IMVISION

API Security is Coming.

Are You Ready?

Industry Survey: Enterprise API Security | 2021

Table of Contents

Introduction and Key Findings 3

Introduction.....4

API security is a top priority for today's security leaders.....5

We're seeing a clear drive for an 'API Security Backbone'.....6

API Management is only part of the story.....7

Mind the Gap: Traditional application security tools don't fit.....8

Who's the Boss? There's a challenge of responsibility.....9

"He Who Pays the Piper Calls the Tune".....10

Enterprises and APIs..... 11

Number of APIs per Company.....12

Types of APIs Used by Organizations.....13

Company's API Strategy.....14

Vulnerabilities & Challenges.....15

APIs with Highest Vulnerability.....16

API Security Top Challenges.....17

Barriers to Improving API Security.....18

Priorities & Best Practices.....19

API Security Priority - Next 12-24 Months.....20

API Security Priorities in 2021.....22

Technology Usage and Plans for API Security.....22

API Security Testing Frequency.....23

Demographics.....24

Acknowledgements.....27

About Imvision.....28

Introduction & Key Findings

Introduction

For the modern enterprise, APIs are no longer just a technological infrastructure. Rapidly becoming the new application layer, APIs connect organizations and users to deliver value in new ways, emerging as an integral part of the business itself. More APIs means greater value, but it also means greater attack surface - and new types of vulnerabilities.

As a leading security company that specializes in discovering, testing and protecting APIs, Imvision asked over 100 senior security leaders in large enterprises how today's organizations are handling API security:

What security methods are in place, and which have security leaders already lost trust in? Who currently has the ultimate authority when it comes to APIs, and who is watching from the sidelines, hoping for more control?

The results paint a fascinating picture of the security landscape today, showing that APIs pose new challenges and vulnerabilities that many organizations are not yet sure how to stay on top of. In many cases, even the responsibility over APIs is difficult to ascertain.

More than anything, this report suggests that cross-team **collaboration is the best way moving forward**: On the one hand, the accumulated experience of the security team from traditional areas of enterprise security, and on the other, the intimate understanding of the API team into the nature of APIs and their unique challenges.

This report highlights how forward-thinking security leaders can stay ahead of the curve, working together with other teams to build something meaningful for the business and accelerating digital transformation.

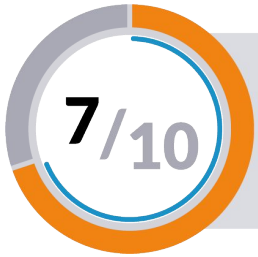
API security is a top priority for today's security leaders

Over the next 24 months, 91% of security leaders will be making API security a priority, while 80% would like to gain more control over their APIs.

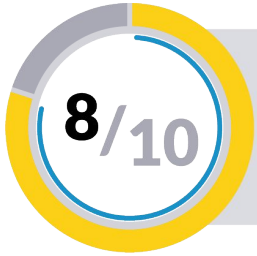
This is not surprising given how many APIs companies currently have: 73% of enterprises use more than 50 APIs, and growing.

This is tough to manage, especially when you consider that 4 out of 5 publish APIs for external consumption by partners and clients.

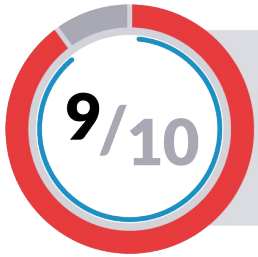
Ultimately, only 1/3 of security leaders think their APIs get the protection they need.



Enterprises use more than 50 APIs



Of security leaders wish to have more control over API security



Of security leaders are API security as a priority over the next 12-24 months

We’re seeing a clear drive for an ‘API Security Backbone’

Security leaders have three top priorities for API security: Access Control (63%), Security Testing (53%), and Anomaly Detection and Prevention (43%). On top of these main capabilities, the key enablers for securing APIs are integration with the organization’s existing systems (52%) and gaining visibility into their APIs in the first place (50%).

While it is tempting to think of API security as a set of separate efforts, technologies and responsibilities, every API is a unique attack surface that needs all the different security components effectively working together around it.

It is becoming increasingly clear to security leaders that if you want a strong foundation for API security, you need to at least get these three items right. **That's how you form the ‘API Security Backbone.’**

API Management is only part of the story

The most widely used technology that supports API security is the API Management (APIM) platform, with 4 out of 5 enterprises using or considering using them. At the same time, most security leaders now recognize that this isn't enough – only 18% see the APIs managed by the APIM as being the highest risk APIs to protect.

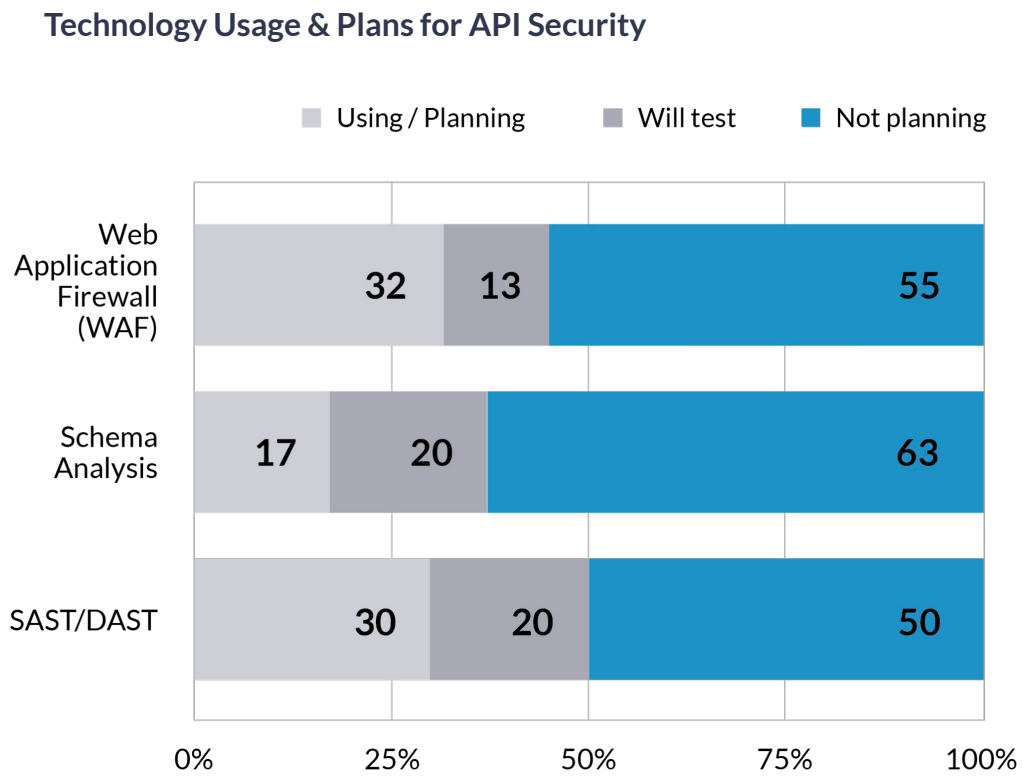
However, while APIM handles Access Control and provides some Runtime Protection as part of the API Gateway, it generally uses basic policies to enforce the schema and lacks critical security capabilities: It doesn't cover the API business logic and functionality, thus failing to stop API abuse. Moreover, it provides no support for security testing. With only 19% of organizations testing their APIs daily, **security testing is emerging as a top factor for security leaders.**

