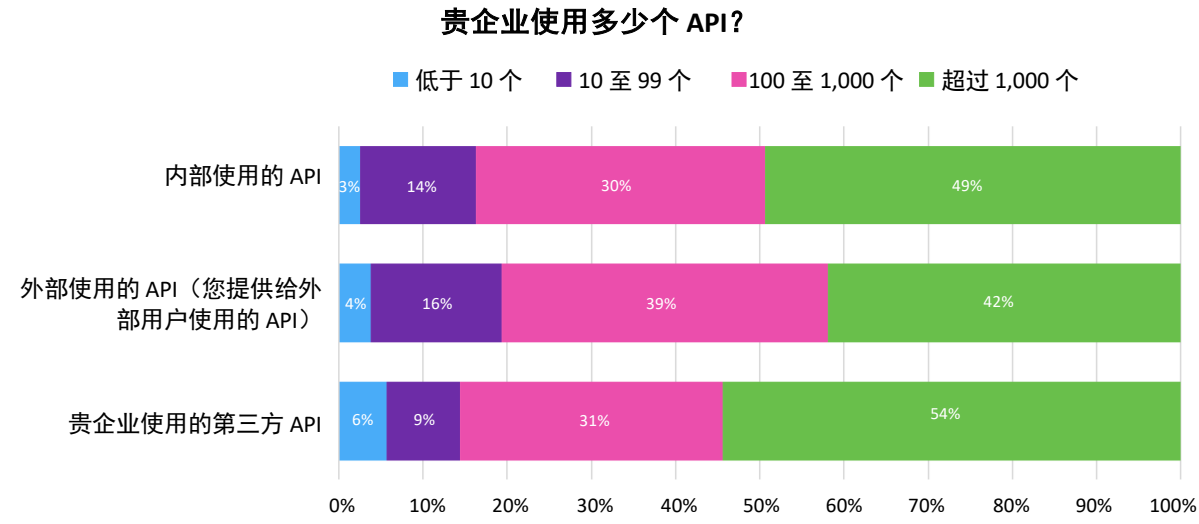
图 1：使用的 API 数量



注：n=160
来源： Omdia

© 2024 Omdia

API 的使用呈上升趋势。与此同时，许多受访者表示遇到了 API 安全事件，包括内部记录泄露和大规模数据抓取等具体问题。

这一情况意味着公司需要立即采取措施来改进 API 安全防护，因为 API 的数量只会持续增加，如果不及时采取措施，安全问题将会愈发严重。随着 API 数量的增加，攻击面也将持续扩大，进而导致更可能受到攻击。

API 安全防护快速入门

常见的 API 安全防护流程围绕着四个主要用例展开，以无限循环的方式运作，这与在 DevOps 流程中使用的“构建-交付-运行-监控”循环类似：

- **发现在环境中使用的 API：**这个流程可以通过多种不同的方法完成，包括提取 OpenAPI (Swagger) 定义、扫描代码库以及主动扫描环境。大部分 API 可以通过分析流量来发现。上传 API 规范文件是一种较少使用的策略，只有在企业知道自己使用了哪些 API 时才会采用。此外，仅采用一种方法通常并不足够：将连续流量和存储库扫描结合使用，就可以获得企业内 API 使用情况的全面视图。

  企业需要审视整个技术资产中的 API 安全问题，而不仅仅是特定的 API 友好环境。在许多情况下，处理旧版 API 的使用需要另辟蹊径。

© 2025 TechTarget, Inc. 保留所有权利。未经授权，禁止复制。