A TYK POINT OF VIEW IN PARTNERSHIP WITH NIMBUS NINETY

Secure Your Path to Revenue Growth

Contents

Acknowledgements

For the purpose of this report, we spoke to senior architectural and technical leaders from industries including retail, media, finance, telecommunications and the public sector. The authors thank the senior leaders who gave their time to be interviewed for this paper in the second half of 2021. Their views, some of which are quoted in the following pages, have guided the direction of this report. We are grateful for their invaluable contributions and insights.

Tyk + Nimbus Ninety

Introduction

Application programming interfaces (APIs) are digital rocket fuel.

APIs connect products and services to a vast array of software programs to leverage data and functionality. They enable mobile experiences, connect businesses to the digital economy and facilitate simple and seamless customer engagement.

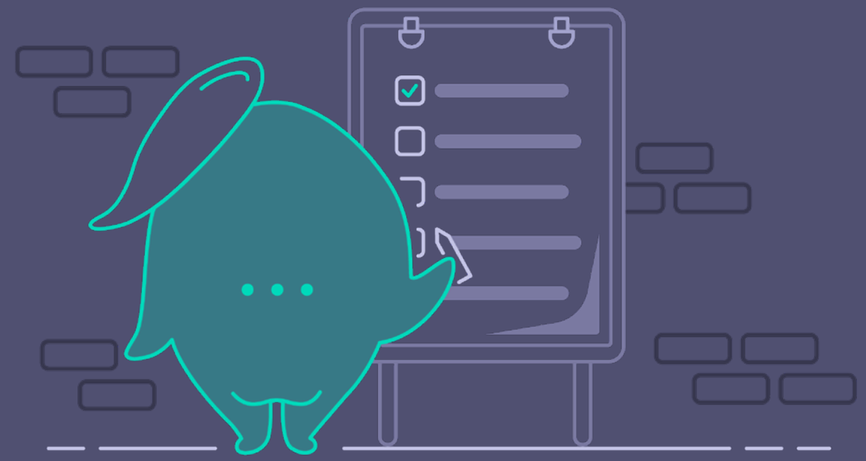
APIs have exponentially proliferated the digital scene in the last decade. Leaders from inside and outside IT departments are increasingly recognising the metamorphic role of APIs to open up their knowledge bases, products and services to ever-wider ecosystems of partners and customers.

But there is a significant catch. Opening access to customer and business data multiplies the points from which hackers with malicious intent can gain control. The development of open APIs, adoption of microservices architecture, containerisation and container orchestration through Kubernetes has the potential to unravel well-established security and governance safeguards quickly. Attackers know this and increasingly they are taking advantage of evolving environments to target emerging vulnerabilities.

Allowing APIs to evolve and flourish in line with business ambitions and customer expectations, while also keeping a tight hold on governance and security, is one of the most taxing conundrums digital leaders face today. To begin to tackle this challenge, it's crucial to consider API vulnerabilities from a number of vantage points. From there, enterprises can develop an API management state of mind: a new way of managing APIs which balances innovation and agility with architecture that is secure by design.

A brief history of APIs

For this research we spoke to a range of industry leaders who each had their own unique set of business objectives, operational models and customer demographics. Despite their differences, a unifying theme was the increasingly ubiquitous and vital presence of APIs for their business.



How have APIs become the bedrock of business?

Embryonic examples of APIs can be traced back to the 1940s and the dawn of computer science. Early examples include library catalogues which told programmers how to call on information in modular software libraries.

The invention of web APIs in the early 2000s was the origin of the omnipresent use of APIs we see today. Following the launch of the world wide web, leading technology companies introduced web APIs to make the vast amounts of data they were sharing more accessible.

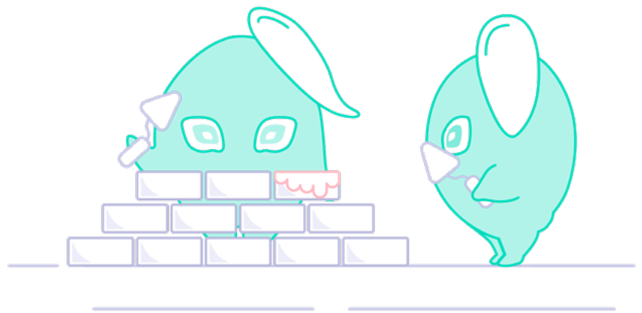
By the end of the decade, the trend for top tech companies to make their APIs open to the public, enabled the API marketplace to grow. The creation of the software architectural styles SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) also supported the wide-spread development of web APIs.

The 2010s brought two key milestones. The first was the shift from web to mobile. This came with changing expectations and more demand for data transacting, interacting and consuming.

