API 安全影响研究 2024

API 事件对您和团队的影响

Akamai《互联网现状》(SOTI) 报告的姊妹篇

目录

3 前言

6 API 安全现状

API 攻击是否会对企业及其安全团队产生重大影响?

对 API 及潜在风险的监测能力是否足够?

API 测试是否足够频繁，可以降低滥用或漏洞风险?

15 API 安全受到关注，但仍缺乏足够重视

企业内不同职位的人员如何看待 API 安全的重要性?

对 API 安全事件的看法不一是否表明企业没有统一的权威信息来源?

18 如何实现更成熟的 API 安全态势

可以采取的措施

20 结论

执行摘要

API 安全影响研究（原《API 安全认知脱节》报告）现已进入第三年，今年的研究对美国、英国和德国（2024 年新增）的 1,207 名领导者和从业人员进行了调查，并根据调查结果探讨了 API 保护的现状。此研究调查的内容包括企业发生 API 安全事件的情况，包括发生的频率、原因和影响；以及安全部门如何应对 API 相关的攻击风险。

为了获得全面的信息，我们调查了不同行业和不同职位的人员，包括：

CISO、CIO、CTO、资深安全专业人士和 AppSec 团队成员，这些人员来自不同规模的企业，从 500 人以下到 1,000 人以上都有

八个行业：金融服务、零售/电子商务、医疗保健、政府/公共部门、制造业、能源/公用事业，以及（2024 年新增）汽车和保险

前言

尽管有数据显示 API 攻击十分普遍而且极具破坏性，API 仍然经常被视为一种*新兴*攻击媒介。我们不妨看看以下数据：

- 根据 Akamai 最近的一份《互联网现状》(SOTI) 报告，2023 年 1 月到 2024 年 6 月，有记录的 API 攻击达到了 1,080 亿次。
- 2024 年 5 月的 Gartner®《API 保护市场指南》提到，“当前数据表明，常规 API 漏洞导致的数据泄露至少是常规安全漏洞的 10 倍。”*
- 攻击活动也日益增多。SOTI 报告还指出，2023 年第一季度至 2024 年第一季度期间，Web 应用程序和 API 攻击合计增加了 49%。

这样的增长并不令人意外。其背后的原因在于，几乎所有推动数字化项目（生成式 AI 工具、面向客户的应用程序、云服务等）的技术都使用 API 来实现通信和数据交换，然而许多 API 并未得到充分的保护，存在身份验证缺失、配置错误甚至彻底被遗忘等问题。这使得 API 成为网络犯罪分子眼中极富吸引力而且经济高效的攻击媒介。攻击者只需要找到一个存在漏洞的 API，然后很快就可以直接获取调用 API 时返回的所有数据，这些数据可能会达到成千上万条记录。

许多 API 未得到充分的保护，使得 API 成为网络犯罪分子眼中极富吸引力而且经济高效的攻击媒介。

总体而言，我们的研究表明，API 安全尚未成为综合安全策略的重要组成部分。大多数企业将 API 攻击视为新兴威胁，然后从攻击数据来看，API 攻击数量正在不断增加，而且攻击者往往会得逞。另外，调查发现 API 攻击造成的财务影响和团队压力也不容忽视。从我们 2024 年的调查结果中，您可以了解 API 安全事件对同行及他们所在企业的影响。我们希望这些数据能帮助您的团队更好地评估 API 保护措施并进行必要的改进。

总体发现：API 事件影响企业正常运营并给团队造成压力

我们 2024 年的研究结果表明，API 是一个日益突出的攻击媒介，给安全团队带来了很大的挑战。受访者在以下几个方面表现出惊人的一致：

- 连续三年见证 API 安全事件增多
- 为解决 API 相关事件并恢复业务正常运行，平均耗费的成本超过五十万（美国首席高管层受访者反馈的平均成本则达到了 943,162 美元）
- 感受到 API 事件给团队成员造成的严重影响，团队遭受的压力和声誉损失（尤其是内部审查加剧了这种压力）严重性排位甚至高于事件处理所耗费的成本

受访者对 API 清单完整性的看法不一，在不同职位人员的反馈中，这种差异更加明显（请参见第 11 页）。值得注意的是，拥有完整 API 清单并且知道哪些 API 会返回敏感数据的企业占比从 2023 年已经不高的 40% 下降到了 2024 年的 27%。

受访者还指出，他们所使用的传统 API 保护工具无法覆盖所有风险。这些工具（例如 Web 应用程序防火墙 (WAF)、API 网关和网络防火墙）常被指责为导致攻击得逞的首要原因（请参见第 17 页 API 事件原因的完整列表，以及第 12 页关于 WAF 和 WAAP 的注释）。

