# The Choice Between Self-Hosting & Outsourcing

## A Guideline for Companies

MATESO
PASSWORD SAFE

**Is cloud computing the future?**

If you ask IT security experts, they have mixed opinions. On the one hand, there are supporters of the „all-cloud strategy“. For them, a hybrid cloud only means a transitional model before their privatelyowned data centres become obsolete. On the other hand, some also view the outsourced operating processes as rather critical. For them, only self-hosting will survive on the market as a long-term compromise solution. But what do companies want? They would like to have both: the flexibility of a cloud solution and the secure feeling of having their data in their control. But is that possible?

**Every company is a software company. It’s no longer just about procuring one solution and deploying one.**

Watts S. Humphrey / Software-Pionieer

As the so-called father of software quality, Watts Humphrey, already found out 20 years ago: „Every company is a software company. (...) It’s no longer just about procuring one solution and deploying one. It’s not about one simple software solution. It’s really you yourself thinking of your own future as a digital company.”

**This white paper, therefore, serves to provide important food for thought to become clearer about the requirements for your business. It weighs up the pros and cons of self-hosted, cloud and MSP models, providing an overview of the benefits and potential risks and also with the use of professional IT security solutions such as Password Safe.**

## Cloud Services

With cloud services, machines, services, and applications can be provided and accessed online. When using the public cloud, the provider supplies at least one platform, which is also managed by the latter. What keeps IT decision-makers from moving to the cloud? Often it concerns compliance and data security. After all, the cloud may also mean that private and sensitive information is outsourced to the cloud provider. Yet, there is sensitive corporate data that doesn‘t necessarily belong in the hands of external providers. Moreover, each state handles access rights to data differently based on its data protection laws and regulations. Customers must be aware that, depending on the location of the cloud provider and the servers, their data is subject to the jurisdiction of that country.

In addition, each provider can set up its own terms of use and data protection regulations, which the German Federal Office for Information Security (BSI) warns against. Therefore, the selection of the cloud provider is crucial if one ultimately decides to hand over data sovereignty to external parties. However, if companies have already invested in their infrastructure, it is worth checking whether cloud services could be a suitable addition.

# Advantages at a Glance

- quick and easy to implement
- manageable costs
- no personal responsibility for updates and security

## Software as a Service

When applications are combined with cloud services, Software as a Service (SaaS) comes into play. It is intended for companies to use the application‘s location independently via the cloud using a browser or API. The provider takes over the maintenance of the software. In this way, they offer an agile and, above all, inexpensive usage model in which the customer buys and pays for exactly what he needs.

However, even with SaaS providers, it is often not clear exactly how the data is processed. This is because it is located on the provider‘s server, which can be critical in EU GDPR. And the larger the provider, the greater the risk of an attack by third parties to tap sensitive data. If there is also a technical problem with the SaaS provider, this can have an impact on the customer‘s entire system and also make it difficult or impossible to access their own data. And what if the provider shuts down its service completely? In this case, no one would know what happens to the data stored. In addition, SaaS applications are often used in an uncontrolled manner, increasing the risk of shadow IT.

# Self-Hosted Solutions

Self-hosting means that the customer installs, operates and accesses the software locally or in the cloud. In addition, technical knowledge and human resources are required internally to manage self-hosted applications. The big advantage here is that they retain complete control of the data as it is not placed in external hands. Critical infrastructures such as financial service providers, federal agencies, and telecommunications providers significantly benefit from this, as they may be required by law to store data in a private, secure environment. Compared to SaaS solutions, self-hosting also offers better performance because resources cannot be impacted by bandwidth constraints – especially beneficial for companies with remote locations in multiple countries.

**Password Safe is available as a self-hosted solution and can be operated either on-premises, hosted (i.e. in the data centre), and in the cloud. Password Safe offers a desktop as well as a web version. The stateless multi-tier architecture means that data is only stored on the database. Password Safe is globally deployable and available as a self-hosted solution and can be scaled as needed.**

# Advantages at a Glance

- full data control and security
- support from the manufacturer
- better, flexible scalability
- regulatory compliance
- cost control and assured performance
- operation adapted to the use case – e.g. extended fail-safety

**What does on-premises mean?**

The vendor provides the customer with its software, which is then installed and operated on the customer‘s own hardware, behind its own firewall, in its own data center. The vendor is responsible for providing the software upgrades, and can also provide support for the software installation, while the customer takes care of the operation of the software.

## Hybrid Cloud as the Connection of Two Worlds

Even though many companies move their data entirely to the public cloud, for some, it may be more beneficial to migrate only part of the applications – for compliance or data sovereignty, for example. In this case, a hybrid cloud model that combines the option of a public cloud with the company's own on-site IT infrastructure is a good choice. Especially for companies that have already invested in their own infrastructure, trained personnel and their own applications, the hybrid cloud is well suited. Existing resources can be used and supplemented with external services, or processes can be outsourced. And investments in traditional IT will not be as high in the future.

**The hybrid cloud model allows companies to control where data sovereignty is to be retained. This is also possible with a principled self-hosted solution such as Password Safe if companies do not have their own suitable IT infrastructure for hosting.**

The key advantage of this model is that, unlike virtually all SaaS providers, customers can use self-hosted solutions without any hardware or combine the hardware with cloud resources for maximum performance. This means that companies – when operating in the cloud – can select appropriate hosting service providers whose IT infrastructure is located in Germany, for example, and the protection of their own data is guaranteed. Thus, with a domestic location, the public cloud solution offers GDPR-compliant data protection, just like the company's own data centre in its doorstep.

## Tips for Implementation

But even a hybrid solution can be tricky to implement. Database hosting requires particular care. Because with the hybrid solution, companies can host the data in the cloud, in the data centre, or in both locations. Since inbound traffic is generally free, it makes sense to send the data from the data centre to the cloud. Databases can be run in the public cloud and smaller ones in parallel in both environments. Running larger systems in the cloud, in particular, can lead to high costs if the data is again to be processed on-premises.

Compared to on-premises environments, in the cloud, all machines can be customized, which can be dangerous in meeting all requirements. It is therefore essential for companies to find out in advance what the requirements are and what potential challenges need to be overcome. In the case of Password Safe, the following requirements apply:

- machines with Microsoft Server operating system for the SQL server with the corresponding system requirements.
- machines with Microsoft Server operating system for the application server with the corresponding system requirements.
- Both machines require a license for the operating system. The SQL server also requires an MSSQL license.

# Advantages at a Glance

- with standardized and open solutions, applications and data can also be moved to other systems if required
- not dependent on one provider
- various hosting options:
  - in the cloud
  - in-house
  - at both locations

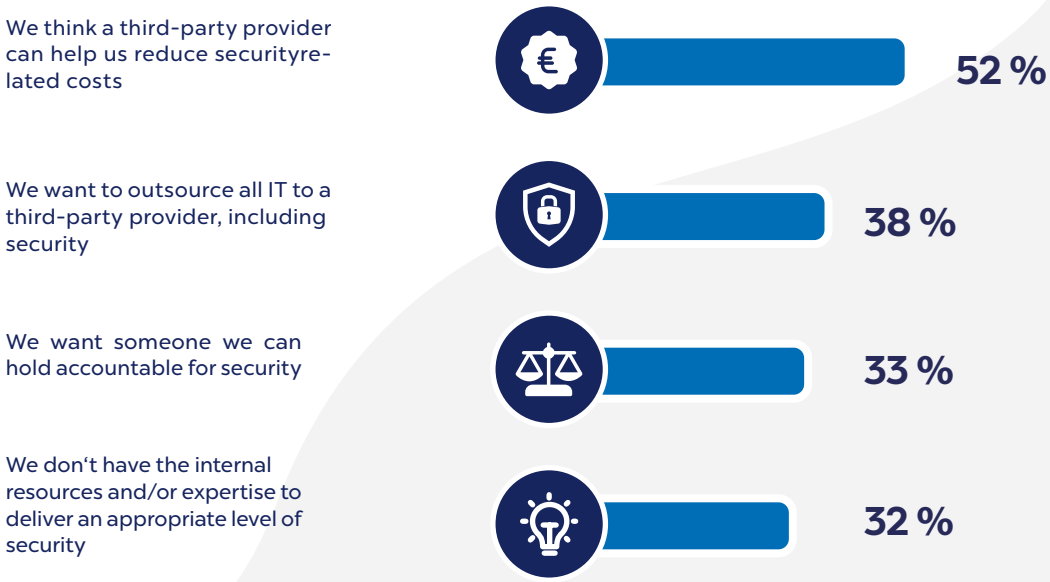
## Managed Services

Managed services, in particular, are now on the rise, enabling smaller and medium-sized companies to offer applications that were previously reserved for large companies and corporations. When conventional IT is considered – the classic provision of dedicated or virtual servers in the company's own infrastructure – self-hosting usually means higher investments for the company itself, which smaller companies find difficult to implement. This requires enormous expertise and experience in IT solutions, from the network to the server architecture, storage and security of solutions. In addition, there are factors such as time and personnel to manage services in-house.

## Why Companies Choose Managed Services

According to a study by Kaspersky, every second company wants to use an MSP primarily to reduce security-related costs. Only around 32% can continue to do business through an MSP due to a lack of expertise and resources. Most strikingly, 74% said that cybersecurity was key when choosing their MSP.

**Reasons for planning to outsource IT security management to an MSP**




Source: Kaspersky MSP Report 2019

If, on the other hand, a company decides to outsource services to a managed service provider, it can also draw on the entire expertise of the MSP. Especially when a server would not be used to 100% capacity and would still have to be paid for in full, companies tend to take a service-based approach instead of a product-based approach to keep their costs as low as possible. The managed service solution is ready for immediate use, and the customer only pays for what is needed and used. When a service is no longer needed, it can be deactivated immediately by the managed service provider. This makes small companies more competitive, as they can react more quickly to new situations and adjust their requirements. In this way, outsourcing processes is also a decision for the company when it has realized that it can no longer handle the effort alone.

**Password Safe is also available as a managed service to offer all companies the right password security solution individually. The Managed Service Providers are extensively trained and certified service suppliers by the manufacturer MATESO itself, who have been chosen by their high level of expertise in the IT security sector. The servers are securely hosted in the DACH region.**

