



THE ENTERPRISE ARCHITECT'S GUIDE TO

UNIVERSAL API GOVERNANCE

Building clarity into complex systems



Executive summary

Governance isn't about bureaucracy. It's about instilling confidence in your teams and gaining competitive advantage through a structured, strategic approach. Done well, it can help define your values as a business, and how those values will impact the customers you serve.

From the trenches of enterprise architecture to the cutting edge of AI governance, this book explores how structured API governance can drive innovation, security and scalability.

The stakes have never been higher...

By 2026, **more than 80% of enterprises will have used generative AI APIs or models**, or deployed GenAI-enabled applications in production environments, up from less than 5% in 2023 ([Gartner](#))

More than 30% of the increase in demand for APIs will come from AI and tools using large language models (LLMs) by 2026 ([Gartner](#))

"The **strategic importance of API governance** cannot be underestimated" - [Forbes](#)

...nor have the risks

37% of organizations experienced an API security incident in the past year, up from 17% in 2023 ([Salt](#))

84% of security professionals reported API security incidents in 2024, marking an all-time high ([Akamai](#))

Universal API governance is now non-negotiable. Packed with real-world case studies, strategic frameworks and resources to support the rethinking of how enterprises manage APIs, this book is a must-read for technology leaders, platform engineers and enterprise architects.

It gives you the blueprint to scale APIs safely and strategically across teams, protocols and platforms, using governance to power innovation.



Contents

- 01 API governance in 2025:** The good, the bad and the dangerous 3
- 02 Universal API governance:** The playbook for managing the API chaos 5
- 03 Automating API governance:** The path to scaling API operations and policies 9
- 04 AI, compliance and trust:** The new governance battleground 14
- 05 Federated API management:** Balancing governance, growth and agility 19
- 06 The modern enterprise API portfolio:** Unifying diverse API protocols and types 22
- 07 Security is not optional:** The API attack surface 26
- 08 API observability:** The missing link in your governance strategy 29
- 09 The road ahead:** API governance as a competitive differentiator 32
- 10 Conclusion** 35
- 11 Acknowledgements** 36



API governance in 2025

The good, the bad and the dangerous

Without governance, APIs become liabilities, and at enterprise scale, the risks grow hand-in-hand with the sprawl. Shadow APIs, security gaps, multi-cloud sprawl, discoverability issues, integration complexity... it's all lurking there ready to come crashing down.

But we can hardly blame enterprises for struggling to keep up. In 25 years of HTTP APIs, we've gone from SOAP to REST to GraphQL and now to event-driven, with AI layering over the top to add to the complexity.

The average enterprise **managed 613 API endpoints last year**. ([Thales](#))

As the use of APIs has boomed, so has the importance of API governance – but not for the reasons you might think. API governance isn't about rigid control and locking everything down. That's an outdated notion. Yes, five years ago the focus was just on the general control and standardization of APIs from a security and compliance perspective. Now, though, governance has much more of a strategic enablement and innovation angle (as well as all the security and compliance benefits).

It means that, implemented well, API governance:



Promotes
creativity
and innovation



Delivers
business ability



Enhances API
reusability



Reduces total
cost of
ownership



Helps measure
return on
investment
(ROI)



Reduces
security risks



Supports a
seamless
compliance
journey

●

2019

"The process of **establishing and enforcing rules and standards for creating and managing APIs**. The focus was on ensuring security, consistency, and compliance across all APIs within an organization to prevent issues like data breaches and inefficient operations."

●

2025

"A comprehensive framework that not only ensures security and compliance but also **drives innovation and strategic alignment**. It involves setting guidelines and using tools to optimize API design, development, and usage, **fostering collaboration and efficiency across teams**, and leveraging analytics for continuous improvement."

▶ Watch the video

Adapted from LEAP 2.0 opening keynote, "Welcome to LEAP" presented by Sophie Laundon (Tyk)

API traffic constituted **over 71% of web traffic** in 2024. (Thales)

It's important to understand the danger of not implementing API governance well (or at all). A lack of governance opens you up to security risks, lost time, wasted resources, poor cross-team interaction and a lack of reusable API products. Hardly a strong foundation for an innovative enterprise looking to beat the competition to market.

Overly rigid rules also don't work. Teams will find loopholes and workarounds, with your governance becoming little more than shelfware while you still face greater risks and inefficiencies than you should. It's crucial to remember that your people are at the center of your governance process. As you embrace technical solutions to overcome governance issues and risks, you'll need to engage your teams with your new structures, frameworks and processes.

“

There's a lot of desire to automate. Once we have a rule, we're like, yes, we have the rule! Let's automate it and put it in place! That rule is nothing without human coordination, human awareness and human understanding.

Kin Lane

From LEAP 2.0 opening keynote, "After 25 Years of HTTP APIs do you have API governance in place?" presented by Kin Lane (API Evangelist)

”

▶ Watch the video

Given the prevalence of APIs, and the fact that AI and emerging technologies are now serving as disruptors reshaping API ecosystems, getting API governance right has never been more crucial.

“

Data shows that there are around **200 million active APIs right now** – and that we are on the path to there being approaching **1.7 billion active APIs by 2030**.

Sophie Laundon, Tyk

From LEAP 2.0 opening keynote, "Welcome to LEAP" presented by Sophie Laundon (Tyk)

”

▶ Watch the video



Universal API governance

The playbook for managing the API chaos

THE CHALLENGE

Shifting the definition of governance from a technical complexity to a business opportunity.

THE SOLUTION

Understanding that governance is about enabling people, not enforcing rigid controls.

Universal API governance isn't about bureaucracy; it's about providing structure around your standards, security and compliance expectations, while delivering essential visibility. It cuts across sectors and industries to deliver powerful results at enterprise scale – provided you follow four key principles. Effective API governance is:



**Easily
understandable**



Easy to follow




**Easily
measurable**



Easy to report

Designing your API governance model in line with these principles means you can keep governance nimble while ensuring it scales across the enterprise. You can move fast and beat your competitors to grab market share, agilely designing and building APIs with security and compliance baked in.


How do you design a governance model that scales? One crucial element is understanding that governance evolves and iterates, just like any other area of your business. So implementing governance isn't just a case of setting standards and walking away. You'll need regular reviews with a wide range of stakeholders – architects, developers, testers and more. These are the people who can tell you if your governance guardrails are clear, relevant and valuable. Skip the consultation and you're back to teams looking for loopholes and workarounds. But engage, train and consult on your governance processes and they'll remain effective as you scale. Successful governance is about people, as well as processes.



Find a common element for what your API governance is delivering. Why are you doing API governance? What is it for? Once people understand, they can actually want to follow it instead of you having to make them.


Bruno Pedro, Author

From LEAP 2.0 panel discussion, "Is the best API governance strategy a boring one?" featuring Bruno Pedro (Author), Bill Doerrfeld (Nordic APIs), Sreekanth Cherukuri (Coforge) and James Hirst (Tyk)




[Watch the video](#)

Designing an API governance model that scales is about creating systems that empower people to collaborate, innovate and stay aligned. Enterprise API governance means achieving that across multiple APIs, protocols, clouds, teams, platforms, geographies and more. Incorporating multiple stakeholders' concerns is key.




**API builders
(developers)**

care about having the autonomy to build creatively, minimizing friction and optimizing locally for efficiency.



**Enforcers
(platform leaders)**

prioritize the big picture, reducing risk with guardrails and visibility while optimizing globally for consistency and safety.



**Strategists
(non-tech leaders)**

care about risk reduction, regulatory alignment and overall ROI – about protecting the business.

Governance is also, obviously, about processes. It needs to be embedded into your API lifecycle, balance autonomy and centralized visibility, and deliver instant insights for compliance reporting and regulatory alignment.

The right tools are important here. For developers and engineers, these encompass API assets (templates, partials, overlays and the like), enforceable middleware, linting tools, integrated and automated testing tools, developer portals and more.

Also key are the right KPIs and dashboards, which can underpin everything from real-time compliance reporting to ROI measurement.

Helpful KPIs support you to measure three main areas:



Productivity drivers

are KPIs such as shorter deployment times and shorter release cycles for faster time to market.



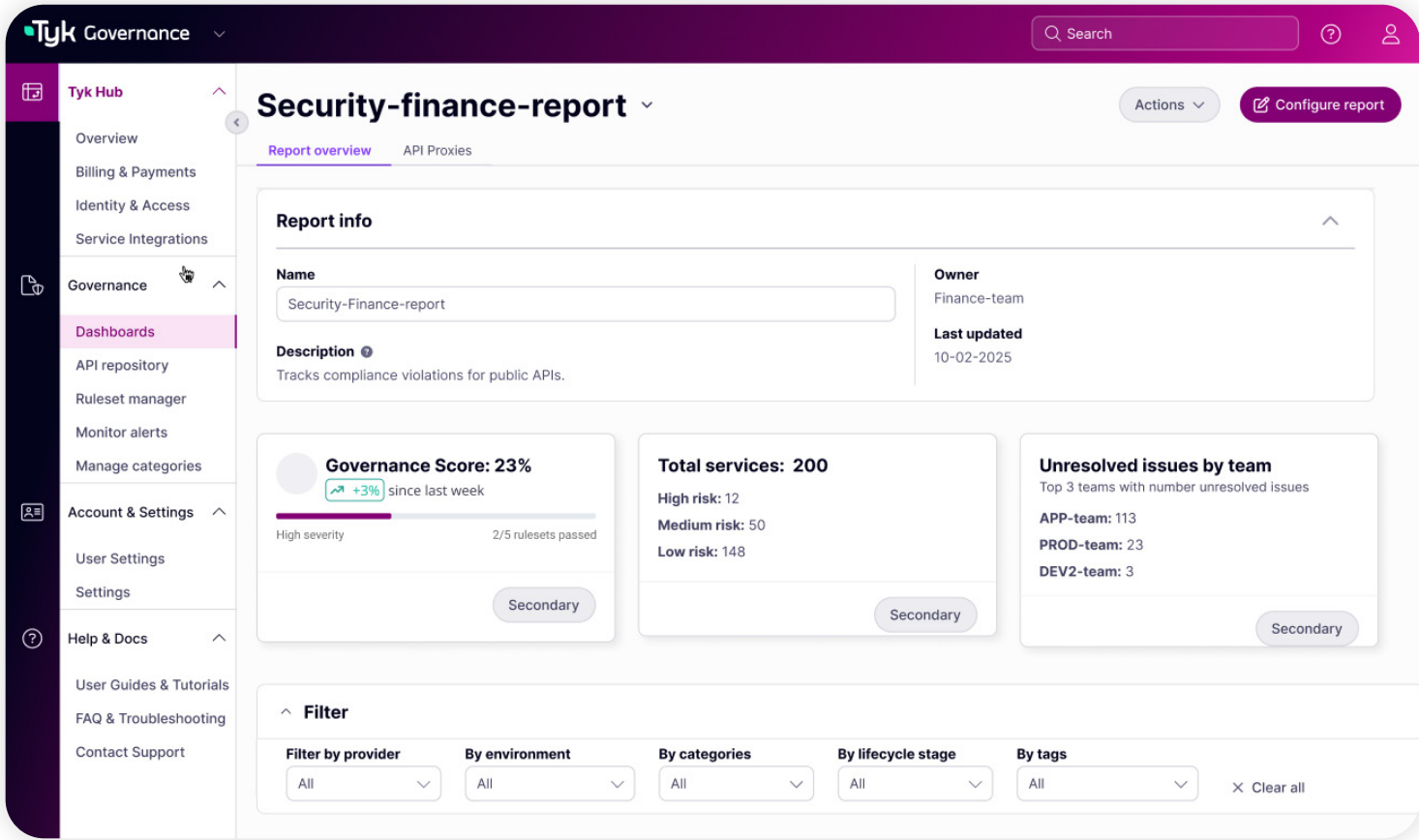
Security and reliability KPIs

measure factors such as API uptime, mean time to resolution (MTTR) and security incident rate (per API), which measure the effectiveness of your governance in mitigating security risks.



