No More Dark Clouds With PaaSword – An Innovative Security By Design Framework

PaaSword

Cloud Forward Conference

Oct 18-20, 2016 – Madrid, Spain

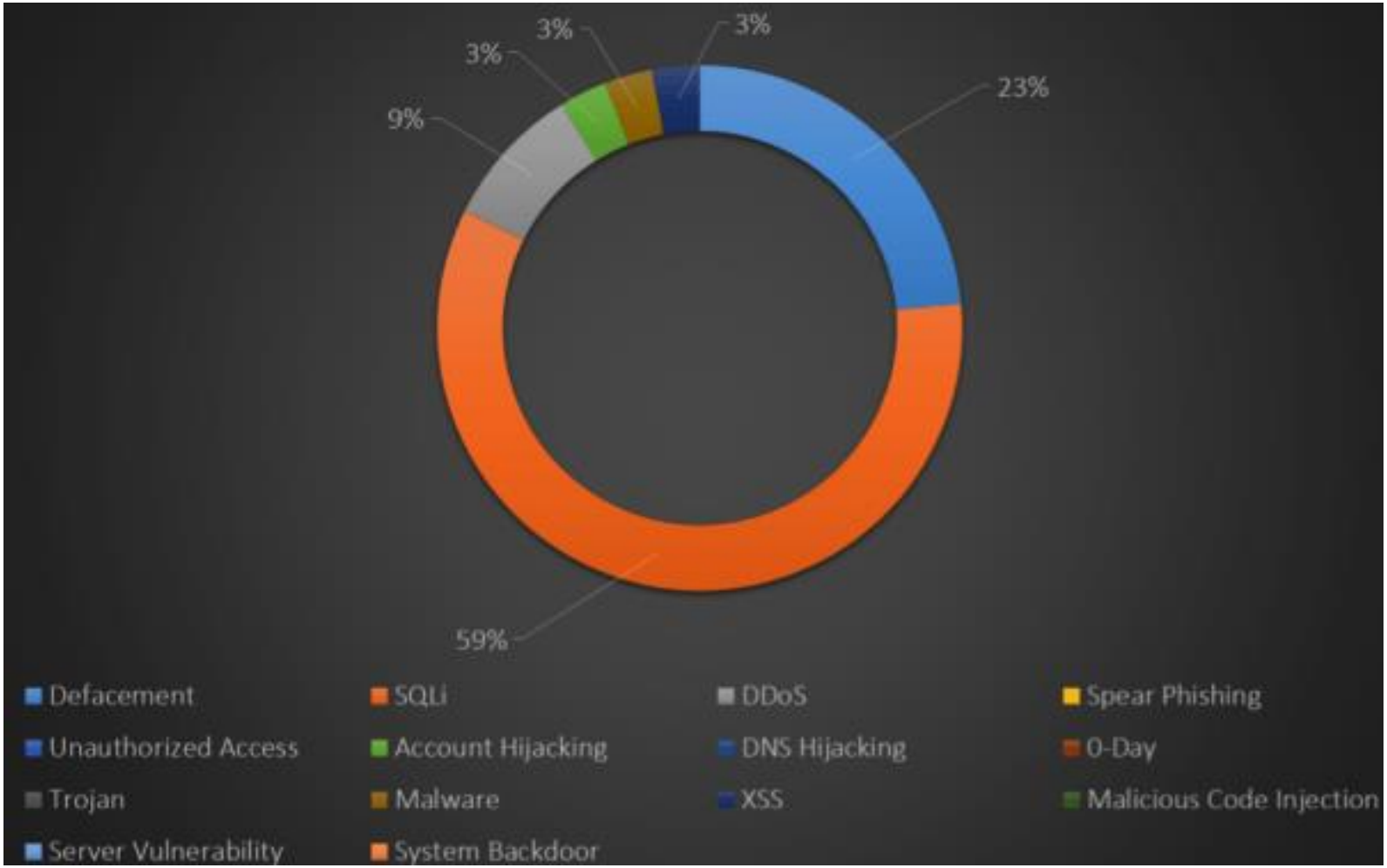
PaaSword

Cloud Paradigm Shift

- The cloud paradigm has definitely prevailed
  - Most application are delivered following the **SaaS** model
  - Many developers rely on **PaaS** offerings for scalablity
  - Nearly all underlying resources (DBs, Queues etc) are outsourced at the **IaaS** level
- Attack vectors have increased
- ‘Raw data’ are the modern hacker’s holy grail
- **The responsibility for the protection of data has shifted to the developer**