Mind the Gap: Traditional application security tools don't fit

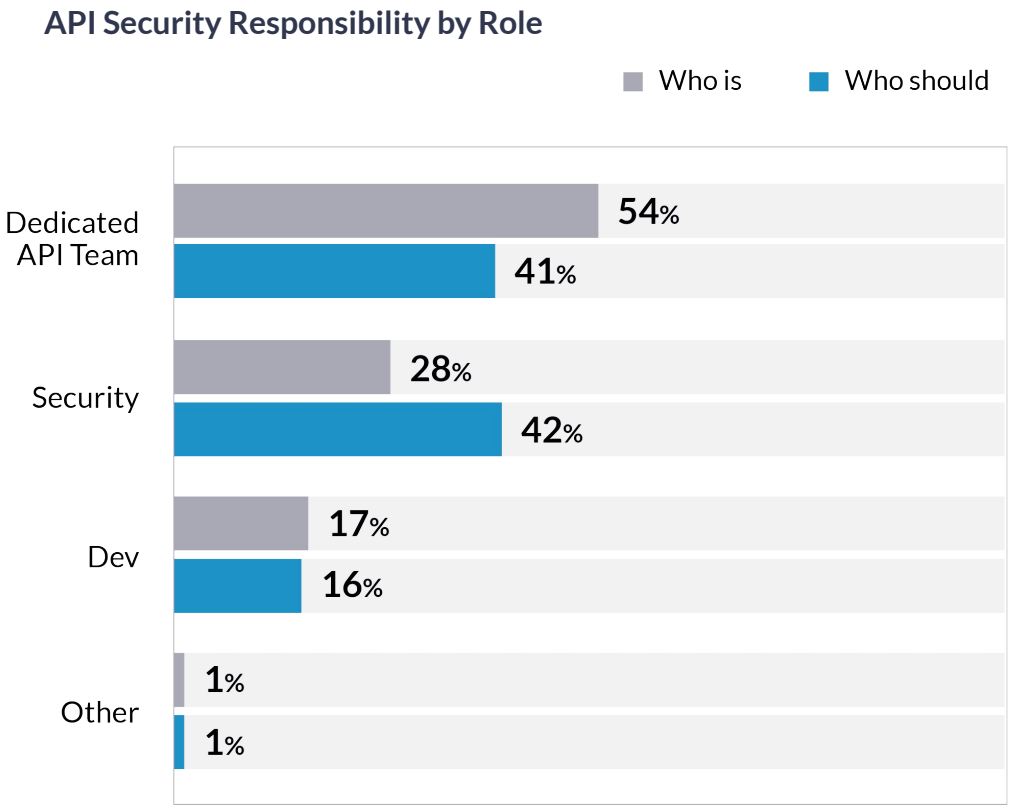
General-purpose application security solutions such as WAF and SAST/DAST are common tools that various vendors put forward also for API security.

However, our respondents overwhelmingly commented that these are not on their roadmap for that purpose – for 50% or more of security leaders, these systems aren't even an option.

As the attack surface grows, today's organizations know that their current tools are limited, but can't find a viable alternative – making it accepted wisdom that there is a need for new technologies for runtime protection and security testing to complement the APIM as part of their API security backbone.



Who's the Boss? There's a challenge of responsibility



Our report shows that most enterprises handle API security by centralized integration teams, whether a center of excellence, a dedicated API team, or some other entity. As these teams commonly operate the API Management platform, it stands to reason that API security falls on them.

However, security leaders believe that they should be in charge of API security, alongside the API team.

This suggests a collaboration is the best way forward: On the one hand, the experience from traditional areas of enterprise security (e.g. network and application) can be leveraged in an API Security program. On the other, the nature of APIs present unique challenges best understood by the dedicated API team.

“He Who Pays the Piper Calls the Tune”

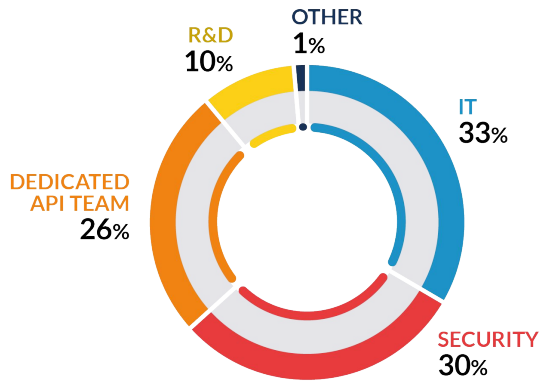
With enterprises opening up and growing their use of APIs along their digital transformation journey, we can see a shift in responsibility - and budget - accordingly.

Once companies have more than 50 APIs, R&D and IT teams take a step back, as security gets more involved with 39% of the responsibility – up from only 5% when there are less than 50 APIs to manage.

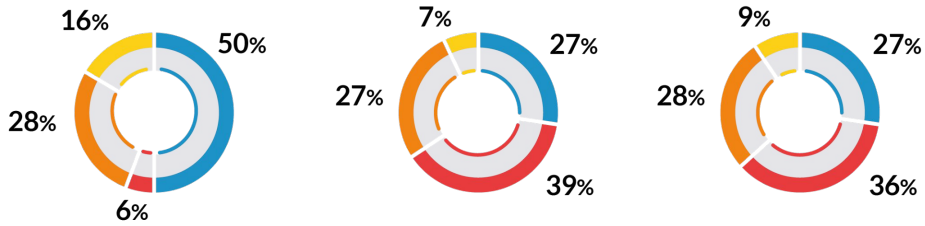
The lack of a clear go-to option for enterprises when it comes to API security budget further reinforces the need for collaboration, as no single team is the obvious choice.

Whoever takes the lead, it is clear that the mutual influence and cooperation is ever more important for helping today’s future-focused organizations achieve the ideal API security backbone.

API Security Budget Owners



API Security Budget Owners by Number of APIs



Enterprises ❤️ APIs

APIs are everywhere

Practically every enterprise these days has APIs.

