Encryption:

Encryption is the process of obfuscating the data by use of key or password.

All use of encryption should use a maintenance of keys, passwords and certificates.

Asymmetric keys: Asymmetric keys use the private key and corresponding public key to encrypt and decrypt

the data. Asymmetric key is resource intensive process but it is more secure than symmetric key.

Symmetric Keys: Symmetric key uses a single key to encrypt and decrypt the data. It is fast in performance and used for database encryption.

Transparent Encryption Key(TDE): TDE uses the symmetric key known as database encryption key. This database key is protected by certificate and

which is further protected by database master key(DMK) and which is further protected by service master key(SMK) and which is further protected by

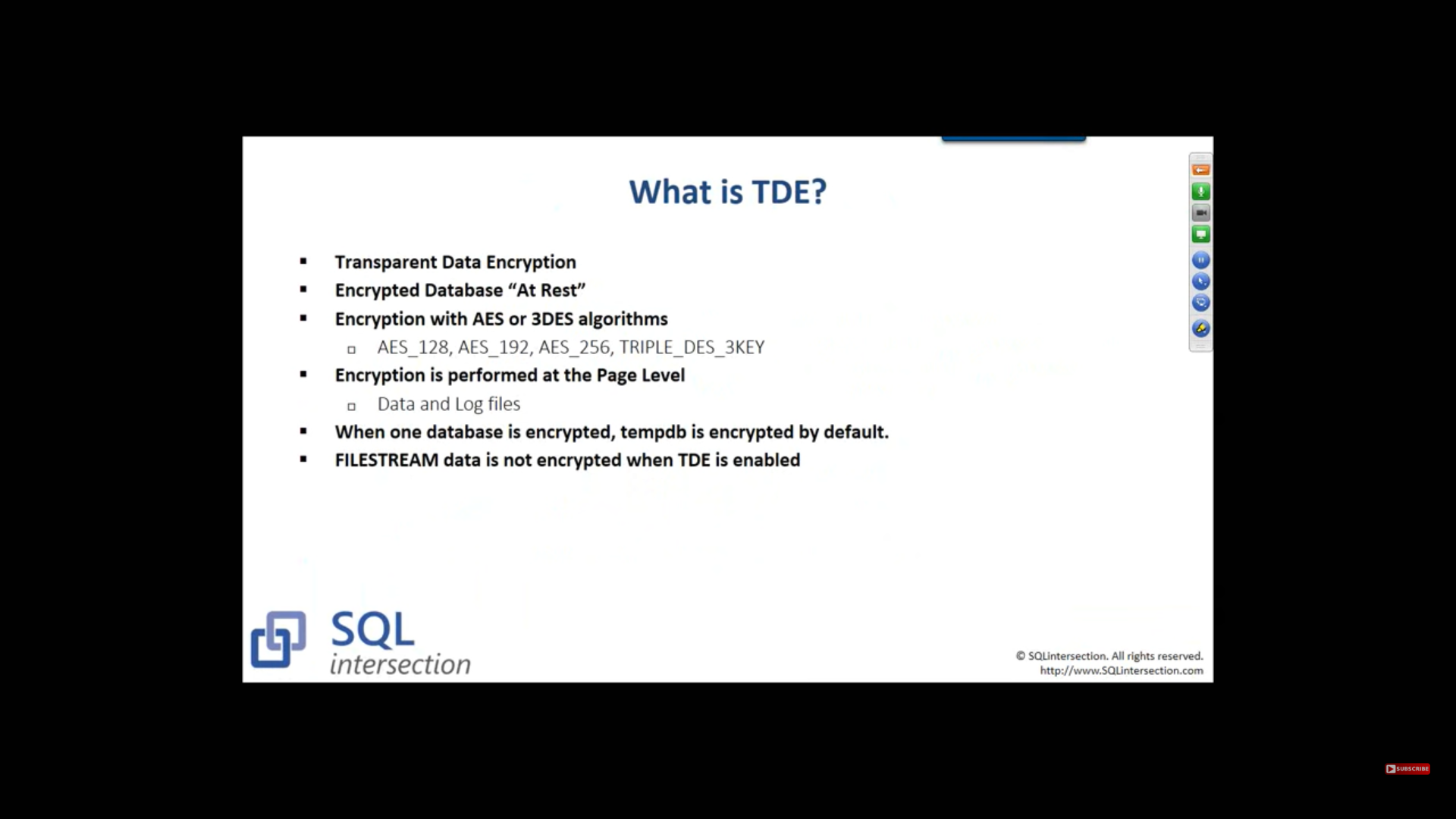
Data protection API (DPAPI) at OS level. DE is an Encryption at rest.

