Gartner Peer Insights

CEQUENCE SECURITY

Balancing API Business Value and Security

The cars we drive, the apps we use on our mobile devices, and the gadgets in our smart homes are all built on APIs and are foundational in driving revenue and business value. However, the explosive use of APIs makes them a prime target for attackers. In response, security teams are using disparate solutions that lack integration, slowing attack detection response times which can result in a failure to provide adequate API protection from theft, fraud and business disruption.

Gartner Peer Insights and Cequence surveyed 300 API security decision makers to explore how businesses are maximizing API business value, while maintaining and ensuring proper security.

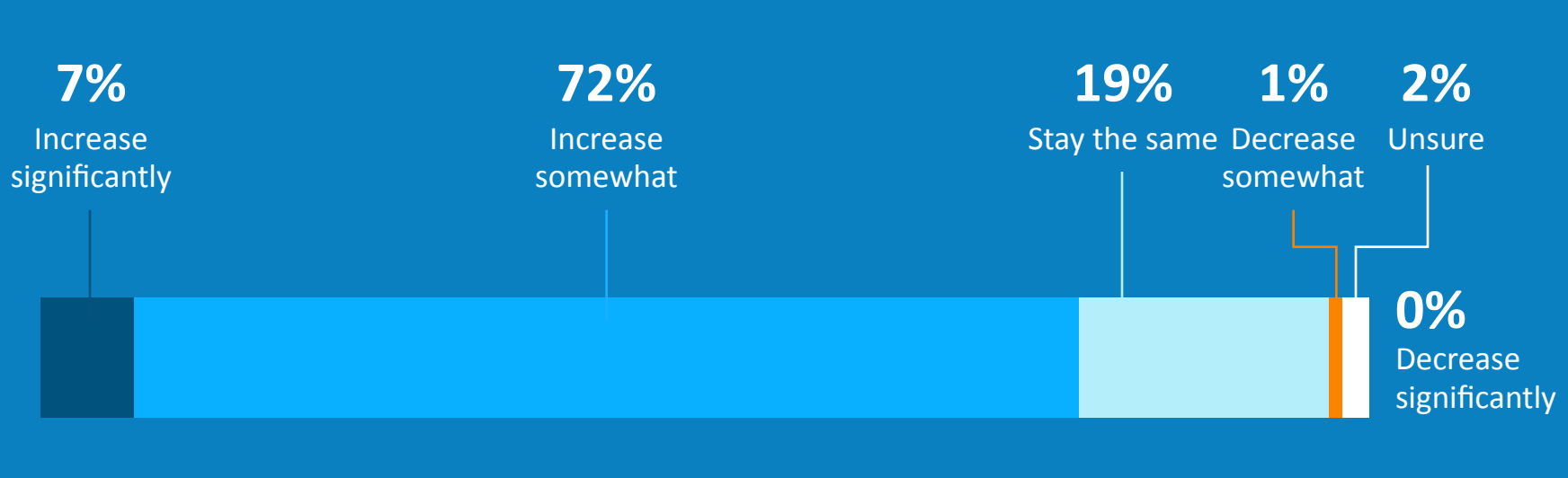
Data collection: August 13 - October 31, 2022

Respondents: 300 IT and security leaders

APIs are the currency of exchange for today's digital businesses

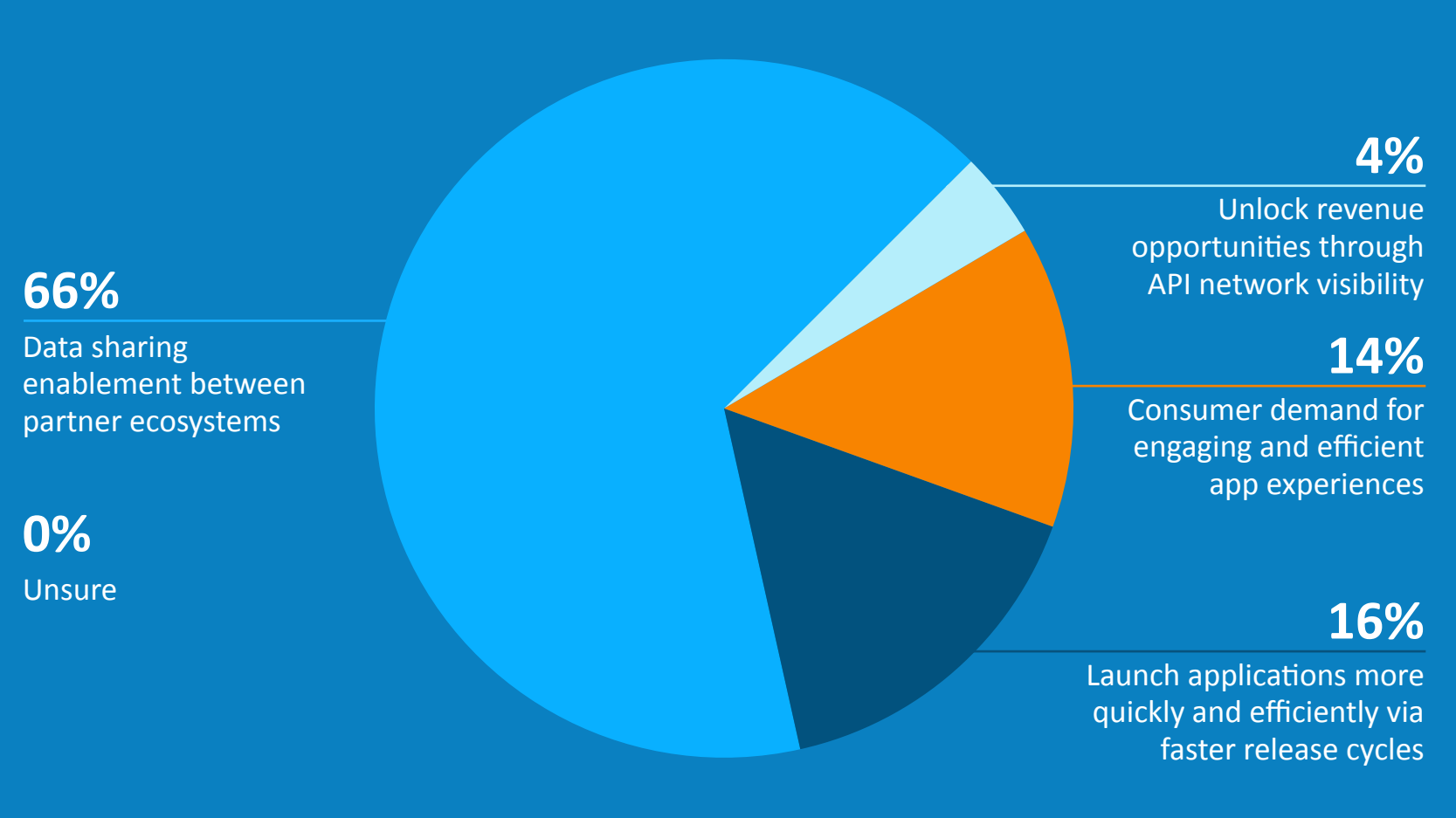
Nearly all respondents (79%) said their organization's revenue dependency on APIs will increase over the next 12 months.