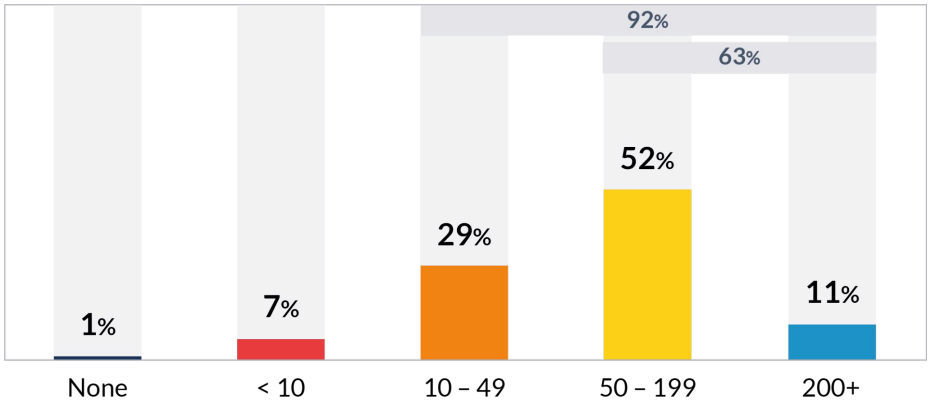
The security leaders survey cited a 92% rate of enterprises with over 10 APIs, and a 73% rate of enterprises with over 50 APIs.

Smaller enterprises seem more comfortable adopting API technology, moving much faster on the digital transformation journey.

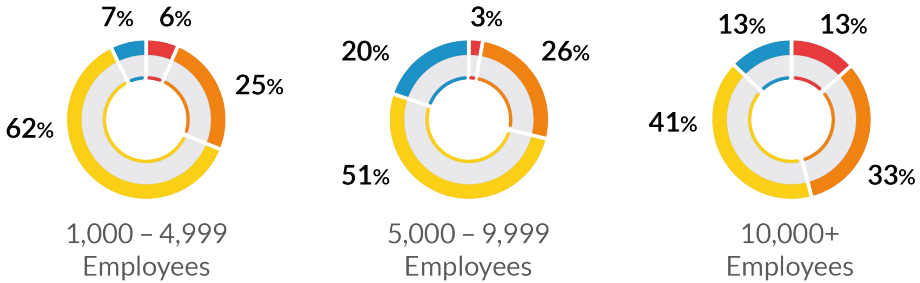
Nonetheless, 54% of large enterprises with 10,000+ employees today have over 50 APIs.

Although an organization may have 50 APIs, the actual number of endpoints can be much higher, increasing the complexity of protecting the underlying functionality.

Number of APIs per Company



Number of APIs per Company by Company Size

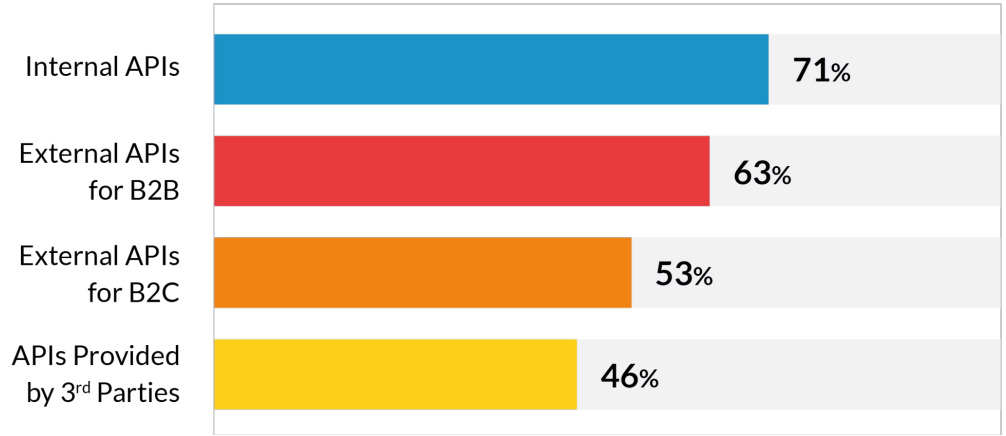


4 out of 5 enterprises enable access to their data through external APIs

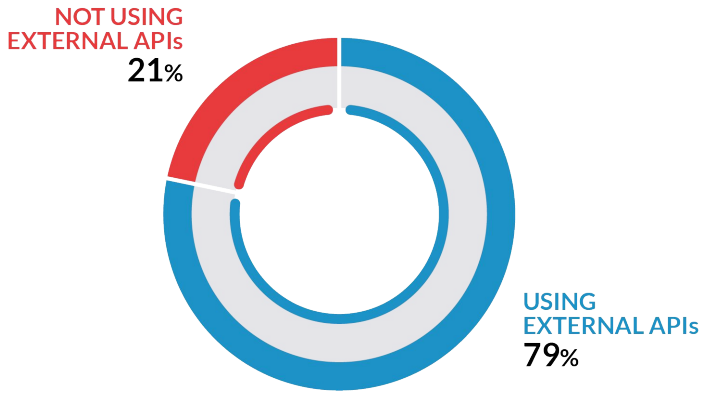
APIs are being used by enterprises for a range of reasons, the most prevalent being Internal APIs - APIs internally used by the organization's developers - with 71% of companies stating they use APIs this way. It was followed by External APIs for B2B (Private APIs published by organizations to be consumed by their business partners) with 63% and External APIs for B2C (Private APIs consumed by consumers via mobile applications) with 53%.

In general, **4 out of 5 organizations enable either partners (B2b) or users (B2C) to access their data using external APIs.**

