

# API Security: Adopting API Specifications



As the number of business applications grows, APIs are becoming increasingly important to the digital landscape of business. Creating API specifications for all APIs gives visibility into this expanding area and helps improve security posture. Luckily there are tools that can help keep inventory, flag new APIs, assess risk, and enforce your specifications, but are businesses taking advantage of these tools?

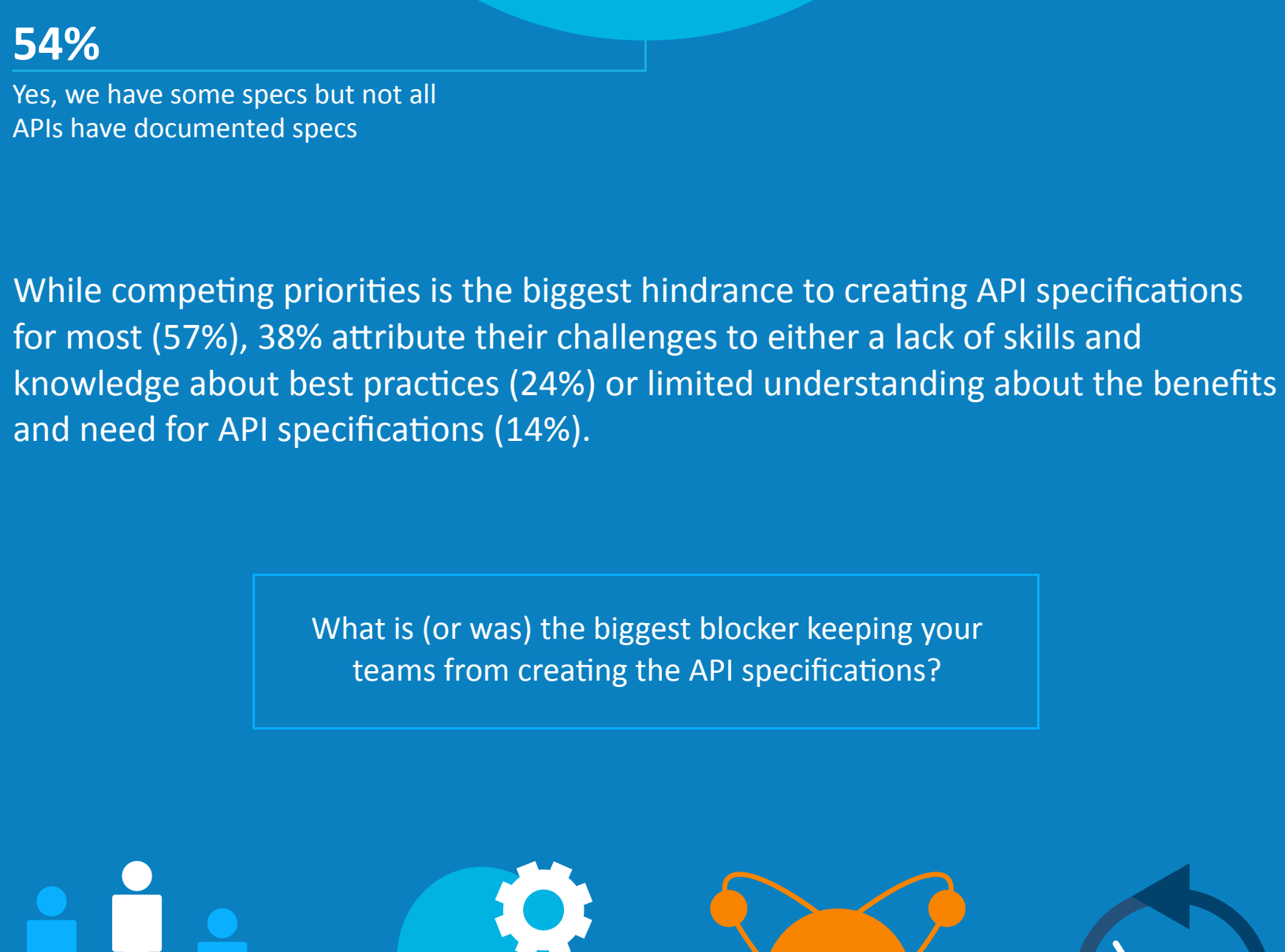
Pulse and Cequence Security surveyed 100 technology leaders to find out how many are adopting API specifications, what they see as the benefits of this approach, what tools they are using to implement API specifications, and how they are approaching API security.

Data collected from July 14 - August 7, 2021

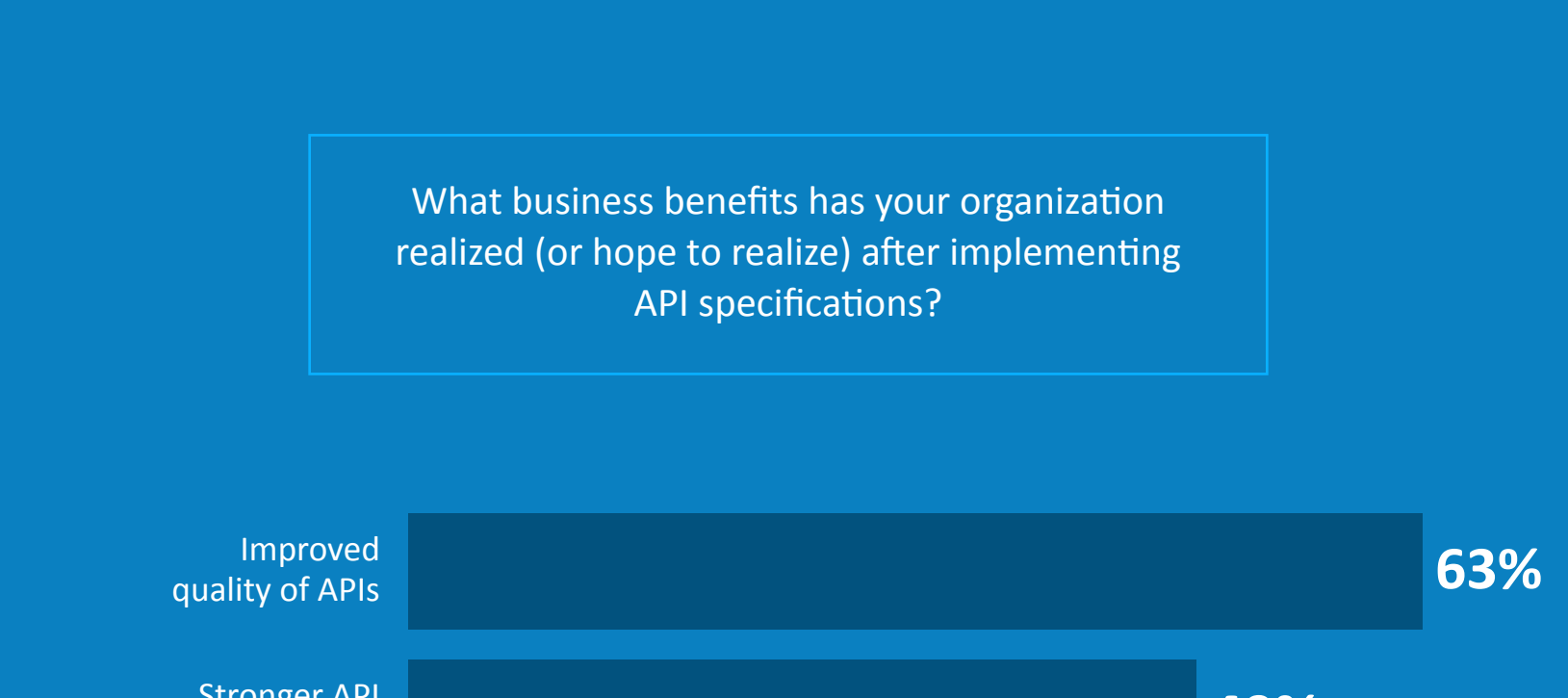
Respondents: 100 technology leaders

## Technology leaders are missing an opportunity to improve API quality, security and consistency

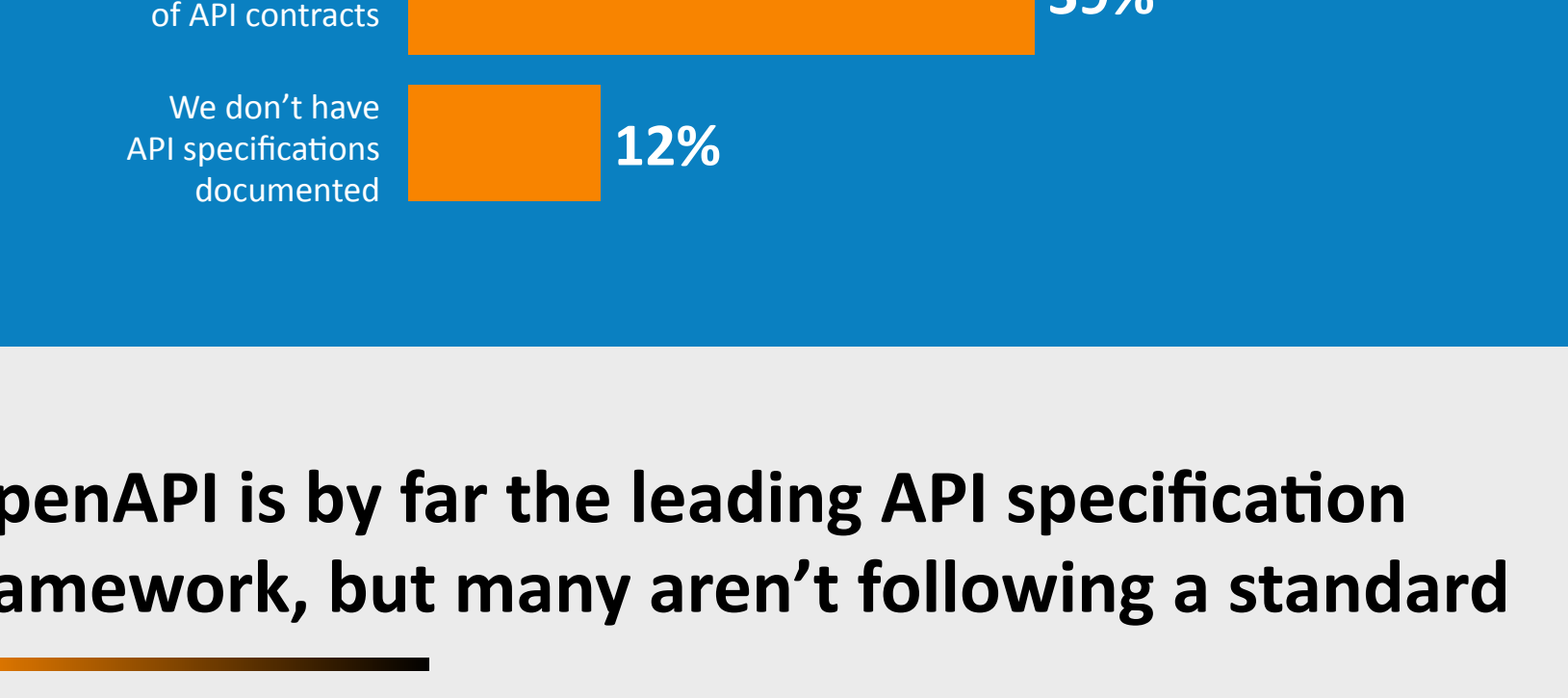
Only 24% of technology leaders say their company requires API specifications for all APIs. That leaves 76% of respondents who lack a full understanding of how all their APIs work and the expected behaviors for those APIs when used.



