## 2024 年 API 安全影响研究

# 政府

API 事件频发。了解政府部门如何应对这一重要安全问题，以及您的企业可以采取哪些措施来确保安全。

**在 API 优先的时代，为保障数字服务安全，世界各地的政府部门面临的压力与日俱增。**2024 年，有 86.1% 的公共部门机构报告曾遭遇 API 安全事件，相比前一年的 76.8% 呈急剧增加之势。这一数据的增长使公共部门超出了整个行业 84% 的平均水平，突显出这一挑战的规模正在日益加剧。从满足《通用数据保护条例》(GDPR) 的要求，到在多云系统中强制执行数据驻留以及应对主权安全威胁，各大政府机构普遍需要提高监测能力、治理能力和内在的韧性。

## 政府部门 API 安全事件的真实代价

越来越多的政府机构在采用 API 来落实数字服务、推动机构间数据共享，并实现基础设施现代化。但这一趋势也带来了一系列新的漏洞，而这些漏洞则成为了攻击者的目标。形同虚设的身份验证机制、错误的 API 配置，加之对关键风险指标的认识不足，使政府部门特别容易受到 API 安全漏洞的影响。这些事件所造成的后果远远不止是数据盗窃，对运营连续性、法规合规性和公众信任都带来了风险。

这一结论从何而来？为了解企业在应对 API 威胁方面的经历，Akamai 对 1,200 多名 IT 和安全专业人士（包括首席信息安全官、应用安全人员等）展开了调研。

本文筛选出了政府部门受访者的调查结果，他们表示 API 安全事件造成的最大影响包括：

- “团队/部门的压力倍增”(28.5%)
- “有损我们部门在高层领导和/或董事会中的声誉”(27.2%)
- “监管机构罚款”(25.2%)

考虑到参与调研的同行表示，他们平均需要花费 71.75 万美元来处理 API 安全事件（这一数字比所有八个受调研行业的平均水平高出 21.3%），上述这些相互关联的后果也就不难理解了。

继续阅读，探索 2024 年 API 安全影响研究行业特定洞察。

## 随着攻击的不断增长，监测能力越来越受到关注

在被要求列举 API 安全事件的最主要原因时，您的同行指出了两大关键漏洞：

- API 身份验证控制缺失 (25.2%)
- 使用传统工具来保护 API 安全 (25.2%)

尽管越来越多的证据表明 API 威胁会造成严重后果（从高昂的补救成本到信任度下降），但我们的研究结果表明，仍有许多政府部门团队尚未将 API 安全防护视为首要任务。事实上，在他们未来一年的网络安全优先事务中，API 安全防护仅排名第六，占比只有 17.9%。

**86.1% 的政府部门机构**报告在 2024 年遭遇过 API 安全事件，相比 2023 年的 76.8% 呈明显增长之势

**API 安全漏洞给美国政府机构造成 71.75 万美元的平均财务损失**，超过所有行业 59,1404 万美元的平均水平

**66.9% 的政府实体维护了一份 API 清单**，但只有 18.5% 能够完整监测哪些 API 在处理敏感数据，因而使其关键信息面临风险

### 三大影响

1. 安全团队压力倍增
2. 团队在领导人和董事会心中的声誉受损
3. 因不合规而遭受监管部门罚款

来源：
2024 年 API 安全影响研究

API 攻击会使政府机构付出高昂的代价，包括财务和人员影响。如果由于违规行为而失去领导层的信任，可能意味着加强审查、运营中断，并使本就压力重重、难以满足合规要求的团队面临更繁重的工作。

Akamai

就像私营部门一样，政府机构很难区分哪些是真正的 API 活动，哪些是恶意的 API 活动。在某种程度上，这要归因于很难发现 API 易受攻击的确切位置。在调研中，尽管有 66.9% 的同行表示其部门已建立了完整的 API 清单，但仅有 18.5% 的受访者能够明确知晓哪些 API 会返回敏感数据，这些敏感数据就包括个人身份信息 (PII)，例如身份证号码、生物识别数据和联系信息。

试想一下，如果政府机构的某个部门或附属机构部署了一个未经授权的 API，但未得到最新中央 IT 或安全团队的配合或监督，结果会怎样?

