Microsoft

Microsoft Future Decoded

31st October & 1st November 2017
ExCeL London

Microsoft

Microsoft SQL – What you need to know for Privacy, Compliance and GDPR *1

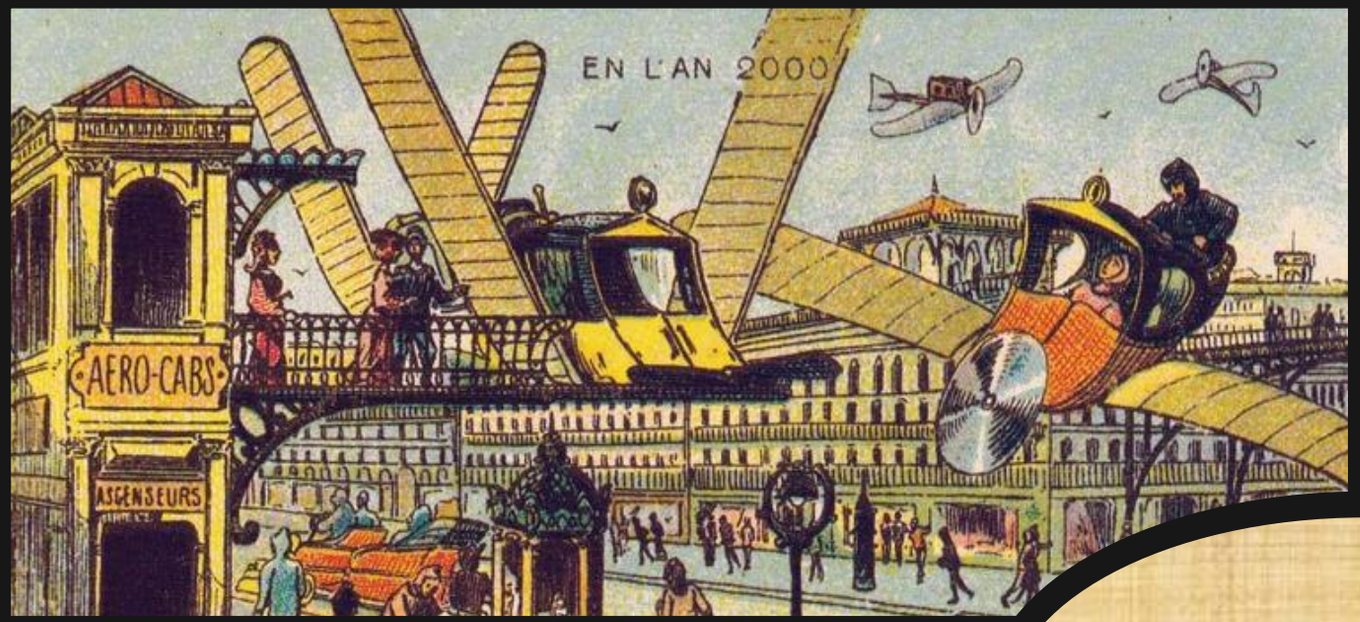
Mark Broadbent

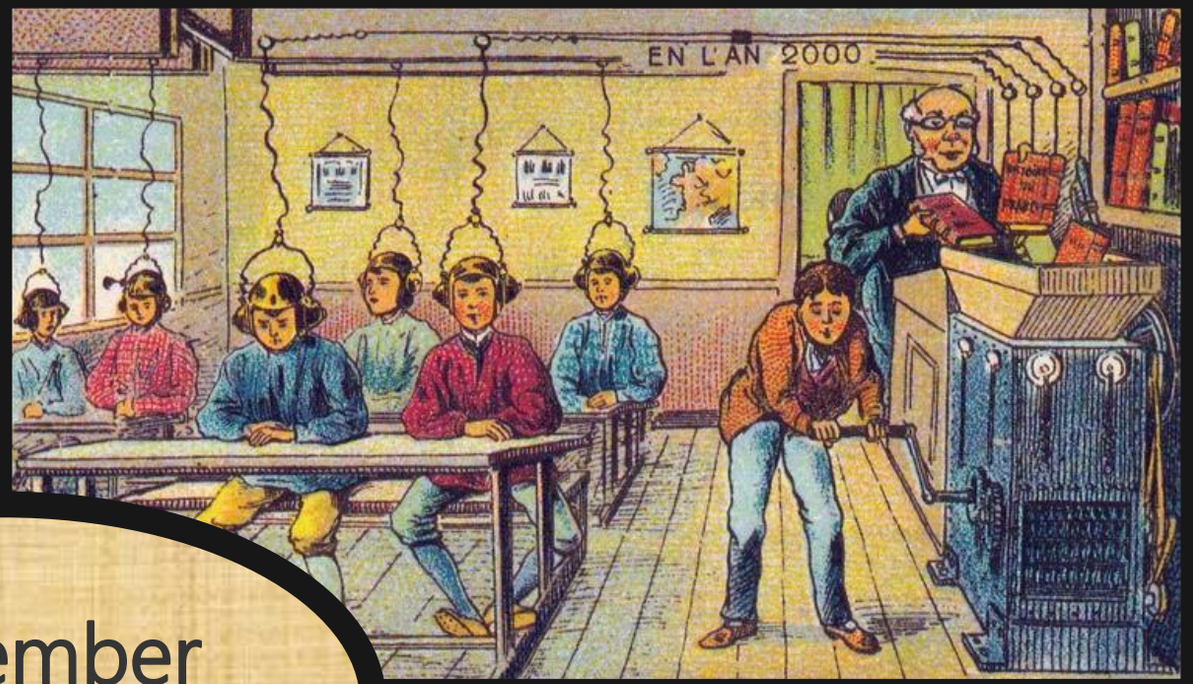
Microsoft Certified Master (MCM) and Data Platform MVP

