API

安全

影响

研究

2025

API 攻击给亚太四国造成的成本支出分析

中国、日本、印度和澳大利亚的安全团队如何看待遭入侵 API 带来的影响

Akamai

Akamai《互联网现状》(SOTI) 报告的姊妹篇

目录

前言

随着应用程序编程接口 (API) 的广泛应用，针对 API 的攻击变得日益频繁、复杂且规模越来越大。事实上，Akamai 在最近发布的《互联网现状》(SOTI) 报告中指出，**从 2023 年 1 月到 2024 年 6 月期间总计记录到了 1080 亿次 API 攻击**。

然而，虽然企业中 API 的数量快速激增，且其中许多都需要访问敏感数据，但研究显示，大多数安全团队并未将保障 API 的安全视为重中之重。企业普遍难以全盘了解 API 及其风险，而研究发现也恰好印证了行业担忧——企业在 API 安全保护方面缺乏统一的负责机制，从跟踪漏洞到衡量数据泄露影响都存在责任不清的问题。

为了解亚太地区 (APAC) 四大经济体的 API 安全现状，最新一期的《API 安全影响研究》收集了该地区 800 多名网络安全从业人员的反馈：中国、印度、日本和澳大利亚。此研究基于 Noname Security（现为 Akamai Technologies 的子公司）进行的一项年度调查，该调查旨在了解安全专业人员在过去三年里如何将 API 纳入其安全计划。结果一如既往，我们的研究发现，尽管人们对 API 漏洞的认识不断提高，但高层领导对 API 安全的重视程度并未相应地提升，因为首席信息安全官 (CISO) 和首席信息官 (CIO) 们都疲于应付日益增多且相互冲突的优先事项。

2024 年，**《API 安全影响研究》**将其传统的调研范围从美国和英国的企业扩大到了德国的企业。该研究发现：

- API 安全事件已连续第三年呈上升趋势。
- 据估计，应对这些事件的成本平均超过了 50 万美元（IT 和安全负责人表示，该成本已接近 100 万美元）。
- 大多数受访者认识到了这些事件给安全团队带来的压力和声誉损失。

这项调查的受访者包括以下八个行业的企业高管（CISO、CIO 和首席技术官）、资深安全人员以及应用安全团队成员：

- 汽车
- 保险
- 金融服务
- 政府/公共部门
- 零售/电子商务
- 制造
- 医疗保健
- 能源/公用事业

调查结果揭示了有关 API 安全实践和优先事项的宝贵见解，包括：

- API 安全事件的原因
- 整体网络安全优先事项
- 与 API 安全事件相关的成本，例如罚款和修复费用
- API 安全事件对安全团队的影响
- API 清点和测试实践的状态
- 对哪些 API 会返回敏感信息的认知
- API 安全在监管合规工作中的现状

什么是 API 安全事件?

安全事件可能包括 API 滥用、API 攻击、以 API 为中心的数据泄露，以及恶意攻击者破坏 API 的所有尝试。

内容提要

这项调查的结果为亚太地区和多个行业的安全团队及领导层提供了宝贵的见解，但一些宏观趋势尤为突出。

1. **中国正将 API 安全作为网络安全战略的重要组成部分。**相较之下，其他地区可能并未对 API 安全给予足够重视。中国的受访者将“保护 API 免受攻击”列为其第一要务。在《2024 年 API 安全影响研究》中，来自美国、英国和德国的受访者将“保护 API 免受攻击”列为其第九大优先事项，排在“防范生成式 AI (GenAI) 驱动的攻击”和“防范勒索软件”等其他优先事项之后。据估计，过去 12 个月内中国在解决 API 安全事件上花费的成本也是最高的，达到了 5,687,373 元人民币（778,271 美元*）。

> “保护 API 免受攻击” | 对于中国受访者来说，这是未来 12 个月内的第一大网络安全优先事项

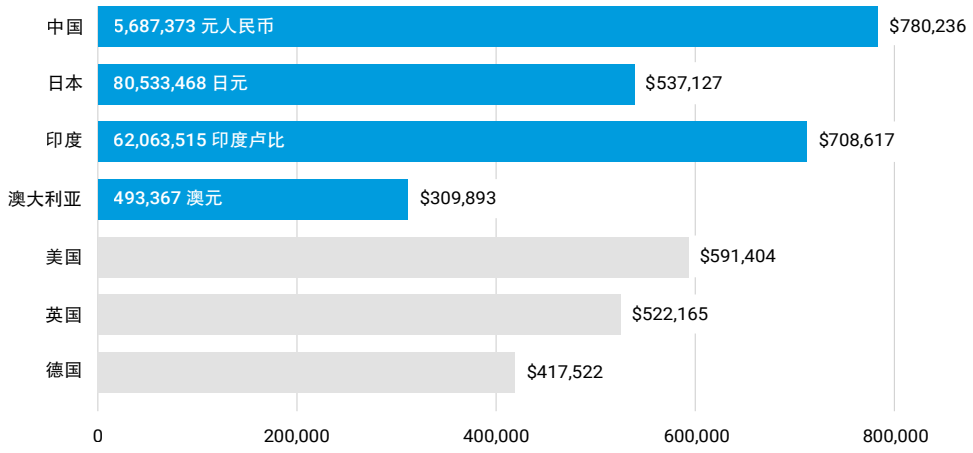
2. **关键的企业角色之间仍然存在脱节问题。**调研结果因角色、国家及行业而异，但总体上呈现出一条明确的信息：在对 API 安全事件造成的成本支出、原因和企业影响的理解以及企业对 API 的了解上，高管层、资深安全专业人员和应用安全团队存在分歧。

例如：

- 中国的高管层受访者估计 API 安全事件造成的成本支出几乎是其他角色所估计的两倍。
- 在日本，企业内各角色之间未就企业所经历的 API 安全事件的主要原因达成一致意见。
- 在印度，表示拥有完整 API 清单的高管层 (77%) 和资深安全专业人员 (75%) 远多于应用安全团队 (41%)。
- 总体来看，92% 的高管层受访者表示其企业在过去 12 个月内经历过 API 安全事件，而应用安全团队中持有相同看法的比例为 80%。

