# GDPR and Beyond…..


**Manoj Bhati**

Pre-Sales Consultant

# Agenda

- GDPR Text
- Gemalto’s Six Step by Step Approach
- Gemalto Vision
- Authentication
- Key Management
- Crypto/Data Protection
- Questions

# GDPR Text

# GDPR Text

- SECTION 2: DATA SECURITY
- ARTICLE 30: Security of processing

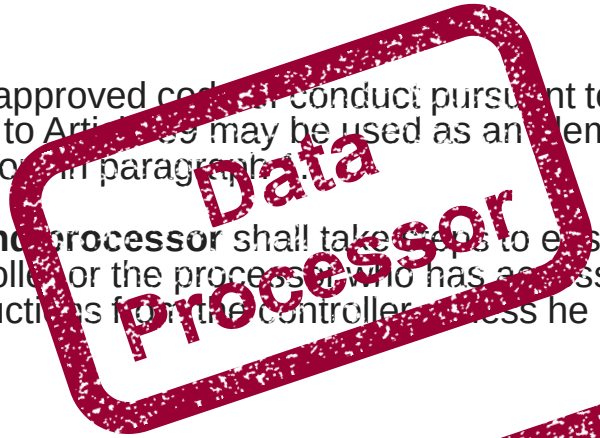
1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall **implement appropriate technical and organisational measures**, to ensure a level of security appropriate to the risk, including inter alia, as appropriate:
   (a) the pseudonymisation and encryption of personal data;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
   (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1a. In **assessing** the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

# GDPR Text

2a. Adherence to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.

2b. The **controller and processor** shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.




- ARTICLE 31: Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, **notify the personal data breach** to the supervisory authority competent in accordance with Article 51, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.

GDPR EXPLAINED

# Step by step

# Overview

- 1. Legal framework / Understand GDPR
- 2. Create roadbook / Data register
- 3. Data classification
- 4. Start with top priorities
  - 4a. Procedures & Policies
  - 4b. Data protection
- 5. Assess & document other risks
- 6. Revise & repeat

# Gemalto vision

# Different types of attacks

- Low skill and Low Focus
  - Go for low hanging tools. They normally look for whatever data is available easily.
- High skill and Low Focus
  - These are the attacks that we normally hear about in news
- High Skill and High Focus (single focus attacks)
  - These are single focused attacks with a very specific reasons.

# A new mindset

SECURE THE BREACH

| | |
|---|---|
| 1 **Accept the Breach** | **Perimeter security** alone **is no longer enough**. |
| 2 **Protect What Matters, Where It Matters** | **Data** is the **new perimeter**. |
| 3 **Secure the Breach** | **Attach security** to the **data** and **applications**. Insider threat is greater than ever. |