Types of APIs used by Organizations



Usage of External APIs



Integration and performance lead, but the business is catching up

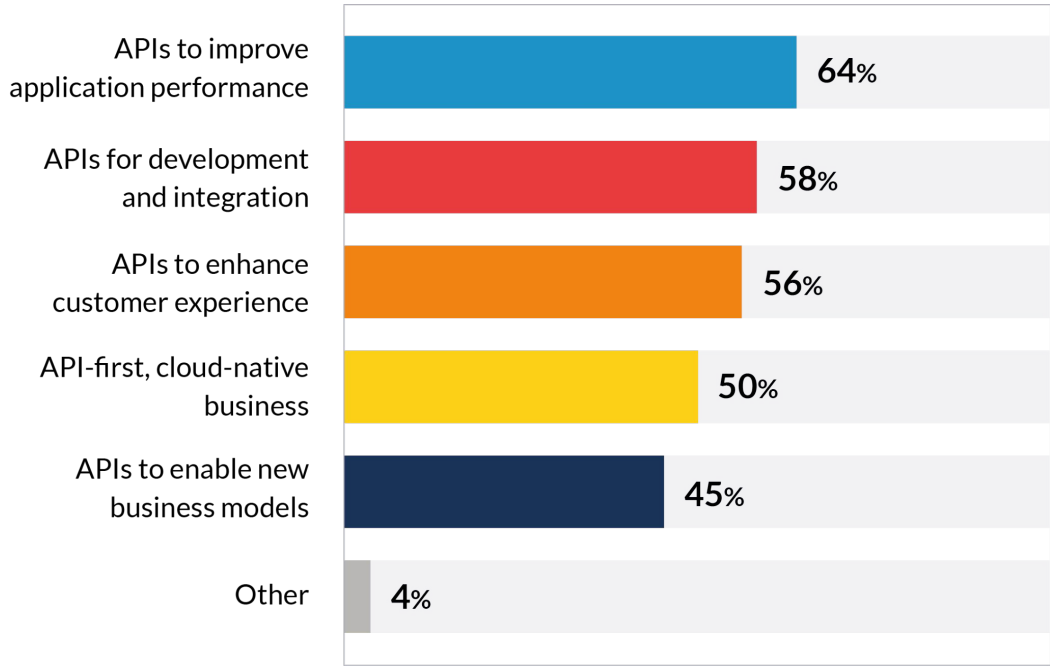
With internal APIs being the leading type used by companies, it isn't surprising that for the majority of enterprises the main thrust of their API strategy is to improve application performance (64%) and development and integration (58%).

But business APIs to enhance customer experience aren't far behind (56%) either, indicating a growing reliance on APIs for the business.

Beyond these drivers of API adoption, it's important to note that for large enterprises there can also be many APIs that originate externally from M&A activities, rather than developed internally.

Organizations are moving into a new digital era, using APIs to deliver value in new ways, making APIs an integral part of the business itself.

Company's API Strategy



Vulnerabilities & Challenges

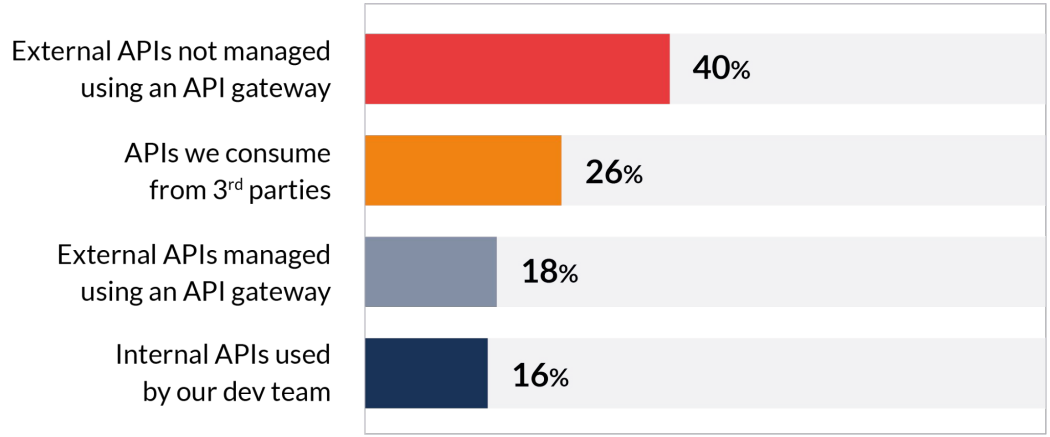
API Gateways are only as good as the APIs they manage

Some APIs are more vulnerable than others.

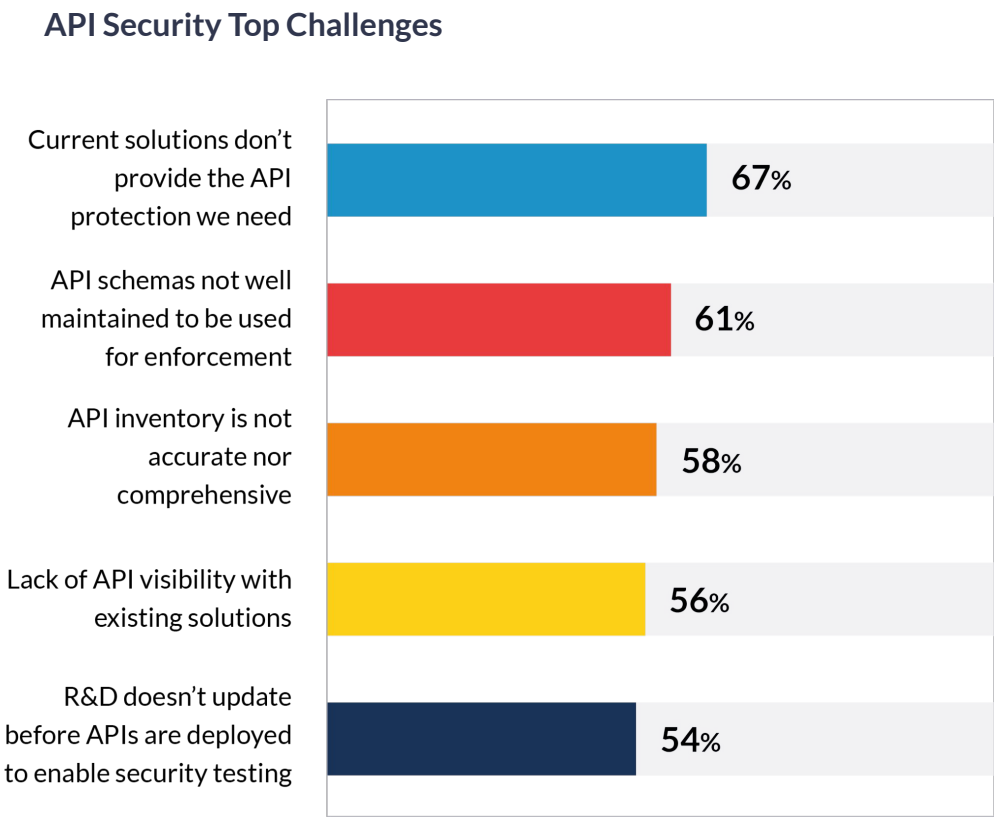
While the API Gateway manages to bring down some vulnerabilities, it's not surprising that the top vulnerability revolves around APIs that are not managed through these platforms - making shadow APIs the most vulnerable according to 40% of survey respondents.

It is interesting to note that APIs consumed from 3rd parties seem to claim the second spot for top API security threats, possibly as a result of the SolarWinds breach that used such APIs.

APIs with Highest Vulnerability



API security is undermined by maintenance of the inventory and schemas



Securing APIs can be a challenging task, and the majority of security leaders agree that the current processes and tools are not up for the task.

When asked what API security challenges companies are facing today, at the top, 64% of survey respondents indicated their current solutions simply do not provide the API protection that they need.

