Boost Your Business with Secure Open APIs

An AdNovum IT Consulting White Paper, March 2020

AdNovum

About AdNovum IT Consulting

AdNovum has been designing, implementing and maintaining high-quality software solutions for companies and authorities for more than 30 years. We impart the knowledge and experience gained from our projects to our customers in the form of advice. We provide manufacturer-independent and product-independent support for complex IT projects. Our range of services includes all solution levels, from technical questions to process design to IT strategy consultation.

Identity and access management and cyber security are core areas of IT consulting services provided by AdNovum.

http://www.adnovum.ch/

About the authors

Silvano Fari, degree in Computer Science HTL with a CAS in Information Security, is a Principal IAM Engineer and has been with AdNovum since 2012. He has more than 15 years of experience as a security engineer and IT consultant, advising clients on identity and access management, security matters with web applications, the NEVIS Security Suite, and the introduction of new authentication solutions.

Leo Bolshanin, Master of Science in Communication Systems EPF, is a Senior IT Consultant and joined AdNovum in 2017 after leaving the security company he founded. He has of a proven track record of 15 years in cybersecurity and possesses solid experience in security consultancy, technology leadership, team and project management.

APIs are everywhere

"APIs form the connecting glue between modern applications. Nearly every application uses APIs to connect with corporate data sources, third-party data services, or other applications. Creating an open description format for API services that is vendor-neutral, portable, and open is critical to accelerating the vision of a truly connected world" – OpenAPI Initiative website.

You have certainly heard numerous stories about APIs promising to change the business world. In practice, however, the following questions have to be addressed:

- What exactly are the benefits of open APIs to my organization?
- Even if business opportunities exist in some areas, is it safe to expose the data and business functionality of my organization on the internet?
- Regulations such as Payment Services Directive 2 (PSD2) force my organization to provide open API. How do we not only comply with these regulations but also manage to benefit from open API?

If you find these questions relevant, you should continue reading this article!

At first, we will provide our view on the business context around open API. Second, we will explain what security measures you need to protect your data and digital assets while "wiring" your business to the open API ecosystem.

Open APIs are changing the digital world

What is the truth behind the big promises of digital open APIs? Will leveraging the open API approach harm or enhance your business?

Before open APIs appeared on the scene, organizations mostly had direct digital channels to their customers. That has changed with open APIs, as customers can now be reached through third-party providers. In this new paradigm, these third-party providers are basing their business on the added value they offer on top of the existing services available through APIs of your firm. This new collaboration model makes the global offering more attractive – which logically should help you increase sales.

We are convinced that a lot of organizations could significantly grow their business through open APIs. Their direct customer contact will in any case be reduced in some areas due to the globalization and digitalization of business. Therefore, leveraging open APIs becomes the natural response in adapting your activities to this challenging economic context. Actually, it may give you the opportunity to focus on your core business while allowing third parties to commercialize or package it in more complex and structured proposals.

As an example, customers may start managing their bank accounts through an app that aggregates account information from different financial institutions. These customers have less interactions with their bank, but they still leave their accounts where they are. Through the new channel empowered by the API, they eventually use them more intensely then before. Accordingly, this strengthens the customer relationship even though the interaction is indirect.

Figure 1: Overview open APIs

Many organizations collect, store, and organize significant amounts of data from their customers. We are convinced that data is the most valuable business asset of today and the future. In consequence, the goal for such organizations should be to optimize and maximize the controlled use of this asset through both direct channels and third parties. This can be achieved by offering APIs to operate on this data and to further monetize its use. Thus, it is not only the direct channel to customers that creates income.

From this perspective, let's have a closer look at the banking sector.

Traditional values of banks such as size, branch network, traditions, regionality are becoming less important and are increasingly replaced by new digital offerings that are boosting speed, innovation, and flexibility. Customer behavior and preferences are changing as customers are becoming less loyal to single institutions.

Indeed, the millennial population is more dynamic. They identify the most with the trendiest services on the internet and start using them right away.

