SARPEDON QUALITY LAB

SQL Server 2016

Security Obscurity and Encryption

Andreas Wolter
Owner: Sarpedon Quality Lab
Database Architect | MCSM, MCM, MVP

1

SARPEDON QUALITY LAB

Andreas Wolter

PASS Summit 2009 UNITE
PASS SQLRally
PASS SQL saturday
BASTA! .NET, VISUAL STUDIO & MORE
SQLGulf
sqlbits
TechNet Conference
SQLServerGeeks Annual Summit 2015

Consultant, Trainer & Speaker
Microsoft Certified Master SQL Server 2008
+ Solutions Master Data Platform (SQL Server 2012)

- Datawarehouse & OLTP-System Architecture
- Performance Tuning
- Security

SQL SERVER MASTER-CLASS by SARPEDON QUALITY LAB

Email: a.wolter@Sarpedon.de
Web: www.andreas-wolter.com
Blog: www.insidesql.org/blogs/andreaswolter/
Facebook: www.facebook.com/SarpedonQualityLab
LinkedIn: www.linkedin.com/in/andreaswolter
Twitter: @AndreasWolter

Microsoft CERTIFIED Solutions Master Data Platform
Microsoft CERTIFIED Master SQL Server® 2008
SQL Server

Microsoft CERTIFIED IT Professional Business Intelligence Developer 2008
SSAS, SSRS, SSIS

MVP Microsoft® Most Valuable Professional

3

SARPEDON QUALITY LAB

Agenda

- Intro: SQL Server under Attack
- Overview of Investments for 2016
- Application Access
  - Row level Security, Dynamic Data Masking
  - Demo
  - Side-Channel Attacks
- Data Encryption
  - Always Encrypted
  - Demo
  - A word on SQL-Injection
- Q&A

4

SARPEDON QUALITY LAB

SQL Server under Attack

5

Note

SARPEDON QUALITY LAB

- Encryption at rest does not protect against all attacks
- In fact no protection alone protects all attack surfaces or attack vectors

6

SARPEDON QUALITY LAB

Security Landscape

Application Access

- Dynamic Data Masking
- Row-level Security

Proactive Monitoring

- Auditing
- SQL Threat Detection

Database Access

- SQL Authentication
- SQL Permissions
- SQL Firewall (server & database)
- Azure Active Directory Authentication

Data Encryption

- Encryption in flight (TLS 1.2 over TDS)
- Encryption-at-rest (TDE)
- Always Encrypted

Cloud-only

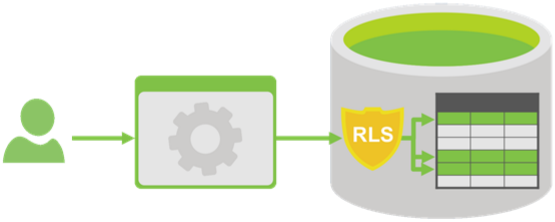
* Featured in this presentation

7

SARPEDON QUALITY LAB

Row Level Security

SQL Server 2016
SQL Database (GA)



- ✓ Fine Grained Access Control
- ✓ Application Transparency
- ✓ Centralized Security Logic

Helps With

- Compliance standards, internal regulations, basic security principles

Scenarios

- Oil & gas exploration, healthcare, multitenant
  - restrict an analyst's access to well production data based on the analyst's region and role
  - restrict a doctor's access to patient data based on the doctor's staffing assignments
  - prevent tenants from accessing data that does not belong to them.