从调查结果中，我们还可以推断 API 安全策略尚未受到重视（尽管有证据表明值得重视）的几个主要原因。其中一个重要原因是，担任重要安全职位的人员对于需要保护的 API 的数量、位置和风险属性没有一致的认识，这很可能是因为对 API 的监测能力较低和缺乏统一的权威信息来源。

我们还发现，安全领导者和从业人员之间对于 API 攻击的原因缺乏共识。问题是出在使用的工具上，还是程序员在开发过程中出现错误，或者生成式 AI 创新产品中的漏洞给攻击者带来可乘之机？不同的受访者有不同的答案。

当然，API 安全在企业安全策略中没有占据更重要的地位还有一个原因，那就是安全团队已经因为其他紧迫的威胁而不堪重负，那些威胁很可能也占据了大部分的财务预算和团队成员的精力。下面我们来深入分析调查结果。

安全专业人员感受到了 API 事件给团队成员造成的严重影响，团队遭受的压力和声誉损失严重性排位甚至高于处理事件所耗费的成本。

84% 的受访者在过去 12 个月内经历了 API 安全事件

过去 12 个月解决 API 事件平均耗费的成本：

美国	英国	德国
$591,404	**£420,103**	**€403,453**

低监测能力

拥有完整 API 清单并且知道哪些 API 会返回敏感数据的企业只占 27%，2023 年这个比例为 40%。

高压力

API 事件的最大影响 *CISO*：损害了部门在高层领导和/或董事会中的声誉。*CIO*：导致团队/部门的压力增加。

测试不足

从 API 开发到生产，对 API 进行实时测试和每日测试的受访者分别只占 13% 和 18%。

API 安全事件的财务成本加剧了团队和领导者所受的影响。事件产生的高额成本引发了高层的关注和审查，可能导致董事会等重要利益相关者认为安全团队没有做好本职工作。这给团队造成了压力。事实上，各地区的受访者均提到，团队遭受的压力是 API 安全事件造成的最大影响。

API 安全现状

过去三年里，报告 API 安全事件的企业越来越多，2024 年这些企业所占的比例达到了 84%（参见下方数据）。这些 API 攻击对企业有何影响？企业为降低风险采取了哪些措施？或者，哪些方面尚待改进？为了解答这些问题，我们对调查结果进行了细分整理。

API 攻击是否会对企业及其安全团队产生重大影响?

简单来说，答案是肯定的。这是我们收集 API 安全事件的财务影响数据的第一个年度，数据结果十分引人注目：根据过去 12 个月内经历了 API 安全事件的那 84% 的企业所报告，处理这些事件所耗费的平均成本（包括系统修复、停机、律师费用、罚款和其他相关的费用）如下所示：

- **$591,404**（美国）
- **£420,103**（英国）
- **€403,453**（德国）

某些职位的受访者认为实际成本要高得多，特别是美国的首席高管层受访者，他们所报告的成本高达 943,162 美元，与美国受访者所报告的平均成本相比，高出将近 60%。

在过去 12 个月内，您是否经历过 API 安全事件?

年份	总计	美国	英国	德国
2022	76%	75%	77%	—
2023	78%	85%	69%	—
2024	84%	83%	83%	84%

不管确切数据如何，API 安全事件的财务成本都加剧了人力方面的影响。事件产生的高额成本引发了高层的关注和审查，可能导致董事会等重要利益相关者认为安全团队没有做好本职工作。这给团队造成了压力。事实上，根据各地区受访者的反馈，“压力”（具体而言指团队受到的压力）是 API 安全事件造成的最大影响，其次是“损害了部门在高层领导和/或董事会中的声誉”，排在第三位的影响是“修复成本”。值得注意的是，排在主要影响中最靠后的三位又全部是内部影响（内部影响最有损团队士气），三者的占比几乎持平（参见下方数据）。

按行业分类的调查结果与此相似：在我们调查的八大行业中，有四个行业的受访者也认为“API 事件导致团队的压力增加”是最显著的影响（请参见第 9 页的侧栏）。这四个行业中包括金融服务业，报告的财务损失高达 832,801 美元，是所有行业中最高的。

受访者提及最多的 API 安全事件影响

1. 导致团队或部门的压力增加—**27.0%**
2. 损害了部门在高层领导和/或董事会中的声誉—**26.6%**
3. 为解决问题而产生的成本—**25.8%**
4. 监管机构的罚款—**25.4%**
5. 失去客户信任和客户流失—**25.0%**
6. 生产力损失—**24.1%**
7. 信任和声誉损失—**23.8%**
8. 失去员工信任—**23.8%**
9. 导致企业加强了对团队/部门的内部审查—**23.5%**

上述数据基于的调查问题：API 安全事件给您的企业带来了哪些成本和/或影响（如果有）？（最多选择 3 项）；受访人数为 1,207 人

从 IT 部门领导者和安全领导者对事件影响的反馈中（每个受访者最多可以选择三个选项），还可以清楚地看到 API 攻击的财务成本和人力成本之间的关系。所有地区不同职位受访者的一个普遍共识是，API 安全事件最大的影响是对员工的影响。