While competing priorities is the biggest hindrance to creating API specifications for most (57%), 38% attribute their challenges to either a lack of skills and knowledge about best practices (24%) or limited understanding about the benefits and need for API specifications (14%).

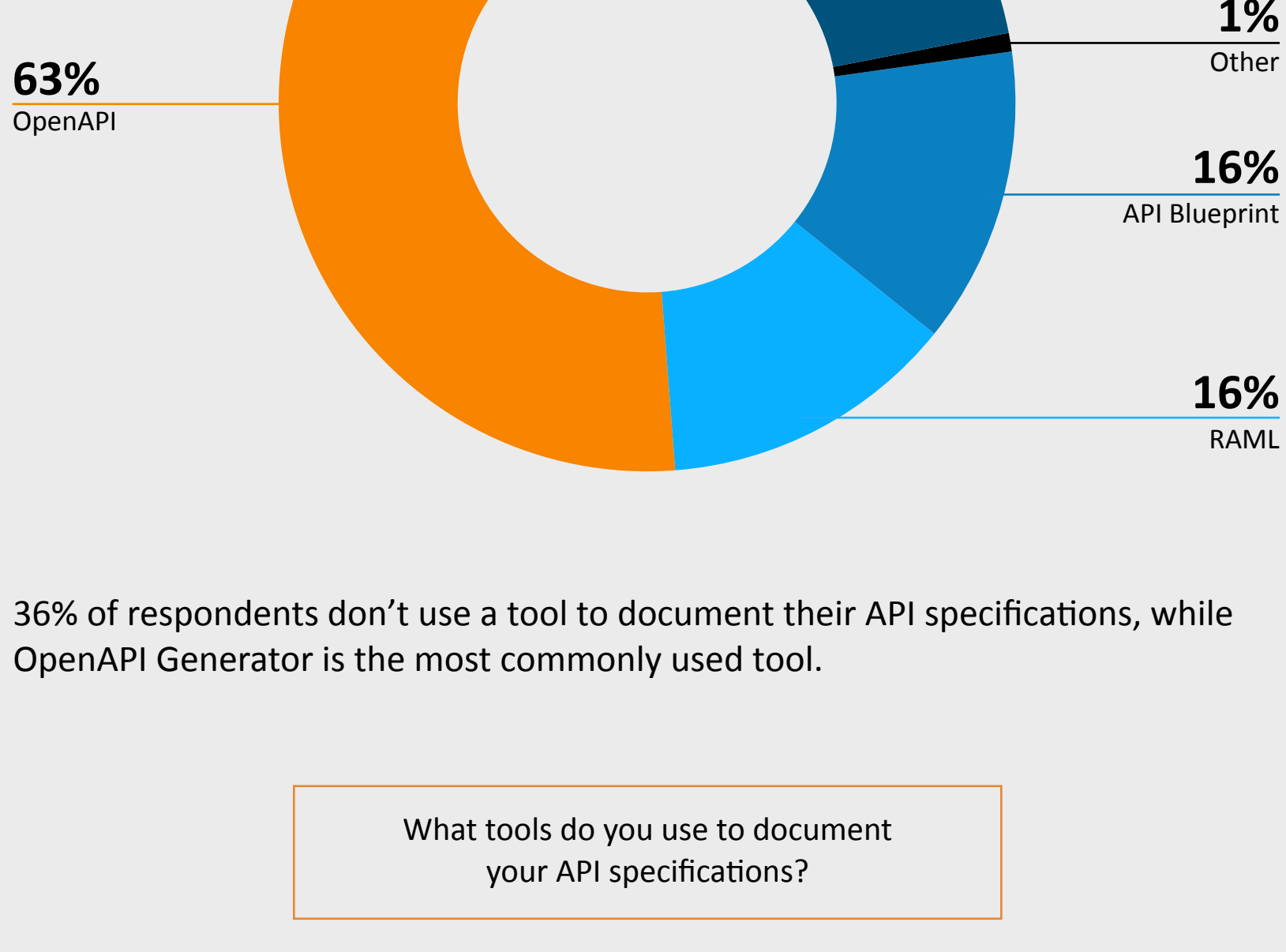


Respondents overwhelmingly agree that quality, security and consistency are the top API specification benefits.

