TREDISEC Project and Framework

Overview

March 2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

About TREDISEC

Trust-aware, **Re**liable and **Di**stributed **I**nformation **Se**curity in the **C**loud

WHY?

Constant **conflict** between **functional, non-functional cloud requirements**, and **security concerns**

AIM

End-to-end security primitives supported by a unified **framework**, which contribute to **increase trust** in **cloud providers** and **facilitate compliance** to **security** and **privacy requirements**

3 Year Duration

6,5 M€ of Budget

Financed with **H2020** Research Funds

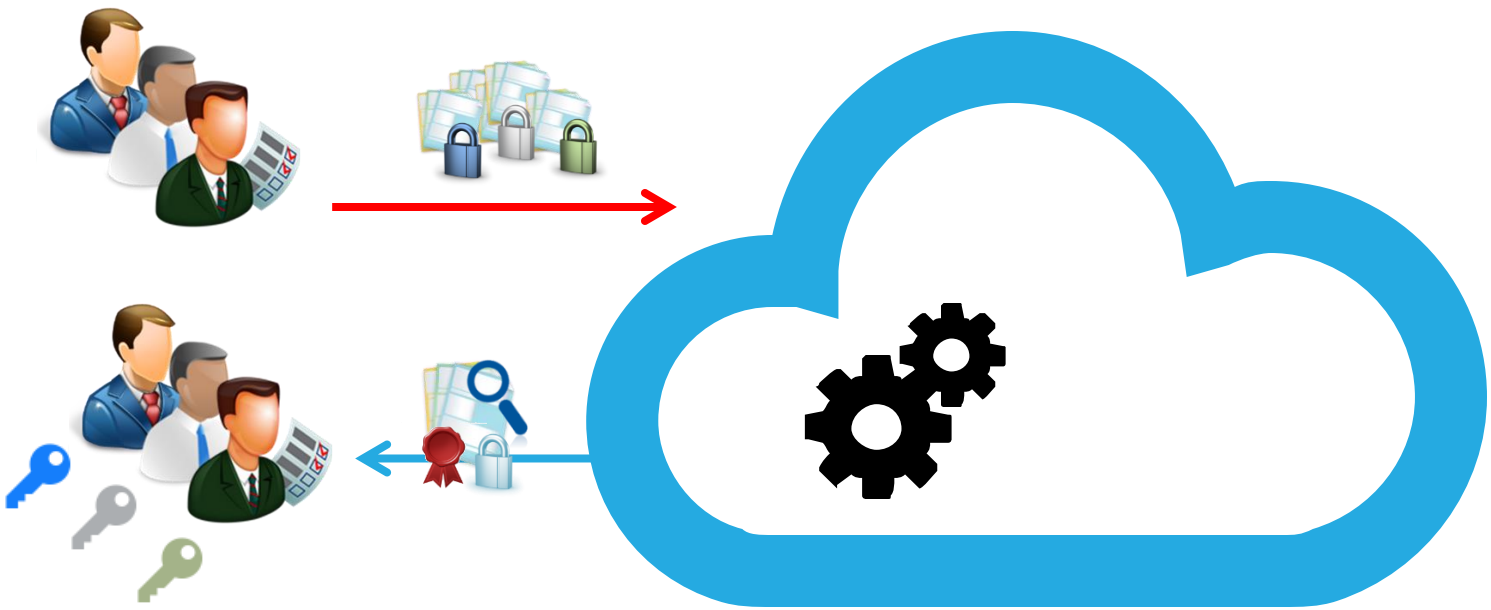
Impact

Increase the range of available specific solutions for cloud computing regarding conflict between **security vs cloud efficiency**

Reduce both **security** or **storage/computing costs** without decreasing performance