*所有货币换算截至 2025 年 3 月 27 日

如果您经历过 API 安全事件，这些事件造成的累计财务损失的估计总额是多少？
过去 12 个月解决 API 事件的平均估计成本

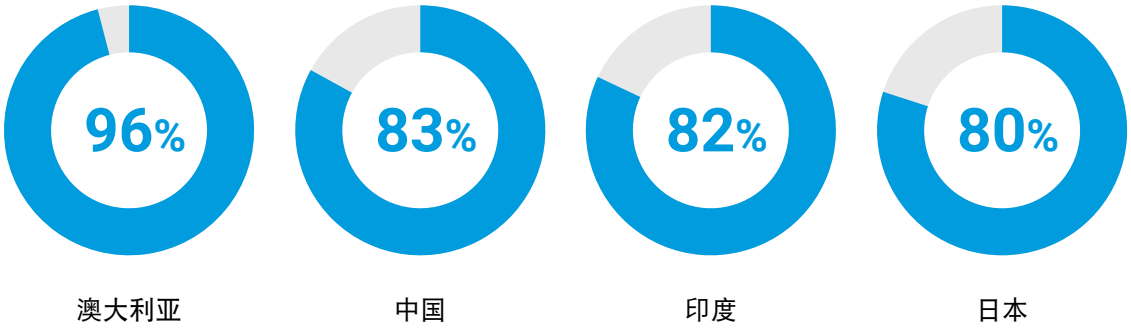


3. **API 安全事件的影响并不局限于占据绝对主导地位的单一事件。**相反，调查结果表明，API 攻击和滥用的影响既深远又广泛。受访者对主要影响的看法有所不同，这与他们的角色和所在地区相关。一些人认为财务影响（例如，修复安全团队未预见到的 API 攻击的成本）是最重要的影响，而其他人将遭受攻击之后的信任损失（例如，在董事会中的声誉受损）视为最大影响；日本的受访者将此项列为头号影响。

> “损害了部门在高层领导和/或董事会中的声誉。”

日本受访者表示，这是 API 安全事件的最大影响

4. 这四个国家的企业目前正面临着频繁发生的 API 安全事件。



这些结果与我们上一份报告中的结果高度吻合。在上一份报告中，来自美国、英国和德国的受访者中 84% 的人表示他们在过去 12 个月内经历过安全事件。

中国、日本、印度和澳大利亚的 API 安全事件影响排名

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）*

地区趋势概况

虽然这四个国家在监管、政治和经济上存在显著差异，但这些结果确实为了解 API 安全防护计划的总体成熟度提供了宝贵见解。该研究的结果也为专业人员制定自己的 API 安全优先事项提供了有用的基准数据。显而易见，攻击者的目标正在转向 API。在 **2024 年有关 API 安全的《互联网现状》报告：攻击趋势揭示了 API 威胁**中，Akamai 指出 API 攻击正在成为亚太地区日益令人担忧的问题。Akamai 研究发现，亚太地区的所有 Web 攻击中有 15% 以 API 为目标。在全球范围内，亚太地区受到的 API 攻击占比位列第三，仅次于欧洲、中东和非洲地区 (EMEA) 的 48% 和北美地区的 27%。

在企业做好准备应对这一不断增长的攻击媒介的挑战时，这些调查结果证明，高层管理人员和一线员工需要就重要的基准问题达成共识，如他们所面临的 API 安全事件的数量、其根本原因以及与之相关的利润和声誉损失成本。

API 安全有多重要?

对于中国来说，API 安全是第一要务。在调研中，所有受访者都需要对明年的网络安全优先事项进行排序。作为世界第二大经济体，中国在这个问题上的回答有些与众不同，也是唯一一个将“保护 API 免受攻击”列为第一要务的国家。

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？（最多选择 3 项）

中国

1. 保护 API 免受攻击 —— 27.6%
2. 保护 IT 特权访问的安全 —— **24.6%**
3. 保护应用程序的安全 —— **24.1%**
4. SIEM ——**24.1%**
5. 防止数据丢失 ——**22.2%**

日本

1. 防御勒索软件 —— **25.5%**
2. SIEM —— **25.5%**
3. 防止数据丢 失—— **25.0%**
4. 保护 API 免受攻击 —— 22.0%
5. 保护应用程序的安全 —— **22.0%**

印度

1. 云安全解决方案 —— **26.9%**
2. 管理和保护开发人员机密信息 —— **24.9%**
3. 保护应用程序的安全 —— **23.4%**
4. 保护 API 免受攻击 —— 22.9%
5. 保护 IT 特权访问的安全 —— **29.9%**

澳大利亚

1. 保护端点的安全 —— **26.2%**
2. 管理和保护开发人员机密信息 —— **24.3%**
3. SIEM —— **23.8%**
4. 保护 API 免受攻击 —— 22.8%
5. 防止数据丢失 —— **22.8%**

中国对 API 的关注可能源于中国安全人员估计的 API 安全事件所造成的成本支出：

- 资深安全专业人员：6,733,916 元人民币（924,000 美元）
- 应用安全团队：6,622,503 元人民币（920,000 美元）

在其他几个国家中，“保护 API 免受攻击”仅位列第四大优先事项。总体而言，“保护 API 免受攻击”位列第二，仅次于安全信息和事件管理 (SIEM)。

几乎未就成本达成共识

虽然中国的资深安全专业人员（6,733,916 元人民币或 925,478 美元）和应用安全团队（6,622,503 元人民币或 910,166 美元）估计的 API 安全事件所造成的成本支出较高，但公司高管层估计的成本支出要低得多（平均为 3,750,897 元人民币或 517,293 美元）。在日本和印度，角色之间也存在这种差异，但澳大利亚除外。不过，这种差异并非只存在于高管层与一线员工之间。例如，在日本，资深安全专业人员估计的成本支出最高，而应用安全团队估计的成本支出最低。角色之间的这种差异表明，在 API 安全事件给企业造成的损失上缺乏共识。它也说明了这些角色在确定 API 安全的优先级方面存在脱节问题。如果这些角色无法在 API 安全事件对企业的财务影响上达成一致，API 安全便无法在优先事项列表中排名前列。