There are new players, so-called FinTechs, that cater to these dynamically changing requirements and expectations of the contemporary customer better than traditional banks can. They explore new ways of interaction between customers and financial institutions – enabling customers to access and steer their financial portfolio from everywhere, at any time, and through multiple channels, such as mobile devices and the traditional web. However, these FinTechs cannot do business without collaborating with established banks, which form the backbone of the financial system. For the established banks, on the other hand, competing with these agile FinTechs would require a huge effort and be extremely costly.

Because of strict financial regulations and capital requirements, FinTechs de facto depend on banks, which are in a position of strength. Such a partnership could form the foundation for a perfect symbiosis between established businesses and innovators.

In summary, we believe that opening the mind for collaboration with third parties represents an interesting opportunity to generate new business. This is especially welcome now among conventional banks operating in a challenging context (regulatory pressure, digitalization, market consolidation). Therefore, it is worth giving a try to open-banking initiatives such as PSD2 as a potential door opener, instead of hiding from the changing world behind the entry portal.

Business use case

In this section, we invite you to put theory into practice with a concrete example. Let's review the case of a peer-to-peer web auction platform.

In such systems, individuals are often simply brought in contact with each other on the platform, and payments go directly from the buyer to the seller, who explicitly pays a fee to the auction platform upon completion.

The ecosystem shown in the following picture is composed of several actors:

- Web auction platform
- Seller
- Buyer
- Seller's bank
- Buyer's bank

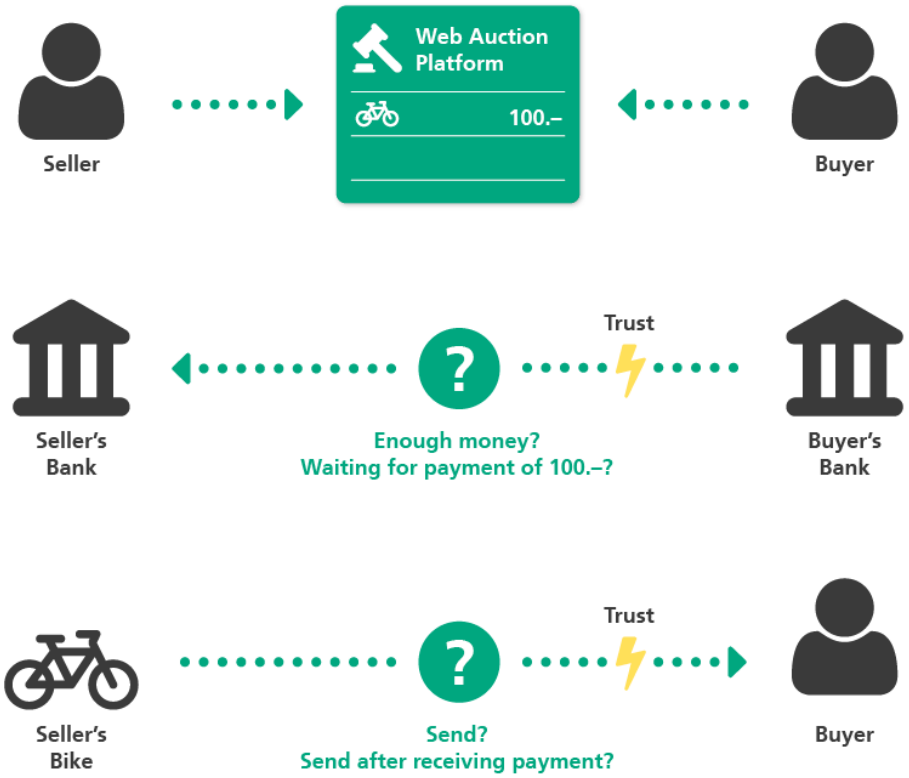

Figure 2: Web auction platform ecosystem

This situation presents several challenges:

- The buyer must blindly trust the seller and send the money in advance. (trust=-1)
- The buyer needs to use his e-banking account, go to the post office, or pay by credit card, which can require entering such data as multi-digit numbers and his address, or entail other cumbersome procedures. (usability=-1)
- The seller's and buyer's identities may be fake, potentially presenting a problem if the transaction fails. (trust=-2)
- The seller rating can be modified using fake reviews. (trust=-3)
- The product delivery is delayed because the seller wants to receive the money first. (usability=-2)
- The seller may defraud the buyer and never send the article after receiving payment. (trust=-4)
- When a buyer wins an auction, the seller has no assurance that the buyer can pay the final auction price. (trust=-5)
- New sellers that are not extensively rated through previous transactions could be disadvantaged by a lack of trust among buyers. (trust=-6)
- The digital auction platform could suffer from user churn if it simply brings people in contact and does not provide other added value that promotes user loyalty. Also, sellers and buyers may be reluctant to pay significant fees, as the platform does not guarantee a successful business transaction. (business=-1)
- Nothing links the buyer and the seller to a particular financial institution. (business=-2)

The overall scores are -6 for trust, -2 for business, and -2 to usability ... but can we improve them?

How can open APIs help for the benefit of all parties involved? The basic issue here is that no party is reliably supervising the whole operational process of the transaction. This is because the auction platform simply cannot follow the entire process, as key parts of it occur in the real world beyond the auction platform's digital systems.

Let’s imagine that a particular banking institution is offering an open API, providing controlled access to the seller’s and the buyer’s bank accounts.

Upon the end users’ consent, the auction platform can now interconnect with such interfaces to become the “trustee” for each transaction. The banking open API can thus offer the following basic services:

- Proof of identity
- Proof of funds
- Payment initiation

Therefore, we have the following process:

1. Upon registration, the auction platform connects to the bank accounts of sellers and buyers.
2. The auction platform verifies the buyers' and sellers' identities.
3. Based on the certified identities, the auction platform checks its registry to verify that the buyer and seller are not fraudsters.
4. The seller starts the auction.
5. With each new bid, the auction platform verifies that potential buyers have enough money in their accounts.
6. When the auction is completed, the corresponding amount is automatically debited from the buyer account and transferred to the auction platform intermediary account, which acts as a “trustee” for the transaction.
7. The seller receives confirmation from the auction platform that the product can be shipped.
8. Upon receipt, the buyer verifies the product condition and gives confirmation to the auction platform to forward the money.

Figure 3: Benefits of open APIs for a web auction platform

We clearly see an emergence of a new interrelated ecosystem including the auction platform, the bank, the seller, and the buyer, which, in comparison to the initial situation, clearly increases trust and provides better services. Moreover, this ecosystem can act as a basis for more value-added services, such as microloans and partial payment, in which the auction platform plays the role of broker for the loan service provided by the bank.

From the bank's perspective, it remains the financial backbone, providing core services to the auction platform, which in turn acts as a third party between the bank and the end customer. Of course, in such a scenario, the contractual part can be fully automated, thus providing an excellent customer experience in comparison with a manual execution of the full workflow.

Security is important

All of the above sounds promising, but it also raises concerns and the following question: "Are the organization's data and the processes with this data still safe from theft or manipulation, despite their exposure?"

The answer is yes! But you need to follow some important security objectives for the setup of your API platform and the processes around it. The following sections explain what the crucial points of API security are.

Note that these security objectives also apply if your APIs are not "open", meaning that they are only exposed for use by your own applications. Even if such APIs are not available to third parties, they are still exposed on the internet and therefore also need strong protection.

Know what to protect

Do you know your organizations APIs? Did you know that modern applications such as single-page applications or mobile apps lead to exposed APIs? Even if they are not public and of an internal nature, they can still be attacked. So security really matters!

Unawareness of exposed APIs implies a risk of insufficient access controls for using them. This could enable attackers to extract data from your organization. Since regulations force you to protect the data of your customers, this could even be a legal issue beside the reputational problem.

Do not become one of the companies who find out the hard way about their insecure APIs and get breached. It is very important that you know your APIs.

An inventory and categorization of your APIs are essential to choose and set up the right security measures. The APIs need to be categorized according to their exposure (private, private trusted B2B, public) and the sensitivity of the data they give access to.