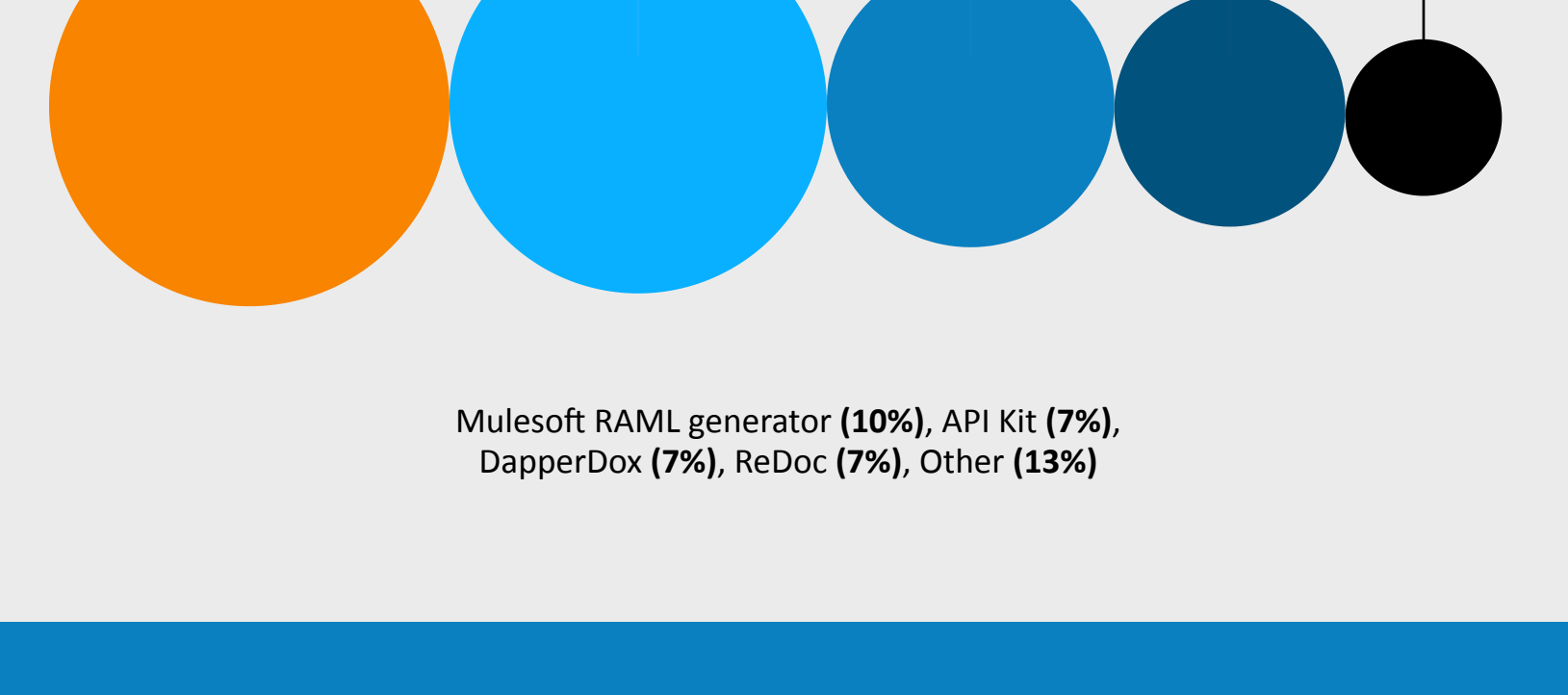


## OpenAPI is by far the leading API specification framework, but many aren't following a standard

With 63% of respondents following it, OpenAPI (formerly Swagger) is the leading standard for API specifications. 27% admit to not following any API specification standard at all.

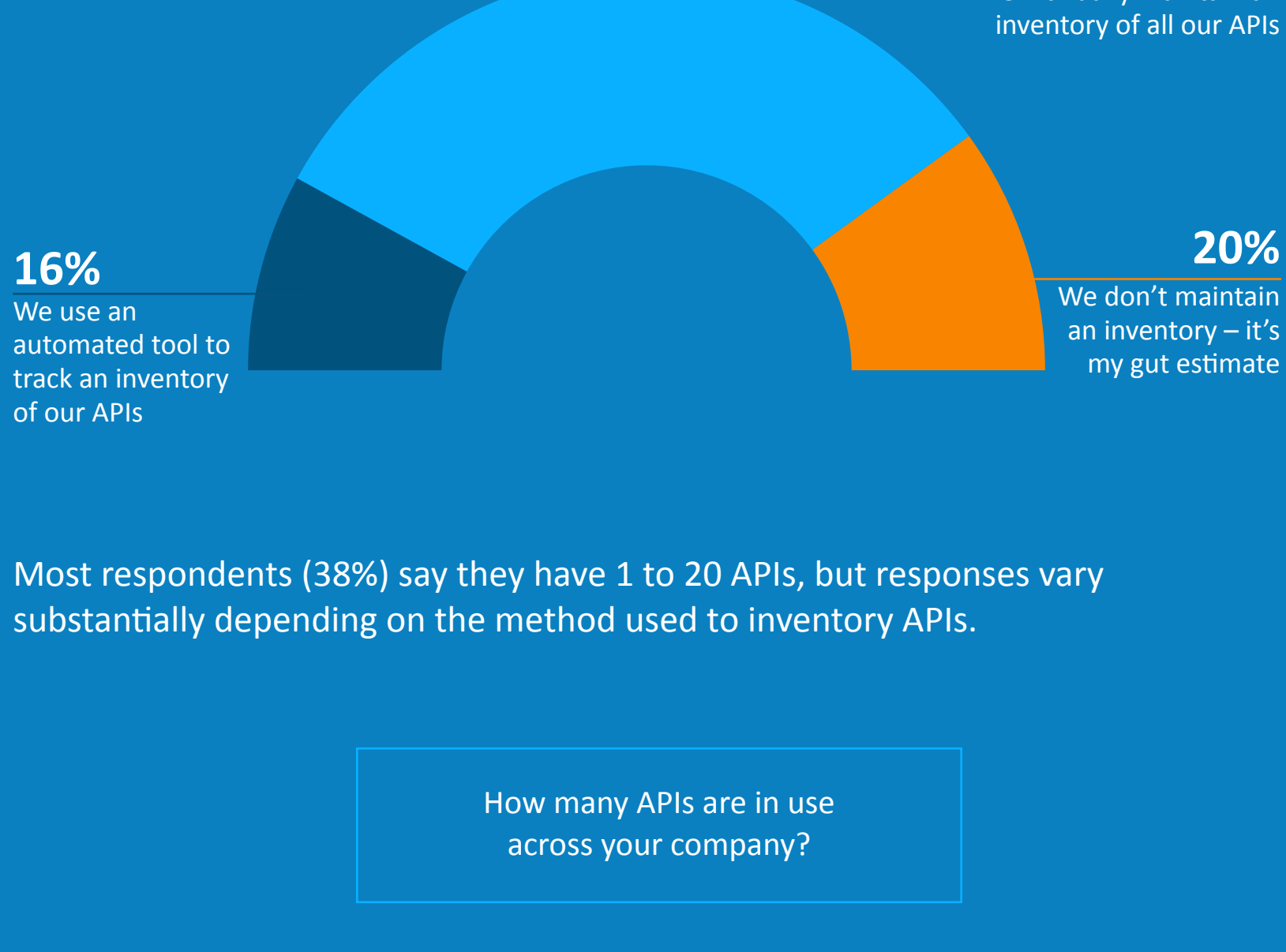


36% of respondents don't use a tool to document their API specifications, while OpenAPI Generator is the most commonly used tool.