*1 Special mention to Ronit Reger - "Prepare for the GDPR and data privacy compliance with Microsoft SQL technologies", Microsoft Ignite 2017, BRK3130

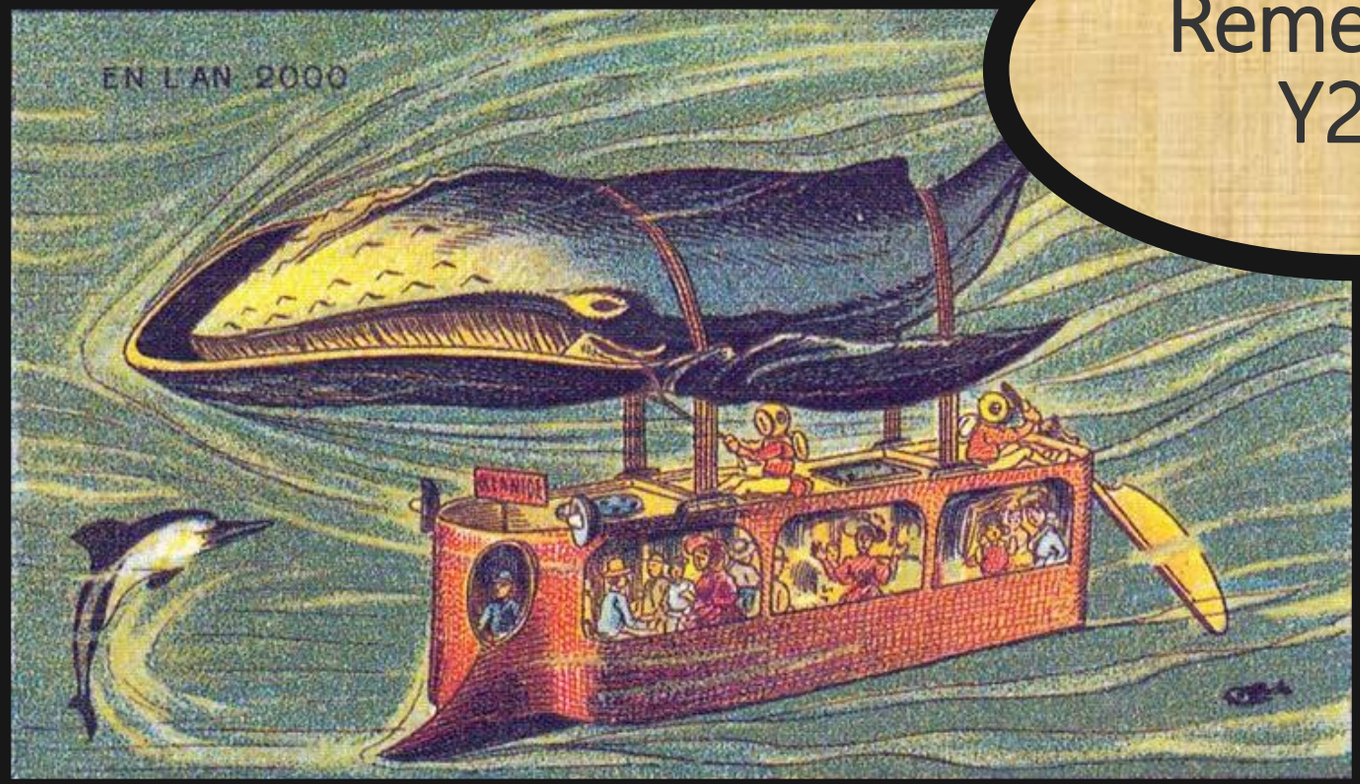
Session goals

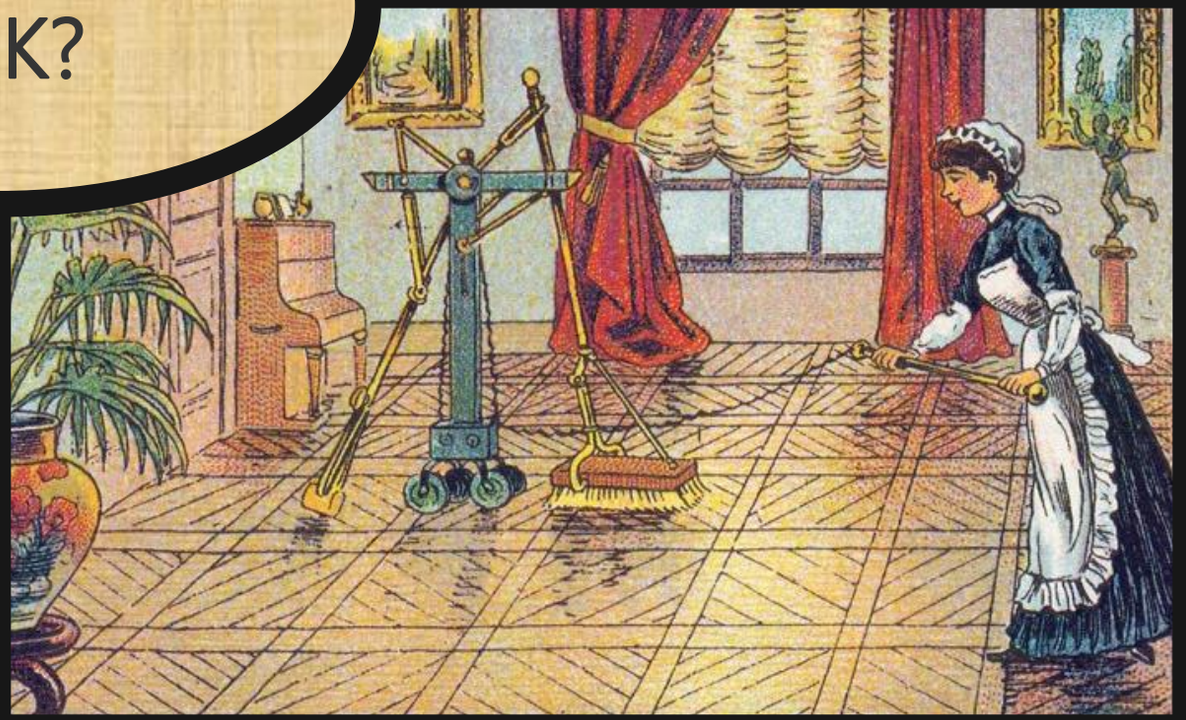
1. Introducing the General Data Protection Regulations
   - What is it?
   - What does it mean for you?
   - Breaking it down into some clear requirements
   - Proposing a step-by-step process
2. How Microsoft SQL technologies can help
   - Making use of built-in capabilities to meet the requirements
   - Introducing the newest innovations that can help!
   - Sneak peak at new and imminent developments…





Remember
Y2K?





