Date: Feb, 2023

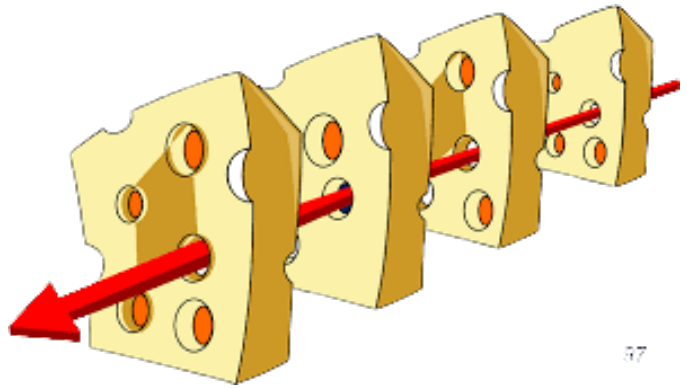
Tamperproof Data Privacy

Protection for your most sensitive data, everywhere

The problem with data privacy protection

- Arms race between data defenders and hackers
- Encryption is the last line of defense…but
- Effective Data protection is only as strong as the weakest link - need to protect data ***everywhere***
- Traditional encryption-solutions are silo-based and assume your IT organization can not be compromised

Complexity and a touch of human error and…

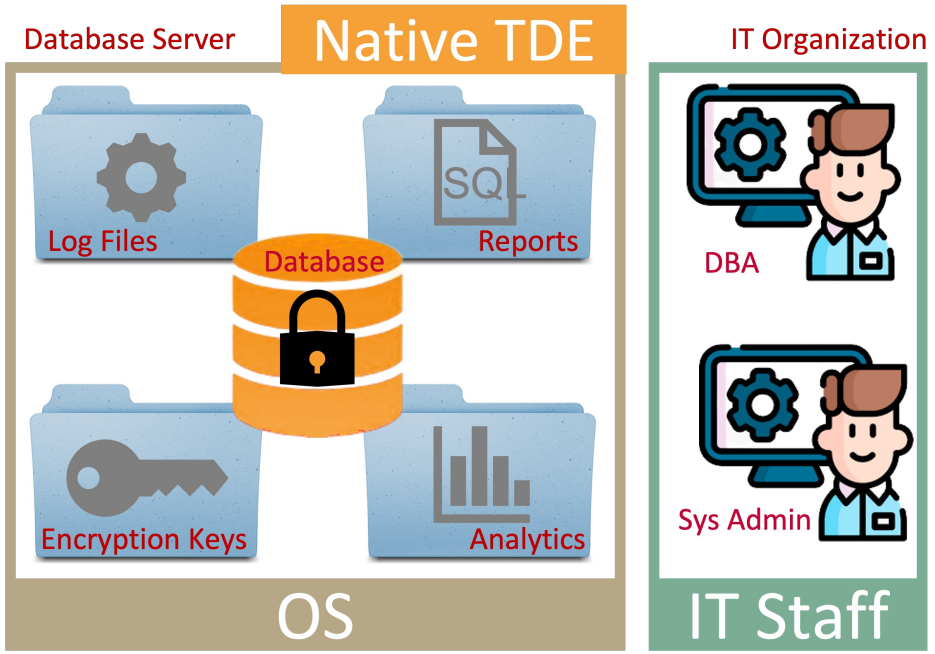


…someone is going to get through eventually

Native TDE protects internal DB data, but not the broader environment

- Echos and traces stored outside on the DB server and shared on other devices such as file server, cloud storage and laptops.
- Attackers can dumpster-dive DB, web app and file servers for reports, test data or analytics systems.
- Privileged DBA accounts (if compromised) can extract or change data and cover their tracks by altering log files.
- Privileged Sys Admin accounts (if compromised) can copy entire DBs, along with their TDE encryption keys

Native TDE protects database contents; broader environment is is somebody else's problem.