The second was a watershed moment for the security and governance of APIs. In 2018, the first European law was passed to govern the use of personal data: the General Data Protection Regulation (GDPR). This regulation dictates how organisations must handle data and the security and governance in place. Since its inception, similar laws have been enacted around the world. Also in 2018, the Cambridge Analytica scandal placed APIs and data privacy firmly in the public consciousness.

As modern APIs settle into their 20s, a range of new challenges and opportunities set the scene. Enterprises worldwide are grappling with how to deliver advanced and agile APIs, while also maintaining the highest levels of data privacy.

In this report, we look at the real-world antipatterns and solutions emerging and consider the important role API management increasingly plays to secure and govern agile and complex APIs.



The API maturity model

We began our research by exploring the maturity of our respondents' approach to API security, as well as their adoption of practices and technologies to mitigate the risks associated with using an increased number of APIs. We asked our respondents a series of questions and found that they fell into one of three categories in our maturity model.

The API maturity model

Beginner

- SOAP is the programming language predominantly in use
- A monolithic architectural style
- APIs operate internally only
- A basic integration is in place between APIs and legacy systems
- Governance is not standardised and is managed in silos.

Intermediate

- REST best practice is observed
- Microservice or service orientated architecture being developed
- APIs are exposed internally and externally
- Kubernetes or high-level orchestration systems are in place
- Governance is clearly defined and standardised
- Authentication is standardised and uses a token-based approach

Advanced

- Conversion capabilities to and from SOAP, REST and GraphQL
- Microservice or service orientated architecture is well established
- APIs are exposed externally and are easily consumable
- A multi-cloud approach with containers is in place
- DevOps principles and agile methodologies are observed
- Governance is managed using an open source API gateway
- APIs are harmonised using an API management tool.

(Fig. A) The characteristics of beginner, intermediate and advanced on the API management maturity model

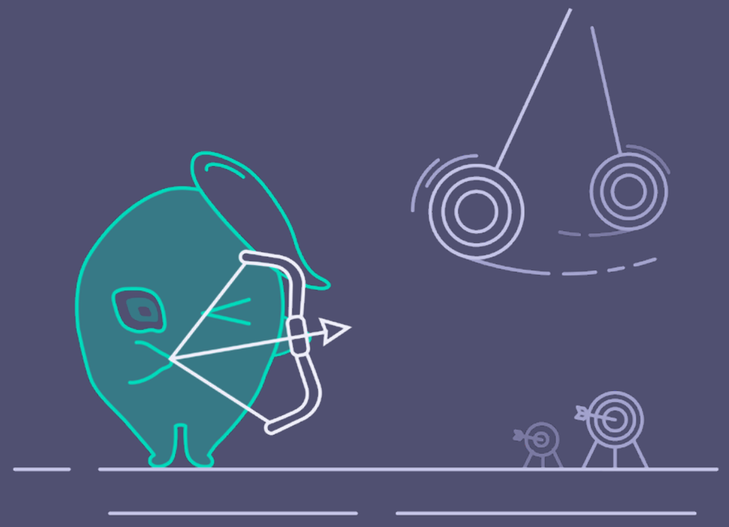
Self-reported levels of maturity

(Fig. B) The percentage of respondents who describe themselves as beginner, intermediate or advanced

A moving target

A moving target: **an idea or situation that continuously changes as you are trying to deal with it.**

So what's holding organisations back from maturing their APIs to drive more business value? We found that the pace of change in API best practice was a key challenge. When we asked our respondents how they advance and govern their APIs simultaneously, the most taxing challenges fell into four distinct categories.



01. Exposing APIs securely: authentication and authorisation

Authentication is the process of verifying who someone is and authorisation is the process of verifying what specific applications, files and data a user has access to. The two are key pillars of any API security process.

Our respondents were utilising open authorisation standards to classify the data resources sitting under their APIs and implement clear frameworks for access control. While we found that authorisation practices were well understood and routinely implemented, authentication was in more of a state of flux.

Token-based authentication was common among small to medium sized enterprises. We found organisations were actively seeking ways to enhance the security of their authentication methods. For example, by automating the expiry and re-allocation of tokens after set periods of time.

Beyond passwords

Across industries and organisational types, we identified a common desire to move away from username and password based authentication. The reasons cited included the risk of password leakage and the poor UX that comes from asking users to repeatedly enter passwords.

Zero Trust

Our respondents described authentication and authorisation best practice methods which aligned with Zero Trust methodologies including:

01. Continuous unit and integration testing and monitoring of datasets and APIs.
    To ensure that authentication and authorisation is effectively in place across all the potential doorways to data.

