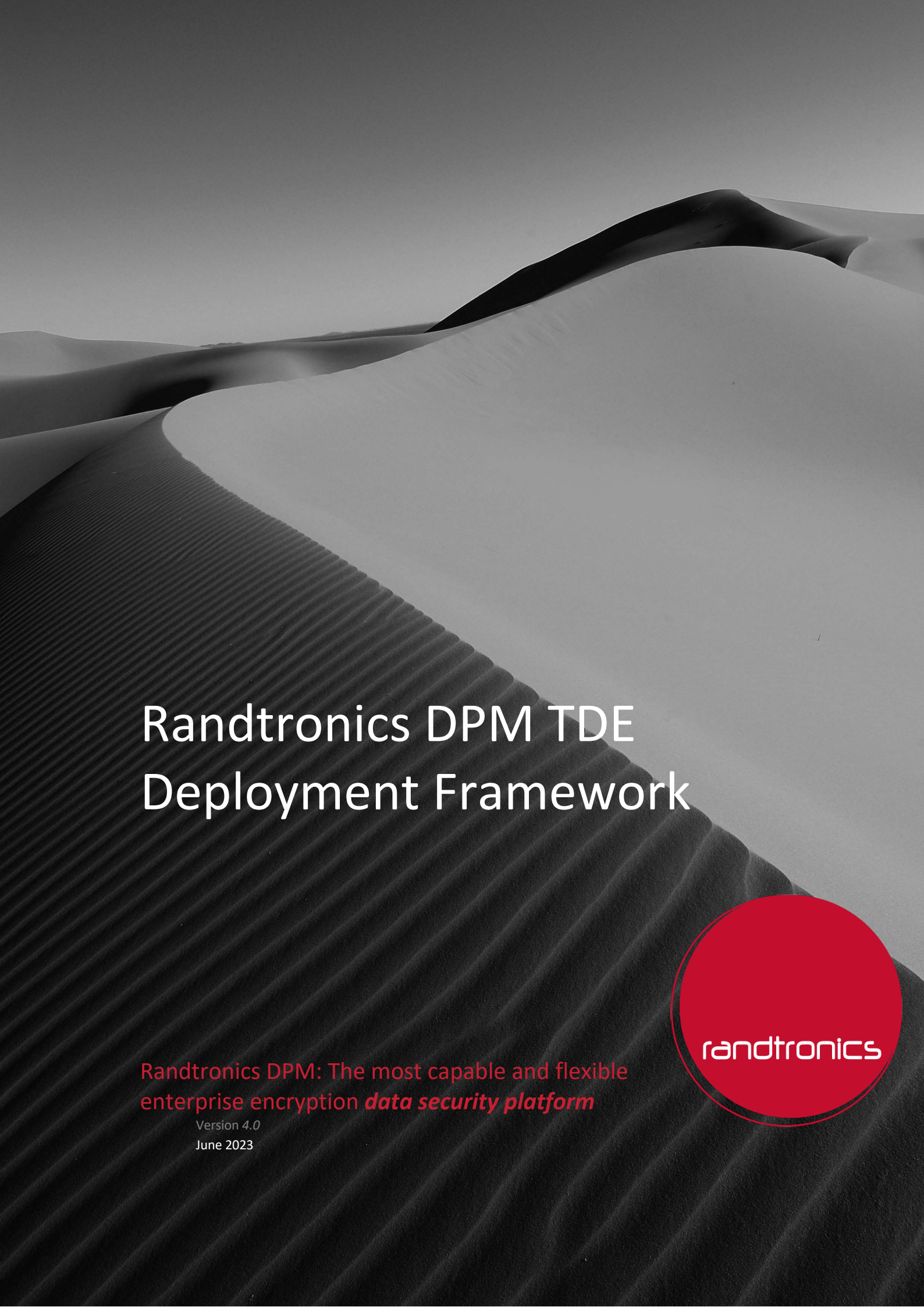

Randtronics DPM TDE Deployment Framework

Randtronics DPM: The most capable and flexible enterprise encryption ***data security platform***

Version *4.0*

June 2023

Randtronics DPM Deployment Framework

Randtronics DPM: The most capable and flexible enterprise encryption data security platform