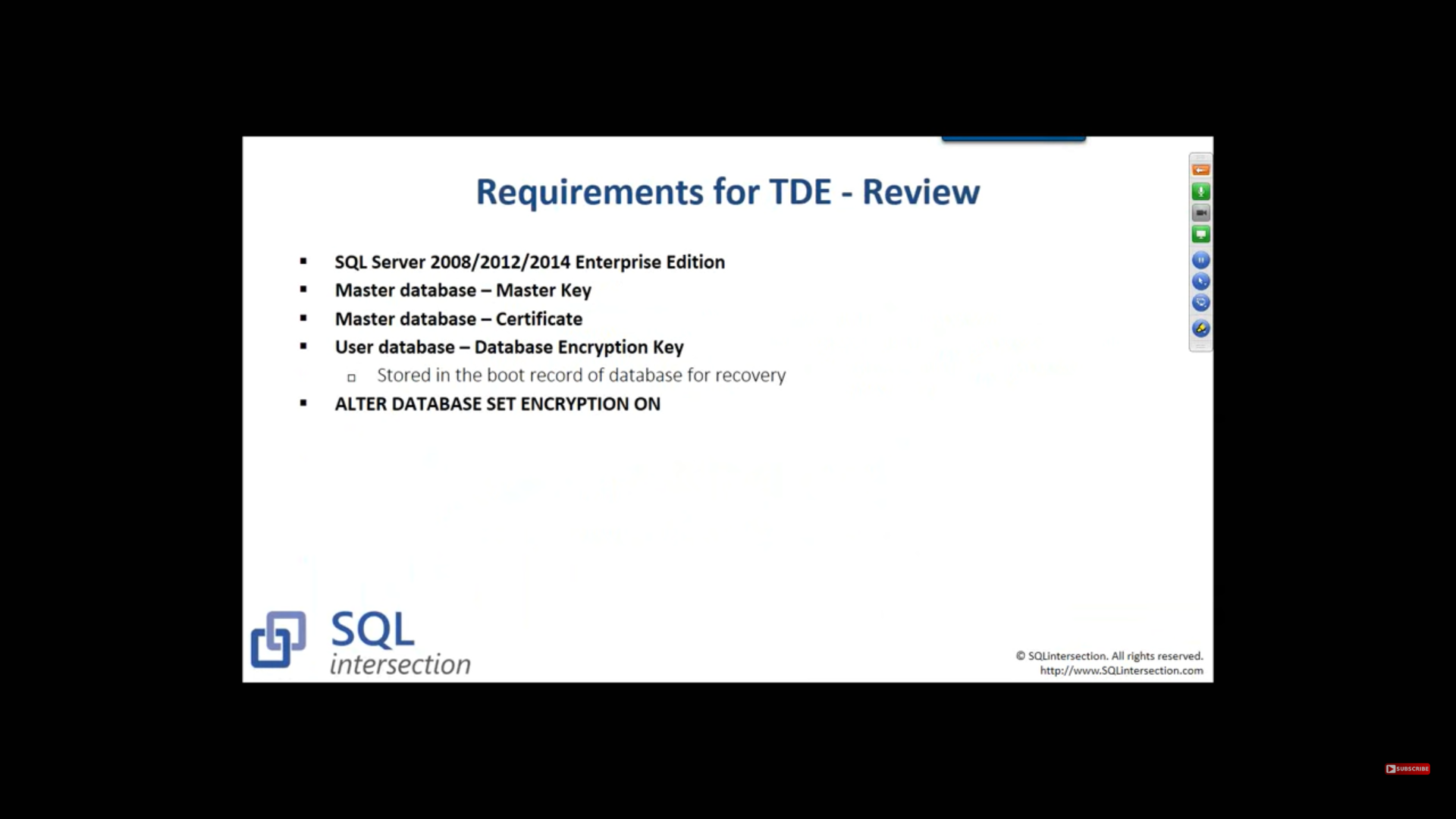
After enable TDE, immediately backup the certificates and private keys. if the certificates become unavailable and if you go to restore the database on another server then you need a backup of certificates and private keys otherwise you can't open the database.