**Gemalto Research: www.breachlevelindex.com**

# Three Pillars

# Authentication

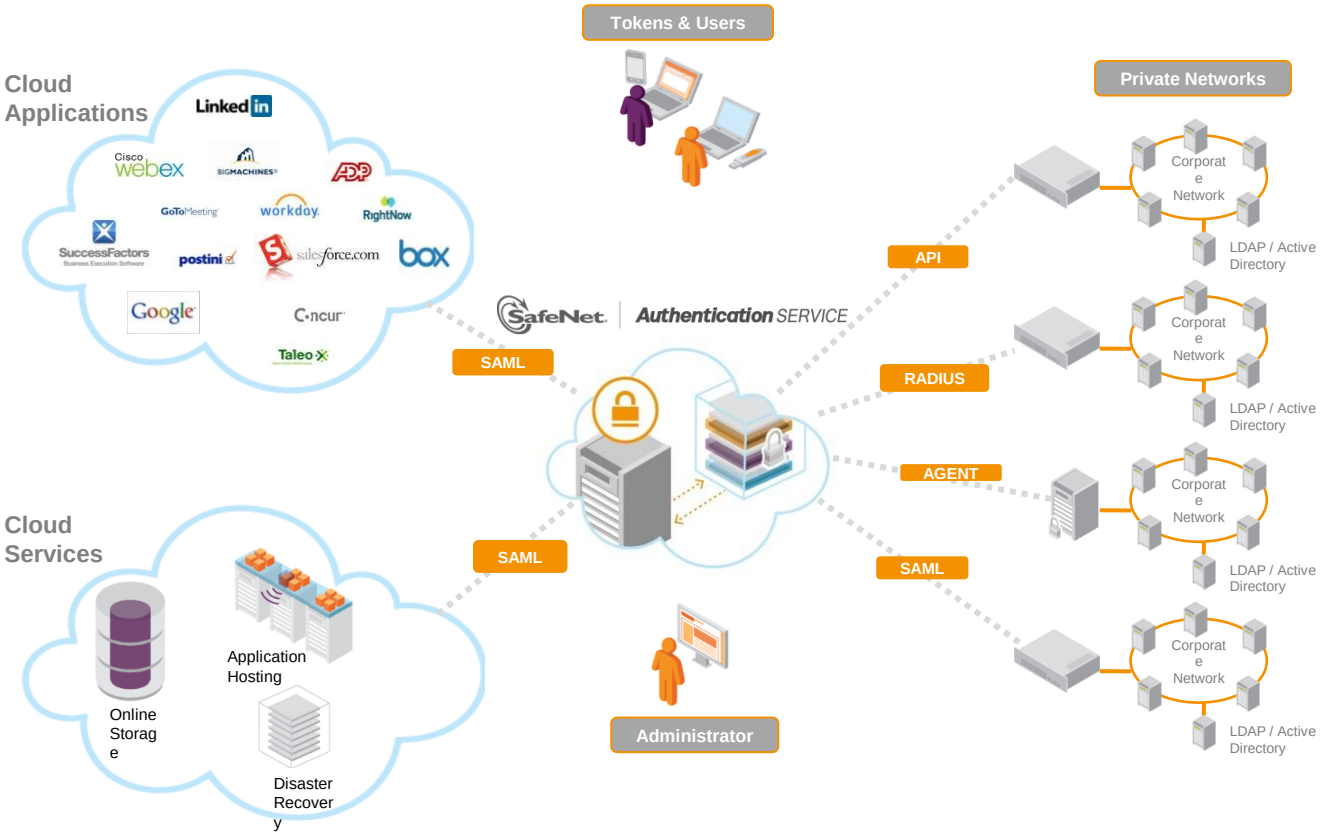
# Why two-factor authentication?

- Audit trail for GDPR compliancy
  - **who accessed**
  - **at what time**
  - which information
- Reduce risk for stolen credentials
  - Breach prevention

# SafeNet Authentication Service by the Numbers

- **Over 4.000.000 users of Cloud Edition**
- **30 minutes to set up**
- **400+ fully-tested integrations**
- **60% lower TCO than other solutions**
- **99.999% Availability SLA**

# Protect Everything and Everyone, Anywhere



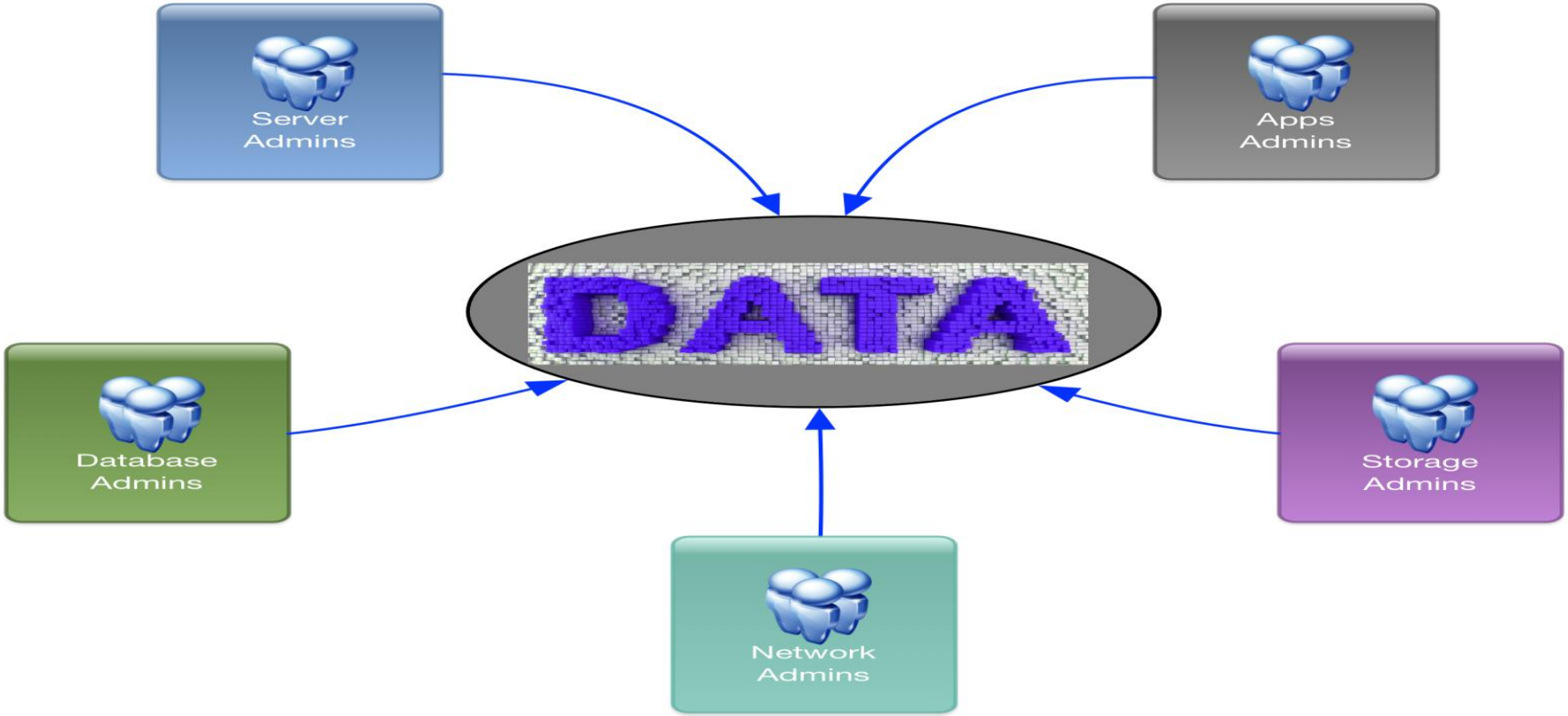
GDPR EXPLAINED

# Key Management

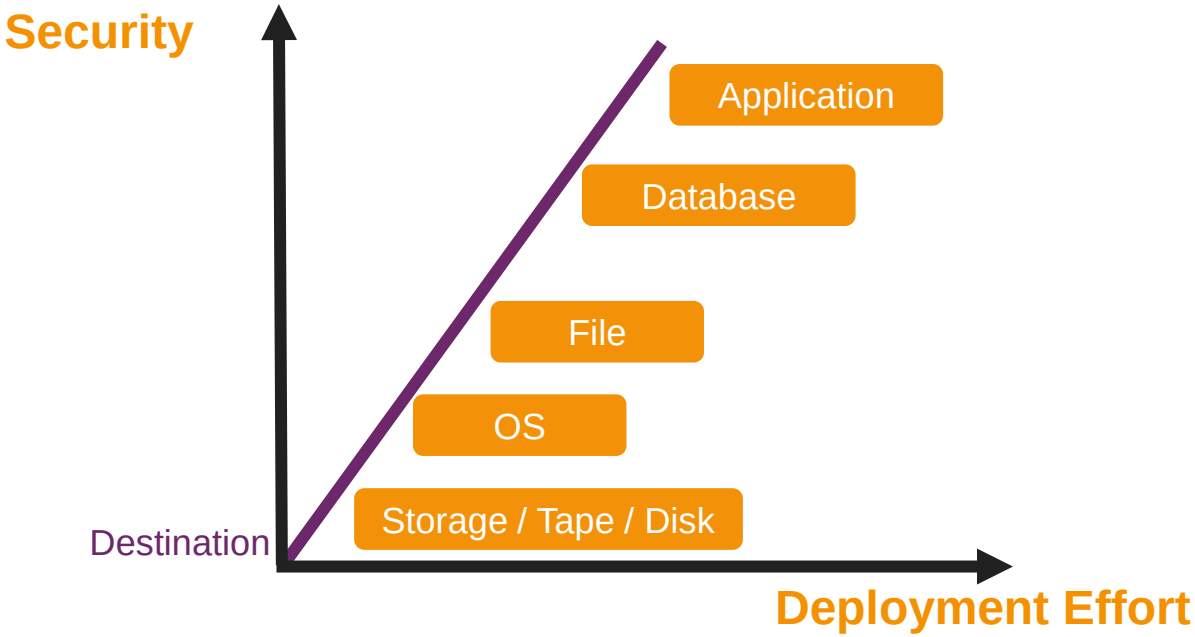
# Why Key Management?