企业认识到 API 安全事件正在发生，但不清楚其发生频率

在 API 安全事件的频率上，也存在脱节问题。以前在其他地区进行的 API 安全影响研究表明，这些地区的安全事件数量随时间的推移呈稳步增长态势。但由于没有中国、日本、印度和澳大利亚往年的相关数据可供比较，因此无法衡量 API 安全事件在这些国家的增长程度。尽管如此，很显然各企业都意识到了这种威胁。总体来看，85% 的受访企业表示他们在过去 12 个月内经历过 API 安全事件，其中澳大利亚的发生频率最高，达到了 95%。

中国、日本、印度和澳大利亚的 API 安全事件发生率

总体来看，85% 的企业表示他们在过去 12 个月内经历过 API 安全事件，其中澳大利亚的发生频率最高，达到了 95%。

这些结果也表明，领导层与一线员工在对 API 安全事件发生频率的理解上存在差距。总体来看，92% 的高管层受访者表示他们在过去 12 个月内经历过 API 安全事件，而安全专业人员和应用安全团队中持有相同看法的比例分别为 83% 和 80%。在一些国家（特别是中国），这一差距更大，其中 97% 的高管层受访者表示经历过安全事件，而安全专业人员和应用安全团队中持有相同看法的比例分别为 78% 和 74%。

API 安全事件的影响广泛

针对脆弱的 API 的攻击会对整个企业产生深远影响，这些影响并不仅仅是与修复 API 相关的成本，还包括对企业公众声誉的损害。攻击的影响还可能包括监管罚款、失去客户（即客户流失）和内部声誉损失，以及安全团队员工面临的压力增大（美国、英国和德国的受访者选择的最主要影响）。

这些结果表明，亚太地区这四个国家的企业在很多方面都感受到了攻击带来的影响。当被问及 API 安全事件给其企业带来的成本支出和影响时，这四个国家的受访者并未指出一个占据绝对主导地位的单一因素。而当被要求提供最多三项成本支出或影响时，他们给出了三个答案：“为帮助解决问题而产生的成本”成为最主要的因素 (29.5%)，紧随其后的是“导致团队/部门的压力增加”(29.2%) 和“失去客户信任和客户流失”(28.8%)。在其他选项中，“失去员工信任”(20.7%) 的得分最低，其次是“未产生任何成本和/或影响”(2.1%)。

API 安全事件的原因不明确

受访者表示，“API 错误配置”是最可能导致发生 API 安全事件的原因，也是澳大利亚和印度的受访者选择最多的原因以及中国的受访者选择第二多的原因。但是，在所有四个国家受访者的回答中，并没有哪一种 API 漏洞比其他漏洞更突出。在总体结果中，当受访者被要求选择最多三项答案时，“API 错误配置”(22.3%) 排在首位，其次是“网络防火墙没有进行拦截”(20.8%)、“API 网关没有进行拦截”(20.7%) 和“授权漏洞”(20.6%)。

前六项答案彼此之间的差距只有几个百分点。这表明，企业认识到 API 漏洞持续存在于各种媒介中，并且企业的 API 安全工作中存在普遍的弱点。以下是面向安全团队的要点：

- 共同关注 API 错误配置可能是合理的。安全错误配置是广受关注的 OWASP 十大 API 安全风险清单中的第八大风险，可能会导致失效的对象级授权（OWASP 的第一大风险）、失效的身份验证（OWASP 的第二大风险）以及过度数据暴露（OWASP 的第三大风险）等漏洞。
- 常用的安全工具（例如，网络防火墙、Web 应用程序防火墙 [WAF]）并非为应对日益增长的复杂攻击而设计，它们的广泛使用也可能令人担忧。虽然这些工具提供了基本保护，但瞬息万变的 API 攻击方法需要更全面的 API 安全防护。

中国、日本、印度和澳大利亚的 API 安全事件原因排名

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）*

在调查范围内的亚太地区四个国家的总体调查结果

API 错误配置	**22.3%**
网络防火墙没有进行拦截	**20.8%**
API 网关没有进行拦截	**20.7%**
授权漏洞	**20.6%**
API 意外暴露到互联网	**19.6%**
大语言模型 (LLM) 等生成式 AI 工具中的 API	**19.2%**
API 编码错误导致的漏洞	**18.7%**
中层软件解决方案 (Slack)	**18.7%**
API 身份验证控制缺失	**18.1%**
Web 应用程序防火墙没有进行拦截	**17.5%**
不受管 API，例如休眠 API 或僵尸 API	**16.6%**
从互联网下载的软件解决方案	**16.3%**
知名的技术工具/服务（Microsoft 等）	**15.8%**
我们从未经历过 API 安全事件	**2.6%**

N = 806

对 API 中敏感数据的认识

总体来看，超过 70% 的受访者表示他们拥有完整的 API 清单。但是，知道其中哪些 API 会返回敏感数据比较困难。只有 37% 的受访者声称拥有完整清单并且知道哪些 API 会返回敏感数据。这些结果也因角色不同而存在很大差异。44% 的高管层受访者表示，他们知道哪些 API 会返回敏感数据（但这一比例在 CISO 中降至 31%），而对于应用安全团队和资深安全专业人员，这一比例分别为 37% 和 28%。

在日本，应用安全团队的受访者声称知道哪些 API 会返回敏感数据 (64%)，这一比例远高于高管层受访者或资深安全专业人员 (24%)。考虑到攻击者可以轻而易举地向 API 发送欺骗性调用并获取敏感数据，安全团队在这个领域中绝对不能容忍各角色之间存在分歧。