Cost savings

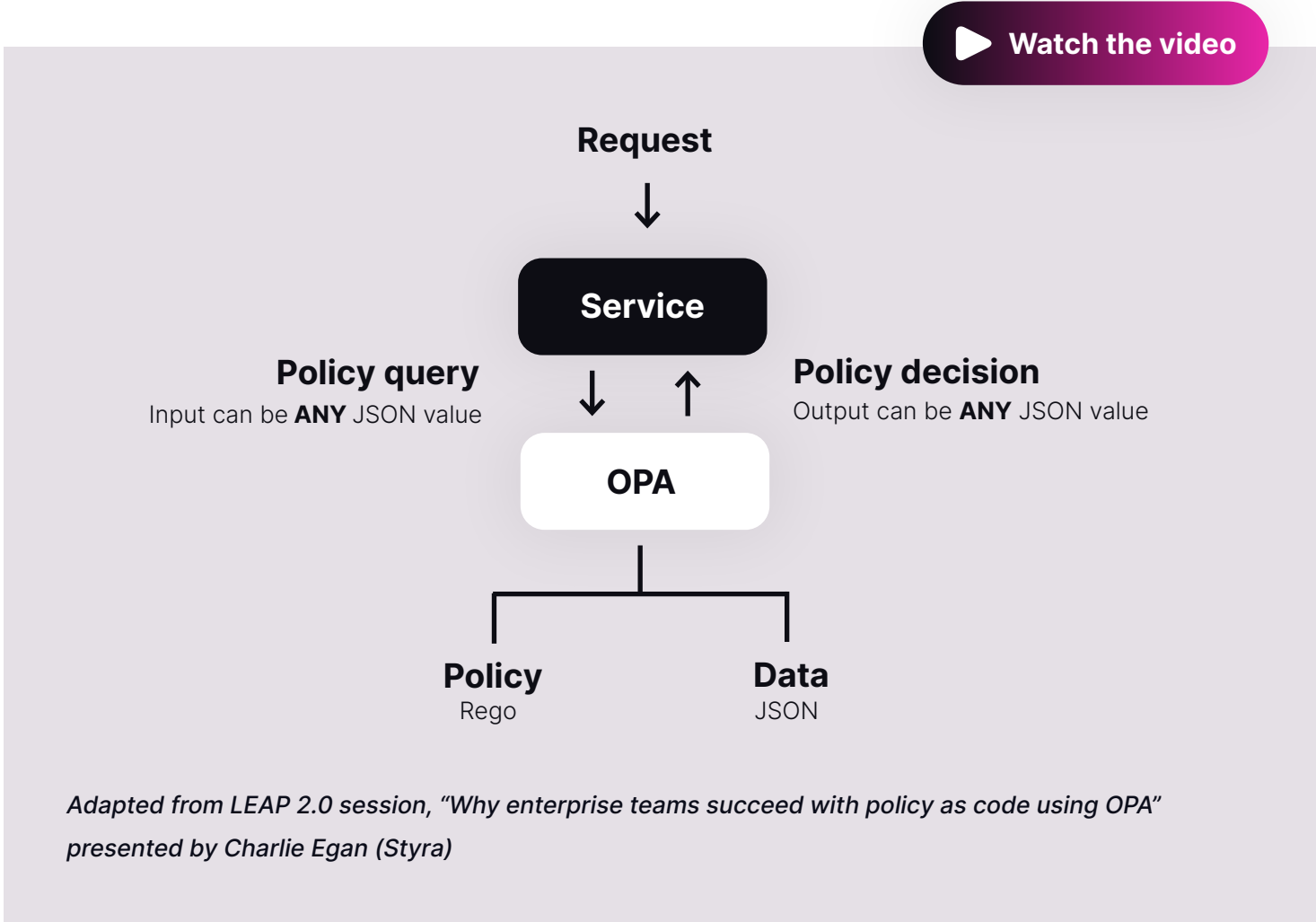
can be measured by the reduction of time spent on maintaining proprietary, non-standard tools and the cost of multiple tools.



Each of these provides a useful indicator of how your governance is supporting your business success. Remember to review your KPIs regularly with this in mind - and move away from any that aren't helping. Measuring things just for the sake of measuring them, when the information doesn't help you in any way, is a waste of effort.

Atlassian, for example, uses **broken client integrations as a governance metric**. This helps measure the overall impact of its investment in API governance.

Policies are also fundamental to governance success. At enterprise scale, embracing Open Policy Agent (OPA) is an excellent way to codify standards and business requirements while supporting developer autonomy. The versioned configurations, policy abstraction, centralized policy management and superior collaboration and testing that OPA enables puts enterprises in a powerful position to govern their disparate teams and systems. It also supports them to comply with strict auditing requirements while optimizing security and performance.



Implementing effective API governance can do much to boost creativity. When you have the right governance tools and processes in place, your developers can build without fear of breaking things. They can experiment and innovate at pace, with your governance model automating or removing tasks that previously slowed them down and added to their cognitive load.

A solid, reliable governance strategy sets clear expectations that you can check API products against (ideally automatically), supporting this creativity to flourish. All while reducing risk, providing greater auditing clarity and boosting reusability to deliver enhanced value.





Automating API governance

The path to scaling API operations and policies

THE CHALLENGE

Governing APIs in a way that ensures their future relevance and reusability while promoting innovation.

THE SOLUTION

Automating governance so developers can innovate and experiment without fear of breaking the business.

Automating API governance empowers you to deliver the guardrails and standardization your business needs, while providing the autonomy developers require to innovate and iterate. Done well (read: when business-led), automation abstracts away practical distractions that stifle developer creativity. Instead of worrying about how to handle rate limiting or which authorization mechanism to implement, all with a background fear of breaking things, developers are free to innovate at pace. By automating API governance, you're controlling what you need to, while gifting your developers the confidence they need to flourish.

The following case studies demonstrate what this looks like in practice at enterprise scale.

- 01** Showcasing business-led governance automation at **Northwestern Mutual**
- 02** Applying GitOps automation to API governance at **Zeiss**

Showcasing business-led governance automation at Northwestern Mutual

Life insurance and financial services company Northwestern Mutual has a mature, effective API governance model that streamlines developer experiences and delivers a whole heap of benefits.




With a 160-year history, Northwestern Mutual had plenty of legacy code and disparate systems. The forward-facing firm needed a way to govern its APIs to ensure they embraced standards and security metrics, while also remaining relevant and reusable years into the future. It needed to address API sprawl, enhance compliance and consistency, and level up the developer experience.

The solution? A full-on automated API governance model featuring:

- Automatic registration of every API within the business within an API registry
- Discovery endorsements to ensure people can find APIs, understand their value and reuse them, resulting in an 80% adoption rate within the business
- Automated insights and trend analysis for outstanding visibility
- Automated API retirement, with workflows in place for moving customers along to better solutions
- Fail fast processes with immediate feedback, enabling engineers to take corrective action

▶ Watch the video

Challenges and outcomes

 API sprawl	Automated up to date API registry with APIs endorsed for discovery and reuse	Automated insights and trend analysis	Automated retirement workflows
 Compliance & consistency	Governance by default	0% high security vulnerabilities	Embedded business relevance
 Developer experience	40 hours time saving per API for first time non prod deploys	Fail fast processes to avoid wasted time	80% adoption rate

Adapted from LEAP 2.0 session, “How Northwestern Mutual streamlined its developer experience through an automated governance model” presented by Justin Russo (Northwestern Mutual)

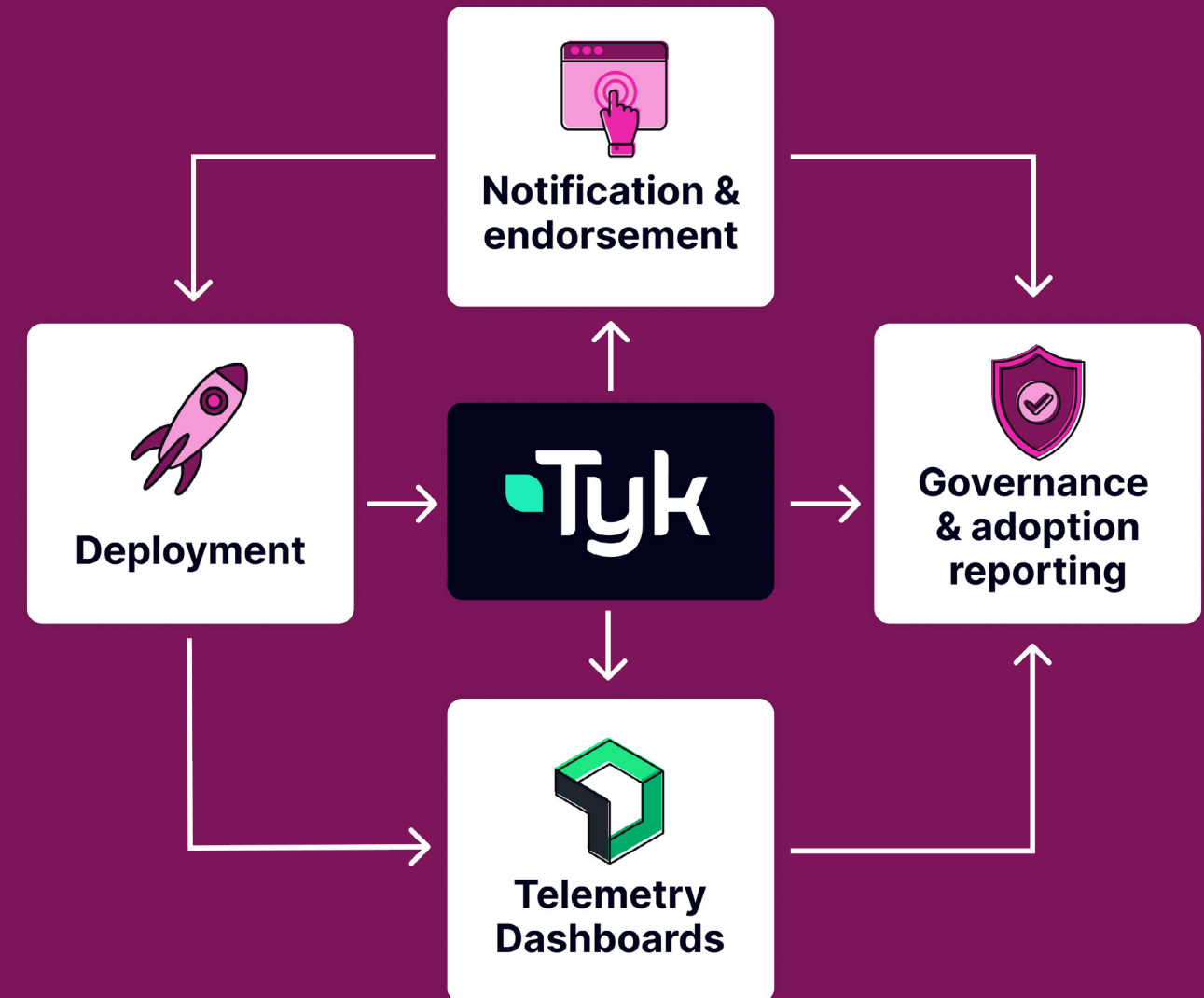
At the core of this is the concept of governance by default, with zero high security vulnerabilities and a sound business purpose for every API.