This was followed by R&D not maintaining the schemas well enough to be used for enforcement (61%) and API inventory not being accurate or comprehensive (58%).

The last two are important because they relate to the security team's ability to define API policies that can be effectively used for enforcement.

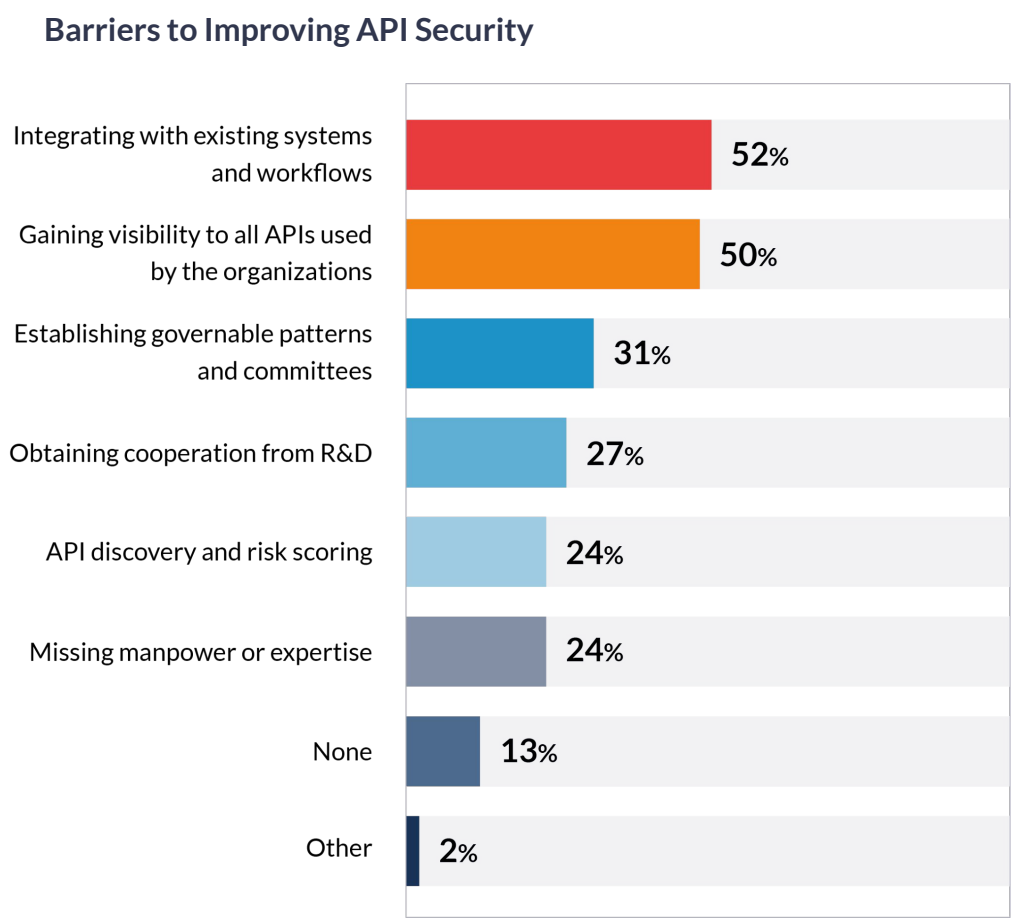
Integration and visibility are seen as main barriers to improving API security

Only 13% of companies have no barriers for improving API security.

For the other 87% of companies, the top two barriers that stand out are integrating with existing systems and workflows (52%) and gaining visibility to all APIs used by the organization (50%).

These two challenges are not surprising, as discovery and integrations are consistent security enablers. Companies struggle to effectively implement security solutions that improve their posture without overcoming these barriers.

Also worth noting that 1 out of 4 security leaders sees cooperation from R&D as a top barrier.



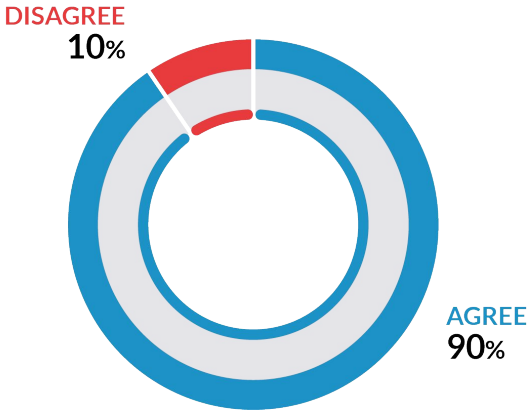
Priorities & Best Practices

The security of APIs is a top priority for most security leaders today

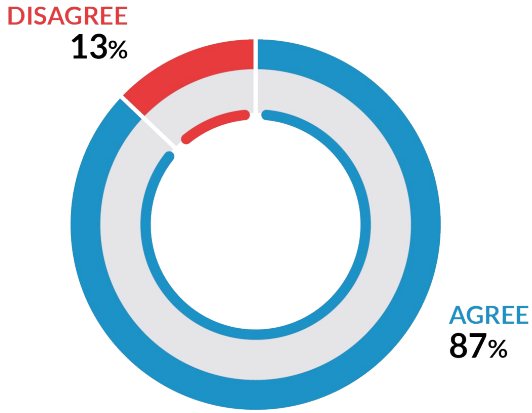
APIs are here to stay, and security leaders are realizing that APIs create a new technological layer that requires special attention.

When asked about the priority of API security over the next 12-24 months, 9 out of 10 said this is a high priority. 87% said they would like to gain more control over their APIs.

"API security is a priority for us over the next 12-24 months"



"I want to have more control over our API security"