- GDPR States to encrypt data
- However when encrypting data:
  - Data is no longer important
  - But Key Management is!

# Who are you protecting against?



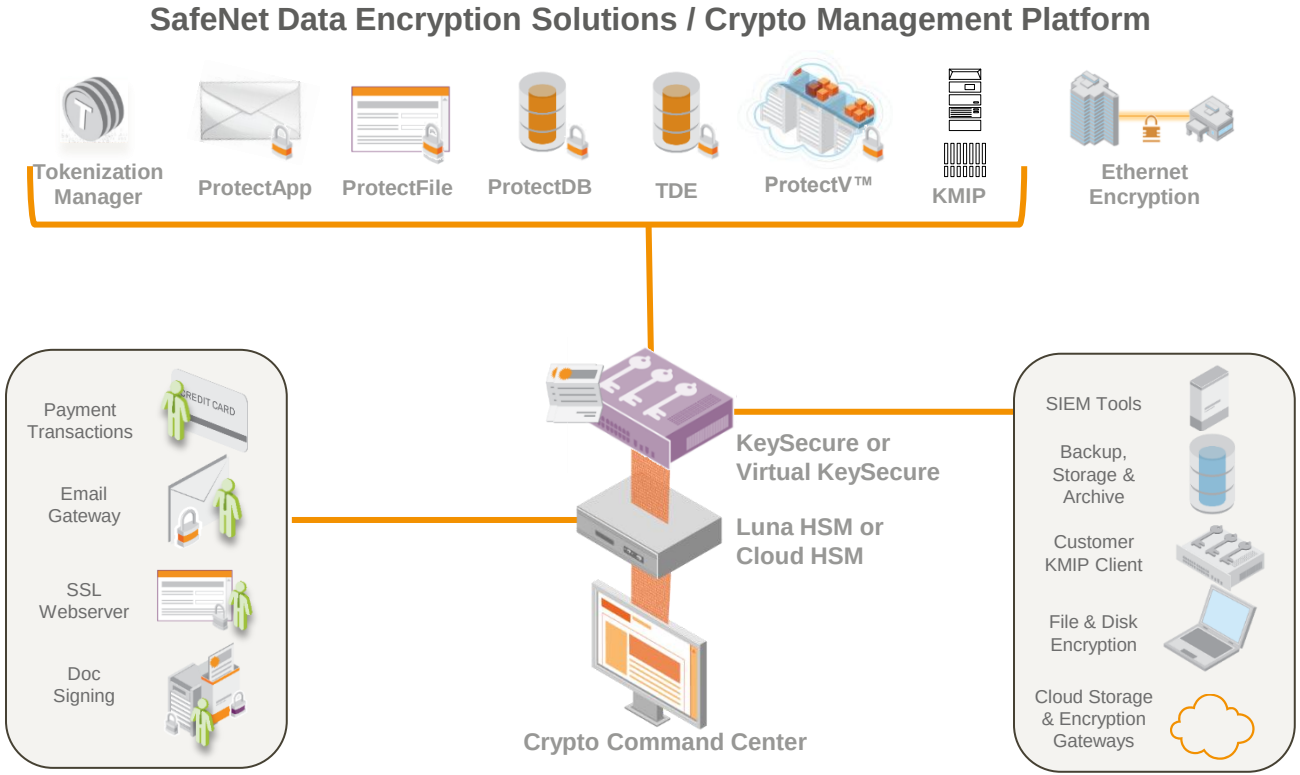
# The Right Kind of Protection



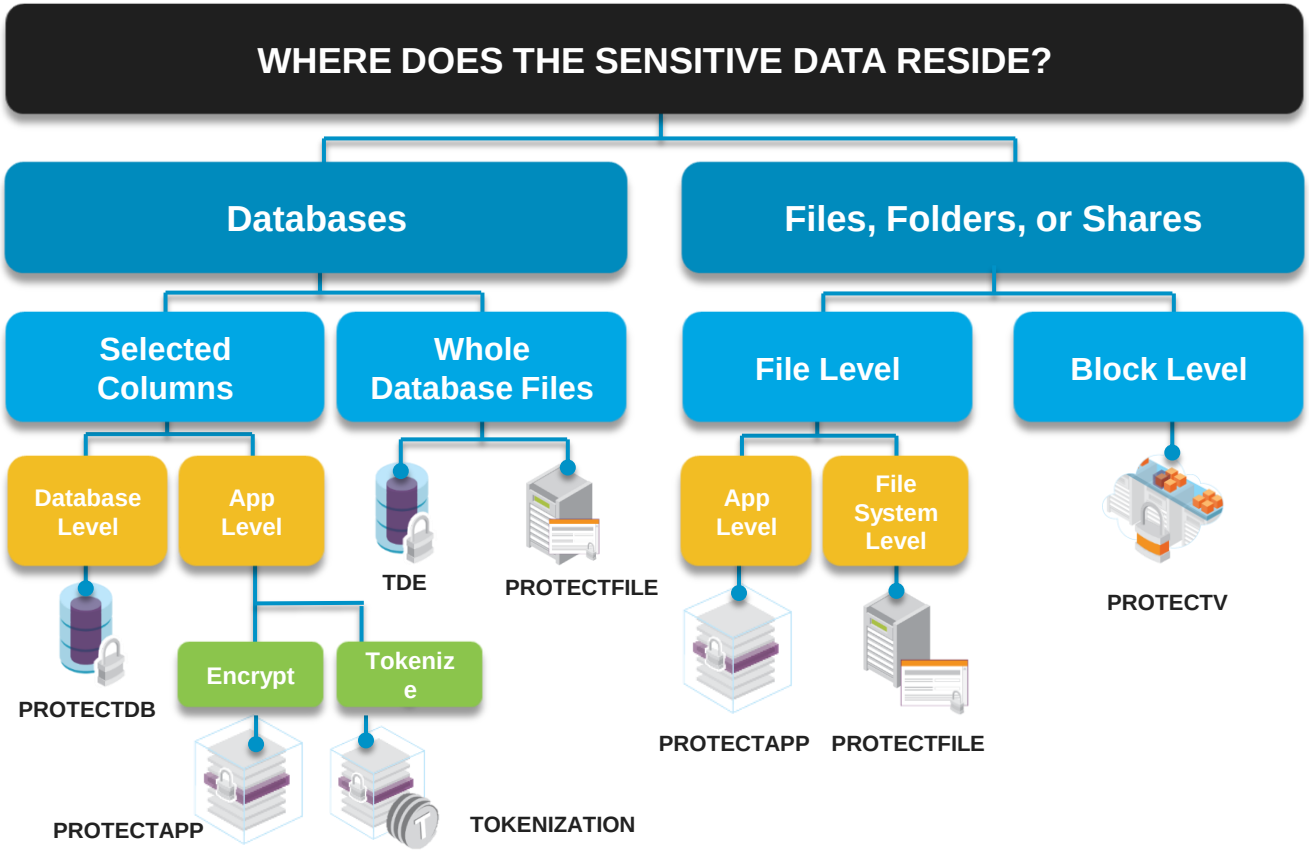

“Many organizations understand the benefits of encryption … but have difficulty on the question of just where to encrypt the data?.”

Jon Oltsik, Senior Analyst, Enterprise Strategy Group

# A new mindset



# The Right Connector For Every Use-Case




gemalto

# Crypto / Data protection

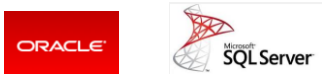
# Why encryption?

- Lost or stolen data in terms of GDPR
  - Only breach notification
  - No user information duty
  - No secrets revealed
  - No bad publicity
- Less business impact
- Breach prevention

# Top HSM Use Cases

- Public Key Infrastructure


- Transparent Data Encryption

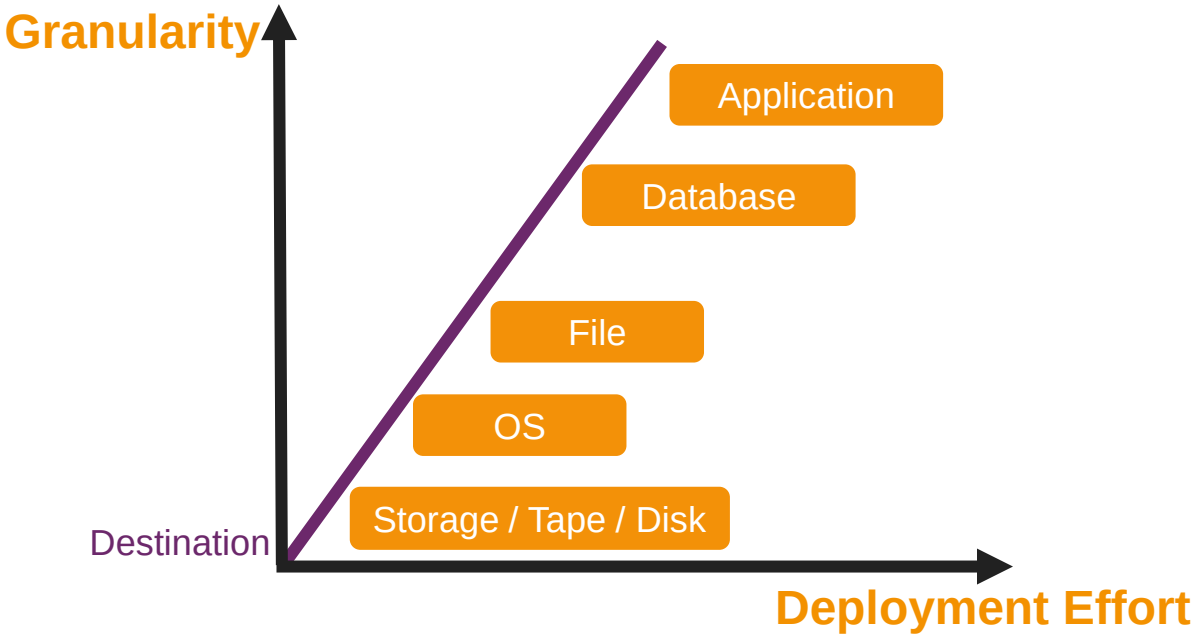



- SSL/TLS Private Key Protection


- Code Signing


- Data Protection for Cloud Apps

# Threats vectors




“Many organizations understand the benefits of encryption … but have difficulty on the question of just where to encrypt the data?.”

Jon Oltsik, Senior Analyst, Enterprise Strategy Group

# Just to avoid this …


https://www.c-span.org/video/?c4578124/opm-ssn

# Questions?

GDPR EXPLAINED

# Thank you