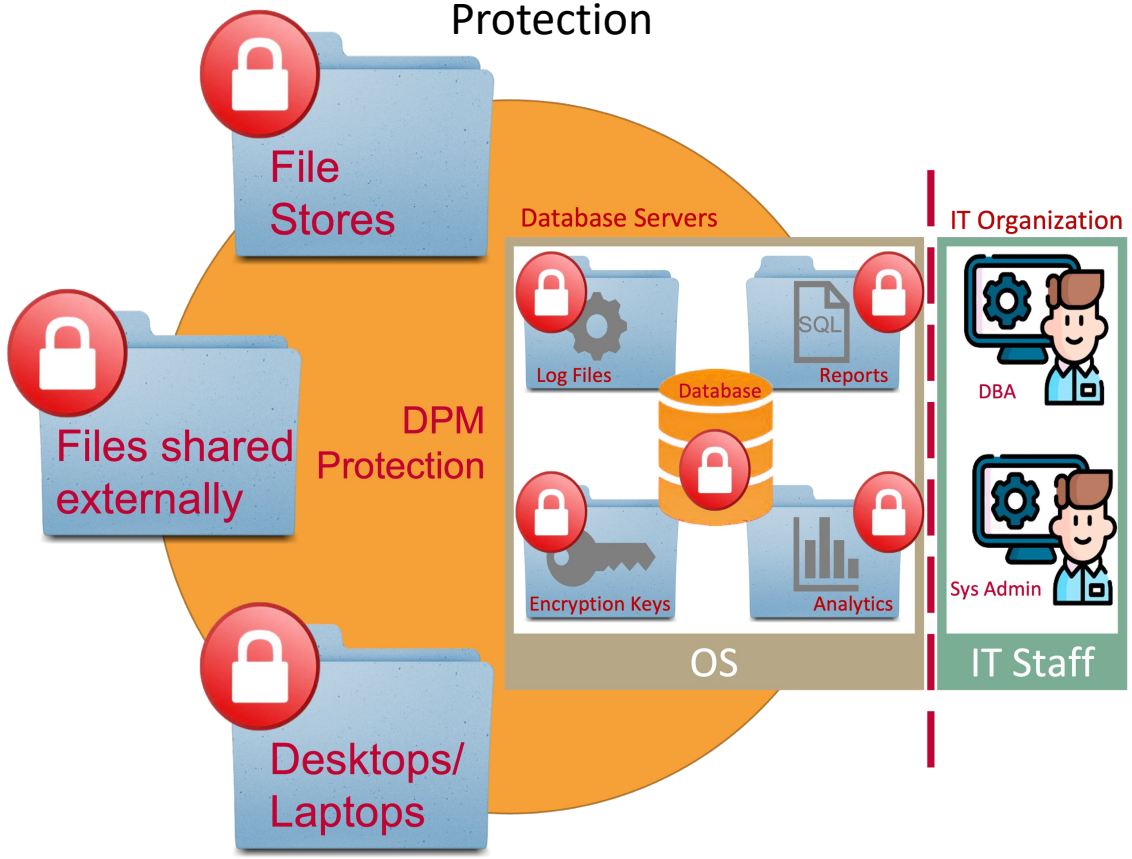


Native TDE = Transparent Data Encryption (TDE) as provided by database vendors

DPM protects your sensitive data, everywhere

- ✓ **Air-gap separation** between your IT organization and your sensitive data
- ✓ **Zero-trust encryption** management system
- ✓ **Standardize encryption management** across multiple DB vendor technologies, web/app servers; and all Windows & Linux VM or Kubernetes container environments
- ✓ **Enhance, extend or replace** native TDE
- ✓ **Policy-based management** of encryption, data de-identification, encryption keys and digital certificates

Randtronics DPM Tamperproof Data Privacy Protection

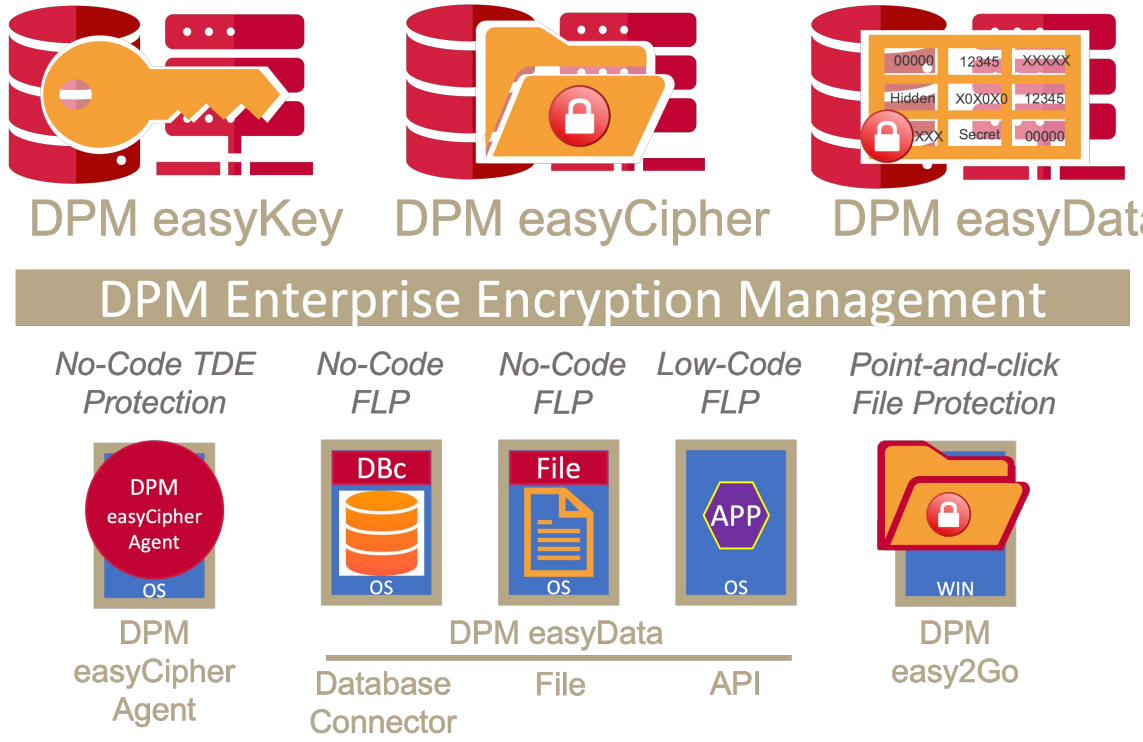


Protect everything, everywhere and isolates sensitive data from IT organization

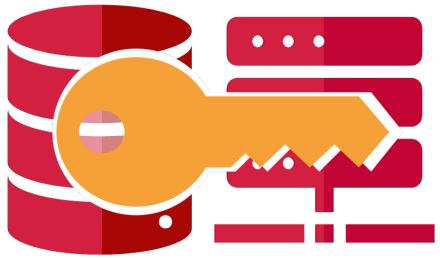
Simplify and strengthen your enterprise encryption protection, quickly, simply with no fuss

- ✓ Standardize encryption management across multiple DB vendor technologies
- ✓ Standardize encryption management for all Windows/Linux VM or Kubernetes container environments on-premise, or on-cloud
- ✓ Standardize key management for all encryption keys and digital certificates
- ✓ Role separation of data privacy protection management with air-gap separation from the IT Organization

Randtronics Data Privacy Manager (DPM)

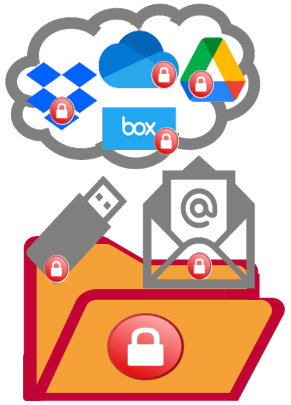


Our Products

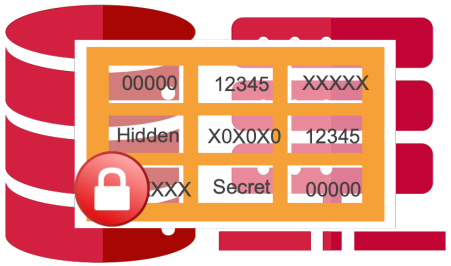


DPM easyKey

DPM easyCipher



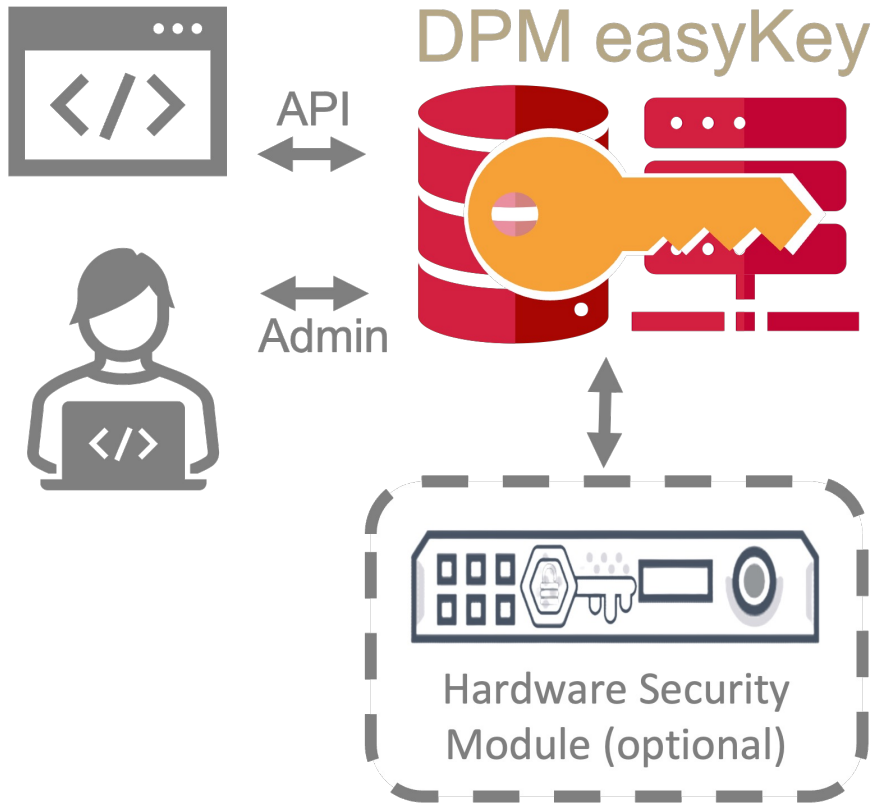
DPM easy2Go



DPM easyData

DPM easyKey – enterprise key management

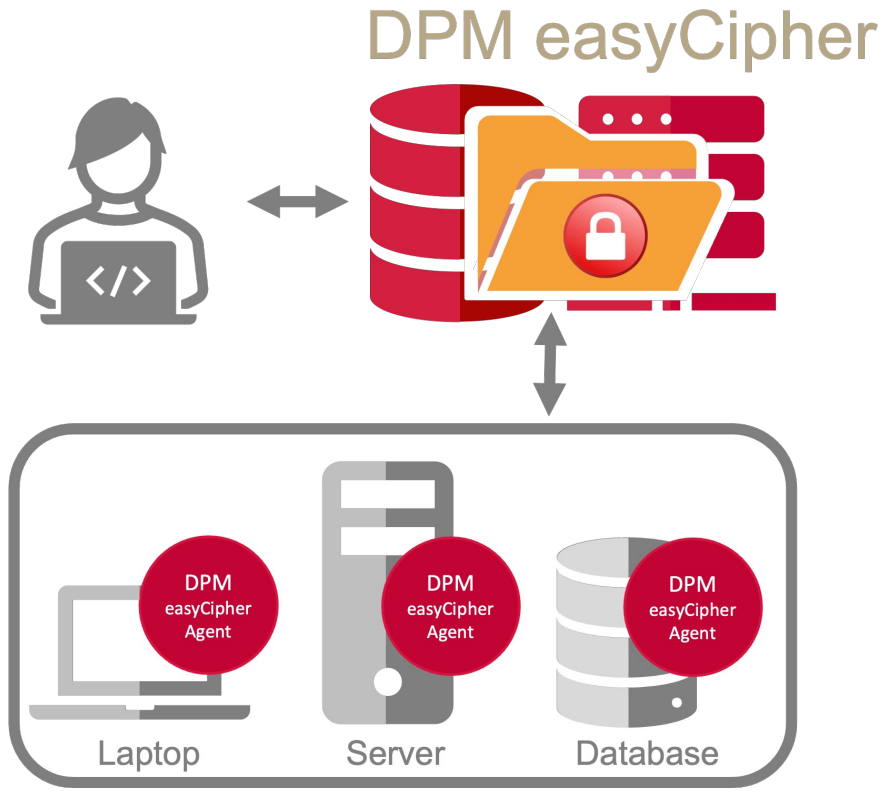
- Provides full key and certificate life cycle management
- Support KMIP protocol and RESTful API for integration with client applications
- Create key generation and access control policies across client applications and multi-vendor HSMs with high key assurance to FIPs140-2/3 Level 3/4 and Common Criteria EAL4+/5+
- Integrates with a cluster of multi-vendor HSM for hardware key generation or Microsoft Azure key vault



Centralized policy-based management of encryption keys and certificates

DPM easyCipher – TDE for databases, files stores and laptops

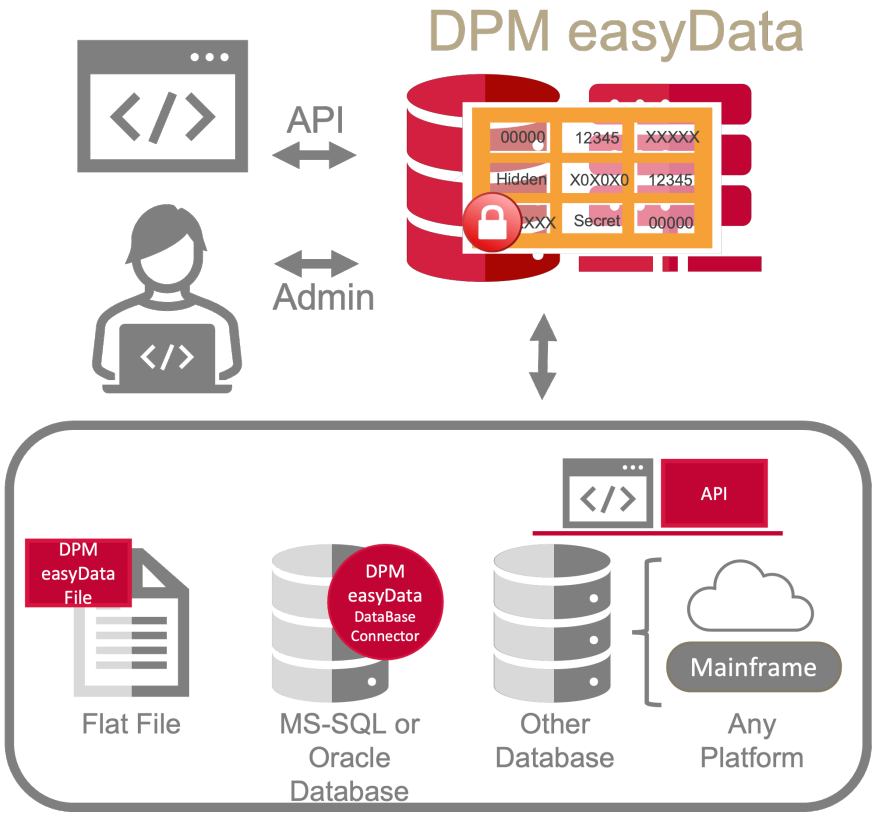
- Provides transparent data encryption of files on laptops and servers
- Supports encryption on cloud file systems.
- Enables transparent data encryption of multi-vendor database
- Centralized managed of security protections – protect from unauthorized users, system administrators and root users
- Integrates with DPM easyKey if centralized key management is required.



Enables users to transparently encrypt files, folders, applications and databases in real time without any code changes

DPM easyData – Field-level Data Protection

- Multi-language pseudonymization, data tokenization, format preserving encryption
- Column level data protection with no application code changes
- Withhold sensitive data from DBAs, software developers, outsourced workers, cloud administrators
- Web service API for client applications to perform
- Full auditing of access to protected data

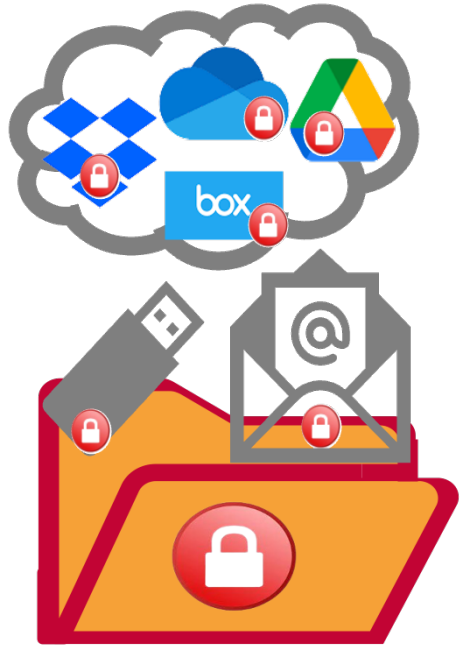


High-performance data-spoofing engine for files, applications and databases

randtronics

DPM easy2Go – safely share files via insecure medium or media

- Protect any file type or folder via password, digital certificate or centrally managed symmetric key
- Works with DPM easyKey for centralized generation and management of policy based digital certificates
- Receiving party also required to install a copy of DPM easy2Go
- Free download for DPM easy2Go reader edition



DPM easy2Go

DPM easy2Go for persistent encryption that follows the file

Software only

Recognizing that most customers have already invested in skills and platforms for running Window/ Linux/ databases environments (SOE), Randtronics has designed DPM as a SOE-friendly, software-only solution for maximum total-cost-of-ownership efficiency:

- ✓ Flexibility, Scalability, Maintainability (so many reasons to pick software over appliance)
- ✓ Standard Windows/Linux skills (only)
- ✓ Plug straight into standard methods for uptime/performance enhancement and management

In short, software is eating the world.

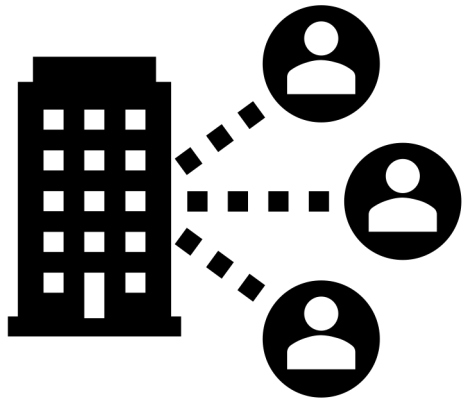
Marc Andreessen
Co-founder Netscape

randtronics

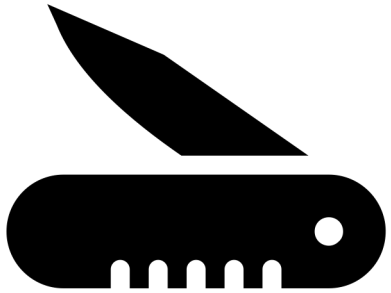
Flexible, quick and simple to Deploy

DPM components are ‘standard’ Windows/Linux/DB apps and as such, are quick and, simple to deploy and cost-effective to manage:

- Lightweight local agents/utilities easy to add to standard build configurations
- Management modules available via SaaS or on-prem installation
- No special skills required (standard Windows / Linux/ database)
- No special architecture (standard methods for backup, n-tier separation and scalability)



Management Modules

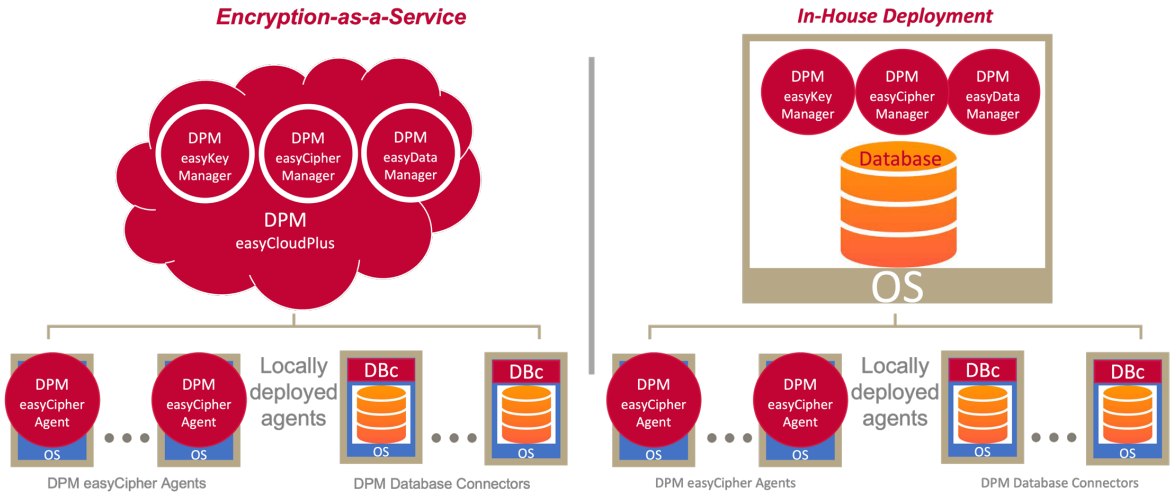


Locally deployed agents and utilities

SaaS or On-Prem

Flexibility, choice and convenience:

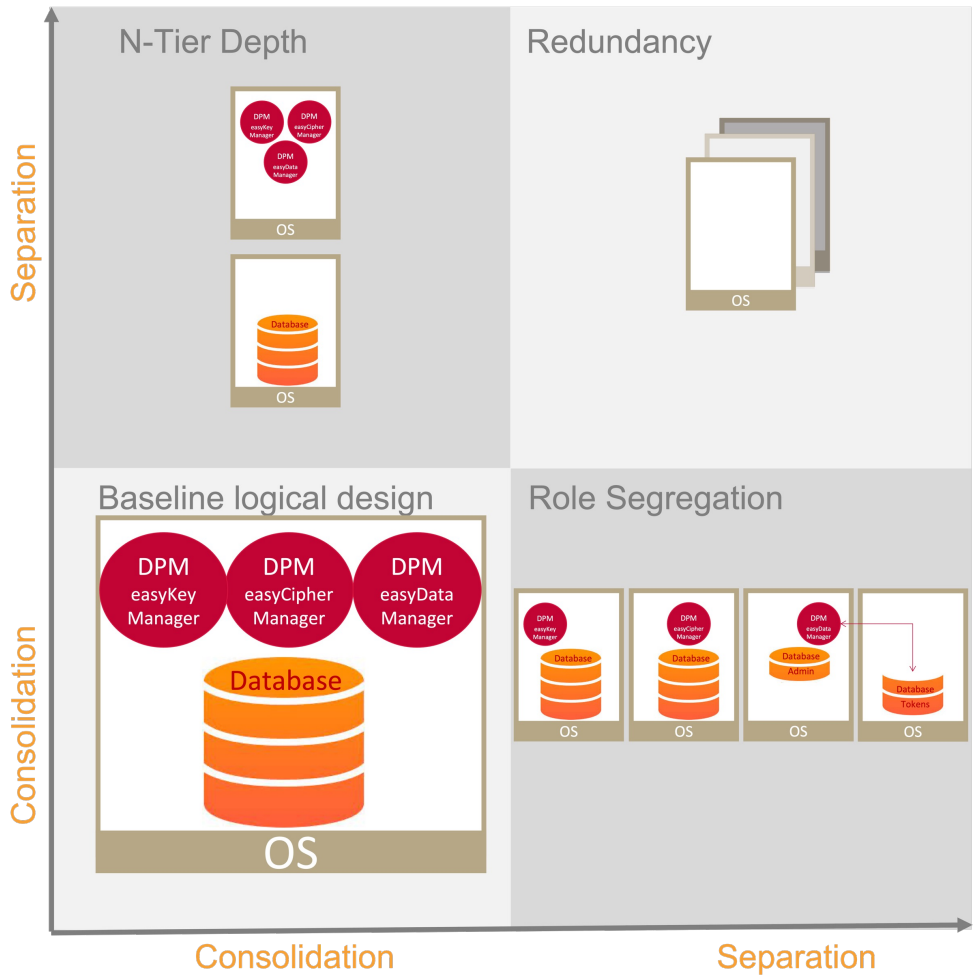
- **SaaS** – let Randtronics take care of running DPM management modules we even offer a full outsource option to run your privacy policy on your behalf
- **On-Prem** – bring it all in-house or under the control of your existing IT service provider. No special skills required.



Standard Methods

Being normal Windows/Linux software applications, standard methods for backup, n-tier separation and scalability apply.

Customer benefits from existing investments in skills and platform for cost-effective management of enterprise applications.



Randtronics LLC

Milpitas CA 95035 United States
+1 (650) 241 2671
enquiry@randtronics.com

Randtronics Pty Limited

S1.1, Level 1, Building A 64 Talavera Road
North Ryde, NSW 2113 Australia
+61 418 226 234

Thank you for your time

email: bob.adhar@randtronics.com

Cell: +614 18 226 234 or +1 650 241 2671