DPM Deployment Architecture Options

Transparent Data Encryption and Enterprise Key Management

DPM software products are installed into standard Windows or Linux environments

Our Transparent Data Encryption (TDE) with Enterprise Key Management solution, comprises three components:

- easyCipher management module which centrally controls policies for data privacy
- easyKey management module which centrally manages keys and certificates
- DPM encryption agents which are installed on end-devices and servers holding data (to be encrypted)
- The DPM easyCipher manager and DPM easyKey applications are installed in a physical or virtual Windows or Linux environment together with a backend database for storing DPM application data.
- DPM agent software is installed on every laptop and server requiring transparent data encryption of content (files, folders, applications or databases)

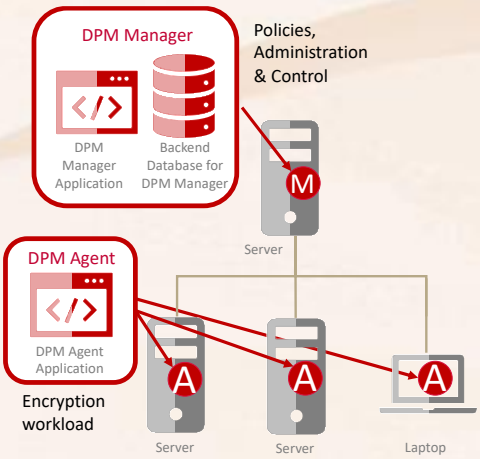


Figure 1 DPM software physical installation

- Protected data is never accessed or stored within DPM management modules whether deployed in-house or accessed via DPM easyCloudPlus SaaS
- The work of the DPM management modules is confined to managing and monitoring DPM Encryption Agents, API and DB Database Connectors activity, data privacy and key management policies

DPM easyCipher manager controls policies for transparent data encryption that is performed by DPM easyCipher agents.

DPM easyCipher agents perform all the heavy lifting of encryption processing on protected servers

DPM easyKey provides centralized key and certificate management services other DPM products or other systems requiring key management.

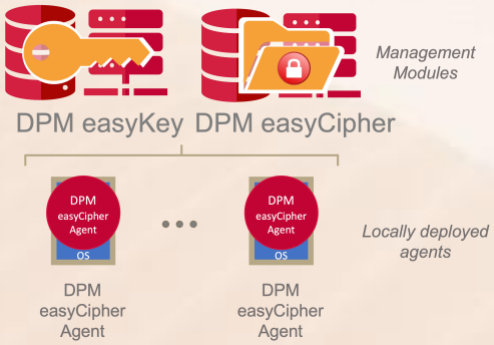


Figure 2 DPM easyCipher, DPM easyKey logical components

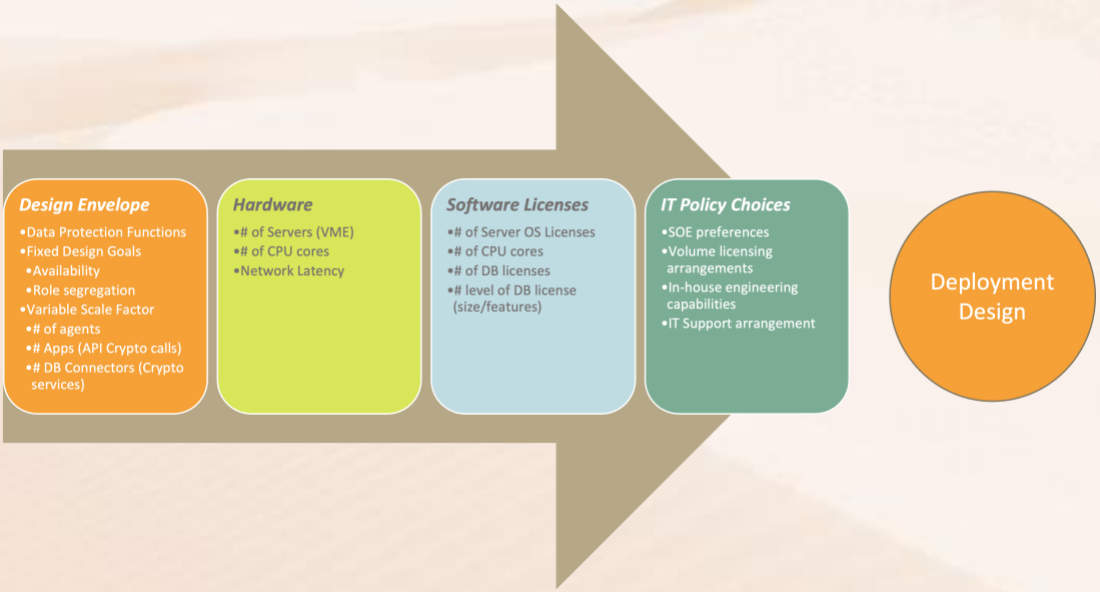
DPM Deployment Architecture Options

Transparent Data Encryption

Deployment Design Process

The deployment design considerations for DPM easyCipher are the same as for any mission-critical application that run in a standard Windows or Linux environment:

- Considerations of depth of redundancy, back-up for disaster recovery along with having an isolated test environment influence the number of DPM manager instances,
- Considerations of performance and role-separation, influence the amount of hardware resources devoted to each DPM manager instance.



Flexibility in deployment design

DPM easyCipher and DPM easyKey can be run in a single environment alongside a shared backend database. Alternatively for customers requiring higher levels of performance, backend database can be split onto a separate server or multiple servers can be running in a load-balancing configuration.