9

SARPEDON QUALITY LAB

How to Implement RLS

dbo.Customers

Col1	Col2	Col3	SalesRepName
			SalesRep1
			SalesRep2
			SalesRep1

```
CREATE FUNCTION dbo.customerPredicate(@SalesRepName AS sysname)
    RETURNS TABLE
    WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS accessResult
    WHERE @SalesRepName = USER_NAME() OR USER_NAME() = 'Manager'
go
```

```
CREATE SECURITY POLICY dbo.customerAccessPolicy
    ADD FILTER PREDICATE dbo.customerPredicate(SalesRepName) ON dbo.Customers,
    ADD BLOCK PREDICATE dbo.customerPredicate(SalesRepName) ON dbo.Customers
go
```

10

RLS Limitations

SARPEDON QUALITY LAB

- Does not protect against ad-hoc access (Side channel attacks are possible)!
- incompatible with Filestream
- incompatible with Polybase
- No indexed views
- Change Data Capture & CT can leak data

11

RLS: Learn More

SARPEDON QUALITY LAB

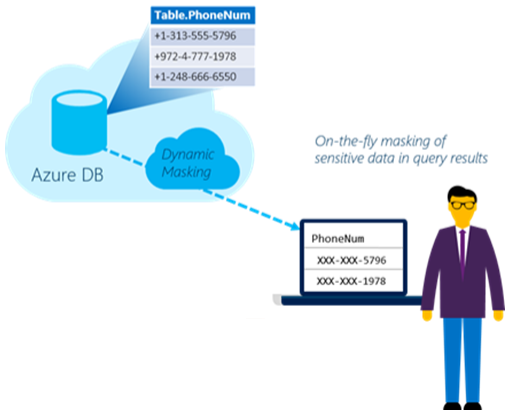
Books Online
https://msdn.microsoft.com/en-us/library/dn765131.aspx
SQL Security Blog (keyword RLS)
http://blogs.msdn.com/b/sqlsecurity/archive/tags/rls/
Overview blog post
http://blogs.technet.com/b/dataplatforminsider/archive/2016/01/21/limiting-access-to-data-using-row-level-security.aspx
Channel 9 Videos
https://channel9.msdn.com/Shows/Data-Exposed/Row-Level-Security-Updates
https:// channel9.msdn.com/Shows/Data-Exposed/Row-Level-Security-in-Azure-SQL-Database
https://channel9.msdn.com/Shows/Data-Exposed/SQL-Server-2016-Row-Level-Security
Code Samples
https://rlssamples.codeplex.com/

12

SARPEDON QUALITY LAB

Dynamic Data Masking

SQL Server 2016
SQL Database (GA)



- ✓ Sensitive Data Protection
- ✓ Agility and Transparency
- ✓ Centralized Security Logic

Helps With

- Compliance standards, internal regulations, basic security principles

Scenarios

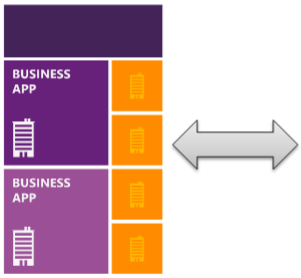
- Public safety, human resources

13

SARPEDON QUALITY LAB

How DDM Works

1) Security officer defines dynamic data masking policy in T-SQL over sensitive data in Employee table
2) App user selects from Employee table
3) Dynamic data masking policy obfuscates the sensitive data in the query results



```
ALTER TABLE [Employee] ALTER COLUMN [SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'Partial(0,"XXX-XX-",2)')

ALTER TABLE [Employee] ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee] ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to admin1
```

Security Officer

```
SELECT [Name],
       [SocialSecurityNumber],
       [Email],
       [Salary]
FROM [Employee]
```

other login

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

admin1 login

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

14

Dynamic Data Masking: Learn More

SARPEDON QUALITY LAB

Getting Started (Azure SQL DB)
https://azure.microsoft.com/documentation/articles/sql-database-dynamic-data-masking-get-started/

MSDN (SQL Server)
https://msdn.microsoft.com/library/mt130841.aspx

Blogs
http://blogs.msdn.com/b/sqlsecurity/archive/2015/10/22/dynamic-data-masking-highlighting-the-latest-improvements.aspx
https://azure.microsoft.com/blog/limit-the-exposure-of-sensitive-data-in-azure-sql-database-using-dynamic-data-masking/

Channel 9 Videos:
https://channel9.msdn.com/Shows/Data-Exposed/Dynamic-Data-Masking-Updates
https://channel9.msdn.com/Shows/Data-Exposed/Dynamic-Data-Masking-in-Azure-SQL-Database

15

Dynamic Data Masking Limitations

SARPEDON QUALITY LAB

- A masking rule cannot be defined for the following column types:
- Computed columns (whether persisted or not)
  - – but will be masked if one of the refered columns is
- Encrypted columns (Always Encrypted)
  - Since SQL Server really does not know the plain data
- Generated always (temporal)
- FILESTREAM
- COLUMN_SET

16

SARPEDON QUALITY LAB

Sample Health Care Application

DDM & RLS

17

SARPEDON QUALITY LAB

Data Encryption Overview

- TDE
  - SQL Server, SQL Database w/ service-managed keys
- Always Encrypted
  - SQL Server 2016, SQL Database (Public Preview)
- Cell-level Encryption*
  - SQL Server, SQL Database
- Azure Key Vault Integration (via SQL Server Connector)
  - SQL Server, SQL-in-a-VM

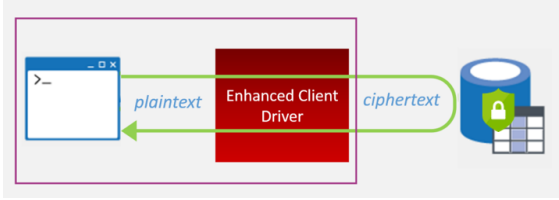
* For compatibility between on premise and Azure

18

SARPEDON QUALITY LAB

Always Encrypted

SQL Server 2016
SQL Database (GA)



- ✓ Prevents Data Disclosure
- ✓ Application Transparency
- ✓ Queries against Encrypted Data

Helps With

- Protection from high-privileged, yet unauthorized users
- Compliance

Scenarios

- Health, finance, insurance

19

SARPEDON QUALITY LAB

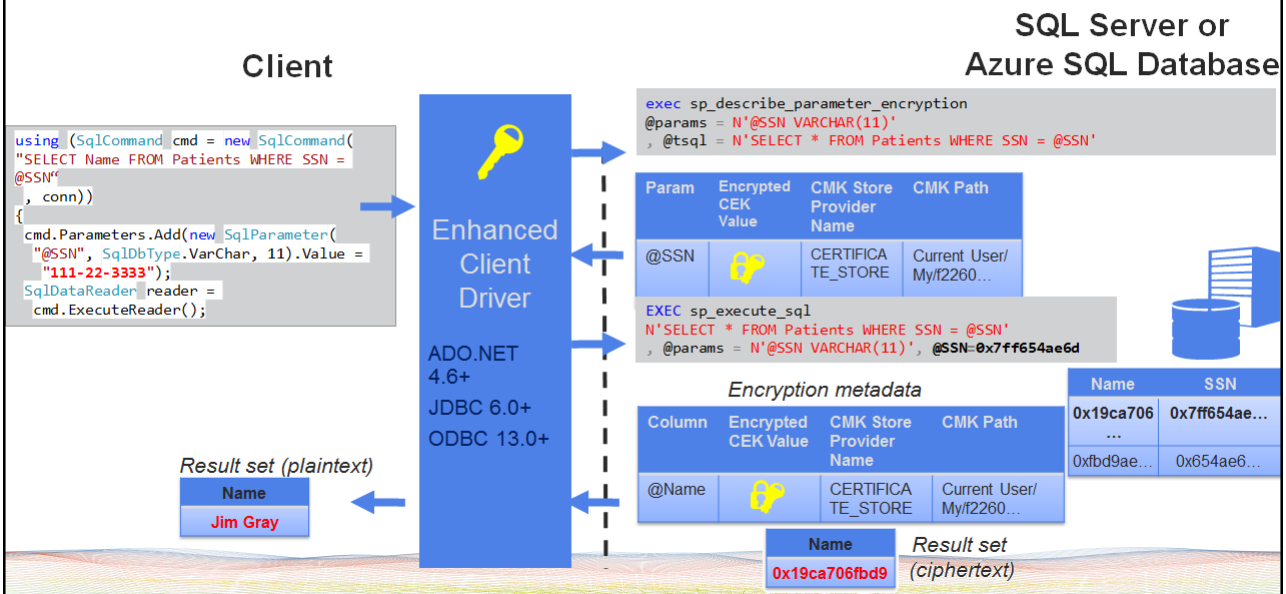
Health Care Demo Cont'd

Always Encrypted
How it looks: Using it all Together

20

SARPEDON QUALITY LAB

How it Works: Exact Match Searches



21

SARPEDON QUALITY LAB

Always Encrypted Limitations

- https://msdn.microsoft.com/en-us/library/mt163865.aspx
- http://blogs.sqlsentry.com/aaronbertrand/t-sql-tuesday-69-always-encrypted-limitations/
- Unsupported data types
  - **xml**, **rowversion**, **image**, **ntext**, **text**, **sql_variant**, **hierarchyid**, **geography**, **geometry**, alias, user defined-types
  - FILESTREAM, non-bin2 collations, ROWGUIDCOL, Sparse column set
  - Columns referenced by statistics
  - default constraints
  - Columns that are masked
  - temporal tables
  - memory optimized tables
  - Stretched tables
- Not supported Features:
  - Transactional or merge replication

22

Always Encrypted: Learn More

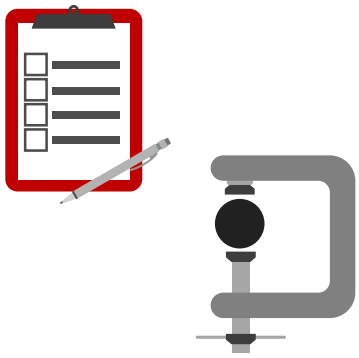
SARPEDON QUALITY LAB

- Books Online
- https://msdn.microsoft.com/en-us/library/mt163865.aspx
- SQL Security Blog (keyword Always Encrypted)
- http://blogs.msdn.com/b/sqlsecurity/archive/tags/always+encrypted/
- Channel 9 Videos
- https://channel9.msdn.com/Shows/Data-Exposed/SQL-Server-2016-Always-Encrypted
- https://channel9.msdn.com/Shows/Data-Exposed/Getting-Started-with-Always-Encrypted-with-SSMS

23

Other security enhancements

- Audit success/failure of database operations
- Enhanced auditing for OLTP with ability to track history of record changes
- Transparent Data Encryption support for storage of In-memory OLTP Tables
- Backup encryption now supported with compression
- Transparent Data Encryption with support for Intel AES-NI hardware acceleration



Azure SQL Database Threat Detection

SARPEDON QUALITY LAB

- 4 PM
  - Azure SQL Database Security - Microsoft product team
  - Ron Matchoro (Microsoft)
  - Dome 3

27

SARPEDON QUALITY LAB

Q&A

28

Thank you

Andreas Wolter

Microsoft CERTIFIED Solutions Master Data Platform

Microsoft CERTIFIED Master SQL Server® 2008

SARPEDON QUALITY LAB

Contact: a.wolter@Sarpedon.de
LinkedIn: www.linkedin.com/in/AndreasWolter
Twitter: @AndreasWolter

29

SARPEDON QUALITY LAB

MICROSOFT® CERTIFIED SINCE 2000

Sarpedon Quality Lab
Your Specialist for Database-Systems based on SQL Server Technologies

We are **one of only 2 companies worldwide** who have reached the **highest technical certifications** from Microsoft for **SQL Server 2008** as well as **SQL Server 2012**!

Microsoft CERTIFIED Solutions Master Data Platform

Microsoft CERTIFIED Master SQL Server® 2008

MVP Microsoft® Most Valuable Professional

We love to support you and use our know-how to your advantage.

our ***Services*** cover:

- *SQL Server Health checks*
- *Performance Analysis & Tuning*
- *Disaster-Recovery & SLA-Compliance-Checks*
- *Security-Checks*
- *Data Rescue in case of corruption*
- *Architecture-Planning, Consulting and Implementation*
- ***Training***: SQL SERVER MASTER-CLASS

Ask us: info@Sarpedon.de

30