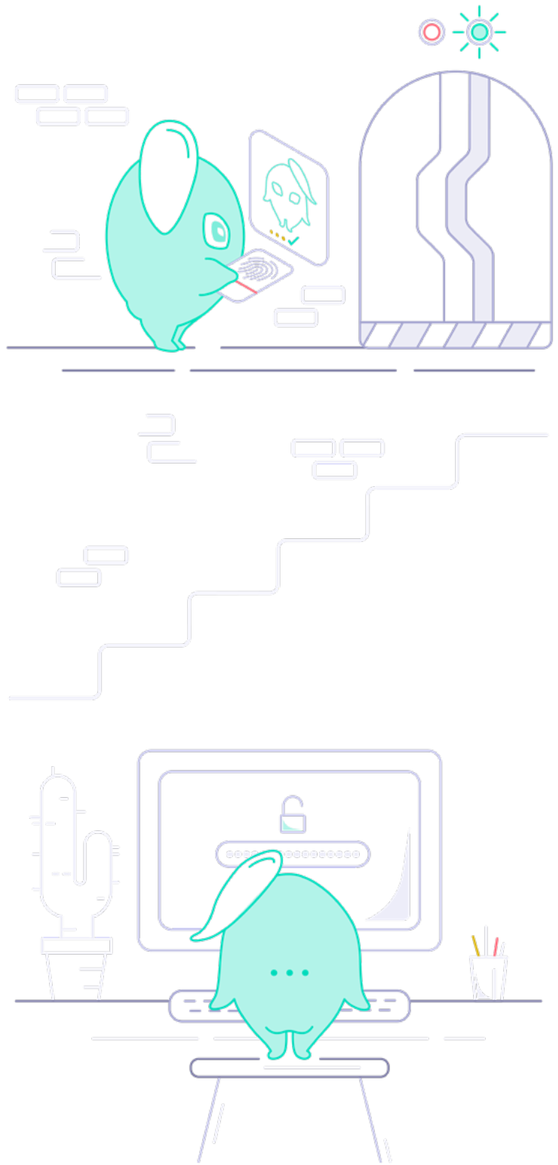
02. Applying no distinction between users inside or outside of an organisation's network.
    So that individuals and devices trying to access an API are continuously validated.

Respondents from highly regulated industries including healthcare, finance and telecommunications were the most advanced in the use of Zero Trust methodologies.

What's stopping organisations from implementing a Zero Trust security model?

On first appearance, the benefits of a Zero Trust environment are self-evident. By eliminating the concept of trust from an organisation's network architecture, organisations can implement the highest levels of access control and security.

Yet counter-intuitively, we found that some organisations reported grappling with security in their transition to Zero Trust. Building a Zero Trust network across a medium or large-scale organisation is no mean feat. It is a highly technical undertaking and requires a skilled team.



Human error

Our respondents told us that it can be all too easy for in-house teams to overlook high quality and standardised implementation of authentication and authorisation protocols in the race to market.

If authentication and authorisation is not implemented and standardised across an ever expanding and changing landscape of devices and users, a Zero Trust strategy can become undermined and ineffective.

Looking for solutions

To combat this, our respondents were increasingly looking to API management tools to oversee authentication and authorisation. This has enabled their internal teams to focus on the business logic of their APIs.

Our respondents recognised the value of having an abstracted layer on top of APIs to add an extra level of security assurance and create a separation of concerns.

> Security is a frontline focus for the whole organisation. It's not an afterthought. It's a secure by design and zero trust mechanism that we apply, so it's embedded into the way we do things.
>
> **Mars**

> Suddenly there's a lot of effort that goes into making your APIs secure. While API security is something everyone wants, if it's not easy, people tend to look for an easier path.
>
> **MIQ**

> We were using multiple ways of authenticating multiple platforms. None of it was standardised and from the perspective of our customers, it was awkward and difficult to integrate.
>
> **Pitney Bowes**

02. Managing access control and good governance

Foundational principles

When it comes to good governance, our respondents cited the need for an overarching strategy which adopts a common set of principles, patterns and frameworks.

Our respondents recommended starting with a standardised set of API specifications. From a strong base, API functionalities can be adjusted and extended to meet the specific requirements of departments or products in ways that are governable and allow for API security protocols to be uniformly implemented.

Governing microservices

Microservices architecture allows for the solution to be split into smaller pieces with dedicated purposes and this enables more personalised and agile delivery.

While microservices offer more flexibility, our respondents told us that its distributed architecture can become complex and complicated to govern.

For businesses with relatively small-scale operations, a monolithic or service-orientated architecture can still offer effective solutions.

For respondents who were pursuing a microservices architecture, we found that maintaining total visibility of their APIs was crucial to ensuring increased complexity didn't lead to increased security vulnerabilities.

