# **Descriptions of Services Deployed**

## ExpressRoute

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Office 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet connectivity models.

Source: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

## Azure Key Vault

Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users.

Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

To access a key vault in either plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute.

Both planes use Azure Active Directory (Azure AD) for authentication. For authorization, the management plane uses role-based access control (RBAC) and the data plane uses a Key Vault access policy.

Source: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

## Azure Data Factory

Azure Data Factory is a managed cloud service that's built for these complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects. Azure Data Factory does not store any data except for linked service credentials for cloud data stores, which are encrypted by using certificates. With Data Factory, you create data-driven workflows to orchestrate movement of data between supported data stores, and processing of data by using compute services in other regions or in an on-premises environment.

**Data encryption in transit**

If the cloud data store supports HTTPS or TLS, all data transfers between data movement services in Data Factory and a cloud data store are via secure channel HTTPS or TLS .

**Data encryption at rest**

Some data stores support encryption of data at rest. We recommend that you enable the data encryption mechanism for those data stores. (Refer to documentation for each data store component for data encryption at rest capabilities.)

Source: <https://docs.microsoft.com/en-us/azure/data-factory/data-movement-security-considerations>

## Azure Data Lake (Gen 2) / Azure Blob Storage

Azure Data Lake Storage Gen2 is a set of capabilities dedicated to big data analytics, built on Azure Blob storage. Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data.

**Data encryption in transit**

You can configure your storage account to accept requests from secure connections only by setting the Secure transfer required property for the storage account. When you require secure transfer, any requests originating from an insecure connection are rejected. Microsoft recommends that you always require secure transfer for all of your storage accounts.

**Data encryption at rest**

Azure Storage automatically encrypts your data when it is persisted it to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

**Access Controls**

Azure Data Lake Storage Gen2 implements an access control model that supports both Azure role-based access control (RBAC) and POSIX-like access control lists (ACLs).

Sources / Additional References:

<https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>

<https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-access-control>

<https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations>

## Azure SQL Databases / Azure Synapse Analytics (formerly SQL Data Warehouse)

Azure Synapse is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics. It gives you the freedom to query data on your terms, using either serverless on-demand or provisioned resources—at scale. Azure Synapse brings these two worlds together with a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine learning needs.

**Data encryption in transit**

Sql Server enforces encryption (SSL/TLS) at all times for all connections. This ensures all data is encrypted "in transit" between the client and server irrespective of the setting of Encrypt or TrustServerCertificate in the connection string.

**Transparent Data Encryption (Data Encryption at Rest)**

Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, TDE is enabled for all newly deployed Azure SQL databases. TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.

**Data masking**

SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users. Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It’s a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

**Data classification**

Data Discovery & Classification provides advanced capabilities built into Azure SQL Database for discovering, classifying, labeling & reporting the sensitive data in your databases. Discovering and classifying your most sensitive data (business, financial, healthcare, personally identifiable data (PII), and so on.) can play a pivotal role in your organizational information protection stature.

Sources / Additional References:

<https://docs.microsoft.com/en-us/azure/sql-data-warehouse/sql-data-warehouse-overview-what-is>

<https://docs.microsoft.com/en-us/azure/sql-data-warehouse/sql-data-warehouse-overview-manage-security>

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview#transport-layer-security-tls-encryption-in-transit>

[https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql](https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql?toc=%2Fazure%2Fsql-data-warehouse%2Ftoc.json&bc=%2Fazure%2Fsql-data-warehouse%2Fbreadcrumb%2Ftoc.json&tabs=azure-portal)

[https://docs.microsoft.com/en-us/azure/sql-database/sql-database-dynamic-data-masking-get-started](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-dynamic-data-masking-get-started?toc=/azure/sql-data-warehouse/toc.json&bc=/azure/sql-data-warehouse/breadcrumb/toc.json)

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-data-discovery-and-classification>

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-best-practice>

## Analysis Services

Azure Analysis Services is a fully managed platform as a service (PaaS) that provides enterprise-grade data models in the cloud. Use advanced mashup and modeling features to combine data from multiple data sources, define metrics, and secure your data in a single, trusted tabular semantic data model. The data model provides an easier and faster way for users to browse massive amounts of data for ad hoc data analysis.

**Network security**

Azure Analysis Services provides security for sensitive data at multiple levels. As an Azure service, Analysis Services provides Basic level of Distributed denial of service (DDoS) attacks automatically enabled as part of the Azure platform. To learn more, see Azure DDoS Protection Standard overview.

**Authentication and Authorization**

At the server level, Analysis Services provides firewall, Azure authentication, server administrator roles, and Server-Side Encryption. At the data model level, user roles, row-level, and object-level security ensure your data is safe and gets seen by only those users who are meant to see it.

**Data storage security**

Azure Analysis Services uses Azure Blob storage to persist storage and metadata for Analysis Services databases. Data files within Blob are encrypted using Azure Blob Server Side Encryption (SSE). When using Direct Query mode, only metadata is stored. The actual data is accessed through encrypted protocol from the data source at query time.

Source: <https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview>

## Power BI

Power BI is an online software service (SaaS, or Software as a Service) offering from Microsoft that lets you easily and quickly create self-service Business Intelligence dashboards, reports, datasets, and visualizations. With Power BI, you can connect to many different data sources, combine and shape data from those connections, then create reports and dashboards that can be shared with others.

Please reference the Power BI Security Whitepaper for all security questions and concerns: <https://docs.microsoft.com/en-us/power-bi/whitepaper-powerbi-security>

Sources / Additional References:

<https://docs.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview>

<https://docs.microsoft.com/en-us/power-bi/service-admin-power-bi-security>

<https://docs.microsoft.com/en-us/power-bi/service-admin-governance>