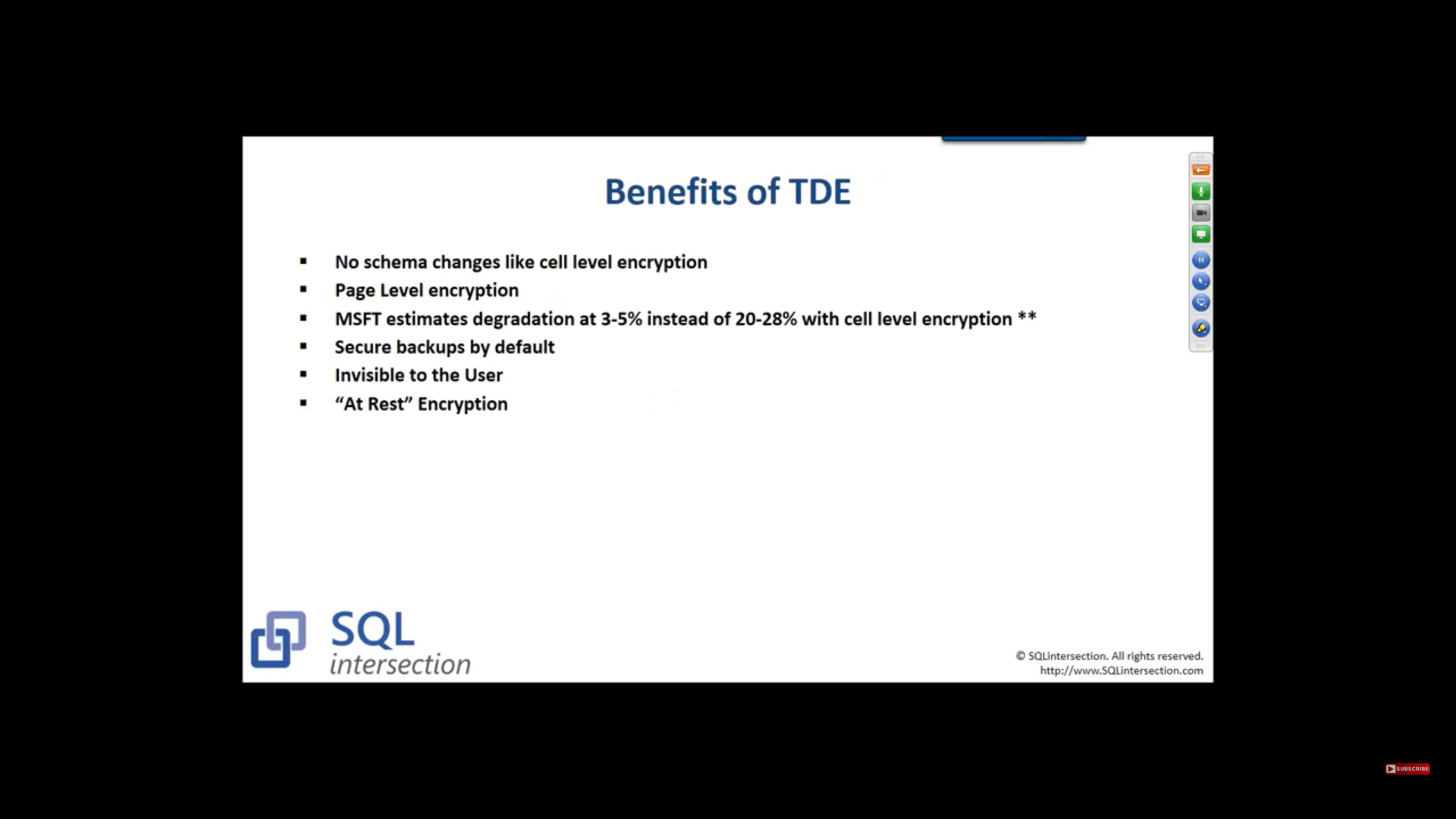
keep the encrypting certificates on place even you have disabled the TDE. you may need those until you take full backup of the database.

