
- Adaptive Security Engine 是 App & API Protector 的一项核心技术，它可以使用本地和全球数据来了解攻击模式，不仅能针对客户具体情况来调整防护措施，还可以适应未来的威胁。
- Akamai Hunt 是一项托管威胁搜寻服务，它充分发挥了 Akamai 专家研究团队的作用，使企业能够采取更积极主动的防御方法。

DORA 和数据安全

《数字运营弹性法案》(DORA) 旨在帮助欧盟成员国的金融服务企业抵御网络攻击并从中恢复。有了 DORA，该行业就拥有了一个有约束力、全面的信息和通信技术 (ICT) 风险管理框架。DORA 的第 3 条要求企业使用的 ICT 解决方案和流程能够：

- 尽可能地减少与数据相关的风险、未经授权的访问和技术缺陷
- 防止数据不可用、数据丢失以及完整性和保密性违规
- 确保数据传输安全

走出合规困局，掌握竞争优势

有效的合规计划必须能够证明其对业务的影响，而不仅仅是“走过场式地”完成监管要求。在实施 Akamai 以合规为重点的安全解决方案后，各企业纷纷表示在三个关键维度都取得了可衡量的改进。

降低合规成本

与采用临时性方法的企业相比，制定了成熟合规计划的企业在合规活动上的开支通常都更低。通过集成的安全平台实现证据收集自动化后，可以显著减少审计准备时间，同时将单点解决方案整合到一个全面的平台上。

改善风险状况

除了降低成本之外，合规工作的改善还能大大降低风险。实施 Akamai 分段解决方案的企业可以限制存在漏洞的横向移动路径，从而直接满足关键的合规要求，同时降低企业风险。

通过消除可能存在未检测到的违规行为的盲点，全面的监控功能可以提升监测能力，从而直接降低风险。

高效运营

合规影响的第三个维度涉及运营效率的提升。预先批准的控制措施和一致的安全模式可能意味着新应用程序获得安全批准的速度大大加快。这样可以提升安全审查过程的流畅度并加快新应用程序的上市速度，从而提升开发人员的满意度。

合规调优

随着监管要求的不断演变和企业的发展壮大，他们需要一种能够适应相关变化的合规方法。Akamai 集成的安全产品组合为合规策略奠定了坚实的基础，使其能够预测监管趋势，并随着企业的发展而扩展。

- 可配置的策略框架无需进行大规模的架构重新设计即可适应新的要求，而可扩展的报告功能能够随着法规的演变适应新的证据要求。
- 新资产的自动化策略部署可确保在企业扩展时合规性覆盖范围能够自动扩大。
- 无论规模如何，集中管理功能都能保持全面的监测能力，而全面的 API 支持可以实现合规流程的自动化，以应对日益增长的复杂性。

此外，企业还需要积极主动建立定期审查法规的机制，并相应更新其合规控制措施。Akamai 会定期更新安全解决方案，这些解决方案专门针对不断变化的合规要求而设计，从而确保无论监管法规如何变化，客户始终能够保持合规。

结论：以合规构筑竞争优势

有效的合规不再只是为了满足监管要求，它还是一项战略性的企业要务，能够直接影响着企业绩效、客户信任和竞争定位。无论您从事哪个行业，也无论在哪个地区经营，积极主动的合规方法都能确保实现强大且敏捷的安全态势。

做好合规准备的四大支柱包括对整个 IT 环境的监测能力、阻止横向移动、阻止未经授权的访问，以及保护敏感客户数据和帐户信息。通过实施涵盖这四大支柱的综合性安全方法，企业将能够奠定可持续的合规基础，在满足监管要求的同时创造可衡量的业务价值。

那些将合规从必要的经营成本转化为战略优势的企业将取得巨大的成功，这种优势既能帮助他们实现数字化转型，又能保护最重要的资产——客户信任、数据完整性和企业声誉。

要了解 Akamai 如何为您的企业提供帮助，请联系我们。

联系我们

扫码关注，获取最新 CDN 前沿资讯

©2025 Akamai Technologies | 支持 | 发布时间：2025 年 7 月