> The dilation of the design principles is key. How do we govern the identity and security of these APIs?
>
> **NCS**

Foundational principles

Governing microservices

Automating out vulnerabilities

Simplifying complexity

Automating out vulnerabilities

Increasingly organisations are looking to automation to effectively govern APIs within complex microservices architectures.

We found that respondents are using automation to reduce or cut out completely the number of individuals involved in requesting and granting access to APIs.

As soon as a new API is created, an access control process is automatically applied to prevent unauthorised access, eliminating the need for this process to be repeatedly enacted manually. By reducing the number of individuals involved in the process, there is less chance of a security breach occurring.

Looking to the future, the technology leaders we spoke to are also aiming to develop automated processes that carry out testing in real-world conditions to support ambitions to create more open APIs that can be shared with customers and partners.

Foundational principles

Governing microservices

Automating out vulnerabilities

Simplifying complexity

Simplifying complexity

As organisations think about how to implement governance models that enable automation, agility and security, they are increasingly seeing the value of an API management tool. An API management platform can mediate between code base, application and identity provider to simplify the governance process and guard against single points of failure.

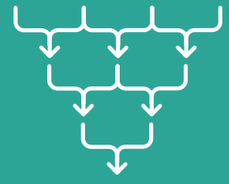
This process effectively mediates a complex ecosystem to enable a holistic and robust approach to governance.

> The big challenge that we currently have is keeping APIs flexible for a changing set of customer needs and at the same time keeping them manageable and governable. We want to have a simpler governance model.
>
> **Lloyds of London**

Foundational principles

Governing microservices

Automating out vulnerabilities



Simplifying complexity

03. Data at rest and data in transit

Our respondents told us that securing data at rest posed fewer challenges than securing data in transit.

Data at rest tended to be locked down with encryption and from there secure APIs operated on-top to pull, modify or insert data as required.

Encrypting data at rest

We found that large organisations grappled with how much data at rest to encrypt. One option is to encrypt all data at rest but for large organisations this creates a lot of overhead.

Instead of encrypting all their data, we found that our respondents tended to encrypt highly identifiable and highly sensitive data with tokenisation.

Data classification

Classifying data clearly was commonly cited by our respondents as essential. Data classification outlines how and where data at rest should be stored. This may be on-premise data centres or in a public or private cloud.

Our respondents noted how important it is to stay on top of data classification during periods of digital transformation.

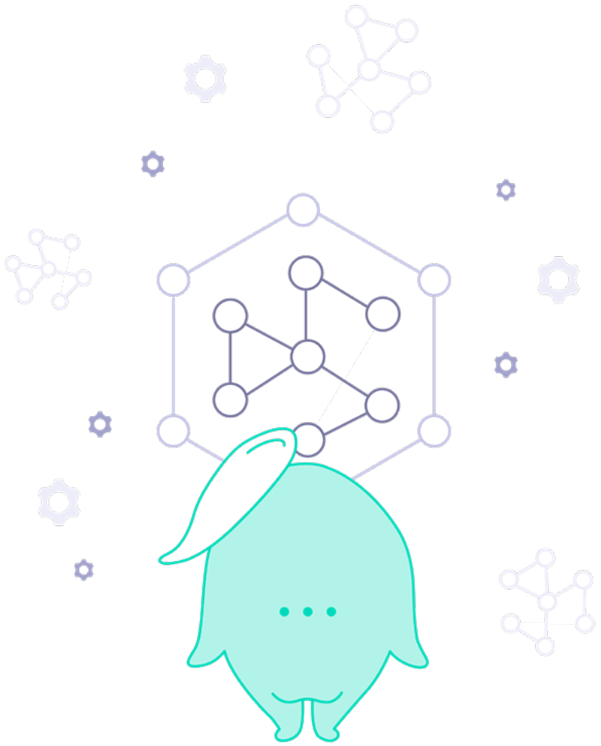
When businesses seek to develop new cutting-edge API functionalities which use data at rest in new ways, we found that this is a particularly high risk time when security errors can creep in.

To tackle this, organisations are turning to API management tools like Tyk's full lifecycle API management platform to identify and address the most serious and prevalent security and governance flaws and vulnerabilities.

Data in transit

A key facet of our respondents' digital strategies involves increasing the exposure of their APIs to the outside world. The leaders we spoke to were carefully considering how to securely manage data in transit to realise this aim.

Our respondents were routinely applying channel-level encryption with HyperText Transfer Protocol Secure (HTTPS), transport level security (TLS) and SSL Secure Sockets Layer. They were also increasingly intefed in exploring new ways to effectively encrypt data in transit.



Service mesh

Service mesh is a technology that was developed to manage communication between different parts of an application primarily in a distributed microservices architecture.

For large organisations, we identified a trend towards using service mesh to manage internal APIs, with an API management solution in place to manage external APIs.