API security differs

Additional risks apply when using APIs because the API model forces users to grant third parties access to the provider's system and the user's data. Regular users do not have the knowledge to assess risks related to this delegation of access (third parties can be malicious). As service providers, we have the obligation to make this understandable to the users.

As an organization that provides APIs, you are responsible for:

- ensuring that only known and trusted client applications can act on behalf of your customers,
- providing proper authorization and consent processes for client applications,
- protecting these consent processes with adequate authentication mechanisms, and
- designing these processes in a form understandable to your customers.

As a customer, you want to have control over:

- which client application can act on your behalf,
- giving and revoking consent to client applications at any time,
- which data can be seen by the authorized client application, and
- having the transparency to see all this.

Access to APIs must be manageable at any time by the the data owner (user) and the organization that offers the APIs.

Delegation model terms

The following image only shows a highly simplified diagram of the mentioned delegation model. The purpose of this image is to explain the terms used in the following paragraphs. The model will be explained in more detail below.

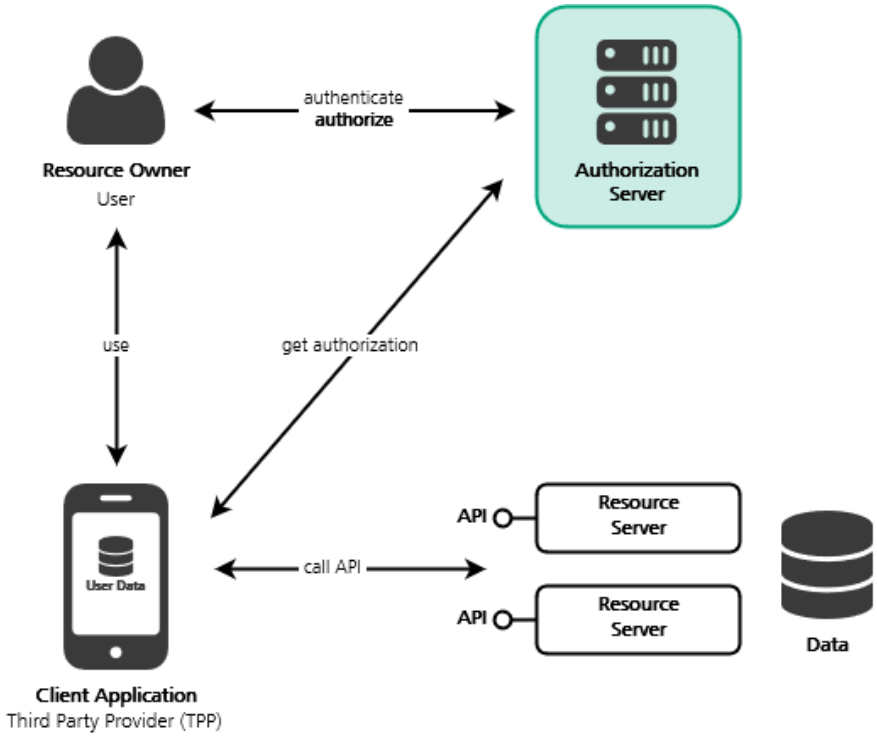

Figure 4: Delegation model for access to open APIs

The image shows how a user **(resource owner)** works on a **client application** to access his data on the **resource servers.** The resource servers provide **APIs** for that purpose. The user **authorizes** the client application on the **authorization server.** In order to act on behalf of the user (resource owner), the client application obtains its **authorization** in form of a token from the authorization server.

API security objectives

The following table shows the most important security objectives that apply to exposed APIs. TPP stands for third-party provider and here is synonymous with client application. The picture further down shows the association of the topics in this table with the components in an API architecture.