How much will your organization's revenue dependency on APIs change in the next 12 months?



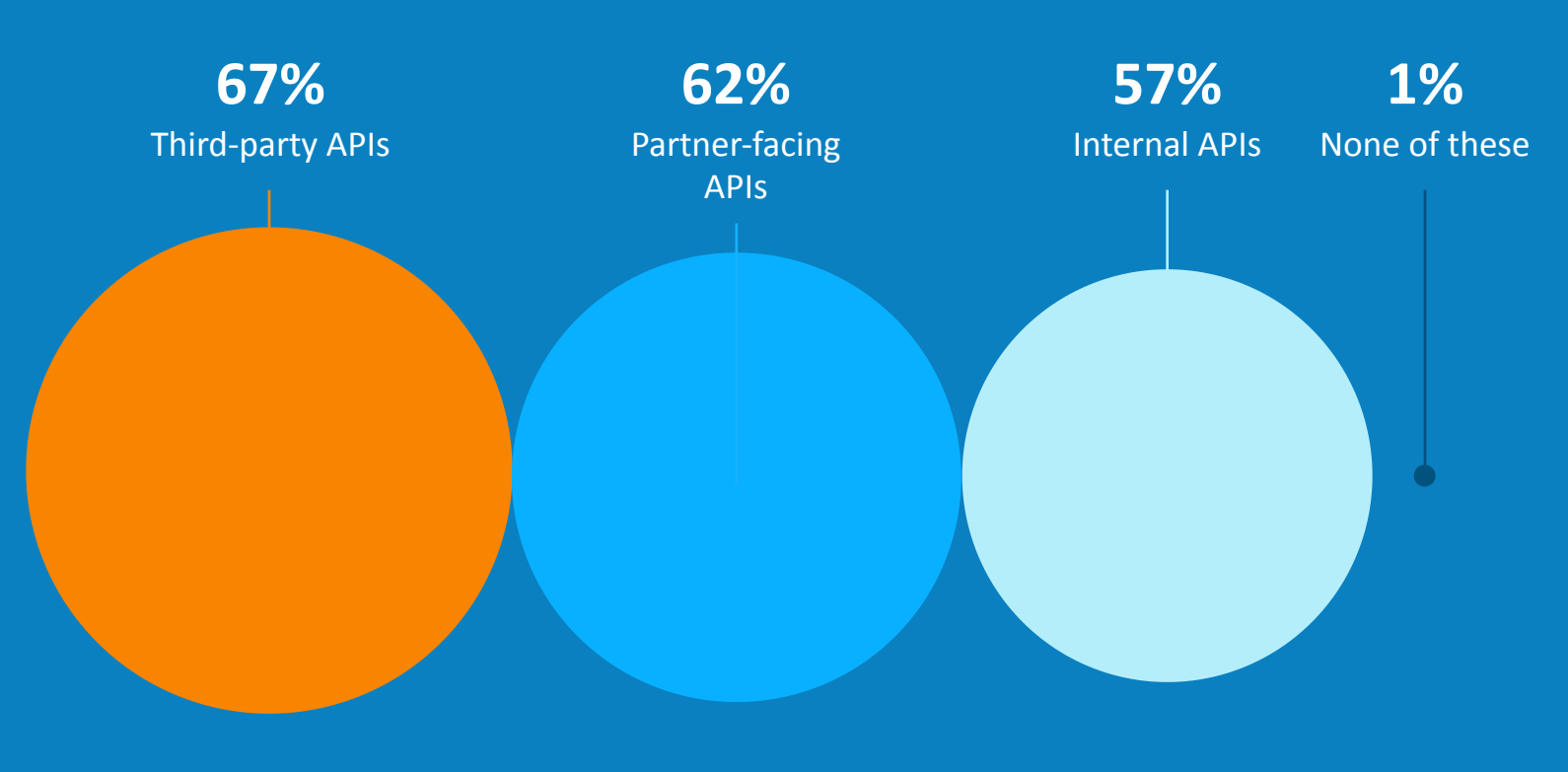
The primary use case reported for APIs was to enable data sharing between partner ecosystems (66%).

What is your organization's primary driver for using APIs?



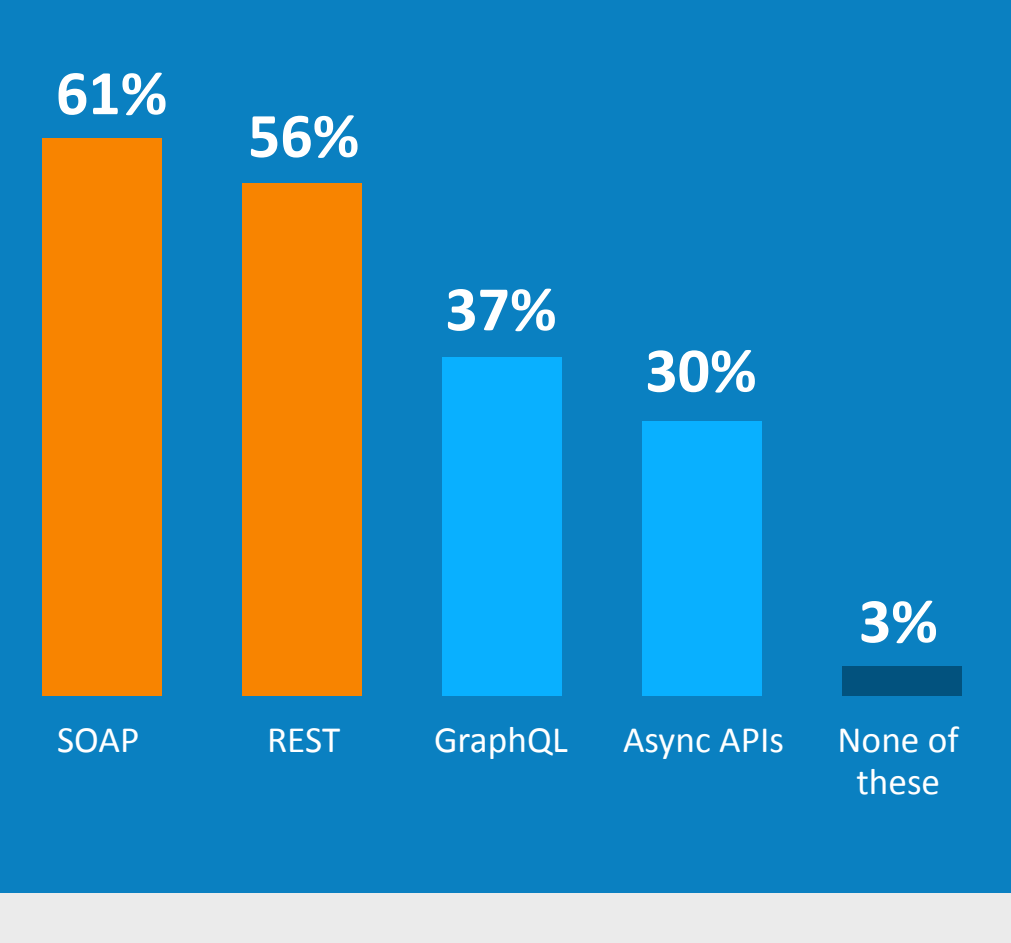
The use of third-party APIs was viewed as the type of API that drives the most business value with 67% while partner-facing APIs came in as a close second at 62%.