Contents

1. Intended Audience 3
2. Introduction 3
3. Rapid deployment 4
4. Defining a deployment design 4
   - 4.1 Select DPM components 4
   - 4.2 Selecting a logical deployment architecture 4
   - 4.3 Physical Deployment Design 5
   - 4.4 Choosing Deployment Resources 6
5. Technology 7
6. Why is Software-only the smarter choice? 7
7. Conclusion 8
8. Appendix: DPM easyCipher deployment examples 9
   - 8.1.1 DPM easyCloud Plus SaaS 9
   - 8.1.2 Small Environment using Microsoft Windows 10
   - 8.1.3 Small Environment using Linux 10
   - 8.1.4 Small Environment with Redundancy 11
   - 8.1.5 Small Environment Minimum Hardware requirements 11
   - 8.1.6 Two-tier Architecture 11
   - 8.1.7 Two-tier architecture Minimum Hardware requirements 12
   - 8.1.8 Two-tier Architecture with Redundancy 12

1. Intended Audience

This document is written for CIO and CISO audience and is a companion document to the DPM Product Overview.

This document is written on the basis that the audience has already selected the DPM product components they require for their business requirement and this document provides a framework for the process of specifying an optimal deployment design – *how many virtual machines; redundancy; physical location; CPU cores, SOE, etc.*

For readers seeking information on the business proposition offered by the DPM Products and guidance as to which components will address their specific requirements, please refer first to the DPM Product Overview.

The Randtronics DPM product suite allows customers to mix and match components, accordingly the Deployment Architecture series contains documents that address the permutations of Transparent Data Encryption (TDE), Field-Level Data Protection (FLP) and/or enterprise Key Management.

2. Introduction

Randtronics DPM is a data security platform that manages encryption protections for structured and unstructured data on-premise and on-cloud without code changes.

This document is for customers seeking Transparent Data Encryption for databases and files (enterprise key management not required) and seeking information on the deployment options for their DPM solution:

- **DPM easyCipher** is our Transparent Data Encryption product that protects both structured and unstructured data stored on any Windows or Linux server in real-time.
- For customers also considering enterprise key management and field-level data protection, please refer to our other documents in this series.

DPM easyCipher comprises two components:

- easyCipher management module which centrally controls policies for data privacy, and
- DPM encryption agents which are installed on end-devices and servers holding data (to be encrypted)

The DPM easyCipher manager application is 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)

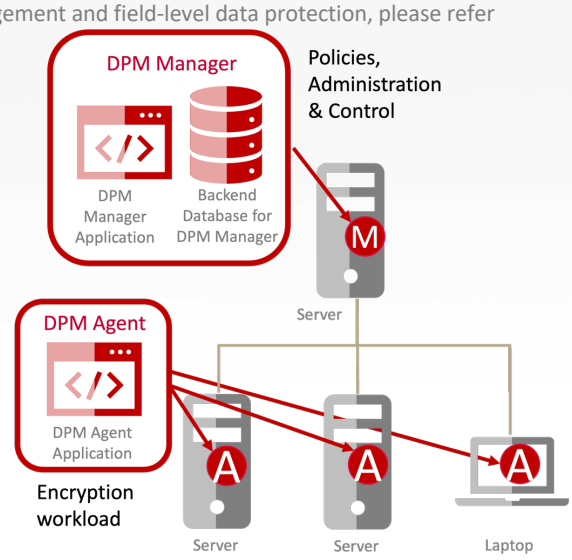

Figure 1 DPM easyCipher Physical Deployment

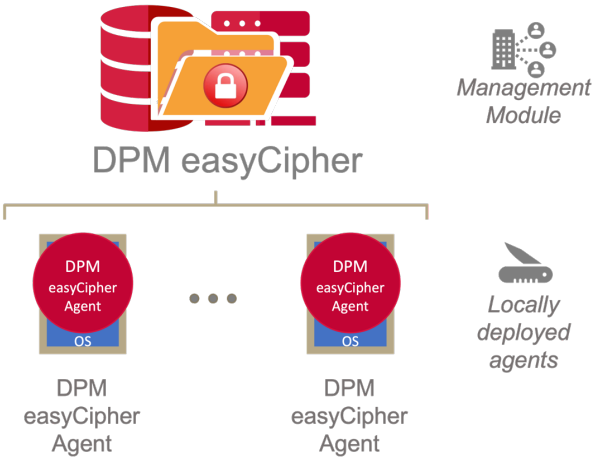

Figure 2 DPM easyCipher Logical Components

Randtronics DPM architecture centralizes data protection management and policies whilst distributing data protection operations for scalability and performance.