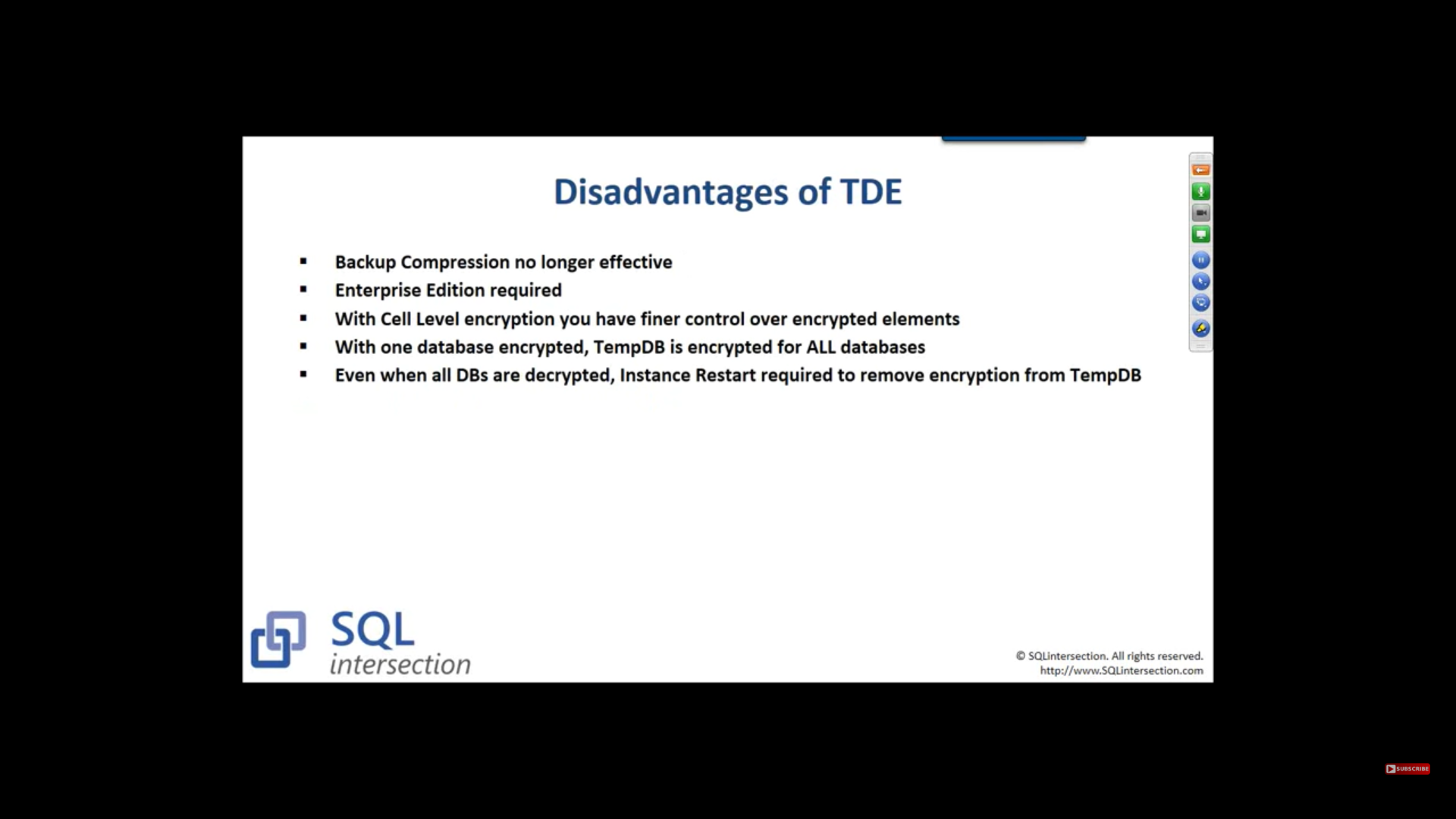
<https://www.youtube.com/watch?v=sIwd09jEO3Y>