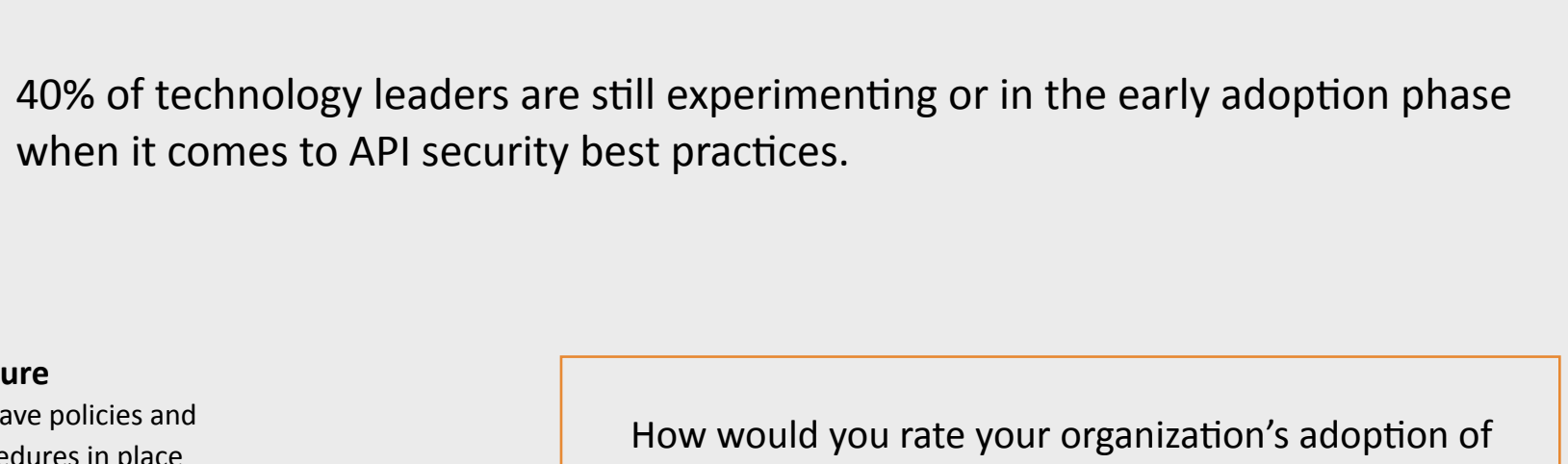
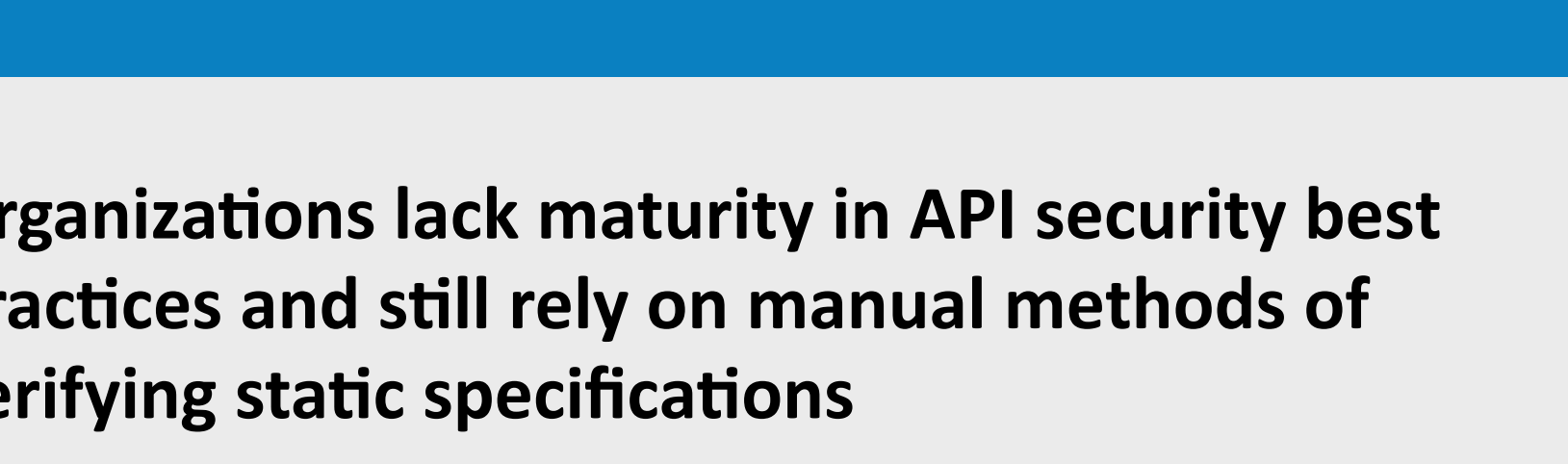