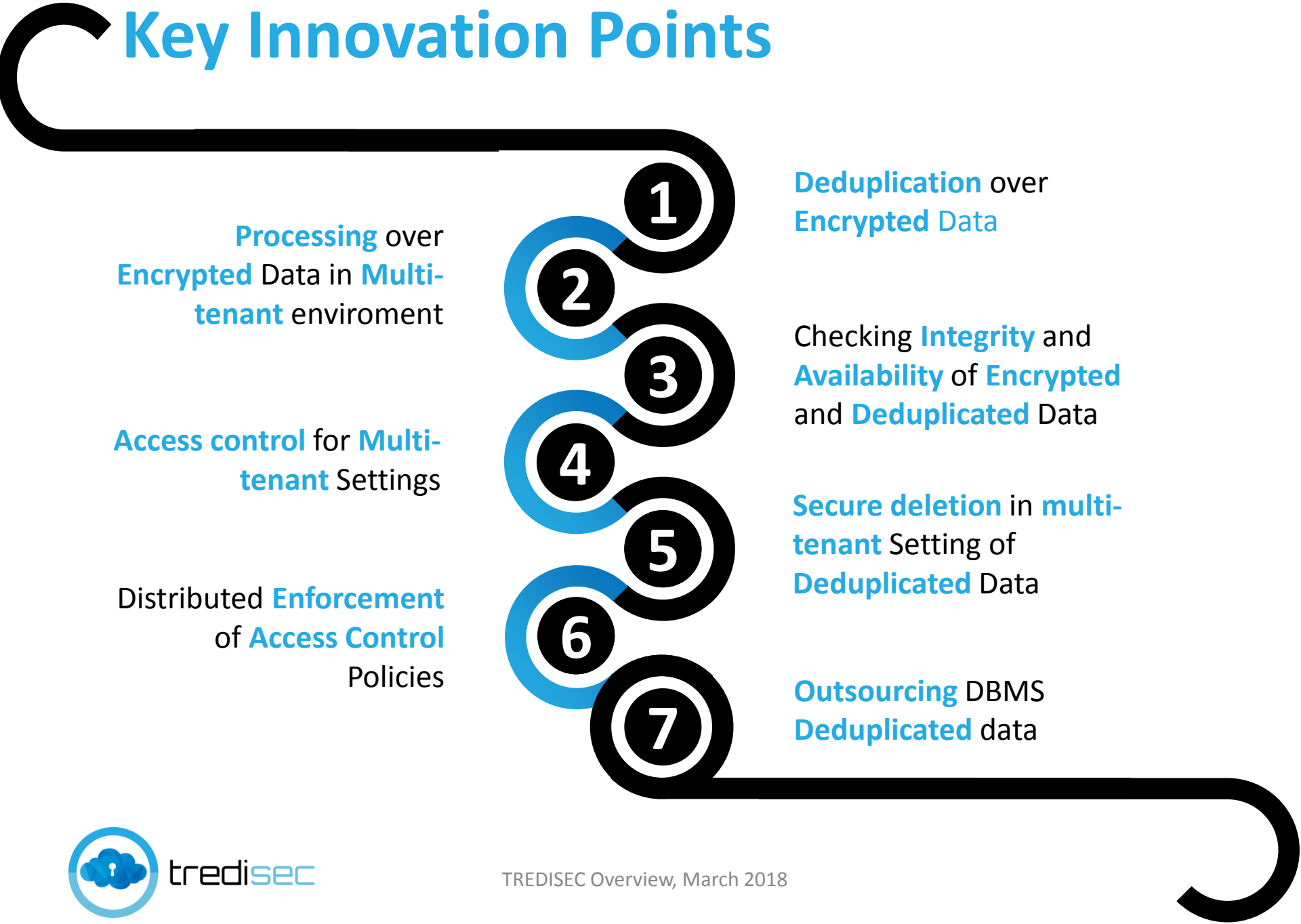
Empower users with **greater control** over their **data.**
End-to-end security.

Scientific Objectives



- Storage integrity with data reduction
- Data confidentiality with cross-tenant data deduplication
- Privacy data processing

Key Innovation Points



Deduplication over **Encrypted** Data

Processing over **Encrypted** Data in **Multi-tenant** enviroment

Checking **Integrity** and **Availability** of **Encrypted** and **Deduplicated** Data