Which types of APIs drive the most business value?



SOAP (61%) and REST (56%) were identified as the top two API technologies driving the most business value, while GraphQL is being used by more than one third of the respondents.

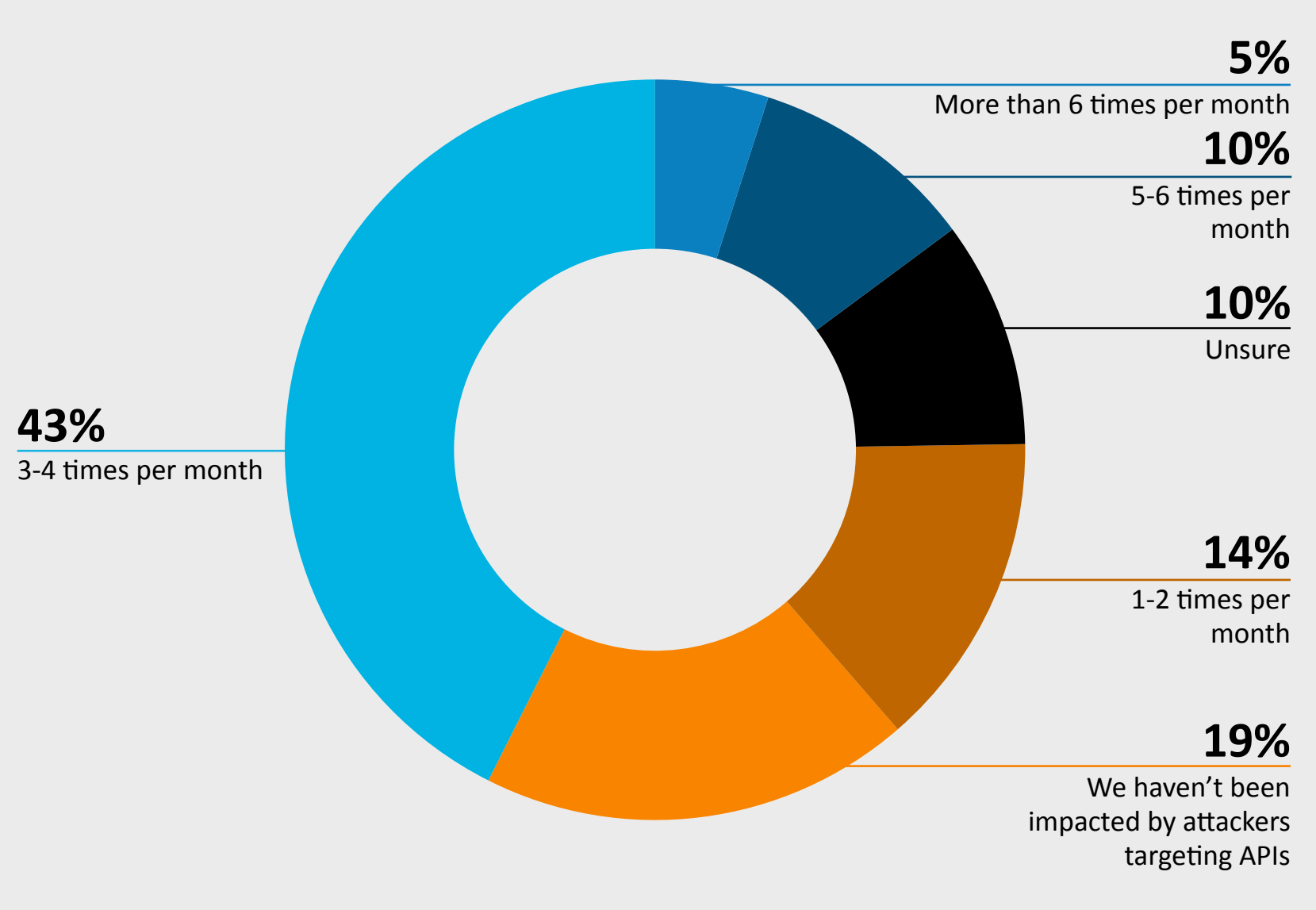
What API technologies drive the most API business value?



APIs are now the number one attack surface exploited by cybercriminals with visibility, authentication enforcement, and content inspection ranking high on the list of API protection priorities.

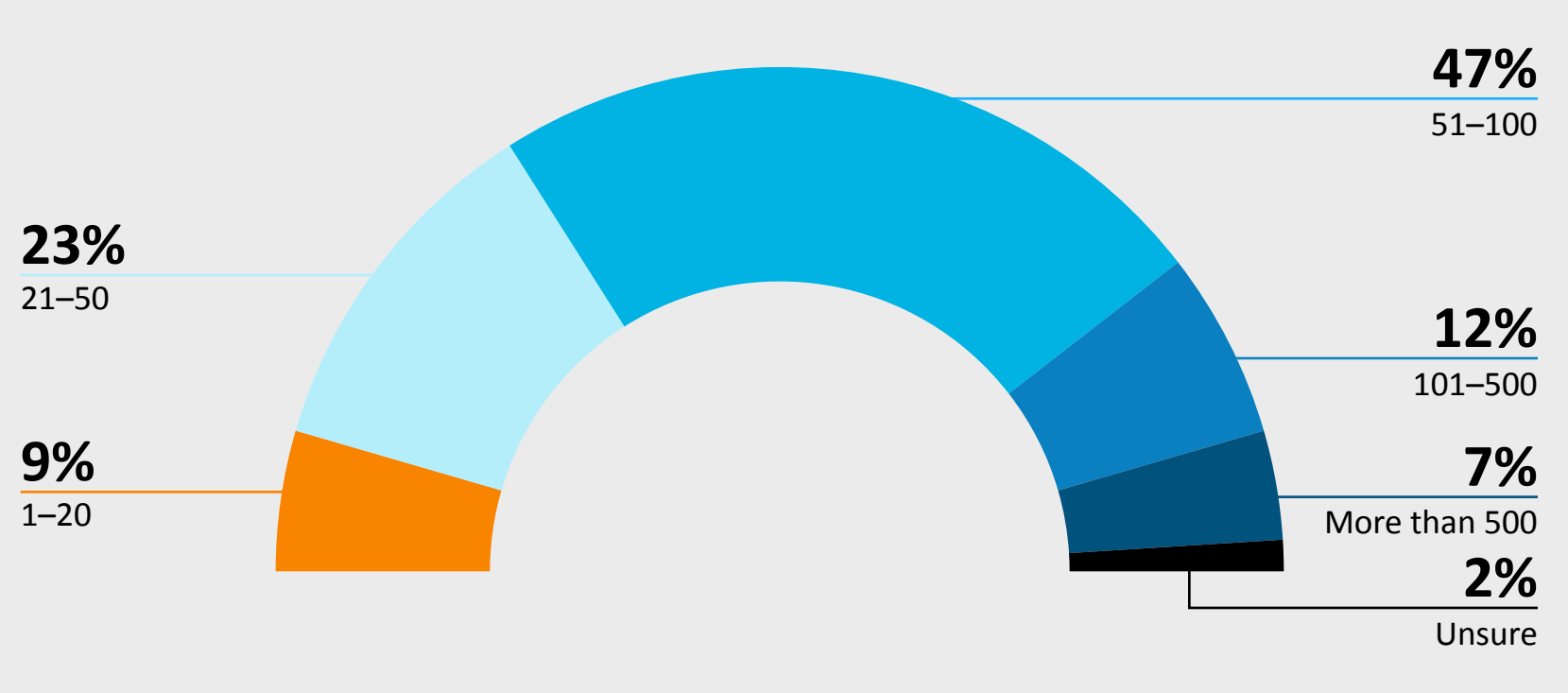
More than half (58%) of the respondents reported that their business has been impacted by more than three API attacks per month. Of greater concern were the 10% who were unsure if they had been impacted.