Data Privacy in today's world

- **Oct 2017** – USB stick found containing 174 documents disclosing Queen's route and security measures to airport, all IDs needed, timetable of patrols, CCTV maps and much more!
- **Sept 2017** – Equifax announces one of largest corporate data breaches in history after hackers obtained (143 million records)!
- **Sept 2017** - Nottinghamshire County Council fined £70,000 for leaving elderly and disabled people's personal data publicly available online for 5 years!
- **Aug 2017** – Online spambot 711 million record dump located

August: 715 million records breached
September: 174 million records breached
October: 55 million records breached

Source: https://www.itgovernance.co.uk/blog/category/other-blogs/breaches-hacks/

TURBULENT TIMES

2 Billion records compromised in the last year

140+ DAYS between infiltration and detection

$15 MILLION of cost/business impact per breach

GDPR enables rights of data subjects and enforces protection on people's personal data!*1

- Right to object
- Right to access, rectification, erasure and portability
- Requires strict consent (and proof)
- Personal data will be held and transmitted securely

*1 personal data is *anything* that is personally identifiable!

EU Directive 95/46/EC aka “Data Protection Directive (DPD)”

UK Data Protection Act

1984

1995

UK Data Protection Act (2)

1998

EU agree (US) Safe Harbor principles meet level

2010

Organisation for Economic Co-operation and Development (OECD) guidelines on transborder data flows

1980

Work commences on GDPR

2011

1951

Article 8, European Convention on Human Rights

2015

EU invalidate Safe Harbor decision, start talks on EU-US Privacy Shield *1

1945

Post war concerns for Protection of human rights

2016

GDPR adopted

2019

Brexit?

May 2018

GDPR enforceable

GDPR "Players"

European Data Protection Board (EDPB)

Reports to

Elizabeth Denham,
UK Information Commissioner

Information Commissioner's Office (ICO)
(Supervising Authority in UK)

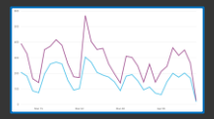
Notifies

BoD

Reports to

Data Protection Officer (DPO)

Directs & DPIA



Data Processor

Data Controller

Compliance

Compliance

Notifies

Third Countries
(countries outside EU)

3rd Parties

Data subject/s

Data privacy-related requirements of the GDPR

GDPR Article 25—Data protection by design and by default

► Control access, Process minimal necessary data, Integrate safeguards

GDPR Article 32—Security of processing

► Pseudonymization and Encryption, Ensure availability, Regular security testing

GDPR Article 33—Notification of a personal data breach

► Detect breach, Assess impact, Actions to take

GDPR Article 30—Records of processing activities

► Monitor access, Maintain audits

GDPR Article 35—Data protection impact assessment

► Document risks and security measures taken

Preparing for GDPR compliance

Questions for leading your preparation:

WHERE does your data reside and who has **ACCESS** to it?

Do you **CONTROL** who can access your data and it's **USE** based on risk assessment in **REAL-TIME**?

Can you **CLASSIFY**, **PROTECT** and apply **POLICY-driven** actions to your data, on devices, between apps, in any location, at rest and in transit?

Can you automatically **DETECT** a data or identity breach? Are you able to **RESPOND** adequately to a breach?

Do you continuously **REVIEW** and **UPDATE** your data protection **POLICIES** and **PRACTICES**?