For smaller organisations, we found that service mesh is not always feasible as it can be challenging to build and maintain.

It is a technology that comes with a set of prerequisites:

01. It needs to be embedded at both the code and infrastructure level
02. It requires microservices architecture and Kubernetes
03. As a niche technology, service mesh requires a highly skilled team
04. As a technology that is evolving quickly, a dedicated team is needed to keep pace with the evolution of the technology and its iterations.

> It's important to make sure that you're identifying your data and then encrypting the right data. Otherwise you're just creating a lot of overhead for yourself.
>
> **BT**

04. Legacy code and integration

Our respondents used and valued a variety of programming languages. We observed a move away from SOAP generally due to its traditionally inflexible functionality. But our respondents told us it did still have a role to play in highly regulated industries, such as financial services.

The migration from SOAP to REST has often been linear. REST provides more flexibility than SOAP and offers a more effective way of bringing together data from various sources to create a more unified experience across multi-channel platforms.

Whilst REST still proves fit for purpose for small and medium businesses, we found that respondents from larger enterprises, with many complex API calls and many servers, were keen to overcome the tendency for REST to over-fetch data.

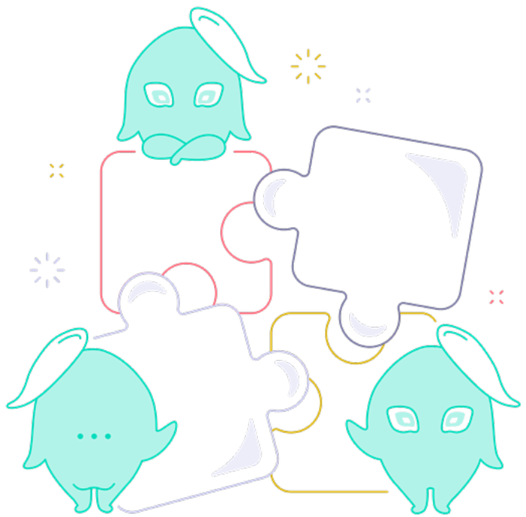
GraphQL helps to address this as it offers the ability to make precise requests to the server for no more or no less than what was needed, especially in an omni-channel setup.

Seamless integration

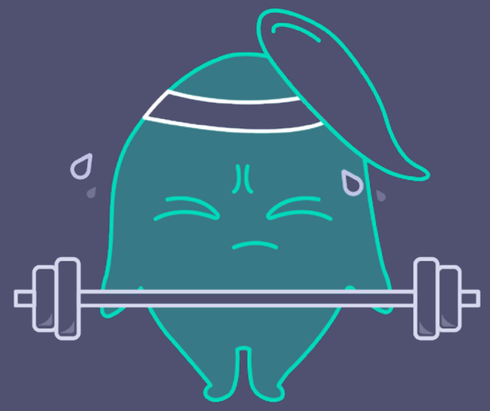
We found that what enterprises appreciate most is the ability to move seamlessly between API styles such as SOAP, REST, GraphQL as well as architectural styles, like monoliths and microservices architectures.

This reticence to migrate entirely from one architectural style to another was also because of the disruption this can cause to business as usual. Instead, our respondents are increasingly applying plug-in solutions to transform requests and responses into the desired programming languages.

Applying an API management tool that can interoperate between different generations of code is transformative. It means that organisations don't have to completely re-architect and re-work their governance and security frameworks, but instead can focus on transforming and scaling to meet demand.



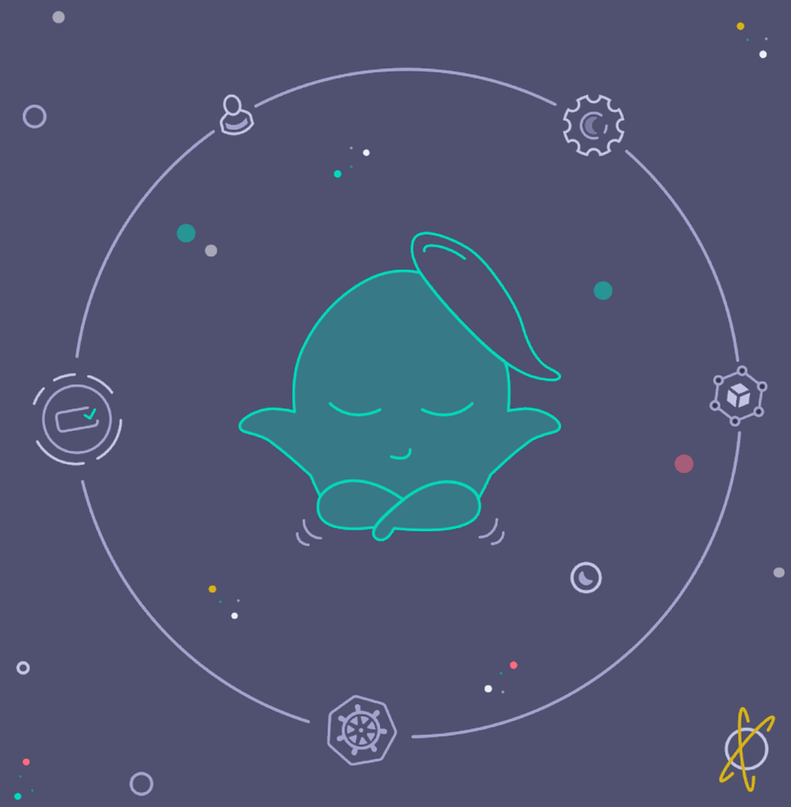
> This is game-changing because it means a digital transformation strategy can now be executed in a quarter.
>
> **Tyk**