No.	API Security Use Case or Process	Possible Threat	How to mitigate?
Client Management			
1	TPP registration	Registered client application could be malicious	Workflow to validate the TPP and contractual obligations
2	TPP governance	Orphan TPPs, TPPs could become malicious during their life cycle	Detect orphan TPPs on data of usage monitoring; revalidate client applications and update the contractual obligations on a regular basis
AAA Authentication, Authorization, Accounting			
3	User authentication	Impersonation	Strong authentication
4	Client application authentication	Malicious client application pretends to be a registered TPP	Require client ID and client secret for granting access; urge TPP to treat credentials securely
5	API authorization	Unauthorized access to data	Proper use of delegation protocol (OAuth2) for authorizing API access by TPPs
6	API accounting	Missing traceability on incident investigations	Log which client uses which API on behalf of whom at what time
Consent Management			
7	User consent	Organization view: Absence of fine-grained consent	Need-to-know principle, explicit fine-grained user consent
		User view: Giving extensive consent	Organization has to provide transparency adapted to user knowledge
8	User consent governance	Organization view: Outdated consent	Consent management portal, awareness program, consent expiry, active life cycle management of consent
		User view: Outdated consent leads to lack of transparency	Actively withdraw consent for unused services, giving minimal consent
Data Security			
9	Content inspection	Malicious code or data injection	Input validation on multiple layers (API implementation, API gateway)
10	Data governance	TPP gets more information than the user wants to give	Dynamic fine-grained authorization on data level according to given consent

11	Data protection	Information leakage, integrity violation	Encryption of data in transit using TLS or even TLS with additional content encryption/signing
12	Quota management	Exfiltrating large amount of data	Limit the use of APIs per client (throttling)
API Management			
13	API governance	Unneeded exposed APIs or API versions	Usage monitoring, integration into security information and event management (SIEM) systems; clear audit trails on API usage; up-to-date inventory of APIs and TPPs; API life cycle and version management
14	API monitoring and analytics	Undetected brute force attacks or improper use of APIs by legitimate TPPs	Anomaly detection with machine learning and/or statistics on data of usage monitoring; maybe provide an undocumented decoy API (fake API with meaningful responses) and monitor its usage; calls to the decoy API are suspicious and give you an indication of malicious activities in a simple manner
Dev Sec Ops			
15	Dev Sec Ops	Buggy APIs get to production	Implement a proper DevSecOps process for building new or changing existing APIs; APIs change and evolve fast, so avoid hasty deployments with a well-defined development process and automated tools

The API Security Top 10 of the Open Web Application Security Project (OWASP) is a list of threats specific to APIs and has been used as a reference in compiling this table. The list is of high value and intends to strengthen awareness for security topics surrounding APIs. We recommend taking this list into consideration as well when securing your API.

Most of the API gateway suites available on the market today offer solutions and tools to implement all the above-mentioned API use cases and processes. To be able to offer robust APIs, there must be an API gateway component that acts as a single policy enforcement point. Such API gateways usually offer standard-based integration possibilities for customer identity and access management (CIAM) systems so you can leverage existing customer accounts and existing authentication and identity management processes.

Realizing the security objectives

The following picture shows a typical API architecture and outlines how these security objectives can be realized using a delegation pattern. The security objective groups from the table above are shown in their area within the API architecture and marked with the corresponding color.