How often is your business impacted by attackers targeting APIs?



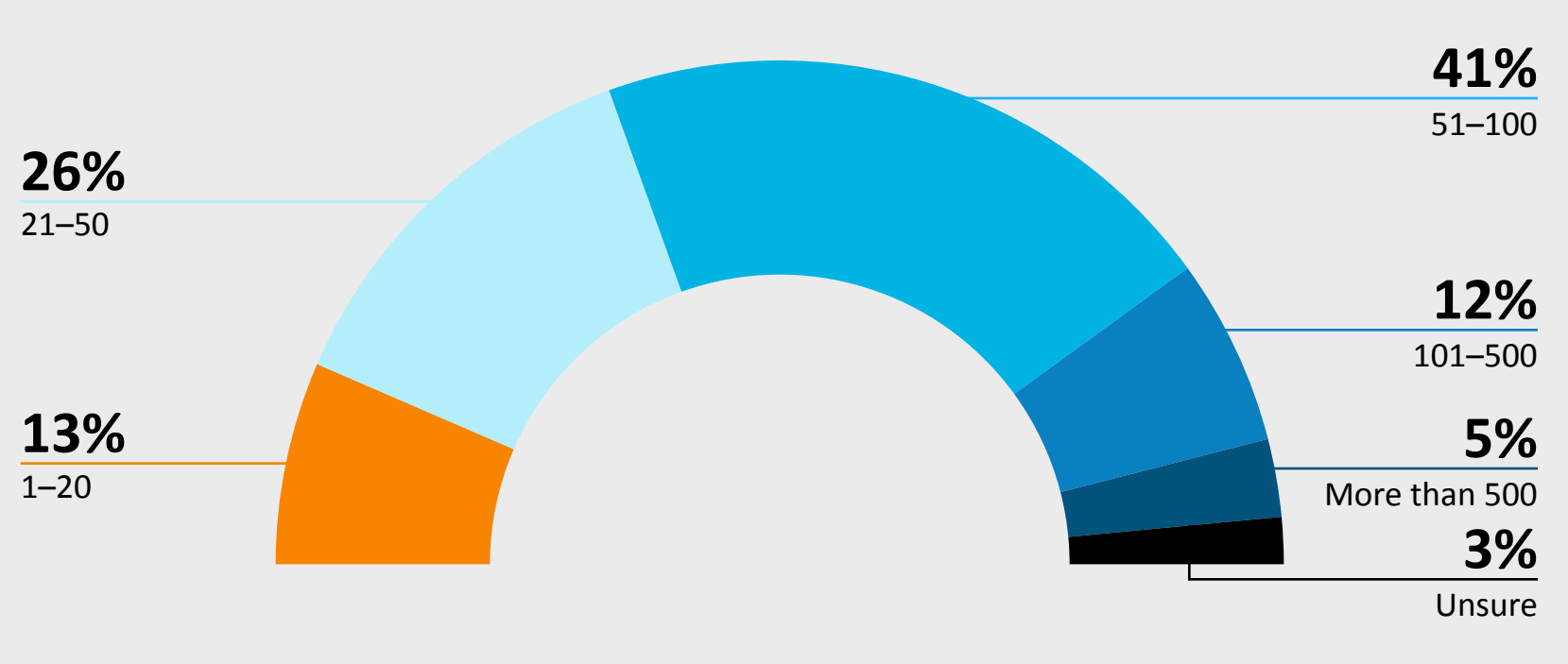
Most IT leaders (70%) reported that their organization was using between 21-100 internal APIs.

How many internal APIs does your organization use?



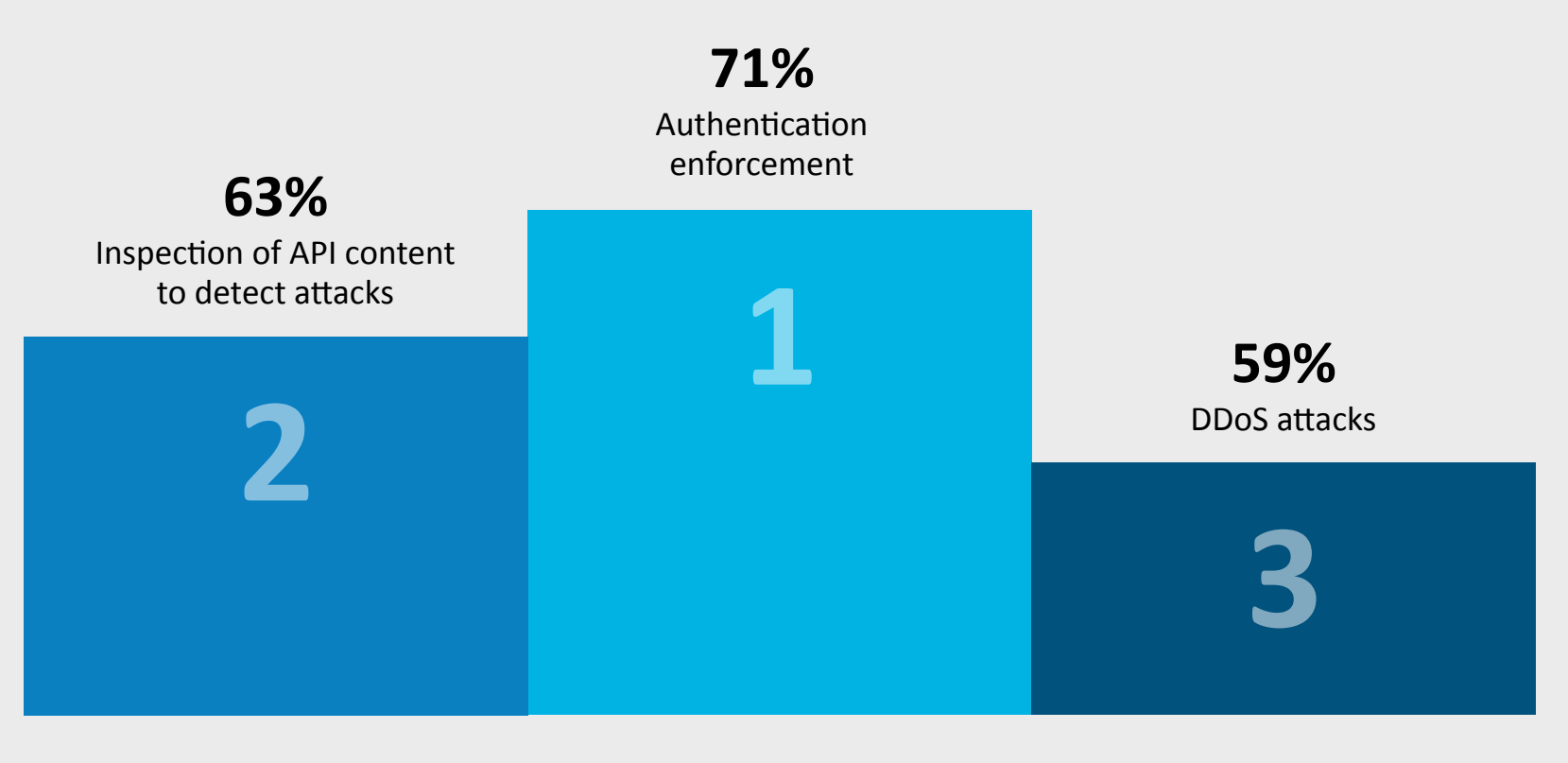
The majority of leaders (67%) also reported that their organization was using between 21-100 external APIs.