(Fig. C) Most to least challenging areas, according to our respondents

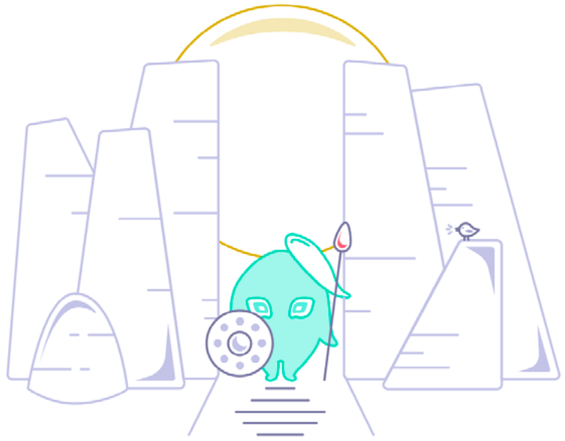
An API management state of mind

To toe the careful line between innovation and governance, businesses are rethinking their approach to API management. From our research, we identified five trends underpinning this new approach.



01. Separation of concerns

For those of our respondents who had already adopted an API management tool, the top reason cited for doing so was to abstract security and governance to a separate, dedicated layer. This separation of concerns enables developers to solely hone in on the functionality of their APIs, instead of endeavouring to roll security and governance into the main code base too.

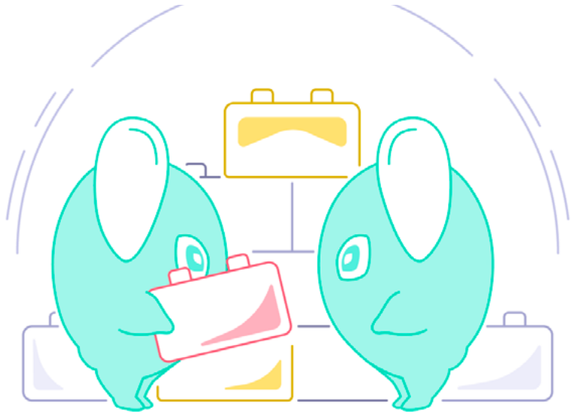


03. A pick-and-mix approach

Many organisations are moving away from large scale migration projects towards a business by business and case by case approach. Enterprises are increasingly prioritising time to market, personalisation and agility. To operate a hybrid environment that can comfortably manage a variety of languages and styles, organisations are applying API management tools to interoperate between a complex patchwork of architectures.

02. Secure by design

Applying an API management layer is inherently more secure because it eliminates a single point of failure. By operating two dedicated layers - one which looks into the business logic of the application and another which manages governability, APIs can evolve and develop from a starting point which has been designed to be secure.