- 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

3. Rapid deployment

Randtronics DPM products are available for instant download and designed for rapid deployment:

- The Windows and Linux versions of the DPM easyCipher agents require only basic IT skills to install on local servers.
- Customers have the choice to either access the DPM easyCipher management functionality provided via Randtronics cloud-based encryption-as-a-service solution Randtronics DPM easyCloudPlus or install the DPM easyCipher management module in-house
- The easyCipher management module is suitable for deployment, monitoring and management in industry standard operating environments (SOE)

4. Defining a deployment design

A completed deployment design specifies the number, configuration and resources of the Virtual Machine instances required for the customer to deliver their functional and resilience goals in deploying DPM products.

The design process involves 4 steps:

1) Select DPM components
2) Define Logical Deployment Architecture
3) Specify Physical Deployment Design
4) Choose deployment resources

4.1 Select DPM components

DPM easyCipher manager and DPM encryption agents (laptop or server) are the necessary components for customers seeking Transparent Data Encryption without enterprise key management.

For more information on DPM components refer to DPM Product Overview.

4.2 Selecting a logical deployment architecture

A deployment architecture defines the number of Virtual Machine (VM) instances to run DPM management modules whilst addressing the customer's requirements for data location, functional separation, and redundancy.

The baseline deployment option for testing and low impact application is easyCipher operating as a single functional block running inside a single VM instance.

Starting from this baseline, the following factors will need to be considered to develop a logical deployment architecture to best address the customers business requirements:

- **N-Tier Depth:** The easyKey, easyCipher and easyData managers rely on backend database. This database may be shared between the managers or separated. Separation can occur on the same VM as the manager or a separate VM.

- **Role-Segregation:** Not applicable to customers only requiring easyCipher
- **Redundancy:** Consideration of N-Tier Depth and Role Segregation will define the number of functional blocks of VM instances in the logical deployment design. The degree of redundancy required will then define the number of VM instances required in each functional block. Organizations with high availability requirements will typically opt to select deployment configurations providing multi-location resilient in addition to other single-site fallback options.

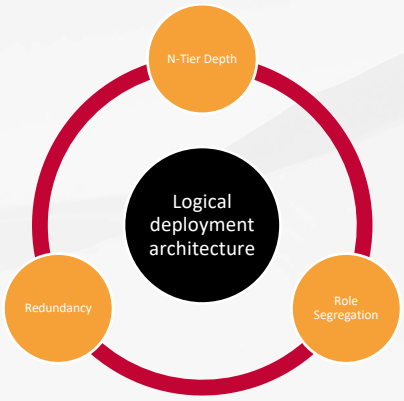

Figure 3 Logical Deployment Architecture design considerations

Diagram below illustrates how increasing N-Tier Depth and Role Segregation both independently increase the number of functional blocks in the logical deployment design. The number of VM instances in the logical design is then determined based on the degree of redundancy selected for each functional block.

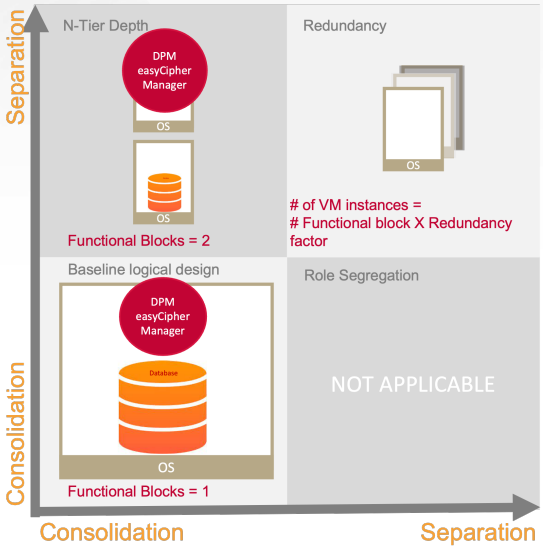

Figure 4 Number of VM instances as a function of design considerations

4.3 Physical Deployment Design

Having defined the number of VM instances required for the logical design now assess computational demands to determine the amount of physical computing resources required to power the VM instance in the logical design and consider locational constraints:

The amount of CPU cores, storage and related resources allocated to each VM varies based on load:

- Resources for DPM easyCipher manager depends on the numbers of DPM encryption agents to be managed

Locational considerations that may constrain or influence physical location of deployed VM instances include:

- Network latency

- Disaster recovery planning
- Data sovereignty

4.4 Choosing Deployment Resources

Having determined a logical deployment architecture and a physical deployment design now select the 'flavour' of computing components to implement the design.