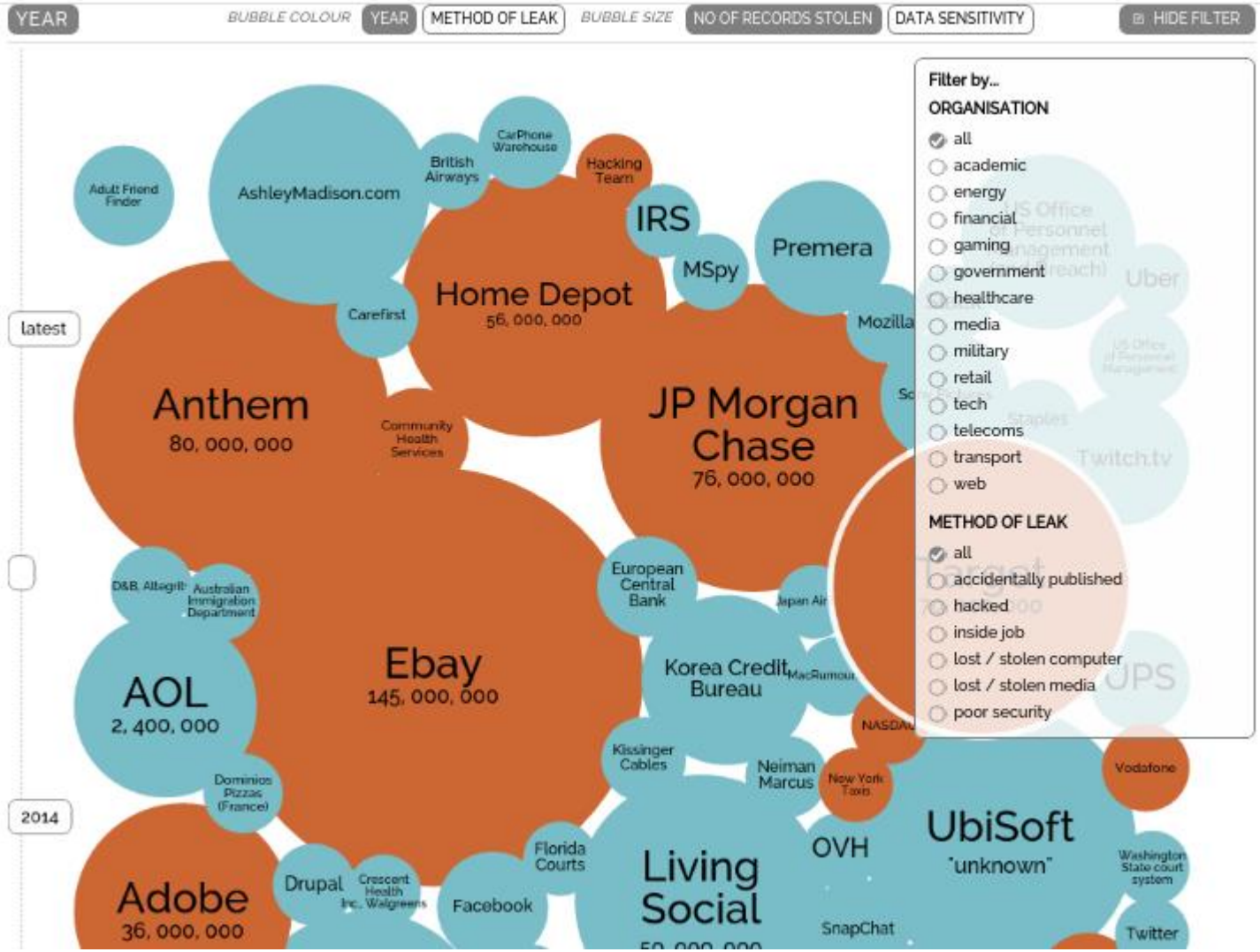
PaaSword

60% of attacks target the database



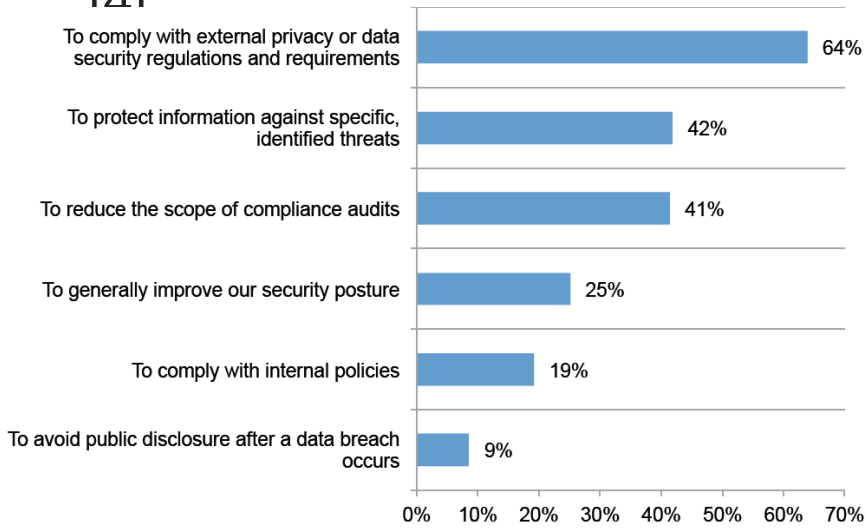
PaaSword

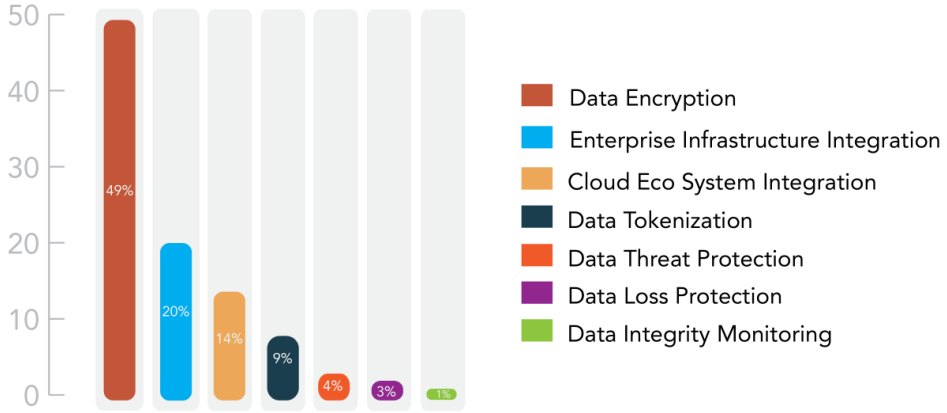
Data leaks



Motivation – Security as an Enterprise Requirement

- Enterprises identify **security concerns** and **data privacy** as the most significant **barriers** of Cloud adoption;
  - In addition:
    - Compliance (e.g., legal, regulatory, industry-standard compliance)
    - Cultural resistance
- **Encryption** and **key management** as **top priority** requirements [3] & [4]





[3] P. Institute, "2015 Global Encryption & Key," Thales, 2015.
[4] CipherCloud, "Global cloud data security report - The authority on how to protect data in the cloud," CipherCloud, 2015.

PaaSword

How shall we lower the barriers?

- Security concerns
  - Protect confidential information
  - Control access
  - Trust cloud provider
  - Secure Cloud Applications
- Data privacy
  - Secure storage
    - Encryption
    - Trustable Key Management
  - Control Access to data