API 漏洞延伸到 AI 领域

在所有这四个国家中，将 API 安全事件归咎于企业生成式 AI 技术漏洞的 CIO 人数是 CISO 的三倍。

他们的担忧不无道理。

企业部署的 AI 应用程序和 LLM，往往需要依赖 API 来实现缺失的功能、集成以及交换数据。攻击者可通过以下手段来利用 AI 安全漏洞：

- 提示注入攻击：攻击者操纵 AI 生成的回答来泄露敏感数据或绕过安全措施。
- 数据外泄和模型窃取：攻击者可以尝试从 AI 模型中提取专有知识。

只有 37% 的受访者表示他们知道哪些 API 会返回敏感数据，因此对于 IT 和安全负责人来说，应将日益增长的针对生成式 AI 应用程序和 LLM 的威胁视为高优先级事项。

在调查范围内的所有四个国家中，将生成式 AI 漏洞视为 API 安全事件首要原因的前三大行业是：

1.政府/公共部门　2.能源/公用事业　3.保险

按国家细分

中国将 API 安全放在首位

在明年的网络安全优先事项方面，中国对 API 安全的高度重视在调查范围内的四个国家中最为显著。在所有回答中，“保护 API 免受攻击”获得了最高分，27% 的中国受访者将其列为第一要务。“保护 IT 特权访问的安全”紧随其后，是能源/公用事业、金融服务、制造、汽车和医疗保健行业的第一要务。

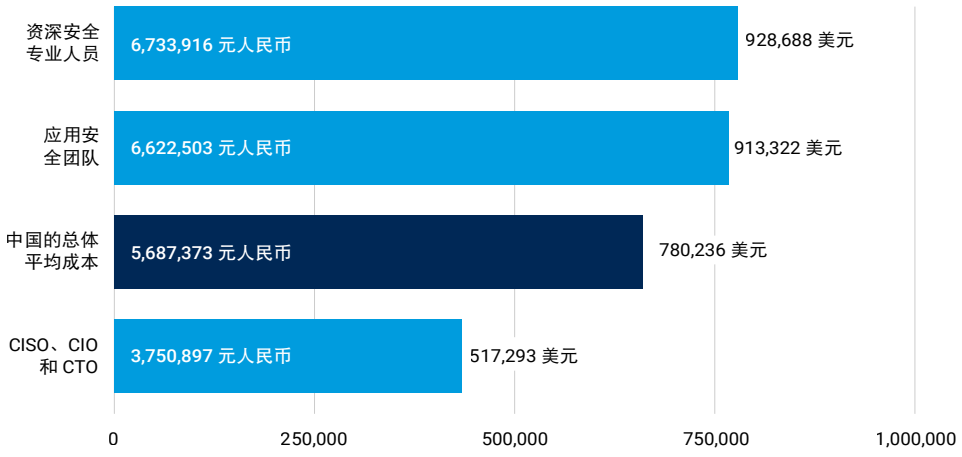
从这些结果来看，中国在 API 测试方面也处于领先地位，这也许并不令人感到意外。超过半数的中国受访者表示，他们会进行实时测试 (22%) 或每天进行测试 (28%)。在应用安全团队中，这一数字高达 65%。这种对测试的专注非常重要。企业认为是安全事件起因的很多 API 漏洞都可以在开发人员团队向公众发布 API 之前被发现并加以修复。

中国企业的高层领导认为 API 安全事件在过去一年中是一个显著的问题。几乎所有高管层受访者 (97%) 都表示经历过 API 安全事件，这比一线员工的报告比例高出 20 个百分点。零售业是去年安全事件发生率最高的行业，100% 的企业都表示经历过安全事件，而保险业的事件发生率最低，仅为 72%。

但是，高管层认为事件产生的成本比一线员工所认为的要低得多。

在中国，97% 的 CISO、CIO 和 CTO 表示经历过 API 安全事件，这比高管层和一线安全人员的报告比例高出 20 个百分点。

如果您经历过 API 安全事件，这些事件造成的累计财务损失的估计总额是多少?
中国的安全负责人和从业人员估计的 API 安全事件成本支出



在 API 安全事件的最大影响方面，中国的受访者之间存在一些分歧。应用安全团队认为最大的是财务影响，而高管层受访者将其团队所面临的压力列为最大影响。考虑到高管层受访者估计的 API 安全事件相关成本最低，这可能并不让人感到意外。值得一提的是，只有汽车、政府/公共部门及保险业将“为帮助解决问题而产生的成本”列为最大影响。

与此相符的是，在对哪些 API 会返回敏感数据的掌握方面，高管层 (53%) 比公司从业人员的看法要积极得多（资深安全专业人员：25%；应用安全团队：40%）。这些角色在是否拥有完整的 API 清单方面的看法基本一致。

对于 API 安全事件，中国受访者所报告的主要原因包括：

- “网络防火墙没有进行拦截”
- “API 错误配置”
- “API 网关没有进行拦截”

尽管有很多中国受访者称会进行实时测试，但紧随上一原因的是位列第四的“API 编码错误导致的漏洞”。共有 50% 的零售/电子商务受访者将“网络防火墙没有进行拦截”列为安全事件的主要原因，这是中国各行业中达成共识度最高的。在其他行业中，只有大约 40% 或更少的受访者提到了主要原因，并且这些行业的受访者将原因归咎于 API 自身固有的问题，例如 API 错误配置。在未来 12 个月的网络安全第一要务方面，中国零售/电子商务行业的受访者也展现出了更高的共识度，有 50% 的人选择了“防止数据丢失”。

您是否知道哪些 API 会返回敏感数据?