- 从 CISO 报告的两个最突出影响（“损害了部门在高层领导和/或董事会中的声誉”和“失去客户信任和客户流失”）可以看出，认为人力影响最突出和认为财务影响最突出的受访者比例刚好持平，均为 31%。
- 同样，从 CIO 报告的主要影响可以看到，认为“导致团队/部门的压力增加”最明显和认为“修复成本”最明显的受访者比例持平，为 34%。

这些结果对于 CISO 和 CIO 来说不难理解：如果他们领导的团队不断遭遇安全事件，导致工作条件恶劣、预算超支、客户不满，那会怎么样？这些领导者不愿意看到优秀人才流失或者部门声誉一落千丈。再加上修复成本和/或客户流失等造成的财务压力，CISO 和 CIO 承担的压力显著增加。事实上，保险和汽车行业的受访者均认为，“失去客户信任和客户流失”是 API 安全事件的最大影响（请参见下一页的侧栏，了解更多行业调查结果）。

其余职位受访者的热门反馈如下所示：

- CTO，30%，“失去员工信任”
- 资深安全专业人士，27%，“损害了部门在高层领导/董事会中的声誉”
- AppSec 团队，31%，“导致团队/部门的压力增加”

各行业受访者提及最多的 API 安全事件影响	
汽车	失去客户信任和客户流失—**33%**
能源/公用事业	损害了部门在高层领导和/或董事会中的声誉—**36%**
金融服务	持平：导致团队/部门的压力增加和监管机构罚款—均为 **29%**
政府/公共部门	导致团队/部门的压力增加—**29%**
医疗保健	持平：声誉受损和生产力损失—均为 **29%**
保险	失去客户信任和客户流失—**28%**
制造业	导致团队/部门的压力增加—**34%**
零售/电子商务	导致团队/部门的压力增加—**29%**

上述数据基于的调查问题：API 安全事件给您的企业带来了哪些成本和/或影响（如果有）？（最多选择 3 项）；受访人数为 1,207 人

对 API 及潜在风险的监测能力是否足够?

答案是否定的。更确切来说，实际上情况变得更糟了。今年，拥有完整 API 清单并且知道哪些 API 会交换敏感数据的受访者比例从 2023 年已经不高的 40% 下降到了 2024 年的 27%。（如果考虑到更多企业正尝试进行全面清查，只是缺少必要的工具来查找 API 并识别每个 API 中的活动，这个结果可能暗含好的一面。）

拥有完整 API 清单并且知道哪些 API 会交换敏感数据的受访者比例**从 2023 年已经不高的 40% 下降到了 2024 年的 27%**。

API 清单和敏感数据认知的当前状态（所有受访者）

	2024	2023
是，**而且我们知道**哪些 API 会返回敏感数据	27%	40%
是，**但我们不知道**哪些 API 会返回敏感数据	43%	32%
我们拥有部分 API 的清单，**而且我们知道**哪些 API 会返回敏感数据	23%	24%
我们拥有部分 API 的清单，**但我们不知道**哪些 API 会返回敏感数据	6%	4%
否，**我们没有**任何清单	1%	—

上述数据基于的调查问题：您是否拥有完整的 API 清单，是否知道哪些 API 会返回敏感数据？（从五个选项中选择）；受访人数为 1,207 人

在参与调查的三个国家/地区和八个行业的领导者中，CIO 倾向于认为他们的企业拥有完整的 API 清单，而 CISO 的看法相去甚远。在从业人员之中，资深安全专业人士和 AppSec 团队成员与大部分 CIO 的看法基本一致，认为所有 API 都已纳入清单。

但是，对于是否了解哪些 API 在调用时会返回敏感数据，五个职位的受访者有什么样的反馈？答案很重要，因为很多此类调用都来自试图利用常见 API 漏洞的恶意方。

攻击者利用以下四类不受管 API 来获取数据

1. **影子 API**（也称为“未明确记录的 API”）存在并运行于企业官方监控的渠道之外。
2. **恶意 API** 是未经授权或恶意的 API，会对系统或网络构成安全风险。
3. **僵尸 API** 包含被新版本或其他 API 完全取代后仍处于运行状态的任何 API。
4. **已弃用的 API** 是由于 API 发生了变化而不再推荐使用的 API。

从这些反馈结果中，我们可以发现关于 API 风险监测能力的一些有趣事实。大多数 CISO 和 CTO 的反馈表明，他们要么拥有完整的清单但*不知道*哪些 API 会返回敏感信息（我们将知道 API 返回哪种敏感数据称为“具备敏感数据认知”），要么拥有不完整的清单但*具备*敏感数据认知。