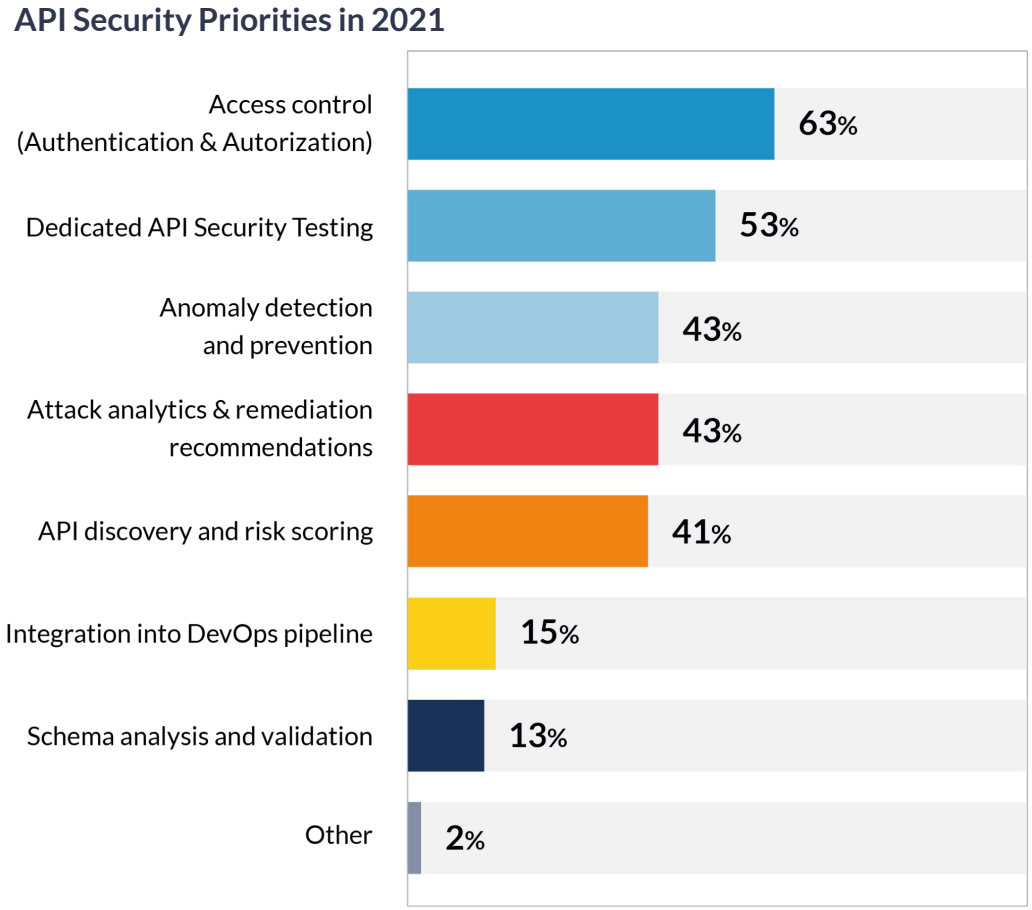


Security leaders are seeking a holistic solution for API protection

While it is tempting to view API security as a set of separate efforts, technologies and responsibilities, every API is a unique attack surface that needs the different security components effectively working together around it.

Security leaders have three top priorities for API security: Access Control (63%), Security Testing (53%), and Anomaly Detection and Prevention (43%).

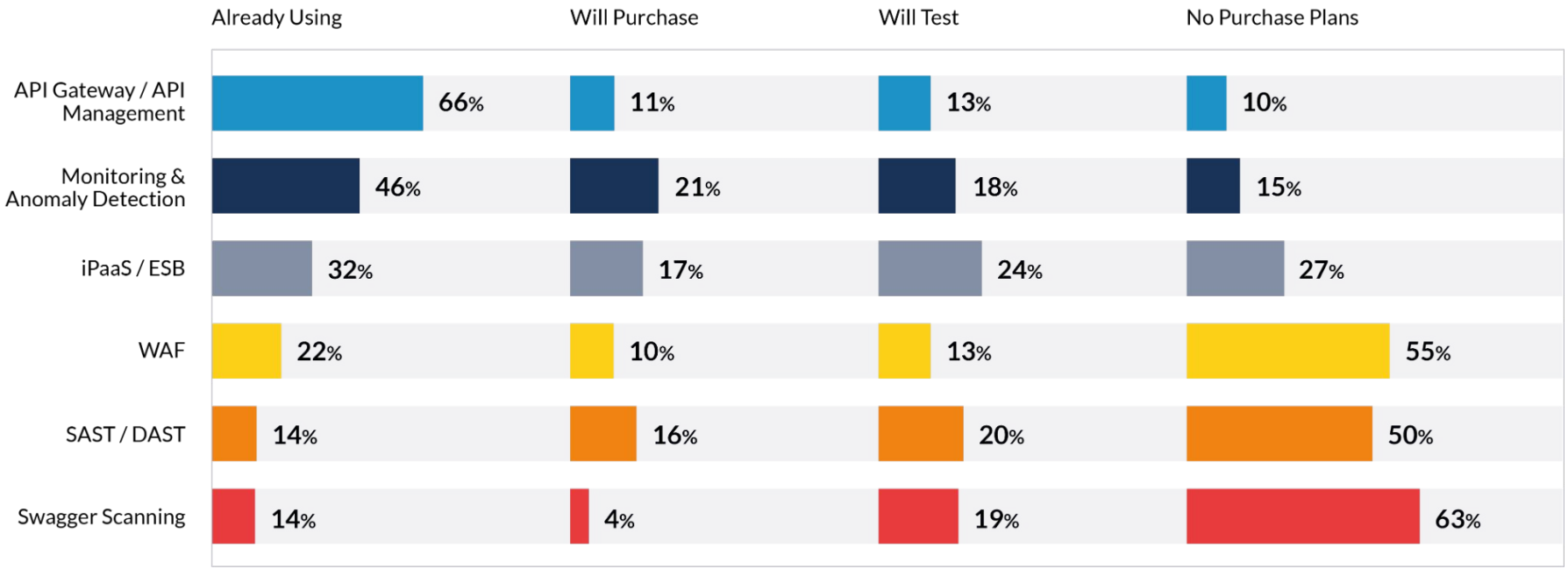
Together, these three components make up the **API security backbone**, a holistic approach that can generate strong foundations towards a mature and robust API security strategy for digital enterprises.



Traditional application security solutions are not on the roadmap

By far, API management/gateway is the most popular technology to enhance management and security of APIs by enabling improved access control and certain runtime protections, with 90% already using, planning to, or considering to test it in 2021.

What is perhaps most interesting is that security leaders overwhelmingly commented that traditional Application Security solutions - WAF and Application Security Testing - are not on their roadmap for securing APIs. For 50% or more of security leaders, these systems aren't even prioritized as an option. As the attack surface grows, organizations know that their current tools are limited.



Consistency of API security testing remains a challenge

Virtually all companies test their APIs.

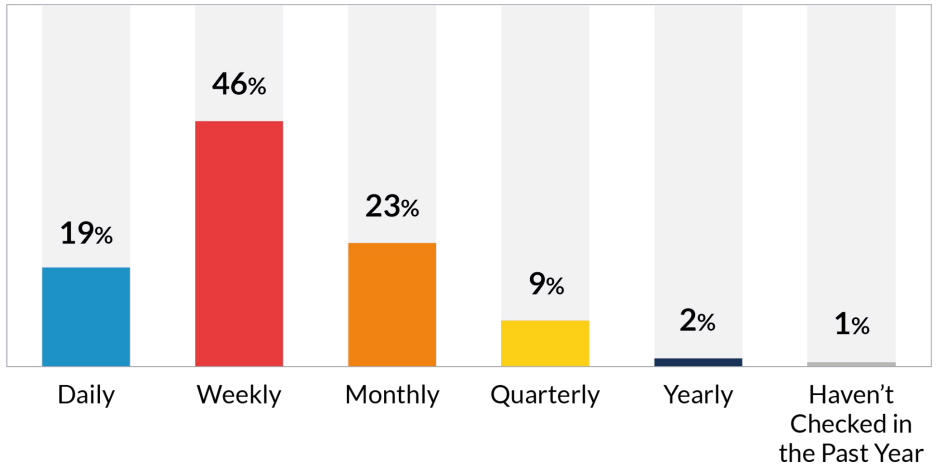
Since the use of APIs is constantly growing, it is essential for testing to be consistent - both in frequency and scope - on a regular basis.