Northwestern Mutual's automated API governance model **saves engineers 40 hours per application they set up.**

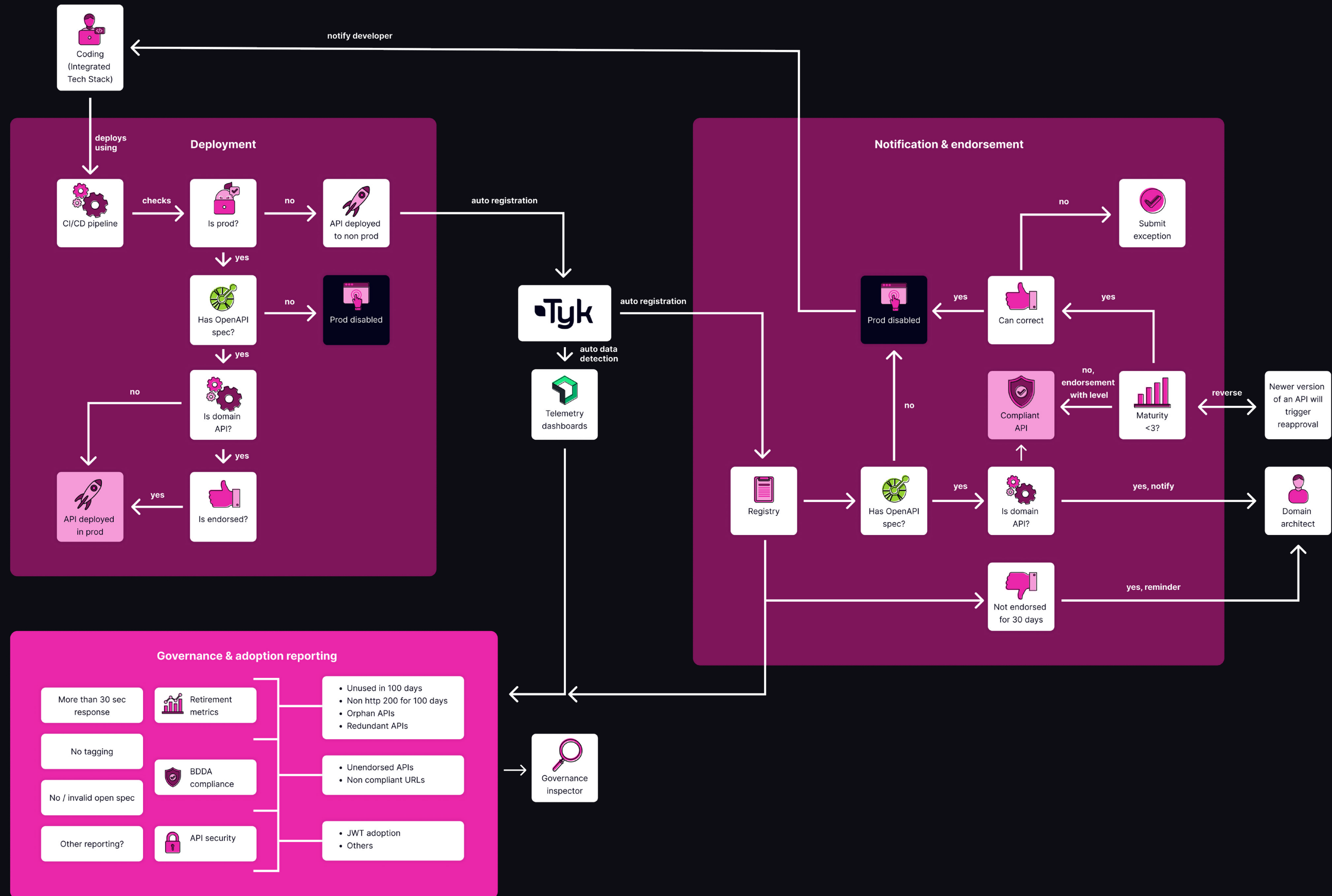
The Northwestern Mutual API governance model covers the entire API lifecycle. Automation centers on three core areas: creating and deploying APIs, notification and endorsements of APIs, and API reporting. The model fosters a culture of collaboration, with all stakeholders regularly reviewing what great looks like from their perspective. It means teams can stand up APIs quickly, confident that they align with business needs and standards. At the heart of the model sits Tyk's universal, centralized API gateway, covering off all documentation and governance needs, enforcing policies and security, exporting metrics and more.

The result? Developers can create faster, compliant APIs with visibility into their usage. Consumers can find compliant APIs, integrate with them and reuse them. API management teams can maintain complete lifecycles in an automated, secure way. Visibility of adoption, standards enforcement, trends, exceptions, usage patterns and more is outstanding.

[Watch the video](#)



Adapted from LEAP 2.0 session, "How Northwestern Mutual streamlined its developer experience through an automated governance model" presented by Justin Russo (Northwestern Mutual)



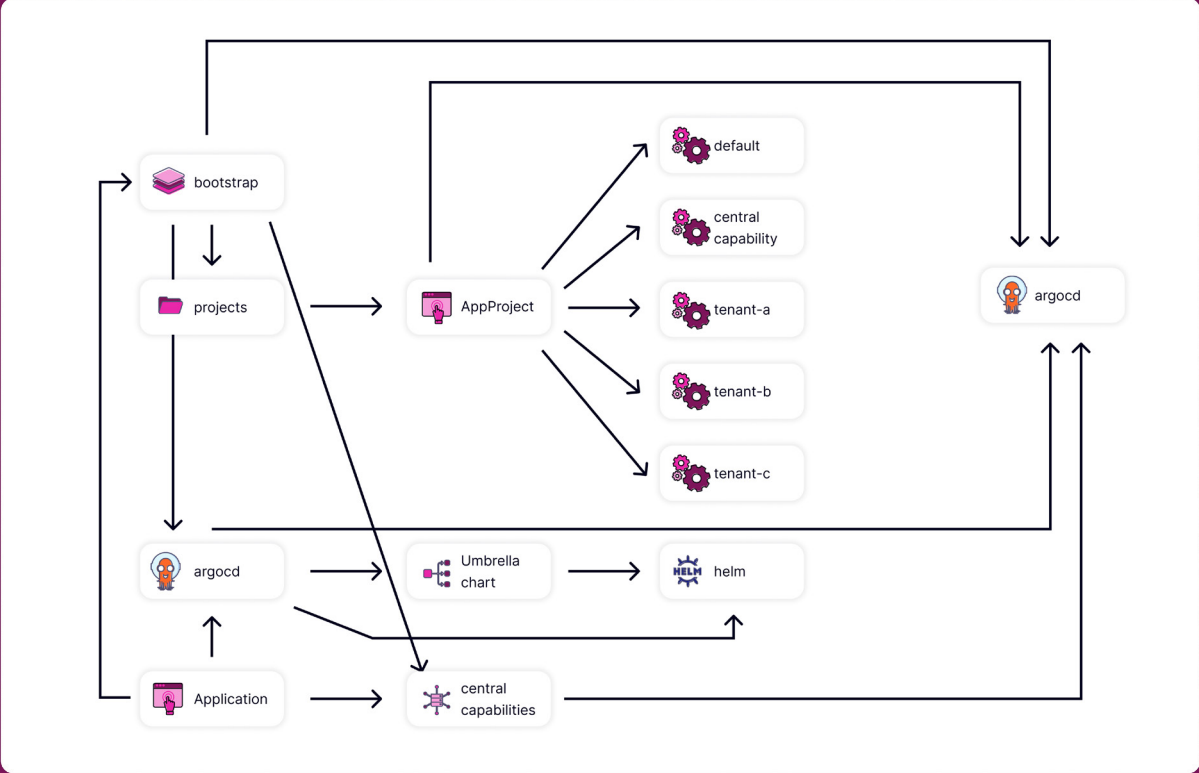
Applying GitOps automation to API governance at Zeiss

Global technology business Zeiss has taken GitOps beyond its infrastructure and applied it to API governance. The business has implemented centralized authentication, authorization, logging and tracing, so that its developers can, well, develop. They can focus on feature development, quickly spinning up new digital offerings aligned to business values, goals and standards.

With a focus on leveraging event-driven microservices running on Kubernetes, Zeiss has embraced the power of Argo CD and Tyk Operator to implement a multi-tenancy governance strategy. It is applying GitOps patterns and practical insights, for automated API provisioning and governance in a cloud-native environment.

Zeiss has implemented automation throughout its model, starting with an Argo CD application called Bootstrap, which can apply a bootstrapping of itself. The bootstrapper pulls in projects and creates app projects, with restrictions for specific tenants. Zeiss uses it to apply security options, such as access restrictions based on specific teams, tenants and namespaces. The Zeiss platform engineering team is one of those tenants, albeit a very large one, meaning it uses the same principles and approaches as all other tenants.

▶ Watch the video



Adapted from LEAP 2.0 session, “Scaling APIM with gitOps: Multi-tenancy, Argo CD and Tyk Operator in action” presented by Alexander Troppmann (Zeiss)

All of this is part of a CI/CD pipeline, with the pipeline just run once at the beginning of setting up a new cluster.

Zeiss adds Helm charts and deploys an isolated custom resource definition (CRD) for Argo CD (this makes it easier to redeploy Argo CD later on). All central capabilities on the Kubernetes cluster, including the Tyk data plane, are installed in this way. Entering the credential needed to access the first bootstrap GitOps repository, along with a tag on Argo CD, takes care of creating the initial namespace for Argo CD.

Between the bootstrapping process and the Helm charts, Zeiss applies GitOps patterns that serve its business needs. The application pointer pattern is one such example, supporting a linking strategy to pull in another GitOps repository for central capabilities and another for projects, including defining security constraints for the application.

Adding new tenants then becomes little more than creating projects for each tenant, along with providing namespaces and GitOps repository locations.

The bootstrapper's final step enables Zeiss to deploy everything to the cluster, showcasing the efficiency and value of such automation.

The platform engineering tenant repository enables Zeiss to use GitOps to deploy Tyk Operator and other Tyk components, including different Tyk versions running on different clusters (making it easy to test new versions and iterate). With Tyk Dashboard in the mix, Zeiss has detailed analytics at its fingertips, as well as the ability to easily deploy and govern its APIs at any scale. This governance foundation means the business is ideally placed to serve the digital touchpoints of tomorrow - even when we don't know today what those touchpoints will be.



“

We moved from a customized solution to a standardized solution. This helps our developers' workload, and what we see in terms of benefit is that Tyk enables us to focus on business features, and not so much on infrastructure complexity or customized solutions with a huge maintenance burden.

Bastian Heilemann, Zeiss

”



AI, compliance and trust

The new governance battleground

THE CHALLENGE

Governing AI in a way that reduces risk, instead of accelerating it.

THE SOLUTION

Effective API governance. Govern the APIs that are feeding your AI well and you can reap business-wide rewards.

AI is transforming APIs, meaning AI governance has quickly become the new enterprise battleground. Every board is asking how its business can control AI risks. But the real issue isn't AI – it's the APIs feeding it.

AI governance starts at the API layer. So, if AI is to deliver true value, API governance must keep pace. As AI models consume data via APIs, poor API governance can lead to the LLM consuming bad data. "Trash in = trash out" quickly becomes a reality, with unverified, biased and insecure inputs corrupting AI outputs.