04. A bird's eye view

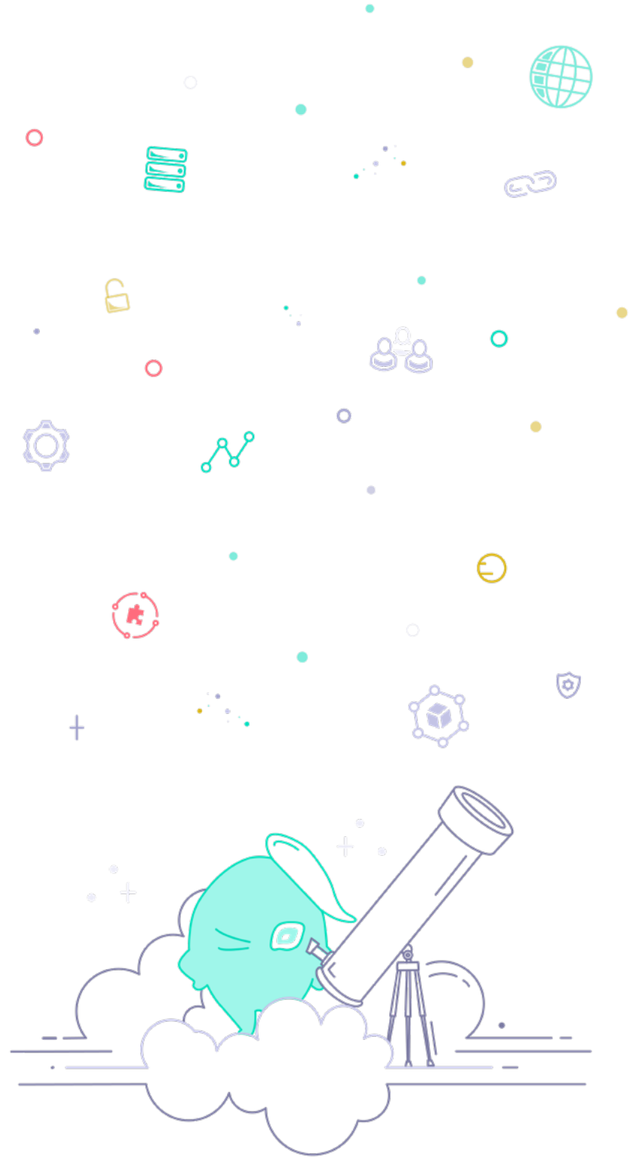
Modern enterprises have a growing array of in-house and third party software essential to the prosperity of their business. Digital vanguards are looking to centre their software around API platforms. An effective API management system mediates complicated software ecosystems to translate complexity into simplicity, allowing organisations to crystallise their digital strategy with a bird's eye view of their APIs.

05. Exceptional APIs with standardised security

DevOps has empowered teams to design and deliver more personalised and effective digital products. Yet all too often, the unintended consequence can be siloed software.

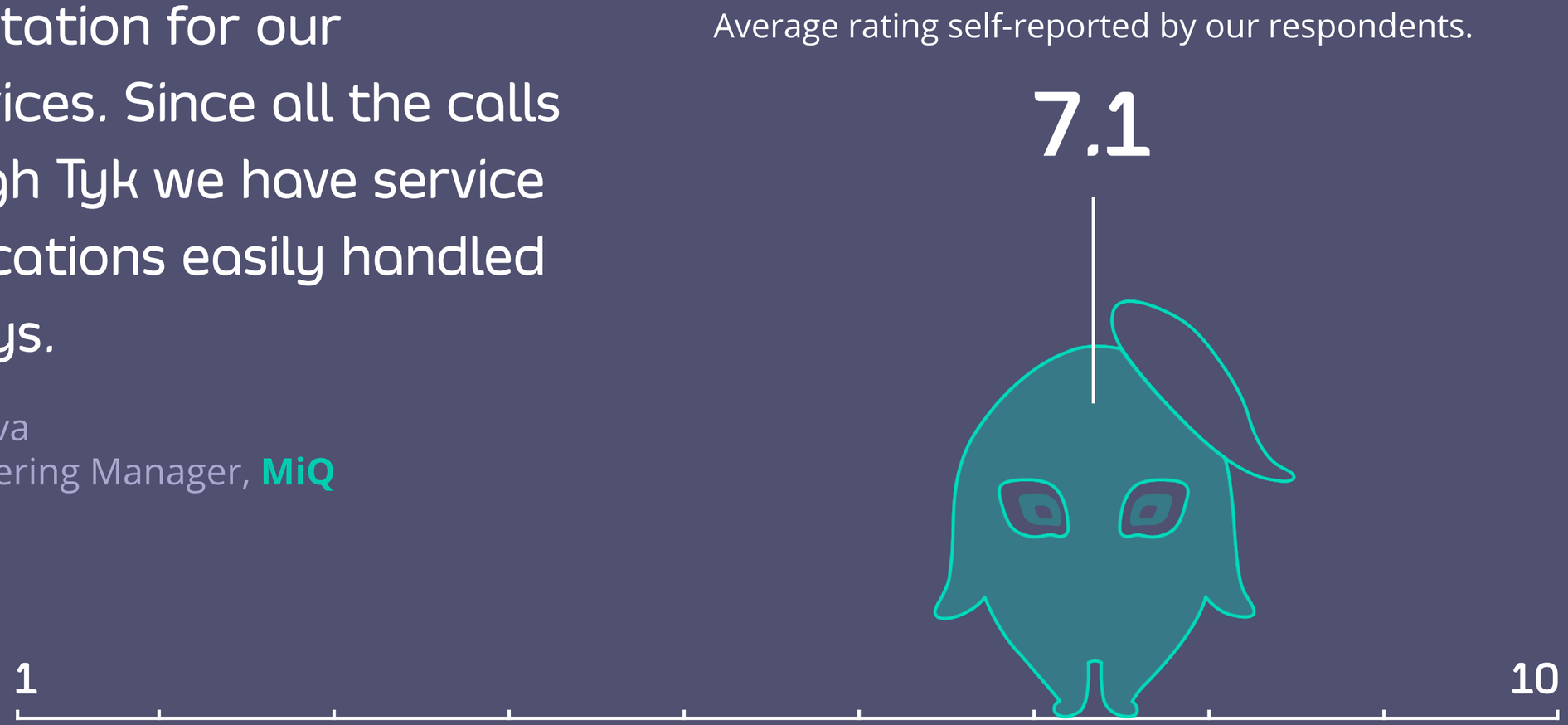
With the dawn of superapps and the drive to aggregate data from many different parts of an enterprise, trying to harmonise data from a variety of complex and modern APIs can bring a halt to operations.