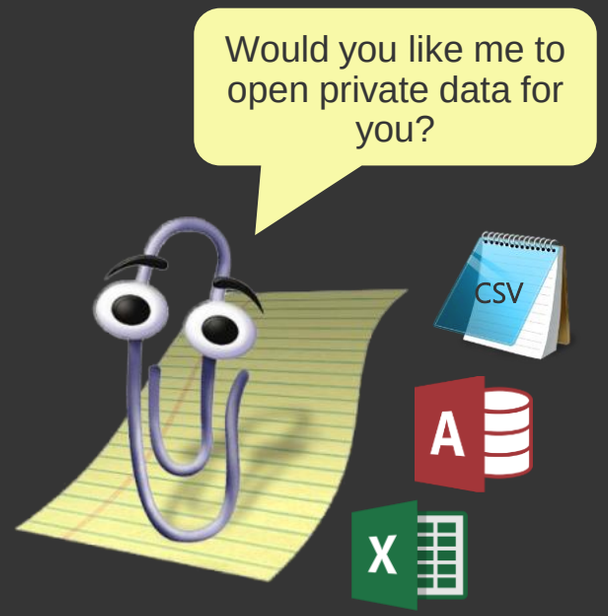
Applicability to the data tier

The database stores much of the organization's sensitive data

Identifying personal data in relational is *fairly* easy

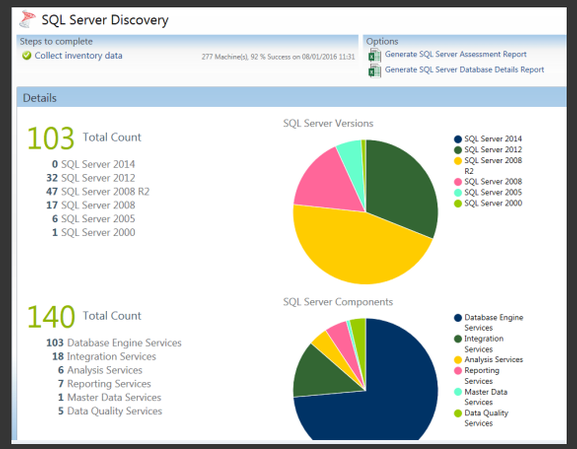
Also consider…

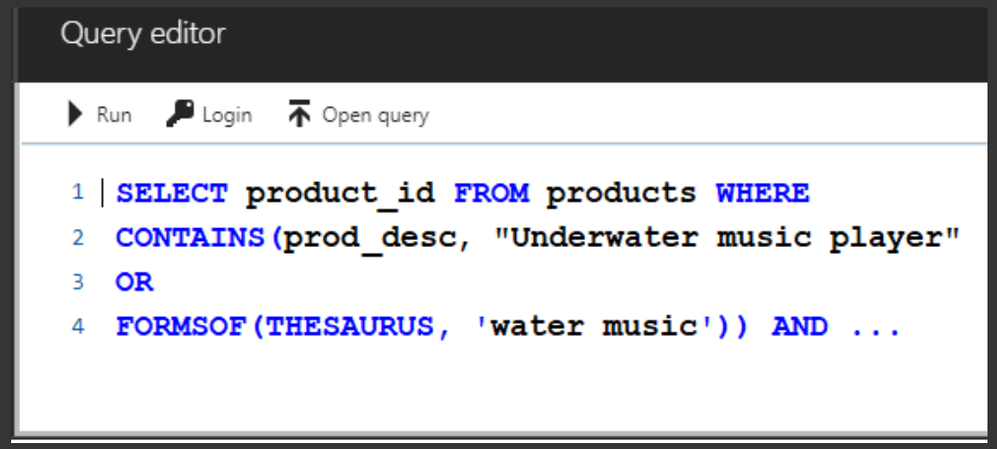
But…

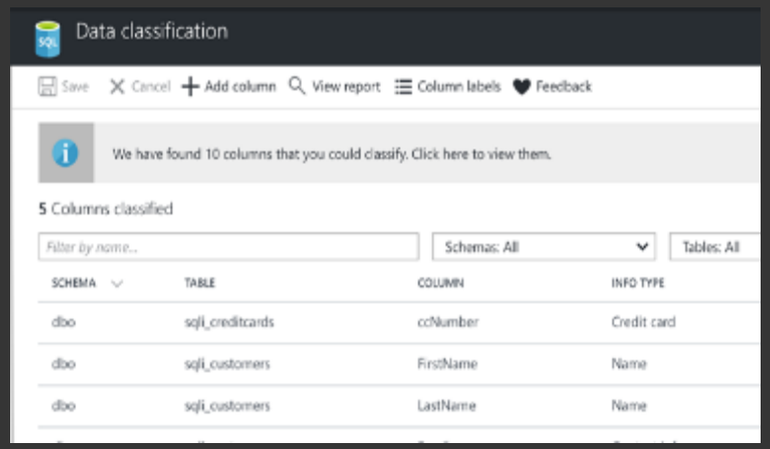


Translated to SQL technologies…

	Process	Technology
1 Discover	Discover database systems	Map Toolkit
	Inventory personal data in database systems	T-SQL Queries, Full Text search
	What is attack surface area & access model?	Vulnerability Assessment new!
	Track data flows and map data lineage	Data classification new!