PaaSword

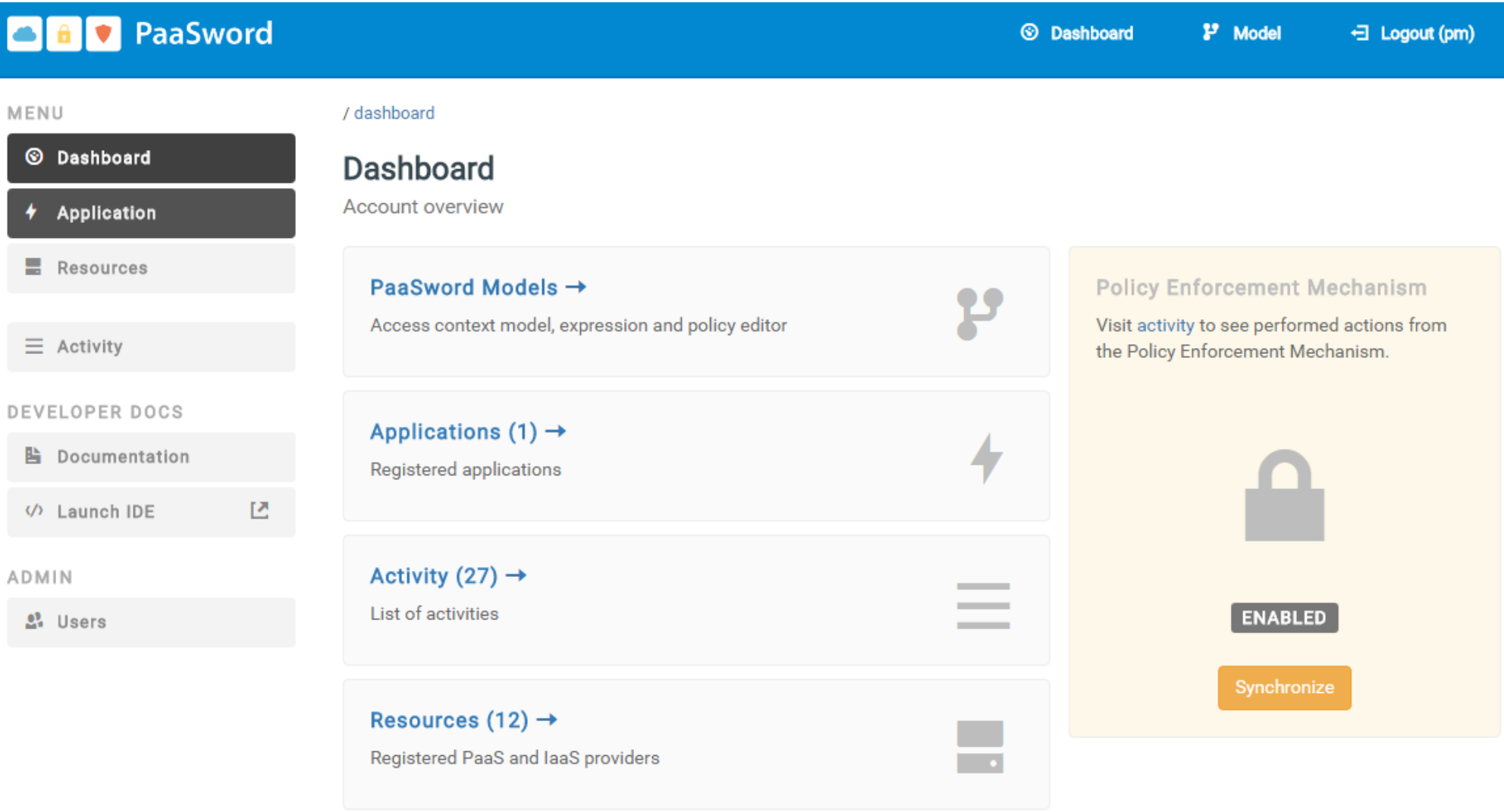
PaaSword

Problem Areas Targeted

- **Insufficient** security and **trust** of cloud infrastructures and services
- Cloud application **developers** have difficulties specifying appropriate **level of security**
- Appropriate **context-aware access control** mechanisms for cloud applications
- Ensure **protection**, privacy and integrity **of data stored** in the cloud
- **Prove** applicability, usability, effectiveness and value of **secure cloud platforms**