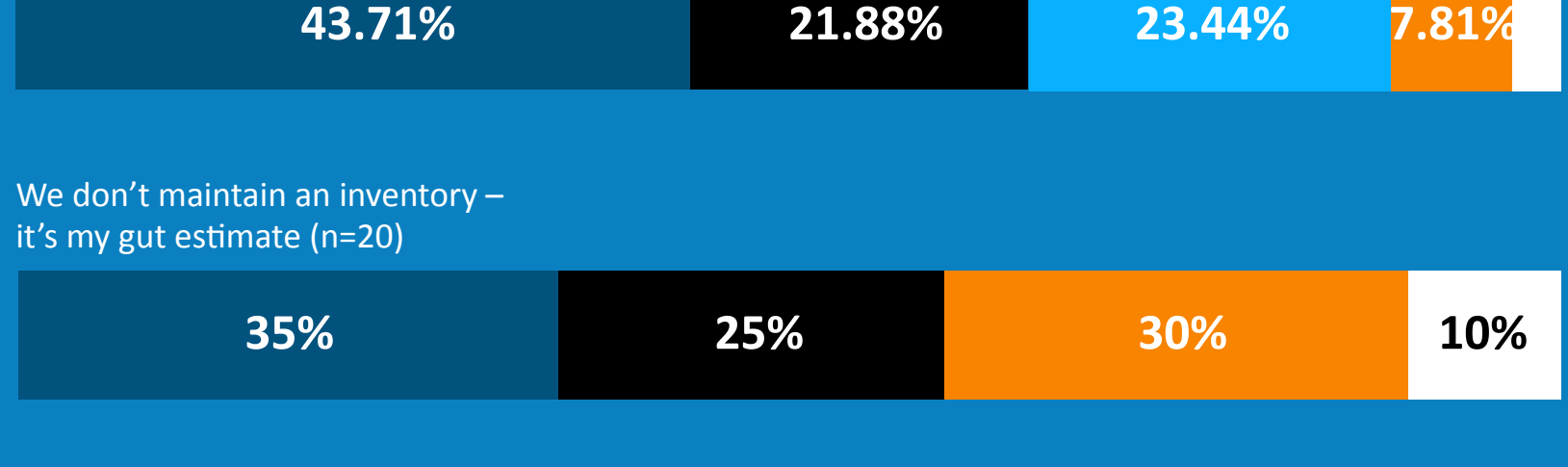
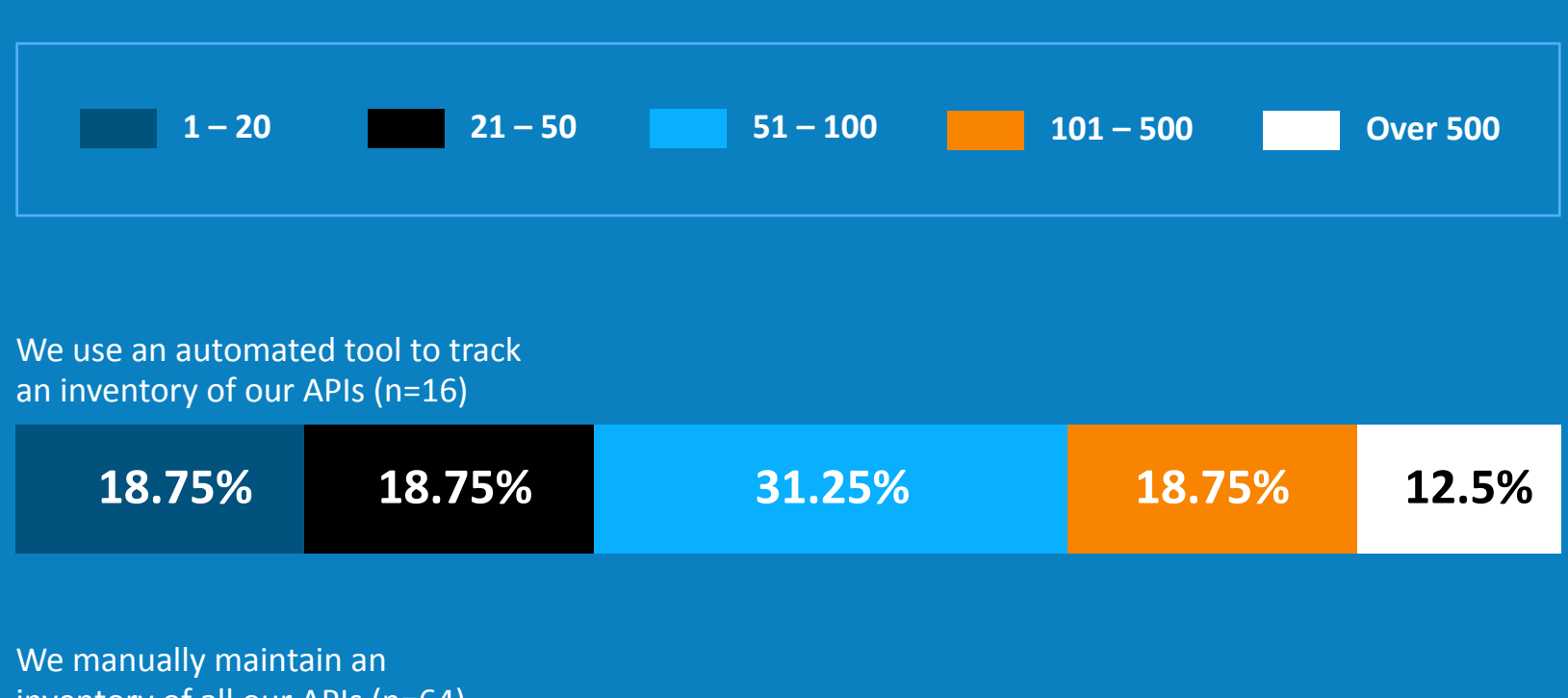