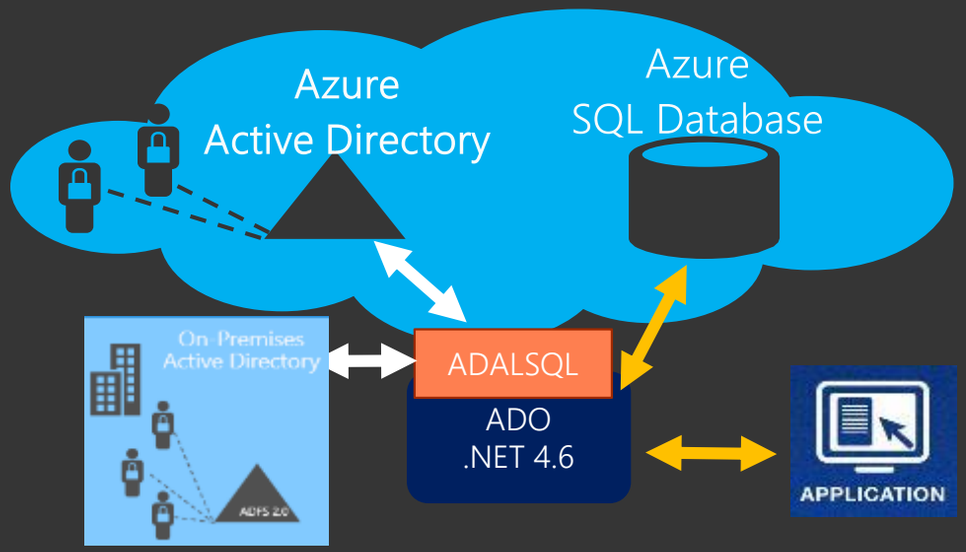


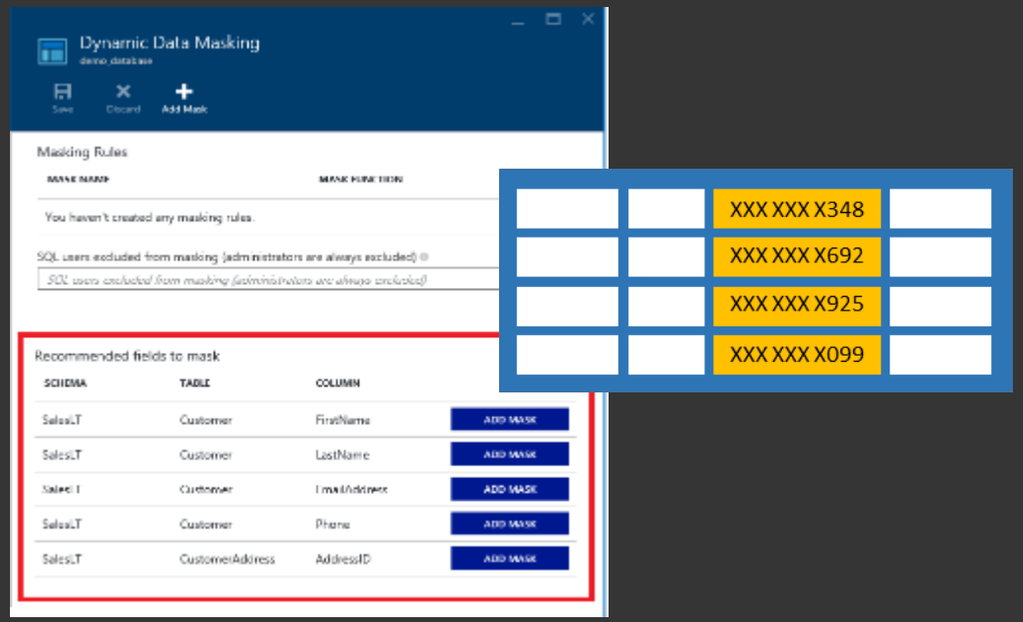
Demo

Resolving Vulnerabilities

Translated to SQL technologies…

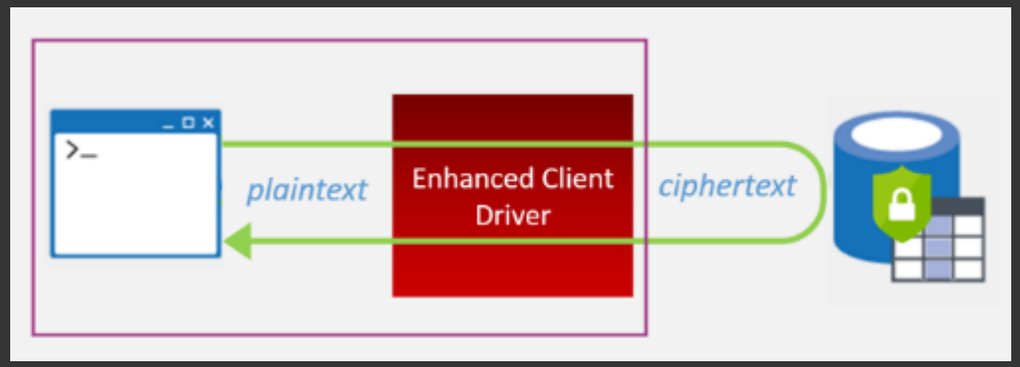
	Process	Technology
2 **Manage**	Manage authentication and authorization mechanisms	Windows authentication, Azure AD auth, role-base security…
	Properly configure database firewall	Azure SQL Firewall
	Limit application access according to authorization principles	Dynamic Data Masking, Row-Level Security

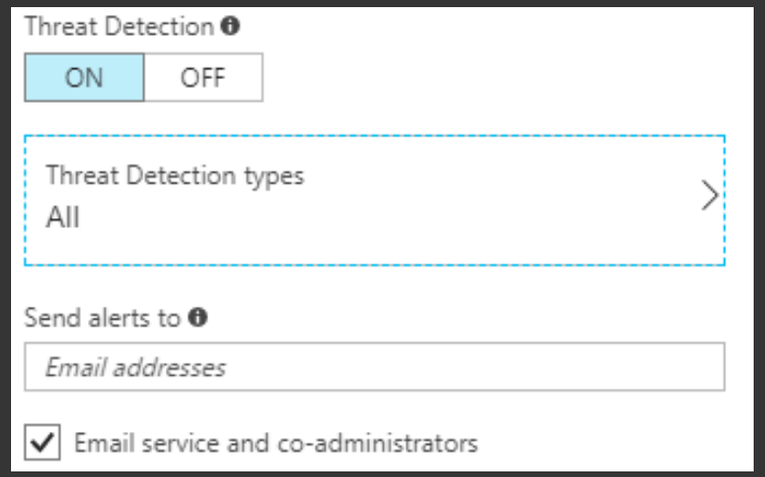




Translated to SQL technologies…

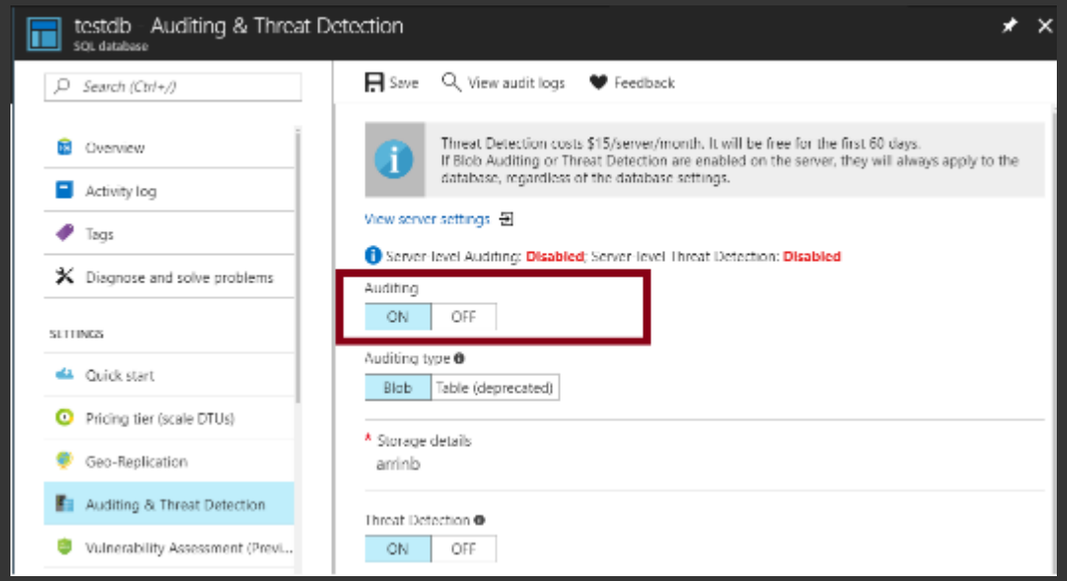
	Process	Technology
3 **Protect**	Encryption of data at rest, in motion, in use	TLS, TDE, Always Encrypted
	Detect data breach and respond accordingly	Threat Detection
	Ensure business continuity	Always On, Active Geo-Replication