拥有完整 API 清单的中国受访者中，只有 39.4% 的人表示知道哪些 API 会返回敏感数据。在对这些重要的 API 风险因素的掌握方面，高管层受访者比公司从业人员的看法要积极得多：

- CISO、CIO、CTO：53%
- 资深安全专业人员：25%
- 应用安全团队：40%

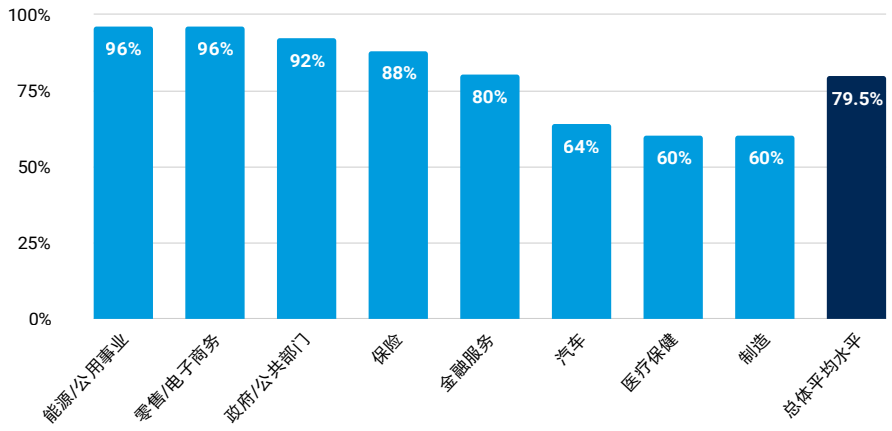
日本对 API 的重视程度较低，而其国内大量使用 API 的行业发生的安全事件较少

在日本“保护 API 免受攻击”是第四大安全优先事项，排在“抵御勒索软件”、“SIEM”和“防止数据丢失”之后。但是，“保护 API 免受攻击”对于资深安全专业人员来说更为重要，他们将此项与“抵御勒索软件”并列为自己的第一要务。“保护 API 免受攻击”也是日本汽车行业的第一要务，这是一个重要的数据点，因为该行业中只有 8% 的受访者表示知道哪些 API 会返回敏感数据。

令人感到意外的是，虽然大约 80% 的日本受访者表示在过去 12 个月内经历过 API 安全事件（远低于中国受访者的数据），但日本大量使用 API 的行业（如汽车、医疗保健和制造业）中只有 60% 的受访者表示经历过安全事件。在角色方面，高管层与应用安全团队的看法一致，他们中大约有 83% 的受访者表示经历过安全事件。

您是否在过去 12 个月内经历过 API 安全事件?

日本各行业的表现与全国的总体平均水平相比如何



与其他国家相比，日本的受访者中将安全工具视为安全事件主要原因的人数较少，更多的受访者选择了外部工具。“从互联网下载的软件解决方案”(22%) 是报告最多的原因，而“中层软件解决方案 (Slack)”位列第四 (21%)。有意思的是，“知名的技术工具/服务（Microsoft 等）”位列最后 (15%)。

日本受访者估计的 API 安全事件成本支出：

- 总体而言：80,500,000 日元（528,000 美元）
- 高管层：74,000,000 日元（485,000 美元）
- 医疗保健：33,216,389 日元（218,000 美元）
- 资深安全专业人员：115,000,000 日元（754,000 美元）
- 应用安全团队：56,000,000 日元（367,000 美元）
- 汽车：228,000,000 日元（1,500,000 美元）

在日本，应用安全团队成员最能感受到 API 安全事件的内部影响。“损害了部门在高层领导和/或董事会中的声誉”是应用程序安全小组中选择最多的结果，而“导致企业加强了对团队/部门的内部审查”位列第三。“导致团队/部门的压力增加”位列第四。

对日本的受访者来说，第二大影响涉及公司的外部声誉受损，即“失去客户信任和客户流失”。而这不仅仅存在于企业中。日本政府组织也将失去民众信任和用户流失视为最大影响，因为这两方面也适用于老百姓。

将近 80% 的日本受访者表示他们拥有完整的 API 清单。另一方面，37% 的受访者表示他们知道哪些 API 会返回敏感数据，但各行业之间存在明显的差异。在日本的汽车和金融服务行业中，只有 8% 的受访者表示他们知道哪些 API 会返回敏感数据，这与零售/电子商务 (80%) 和政府/公共部门 (64%) 形成了鲜明对比。

各角色之间也存在差异，其中只有 23% 的高管层和资深安全专业人员声称知道哪些 API 会返回敏感数据，而对于应用安全团队，这一比例为 64%。

只有 11% 的日本受访者会进行实时测试，此数据大幅落后于中国的 22%。但是，在日本的资深安全专业人员中，将近 20% 的人表示他们会进行实时测试，而 12% 的人表示由于缺乏资源而不会对 API 进行任何测试。同样地，在日本的医疗保健行业中，20% 的受访者表示由于缺乏资源而不会进行任何测试。不过，大多数企业都会进行一定程度的 API 测试。就日本整体而言，只有 4% 的受访者表示他们不会对 API 进行任何测试。

日本汽车制造商缺乏对 API 风险的了解

只有 8% 的日本汽车公司知道哪些 API 会返回敏感数据。考虑到汽车行业对日本经济的重要性，以及各公司将大量使用 API 的技术嵌入联网汽车等产品中的频繁程度，这种情况多少有点出人意料。您无法保护自己看不到的东西。

日本的 API 安全性和合规性

在中国、印度和澳大利亚，将近 90% 的受访者表示他们会在满足法规要求时考虑 API 安全性。这种情况在日本不太可能出现，22% 的受访者表示他们不会在合规工作中考虑 API 安全性，理由是：

- 缺少时间或资源
- 认为监管机构尚未要求这样做

日本受访者的总体回答在很大程度上受到了高管层的影响：日本企业中 28% 的 CISO、CIO 和 CTO 表示 API 在他们的合规性计划中没有一席之地。

印度的调查结果表明员工与领导层之间存在严重的脱节问题

在 API 安全事件的发生率方面，印度与日本基本一致。总体来看，82% 的印度受访者表示他们在去年中经历过 API 安全事件，其中能源/公用事业行业的每位受访者 (100%) 都表示经历过安全事件。保险行业的安全事件发生率最低，有 60% 的受访者经历过安全事件。

