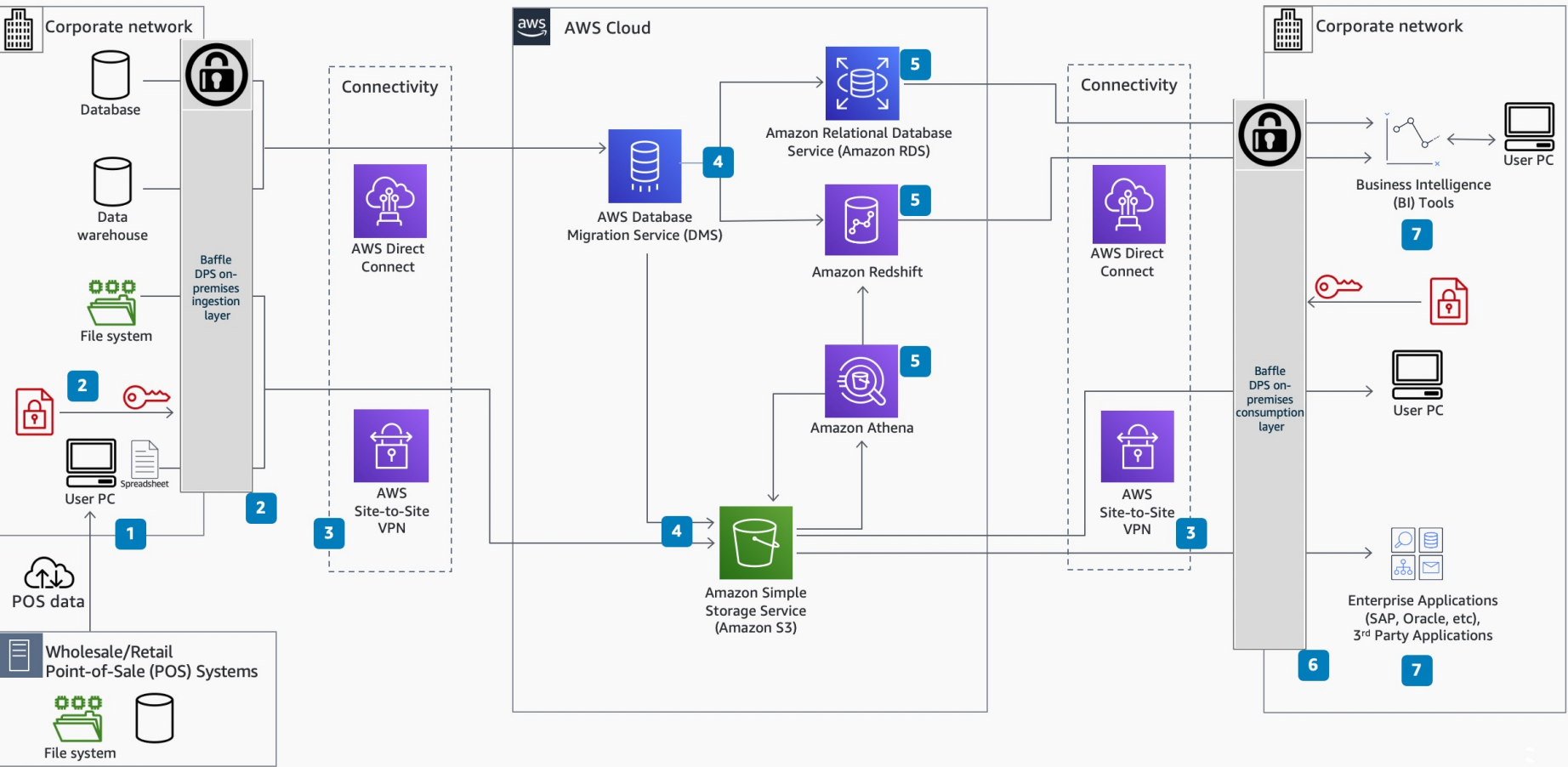


# Protect Your Data in AWS with Hold Your Own Key (HYOK) Solutions provided by Baffle Data Protection Service (DPS)

[Baffle DPS](#) provides a Hold Your Own Key (HYOK) solution to enable customers who require additional data-centric protection measures to address more stringent privacy regulations, such as not storing encryption keys in AWS. For more details on customer responsibility for data stored on AWS, see the AWS [Shared Responsibility Model](#).



- 1 End-of-day point-of-sale (POS) data is downloaded from wholesale/retail partner systems and saved on-premises.
- 2 Baffle DPS data ingestion layer uses the encryption key held on-premises with Format-Preserving Encryption (FPE) mechanism to tokenize, anonymize, and map data flow for both structured and unstructured data, when additional protection is needed, before the data is sent to AWS.
- 3 Customer's choice of dedicated connection (**AWS Direct Connect**) or **AWS Site-to-Site VPN** for security of the data while it's in transit.
- 4 Encrypted data arrives to AWS and is stored without the encryption key, in either structured or unstructured format.
- 5 Encrypted data can be queried in AWS with various services but the data will remain encrypted.
- 6 Baffle DPS data consumption layer uses the decryption key held on-premises to decrypt, de-tokenize, and map data flow back to its clear-text form before it is used by the on-premises applications or users.
- 7 Clear-text data is used for business intelligence or by downstream applications.