## Organizations may also lack clear visibility of the number of APIs they have implemented

Only 16% are using an automated tool to track and inventory their APIs. A whopping 64% are manually maintaining their API inventory. These different methods of inventorying may be leading to inaccurate estimates.

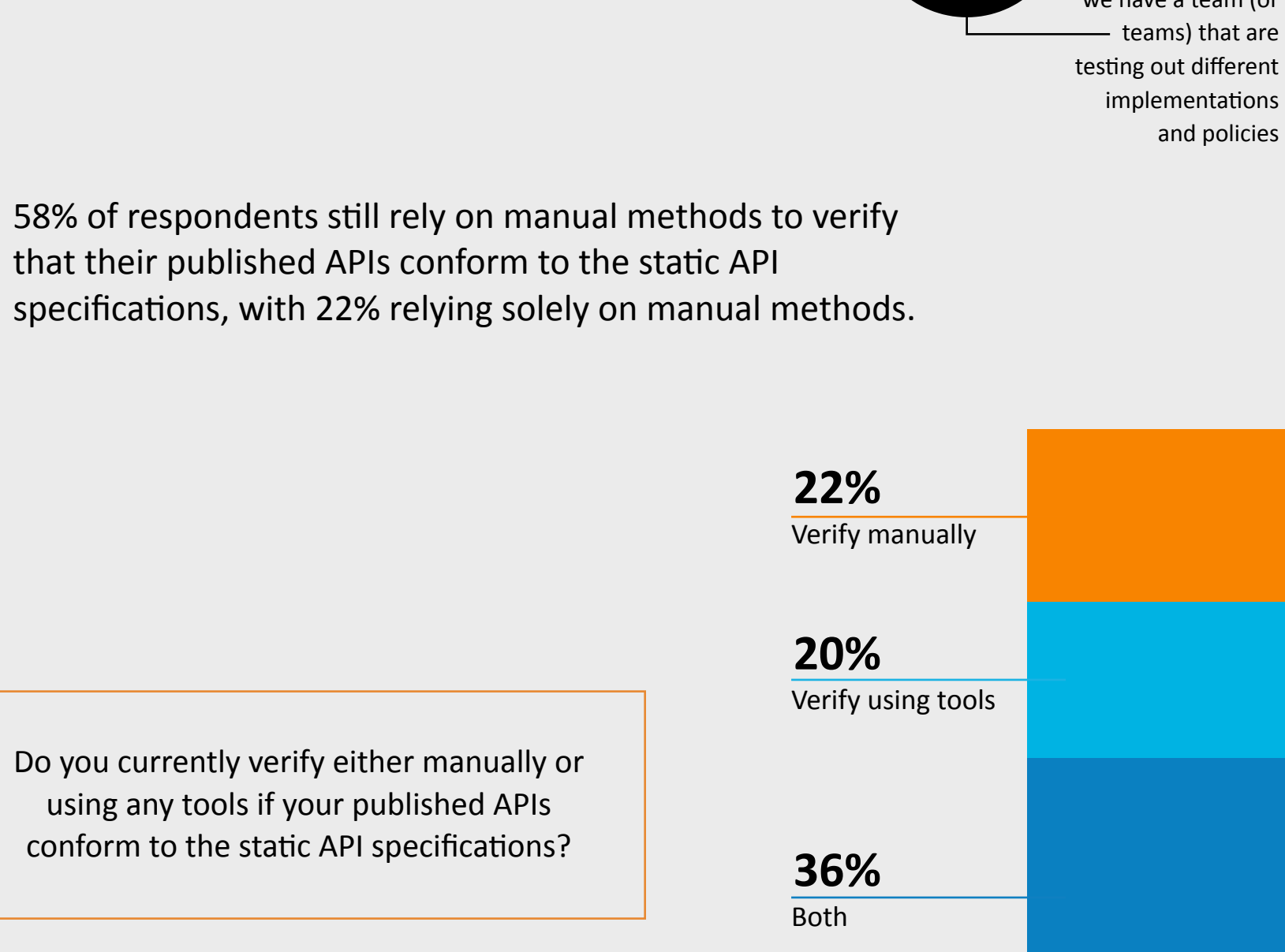


Most respondents (38%) say they have 1 to 20 APIs, but responses vary substantially depending on the method used to inventory APIs.