Lack of API governance also becomes a compliance nightmare. After all, if you lack insight into what data your AI is using, so will your regulators. Compliance rules – whether for GDPR, the AI Act, Securities and Exchange Commission requirements or anything else – start at the API layer.

Traditional API governance (static policies, traffic monitoring) is a good starting point but needs to go further. AI isn't static. As it ingests, learns and changes, API governance must adapt and keep pace. API governance without this AI-awareness is outdated.

API governance in a world where enterprises aspire to be AI ready requires three key elements:



Dynamic, real-time governance with API policies that are easy to adapt and iterate as the AI evolves.



Anomaly detection at the API level that can flag unexpected API behaviors and take appropriate measures before AI makes decisions fed by bad data.



API-driven data governance, with tight data controls that extend beyond just API security.

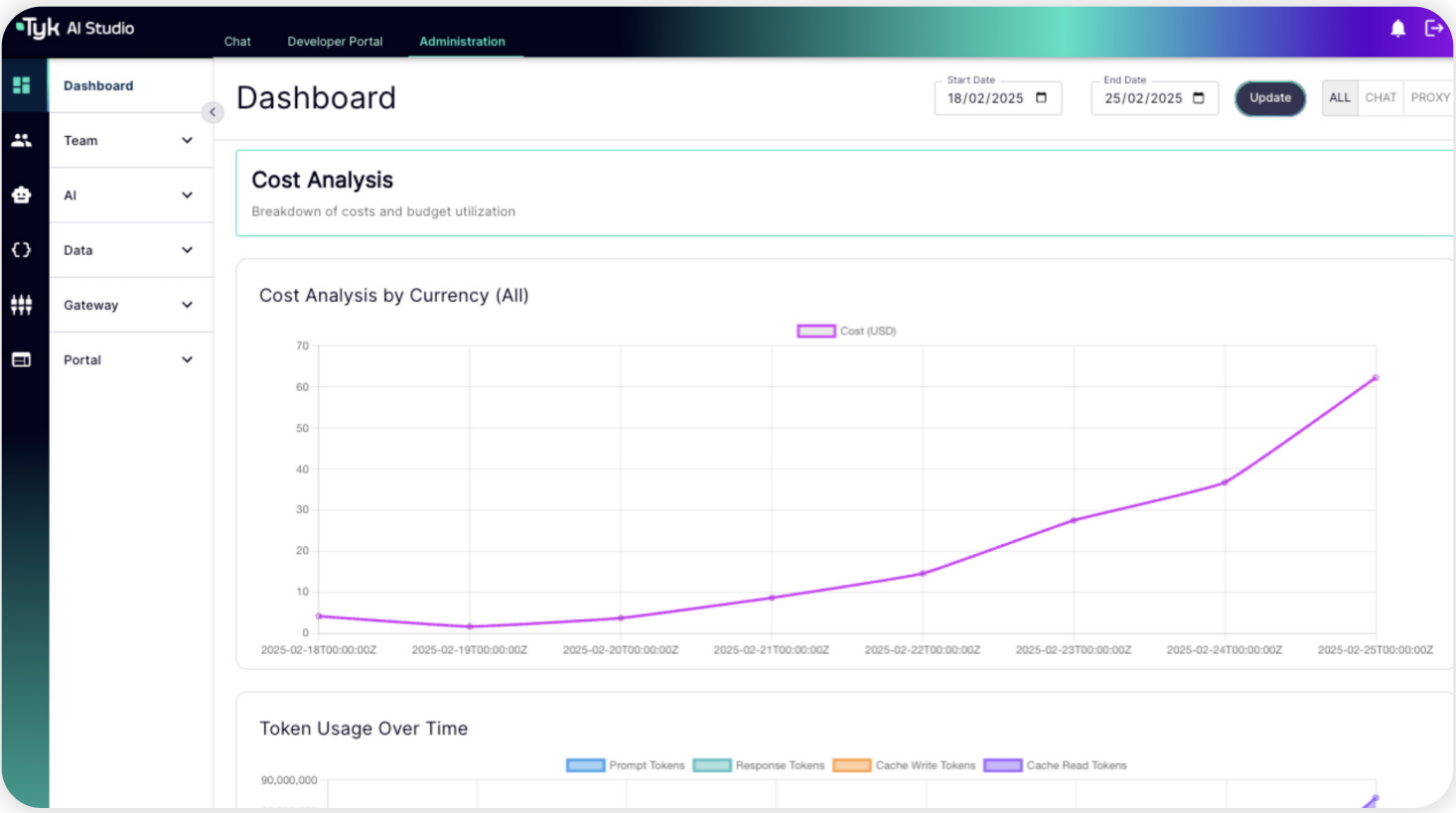
Not implementing this kind of API governance is reckless. It increases risks across the business, from security and compliance concerns to elevated costs, wasted resources and reputational damage resulting in customer churn.

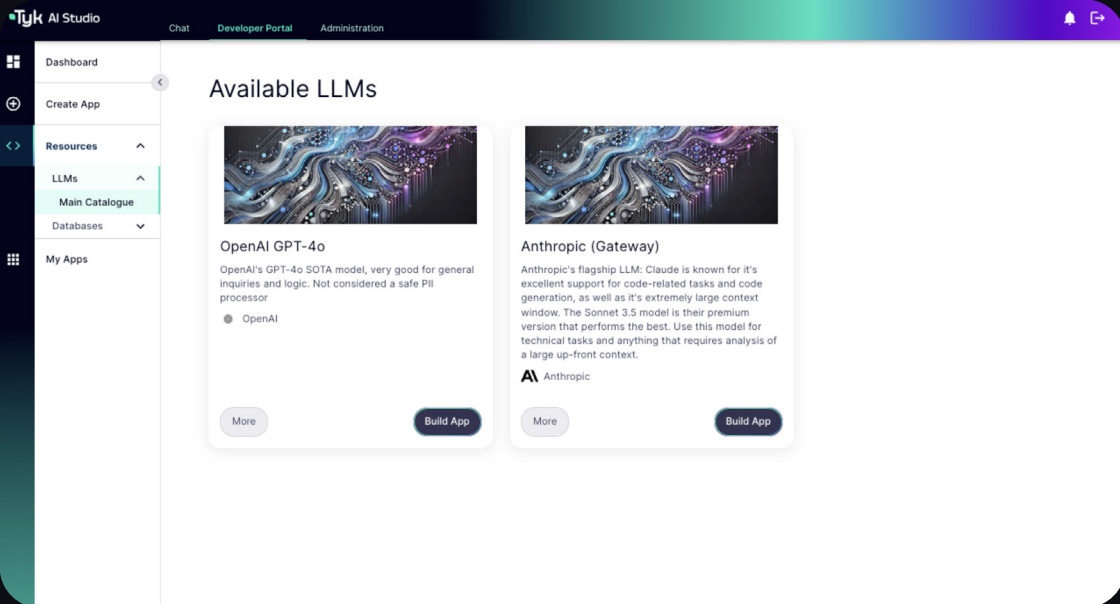
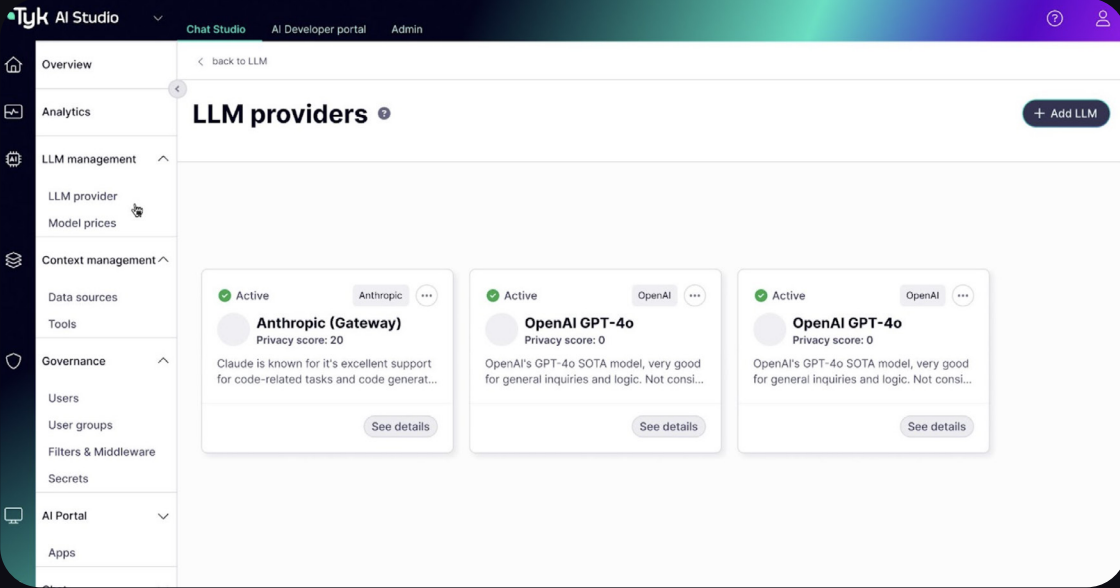
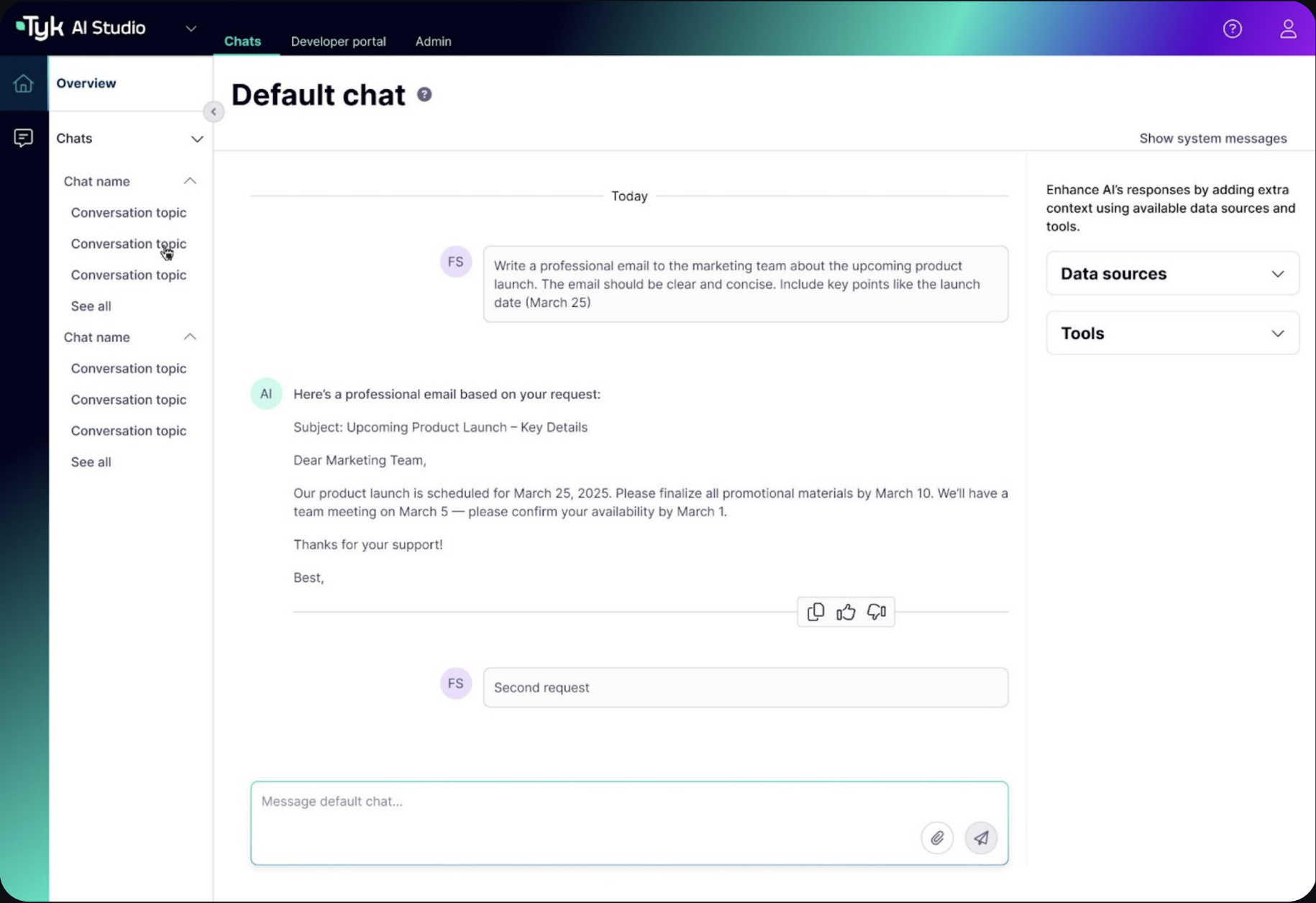
74% of companies struggle to achieve and scale value when adopting AI. (BCG)

Yet the steps to making the most of the AI revolution aren’t difficult to implement. First, you need to get your house in order in terms of API governance. Doing so addresses the risk of AI models consuming poorly governed APIs. You’re cutting out the “trash in” element, to reduce the risk of “trash out.”