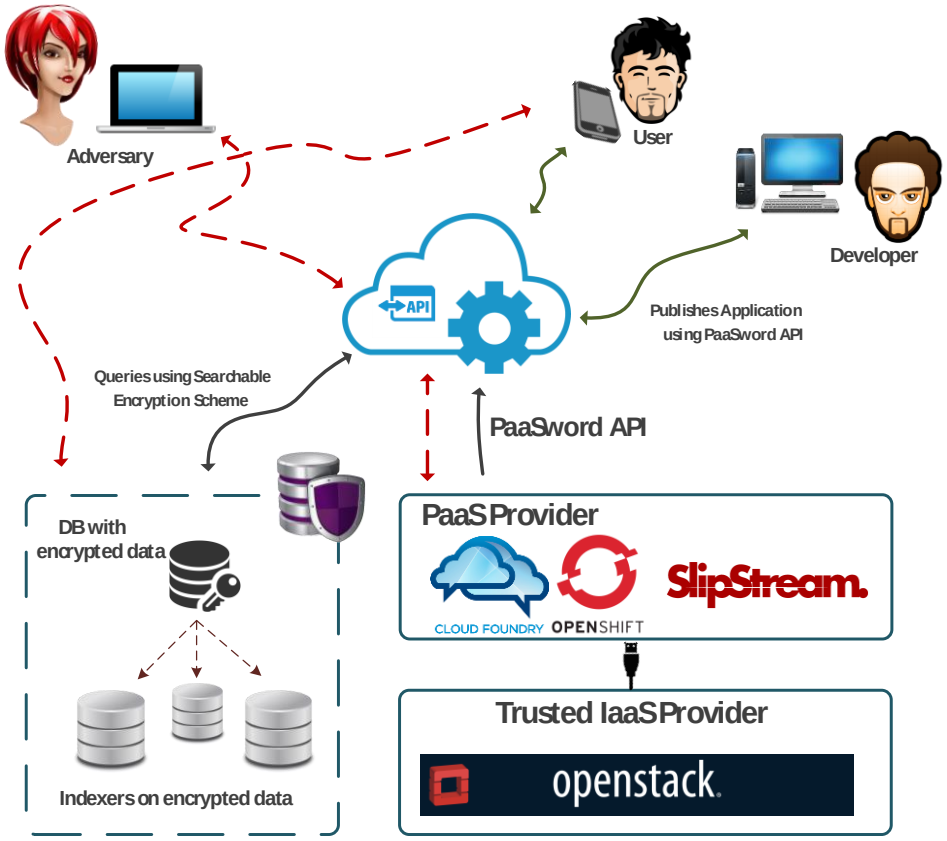
PaaSword

PaaSword Platform



PaaSword

PaaSword Features



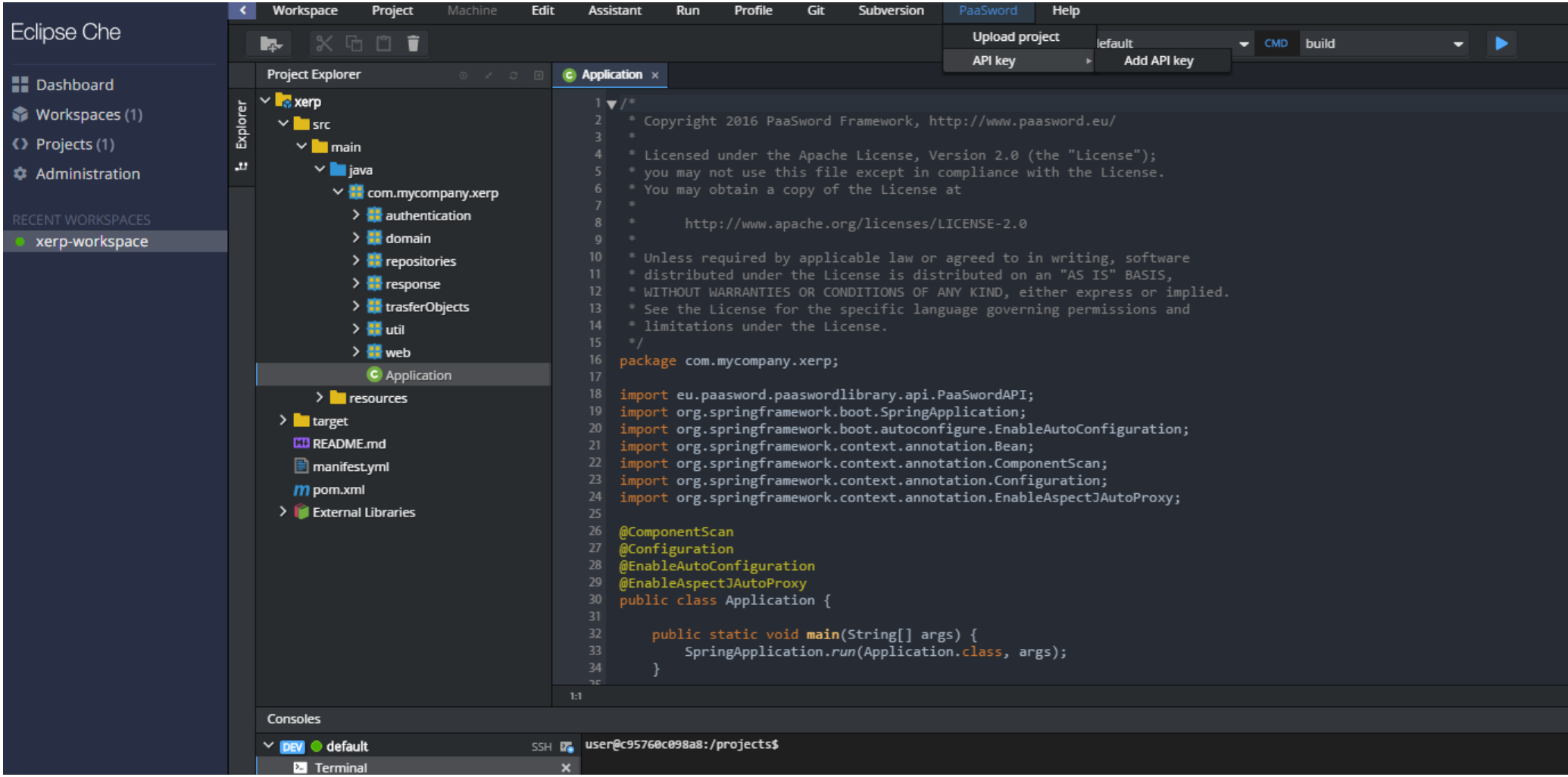
- A **security-by-design framework** which will allow developers to engineer secure applications
- **Leverage the security and trust** of data that reside on outsourced infrastructure
- Facilitate **context-aware access** to **encrypted** and (even) **physically distributed** datasets stored in the cloud
- Prove **applicability, usability, effectiveness** and value of our framework in real-life Cloud infrastructures, services and applications