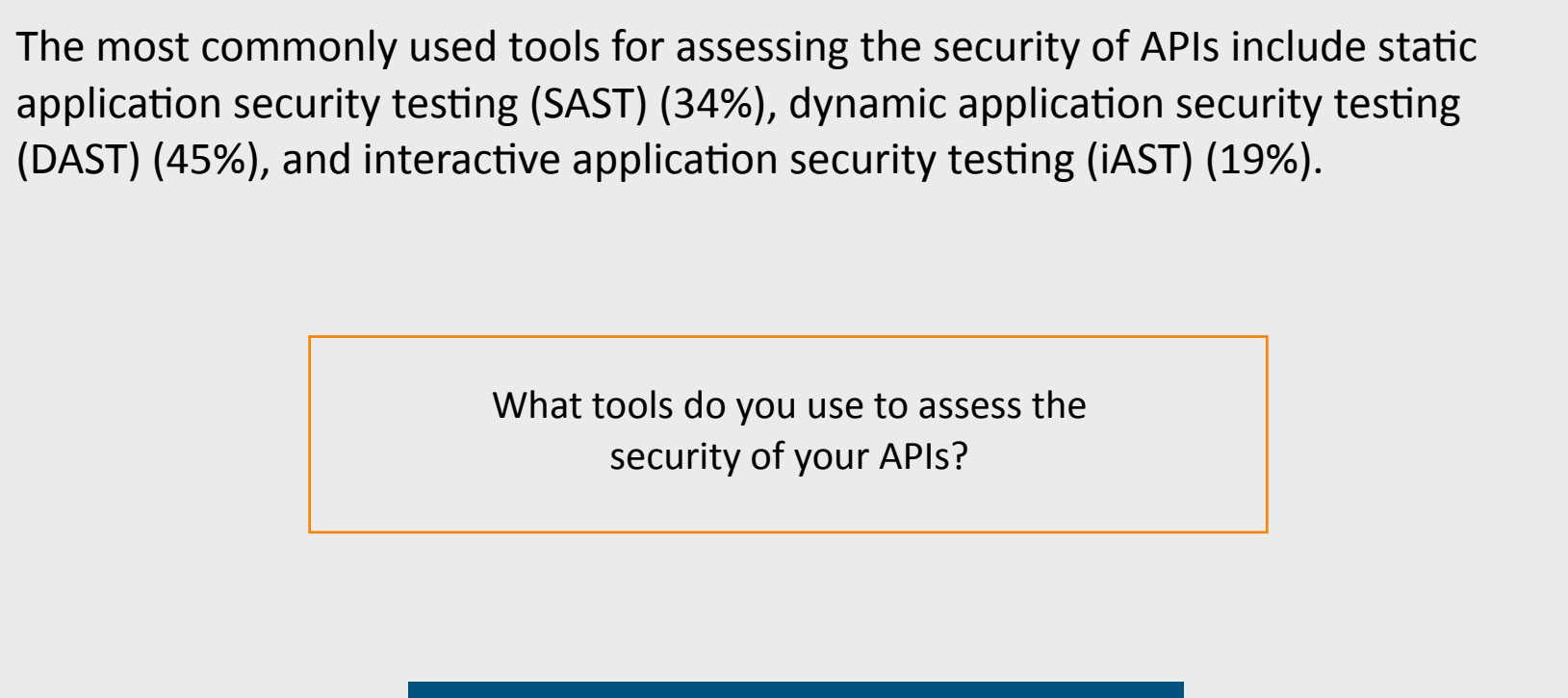


## Organizations lack maturity in API security best practices and still rely on manual methods of verifying static specifications

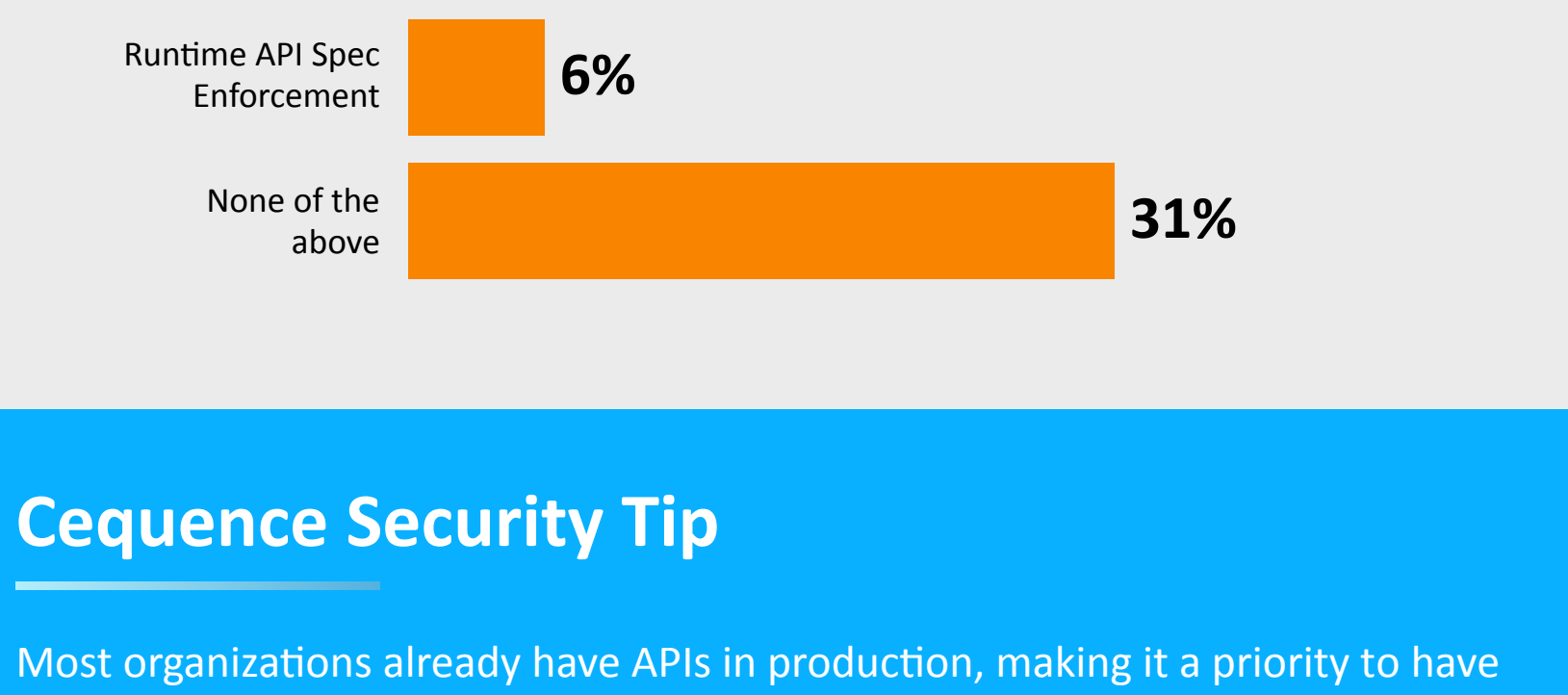
40% of technology leaders are still experimenting or in the early adoption phase when it comes to API security best practices.



58% of respondents still rely on manual methods to verify that their published APIs conform to the static API specifications, with 22% relying solely on manual methods.



The most commonly used tools for assessing the security of APIs include static application security testing (SAST) (34%), dynamic application security testing (DAST) (45%), and interactive application security testing (IAST) (19%).



## Cequence Security Tip

Most organizations already have APIs in production, making it a priority to have runtime tools that will assess risk and enforce API specs — even ahead of assessment tools used in the API build stage.