大多数 CIO 称他们拥有完整的 API 清单，其中有 42.9% 还表示他们具备完整的敏感数据认知，而 36.3% 表示不具备这种认知。资深安全专业人士与 CIO 的反馈一致（有 75% 表示拥有完整的清单），但在敏感数据认知方面则*刚好反过来*：32.5% 的资深安全专业人士表示他们具备敏感数据认知，而 42.5% 表示他们不具备这种认知。

最后，AppSec 团队成员的反馈（他们大概是所有受访者中亲身实践最多的）提供了所有五个职位中最高的单项比例。有将近一半的人表示他们拥有完整的清单，但不具备敏感数据认知。另一半的情况大致分为以下两类：

- 拥有完整的清单并且完全具备敏感数据认知
- 拥有不完整的清单，但对清单内的 API 具备完全的敏感数据认知

我们可以发现，API 清单的评估还不够标准化，无法形成统一的 API 数量来源。考虑到这种差异，拥有完整清单的更多企业也可能*不具备*充分的敏感数据认知。了解哪些 API 会返回敏感数据始终很重要。然而，清单不完整可能是最危险的，因为影子 API、恶意 API、僵尸 API 和已弃用的 API 缺乏保护，经常成为攻击目标，而且通常会躲过传统安全工具的检查。

API 清单和敏感数据认知的当前状态（按职位细分）。

	CISO	CIO	CTO	资深安全专业人士	AppSec
我们拥有完整清单，**并且知道**哪些 API 会返回敏感数据	17.2%	42.9%	16.5%	32.5%	26.4%
我们拥有部分清单，**但不知道**哪些 API 会返回敏感数据	41.4%	36.3%	34.8%	42.5%	47.4%
我们拥有部分 API 的清单，**而且我们知道**哪些 API 会返回敏感数据	32.5%	15.4%	39.9%	18.3%	20.4%
我们拥有部分 API 的清单，**但我们不知道**哪些 API 会返回敏感数据	8.3%	5.5%	8.2%	5.8%	5.2%

上述数据基于的调查问题：您是否拥有完整的 API 清单，是否知道哪些 API 会返回敏感数据？（从五个选项中选择）；受访人数为 1,207 人

在不受管 API 无序蔓延且传统安全工具难以检测的现状下，这些发现揭示了一个让 API 攻击媒介对攻击者更具吸引力且广泛存在的安全缺口。

当然，安全团队需要检查和评估的 API 不止这一种，而是至少有五种，不受管 API 只是其中一种。这五种 API 包括：

- **存在已知漏洞的 API**，并且这些漏洞尚未修复
- **不受管或被遗忘的 API**（影子 API、恶意 API、僵尸 API、已弃用的 API）
- **暴露到外部网络的 API**（例如具有您无法控制的凭据、密钥和变量）
- **存在操作员错误的 API**（操作员错误是指基础架构和服务中的安全配置错误）
- **存在未发现的漏洞和错误的 API**，这些漏洞和错误可被攻击者发现和利用

从不同职位的受访者对于 API 清单和 API 漏洞监测能力的反馈中，我们至少可以得出这样的结论：

- 企业仍然在使用那些并非专门为发现和保护 API（尤其是高风险、不受管 API）而设计的安全产品。
- 安全部门尚未定义需要检查和评估的 API 风险属性，也尚未在众多业务单位、开发团队和供应商之间就 API 发现和清查策略达成共识。

解决这种脱节问题将会是一个不错的开始，可以成为企业投入更多资本来强化 API 保护能力的有效理由（请参见第 18 页“如何实现更成熟的 API 安全态势”）。就目前的情况而言，API 安全通常缺少获取预算分配所必要的关注和支持，因此安全团队很难确定工作优先级并为相关项目提供资金支持，这些项目不仅可以强化 API 和 Web 应用程序的风险防御能力，还可以改善企业的整体安全态势。

协调统一，筑造更强防线：WAAP + API 专用的保护措施

Web 应用程序和 API 保护 (WAAP) 扩展了 WAF 的传统保护范围，可以快速识别和抵御来自多种攻击媒介的威胁。**API 安全解决方案协同工作，将保护范围进一步扩展到防火墙之外，建立更强大的防御系统。**

API 测试是否足够频繁，可以降低滥用或漏洞风险？

不，还不够频繁。面向公众的 API 如果存在配置错误、缺乏身份验证控制、嵌入了编码错误或者暗藏其他可预防的风险，对于攻击者来说刚好是他们要找的目标，而且攻击者已经越来越擅长找到这些目标。

因此，每次开发团队将这样的 API 投入生产（而没有先进行全面的测试），就相当于无意中给安全团队增加了未来的工作负担（这样的工作无疑都将是紧迫的，并且会给安全团队造成压力，正如调查所发现的那样）。

