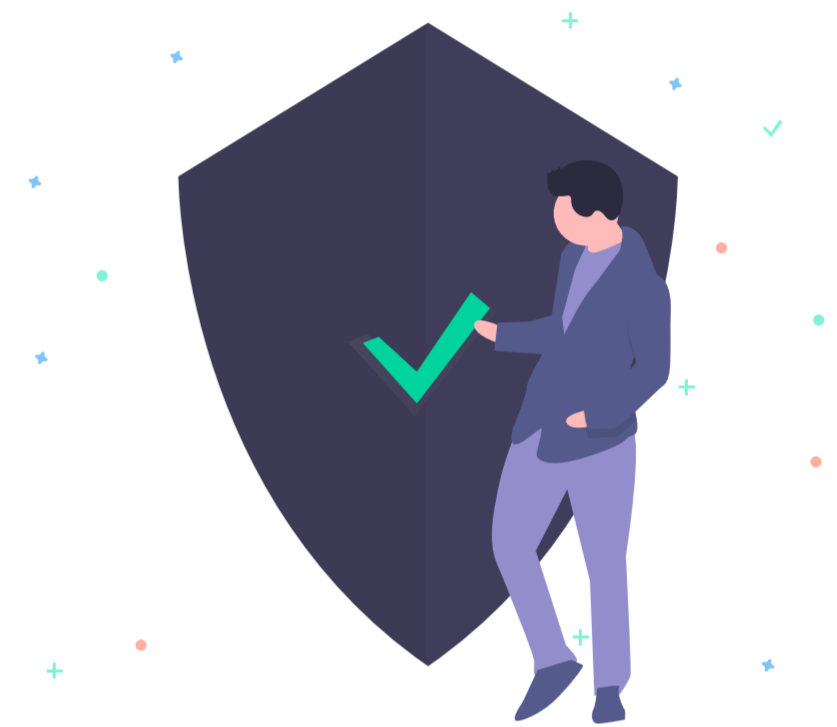# Data Platform Security Check

Cloud Security Care

More and more organizations are switching to the Microsoft Azure cloud to realize their modern data platform. With excellent reasons: it is easy to use, scalable and cost-efficient. Yet another essential theme plays a role in the transition to Azure: security.

Data Platform Security Check

Motion10 clearly states that Microsoft provides a secure infrastructure for your cloud environment, including your data platform. However, correctly configuring the platform and associated services is your responsibility. The same applies to taking specific security measures and maintaining access control for users and applications. Unfortunately, many organizations are insufficiently aware of this, which means that too little attention is paid to securing their data platform as a whole. As a result, they run unnecessary risks, such as unwanted access to the platform, data leaks and non-compliance with GDPR legislation.

The most common security challenges that we encounter in practice are:

- *Granting access from all Azure services to SQL DB*
- *Providing access for external consultants and own employees to the entire resource group*
- *Establishing Data Factory connection tot a database with hardcoded usernames and passwords*
- *Failture to comply with GDPR rules*
- *Not withdrawing rights after the departure of an employee or consultant*
- *Infrequent or non-automatic regeneration of Azure Storage Access Key*
- *Granting too many rights and not or hardly granting limited or temporary rights (least privilege)*

Based on various studies, Microsoft guidelines and its own practical experience, Motion10 has drawn up a list with more than 100 checks and best practices for a secure data platform: the Data Platform Security Check. The Data Platform Security Check is constantly kept up-to-date and expanded and is made up of a security maturity model for ten essential sub-areas within a modern data platform:

1. *Data Bricks*
2. *Key vault*
3. *SQL DB*
4. *Network*
5. *Firewall*
6. *General*
7. *Blob Storage*
8. *Resource groups*
9. *Data Factory*
10. *Power BI*

Based on a targeted assessment of the areas that apply to your organization, we assess where your organization stands in terms of the security of your cloud data platform. After completing the Data Platform Security Check, you will have a concrete step-by-step plan with improvement initiatives for achieving a secure modern data platform in Azure.

From intake to insights in just two weeks

Workshop
- Workshop with IT, admin and management
- Coordinate and arrange access to the data platform

Assessment
- Going through checklist on relevant sub-areas
- Scoring security (overall and subareas) and elaborating the advice

Advice
- Final presentation with results in 10 sub-areas
- Roadmap improvement initiatives with time estimation

Want to know more or get started right away?

Would you like to know more about what the Data Patform Security Check can deliver to your organization? Please contact Jorgo de Muinck, Solution Lead Data & Analytics, via +316 27 32 29 92 or jorgo.demuinck@motion10.com or contact your Motion10 Account Manager.