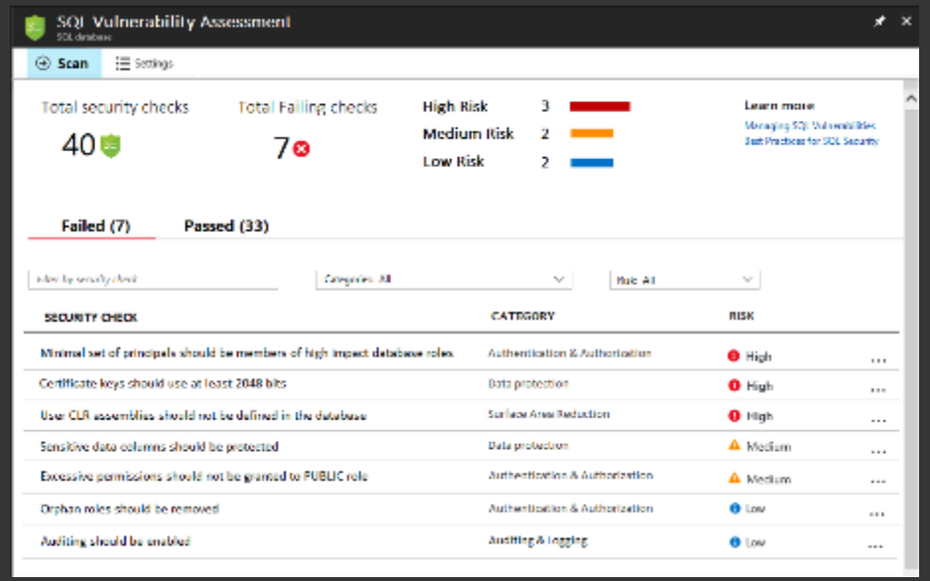




Translated to SQL technologies…

	Process	Technology
4 **Report**	Maintain audit records of database activities	Auditing, Temporal tables
	Continuously assess and analyze security measures	Vulnerability Assessment new!



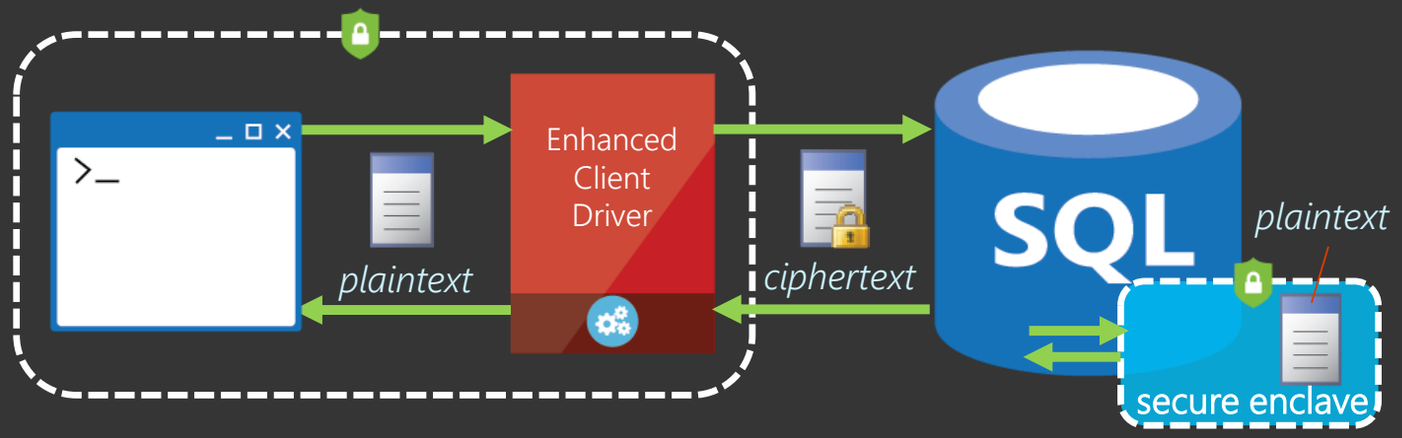


Demo

Auditing Database Activities with SQL Audit and Temporal Tables

Always Encrypted using Secure Enclaves

Early Access Preview



- Confidential computing brings secure enclaves to Azure
  - Trusted execution environments protecting data in use
  - First cloud to offer Intel Software Guard Extensions (SGX) enclaves
- Enhancing Always Encrypted with enclaves
  - Rich computations on encrypted data
  - In-place encryption and key management

Sign up for Early Access Preview at:
https://aka.ms/SQLEnclavesPreview

VNET Service Endpoints

Preview

Restrict access to the database from VMs in a given VNET/subnet

- ✓ Separation of roles between networking and database admin teams
- ✓ Keep data on the Azure network
- ✓ Simplify management of Virtual IPs and Firewall rules (ie. no *"Allow all Azure Services"*)

Roadmap

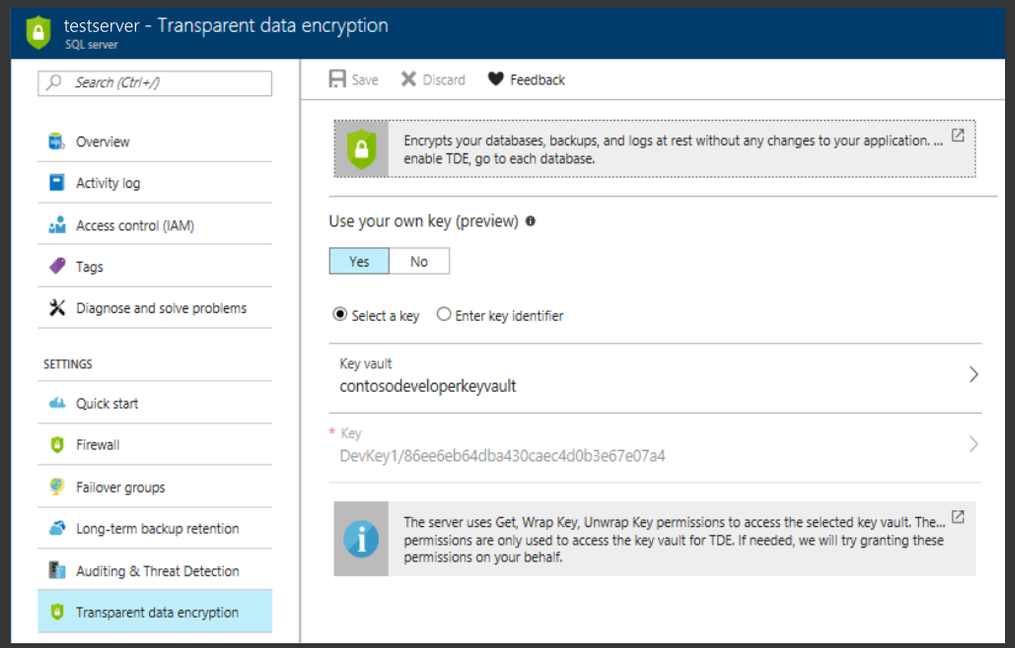
- Remove SQL Database from the public IP
- Removing outbound to SQL Database IP on Network Security Groups
- Configure VPN/ Express Route Private Peering
- Ability to assign private IPs to SQL databases

TDE with Bring Your Own Key support

Preview

Control **who** *has access to keys used for encryption-at-rest and* **when**

- ✓ Simplify key management via Azure Key Vault and centralize application secrets, passwords, and encryption keys on one platform.
- ✓ Leverage Key Vault's scalability, security, and redundancy with built-in hardware security modules (HSMs) and redundant provisioning of vaults across datacenters worldwide.
- ✓ Strengthen trust in the cloud by having control over resources who have access to TDE keys.
- ✓ Help meet compliance requirements by separating data and key management.



SQL VULNERABILITY ASSESSMENT

Preview

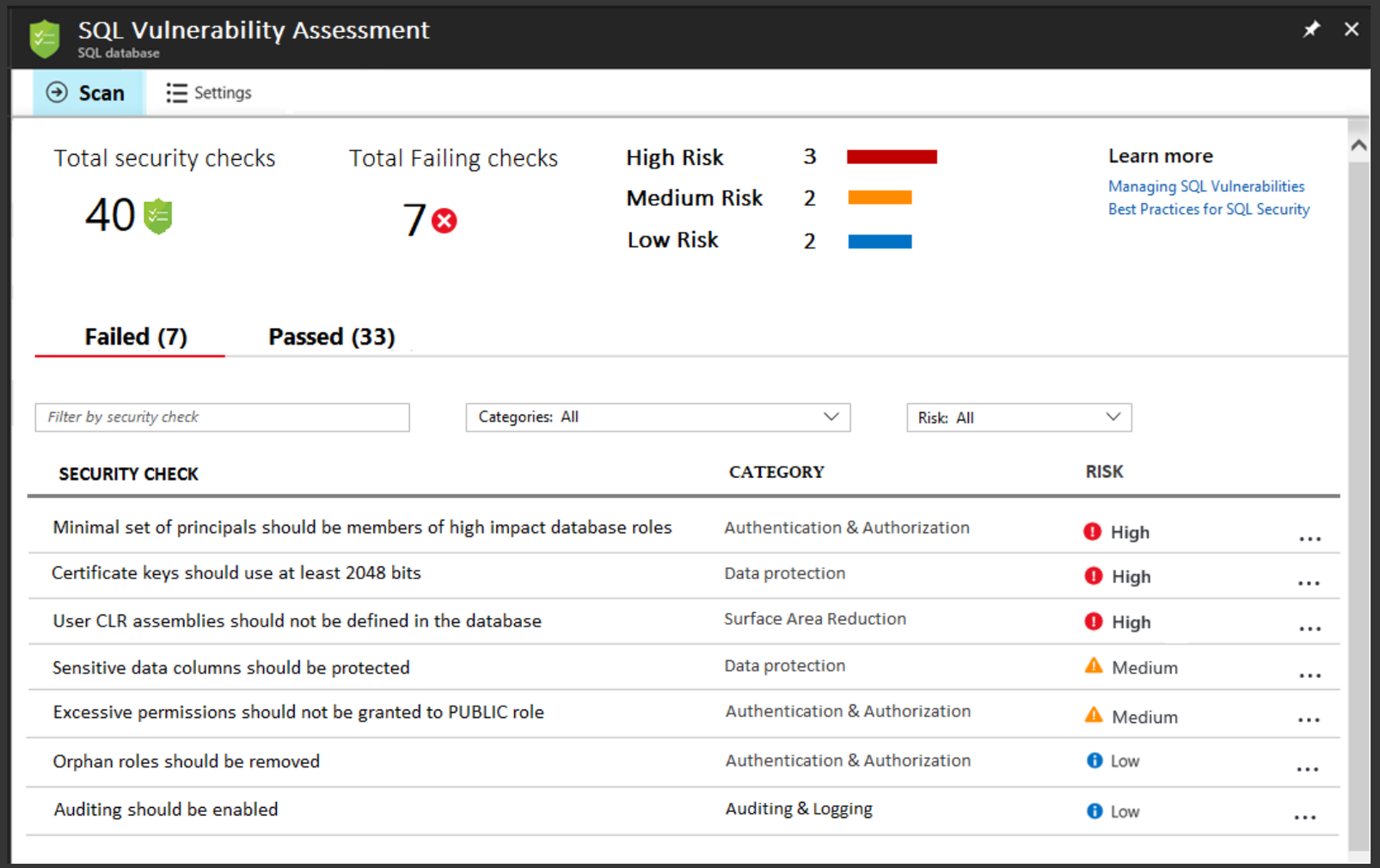
*A one-stop-shop to **track** and **improve** your SQL security state*