A key benefit of the Randtronics DPM product suite is that it runs in standard operating environments (SOE):

- Compatible with industry-standard approaches for increasing resilience and redundancy including standard database synchronization techniques for backend databases, load balancers for applications, etc.
- No special skills or resources required beyond those typical for supporting any other mission-critical enterprise grade applications

Randtronics' customers have the flexibility to deploy DPM on the systems that they find to be most cost effective to acquire, support and manage.

For most customers this boils down to adding in-house deployment of DPM managements modules to their existing fleet of mission-critical applications using existing trusted service providers:

- Many of our customers have well-defined SOEs for mission-critical applications including pre-existing OS and DB volume license arrangements, skillsets and support arrangements.
- For customers with a preference to minimize third party recurring licenses and a willingness to engineer their own mission-critical systems have the option of using Open Source server OS and DB.

Summarizing, defining a deployment design involves a process of determining the customers business requirement, designing a logical and physical design to address this requirement then selecting the component computer resources which are most cost effective for the customer to acquire, support and manage.

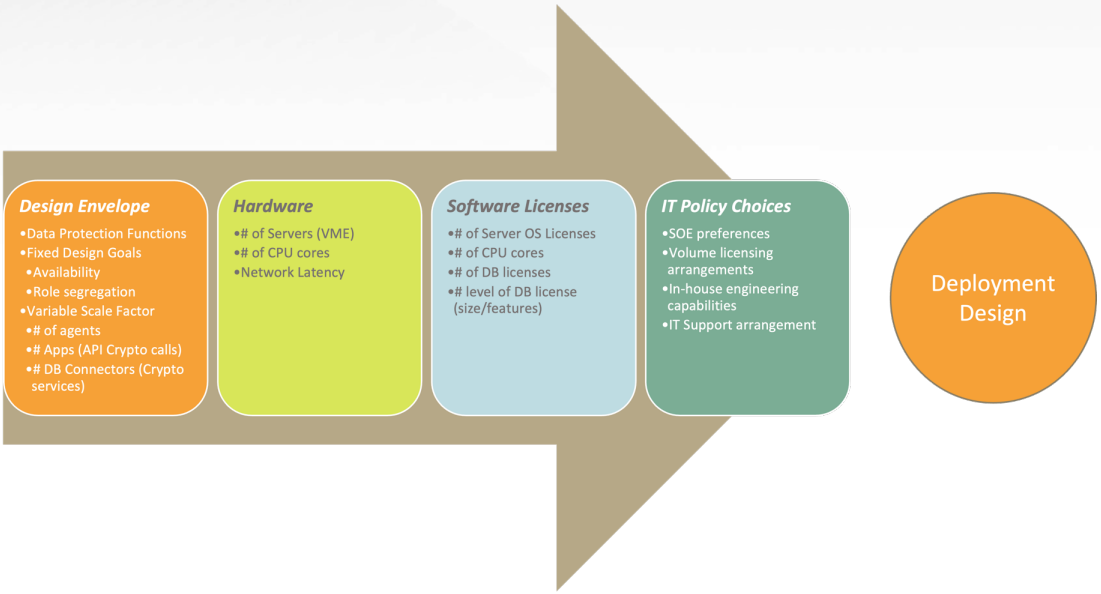

Figure 5 Process for defining deployment design

5. Technology

Randtronics DPM management modules are software applications that run within Apache Tomcat and store their configuration data and audit logs in a backend database.

Randtronics DPM management modules are suitable for deployment on either Windows and Linux platforms (physical or virtual) supported by a backend MySQL or MS SQL Server database to store meta data about its activities.

