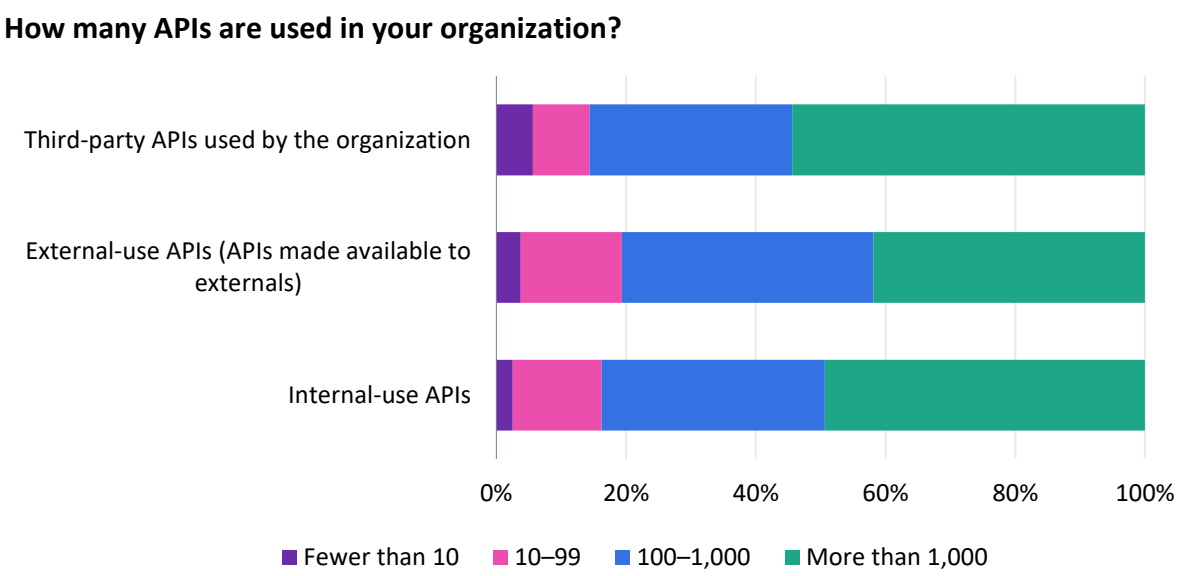
Figure 1: Number of APIs in use



Note: n=160

Source: Omdia

Use of APIs is rising. At the same time, many of our respondents reported API security incidents with specific issues such as the exfiltration of internal records and large-scale data scraping.

This scenario means companies should improve their API security efforts now, because the increase in APIs will only continue, thereby compounding the security problems unless such steps are taken. As the number of APIs increases, the attack surface will continue to expand, resulting in even more potential attacks.

A quick primer on API security

The common flow for API security is centered around four main use cases that operate in an infinite loop, not unlike the build-ship-run-monitor cycle used in DevOps:

- **Discovery of APIs being used across environments:** This can be done in many different ways, including ingestion of OpenAPI (Swagger) definitions, scanning code repositories, and active scanning of environments. Most APIs are discovered by analyzing traffic. Uploading API spec files is a less-used tactic and is only possible when the organization already knows what APIs it has. Additionally, no one approach is sufficient: The combination of continuous traffic and repository scanning is likely to yield a comprehensive view of API usage within organizations.

  Organizations need to account for API security considerations across their entire technology estate, not just specific API-friendly environments. In many cases, handling legacy API usage requires a different approach.