Forward-thinking businesses are applying a layer of API management on top. So regardless of how a business organises its teams, which programming language it uses or the frameworks they have in place, it has a standardised approach to API security management.



> One major advantage was to streamline the security implementation for our microservices. Since all the calls go through Tyk we have service communications easily handled by API keys.

Rohit Srivastava
Senior Engineering Manager, **MiQ**



(Fig. D) On a scale of 1 to 10, to what extent would you describe your API security features as fit for the future?

> Our core purpose is to solve our customers' payments problems. It makes sense to work with a partner, someone who could help us with the routing and the security management.
>
> Ritesh Tendulkar, Chief Technology Officer, **Modulr**

> Tyk has provided Einhell Germany AG with peace of mind as a result of the enhanced security of its APIs, as well as superb management oversight through greater control and monitoring abilities.
>
> Christoph Kufner, Senior IT Architect at **Einhell Germany AG**

> We were working on a data exchange strategy to optimise the way applications could talk to each other. We needed to broaden, facilitate and track the IS data consumption. We had several APIs but each had its own governance. We wanted to normalise governance and ease API visibility and security management as well as centralise the operational metrics. The need for an API gateway was evident.
>
> Olivier Vermont, Project Management Deputy Director, **VINCI Construction**

Conclusion

The global pandemic has amplified the drive towards full digital transformation and enablement. Enterprises across a wide range of industries believe APIs have the potential to drive this transformation. But businesses are held back by the complexity of their API architectures.

Large organisations are grappling with how to harmonise advanced APIs with years of legacy code that sits in silos across their business. Start-ups and scale-ups are debating how best to choose between niche and complex architectural styles to best serve their business and their customers.

When it comes to choosing an API style, we found that no one rule fits all. Each enterprise must choose the programming language and architectural style that aligns most with their unique vision and mission.

What organisations must streamline is their approach to API security and governance. Digitally forward-thinking businesses are extracting their API security and governance by adding a dedicated API gateway to their technology stack. With a dedicated API gateway that covers both functionality and security - expert teams can focus on mastering the uniqueness of their APIs to drive future growth.

Tyk is the fastest-growing and the most exciting API gateway and management platform on the market, comprising an open source gateway, coupled with a proprietary management dashboard. We power millions of transactions per day, for thousands of innovative organisations including AXA, Cisco, and the Financial Times.

API analytics, out-of-the-box developer portal and multi-cloud capability are some of the most popular features of the Tyk management platform, but only just touches the surface of what this powerful product can do. Fast, flexible, and highly-performant, Tyk is available to install on-premise, as a cloud service, or hybrid.

Get started with Tyk at tyk.io/get-started-with-tyk or contact us for more information at tyk.io/contact/

Nimbus Ninety

Nimbus Ninety is a vibrant and diverse community of forward-thinking business and technology leaders. Since 2005, we've been connecting innovators, change-makers and disruptors from all sectors to enable them to share their experiences of disruption and move forward together.

Our community is made up of senior stakeholders from global blue-chip organisations, SMEs and the public sector, who are responsible for driving digital innovation across their businesses and industries. At the heart of what we do is a passion for driving value creation across the community.

We foster engagement and collaboration between our members, our solution providers and our partners through our highly engaging activities, in-depth research and thought-provoking content. For more information, visit www.nimbusninety.com or follow us @NimbusNinety.

Tyk

Singapore

High Street Centre
1 North Bridge Road
#08-08
Singapore 179094
info@tyk.io
+65 681 32083

London

87a Worship Street
London
EC2A 2BE
UK
info@tyk.io
+44 20 3409 1911

Atlanta

22 Technology Parkway
South Peachtree Corners
GA 30092
USA
info@tyk.io
+1 (404) 4511123