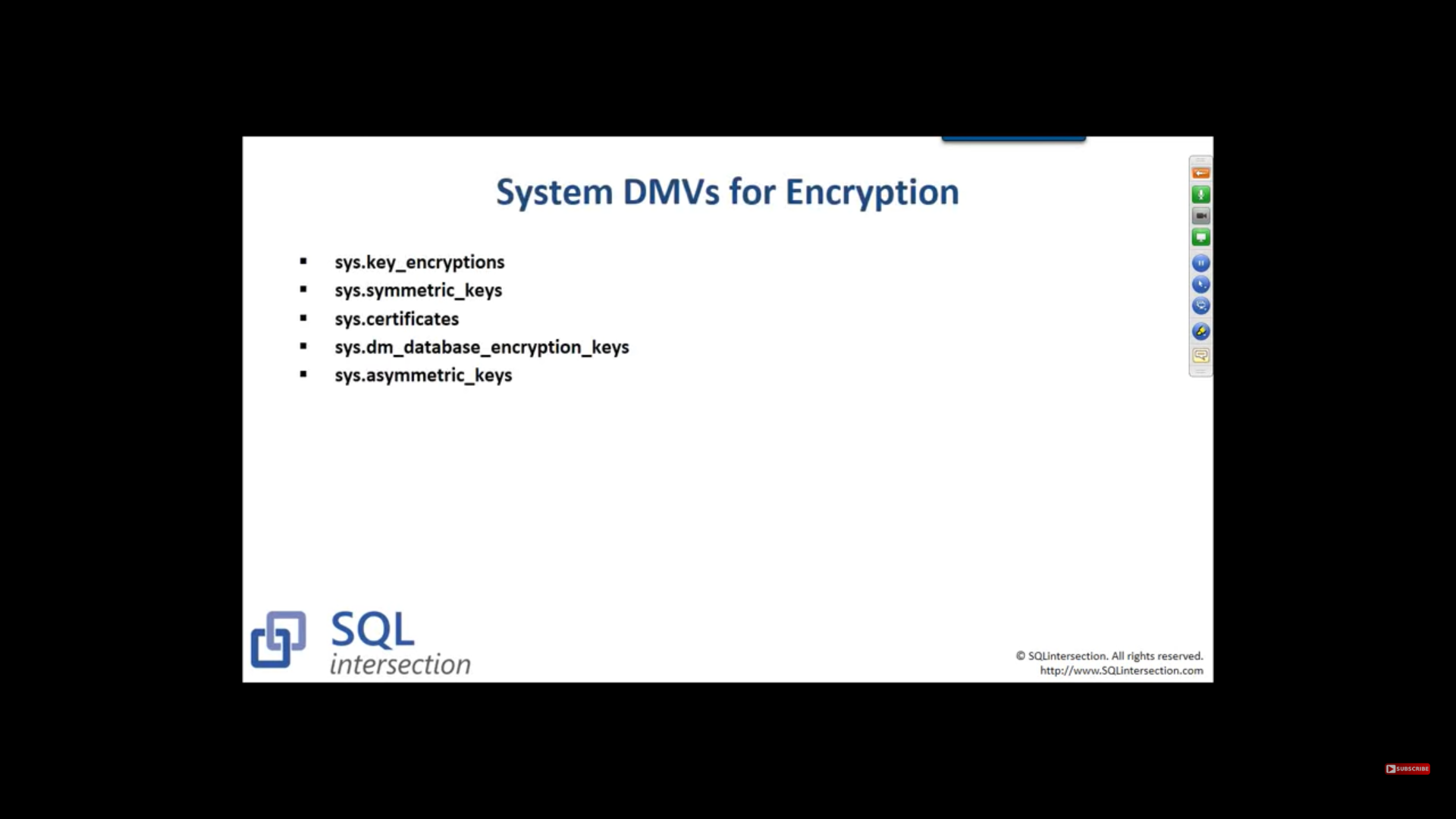






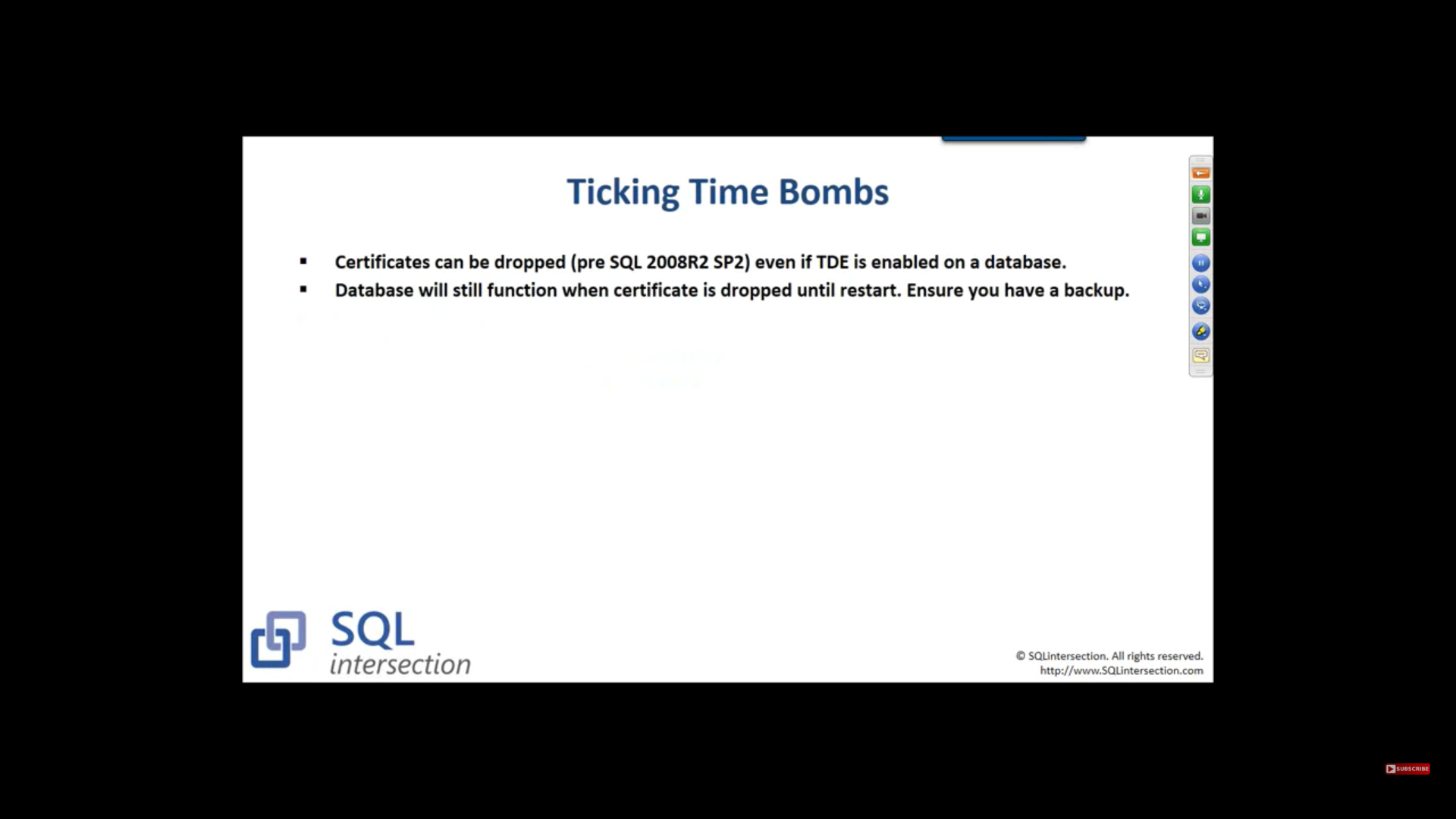


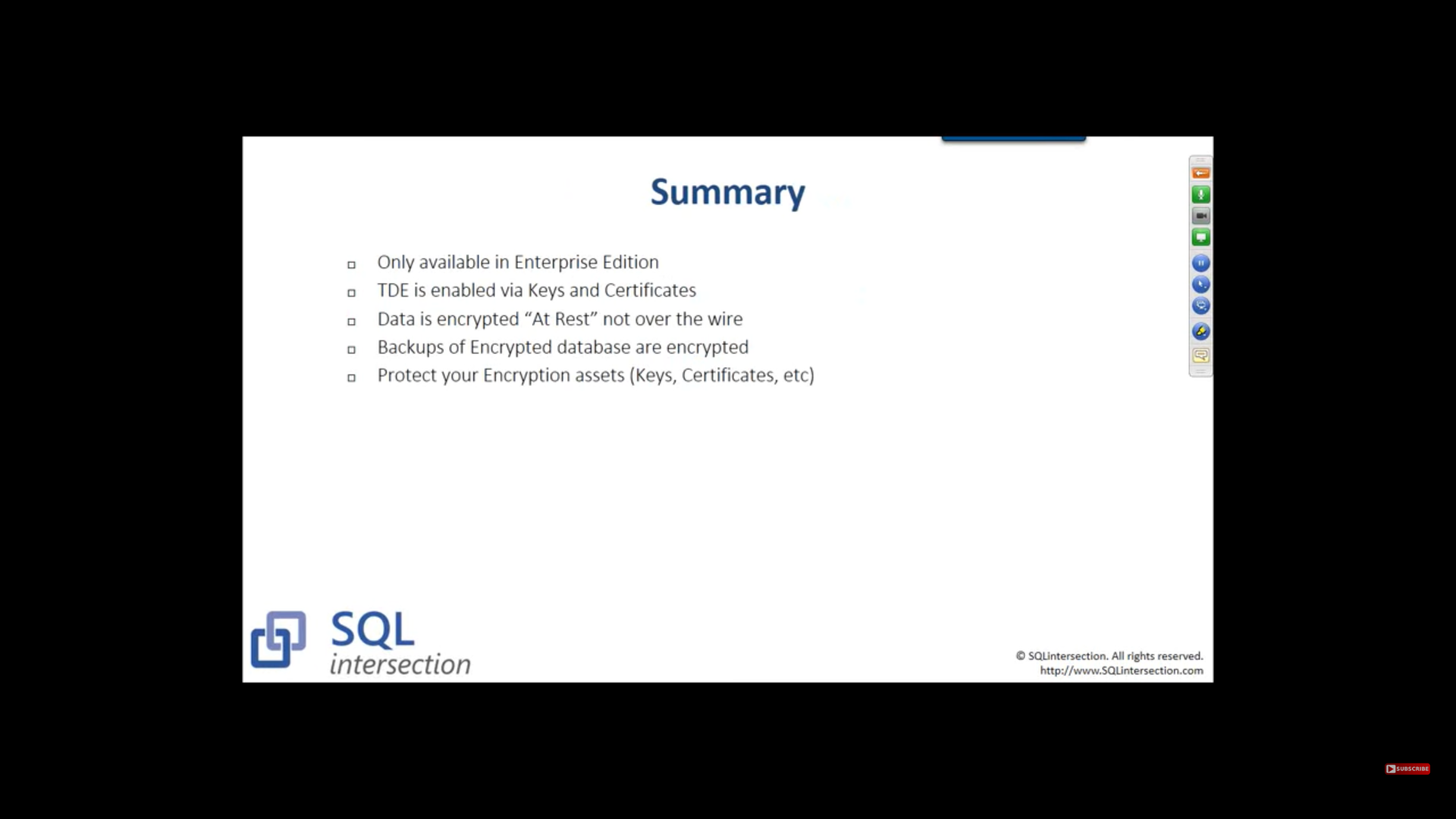




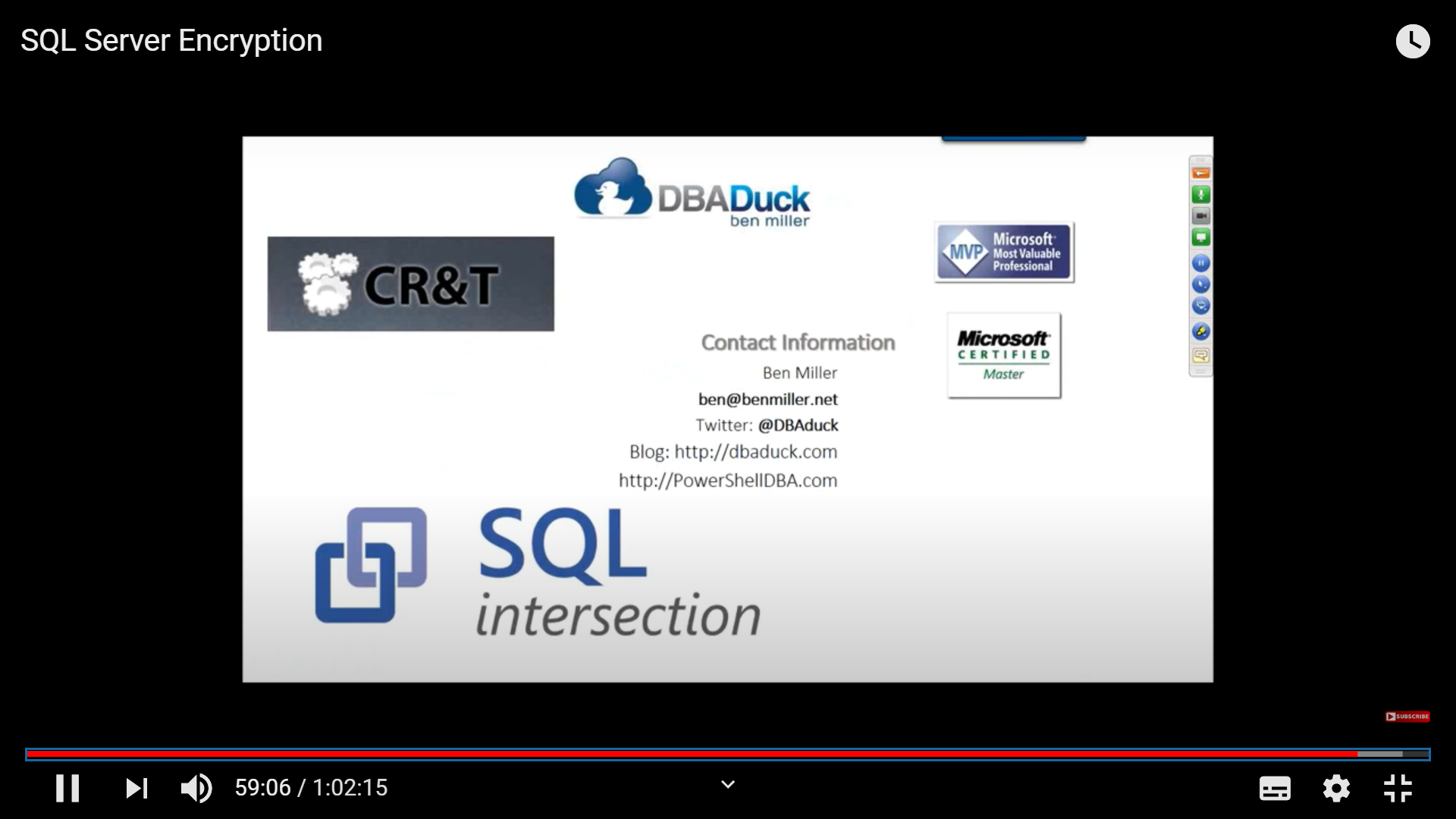


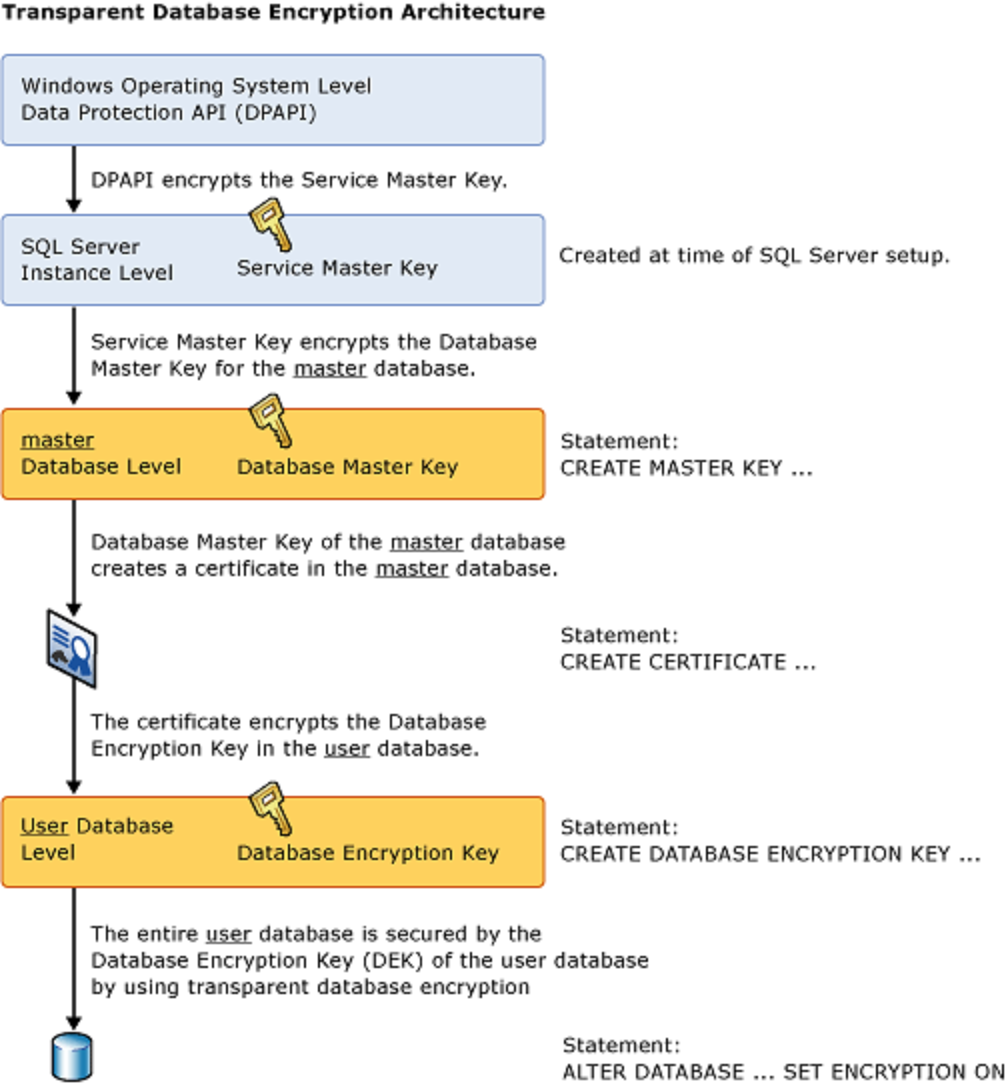
Do TDE before set up Mirroring











**Enable TDE**

To use TDE, follow these steps.

**Applies to**: SQL Server.

1. Create a master key.
2. Create or obtain a certificate protected by the master key.
3. Create a database encryption key and protect it by using the certificate.
4. Set the database to use encryption.
5. USE master;
6. GO
7. CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
8. go
9. CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
10. go
11. USE AdventureWorks2012;
12. GO
13. CREATE DATABASE ENCRYPTION KEY
14. WITH ALGORITHM = AES\_128
15. ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
16. GO
17. ALTER DATABASE AdventureWorks2012
18. SET ENCRYPTION ON;

GO

The encryption and decryption operations are scheduled on background threads by SQL Server.

DMV’s

[sys.databases (Transact-SQL)](https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-databases-transact-sql?view=sql-server-ver15)

[sys.certificates (Transact-SQL)](https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-certificates-transact-sql?view=sql-server-ver15)

[sys.dm\_database\_encryption\_keys (Transact-SQL)](https://docs.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-database-encryption-keys-transact-sql?view=sql-server-ver15)

To monitor changes in the TDE status of a database, use SQL Server Audit or SQL Database auditing. For SQL Server, TDE is tracked under the audit action group DATABASE\_CHANGE\_GROUP

Replication doesn't automatically replicate data from a TDE-enabled database in an encrypted form. Separately enable TDE if you want to protect distribution and subscriber databases.

To remove encryption from database

ALTER DATABASE <db\_name> SET ENCRYPTION OFF;