但是请注意，我们提到了*可预防*的风险。

如果在将 API 发布到生产环境*之前*，通过自动化方式在开发环境中对 API 进行频繁高效的测试，那么企业、开发人员和安全团队都将占得先机。这样做的好处是非常显而易见的，可以降低未知漏洞造成的压力，并确保生产环境中不会出现错误，因为这个阶段一旦出现错误，修复的难度和成本都将成倍增加。

然而，根据受访者的反馈，到目前为止，API 测试并没有任何改观。选择在整个 API 生命周期（包括生产阶段）频繁测试 API （实时和每日）的受访者所占比例相比去年有所减少。

- 2023 年，美国和英国受访者中有 18% 表示他们进行了实时测试。在 **2024 年**的同一组受访者中，**这个数字下降到了 13%**。
- 2023 年，美国和英国受访者中有 37% 表示他们每天至少测试一次。**2024 年，只有 13% 的受访者按照这个频率进行测试**，但德国受访者中有 26% 表示他们每天测试一次。

如果在将 API 发布到生产环境*之前*，通过自动化方式在开发环境中对 API 进行频繁高效的测试，那么企业、开发人员和安全团队都将占得先机。

每周执行一次 API 测试是各个地区受访者最常见的做法，但在任何地区，这个比例都没有达到 50%。此外，API 测试的频率在各个地区也有很大差异，从*实时测试*到*完全不测试*都有。值得注意的是，只有 6% 的受访者称“我们只在发布到生产环境之前测试 API 安全性。”理想情况下，团队将在整个 API 生命周期中持续进行测试。

持续测试 API 意味着什么？

API 生命周期的任何阶段都可能存在漏洞，从开发过程中的编码错误，到用户开始与 API 交互时出现的安全漏洞，都可能出现。因此，理想情况下，应在开发过程中进行 API 测试（左移），并在生产过程中持续测试（右移）。

开发过程中的 API 测试示例如下：

- 运行模拟恶意流量的自动化测试。
- 依据已制定的治理策略对 API 规范进行检查。
- 根据需求进行 API 测试，或者将 API 测试作为 CI/CD 管道的一部分。

生产过程中的 API 测试示例如下：

- 持续监控 API 流量并评估流量元数据。
- 通过自动分析识别现有 API 中的变化。
- 实时发现问题并在攻击者察觉之前解决问题。

您的 API 安全协议是否满足合规要求？

许多数据保护法规均未提及 API，但法规要求明确侧重于应用程序和基础架构（API 运行环境）的保护。合规要求一直在不断变化，更多与 API 相关的法规已在制定中，其中包括《美国隐私权法案》（目前为草案）和《欧盟网络弹性法案》。

目前对 API 安全有直接影响的法规和框架包括：

- PCI DSS（当前版本为 4.0.1）
- 《通用数据保护条例》(GDPR)
- 《数字运营弹性法案》(DORA)
- 《健康保险流通与责任法案》(HIPAA)
- 《网络和信息安全 (NIS2) 指令》

API 安全受到关注，但仍缺乏足够重视

如果说 API 攻击会造成巨大的代价并招致罚款，还会导致客户信任度下降、员工压力增加、企业董事会信任度下降等一系列问题，为什么安全团队没有采取更果断的行动？受访者对以下几个问题的反馈可以帮助我们理解这一点。

企业内不同职位的人员如何看待 API 安全的重要性？

我们邀请了受访者确定未来 12 个月内网络安全方面的主要优先事项，让他们从一份详尽的列表中选择最多三项（请参见侧栏）。对于提及最多的前六个优先事项，受访者比例只相差 2%，而提及后六个优先事项的受访者比例只相差 1%。这表明不同地区和行业对于网络安全优先事项的看法相似，而且安全团队经常不得不兼顾所有这些优先事项。

但是，在某些行业，API 排位的差异却说明了另一种情况。例如，相比所有其他行业，能源/公用事业部门最不重视 API 安全，只有 13.2% 的受访者将 API 安全列为优先事项（低于所有调查受访者 18% 的平均比例）。与此同时，能源/公用事业部门报告 API 安全事件的比例却是所有八个行业中最高的，为 91%，高于 84% 的平均水平。这说明什么？对 API 安全重视不足，攻击率就高。

受访者提及最多的未来 12 个月安全优先事项

1. 防御生成式 AI 辅助的攻击—21.2%
2. 防御勒索软件—20.5%
3. 确保员工用户身份验证的安全—19.7%
4. 管理和保护开发人员机密信息—19.6%
5. 保护端点的安全—19.2%
6. 云安全解决方案—19.1%
7. 保护 IT 特权访问的安全—18.6%
8. 防范数据丢失—18.6%
9. 保护 API 免受攻击—17.9%
10. 保护应用程序的安全—17.7%
11. 安全信息与事件管理—17.6%
12. 事件响应和管理—17.6%