The following OS versions and editions are supported:

Windows server 2019, 2022 - Windows Server Standard, Windows Server Datacenter

- RHEL – 7, 8
- Ubuntu 18.04, 20.04, 22.04
- CentOS 7, CentOS 8 Stream

The following database versions are supported:

- MS SQL Server 2017, 2019, 2022 - Enterprise, Standard, Developer
- MySQL 5.7, 8 – Community, Standard, Cluster

For customers with a preference for Microsoft technologies a typical high-availability configuration requires:

- Windows Server Standard Edition and
- MS SQL Server Standard Edition

For customers with a preference for Open Source technologies and the capabilities for more advanced in-house engineering, our support for Ubuntu and MySQL 8 enables solution deployment architecture that minimizes third-party license fees.

Typical server configurations for deploying DPM management modules include:

- Single instance
- Two instances in active-active configurations (both DPM nodes are running and accepting connections at the same time)
- Two instances in active-passive configuration (both DPM nodes are running but only one node is accepting connections; if the first node fails then connections are redirected to the second node)
- Three or more instances in active-active configuration
- Three or more instances in active-passive configuration
- Load balancing

Backend database configuration options

DPM managers are stateless allowing multiple DPM managers to point to one database or a cluster of databases. Database clusters should be kept in sync using the database vendors recommended method. For example, using replications or mirroring for MS SQL server or MySQL.

6. Why is Software-only the smarter choice?

The first generation of encryption management systems grew out of the need for vendors of Hardware Security Modules to provide tools to simplify the management of encryption of servers and applications.

Unsurprisingly, it suits the business model of hardware vendors to package their encryption management systems as hardware appliances and tout the benefits of a single-solution ‘all in the box’.

For customers open to thinking outside of the box, Randtronics DPM offers a software-only solution that we believe offers customers a solution that is simpler to implement, more flexible and overall a smarter choice for addressing their enterprise encryption requirements:

Faster to implement:

- Easy download and install of agent software on servers
- Immediate access to DPM easyCloudPlus or easy download and deployment of DPM management modules in-house

- Straightforward to define data privacy and key policies centrally and enforced via DPM encryption agents on target devices and servers

More cost-effective:

- Customers have the flexibility to optimize the performance and cost of their deployment through careful choice of depth of redundancy and selection of technology components to achieve a solution that is both aligned with their specific business needs whilst optimizing to address their individual business resource constraints
- Customers who have already negotiated volume licensing arrangements with Microsoft or Redhat may already have access to the licenses required to construct their deployments consistent with existing Standard Operating Environments without additional recurring license fees
- Customers with strong in-house engineering capabilities may prefer to invest in constructing their architectures from Open Source components such as CentOS, Ubuntu and MySQL to minimize recurring commercial OS and DB license fees

Better longevity:

- Customers can tailor DPM deployments to meet their precise business requirements
- Customers have the flexibility to modify deployment resources over time as business requirements change
- Customers with sovereign location requirements have the flexibility to locate their key stores independently of the servers running their DPM system.

7. Conclusion

Randtronics DPM is designed to make encryption easy. Our products are easy to deploy and manage.

Our Encryption-as-as-Service DPM easyCloudPlus service offers customers the option for near-instant deployment with minimum fuss.

Our easy to download and install DPM management modules offers customers the option to implement and control every aspect of their enterprise encryption solutions within their own familiar standard operating environments.

Randtronics DPM provides customers flexibility, convenience and the freedom to change as their business grows:

- DPM management modules via in-house instance or SaaS
- Design a solution tailored to meet your specific needs for scale, redundancy and role segregation
- Flexibility to design an architecture whose data sovereignty, data-privacy enforcement, resilience, and performance parameters are aligned to your specific business needs
- Support of industry-standard server and database elements enabling you to cost-effectively deploy your design using existing in-house skills, familiar tools and existing IT support arrangements.

8. Appendix: DPM easyCipher deployment examples

Randtronics provides customers the choice deploying the management module component of easyCipher on-premise installation or accessing this function as Software-as-a-Service (SaaS). In either scenario DPM Encryption Agents must be installed locally.

8.1.1 DPM easyCloud Plus SaaS

DPM easyCloudPlus is hosted and managed SaaS offering providing customers instant access to DPM management functionality to manage their locally deployment DPM encryption agents.

DPM easyCloudPlus provides every customer:

- A highly secure DPM management environment that is always available, always backed-up
- High availability options for multi-location redundancy
- Self-managing encryption policies
- Data resides with customer
- Data sovereignty assurance option
- Supported features are as per easyCipher
- Option to outsource day to day encryption key and policy management to Randtronics and its global certified partners.