Major Assets developed so far…

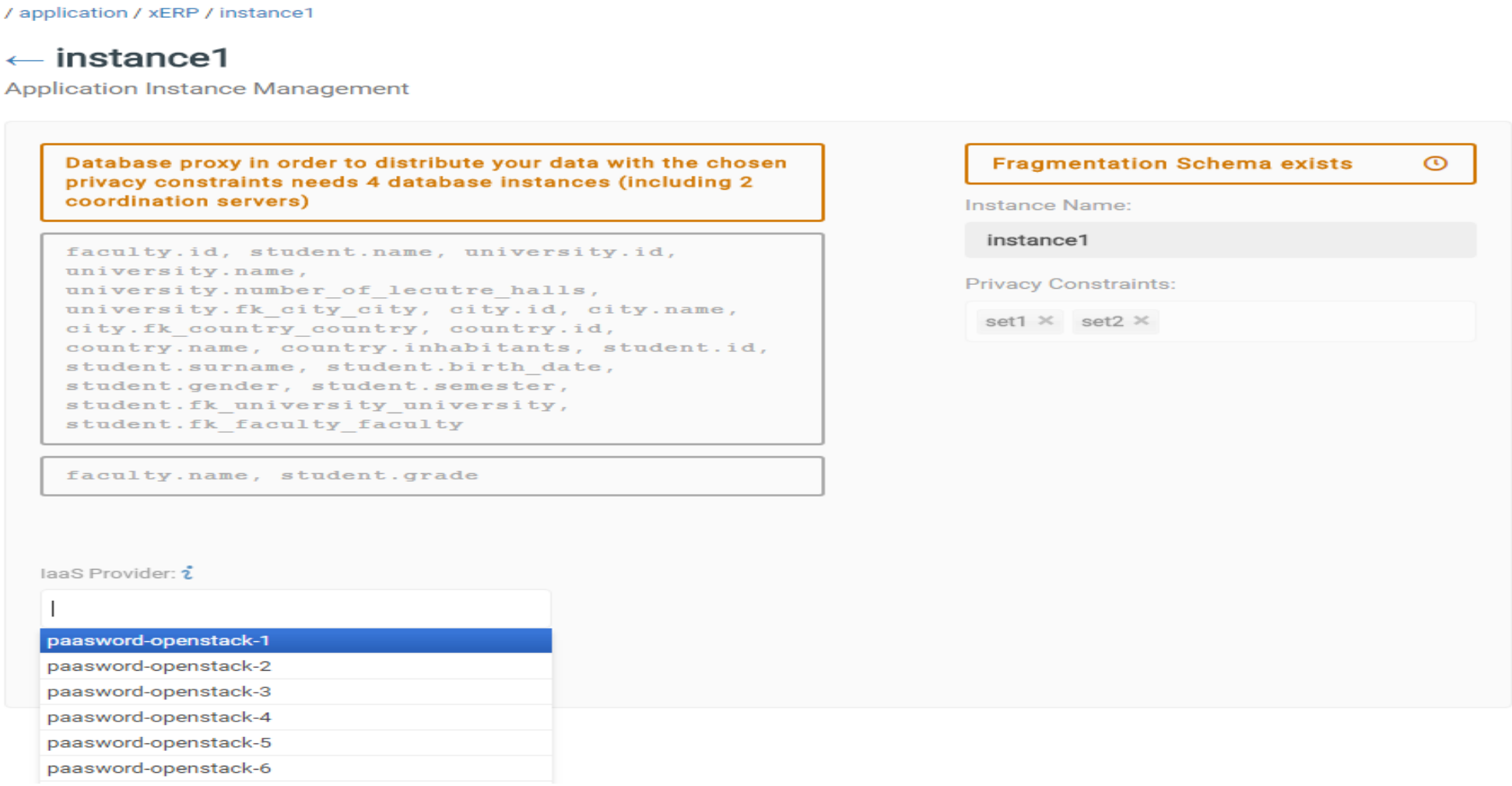
- A JAVA annotation library that can be used during development in order to annotate database models (using JPA)
  - These annotations are translated during runtime to privacy constraints that drive the fragmentation of the database
- A **virtual-database proxy** that is able to handle any SQL query by translating it in the proper format based on the fragmentation scheme
- An **XACML-compliant authorization engine** that is able to perform reasoning prior to attribute-evaluation
- An **integrated IDE environment** where developers can submit and control their PaaSword-enabled applications

PaaSword

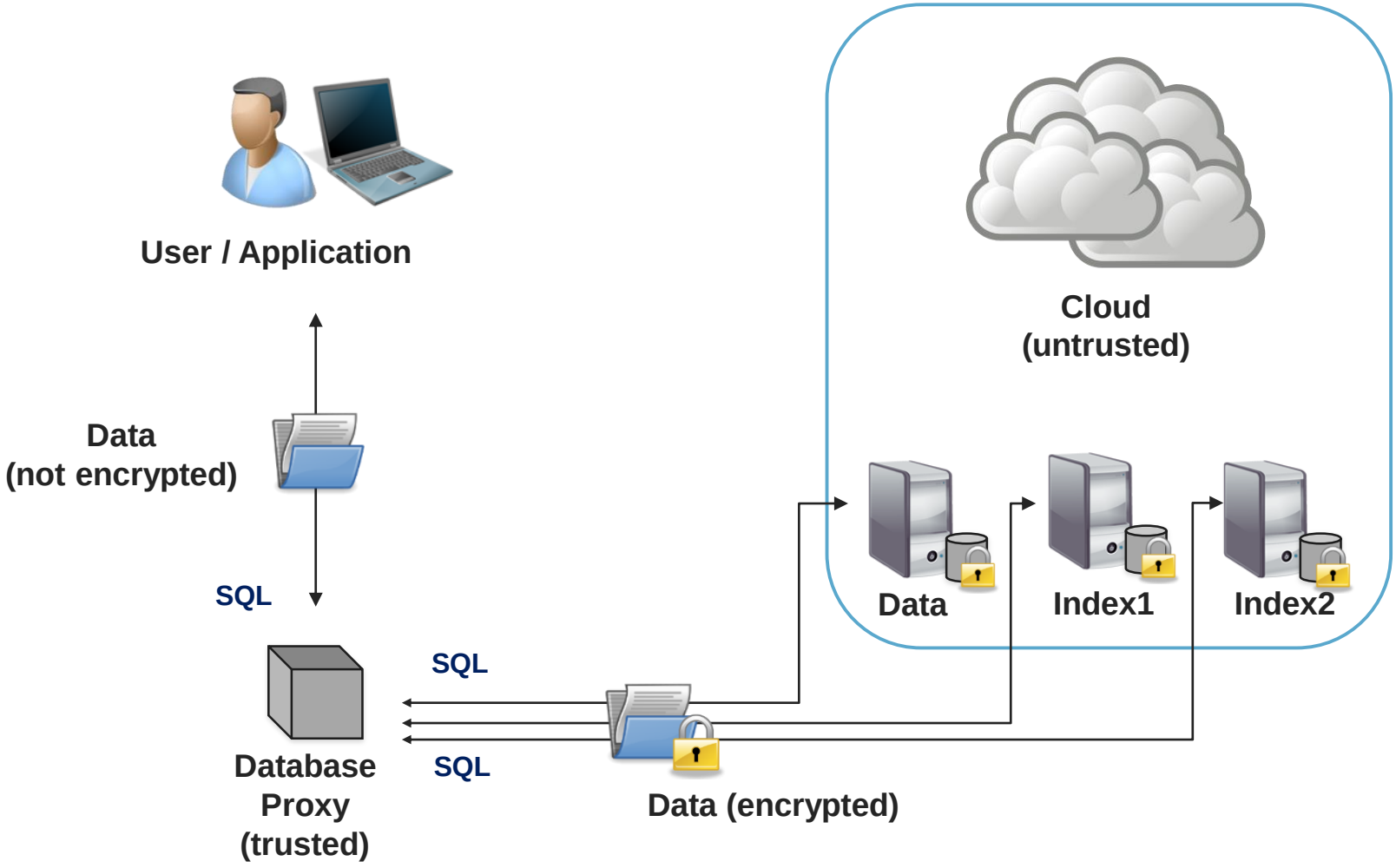
Integration of Eclipse CHE IDE



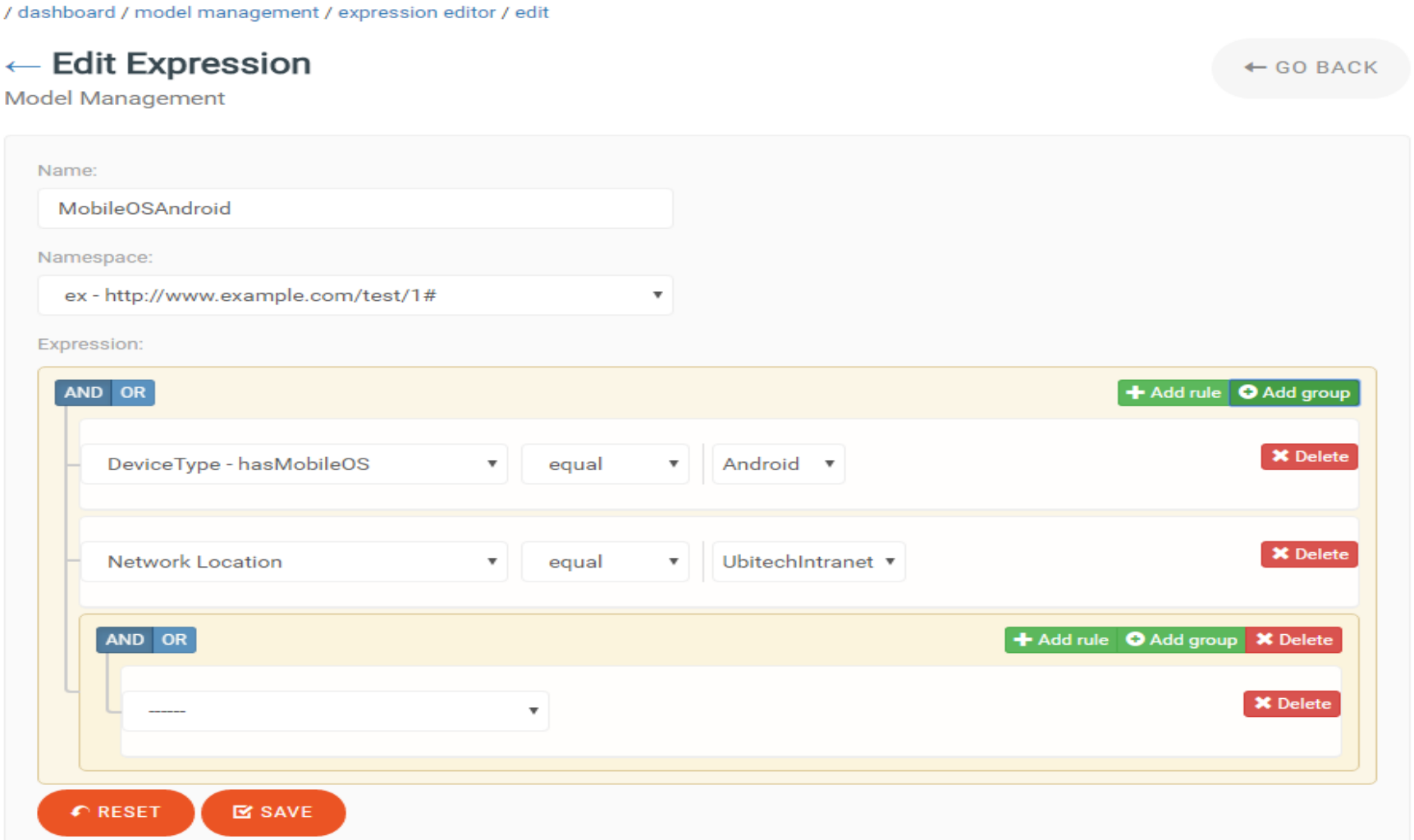
Native Integration with OpenStack



Asset: Virtual Database Architecture

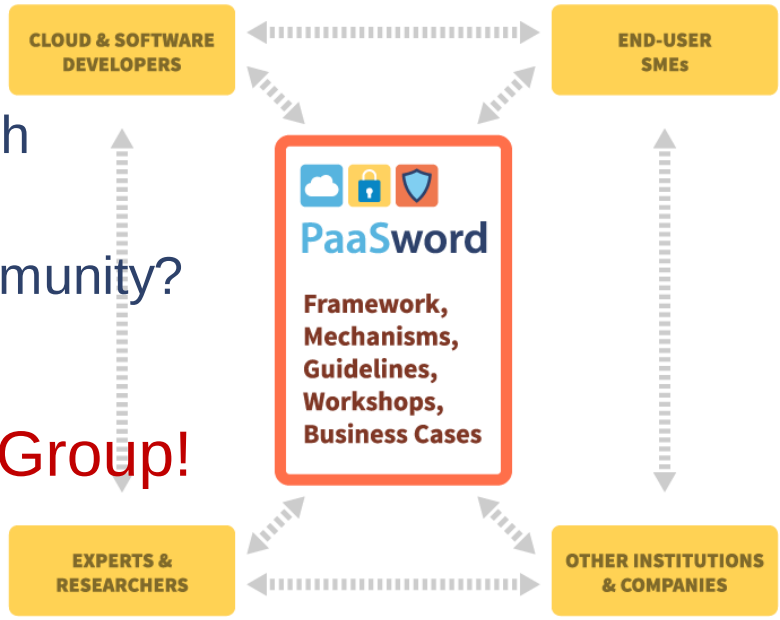


Model-driven Expression editing



Interested in… ?

- Getting access to early results?
- Shaping and expanding PaaSword?
- Networking with leading companies & research institutes?
- Collaborating with us and the PaaSword Community?



Join the Cloud Security Industrial Focus Group!

Register at:

https://www.paasword.eu/register/

PaaSword

Join our Industrial Focus Group Today!

Visit us:

www.paasword.eu

Acknowledgements:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644814.