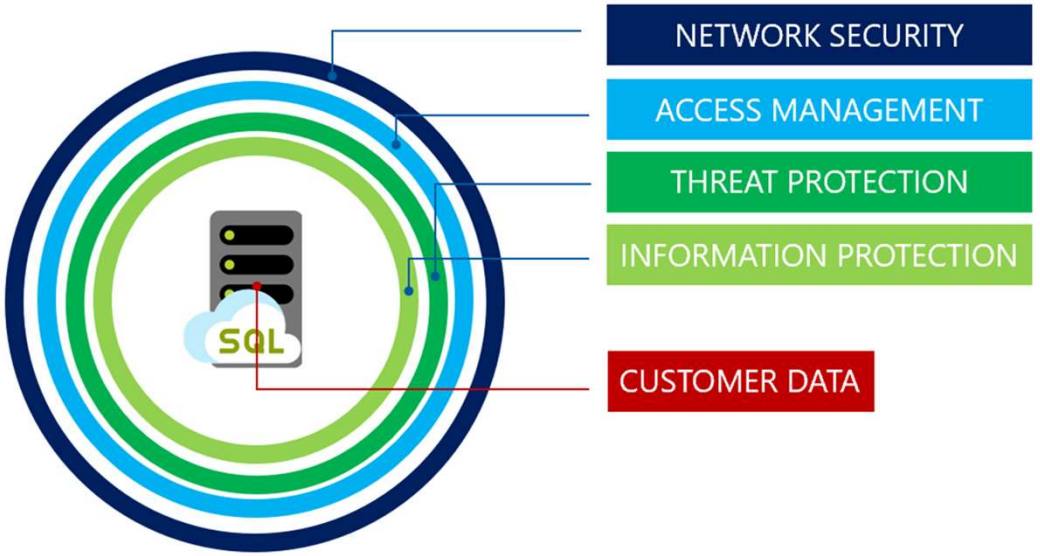
Defender for SQL as part of your Defense in-depth strategy

What

- … is Defense in Depth
- … is the role of Defender for SQL
- … is required to run Defender for SQL
- … is a typical implementation
- … evidence is there
- … questions do you have
- … about me

Defense in Depth



https://rob-litjens.nl


Microsoft Defender
Advanced Threat Protection
Threat & vulnerability management
Attack surface reduction
Next Generation Antivirus
Endpoint detection & response
Auto investigation & remediation
Microsoft Threat Experts
Management & APIs
DATA SATURDAY OSLO 2023

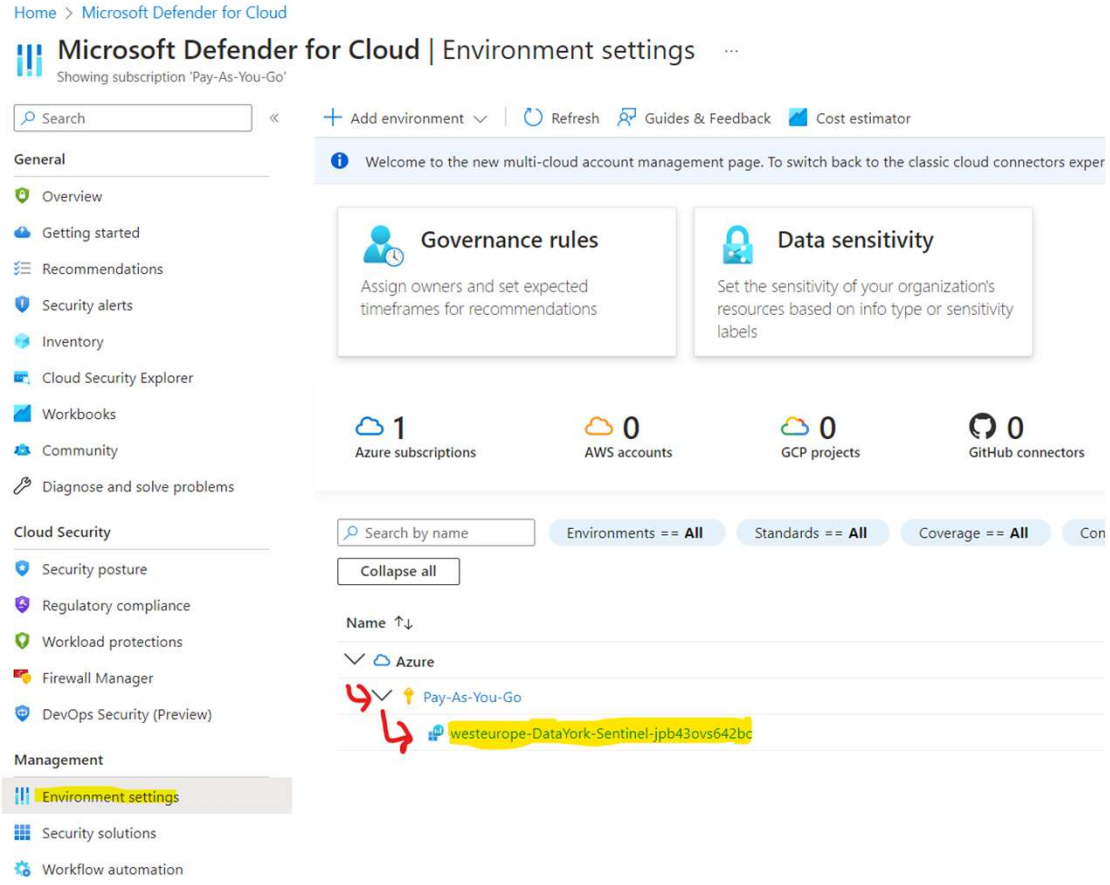
Requirements to use Defender for SQL

- Azure Tenant
  - Some Bicep knowledge
- SQL Servers
  - On premise
    - Endpoint Protection
  - Cloud
- Not supported:
  - SQL2012 and below
  - Reporting Services, Analysis Services

https://rob-litjens.nl

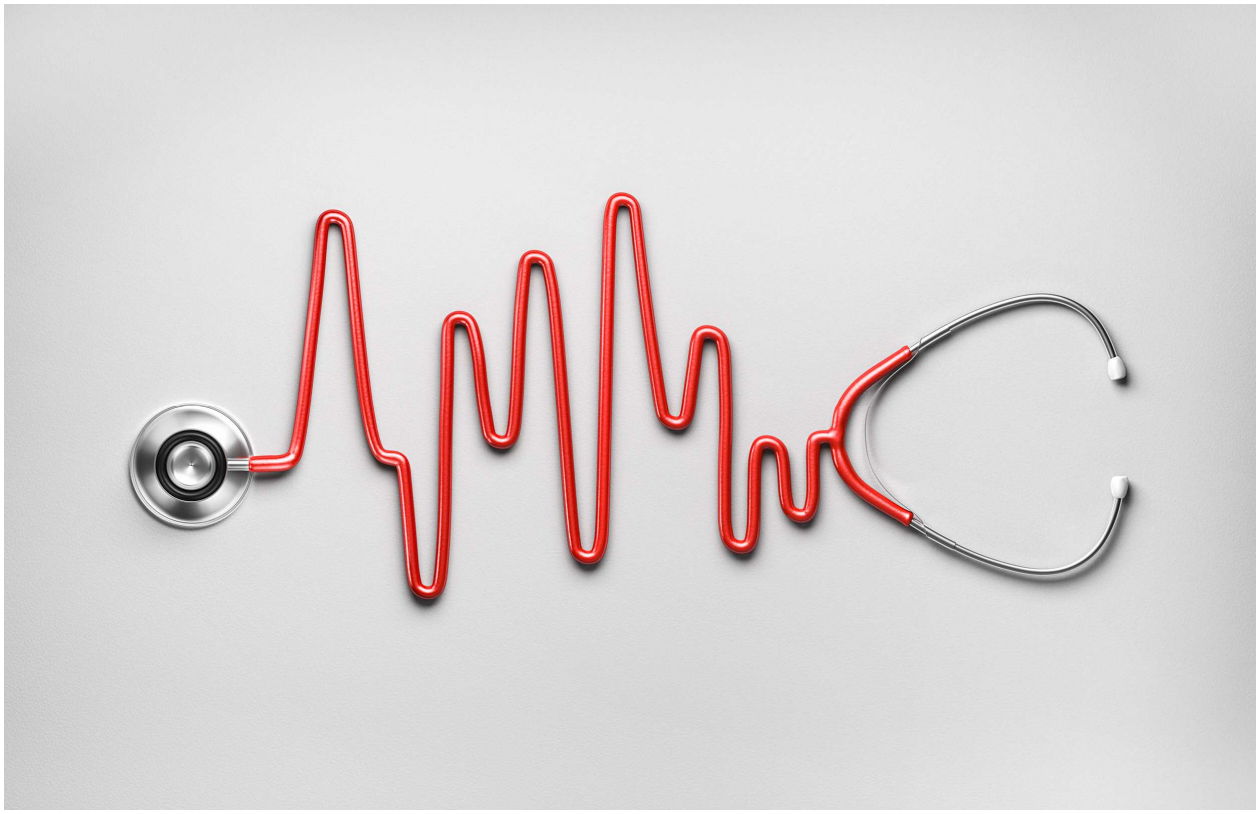
The implementation

- Connect to your tenant
- Implement:
  - A subscription
  - Resource Group
  - A Log Analytics Workspace
- Configure Workspace
- Configure Client



https://rob-litjens.nl

Demo Implementation



https://rob-litjens.nl

Done so far

Setup Azure

Setup Log Analytics Workspace

Setup Client

But…

We need proof it is working

Evidence

https://rob-litjens.nl

Questions

Defender for SQL as part of your Deense in Depth strategy

https://rob-litjens.nl

About me

Rob Litjens

SQL Server Automation Engineer at Financial Institute

Working with SQL since ages (version 6.0), automating since then. Interested in Data Protection and Security, audits and auditing.

Personal interests: Mountainbiking, traveling and work (not always on ☺)

@Socials

LinkedIn:	https://www.linkedin.com/in/litjensr/
Bsky:	roblitjens.bsky.social
Mastodon:	https://dataplatform.social/@RobLitjens
Blog:	https://www.rob-litjens.nl