How many external APIs does your organization use?



IT leaders are most concerned about authentication enforcement (71%), inspection of API content to detect attacks (63%), and DDoS attacks (59%) when it comes to their organization's use of APIs and the impact on API security.

What are your top three security concerns about using APIs?

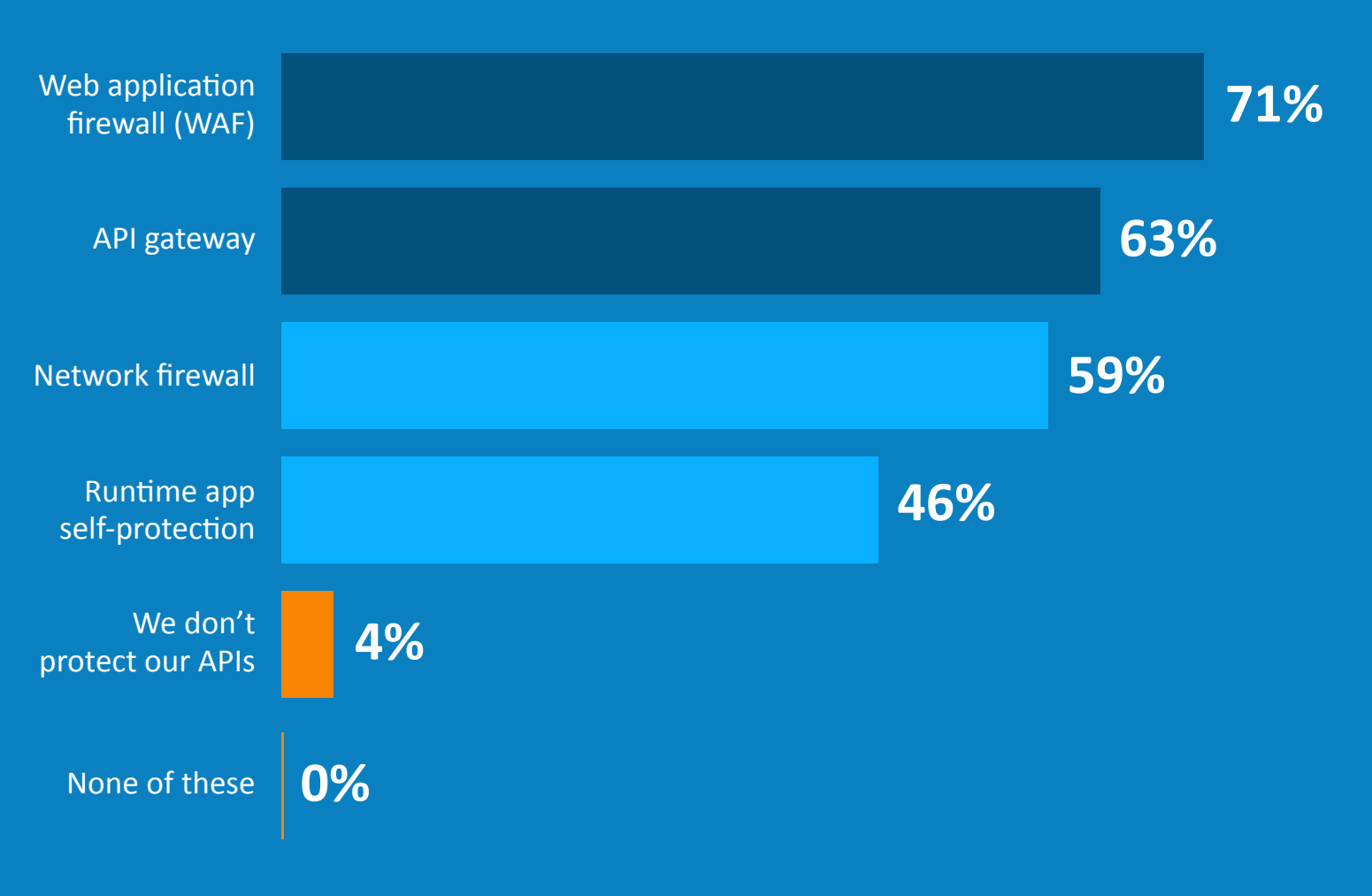


Bot attacks **34%**, Lack of context **27%**, Profile APIs **23%**, No concerns **2%**

API protection deployments remain a mixed bag of disparate solutions that lack sufficient integration to enable rapid response to an API attack.

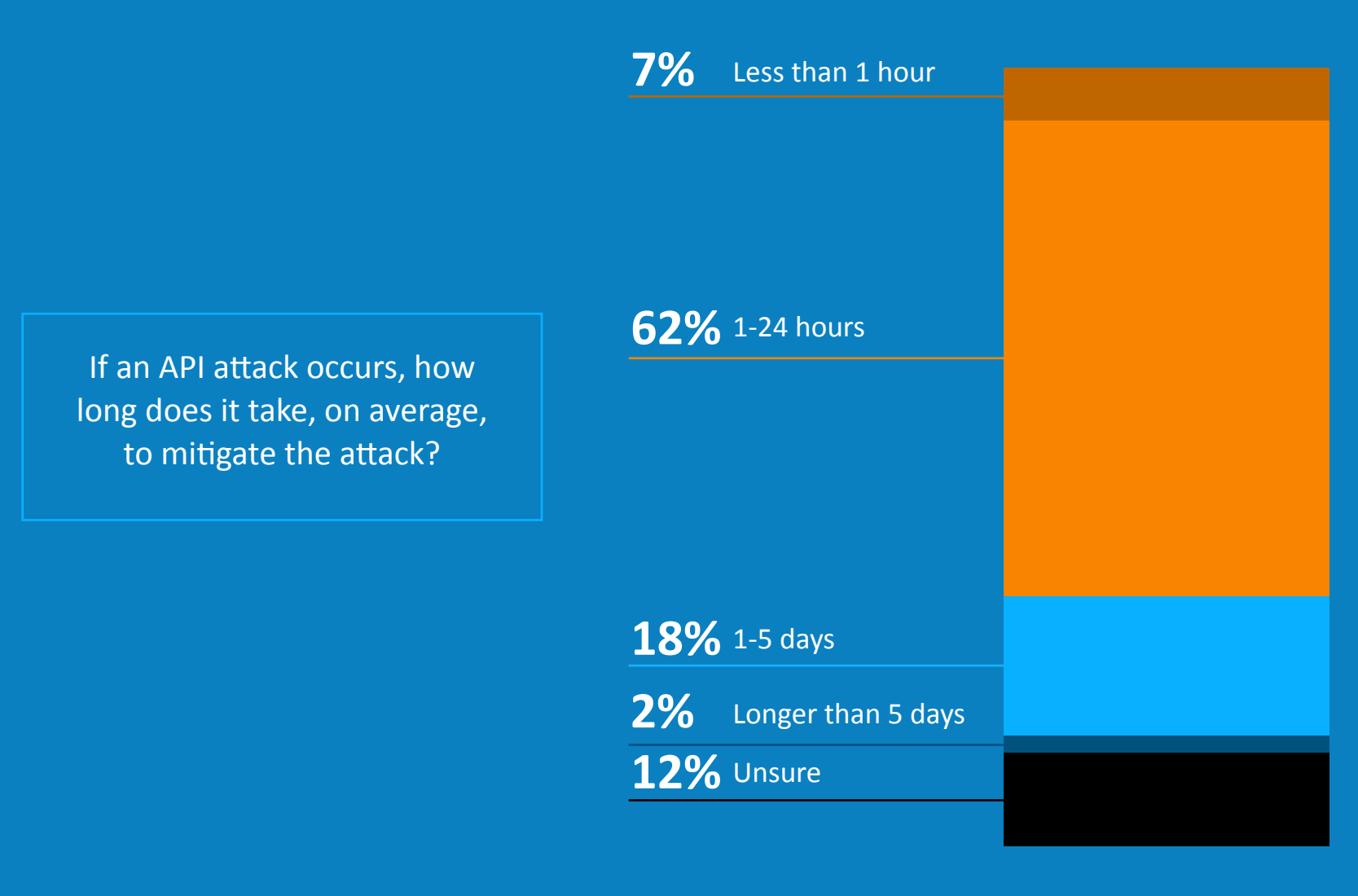
The majority (71%) of IT leaders have deployed either a web application firewall (WAF) and/or an API gateway (63%) to protect their APIs.

Which of the following has your organization deployed to protect your APIs?



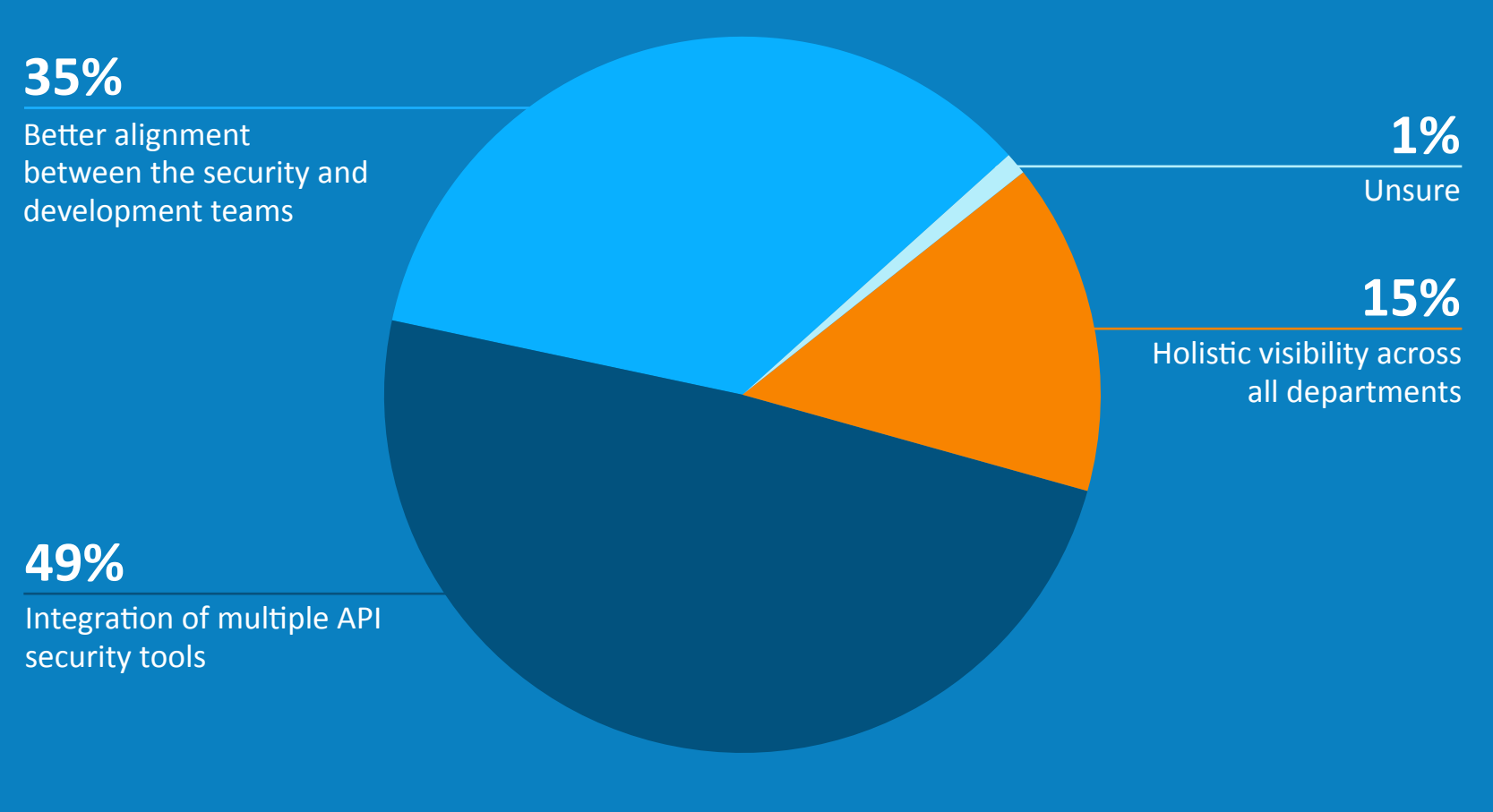
Most IT leaders (69%) are able to mitigate an API attack within 24 hours, yet 20% report that mitigation can take an entire day or longer.

If an API attack occurs, how long does it take, on average, to mitigate the attack?



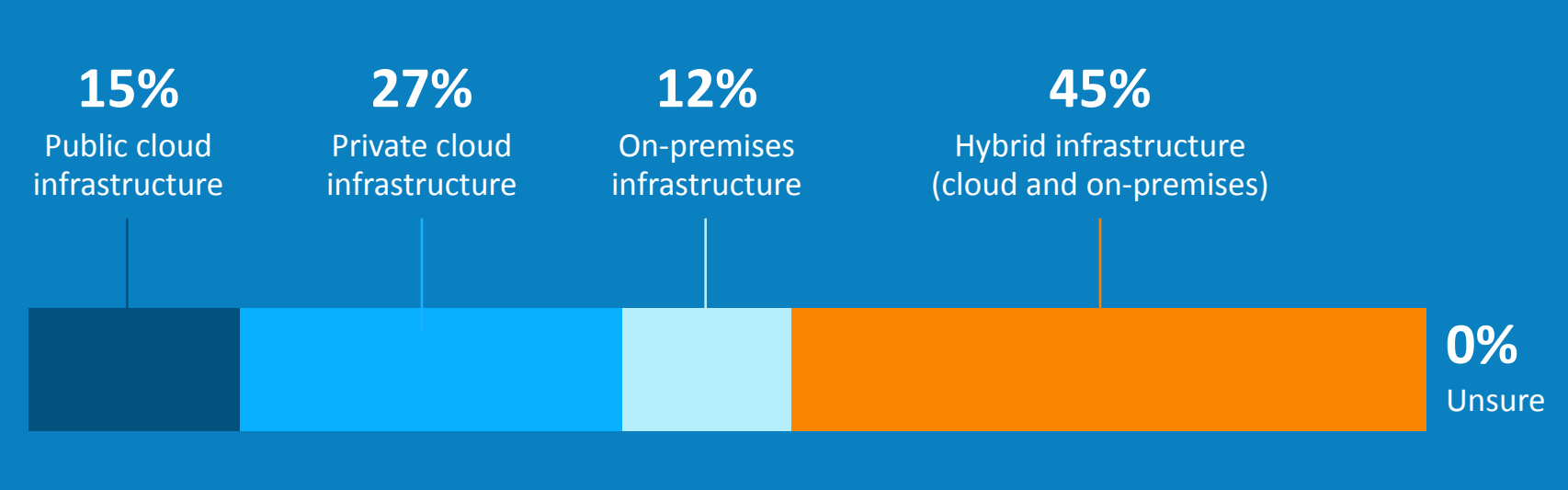
Nearly half (49%) of respondents report that integration with multiple API security tools would have the greatest impact on transparency to their organization's API security tools.

Which of the following would make the greatest impact on transparency in your organization's API portfolio?



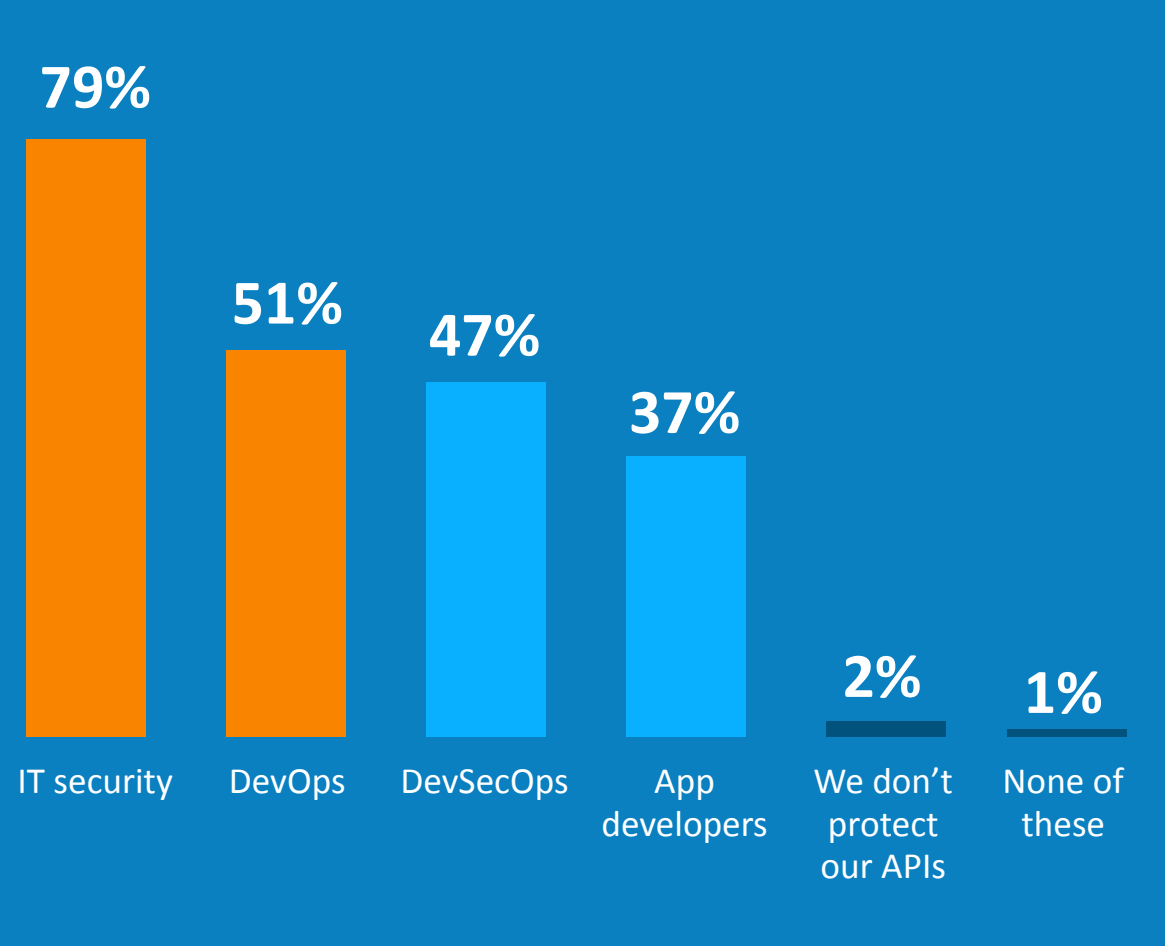
Most respondents (88%) are operating on hybrid or cloud infrastructure.

What is your business infrastructure deployed on?



Most respondents (79%) reported their IT security team oversees API protection.

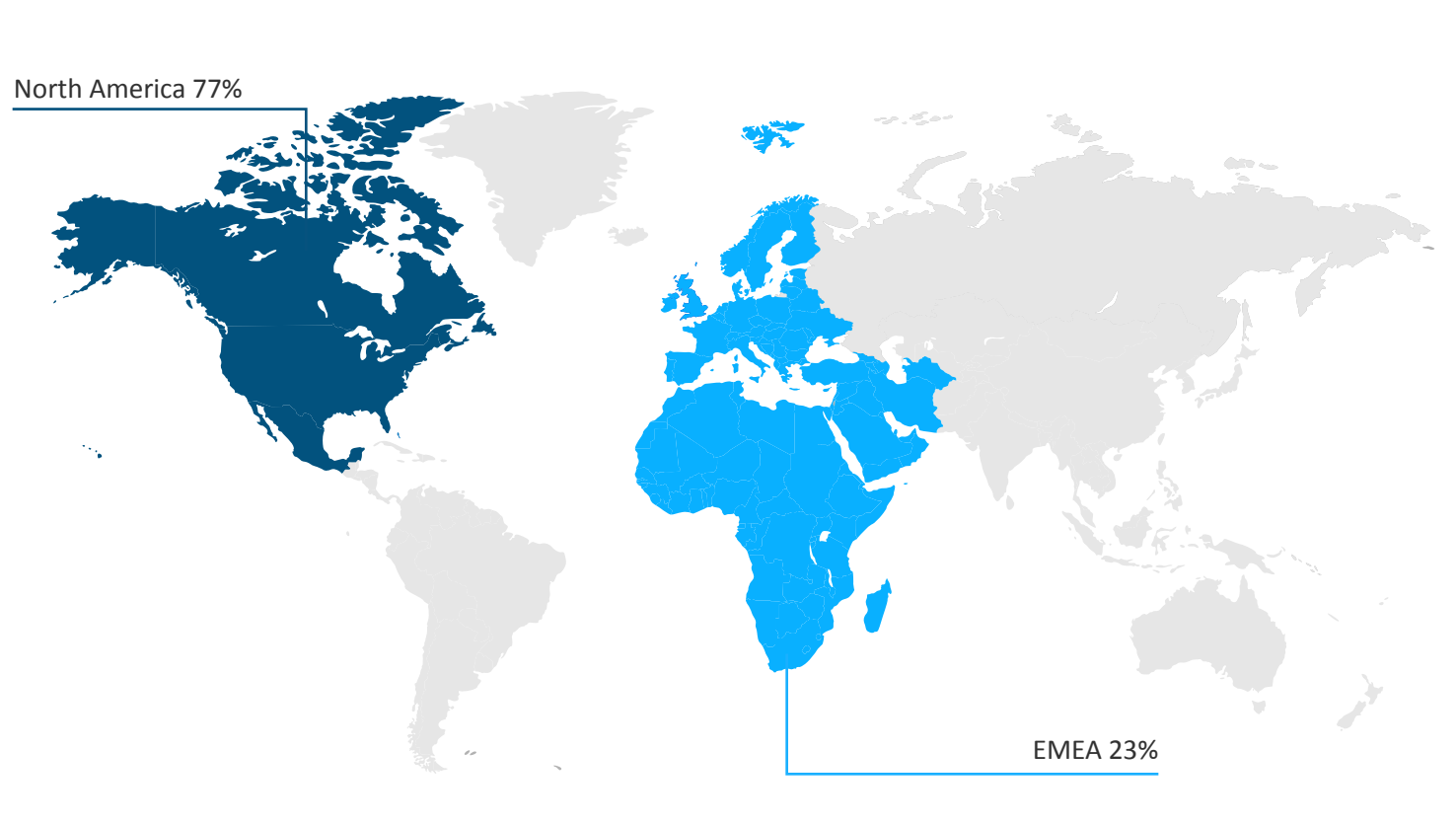
Which team(s) oversees deployment and ongoing API protection?



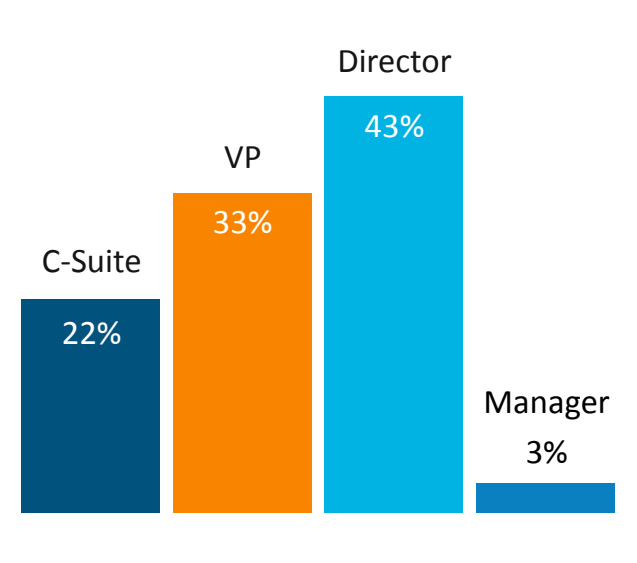
Cequence Security protects today's hyper-connected enterprises from fraud, business abuse, data loss and non-compliance caused by attacks against web, mobile, and API-based applications. To get a free API security assessment and an attacker's view of your API threat footprint, visit **cequence.ai/assessment/**.

RESPONDENT BREAKDOWN

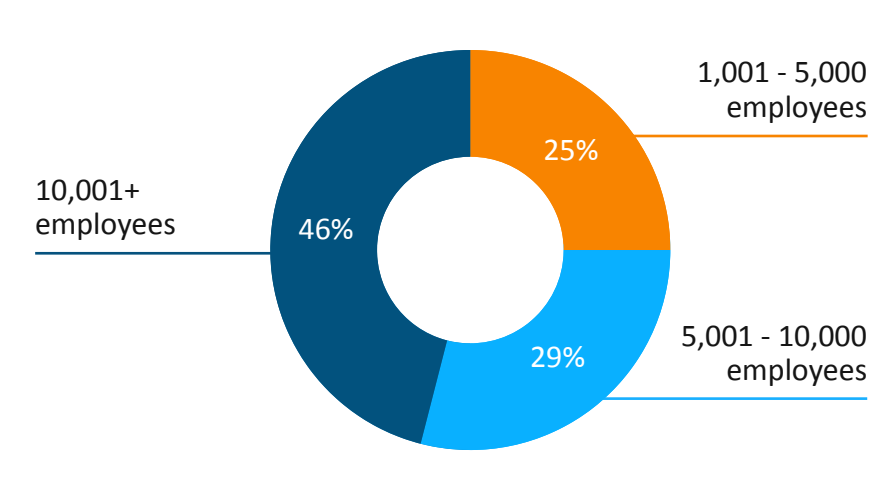
REGION



TITLE



COMPANY SIZE



Gartner

Source: Gartner Peer Insights, Maximizing API Business Value