该 API 可能会发生以下情况：

- 其设计会在没有适当授权控制的情况下提供对公民个人或财务数据的访问，从而可能暴露敏感信息
- 已替换为新版本，但未按正确方式下线，使过时的端点容易被利用
- 在中央 IT 和安全团队的监测之外运行，逃避传统的监控工具和合规检查
- 被恶意攻击者利用，使其能够未经授权访问政府系统，从而有可能导致数据泄露、身份盗窃或财务欺诈

这不仅仅是假设——美国政府机构的网络安全形势已经面临着重大挑战。网络新闻商业数字指数表明，许多政府机构和部门都在努力保持稳健的安全态势，近十分之四 (38.8%) 的机构和部门在评估中得到“重大风险”评级，有 75% 的机构遭遇了数据泄露。

这些统计数据反映了政府安全团队所面临的复杂现实，他们必须在任务目标、旧有系统和不断演变的威胁之间取得平衡，同时在与众不同的约束和审查下顺利开展运营。随着这些挑战的加剧，特别是在 API 安全领域之内，各大机构要求其合作伙伴既能了解其具体需求，又能提供适合政府环境的解决方案。

## API 事件对信任度、成本以及团队压力有何影响

考虑到 API 攻击的频率和成本，保护 API 成为全球政府部门日益优先考虑的问题也就不足为奇了。美国总务管理局掌管着一项 Data.gov 计划，其目的是在各个联邦机构之间实现 API 标准化，以提高一致性、安全性和互操作性。同样的工作在全球范围内随处可见，从欧盟和英国的开放数据框架到亚太和中东地区的数字化转型举措，各国政府都在采用标准化的 API 来确保安全、无缝的数据交换。

其中许多举措都与地区性法规相呼应，例如欧盟的《通用数据保护条例》(GDPR)、澳大利亚的《可通知数据泄露方案》和日本的《个人编号法案》。通过实施通用的标准和框架，各国政府正在努力确保安全的数据交换，同时降低由于第三方集成和未经授权访问而造成的风险。

| | 政府 | 所有行业平均值 |
|---|---|---|
| 美国 | $717,500.50 | $591,404.01 |
| 英国 | £378,140.69 | £420,103.18 |
| 德国 | €296,975.79 | €403,453.26 |

*问题 3：如果您经历过 API 安全事件，这些事件的累计总财务影响估值是多少？请包括所有相关费用，如系统维修、停机时间、法律费用、罚款以及其他相关费用。*

很明显，政府机构已经敏锐地意识到了 API 威胁的后果。在本次调研中，我们首次向来自三个不同国家的受访者征询其所在机构在过去 12 个月内因 API 安全事件所造成的经济损失估值。

尽管财务损失十分显著，但受访者明确强调，这些安全事件带来的影响远超财务层面的范畴。

当被问及 API 安全事件的最大影响时，答案并不是财务损失，如前所述，我们的受访者表示，“团队/部门的压力倍增”以及“有损我们部门在高层领导和/或董事会中的声誉”排名前两位。

这些后果会造成长久的影响。数据泄露会破坏信任感，而这可能会危及未来的融资并削弱公众信心。与此同时，本就已压力重重的机构一旦出现生产力下降，还可能会导致倦怠和员工敬业度降低。

而这一压力并不只是出现在少数几个地区。虽然此报告侧重于某些特定市场，但 API 安全已成为全球公共部门机构的一个重大问题，因为无论是亚洲、拉丁美洲还是其他地区的政府机构，在确保数字基础架构安全、满足合规标准以及保护敏感数据免受不断演变的威胁方面都面临着类似的挑战。

## 通过积极的 API 安全防护降低风险和压力

针对政府部门的 API 攻击正在迅速升级，其范围、规模和复杂性在不断扩大。其中包括生成式 AI 驱动的爬虫程序攻击，它们能够迅速适应，并绕过传统的 API 安全工具和其他外围防御措施。许多同行业的安全团队已经切身体会到这些威胁所带来的财务和人力影响。然而，即便企业意识到了 API 威胁的严重性，他们仍然面临一个亟待解决的问题：如何应对这些威胁？

立即采取措施以更好地保护您的 API 及其交换的数据，可以帮助您的企业保护收入，减轻安全团队的压力，同时维护董事会和政府部门领导人的宝贵信任。这些措施包括增强团队对高级 API 威胁的了解，并发展防御这些威胁所需的能力。


如需阅读完整报告，并了解有关 API 监测与保护的最佳实践，请下载**《2024 年 API 安全影响研究》**。

准备好与我们探讨您的挑战，以及 Akamai 将如何为您提供帮助了吗？

**申请定制化的 Akamai API Security 演示**

Akamai

Akamai 安全部门致力于为您的应用程序提供全方位安全防护，从而助力您的业务发展，确保实现卓越的性能和流畅的客户体验。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：2025 年 5 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