上述数据基于的调查问题：未来 12 个月，您的企业在网络安全方面有哪些主要优先事项？（请选择最多 3 项）；受访人数为 1,207 人

按照职位进行细分之后，我们得到了更能说明问题的数据：

- CISO 认为生成式 AI 辅助的攻击和 API 保护的优先级最高，持此观点的受访者占比分别为 **25.5%** 和 **24.8%**。
- AppSec 团队成员与 CISO 保持一致，认为生成式 AI 辅助的攻击优先级最高，持此观点的受访者占比为 **22.5%**。
- CIO 和 CTO 都看重特权访问，而 CTO 还同样看重事件响应。
- 将勒索软件列为最高优先级的只有资深安全专业人士。

这些差异再次引发我们的疑问：为什么 IT 安全企业的不同层级似乎都在各行其是？为什么高层安全领导者和一线员工似乎对 API 在生成式 AI 辅助的攻击中扮演的重要角色及其风险有一致看法，而其他职位的人员并非如此？

这也许是因为 CISO 认识到业务部门为满足需求而匆忙推出各种创新产品，例如生成式 AI 驱动的应用程序等，而 AppSec 团队成员也注意到同样的情况；只有*他们*知道，涉及敏感数据的 AI 组件（例如 LLM）究竟潜藏多少未知的漏洞。除此之外，AppSec 团队可以第一时间发现许多警告信号，这些信号暗示攻击者正在将生成式 AI 融入到攻击方法中。

但主要原因可能也是最简单的原因：自上而下和自下而上的沟通不够频繁（尤其是在大型企业中），导致高层领导者的优先事项与一线团队每天*必须*处理的优先事项之间出现脱节。

最后，我们来将受访者提出的网络安全主要优先事项与他们认为的 API 安全事件原因进行比较。如第 17 页所示，他们提及最多的三个原因都涉及传统应用程序安全工具无法检测 API 问题。通过比较，我们可以借此展开讨论，了解为什么 API 发现和测试解决方案不仅可以增强企业 API 安全性，还可以为他们的几乎所有安全优先事项提供辅助。

换句话说，如果合适的 API 安全工具不仅可以保护 API，还可以提高数据、云和应用程序等领域的安全性，那么 API 安全在利益相关者眼中就不再是一个孤立的小众领域。从大局出发会更容易获得认可，从而将 API 列入优先事项列表中。

如果合适的 API 安全工具不仅可以保护 API，还可以提高数据、云和应用程序等领域的安全性，那么 API 安全在利益相关者眼中就不再是一个孤立的小众领域。

对 API 安全事件的看法不一是否表明企业没有统一的权威信息来源?

我们前面分析了首席高管层与一线员工在安全优先事项方面的总体差异，在更具体的 API 威胁问题中，这些差异依然存在。例如，就 API 攻击的认知而言，CIO 与 AppSec 团队表现一致（每个职位约有 88% 的人报告称经历过 API 安全事件）。相比起来，CISO、CTO 和资深安全专业人士的这一比例全都低大约八个百分点，约有 80% 的人报告称经历过 API 安全事件。

不同职位受访者提及最多的 API 安全事件原因也各不相同，大多数 CISO 和资深安全专业人士认为是因为 API 网关没有进行拦截，而其他三个职位的受访者分别指出了不同的原因：

- CISO：API 网关没有进行拦截—**26.8%**
- CIO：意外暴露到互联网—**28.6%**
- CTO：WAF 没有进行拦截—**25.9%**
- 资深安全专业人士：API 网关没有进行拦截—**23.3%**
- AppSec 团队：API 配置错误—**23.2%**

所有受访者提及最多的 API 安全事件原因

1. API 意外暴露到互联网—21.8%
2. Web 应用程序防火墙没有进行拦截—21.8%
3. API 网关没有进行拦截—20.2%
4. LLM 等生成式 AL 工具/技术的 API—20.0%
5. API 配置错误—19.9%
6. 网络防火墙没有进行拦截—19.6%
7. 微软等知名的技术工具/服务—19.2%
8. API 编码错误导致的漏洞—19.1%
9. 不受管 API，例如休眠 API 或僵尸 API—18.9%
10. API 身份验证控制缺失—18.8%
11. 授权漏洞—18.7%
12. 从互联网下载的软件解决方案—17.6%
13. 中层软件解决方案，例如 Slack—16.3%

上述数据基于的调查问题：您认为您所在的企业发生 API 安全事件的原因是什么？（最多选择 3 项）；受访人数为 1,207 人

受访者报告的 API 安全事件成本也显示出从上到下不同职位的认知不一致，但必须指出的是，按职位*和*地区进行细分必然会导致样本量变小。不过，各子集中存在的差异仍然值得注意，尤其是在美国，CIO 和 CTO 报告的成本约为 100 万美元，CISO 报告的成本约为 73.7 万美元，而资深安全专业人士和 AppSec 员工报告的成本分别为大约 37.5 万美元和大约 44.4 万美元。