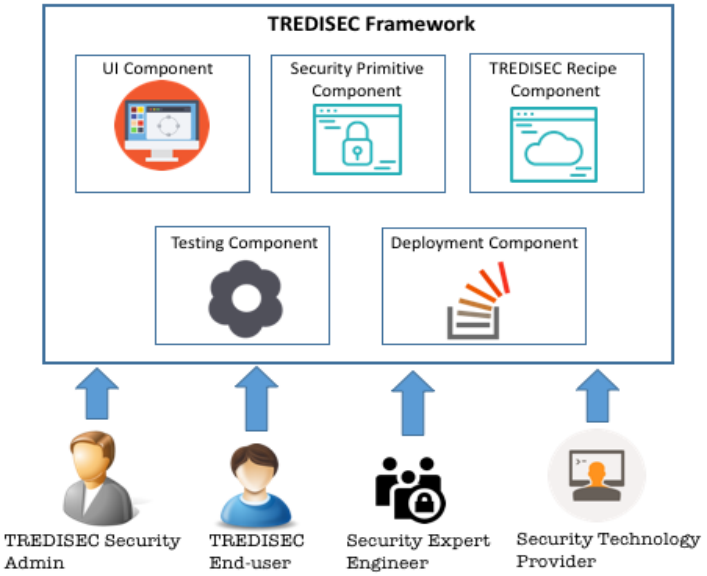
Access control for **Multi-tenant** Settings

Secure deletion in **multi-tenant** Setting of **Deduplicated** Data

Distributed **Enforcement** of **Access Control** Policies

Outsourcing DBMS **Deduplicated** data

Innovation oriented to exploitation



Framework

Primitives

Recipes

IDENTIFICATION OF MOST MATURE RESULTS
DEFINITION GO-TO-MARKET STRATEGY

Goals of TREDISEC

- Design and develop solutions that fulfill both security and functional requirements of cloud systems (**security primitives**)
- Develop a **framework** that supports the creation, management and use of such solutions

TREDISEC - Results

Security primitives

- **Security primitives** provide a joint solution for functional and security requirements for cloud systems
  - (e.g. multi-tenancy with encryption, secure data migration service, etc.)
- Provided at design and implementation level