Encryption-as-a-Service

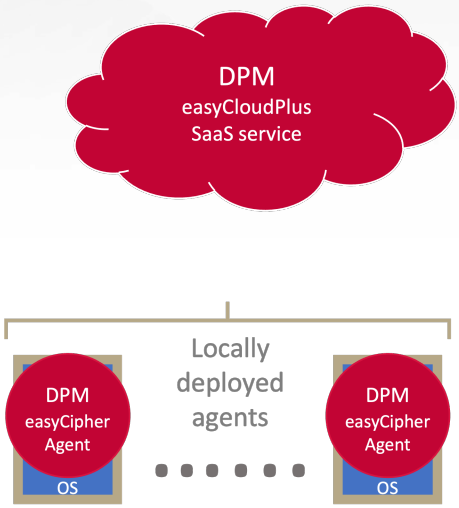

Figure 6 easyCloudPlus Encryption-as-a-Service

8.1.2 Small Environment using Microsoft Windows

DPM easyCipher and backend database are deployed on a single server (virtual or physical).

Typical use cases include:

- Test or proof of concept
- Deployment within minutes – software downloads
- Production use in small deployments
- No redundancy needs as customer uses snapshots and backup/retore routinely
- Customer prefers to use Windows and have in-house Windows technical skills

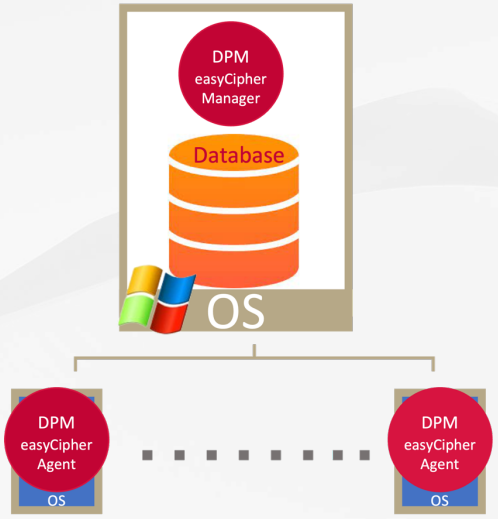

Figure 7 easyCipher Windows small environment

8.1.3 Small Environment using Linux

DPM easyCipher and backend database are deployed on a single server (virtual or physical).

Typical use cases include:

- Similar comments as above
- Customer prefers to use Linux CentOS or Ubuntu and MySQL DB to eliminate recurring OS and DB license fees
- Customer has selected Redhat Linux as their Standard Operating Environment for servers

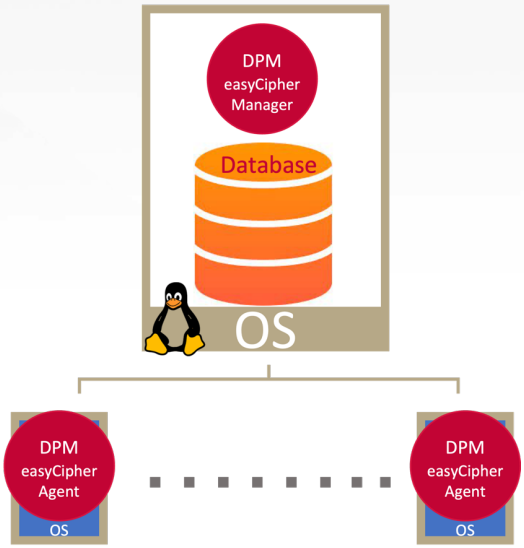

Figure 8 easyCipher Linux small environment

8.1.4 Small Environment with Redundancy

DPM easyCipher and backend database are deployed on two servers in cluster configuration. Redundancy can be built on both Windows and Linux platforms. In total there are 2 VM instances.