在英国，不同职位的受访者报告的成本总体上更一致，但 AppSec 团队成员报告的成本最高，为 74.9 万英镑，而 CISO 报告的成本最低，为 19 万英镑。（中间职位报告的成本最高为 37.4 万英镑，最低为 22.2 万英镑。）德国受访者报告的成本差异与英国相似，职位最低、亲身实践最多的员工报告的数据最高，为 34.5 万欧元，而职位最高的 CISO 报告的成本最低，为 19.7 万英镑（与美国的调查结果相反）。所有地区不同职位受访者的一个普遍共识是，API 安全事件的最大影响是对员工的影响（请参见第 7 页关于“影响”的数据）。

如何实现更成熟的 API 安全态势

如前所述，我们的研究结果表明，企业不同层级的安全团队成员对 API 安全的看法明显各不相同。但另一方面，他们之间很显然也存在一些共识。他们知道 API 事件的成本（财务和人力成本），也承认目前使用的工具不能满足需求。

鉴于 API 安全对企业有如此大的影响，接下来您不妨先确定哪些方面需要加强、哪些方面需要改变，并向领导者证明保护 API 安全可以帮助提高盈利水平。您可以在安全部门内从 CISO 到 AppSec 团队建立起关于 API 安全优先级的共识，这是一个不错的开始。然后进一步促进领导层与一线 AppSec 团队成员以及中间管理层的开放式沟通。

可以采取的措施

在报告的结尾，我们整理了一系列渐进的措施，安全团队可以参考这些措施来启动或强化 API 安全策略，建立成熟的 API 保护机制。

1 从 API 发现和监测能力入手

为了对所有 API 资产进行全面清查，您需要寻找能够用自动化方法发现 API 及其支持的微服务的工具。覆盖范围的广度至关重要，因为不受管 API（请参见第 10 页的侧栏）是攻击者的主要目标。

2 完善 API 测试

选择一种 API 安全解决方案，让您能够轻松测试 API 是否有编码措施，是否可以发挥预期作用。理想的做法是在部署之前进行测试，但对生产环境中的所有 API 进行测试也很重要，包括对流量进行实时分析，来识别潜在的漏洞。

3 对 API 进行充分记录

审核整个 API 环境以识别 API 配置错误或其他错误非常重要。审核过程还应确保对每个 API 进行充分记录，并确定 API 是否包含敏感数据或缺乏适当的安全控制。这也有助于您做好必要的准备，确保满足与 API 安全直接或间接相关的合规要求（请参见第 14 页）。

4 使用运行时检测工具

利用 API 安全解决方案的自动运行时检测功能，您将能够区分“正常”和“异常”的 API 活动。通过这种方式监控 API 交互，您可以实时检测威胁行为并采取行动。

5 应对可疑行为

通过将 API 安全解决方案与现有的安全产品组合（例如 WAF 或 WAAP）进行集成，您将能够发现高风险行为并在可疑流量抵达关键资源之前进行拦截。

6 调查和搜寻威胁

在 API 安全防护更为成熟的阶段，您将能够对过往的威胁数据进行取证分析，了解系统是否正确识别不同的威胁并触发相应的告警，并确认是否出现了新型攻击模式，然后使用先进的工具结合人类智慧，主动搜寻未来可能出现的威胁。