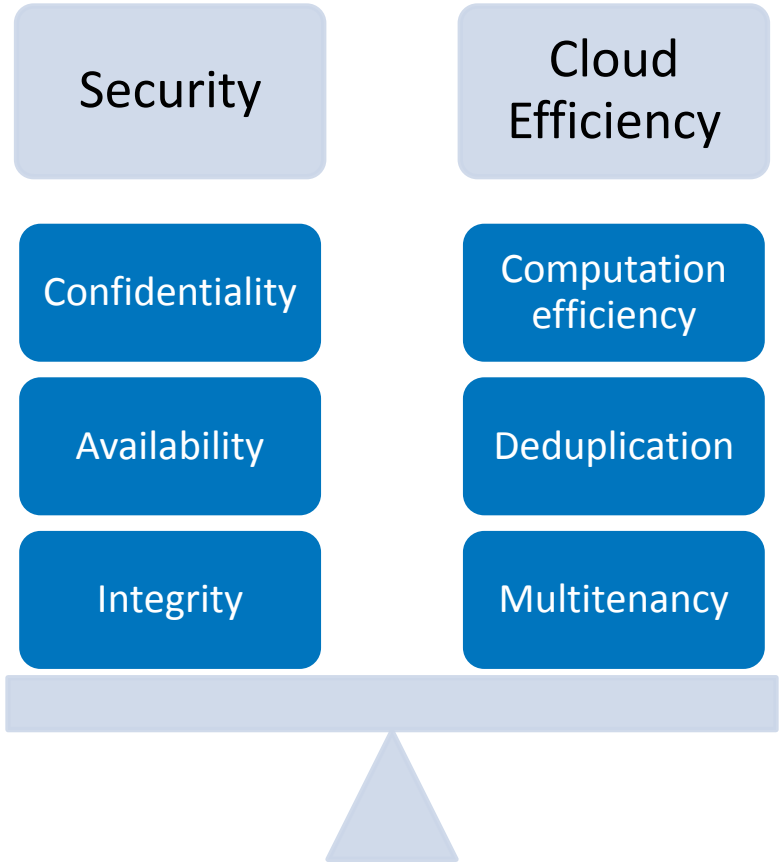
TREDISEC - Results

TREDISEC Recipe

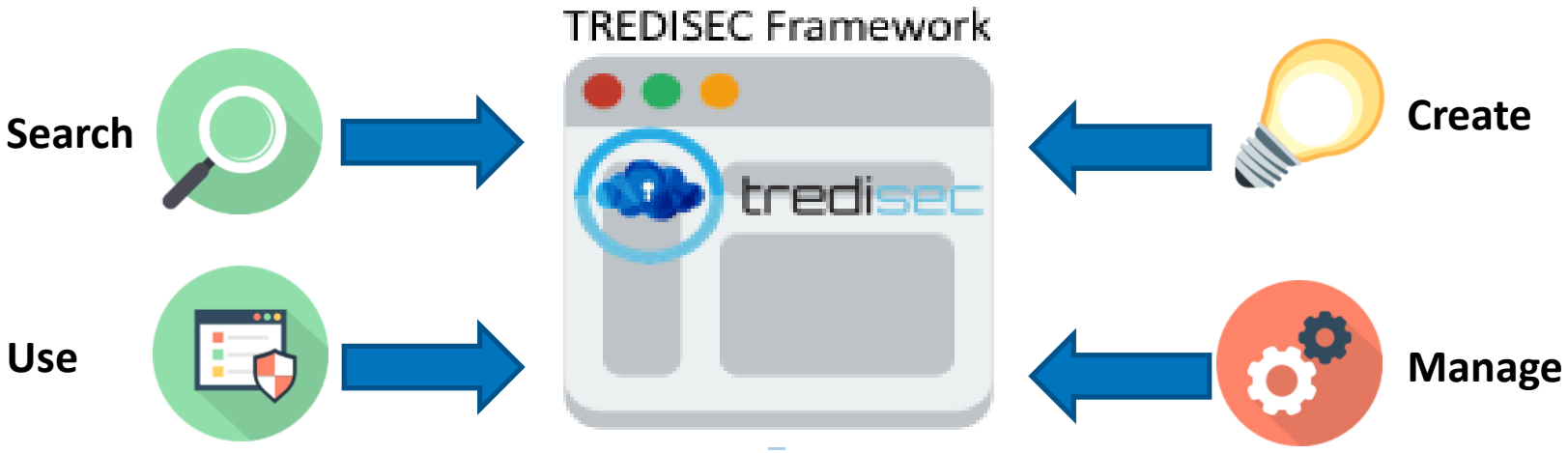
- **TREDISEC Recipes** are the “deployment-ready” version of the security and functional solutions
- They are composed of one or more security primitives, fulfilling multiple security and functional requirements
- Customized for a particular cloud environment

Security Primitives

- Software components
  - Address specific combinations of requirements
  - Some may need specific hardware to run
  - Some may work only in specific cloud settings



TREDISEC - Framework



TREDISEC - Framework

Support of different roles

User-friendly

Automatic deployment and testing

Repository of security and functional solutions

How to use the TREDISEC Framework?

- **Security engineer**

Publish design of security primitives

How to use the TREDISEC Framework?

- **Developer of security solutions**

Create implementation of a security primitive

Test implementation in a testing environment

Provide public information of testing and results (e.g. performance)

How to use the TREDISEC Framework?

- **Integrators**

Use implementations for creating a TREDISEC Recipe

Develop deployment and testing functionalities
for the TREDISEC Recipe

Provide public information of testing and results in a testing environment

Make available cloud testing environment for checking the TREDISEC Recipe

How to use the TREDISEC Framework?

- **Cloud service providers**

Search for solutions based on their requirements

Link their cloud environments in order to deploy and test the solutions directly in their systems

Provide feedback of the use and behaviour of the solution

TREDISEC Framework - Demo

1. 

How to create security primitives and TREDISEC Recipes

2. 

Explore existing solutions in the TREDISEC Framework

3. 

Cloud testing environments of the TREDISEC Framework

4. 

Deployment and testing functionalities

Thank you!

Contact:
Beatriz Gallego-Nicasio Crespo
TREDISEC project coordinator
Atos Research & Innovation
beatriz.gallego-nicasio@atos.net

Rodrigo Diaz Rodriguez
Head of Cybersecurity Lab
Atos Research & Innovation
rodrigo.diaz@atos.net

The work described in this presentation has been conducted within the project TREDISEC. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 644412. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.