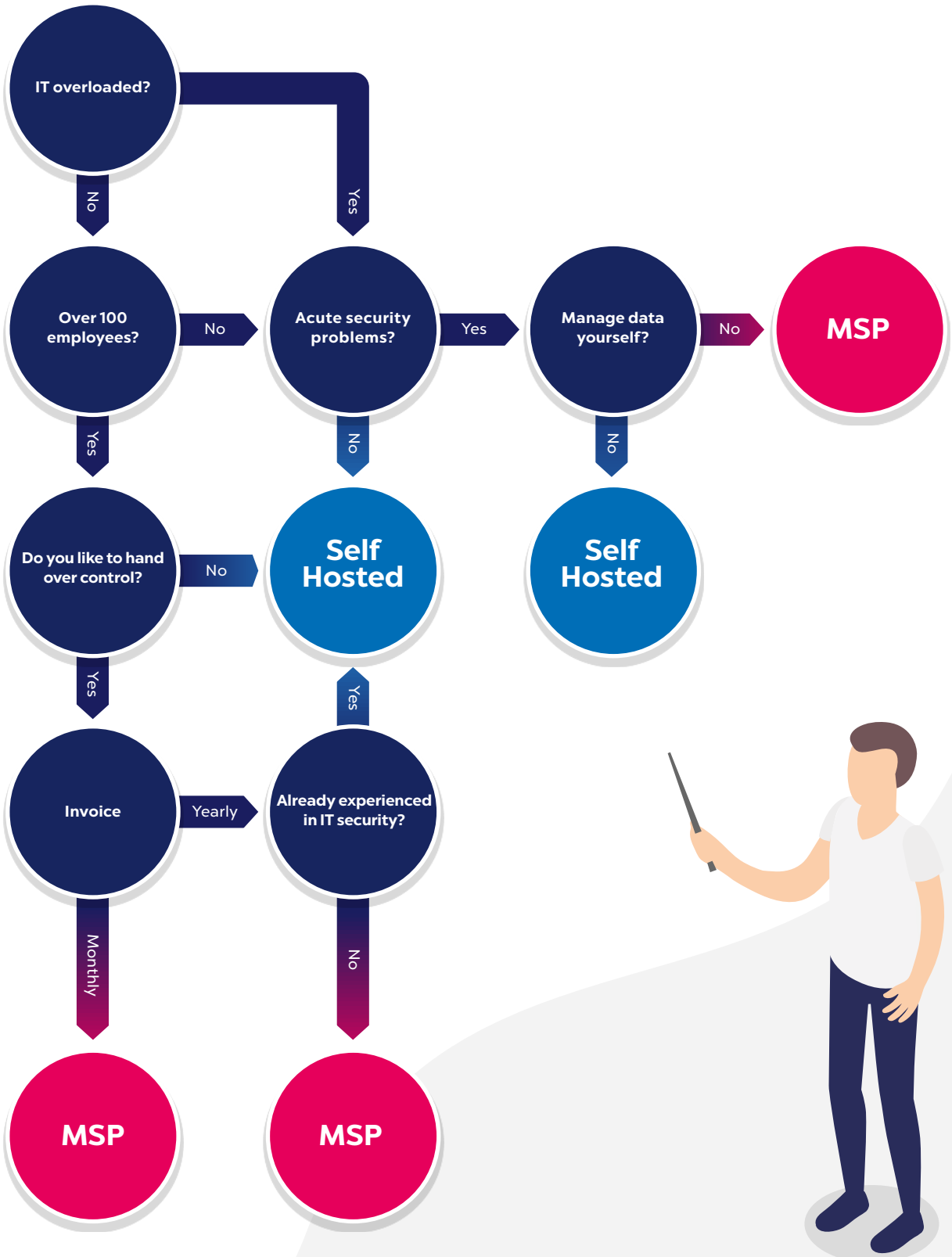
**More information about Password Safe MSP**

## Advantages at a Glance

- data sovereignty with certified partners in the DACH region
- great expertise and experience through personal contact person and consultant
- standardised and personalised possible
- saves investments and capacities in line with costs
- available everywhere
- no more own server effort and responsibility
- simply request new functions from the partner without having to carry out updates yourself
- no more need to worry about backups

# Decision Aid MSP / Self-Hosted

Not sure if you should self-host or use an MSP? Use our decision-making tool for an initial assessment.



## Conclusion

To react more flexibly to new market requirements and customer wishes, many companies are already using public cloud solutions for their workloads. The acceptance of cloud infrastructures in this respect is continuously increasing. However, it may be more costeffective for a company to keep applications with specific dependencies on-premises and migrate only part of the services to the cloud. Therefore, it needs to be assessed on a case-by-case basis whether certain workloads need to be managed internally for compliance and data sovereignty reasons. If this is the case, a hybrid cloud model is recommended.

**For all advantages and disadvantages, companies should ask themselves one crucial question: „do I like hosting yourself or do I find it more of a nuisance?“ After all, with all the pros and cons of price, time and security factors, the bottom line is that the decision is one of „will“. It can only be made on an individual basis and may already have become superfluous as a result of the above question. One thing is certain – professional systems should be able to adapt to these individual decisions with or against the cloud and offer the right solution in every case.**

## MATESO

MATESO is a leading German IT company, which has successfully established in the DACH region since the company was founded in 2006. The developed password security solution Password Safe is distributed internationally by its worldwide partner network. Well-known references testify to the technological and know-how advantage of the IT software.

Today the constantly growing enterprise registers over 10,000 corporate customers with several million users worldwide - including 21 Dax 30 companies.

## PASSWORD SAFE

**Pioneer in Enterprise Password Management**

Password Safe serves companies as a central digital safe for securing, managing and monitoring sensitive data such as passwords, documents and secrets.

**MATESO GmbH**
Daimlerstraße 15, D-86356 Neusäß
**Web:** www.passwordsafe.com
**E-mail:** sales@passwordsafe.de
**Tel:** +49 821 74 77 87-0

MATESO
PASSWORD SAFE