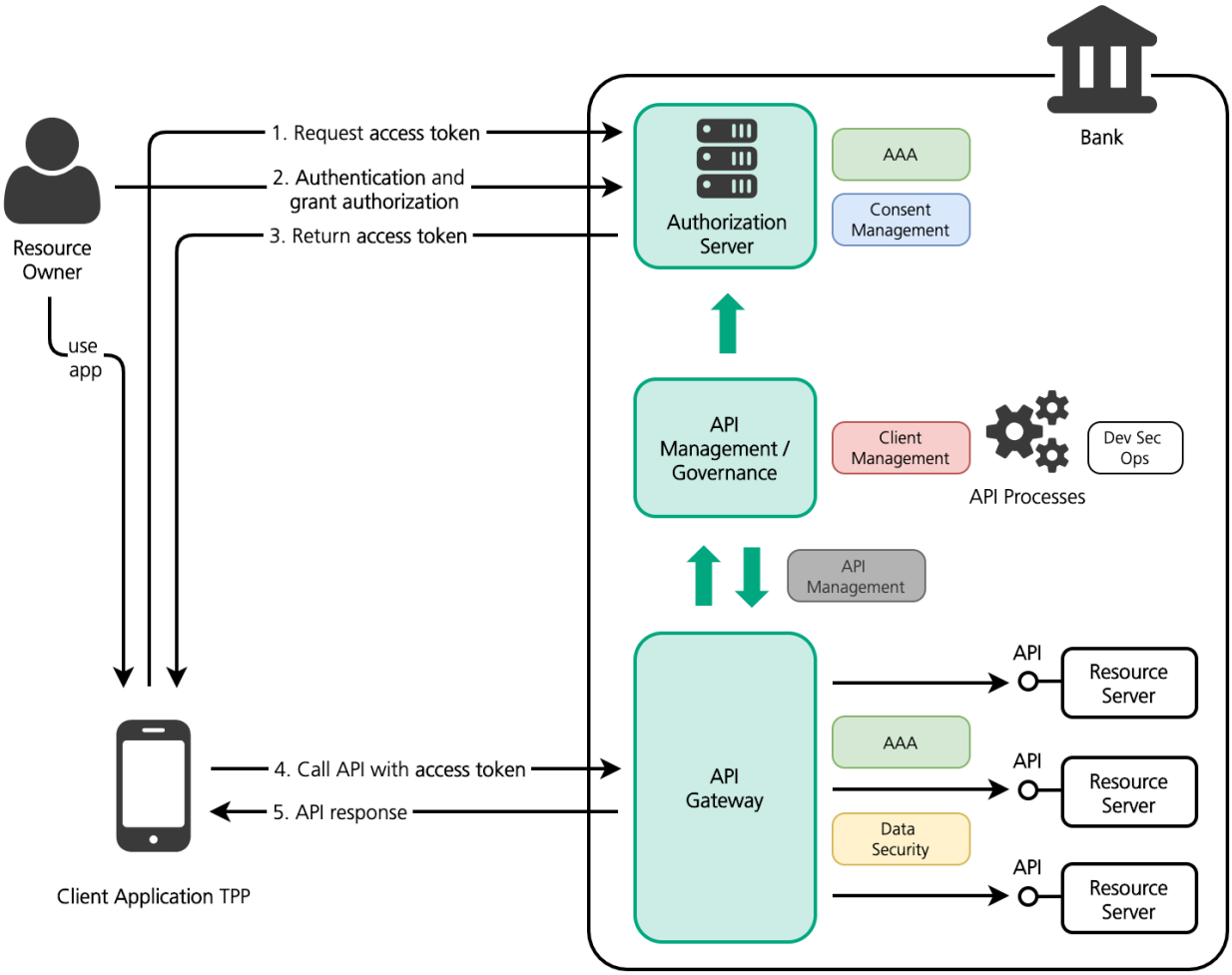

Figure 5: Open API platform

So how is security implemented in environments that provide APIs? This paragraph outlines what is needed to provide APIs in a secure manner. The definitions in bold here are also visible in the image above.

The access control to APIs is usually realized with a delegation pattern. Delegation in this context means that the user authorizes an application to access its data. This application is often from a third-party provider (TPP) and may use APIs from different organizations. Delegation allows the client application to act on behalf of the user on the API and therefore access the user's data.

It is all about a **client application** that works on services that are available over an API, the so-called **resource servers.**

- The client application calls the API on behalf of a particular person, the so-called **resource owner**.
- To make this possible, the resource owner **grants authorizations** (also called giving consent) on the **authorization server** to the particular client.
- To do this, the authorization server asks the resource owner for **authentication** and to confirm the requested authorizations for the client. Ideally, consent for the user data can be given or withdrawn at any time by the resource owner.
- The authorization server issues an **access token** for the client. The client application can collect this token at the authorization server by authenticating itself (technical user).

All this allows the client application to work on behalf of the resource owner on the resource server according to the granted authorizations. This process is also often called delegation, because work with some resources has been delegated.

Since this process has a lot to do with authentication and authorization, the authorization server is often provided by the customer IAM solution (CIAM) of an organization. But it still needs a close integration with the API management suite, since the management of the client applications and the APIs is done there.

The recommended protocol to be used for this delegation is OAuth2. OAuth2 enables the client to work on the API on behalf of the resource owner using the OAuth2 access token.