与其他国家的整体结果类似，在印度，“API 错误配置”是报告最多的 API 安全事件原因 (23%)，紧随其后的是“知名的安全工具/服务（Microsoft 等）” (22%) 和“生成式 AI 工具中的 API”(22%)。以下是印度的 API 安全事件原因的一些额外要点：

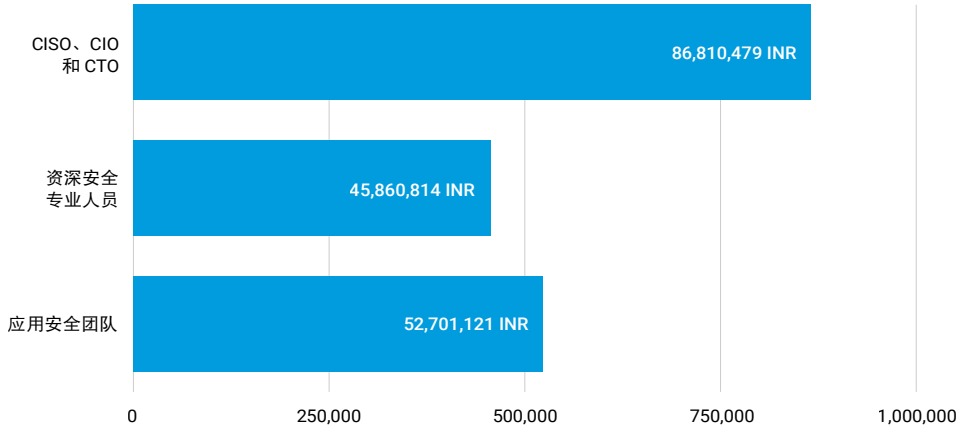
- 将原因归咎于“API 编码错误导致的漏洞”的受访者人数最少。
- 能源/公用事业和医疗保健是将原因归咎于“LLM 等生成式 AI 工具中的 API”最多的行业。
- 资深安全专业人员选择最多的原因是“生成式 AI 工具中的漏洞”，比印度的总体平均水平高出将近 10 个百分点。
- 制造和零售/电子商务是将原因归咎于“知名外部技术工具或服务”最多的行业。

API 安全事件往往会在内部、基于员工的因素等方面影响印度的企业，因为大多数受访者将“导致企业加强了对团队/部门的内部审查”(32%) 和“导致团队/部门的压力增加”(31%) 视为最大的影响。保险和零售/电子商务行业将“失去客户信任和客户流失”视为最大的影响。

在印度，所报告的 API 安全事件平均成本为 62,063,515 卢比 (INR)，并且这里的高管层估计的成本远高于一线安全人员估计的成本。

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）

印度安全负责人和员工如何看待 API 事件造成的成本支出

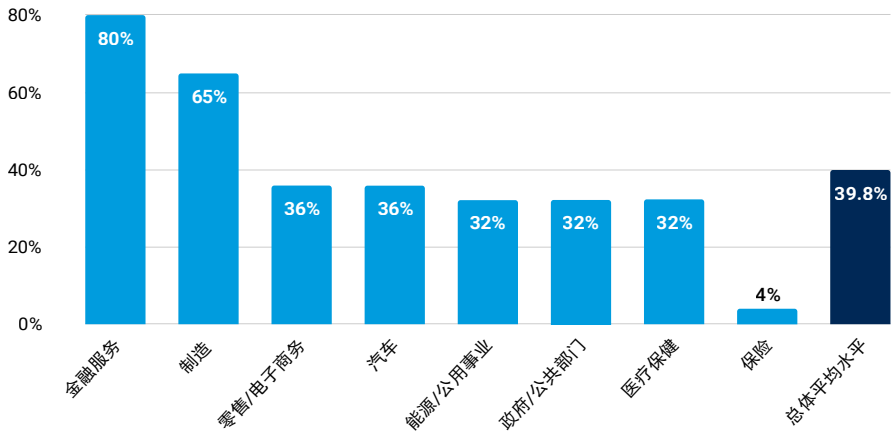


印度的两个行业尤其拉高了整体的平均成本：金融服务（128,288,777 印度卢比或 1,480,552 美元）和零售/电子商务（117,978,722 印度卢比或 1,361,566 美元）。

在印度，64% 的受访者表示拥有完整的 API 清单，但其中只有 39% 的人表示知道哪些 API 会返回敏感数据。此结果与中国 (39.4%) 和日本 (37%) 大致吻合，但高于澳大利亚 (27.9%)。金融服务 (80%) 和制造业 (65%) 的大多数受访者表示，他们知道哪些 API 会返回敏感数据，而保险业中只有 4% 的受访者表示他们知道此情况。

您是否拥有完整的 API 清单*并且*是否知道哪些 API 会返回敏感数据?

印度各行业的表现与全国的总体平均水平相比如何



不同角色的了解程度差距更为明显：

- 高管层 (77%) 和资深安全专业人员 (75%) 中表示拥有完整的 API 清单的人数比例远高于应用安全团队 (41%)。
- 高管层 (65%) 和资深安全专业人员 (43%) 中表示知道哪些 API 会返回敏感数据的人数比例也远高于应用安全团队 (11%)。

这可能是应用安全团队将“保护 API 免受攻击”列为其第一要务 (24%)，而高管层更可能优先考虑“云安全解决方案”(35%) 的原因。另一方面，高级安全负责人通常将“管理和保护开发人员机密信息”(36%) 视为第一要务。

总体来看，“保护 API 免受攻击”(21%) 在印度是第四大网络安全优先事项，排在“云安全解决方案”(27%)、“管理开发人员机密信息”(25%) 和“保护应用程序”(23%) 之后。

