magora

HOW TO PROTECT YOUR DATA WHILE USING API SERVICES

Risks of hacking, information leakage and disclosure of confidential information terrify most business owners. Protected cloud solutions are often seen as a miracle cure for such security issues.

It's true that many risks can be minimised by using SaaS cloud technology. Organisations often apply protected third-party cloud services, but use non-protected API services to implement data exchange. This creates an opportunity for outsiders to access to confidential data.

- **Cloud computing** is a model for providing convenient, on-demand online access to the owner's data.
- **API (Application Programming Interface)** is a protocol that permits communication between different applications or program blocks to provide the company with quick access to their data collected in the cloud or on the remote server.

Let's investigate what should be done in order to avoid API hacking.

What does an API do

API services are used as part of the microservice architecture, making it very convenient to also access a remote server or cloud.

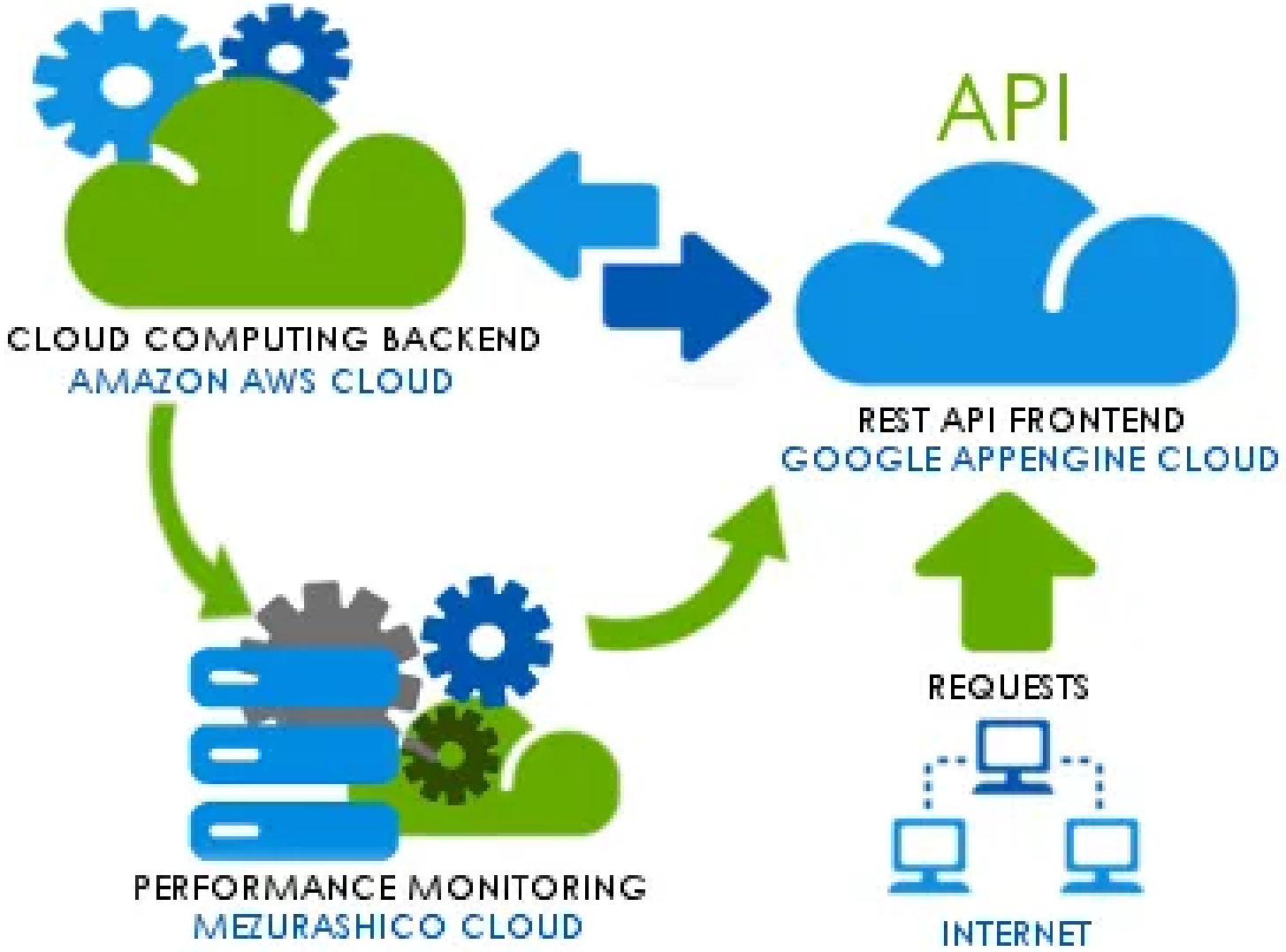
magora

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

TRIPLE CLOUD ARCHITECTURE

UNPRECEDENTED RELIABILITY & AVAILABILITY



+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

Security risks

The fact that every application programming interface can be potentially entered by hackers carries potential security risks.

In fact, without proper attention to the vulnerability resistance of the API itself, the service can become the weak spot in your security system. How can one prevent such a deplorable outcome?

In Magora, we minimise related security risks with appropriate API management. We are well aware that even though there are tools that can guarantee a high level of security, the best way to avoid any leaps is to take these risks into account at the development stage.

The three most common problems with API services:

- **unauthorised changes to information.** Being unable to guarantee your clients secure API components can drastically affect the reputation of your brand. For instance, a cyber attack forced a shutdown of the Sony Pictures website and jeopardised its authority.
- **information leakage.** Facebook is notorious for private information leaks. One of the reasons behind such outcomes is insecure APIs.
- **interference with legitimate activity.** If outsiders gain access to your software or website, the minimum level of damage is the fines based on the GDPR.

What can be done

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

To ensure the security of API services, we follow these three routines:

1. **Achieve multi-zone networking.** We make apps run in a container and make only a few services visible to outsiders. For example, we utilise Docker containers that encapsulate the code and all its dependencies so that applications can run swiftly and reliably from one computing environment to another.
2. **Guarantee network connection revision.** An adequate network management policy helps us to control the traffic to the programming interface address. It checks the IP address of the source of the messages and passes over only proper messages.
   Even if a hacker doesn't manage to harm to the code directly, hostile messages can negatively affect the workflow of an API, for example, by slowing it down. However, this measure helps to minimise such risks.
3. **Utilise encryption.** To secure the API from unauthorised attempts to access it directly, we organise encrypted cloud storages. Improperly encrypted messages will not pass and will be

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

removed.
It is preferable for the encryption to be generated by a corporate programmer and not an API manager. But be sure that the manager will be able to interpret the encryption. Otherwise, the requests will need to be decrypted and then encrypted again, which creates delays.

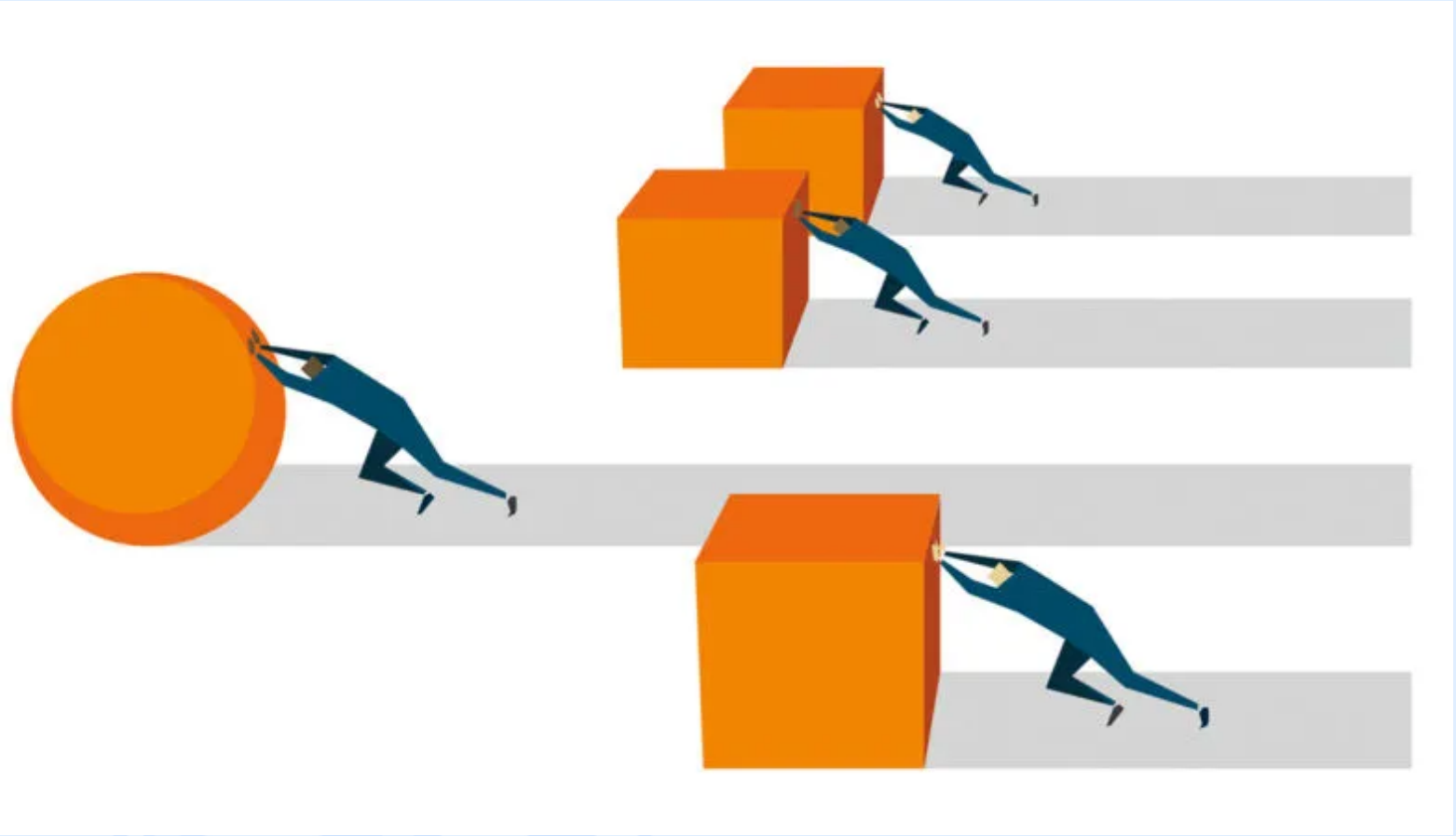
For better security we do not apply just one of these methods. The combination of the three approaches equals solid, secure API practices.

Tip: In any case, if you decide to secure the APIs yourself instead of asking for help from a professional team, remember this: apps share components accessed through APIs with each other. While this reduces costs and accelerates response, it also exposes private information that results in loss of control over the functioning of the API.

Avoiding performance issues

Developing an internal API monitoring policy is like strategising the creation of any other product. Once we have direct access to the codebase, the same set of instruments that is used to check the health of any application or software can be taken advantage of within the API architecture.

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk



The first thing our team of developers does is locate those areas that appear most problematic in the infrastructure and codebase. The main thing we are looking for is request latency. The longer it takes the software to process database queries, the more negatively your consumers' experience with this API will be affected.

Reduction of the time these procedures demand is often an extremely project-tailored solution, but load-balancing and data-caching greatly decrease the amount of operations a program has to perform over a small period of time.

Tip: Internal API performance is simpler to test than external, especially in the case of an external third-party API. Written by an outside programmer, APIs are like black boxes: queries go in and answers go out with no transparency about what occurs in between. But the same tools can still be used to monitor its conditions.

Software for monitoring

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

These are the programs we usually use when checking the health of your API:

New Relic

This compact and easy-to-use tool helps you to evaluate both the backend and frontend performance of an API. New Relic allows you to monitor all the data in one place and see it in a well-defined context.

Scout

A powerful and convenient tool for monitoring Ruby, Python and Elixir-based components, Scout can check database queries, identify information leaks and reduce guesswork for you or your programmers.

Sumo Logic

The cloud solution control platform Sumo Logic deals with log management and time series metrics. With it, you'll be able to use a bunch of professional tools to monitor and troubleshoot the infrastructure of your APIs.

Where to get your cloud computing solution

If you are ready to take the safety of your company to a new level and need a bespoke cloud solution, contact the Magora development team.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk