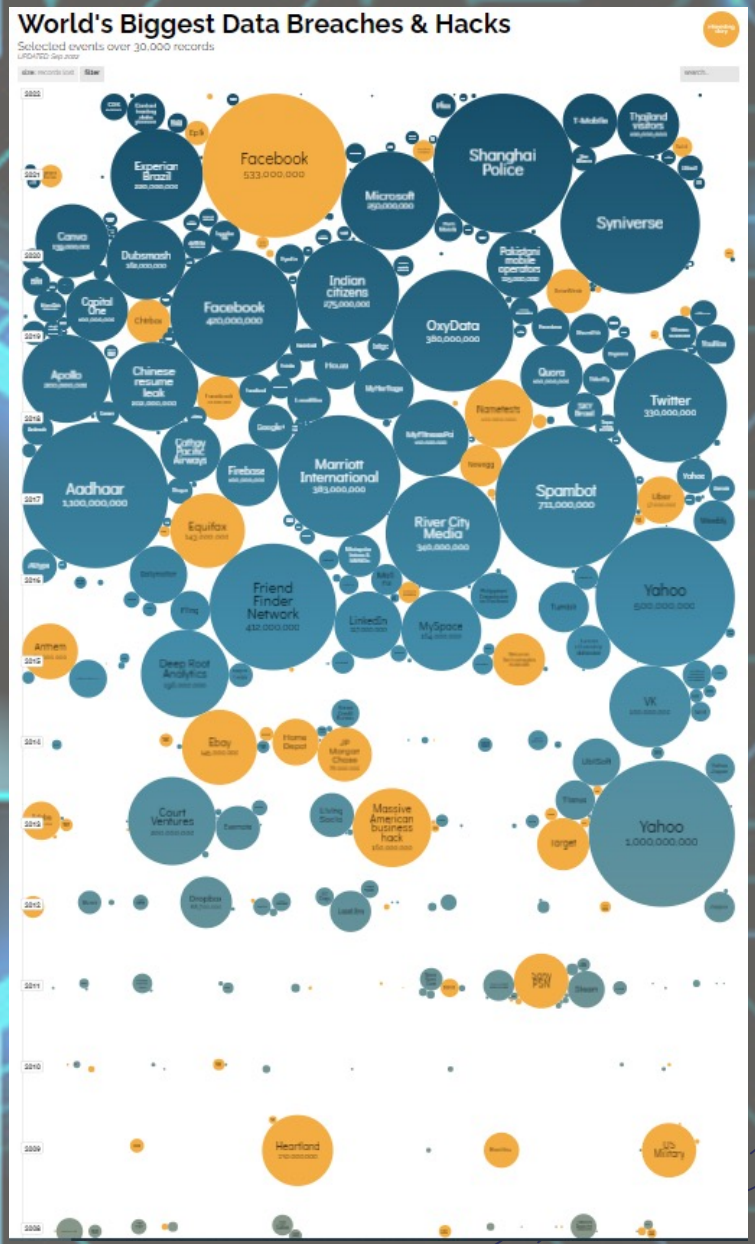
White Paper
Encryption and Field-Level Data protection:
Fortifying your last line of defense

Information is Power

Businesses are amassing data on their consumers, employees, suppliers, and competitors.

Data breaches are becoming more prevalent.

2022

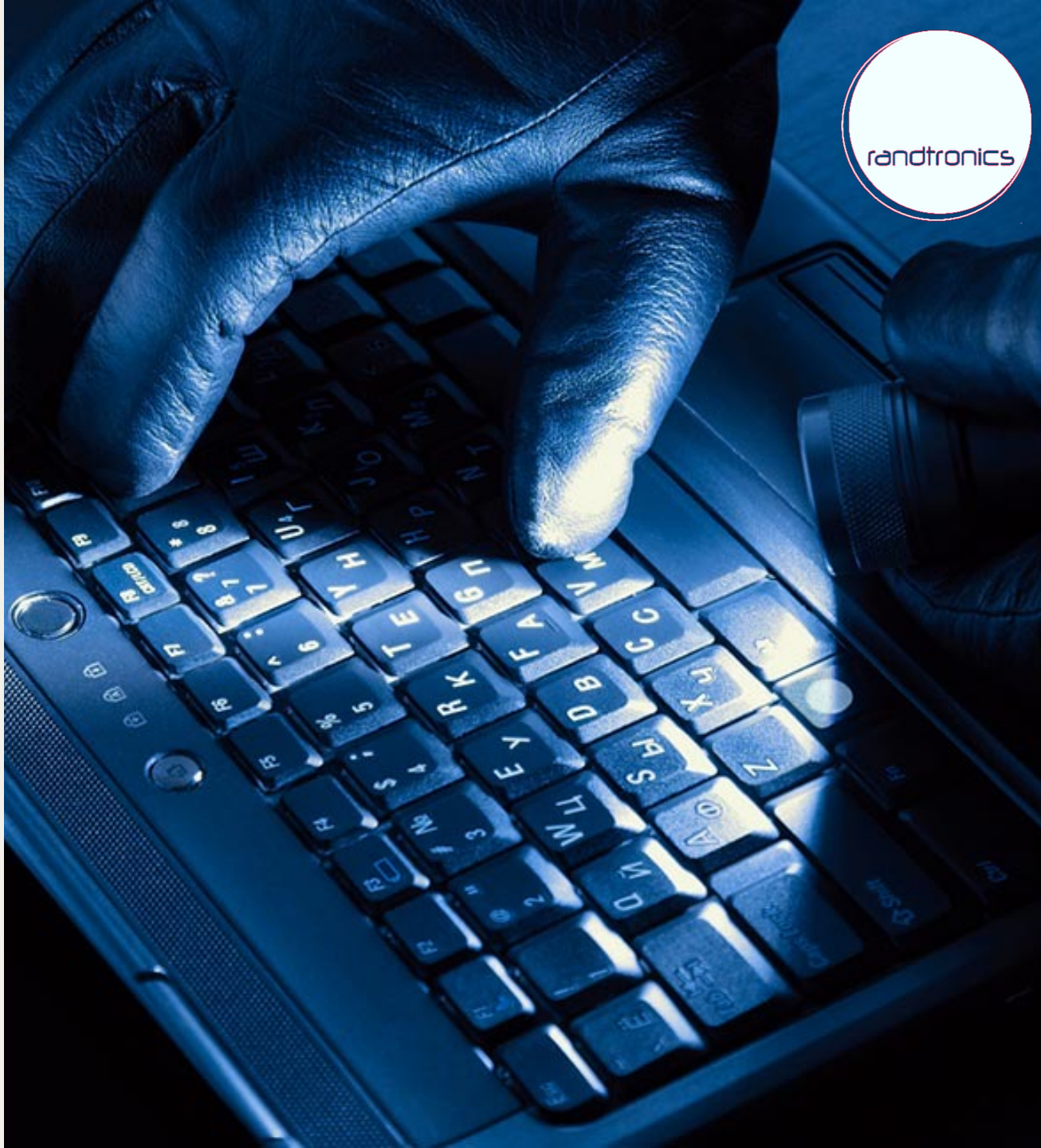


2004

World's Biggest Data Breaches & Hacks, source [Information is beautiful](https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/) https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Times Have Changed

People used to be terrified that their money might be snatched physically from their possessions. Now, in the year 2023, the true danger comes from hackers who are stealing your information on the internet.

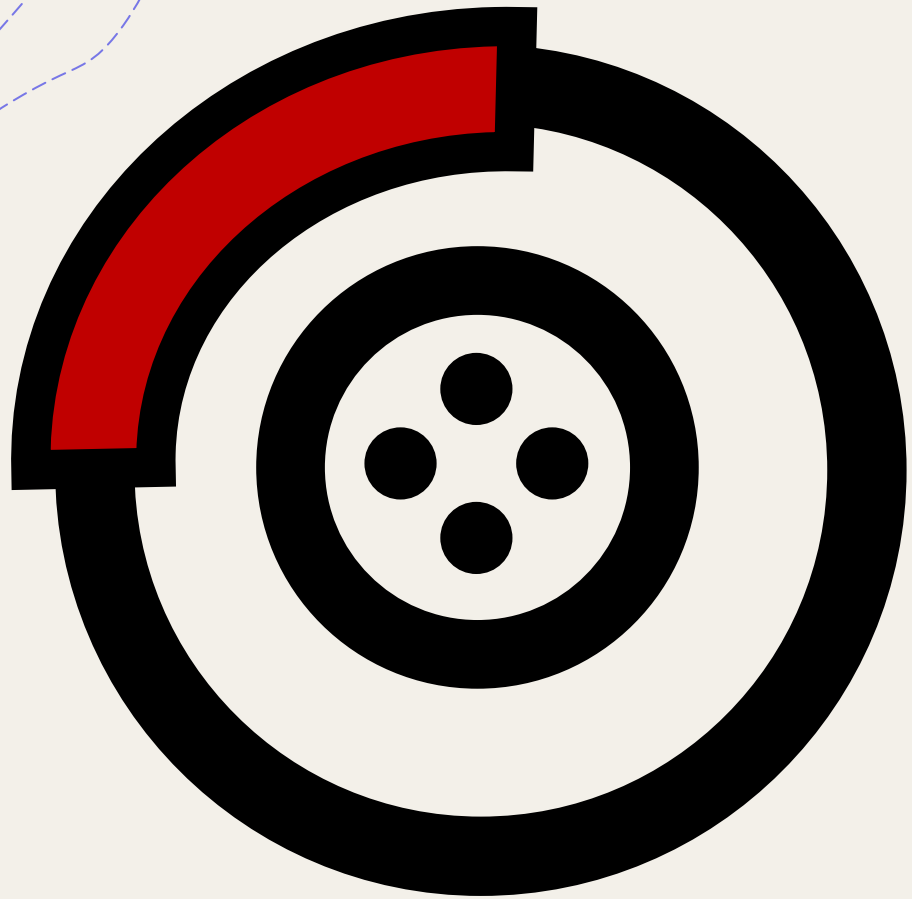


Delays discovering data breaches

The average time required to uncover malicious assaults is over six months (IBM Ponemon Report), which can result in irreversible brand harm, financial loss, customer churn, share price decline, or the permanent liquidation of your organization. According to HIPAA, only encryption eliminates the risk of health records being breached.

C-Level executives are liable

Breach of data is no longer solely an IT issue. “Board members and the C-suite can no longer ignore the drastic impact a data breach has on company reputation” (Experian). Encryption prior to a breach indicates the highest concern for a customer's sensitive data. If you can demonstrate to regulators that you employed encryption following a breach, you eliminate financial exposure, safeguard your reputation, and keep consumer loyalty.



Preventing incidents becoming disasters

- Everything is going digital and online
- Accelerating pace of change
- Hacking attacks are multiplying
- Can’t always keeping the bad guys out
- Encryption is the last-line of defense
- The *emergency brake system* to stop sensitive data loss when all else fails

Encryption is essential

randtronics

IT Security focuses on the wrong areas

Organizational resources are mostly invested in protecting the perimeter – not your data

Breaking through firewalls is easy

Professional hackers can penetrate most firewalls easily

Encryption is hard to crack

Using 256-bit length keys, AES has 2^{255} possible key combinations that could take 3 x 10^{51} years to break

Encryption of data eliminates legal liability and stops breaches

Penalties are increasing for organizations that fail to protect personal data

Lose personal data you may face risk penalties and criminal charges:

+ GDPR fines up to €20m or 4% of revenue.
+ Lots of companies being fined in Europe, US….

But if you are using encryption effectively:

+ reduces the risk of a breach in the first place, AND
+ provides a valid legal defence to avoid against penalties if a breach occurs

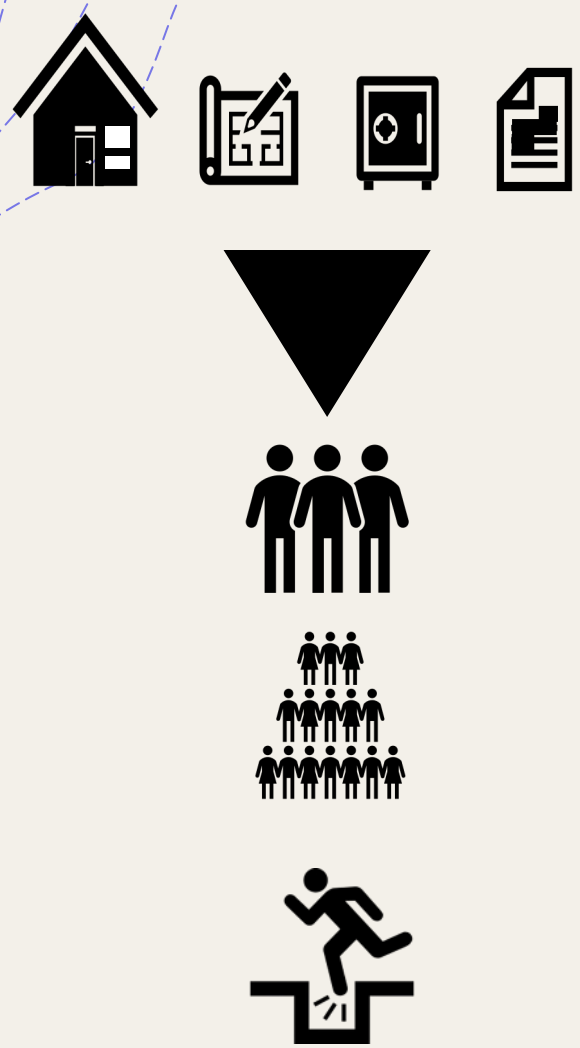
A sound encryption strategy strikes the right **balance** between protection and access

Strong (enough) Data Protection

Everywhere

Whilst
Minimizing Business Friction

Foundational concepts – Encryption 101



- **Object Level** – what level of object are we protecting?
- **Method** – its not just encryption: choosing the right data privacy method
- **People** – are we achieving protection AND still allowing people to do their jobs?
- **Scale-Up** – how well does our protection system work when scaled up across the organisation
- **Gaps** – are closing gaps where sensitive data might leak?

Why use a safe, if you have locked the front gate?

When something is really valuable, we use multiple levels of protection

Q1: What 'thing' are we protecting?

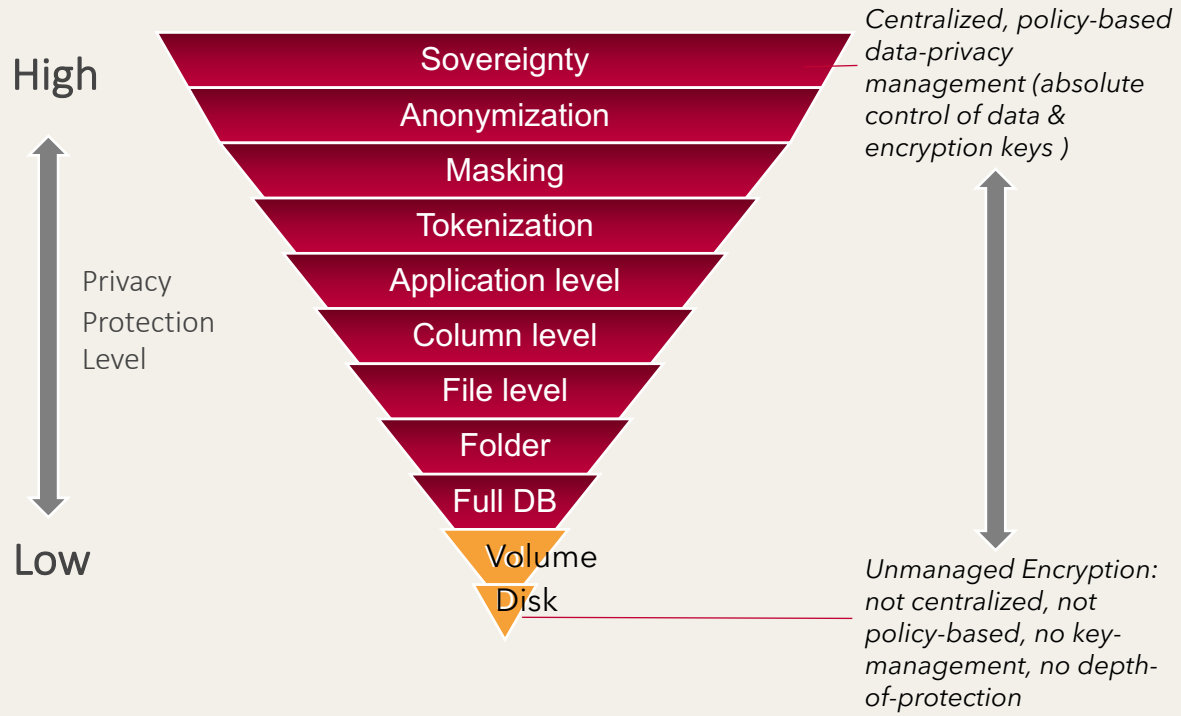
House Room Box Document

Just having encryption doesn't ensure effective protection:

+ 'House' - Full Disk Encryption Encryption: Unlocked the front-door and anyone can get in
+ 'Room' – Volume Encryption – unlock the room door and anyone can get in
+ 'Box' – File/Folder Encryption – protect secrets from others in house/room
+ 'Document' – redacted document shares information but protects secrets

One size doesn't fit all. Need to select the method that effective protection without interfering with business operations

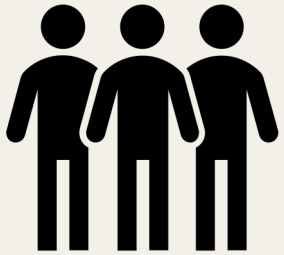
Q3: How best to protect a specific data in a specific context?



Data Privacy Protection Methods

Access control determines who has access to what – data protection enforces the rules

Q3: Who has access (to What)?

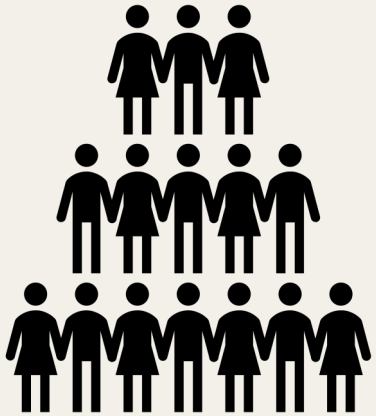


Data secure organizations enforce the ‘least access’ principle:

+ Fine-grain access control of who has access to what
+ Data-masking, enabling valid use whilst shielding non-pertinent sensitive data
+ Minimum access necessary to perform role

To be effective, a data protection system needs to scale-up to protect the entire organization

Q4: How to ensure consistency, everywhere?



Data secure organizations use policies & platforms to standardize protection … everywhere

+ Policies: standardizing protections for data … and.. for encryption keys
+ Platforms: to automatically implement policies everywhere --- ideally across all systems, all locations, all people

Auditability – visible demonstration of compliance and effective protection

Privacy protection is not effective if data can leak through gaps

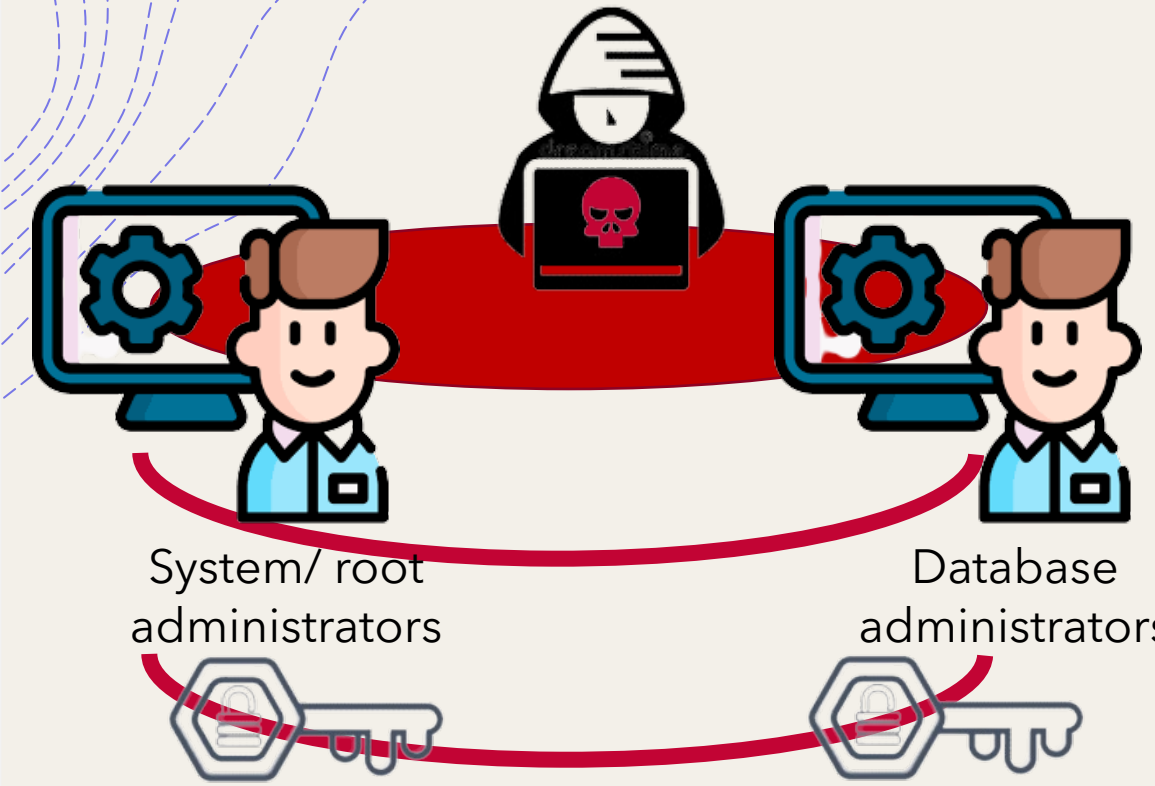
Q5: How to avoid gaps?

Mind the gap

Common gaps include:

- Privileged users able to bypass data privacy controls
- Patchworks of data privacy systems with pockets of unprotected data
- Separately managed data protection silo's that need to be manual kept in-step

Protecting against privileged users

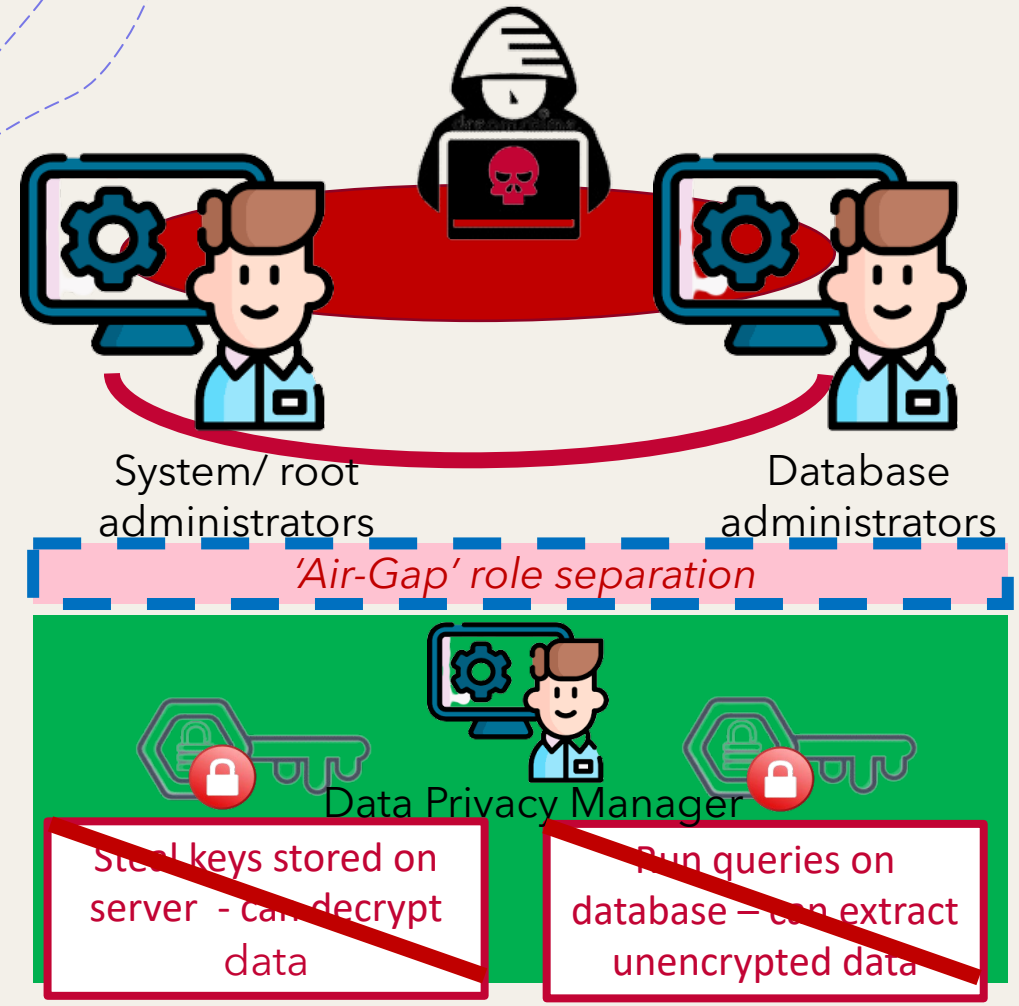


Steal keys stored on server - can decrypt data

Run queries on database – can extract unencrypted data

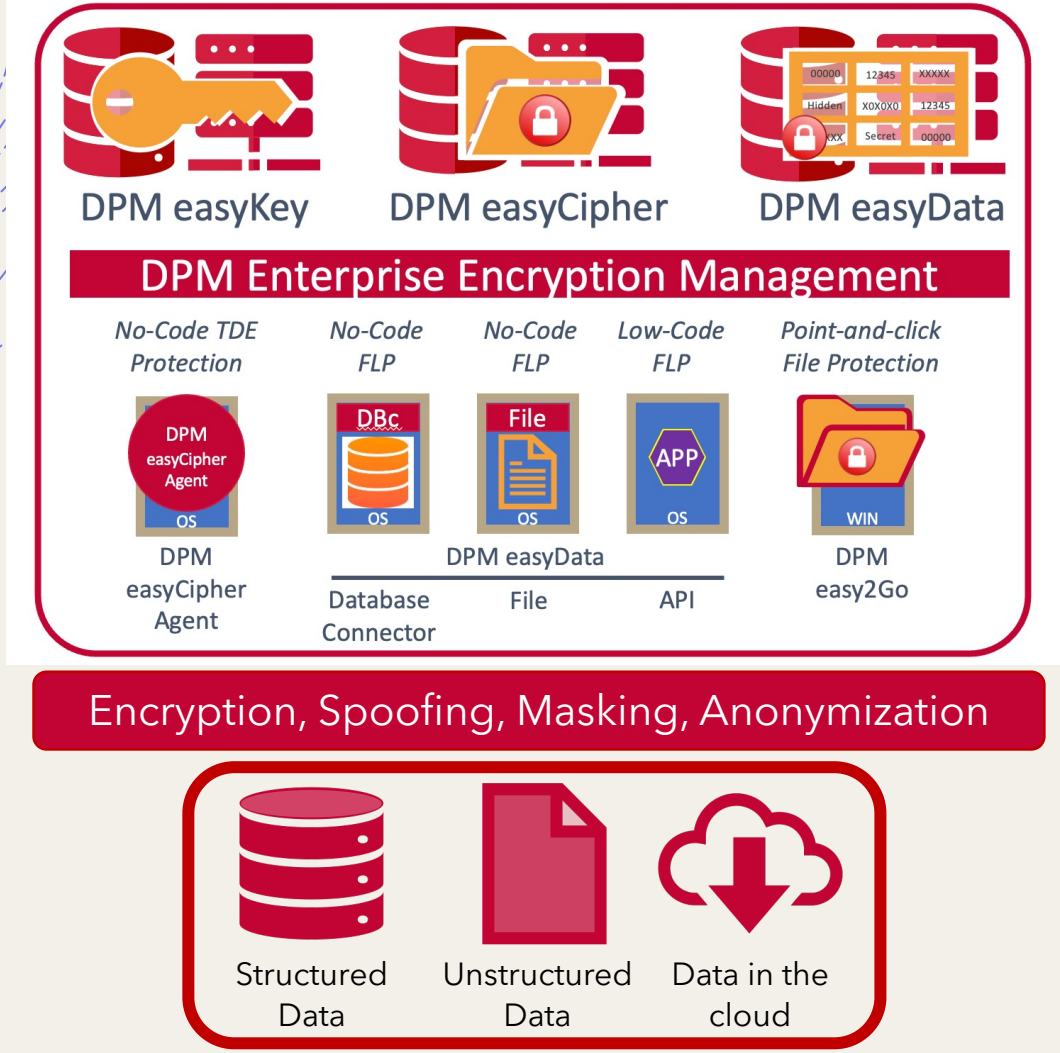
- Once inside, hackers hunt for privileged user credentials
- Native encryption tools built inside database products can be bypassed
- Databases administrator can run queries to extract underlying data
- System administrator can find keys stored on server and copy database
- Best strategy – trust no-one

Need to isolate sensitive data from privileged users



- A Zero Trust Encryption that operates independently of file systems, databases and applications
- 'Air-gap' role separation stops a compromised privileged user accessing sensitive data or keys
- Data management team has exclusive responsibility for encryption policies and operations across whole organisation

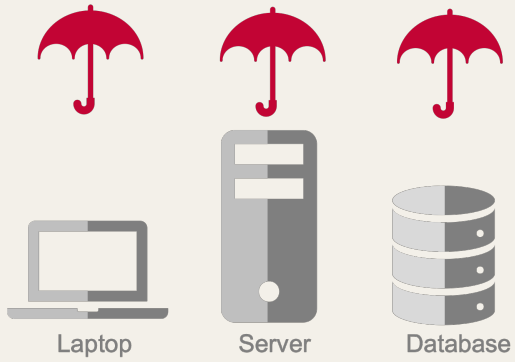
Randtronics DPM:
Data Privacy Manager



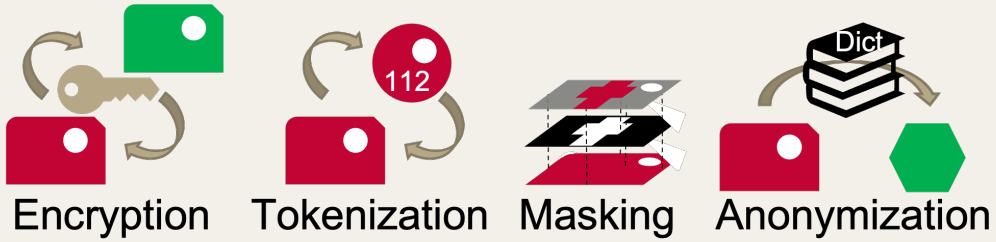
Introducing: Randtronics DPM

- DPM unifies and simplifies encryption across file systems, databases and applications
- Encryption occurs outside of database
  - Uniform protection for all environments
  - Encryption complexity handle by DPM
  - Not reliant on deep knowledge across all platforms
- Data privacy team empowered to define and implement encryption policies for the whole organization

Randtronics DPM:
Transparent Data Encryption



Randtronics DPM:
Field-Level Data Protection



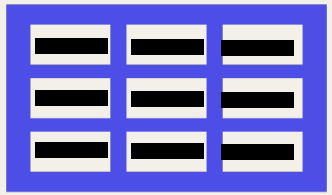
Full range of Protection options

- Transparent Data Encryption (TDE)
  - Object-level "whole of file" protection of files, folders and databases
  - Fine-grained, policy-based access control
- Field-level Data Privacy (FLP)
  - Field-level protection of data fields and database columns
  - Full range of protection methods
  - Works with Databases, Flat files and applications

Field-level encryption and other forms of data protection

Encryption

Document



Database

Data de-identification

Masking Anonymization Tokenization

Encryption – offers the strongest form of protection for column/field level data however:

+ Format preservation option enables use with strongly-typed DB fields, but
+ it is pretty hard to operate if all data remotely sensitive is 'blacked out'

Data de-identification - non-encryption methods for protecting content in databases and files:

+ Masking – pattern partially or fully replaces data
+ Pseudonymization – real data replaced with safe but still somewhat useable data. Can be potentially defeated by assembling multiple data sources to re-identity an invididual
+ Anonymization – real data replaced with safe data but unusable data.
+ Tokenization – voucher/ 'cloakroom ticket', substitute data with a token

Example

Name: Mary Stewart
Gender: Female
eMail: Mary.Stewart1542@gmail.com
Bank Account Number : 9578 2318
Credit Card: 4487 8239 271

Name: Robert Scott
Gender: ###
eMail: ####.#####1542@gmail.com
Bank Account Number : #### 2318
Credit Card: 9987 3621 349

Anonymized name:

+ Picked from a dictionary of names.
+ De-identify gender
+ Remains easy for human staff to work with
+ Complies with name field validation rules

Masked - gender, email, bank account number:

+ Data obscured in an obvious way
+ Mask selected to protect information whilst enabling staff to perform role
    + Last 4 digits of bank account
    + Distinguish between email addresses
    + Recognize domain address

Tokenized Credit Card

+ Substituted number that satisfies data type rules
+ Original data stored with token in token vault

Provides Protection-in-depth

Different tools for managing different risks:

- **Physical theft** – disk or volume protection is great but can become a helpdesk nightmare in absence of Enterprise Key Management
- **Hacking** - fine-grain data privacy controls mitigate downside of a compromised ID
- **Sharing** – Masking/ Anoymization enables safe sharing of data for analytics, customer service, testing without disclosing sensitive information

Randtronics DPM: Zero-Trust Encryption made easy

Performance

Will systems run slower after encryption?

Randtronics DPM uses proven methods and systems of Windows, Linux, database, cloud and hardware accelerators where user experience before and after encryption is the same

Randtronics DPM: Zero-Trust Encryption made easy

Deployment

Will we need to change software code for applications to use encryption? What about ROI?

Randtronics DPM deployment is transparent and reduces scope of compliance and business risk

Randtronics DPM: Zero-Trust Encryption made easy

Availability

Is my data lost forever if encryption fails? What safeguards are available? What about reliability and availability?

Randtronics DPM uses familiar proven systems and methods of load balancers, disk mirroring and database clustering for automated backups and redundancy used by businesses for decades

Randtronics DPM: data protection - made easy

Usability

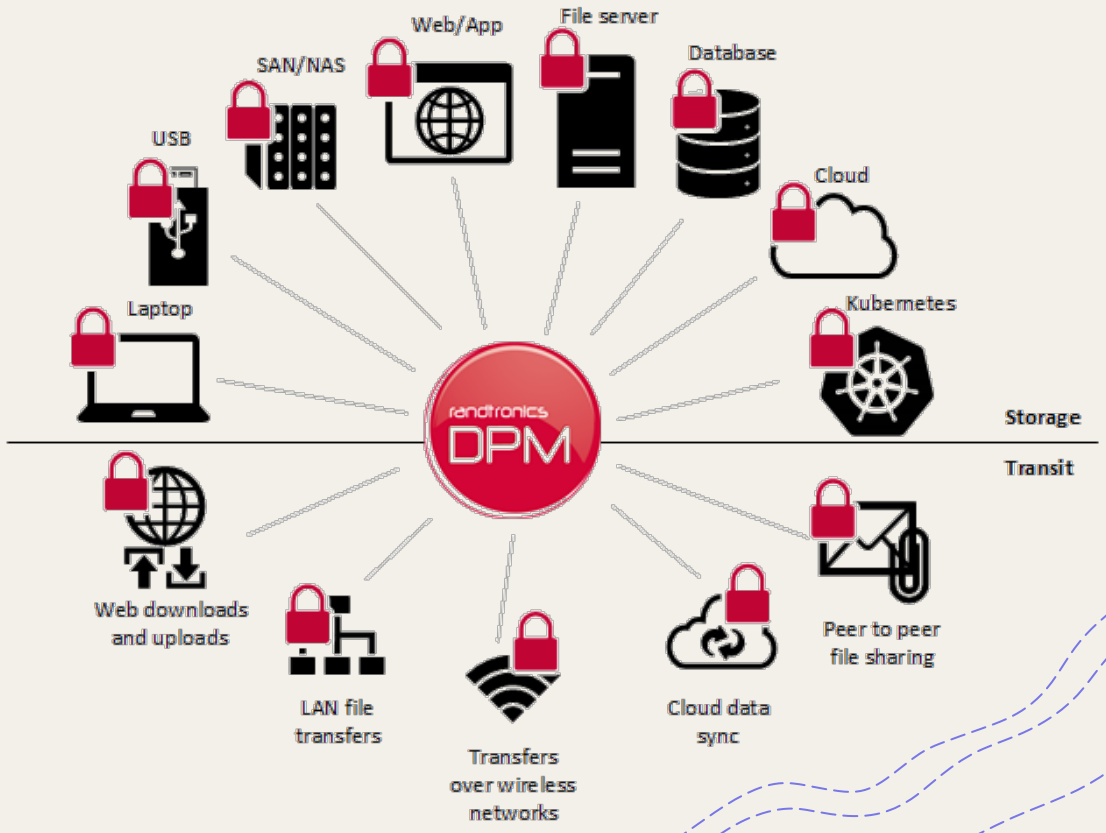
Will encryption require retraining due to changed business processes? What about ease of use?

DPM is easy to use and requires no business process changes, as it uses familiar Windows/Linux/database technologies and transparent data encryption integration

Randtronics DPM data protection - made easy

DPM is easy to deploy and use

DPM transparent data encryption and spoofing requires no software code changes and supports laptops, servers, any application, multi-vendor databases, Kubernetes containers, on-prem and multi-vendor clouds. DPM SaaS offering enables outsourcing all to Randtronics

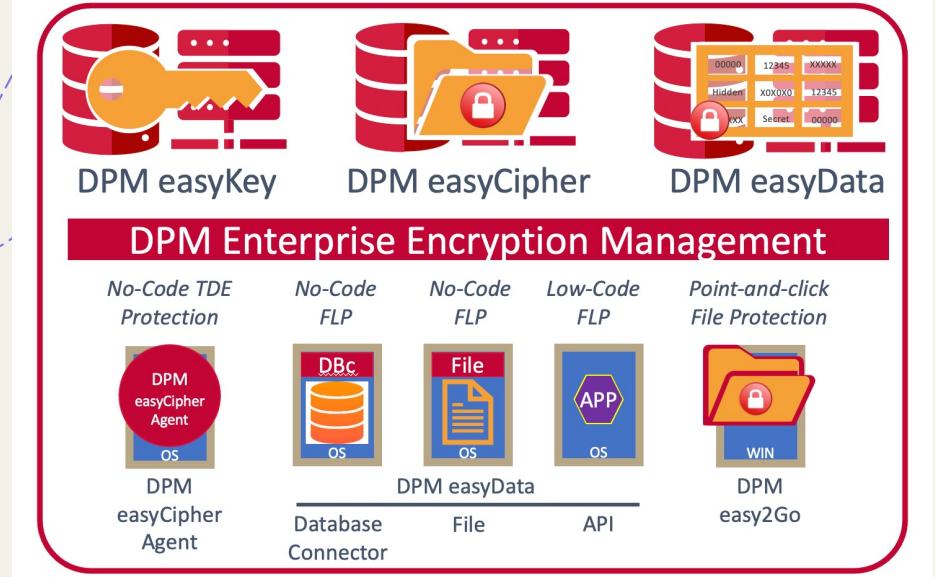


Randtronics DPM: data protection - made easy

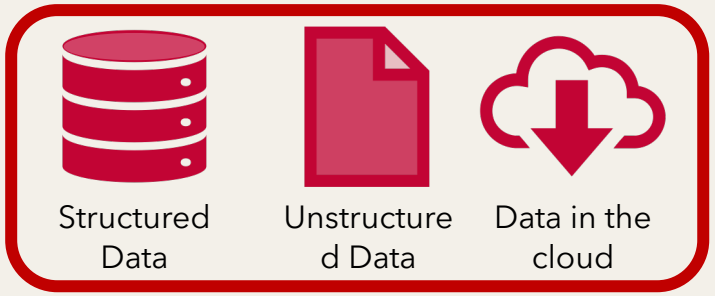
Rapid Return-on-Investment

DPM enables reduced compliance scope and lower operational costs, through better management of risks associated with privacy, compliance, employees, contractors, outsourced workers, remote workers and public cloud usage

Data Protection – made easy



Encryption, Spoofing, Masking, Anonymization



DPM is *your toolkit* for achieving comprehensive data protection:

- ✓ **Works Everywhere:** Enterprise-wide protection. On premise, in the cloud and within hybrid deployments.
- ✓ **Does Everything:** Comprehensive and adaptable data protection toolkit.
- ✓ **Easy to install:** Deploys quickly and easily, with little to no impact to the network
- ✓ **Easy to staff**: deployed using standard operating systems and databases. Easy to administer without special skills. *No encryption expertise required.*

randtronics