Get Visibility
Discover sensitive data and potential security holes

Remediate
Actionable remediation and security hardening steps

Customize
Baseline policy tuned to your environment, so you focus on deviations

Report
Pass internal or external audits, facilitates compliance



Limited Preview

Azure Managed Instances

(Easy migration to Cloud: nearly 100% like SQL Server!)

Data migration

- Native backup/restore
- Log shipping (DMS)

Security

- TDE
- SQL Audit
- Row level security
- Always Encrypted

Programmability

- Global temp tables
- Cross-database queries and transactions
- Linked servers
- CLR modules

Operational

- DMVs & XEvents
- Query Store
- SQL Agent
- DB Mail (external SMTP)

Scenario enablers

- Service Broker
- Change Data Capture
- Transactional Repl

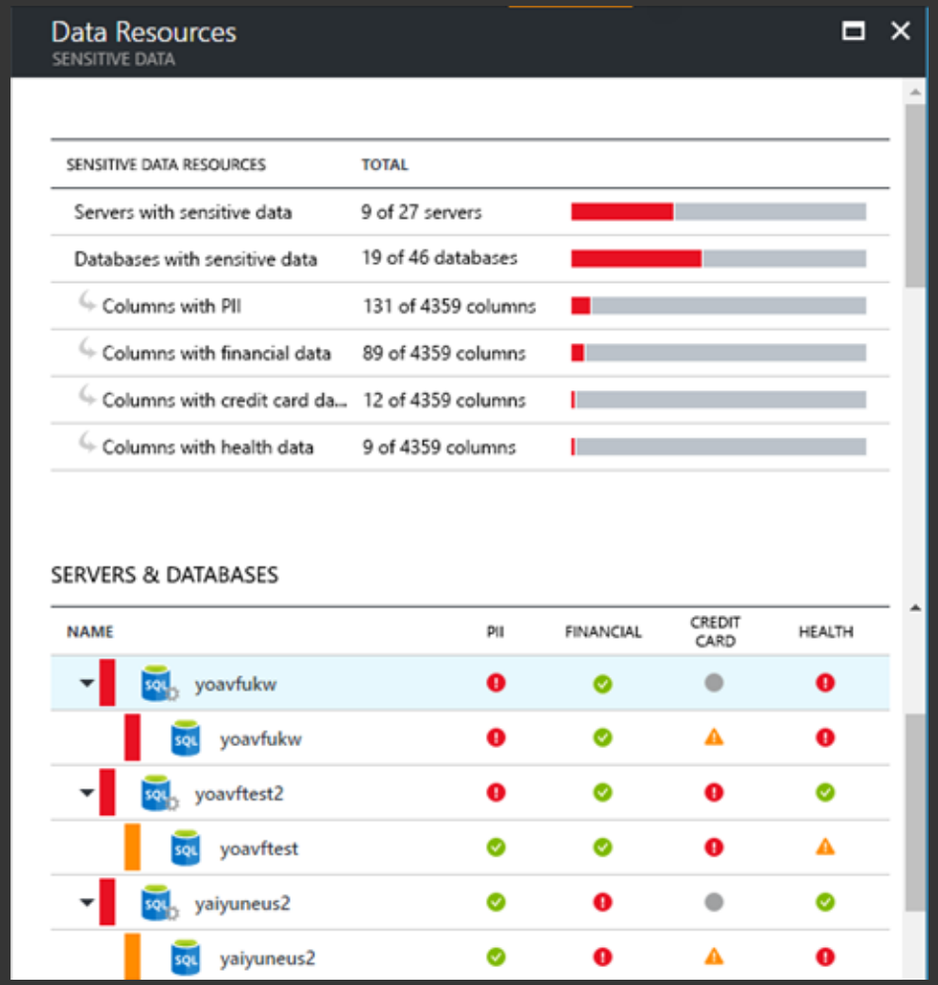
Note: features will be added in stages until General Availability of Managed Instance

SQL Data Classification

Limited Preview

Secure the **data**, not just the database

- ✓ Auto discover sensitive data location in servers, databases and columns
- ✓ Data classification: enrichment of classification logic that obtains historical context
- ✓ Persistent tagging: sensitive data tags that stay with the data as it flows outside the database boundaries



Demo

Comparison with Azure security options

Resources

SQL Security

SQL and GDPR Guide - https://aka.ms/gdprsqlwhitepaper

Azure SQL Database Security Overview | Microsoft Docs

Security Center for SQL Server Database Engine and Azure SQL Database

SQL Server Security Blog - blogs.msdn.microsoft.com/sqlsecurity/

SQL Server Security | Microsoft Docs

GDPR @Microsoft

https://www.microsoft.com/GDPR

https://www.gdprbenchmark.com/

Presentation Materials

https://github.com/retracement/GDPR