结论

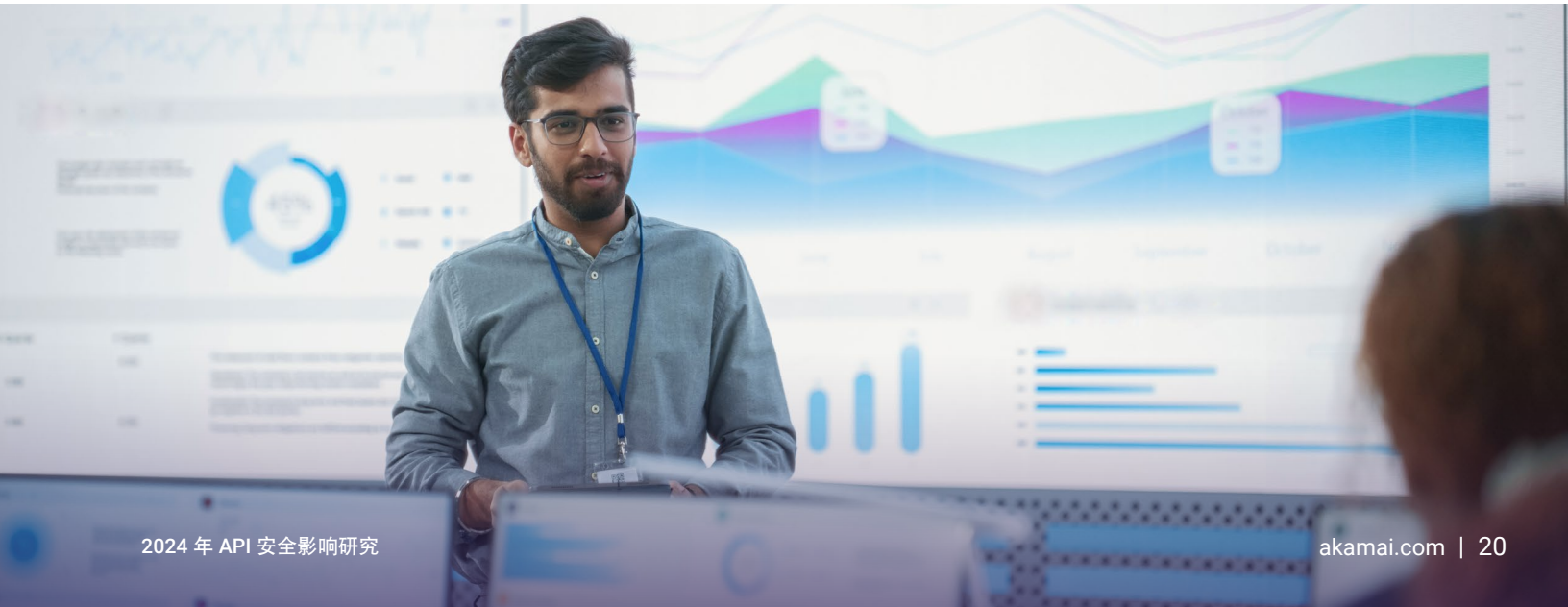
今年的报告明确指出，网络安全（本报告中具体指 API 安全）不仅仅涉及威胁列表或工具，还与人为因素息息相关。

我们的研究证实，安全团队已经不堪重负，从团队的工作负担来讲，增加一种全新的攻击媒介似乎让人难以接受。但 API 的激增不会停止，而且采取 API 保护措施可以对其他许多高优先级事项产生显著的协同效应。例如对于生成式 AI 漏洞，可以保护与 LLM 交换数据的 API；对于云安全，可以降低迁移的工作负载中每个 API 的风险。

我们深信，积极主动地对待 API 安全不仅可以保护企业，还可以让安全团队在同行、领导者和董事会眼中更加可靠和可信，能够就这一关键攻击媒介达成一致观念并获得相关支持。这对于减轻团队的压力大有益处，因为根据调查结果，API 安全事件及其引发的审查，以及在同事和客户中的信誉损失，都会给团队带来严重的影响。

现在采取措施还可以提前减轻合规计划和报告的工作量，更不用说及时避免监管机构罚款了。不如现在就开始着手吧？

- 如果您已准备好为建立成熟的 API 安全态势迈出第一步，建议您先阅读我们的《API 安全基本现状》白皮书。
- 如果您准备探讨目前面临的挑战和我们能够提供的帮助，只需申请 Akamai API Security 定制化演示，操作很简单。



API 安全影响研究介绍

2024 年 API 安全影响研究由 Opinion Matters 在 2023 年 6 月 12 日至 2024 年 7 月 7 日期间完成。该公司的团队共调查了 1,207 名受访者，按其公司所在地细分如下：404 名来自英国，402 名来自美国，401 名来自德国。三分之一的受访者是 CIO 或 CISO；三分之一是资深安全专业人士；三分之一来自应用程序安全团队。这些受访者就职的公司规模从 500 人以下到 1,000 人以上不等，业务涉及八个重点行业：汽车、金融服务、零售/电子商务、医疗保健、保险、政府/公共部门、制造业以及能源/公用事业。

Opinion Matters 遵守市场研究协会的规定并聘用协会成员，遵守 MRS 行为准则和 ESOMAR 原则。Opinion Matters 也是英国民意调查委员会的成员。

致谢名单

主笔人
Annie Brunholzl

总编辑
John Natale

研究总监
Mitch Mayne

文稿编辑
Randi Kravitz

推广
Barney Beal

营销与发布
Georgina Morales Hampe

审稿和主题撰稿
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

互联网现状/安全性

《互联网现状/安全性》报告由 Akamai 精心呈献，获得了各界的广泛赞誉。请前往以下网址回顾往期报告，并关注即将发布的新报告：**akamai.com/soti**

Akamai 威胁研究

关注最新的威胁情报分析、安全报告和网络安全研究的动态。**akamai.com/security-research**

Akamai API Security

了解 Akamai 如何利用 API 发现、态势管理、运行时保护和 API 安全测试等关键功能，在 API 的整个生命周期（从开发到生产）保护 API 安全。
https://www.akamai.com/products/api-security