
As Power BI becomes more prevalent in data analytics and visualization within the enterprise, data security becomes a significant concern. Companies who have made the leap to cloud technologies such as AWS, Microsoft Azure, Salesforce and Microsoft Office 365 should have an understanding of the data compliance and security capabilities of those solutions.

I have been involved with data and cloud security questions a lot the past few years. With Power BI's rise in significance, I had to answer more specific questions about the service. This is the first of a series of blog posts on various data security items in Power BI following my webinar on the topic. The series will cover the following topics: sharing data, on-premises data gateway, privacy levels and data classification. The focus of these articles are related to using the Power BI service, as this is the cloud implementation of Power BI. The desktop has settings which impact deployment of assets, but is not the focus of this series.

***The Power BI service is updated frequently. These articles were created based on the Power BI implementation in early April 2017. You may find improvements and changes that impact your experience that are based on newer releases. Feel free to add comments to highlight changes.***

# Power BI Compliance

Let's start with the highest level of data security: compliance. I previously published a post about Power BI's inclusion in the Microsoft Trust Center. Power BI became compliant nearly a year ago in April 2016. This was a huge step forward for being able to use Power BI in the enterprise.


You can find the latest Power BI compliance here. This same site has additional security information I will refer to throughout the posts including high level information about data security and privacy.

# Power BI and Data Encryption

One of the key areas of concern is related to data when it is added or passed through the service. In this section, we will review how Power BI handles data at rest and data in transit. The content below is summarized from the Power BI Security Whitepaper (published September 2016).

# Power BI Data at Rest

Data at rest is always encrypted in Azure. Depending on the type of data, Power BI uses encrypted storage in Azure Blob Storage and Azure SQL Database. Refer to the security whitepaper for details on how the encryption keys are handled.

The table below gives a summary of how data at rest is handled based on the data source or how the data is delivered to the visuals.

| DATA SOURCE | METADATA | DATA |
|---|---|---|
| Live Connection (Analysis Services) | Nothing stored except database name encrypted in Azure SQL DB | Nothing Stored |
| Direct Query (SQL Server, Oracle, etc.) | Encrypted in Azure Blob Storage | Nothing Stored |
| Pushed or streamed data | Encrypted in Azure Blob Storage | Depending on version, encrypted in either Azure Blob Storage or Azure SQL Database |
| Data loaded into model (data may be refreshable or nonrefreshable) | Encrypted in Azure Blob Storage | Encrypted in Azure Blob Storage |

# Power BI Data in Transit

Simply put, data is always encrypted in transit. The following is a direct quote from the security white paper:

*All data requested and transmitted by Power BI is encrypted in transit using HTTPS to connect from the data source to the Power BI service. A secure connection is established with the data provider, and only once that connection is established will data traverse the network.*

# Power BI Data “in use”

As data moves to the dashboards and reports to be visualized, some data elements are cached to improve performance. Data is often cached for even Direct Query connections to improve dashboard performance. Cached data is encrypted and stored in an Azure SQL Database. Pinned visuals in the Power BI dashboards such as Excel and SSRS visualizations are also encrypted and cached in an Azure SQL Database.