The next step is to ensure you have full visibility of your AI, growing your confidence in its accuracy and efficacy. A product such as Tyk AI Studio delivers precisely this, enabling you to accelerate AI innovation with confidence, without sacrificing control. It empowers you to govern AI with role-based access control, rate limiting and audit logging while monitoring usage, costs, budgets and performance in real-time. It sits at the critical intersection of AI and API management, while leaving you free to build your AI supply chain flexibly, with no vendor lock-in.

With robust governance in place, you’re well positioned to enable new revenue streams and position your enterprise at the forefront of those using AI effectively. All while you enjoy the peace of mind that comes with confidence in the quality of your AI.







▶ Watch the video

The building blocks of AI adoption are vendors, interfaces, data and tooling – your governance layer, providing monitoring, security and compliance. If you're trying to add value or improve performance, all of these come into play.

Martin Buhr, Tyk



Vendors

AI models (OpenAI, Anthropic, Meta etc.)



Interfaces

Applications where AI is used (chatbots, dev tools, enterprise dashboards)



Data

What makes AI useful: internal docs, customer interactions, logs, etc.



Tooling

The governance layer (monitoring, security, compliance)

Adapted from LEAP 2.0 keynote session "AI governance in action: Structuring the AI supply chain for success" presented by Martin Buhr (Tyk)



With confidence in your AI systems and processes, your enterprise can leverage the power of AI-driven observability. This is where governance meets machine intelligence to deliver powerful, business-wide results. You can leverage AI-driven tools to enhance decision-making, benefitting significantly as a result of your earlier focus on API and AI governance.



▶ Watch the video

Teams are deploying AI in silos and employees are using unauthorized AI tools, with no central oversight. That's shadow IT at work, with AI. It's risky, inefficient and costly. At enterprise level, we're seeing solutions akin to the bring your own device movement, but these can only work if you have oversight. If you don't, these shadow use cases become uncontrollable.

Martin Buhr, Tyk

Adapted from LEAP 2.0 keynote session "AI governance in action: Structuring the AI supply chain for success" presented by Martin Buhr (Tyk)



By centralizing AI access and enabling seamless connections to tools and models through an AI gateway and AI portal, you can tackle the risk of shadow AI head-on. You can also track and monitor everything you need to ensure compliance with regulations such as GDPR and the California Consumer Privacy Act (CCPA).

Whether you're coming at this from a leadership, platform engineering or enterprise architecture stance, robust API governance sits at the heart of AI readiness.





Federated API management

Balancing governance, growth and agility

THE CHALLENGE

Growing at scale and at pace while managing multiple teams across multiple regions and business domains.

THE SOLUTION

Federated API management with centralized governance, for consistency and standardization that supports agile scaling.

Federated API management acknowledges the complexity that results from organic business growth. From bespoke and legacy systems to those brought in-house during acquisitions, enterprise API ecosystems can be messy. Federated API management works with this, rather than against it.

Through federated API management with centralized control, you can apply a single management and governance layer. Under this you can have multiple API gateways from different vendors, various event brokers and repositories, multiple deployment patterns and protocols – everything you rely on to operate flexibly and scale agilely.



[▶ Watch the video](#)

Modern API management isn't about just finding a tool that works easily out of the box. It's about understanding what an organization really needs and what will add value. That means understanding federated API management.

Daniel Kocot, codecentric AG

From LEAP 2.0 session, "Federated API management: Balancing governance and agility" presented by Daniel Kocot (codecentric AG)



Federated models let distributed teams innovate while maintaining governance standards. The benefits of this include increased agility, scalability and flexibility. You can tailor policies and tooling to meet specific needs without compromising overall



Centralized

- Single, centralized gateway manages all API traffic and lifecycle activities (e.g. security, policies, traffic routing)
- Works well in smaller, less complex environments
- Limitations:
 - Reduced scalability
 - Slower response times to changes
 - Potential bottlenecks as the organization grows

Federated

- Multiple gateways across different regions or departments, each capable to enforcing policies and handling API traffic locally
- Enhances scalability, flexibility, and allows tailored API policies for specific needs without compromising overall governance
- Advantages:
 - Higher agility
 - Better suited for global or multi-cloud enterprises

Adapted from LEAP 2.0 session, “Federated API management: Balancing governance and agility” presented by Daniel Kocot (codcentric AG)

Is federation free from challenges? No. But with a few key elements in place you can balance governance and agility strategically. To implement a federated model effectively, bear in mind the vital role of:



Discovery

in ensuring your APIs can be consistently discovered, reused and registered across numerous federated environments.



Policy enforcement

in governing API usage and applying consistent standards.



Security enforcement

in keeping APIs safe and secure across federated domains, ensuring teams have the confidence to innovate without risk.

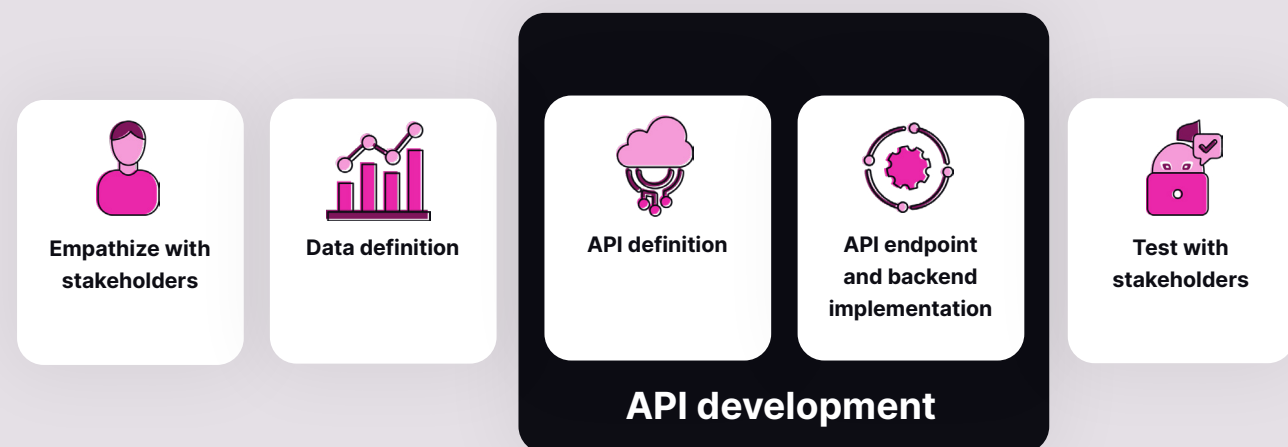
There’s a people element to this, too. Different teams will use different terminology, tools and approaches. Consulting with them on these and then implementing a specification framework that standardizes basic terminology and concepts (discovery, registration, management, security), can deliver consistency. It helps the business benefit from centralized governance, in the form of reliable security, enhanced scalability, easy interoperability and so on. Crucially, stakeholder engagement can also head off any resistance to change that might be triggered by the implementation of federated API management.



▶ Watch the video

Having a framework means it's easier to maintain order across complex systems while also meeting demands for agility and speed. After all, everybody wants to get to market first.

Daniel Kocot, codecentric AG



Adapted from LEAP 2.0 session, "Federated API management: Balancing governance and agility" presented by Daniel Kocot (codecentric AG)



Successfully implementing federation involves plenty of strategic thought. You'll need to think through integration complexity, putting training and tooling in place to ensure everyone has what they need. You'll also need to factor in compliance, avoiding the risk of inconsistent standards, security blind spots, shadow APIs and regulatory headaches arising from teams working around policies rather than within them.

Automation is your friend here, particularly with it comes to compliance checks and ensuring your APIs align with regulatory standards. By automating reviews and

feedback, you can loop into the creative process in a proactive way, meeting developers where they're at and empowering them to succeed.

Ultimately, federation is about delivering enterprise-wide policies while supporting creative local autonomy. With centralized governance, you can build in automated security and compliance while enabling your teams to innovate. You're giving teams the frameworks and tools they need to govern themselves with confidence – without wasting energy and resources on trying to control everything and turning governance into a roadblock.

Achieving this at scale across hybrid and multi-cloud environments starts with inventorying your existing APIs and tooling and identifying any gaps. You can then design your specification framework, with clear objectives and standardized processes and policies. Everything else – your ops cycles, automations in your design, deployment and management processes and so on – flows from that framework. It ensures you align business value with delivering consumer-centric APIs.

Remember to pilot your framework with a select few APIs to validate it, and to roll out stakeholder training to bring everyone on board. Then it's time to monitor everything and gather insights, ready to evolve and iterate (both your APIs and your framework) as you scale.

Following these best practices means you can empower your distributed teams while levelling up operational efficiency, enabling the business to achieve value aligned with its objectives. This is what balancing governance with agility is all about – delivering local autonomy within a global framework, while supporting better scalability and optimization for hybrid and multi-cloud environments.





The modern enterprise API portfolio

Unifying diverse API protocols and types

THE CHALLENGE

Multi-protocol APIs require you to bring governance consistency to different API types and protocols, while ensuring interoperability, security and compliance.

THE SOLUTION

A flexible, multi-protocol approach to API governance that embraces the commonalities and specificities of different types of APIs while making it easy to maintain at scale.



[▶ Watch the video](#)

Somewhere **between 50% and 75%** of all traffic is now APIs – and growth is still accelerating.

Kin Lane

From LEAP 2.0 opening keynote, “After 25 years of HTTP APIs do you have API governance in place?” presented by Kin Lane



The API boom has seen enterprises race to embrace the potential of GraphQL and event-driven, async APIs, all the while building on top of REST and gRPC architectures that themselves layer over legacy SOAP APIs. API diversity within enterprises is an unavoidable reality. But does that mean your governance has to be fragmented? Absolutely not!

Key to API governance success for modern enterprises is the ability to extend one governance model to every API type. It means you can embrace the

web-friendliness of REST, the speed of gRPC, the flexibility of GraphQL, all your SOAP building blocks and the real-time, event-driven capabilities of async APIs, even as you bring AI into the fold.

Multiprotocol API governance, focused on cross-protocol security, compliance and observability, is your key to unifying these diverse API protocols and types. It helps you address the hidden cost of API silos, reducing inefficiencies and security fragmentation, and supporting you to scale with confidence and ease. It also serves as a significant force multiplier.

“

 Watch the video

Taking those extra steps in defining your API governance and helping teams and directing them has a force multiplying effect. So, there's a lot more to governance than just policies and procedures.

James Higginbotham, LaunchAny

From LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)

”

For enterprises looking to govern REST, GraphQL, gRPC, SOAP, async and other APIs, the strategizing starts with understanding that optional practices mean inconsistent practices. Options and variations are important, certainly, but within a primary procedure or standard. Secondary procedures can complement that, to fit common situations, but there needs to be core guidance in place that spans all API types and protocols consistently.

With that in mind, your strategy for achieving a transformational API platform that supports solid governance across your ecosystem can be summarized in five steps:

- 01 Align with business architecture**
- 02 Create multiple engagement models**
- 03 Scale your efforts with federated API coaches**
- 04 Collaborate with other practice areas**
- 05 Establish API pillars**

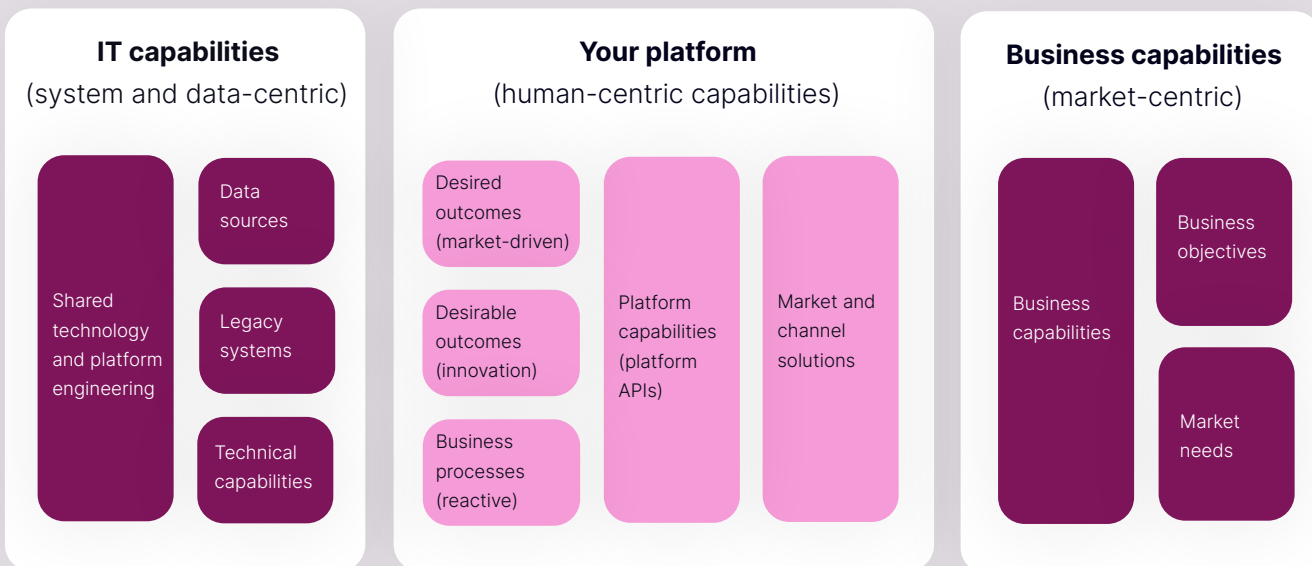
This strategy begins with mapping out your IT capabilities and your business capabilities. Your API platform sits at the heart of this, combining those capabilities so that your API consumers can have experiences that turn your business capabilities into digital capabilities. Your governance will drive all this, blending those capabilities to deliver a multiplying impact for your enterprise.



Watch the video

Governance policies and practices can drive business effectiveness. So, aligning efforts around governance with the goals of the business is important.

James Higginbotham, LaunchAny



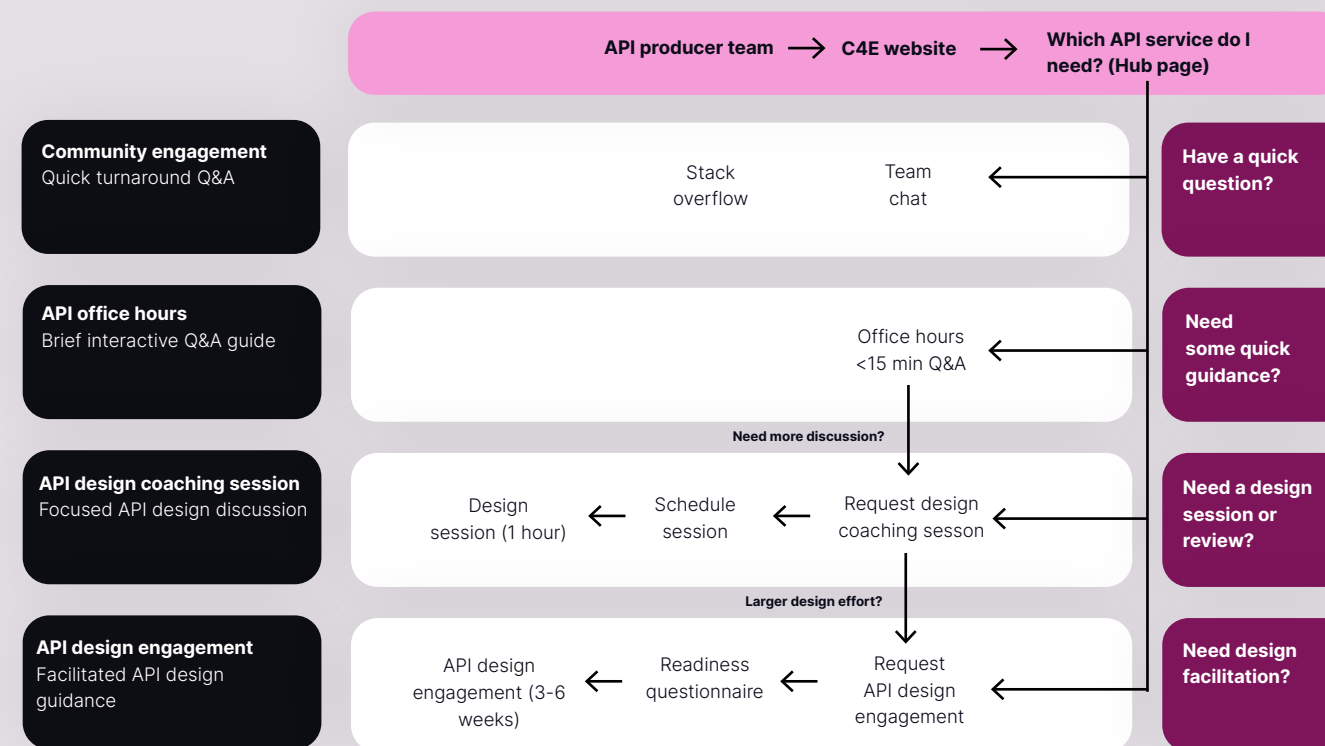
Adapted from LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)



Key to this is considering how your API platform can express your business as a topology of those different capabilities. The governance aspect flows from that structure, with the structure incorporating all your domains, capabilities, APIs and so on. You also need to think about the digital ecosystems that your enterprise supports – partners, customers, consumers, service providers, your workforce and so on. Your governance needs to factor in all of this.

You'll also need to create multiple engagement models, connecting with different teams in different ways, to ensure everyone has the support they need. One size doesn't fit all when it comes to team engagement, so map out how you're going to engage, bearing in mind each team's goals and timelines, as well as the wider business alignment.

Watch the video



Adapted from LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)

By incorporating all these different capabilities, digital ecosystems and team engagement models, you can pull together a governance approach that applies across your entire business, no matter which API types and protocols you use.

This overarching strategy will support you to maintain consistency as you scale, as well as compliance across different verticals and regions.

Once you address the principles and the people elements, you can take care of the technical side within that framework using the right approaches and tools to fit your requirements. A federated API model with a centralized governance body and federated coaches is one example of how to tackle this. On the tooling side, a unified API platform can empower you to simplify API integration and management across protocols.

The right platform can make it easy to apply your policies across diverse API landscapes, bringing consistency to the complexity, ensuring robust security and powering interoperability. You can apply policies, security and standards consistently, while still accounting for the distinct challenges that different APIs present within that framework.

“

A unified platform that delivers a centralized governance and security solution means you can use pre-built templates, centralized control and automated audits, to ensure compliance without slowing innovation. You can apply robust security features such as rate limiting, authorization modes and instant patching reduce downtime and boost confidence.

Budhadya Bhattacharya, Tyk

”

Fundamental to the success of this strategy is avoiding vendor lock-in and taking a protocol-agnostic approach. Doing so means you can future proof your API governance for emerging protocols. It’s not about picking a single protocol for your APIs, but about embracing a unified governance model that handles them all.

This approach to multiprotocol API governance also means you can enjoy full observability. So, not only can you apply consistent standards, but you can observe everything in a way that feeds better business decision-making.





Security is not optional

The API attack surface

THE CHALLENGE

Protecting your diverse, complex business ecosystems and data from attack while still enabling developer creativity to flourish.

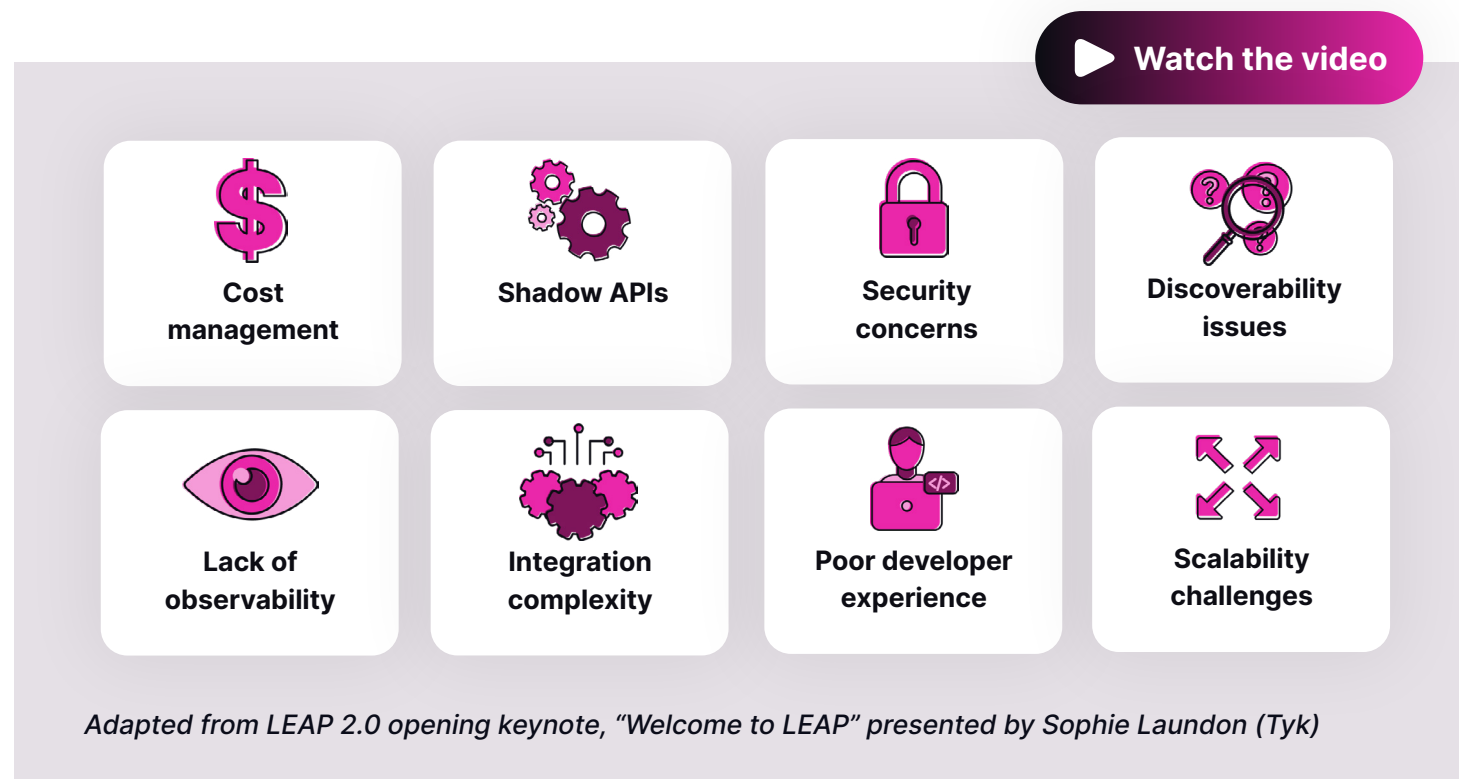
THE SOLUTION

Robust API governance that applies consistent security as standard across your multiprotocol, multi-vendor, multi-cloud API landscape.