Also concerning access control, the **API gateway** needs to ensure the validity of the access token with each request. Additionally, it checks if the access token contains the particular authorization needed for the requested API. Furthermore, the API gateway also protects the APIs with traffic limitations and web application firewall features to inspect the requests and their content. This is also the time to collect data for the monitoring of APIs and to detect and react to anomalies such as improper calls and attacks on APIs.

Management and governance of APIs are realized by adding a component to the API gateway, e.g., a portal, a console, and/or programmable interfaces. Tasks such as the registration of new client applications, deploying new APIs or new API versions can be executed with this component. Data collected during run-time on the API gateway also gets processed by this component for monitoring and audit reasons.

A common API suite provides you with all the tools needed to operate a secure API infrastructure. Nevertheless, clear and well-defined **API processes** concerning design, development, deployment, and decommissioning of APIs are also important for running a secure API platform.

Conclusion

Once you have the API platform in place, it is simple to extend the range of offered APIs, allowing your business ideas to be implemented faster. A well-designed and secure API environment ensures a fast "go-to-market". Such an API platform can be used to collaborate efficiently with other businesses and third parties (e.g., open banking, PSD2). Of course, it can also host the private APIs that are only used by your own applications but still need to be accessible through the internet. In general, APIs are an effective measure to grow your digital potential and open up new channels to reach customers through third parties.

When proper security measures covering data, processes, and customer information are implemented to protect your API platform – the security becomes truly scalable. Authentication, authorization, and the API gateway, serving as a policy enforcement point, can be reused for all APIs, users, and client applications. New applications do not need to reinvent the wheel and can just be plugged in. Bug fixes and improvements to the security layer automatically apply to all of the APIs. Usually, when a company extends their business services, this implies new security risks. With an established API platform, a new service offered through an API inherits the security baseline already in place, making it possible to extend your digital business safely and with little effort.

Therefore, by leveraging APIs, you can boost innovation and push your business to the next level!

AdNovum can help you become part of this new business ecosystem:

We have hands-on experience in multiple areas of API technology.

Thanks to numerous IAM projects and the NEVIS solution, we can provide an authorization server that is highly secure yet flexible enough to implement almost any kind of authentication workflow. It can be integrated into any API management suite on the market. NEVIS solution offers solution guides with defined blueprints covering various integration scenarios with API management suites.

Our security experts can help you define the security requirements and measures needed on your API gateway and assist in the implementation of processes in API management and governance.

And if you are starting from scratch and need to create your APIs first, you can rely on our solid software development experience in designing and developing APIs for even the most demanding of industries.

AdNovum Zurich

Headquarter

AdNovum Informatik AG

Roentgenstrasse 22, CH-8005 Zurich

Phone: +41 44 272 6111

E-mail: info@adnovum.ch

AdNovum Bern

AdNovum Informatik AG

Brueckfeldstrasse 16, CH-3012 Bern

Phone: +41 31 952 5858

E-mail: info@adnovum.ch

AdNovum Suisse Romande

AdNovum Informatique SA

Avenue de l'Avant-Poste 4, CH-1005 Lausanne

Phone: +41 31 952 5858

E-mail: info@adnovum.ch

AdNovum Hungary

AdNovum Hungary Kft.

Bókay János utca 44-46, H-1083 Budapest

Phone: +36 1 701 0670

E-mail: info@adnovum.hu

AdNovum Portugal

AdNovum Portugal, Unipessoal Lda.

Campo Grande 378, 1700-097 Lisbon

Phone: +351 211 207 300

E-mail: info@adnovum.pt

AdNovum Singapore

AdNovum Singapore Pte. Ltd.

3 Shenton Way, #23-03 Shenton House

SG-068805 Singapore

Phone: +65 6536 0668

E-mail: info@adnovum.sg

AdNovum Vietnam

AdNovum Vietnam LLC

e.town 2 · 5th floor

364 Cong Hoa Street · Tan Binh District

Ho Chi Minh City

Phone: +84 28 3816 8200

E-mail: info@adnovum.vn