Typical use cases are:

- Production use in small deployments
- High availability to 99.9% and higher

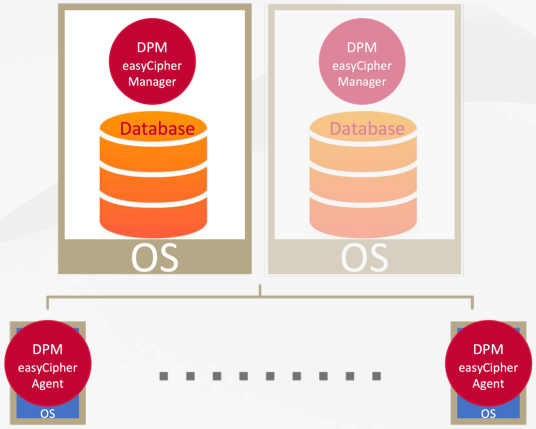

Figure 9 easyCipher small environment with redundancy

8.1.5 Small Environment Minimum Hardware requirements

Computing Resource	*Minimum Configuration*	*Incremental requirements with additional agents in management pool*
CPU	2 cores 2.1 GHz 64 bit	n/a
RAM	8 GB	n/a
Hard disk	60GB	120MB per database encrypted 10MB per end device encrypted

8.1.6 Two-tier Architecture

DPM easyCipher is deployed on one server and its backend database is deployed on a separate server. In total there are 2 VM instances.

Typical use cases include company SOE policy stipulating separation of application and database.

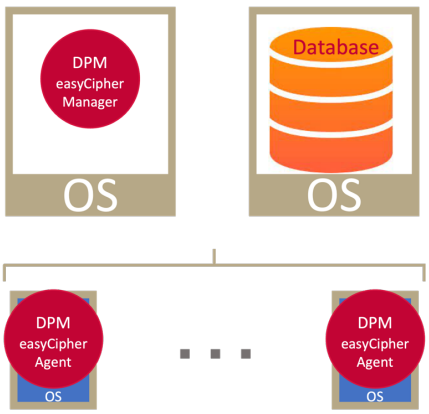

Figure 10 easyCipher two-tier architecture

8.1.7 Two-tier architecture Minimum Hardware requirements

Computing Resource	*Minimum Configuration*	*Incremental requirements with additional agents in management pool*
Application CPU	2 cores 2.1 GHz 64 bit	n/a
Application RAM	4 GB	n/a
Application Hard disk	30GB	n/a
Database CPU	2 cores 2.1 GHz 64 bit	n/a
Database RAM	4 GB	n/a
Database Hard disk	30GB	120MB per database encrypted 10MB per end device encrypted

8.1.8 Two-tier Architecture with Redundancy

DPM easyCipher is deployed on two servers in active-passive or active-active cluster configuration and backend database is deployed on two servers in a cluster/mirroring configuration. In total there are 4 VM instances.

Typical use cases include customers requiring extreme high availability to 99.999% and above.

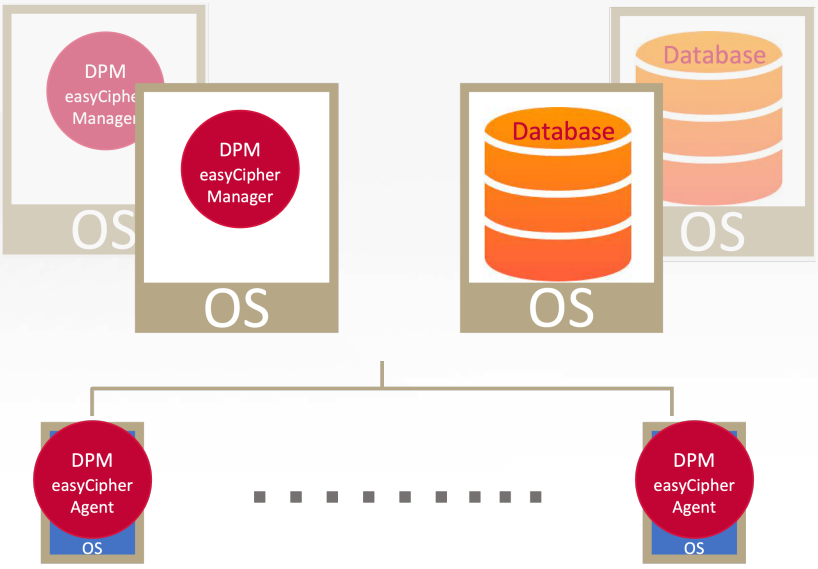

Figure 11 easyCipher two-tier architecture with redundancy

Copyright Information

Contact Randtronics to arrange an evaluation download - **enquiry@randtronics.com**

Randtronics

America: Milpitals, CA. Ph: +1 650 241 2671
Australia: North Ryde, NSW. Ph: +614 1822 6234

www.randtronics.com

randtronics