APIs are hackers' new favorite target – and for good reason. They introduce multiple avenues through which hackers can try and get at your sensitive data. The pace at which the API industry is evolving means many enterprises are racing to try and keep up with the latest protocols and approaches. This opens the door for errors and vulnerabilities that hackers are quick to exploit.

27% of API attacks target business logic vulnerabilities, **up 10%** from last year ([Thales](#))

APIs are prime targets for attacks. Not only do they expose sensitive data, but the sheer scale of their use and the issue of API sprawl creates opportunities for hackers. Many enterprises struggle with shadow and rogue APIs, some of which bypass governance completely. This introduces significant security vulnerabilities and compliance risks. Then there's the API platform stack, where each component has its own security considerations and potential vulnerabilities.



Only 27% of enterprises with full API inventories know which APIs return sensitive data – **down from 40% in 2023**. ([Akamai](#))

To shore up such a broad attack surface, enterprises need processes in place to ensure that security is robust across their API ecosystem – and that comes down to effective governance. The enterprise decides its approach to different security matters (authorization mechanisms, for example), then governance enables this, standardizing the approach across the business, supported by the right tools to enforce it.

Enterprises also need to ensure that one compromised component doesn't compromise all the others in their platform. This leads into a zero-trust security approach, taking governance far beyond authentication.

63% of organizations worldwide have fully or partially implemented a zero-trust strategy. ([Gartner](#))

Realtor.com provides an excellent example of how a coordinated, consistent approach to API security and governance can deliver results at scale. Millions of home shoppers use the company, which is operated by Move, Inc, to find properties, information and tools for making informed real estate decisions.

Like many growing enterprises, Realtor.com ended up with a complex ecosystem that lacked standardization. It had seven different teams doing rate limiting seven different ways. It also had a custom authorizer for mobile requests that was costing it \$30k per year. Pushing releases live took an average of 45 days, with an average deployment time of 1.5 hours.

By standardizing rate limiting and implementing OAuth, Realtor.com used governance to bring consistency to its API security while also empowering its developers. The average time to push releases live dropped from 45 days to one day, while the 1.5-hour deployment time dropped to an average of five minutes. The business also no longer needed its custom authorizer, instantly saving \$30k from its annual budget. All while delivering a more consistent and robust defense against potential security incidents.

Cost is no small consideration when it comes to enterprise-level API security. Not tackling security consistently can be costly, as the Realtor.com example shows. The cost of security incidents can also be huge. Staff time spent investigating, rectifying and reporting, distraction from business as usual, loss of customers due to services outages and reputational damage, regulatory fines... the costs quickly mount.

API-related security issues now **cost organizations up to \$87 billion annually.** ([Thales](#))

With all this in mind, effective API governance is not a ‘nice to have’ – it’s an essential part of modern enterprises’ approach to security. Enterprises need to use policy automation to enforce governance everywhere. They need to secure APIs at the data level, as well as the traffic level. They need to secure individual components to prevent a domino effect if one is breached. And they need to combine API gateways with centralized observability into the entire API ecosystem.

This isn’t just about control. It’s about enabling teams to create and innovate with the confidence that security is baked in courtesy of governance guardrails. It means teams can build to those standards, with essential visibility, automation and adaptability underpinning future growth. API security isn’t a technical challenge – it’s a business-critical risk that demands robust governance.



API observability

The missing link in your governance strategy

THE CHALLENGE

Understanding where observability fits in the realm of governance and which metrics help drive business outcomes.

THE SOLUTION

Integrating observability into the development pipeline to monitor and measure both SLOs and KPIs across the business.

Governance without observability is a shot in the dark – you can't see those essential insights that are fundamental for performance tuning, troubleshooting, security, compliance and more. But with observability, your governance framework can drive business outcomes, enhance decision-making and fuel system performance improvements.



[▶ Watch the video](#)

Observability gives you the insights that you need – the transparency to understand your API landscape and to ensure you're following governance best practices as you scale and have more engineers exposing and using APIs.

Andreas Grabner, Dynatrace

*From LEAP 2.0 panel discussion, "API observability: The missing link in your governance strategy"
Budha Bhattacharya (Tyk), Andreas Grabner (Dynatrace), Hazel Weakly (Nivenly Foundation), Marylia Guitierrez (GrafanaLabs), Derric Gilling (Moesif)*



Like so many other aspects of governance, observability is more than simply a technical challenge. It's about moving your thinking beyond engineering to glean insights that help enable your business. It's an enabling force that can drive company-wide value.

With the right observability approach, your enterprise has much to gain:



Understand how your APIs are functioning in terms of performance, usage, latency and errors – and how to optimize them.



Monitor traffic patterns to detect anomalies, ensure fair usage and identify monetization opportunities.



Identify security vulnerabilities and take proactive corrective action.



Understand third-party service dependencies.

All of this contributes to a comprehensive view of your entire API landscape. It lets you see the big picture, as well as making everything from enforcing governance policies to issue detection to performance optimization easier and more efficient.

To gain maximum benefit from using observability to drive business outcomes, best practice means integrating it into your CI/CD pipelines, embedding it into your development processes for early identification of vulnerabilities and continuous performance monitoring.

You can use OpenTelemetry to embed observability incrementally as part of your governance framework. You can start with basic auto-instrumentation then expand your data collection across different systems. This step-by-step approach helps gain stakeholder buy-in, ensuring teams don't become overwhelmed and enabling them to see the benefits of observability and then tailor it to meet their specific needs.

This is where it's important to think about metrics and how they align with your business goals. What will metrics such as adoption rate, API traffic, churn rate, retention rate and net revenue retention contribute to your measurement of API performance and success? How will you use them to inform your decision-making? Strategic thinking on what works best for your particular use cases will pay dividends. Regular reviews with all stakeholders will also ensure your metrics remain relevant over time.

When you're just starting out with observability metrics, focusing on performance and security can be helpful. Visibility into these core elements can do much to level up your governance approach, as well as guiding your understanding of the powerful insights that metrics can produce.

As with many areas of governance at scale, observability is not without its challenges.

“

[Watch the video](#)

Security and observability are often seen as directly conflicting with each other. You secure something in a compliant way but then, with observability, you have this side channel, all this extra data. The challenge is how you enable this ability without having to redo all of your security and compliance work times ten.

Hazel Weakly, Nivenly Foundation

From LEAP 2.0 panel discussion, “API observability: The missing link in your governance strategy”
Budha Bhattacharya (Tyk), Andreas Grabner (Dynatrace), Hazel Weakly (Nivenly Foundation), Marylia Guitierrez (GrafanaLabs), Derric Gilling (Moesif)

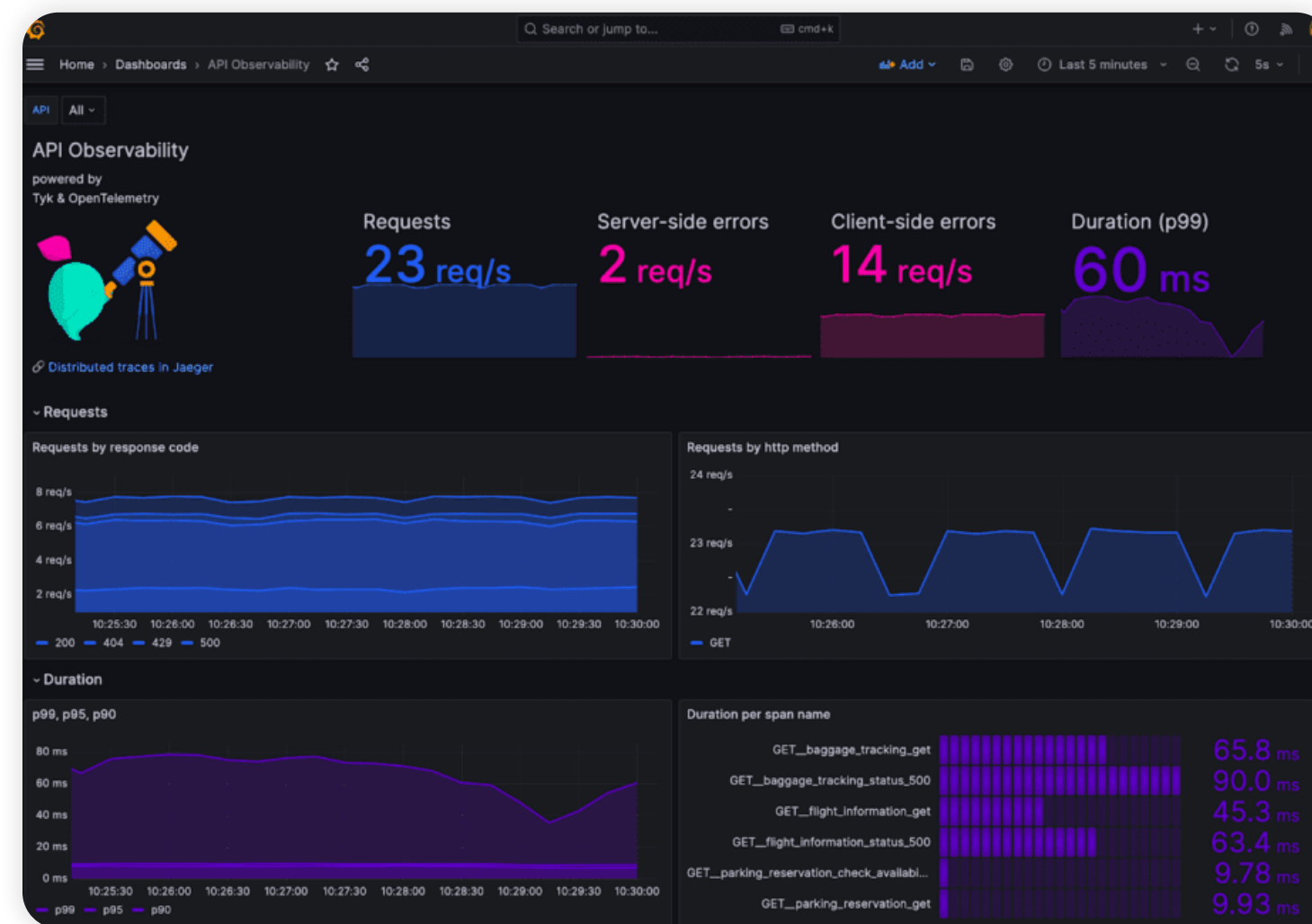
”

Gaining visibility into system behavior and while also protecting data and user privacy comes down to the way you implement data governance practices. You'll need a strategy that encompasses data scrubbing, redaction and deletion to get the best out of your observability while also making security and privacy top priorities.