这就引出了一个重要话题：API 测试的作用。在调查范围内的四个国家中，印度受访者将 API 安全事件的原因归咎于“编码错误导致的漏洞”的人数最少，它在 13 项原因中排名最后。由于编码错误是在开发过程中出现的，因此值得探讨企业对 API 进行测试的频率。所面临的挑战是，如果不进行实时测试，甚至难以知道 API 攻击是否由编码错误引起。如果企业无法发现漏洞，就不可能将其视为引起攻击的原因。

我们询问受访者他们进行 API 安全测试的频率（在生产期间和整个 API 生命周期内）以查找滥用迹象。以下是印度总体 API 测试频率的细分情况：

- 每周：31%
- 每天：21%
- 实时：15%

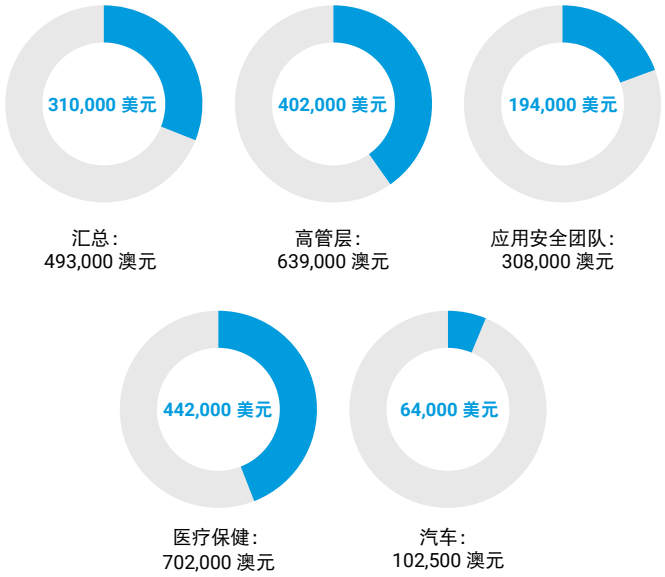
如果仅关注对其 API 进行实时测试的企业，则以下细分情况显示了印度各行业的表现与 15% 的全国总体平均水平的对比：

- 金融服务：24%
- 医疗保健：20%
- 制造：19%
- 汽车：4%
- 能源/公用事业：4%

澳大利亚企业遭遇了最多的 API 安全事件

在调查范围内的四个亚太国家中，澳大利亚过去 12 个月内的 API 安全事件发生率最高，有 95% 的受访者表示经历过安全事件。大多数受访者将这些事件归咎于“API 错误配置”(23%) 或“API 网关没有进行拦截”(23%)，但很多其他受访者选择了内部流程作为原因，包括“授权漏洞”、“API 编码错误导致的漏洞”以及“API 意外暴露到互联网”（比例分别约为 21%）。

如果您经历过 API 安全事件，这些事件造成的累计财务损失的估计总额是多少?
五组澳大利亚受访者如何看待 API 事件造成的成本支出



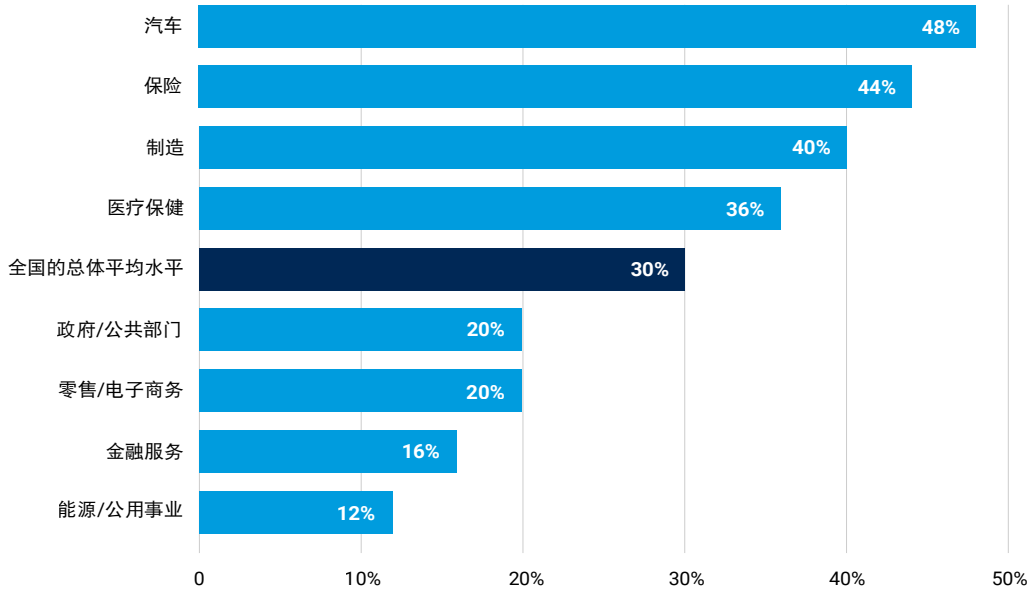
与调查范围内的其他亚太国家相比，澳大利亚受访者将 API 安全事件造成的成本支出视为一项更大的影响，该项位列第二 (32%)，排在“损害了部门在高层领导和/或董事会中的声誉”(33%) 之后。虽然“监管机构的罚款”在整体影响中仅排第四，但在资深安全专业人员眼中以及保险、能源/公用事业、制造业这三个行业，它却居于影响之首。

澳大利亚企业的 CISO、CIO 和 CTO 高度关注 API 安全事件的内部后果。以下两项选择最多的影响所占比例均为 32.8%：“导致团队/部门的压力增加”和“损害了部门在高层领导和/或董事会中的声誉”。

此外，在调查范围内的四个国家中，澳大利亚受访者中声称拥有完整 API 清单的人数占比最高 (81%)，但这组受访者中表示知道哪些 API 会返回敏感数据的人数占比最低 (30%)。只有一家公司表示他们根本没有 API 清单。

您是否拥有完整的 API 清单***并且***是否知道哪些 API 会返回敏感数据?