Only 19% of survey respondents test APIs daily, while 35% do so on a monthly basis - or less.

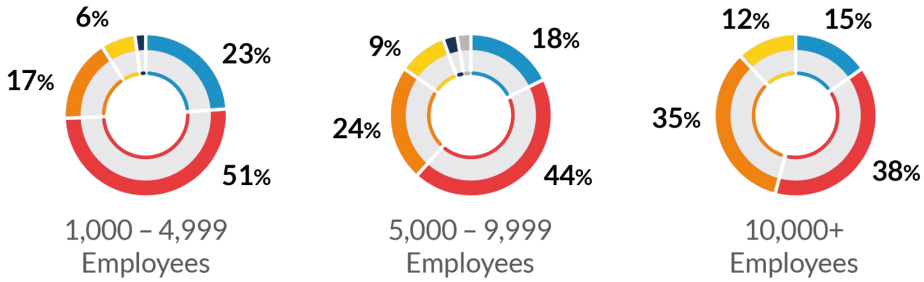
As we break down testing frequency by company size, we can see that testing frequency declines with increasing company size.

Companies with 10,000+ employees test less often (53% on a weekly or daily basis) compared to those with 1,000-4,999 employees (74%).

API Security Testing Frequency



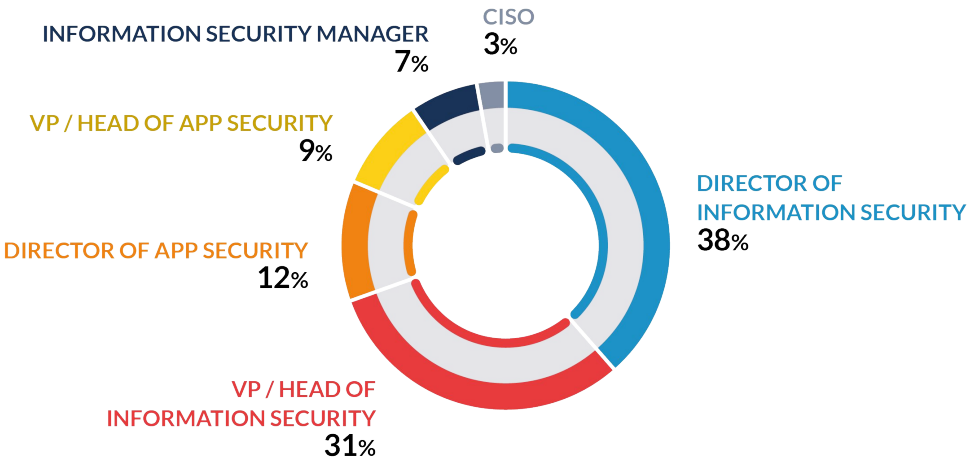
API Security Testing Frequency by Company Size