You can also embrace automation in your observability processes, using (appropriately governed) AI to track system health, monitor performance, detect issues (and resolve them) and more. AI can also power automated performance tuning, delivering incremental enhancements to level up your business within the boundaries of your governance guidelines.

Investment in and successful deployment of observability platforms

leads to revenue loss avoidance and enables faster product development cycles and improvements in brand perception. ([Gartner](#))





The road ahead

API governance as a competitive differentiator

THE CHALLENGE

Implementing governance aligned to business values and focus, so that it serves as a future-focused enabler.

THE SOLUTION

An API governance framework aligned to core pillars that flow organizational values throughout policies and processes, while taking your people along on the journey.

When you embrace governance as a framework of policies, processes and procedures, aligned with business goals and implemented with a people focus, you're ready for it to become a competitive differentiator. It embeds your values across the business, serves as a force multiplier and even creates coaching and career opportunities within your teams.



Watch the video

API governance creates opportunities for us to help people understand deeper about APIs and the dynamics we deliver, both organizationally and generally in terms of protocols, technologies and developer experience. That's a powerful opportunity for coaching and career growth.

James Higginbotham, LaunchAny

1. **API governance defines our values** and how they will impact the ecosystems and people we serve.
2. **API governance is a force multiplier** - an API provider team and the business can have a positive impact for many API consumers.
3. **API governance creates opportunities for coaching**, resulting in individual career growth.

From LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)



Aligning your API governance with your business architecture and values means you're well positioned to scale and embrace the future, bringing consistency to your business across multiple systems, vendors, clouds, regions and more. Having multiple engagement models in place further supports this, ensuring you're bringing your people with you as part of your governance efforts.

One essential part of this is to establish API pillars, within the three headline categories of API strategy and enablement, API management and API operations.

Watch the video



API strategy and enablement

Pillars related to the platform strategy, business alignment, governance, and enablement associated with the API platform



API management

Pillars related to the ownership and management of the overall API platform and individual platform APIs



API operations

Pillars related to security and operations of the API to ensure that all platform APIs are continually evaluated for proper security measures, optimized deployment, and continuous monitoring and improvements

Adapted from LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)

API pillars are broad statements that outline the core principles and areas of focus you need for your enterprise to operate successfully.



Watch the video

Pillars are the foundational elements that help you figure out what all your policies and everything else should entail. They focus on strategy enablement, management and operations. From there, you can figure out where you need to be to walk, run and fly with your organization.

James Higginbotham, LaunchAny

From LEAP 2.0 closing keynote, "The API governance survival guide" presented by James Higginbotham (LaunchAny)



With pillars underpinning the standards, practices and policies that support your overall API platform strategy, you can support teams to make decisions quickly and easily while ensuring those decisions are aligned with organizational principles and focus. With them in place, you can evaluate your strategy, policies, practices, design, documentation – your full API lifecycles – against the backdrop you need to enable organizational success and set you apart from the competition.

This high-level focus means that all the elements of your API governance will come together to support consistency and reusability. You can say goodbye to siloed APIs and wasted developer focus. Instead, you have a stable and strong foundation for API marketplaces that boost discovery, productization and monetization – all in a way that’s aligned with your business purpose.

This is about using API governance as more than just a compliance, security or visibility tool. It’s about taking all of that and turning it into a strategic weapon that gives you an edge over the competition. You can embrace the processes and platforms to govern all APIs across multiple protocols, types, vendors, clouds and so on. Doing so means your enterprise will be ready to scale at pace in an event-driven world, while also levelling up your AI readiness.

By 2028, 50% of API usage will not involve a developer. By 2029, 50% of API monetization will be supported by machine/nonhuman customers.
(Gartner)

Being ready for the future of API governance has never been more strategically important. The pace of the API boom is accelerating and will continue to do so. If your enterprise plans to take advantage of all that new technologies and concepts offer, a firm API governance foundation is non-negotiable. It is fundamental to your future success.



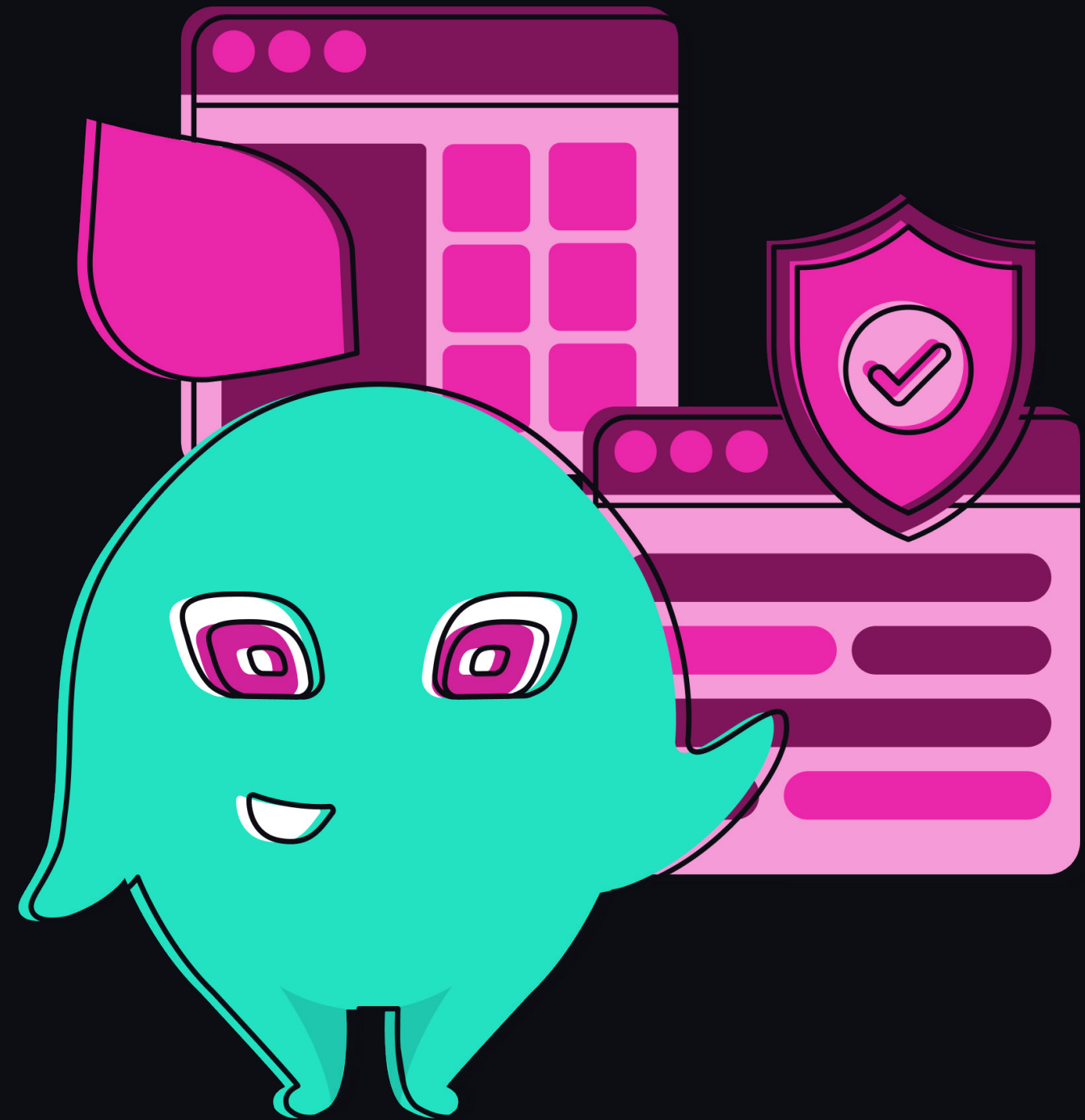
Conclusion

Universal API governance isn't about red tape – it's about unlocking the full potential of your APIs without exposing your business to risk. Done well, it fuels innovation, scalability and security, ensuring your enterprise can not only excel now but be ready to embrace emerging and evolving future technologies. Done wrong – or ignored – it's a recipe for disaster.

If you want to architect a better future for your enterprise, the time to act is now. As a key decision-maker within a large and complex organization, you can embrace API governance as a business-led solution to business problems, working with your unique architecture and teams to empower your enterprise.

The platforms you choose can enforce your API governance in a way that makes it easy for people to comply and gives them the confidence they need to fly.

Get in touch to discuss Tyk's new universal API governance solution.



Acknowledgements

This content was created by Tyk, but would not have been possible without the inspiration, creativity and technical expertise of the following contributors.

Thank you, everyone.

- **Abby Bangser**,
Principal Engineer at Syntasso
- **Ahmet Soormally**,
Head of Research at Tyk
- **Alexander Troppmann**,
Lead Cloud-native Architect for Platform Integration at Zeiss
- **Andreas Grabner**,
DevOps Activist at Dynatrace and CNCF Ambassador
- **Bill Doerrfeld**,
Tech Journalist at Nordic APIs
- **Bruno Pedro**,
Author of Building an API Product
- **Budhaditya Bhattacharya**,
Director of Product Ecosystem at Tyk
- **Carlos Villanúa Fernández**,
Presales Solutions Architect at Tyk
- **Carol Cheung**,
Senior Product Manager at Tyk
- **Charlie Egan**,
Senior Developer Advocate at Styra
- **Daniel Kocot**,
Head of API Consulting at codcentric AG
- **Derric Gilling**,
CEO at Moesif
- **Hazel Weakly**,
Fellow of the Nivenly Foundation
- **James Higginbotham**,
API Strategist at LaunchAny
- **James Hirst**,
COO at Tyk
- **Jennifer Riggins**,
Tech Journalist at NewStack
- **Juan Cruz Viotti**,
Founder at Sourcemeta
- **Justin Russo**,
Senior Systems Software Engineer at Northwestern Mutual
- **Kin Lane**,
API Evangelist
- **Leonid Bugaev**,
Head of Engineering at Tyk
- **Lorna Mitchell**,
Technical Steering Committee Member at OpenAPI Initiative
- **Lukasz Gornicki**,
Executive Director at AsyncAPI Initiative
- **Martin Buhr**,
CEO at Tyk
- **Marylia Gutierrez**,
Staff Software Engineer at Grafana Labs
- **Matt Tanner**,
Head of Growth Engineering at SingleStore
- **Nancy Chauhan**,
Tech Advisory Group - Env Sustainability at CNCF
- **Omri Gazitt**,
Co-founder and CEO at Aserto
- **Sedky Haider**,
Director of Solutions Architecture at Tyk
- **Siddhant Khare**,
Software Engineer at GitPod
- **Sophie Laundon**,
Head of Product at Tyk
- **Sreekanth Cherukuri**,
SVP - Global Head of Integration Solutions at Coforge
- **Swen Helge-Huber**,
Senior Director, Office of the CTO at Solace
- **Tamara Evans**,
Account Director at Tyk