澳大利亚各行业的表现与全国的总体平均水平相比如何



尽管澳大利亚的 API 安全事件发生率很高，但“保护 API 免受攻击”并不是澳大利亚受访者的第一要务，在所有网络安全优先事项中位列第四 (21%)，排在“保护端点的安全”(26%)、“管理和保护开发人员机密信息”(24%) 和“SIEM”(24%) 之后。在澳大利亚企业的第一要务中，“保护 API 免受攻击”与“防止数据丢失”并列，分别约占 21%。

关于在生命周期早期发现 API 漏洞方面，澳大利亚受访者的实时 API 测试率在四个国家中最低 (6%)，但进行每日或每周测试的占比最高，分别为 34% 和 35%。澳大利亚金融服务、医疗保健或制造业的受访者中没有一个人表示他们会进行实时测试。

在澳大利亚，缺少实时测试令人担忧并且值得探讨。正如下一节关于 API 安全性和合规性的内容所述，澳大利亚的《消费者数据权利》法规包含确保各公司的开发人员以标准化的安全方式构建 API 的标准。

嵌入了编码错误或其他可预防风险的 API 正是攻击者梦寐以求的。如果企业尽早并频繁地对 API 进行测试，其安全和开发人员团队便会处于优势地位。

企业是否将 API 风险纳入其合规性计划中？

世界各地的监管机构越来越多地要求企业对 API 进行记录和说明，而且他们的信息似乎正在得到采纳。在调查范围内的四个国家，受访者都深刻认识到 API 和 API 安全性在满足监管要求方面的重要性。

在中国、印度和澳大利亚，将近 90% 的受访者表示他们会在满足法规要求时考虑 API 安全性。这种情况在日本不太常见，22% 的受访者表示他们不会考虑 API 安全性，其理由是缺少时间或资源或者认为监管机构尚未要求这样做。日本受访者的总体回答在很大程度上受到了高管层的影响；日本企业中 28% 的 CISO、CIO 和 CTO 表示 API 在他们的合规性计划中没有一席之地。

然而，在调查范围内的四个国家中，真正采取必要的措施将 API 纳入其合规性计划中的企业并不多。在大多数表示确实考虑了 API 的受访者中，只有不到一半的人将其纳入了大多数监管机构要求的三个重要领域：风险评估、报告和安全计划。事实上，只有 41% 的受访者会将 API 纳入风险评估中，并且只有 40% 的受访者会将 API 纳入报告要求。

为什么这些差异很重要？攻击者知道，他们直接以保护措施不到位的 API 为目标就可以简化数据泄露方法。

《个人信息保护法案》（日本）：

要求执行数据保护影响评估，以识别和降低处理大量个人数据或涉及高风险数据处理活动的 API 的风险

《中华人民共和国数据安全法》：

要求实施强有力的措施，以保护通过在应用程序、系统和云环境之间交换信息的各种技术（如 API）对客户数据的访问

《数字个人数据保护法案》（印度）：

要求实施相关机制来检测数据泄露（包括通过 API 发生的数据泄露），并进行定期合规性审计，其中应包括对 API 的说明以及为保护 API 所采取的措施

《消费者数据权利》（澳大利亚）：

包含确保开发人员以统一、安全的方式构建 API 的标准，同时强调了在传输和访问（包括通过 API）过程中保护消费者数据的协议

面向安全团队的关键要点和后续行动

对于希望了解 API 安全在其优先事项中如何定位的安全负责人和团队成员来说，这些调查结果提供了几个令人信服的切入点：

- 在调查范围内的四个国家中，攻击、滥用和数据泄露等 API 安全事件频发。
- 在这些事件造成的成本支出以及失去信任等其他影响方面，高管层（CISO、CIO、CTO）、资深安全专业人员与应用安全团队之间存在严重的脱节问题。此外，这些角色在对 API 的了解以及对这些 API 是否会返回敏感数据的了解上也存在分歧。
- 要么企业对其 API 的脆弱性了解有限，要么攻击者可以利用的漏洞广泛存在，或者这两种情况兼而有之。这可能是由于内部流程不完善以及现有 API 安全解决方案存在缺陷造成的。

要实现有效的 API 安全方法来保护关键数据、客户关系和内部团队成员，企业首先需要在 API 安全事件的原因、影响和优先级上达成共识。在此基础上，他们将受益于创建明确而全面的流程，以保护开发和生产过程中的 API。最后，他们需要可以帮助完成这些任务的安全工具。

以下是用于构建持久 API 安全策略的分步方法：

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。覆盖广度至关重要，因为不受管 API 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 的编码是否能够实现其预期功能。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。

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 Web 应用程序和 API 保护）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，然后使用将先进工具与人类智慧相结合的主动威胁搜寻功能。

有关 API 安全保护最佳实践的更多见解，请阅读以下两篇文章：

- **防范 OWASP 十大 API 安全风险**
- **API 威胁检测和响应的 11 个关键功能**

如需获得更多帮助，请预约定制化 **Akamai API Security 演示**。

API 安全影响研究介绍

《2025 年 API 安全影响研究》报告的调研工作主要面向中国、日本、印度和澳大利亚的企业，由 Opinion Matters 公司在 2024 年 10 月 14 日至 30 日完成。Opinion Matters 共邀请了 806 名受访者参与调研，每个国家至少有 200 名受访者。其中三分之一的受访者是企业 CIO、CTO 或 CISO；三分之一是资深安全专业人员；另三分之一来自应用安全团队。这些受访者就职的公司规模从 250 至 400 名员工到 1,000 名员工以上不等，涉及八个主要行业：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

Barney Beal

总编辑兼内容策略师

John Natale

文稿编辑

Cullen Pitney

推广

Ellen O'Brien

营销与发布

Georgina Morales Hampe

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。
https://www.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

访问本报告中的数据

查看本报告中引用的图片和图表的高画质版本。这些图片可供免费使用和引用，但必须注明转载来源，并保留 Akamai 徽标。**https://akamai.com/api-security-study-asia-data**

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