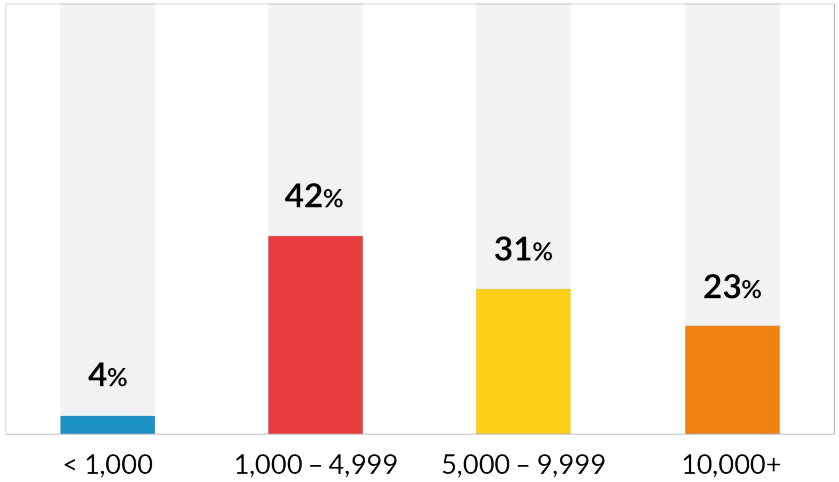
Demographics

Respondents by job role and company size

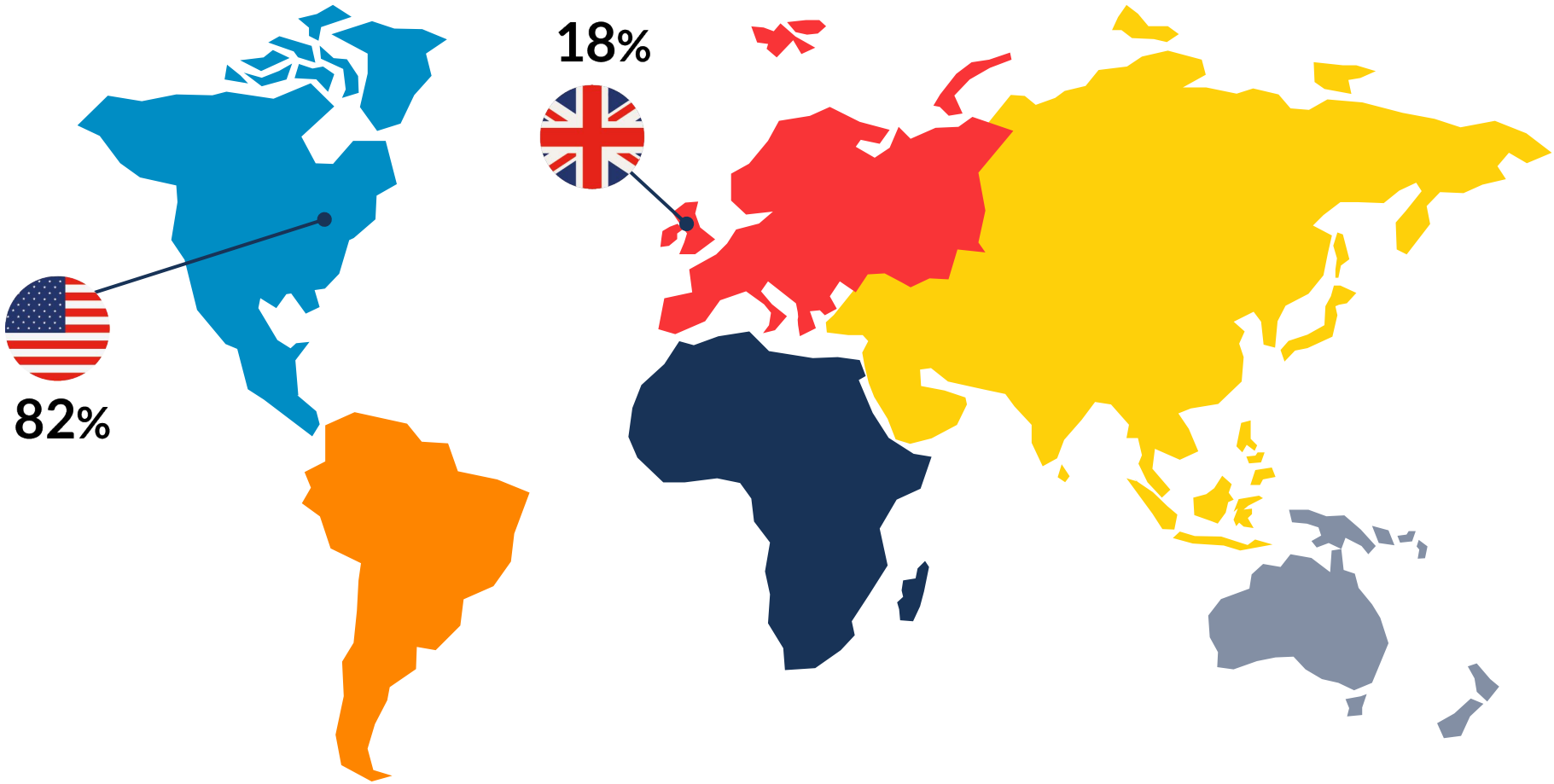
Job role



Company size



Respondents by country



Acknowledgements

Imvision wishes to thank the following experts for their valuable professional contribution to this report:

Rahul Agarwal

Product Manager for Dell Boomi API Management Platform

Bill Doerrfeld

Editor in Chief
Nordic APIs

Corey Ball

Cybersecurity Consulting Manager, Author '*Hacking APIs*' (upcoming book)

Anthony Lonergan

API Security consultant
insidedefense.net

Ravi Krishnan MuthuKrishnan

Security Expert

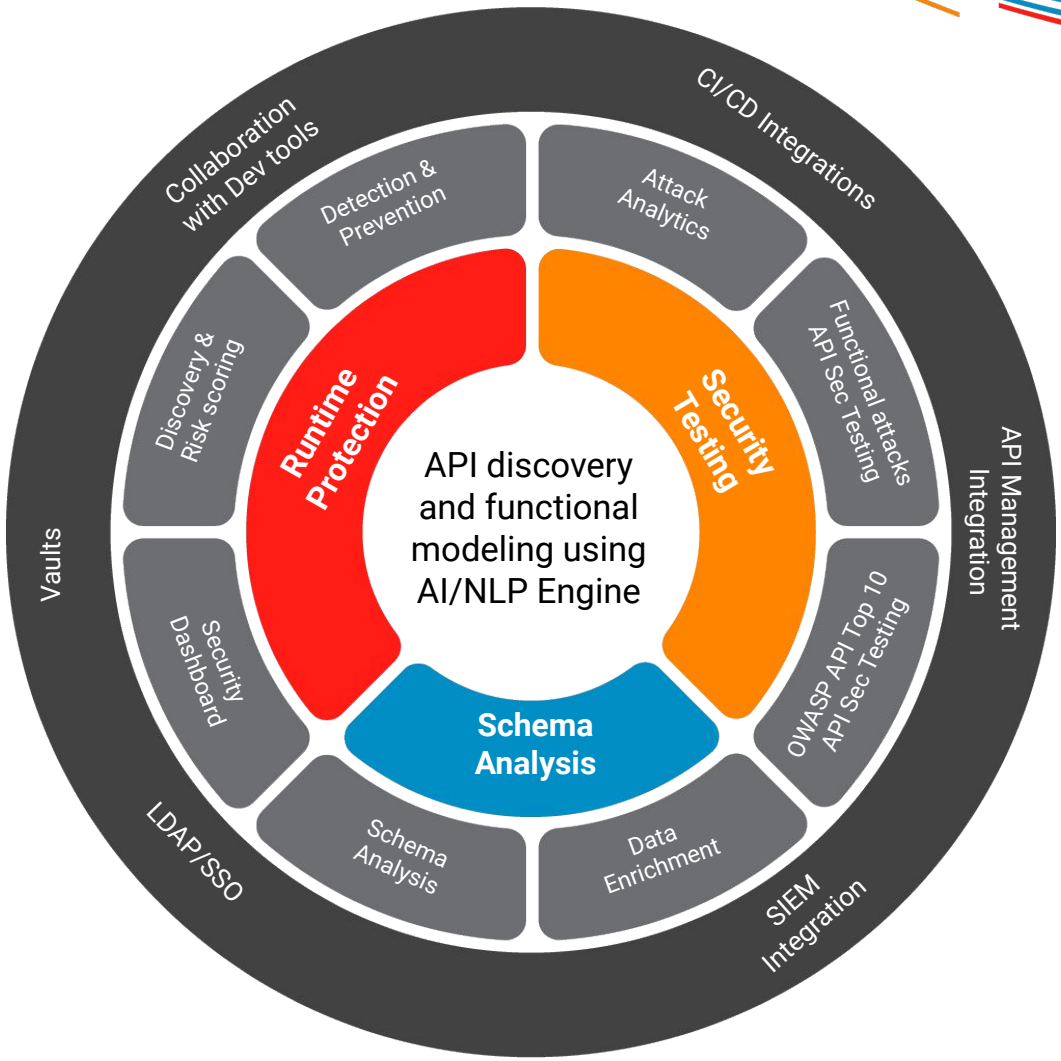
About Imvision

At Imvision, we help enterprises to open up without being vulnerable. It's about making sure that every interaction between people, businesses, and machines can be trusted.

Imvision's platform helps enterprise security leaders, including Fortune 500 companies, discover, test, detect and prevent API breaches. We help you automatically give every API the protection it deserves - at any scale, across the lifecycle.

By using NLP-based technology to analyze each API's unique dialogue and understand the application's behavior, security and development teams can stay ahead of attackers, focus on what really matters and minimize time-to-remediation.

Only when we know that our data is secure can we begin reimagining the boundaries of how it can be used.



Start Free 90-Day Trial

For more information: