Upgrade to avoid end of support for SQL Server 2008

SQL Server 2008 and SQL Server S008 R2 will no longer be supported by Microsoft starting in July 2019. Avoid challenges and vulnerabilities caused by end of support.

What end of support means:

No security updates
There will be no access to critical security updates, opening the potential for business interruptions and loss of data.

Compliance concerns
As support ends, your organization may fail to meet compliance standards and industry regulations.

Higher maintenance costs
Maintaining legacy servers, firewalls, intrusion systems, and other tools can get expensive quickly.

More than an upgrade with SQL Server 2017

With SQL Server, you don't just get an update – you get in-memory performance across workloads, mission-critical high availability, end-to-end mobile BI, and in-database advanced analytics with security features to help protect your data at rest and in motion – now on Linux and Docker.
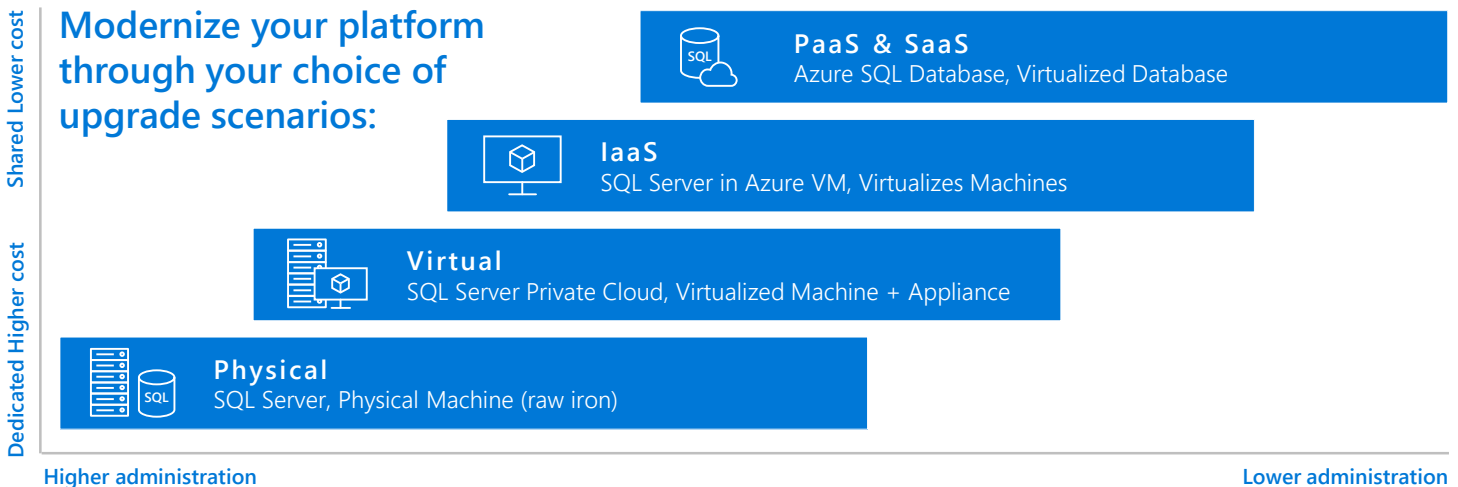
#1 OLTP performance[1]

#1 DW performance on 1TB[2], 10TB[3], and 30TB[4]

#1 OLTP price/performance[5]

#1 DW price/performance on 1TB[2], 10TB[3], and 30TB[4]

Modernize your platform through your choice of upgrade scenarios:

Shared Lower cost
Dedicated Higher cost

PaaS & SaaS
Azure SQL Database, Virtualized Database

IaaS
SQL Server in Azure VM, Virtualizes Machines

Virtual
SQL Server Private Cloud, Virtualized Machine + Appliance

Physical
SQL Server, Physical Machine (raw iron)

Higher administration   Lower administration

New features for compliance since 2008

SQL Server 2017 includes loads of additional features since SQL Server 2008, however the following key features directly help meet industry compliance regulations like GDPR and help keep your applications secure and performant.

Features for the four steps to GDPR compliance

1. Discover Right to Erasure Right to Data Portability	2. Manage Documentation Privacy by Design	3. Protect Data Security Data Transfer	4. Report Documentation Breach Response and Notification
Metadata queries Helps you search and identify personal data using queries	**Data governance** Using Windows permissions, administrators can manage and govern access to data	**Transparent Data Encryption** Secure personal data at the physical storage layer using encryption-at-rest	**SQL Server Audit** Maintain audit trails
Full text queries Using full-text queries against character-based data in SQL Server tables	**Role-based access control** Apply role-based access control to manage authorization policies and to implement the separation of duties principle	**Always Encrypted** Prevent unauthorized, high-privileged users from accessing data in transit, at rest, and while in use	**Vulnerability assessment** Reports that serve as a security assessment for your database. These reports can also be used as part of a Data Protection Impact Assessment (DPIA)
Extended properties Helping facilitate data classification using the Extended Properties feature to create data classification labels and apply them to sensitive personal data	**Row-level security** Prevent access to rows in a table (such as those that may contain sensitive information) based on characteristics of the user trying to access the data	**Row-level security and Data Masking** Protect personal data using Row-Level Security and Dynamic Data Masking features, which limit sensitive data exposure by masking the data to non-privileged users or applications.	**SQL Server Audit** Gain useful input for performing a DPIA
SQL Queries and Statements Identify and delete target data	**Master data services** Keep personal data complete and ensure that requests to edit, delete, or discontinue the processing of data are propagated throughout the system	**Vulnerability assessment** Scan databases for insecure configurations, exposed surface area, and additional potential security issues	
	SQL Server Audit Verify changes to data that occur in a SQL Server table	**Always On Availability Groups** Maximize the availability of a group of user databases for an enterprise	
		SQL Database Threat Detection Get help detecting anomalous database activities indicating potential security threats to the database	
		SQL Server Audit Understand ongoing database activities, and analyze and investigate historical activity to identify potential threats or suspected abuse and security violations	

Support becomes vital with GDPR

General Data Protection Regulation is an important industry regulation requiring organizations doing business in the European Union to maintain appropriate security of personal data.

Unsupported SQL Server may be non-compliant, which could result in significant penalties.

CCR
CENTER for COMPUTER RESOURCES

Microsoft