



OWASP

Open Web Application
Security Project

Cloud encryption – Encrypt all the things!

Walter Tighzert

German Owasp Day 2014

About me

- Security researcher at SAP SE
walter.tighzert@sap.com
- Focus on search over encrypted data

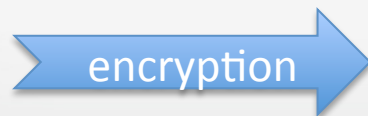


Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

SQL operators:
SELECT, COUNT

Animal
cat
dog
cat



Animal
09122014...
080012...
0171633...

AES - CBC



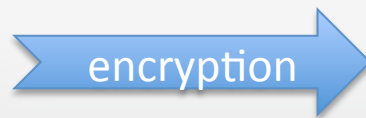
OWASP
Open Web Application
Security Project

Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

SQL operators:
=, DISTINCT, GROUP
BY, JOIN

Animal
cat
dog
cat



Animal
09122014...
080012...
09122014...

AES - ECB



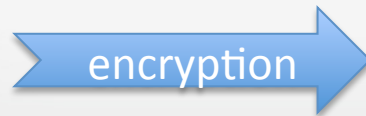
OWASP
Open Web Application
Security Project

Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

SQL operators:
<, ORDER BY

Animal
cat
cat
dog



Animal
0171633...
0171633...
080012...

BOLDYREVA



OWASP
Open Web Application
Security Project

Cryptographic interlude

- Randomized encryption
- Deterministic encryption
- Order preserving encryption
- Homomorphic encryption

$$\text{ENC}(f(x,y)) = g(\text{ENC}(x), \text{ENC}(y))$$

SQL operators:
SUM

PAILLIER



Cryptographic interlude

- **SELECT** animal, **SUM**(food)
FROM animals
WHERE quantity > 1
GROUP BY animal



- **SELECT** animal_**RND**, **SUM**(food_**HOM**)
FROM animals
WHERE quantity_**OPE** > 05ef
GROUP BY animal_**DET**



Agenda

- Motivation
- State of the art
- Demo
- Challenges

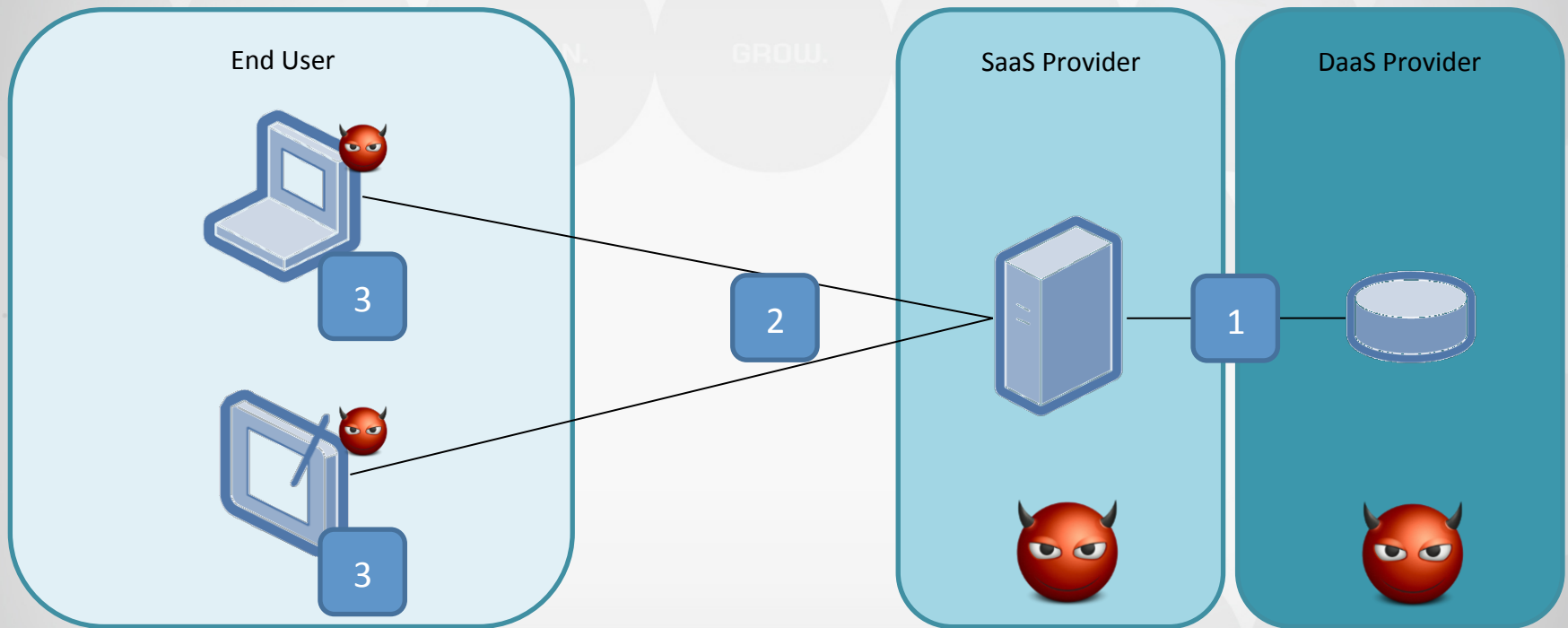


Motivation - Cloud

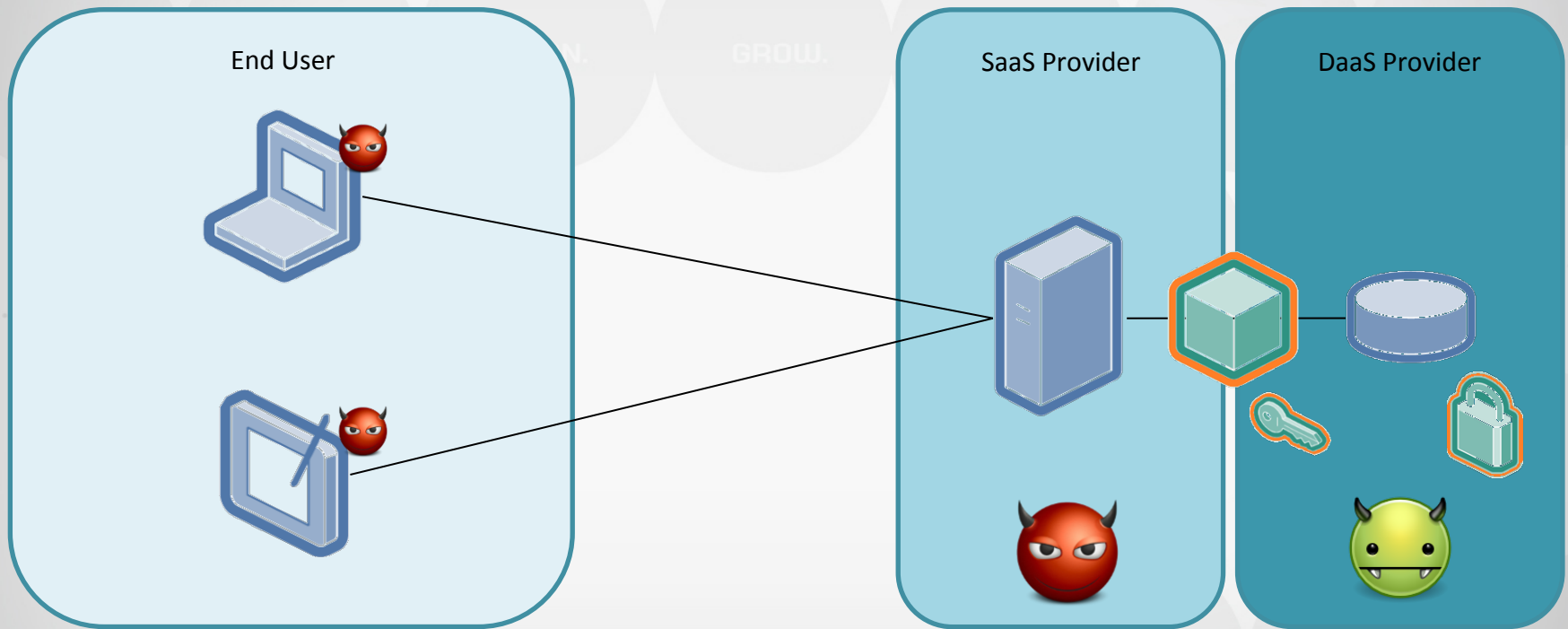
- From personal finance ([Mint](#)) to company finance ([Workday](#))
- What happens with my data?
- Encryption?



Cloud scenario

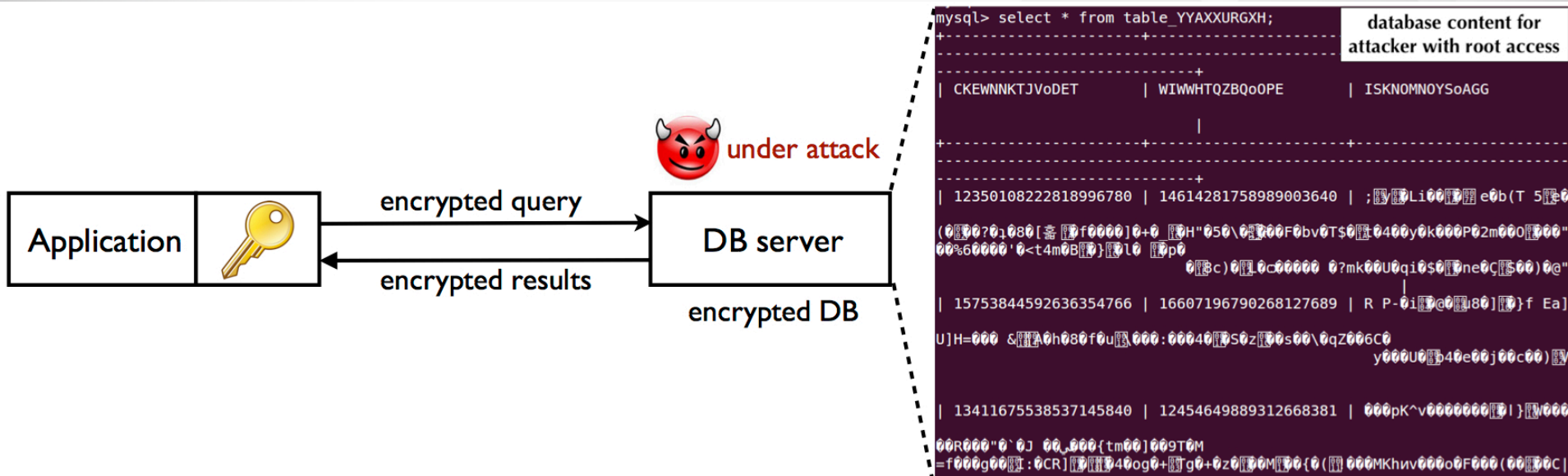


Solution 1: between DaaS and SaaS



Solution 1: between DaaS and SaaS

- Attacker model: DaaS honest but curious
- [CryptDB](#)

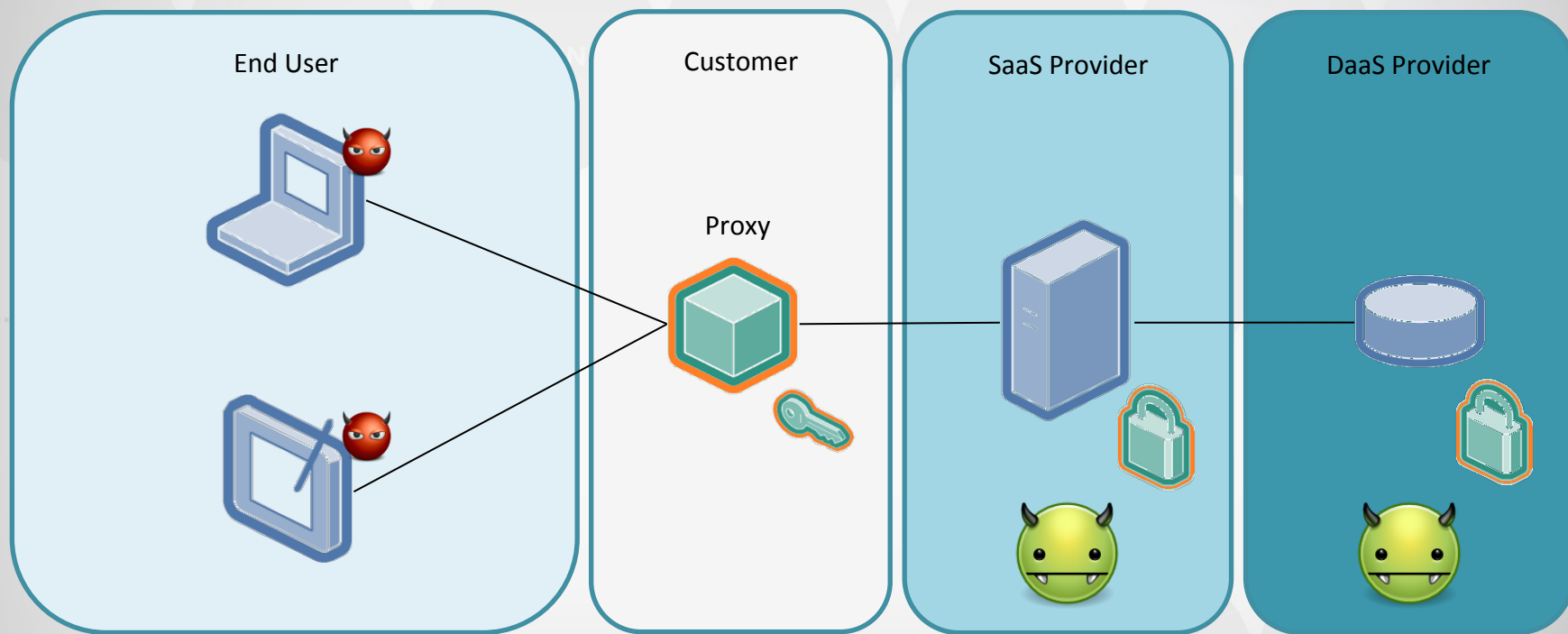


Solution 1: between DaaS and SaaS

Advantages	Disadvantages
Complex queries supported	Encryption keys in the cloud
Transparent for the application	Plaintext on the SaaS



Solution 2: between End User and SaaS



Solution 2: between End User and SaaS

- Attacker model: SaaS honest but curious
- Commercial solutions from 3rd parties ([CipherCloud](#), [Vaultive](#)...)
- HTTP Encryption Proxy for specific applications
- No application changes possible

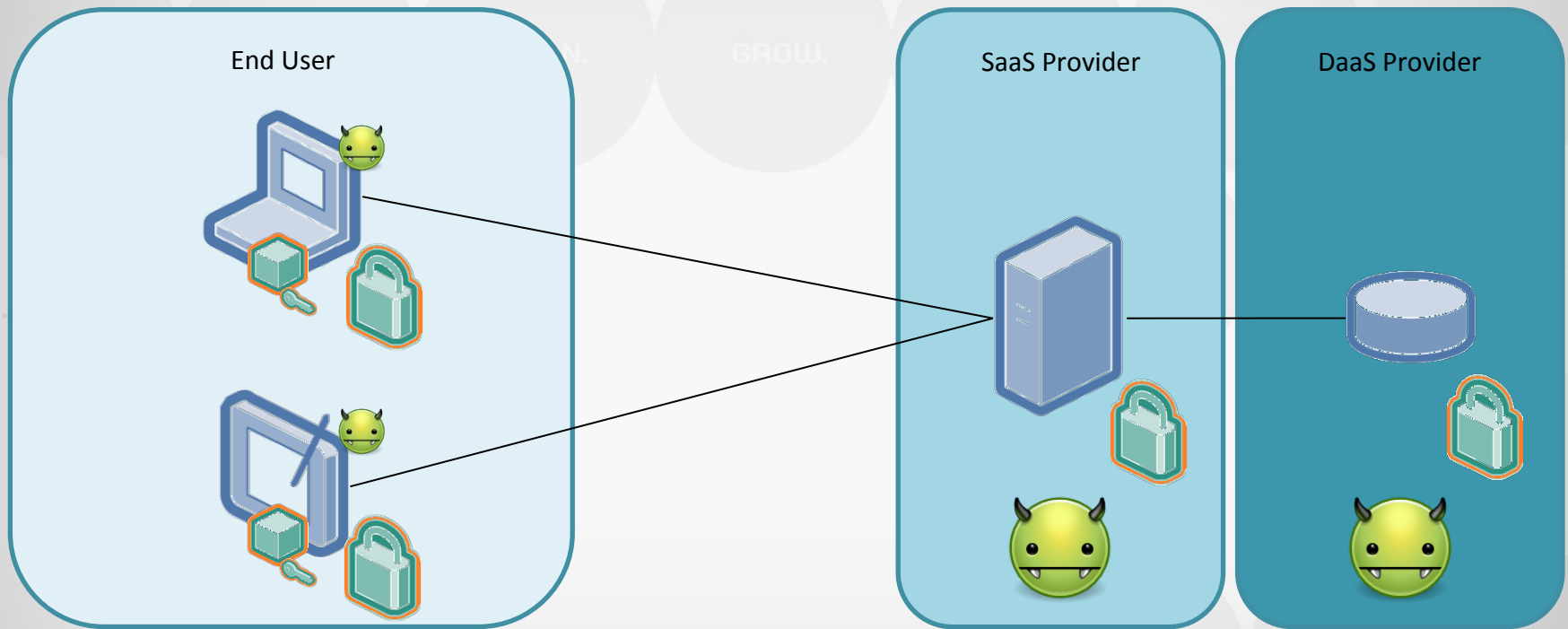


Solution 2: between End User and SaaS

Advantages	Disadvantages
Keys stay at the customer	Only a few applications are supported
	Proxy at the customer
	Simple queries (only textual values)



Solution 3: between Browser and End User



Solution 3: between Browser and End User

- New attacker model: SaaS malicious/compromised
- Research prototypes: [ShadowCrypt](#), [Mylar](#)...
- Plaintext is encapsulated in a sandbox



Solution 3: between Browser and End User

CONNECT.

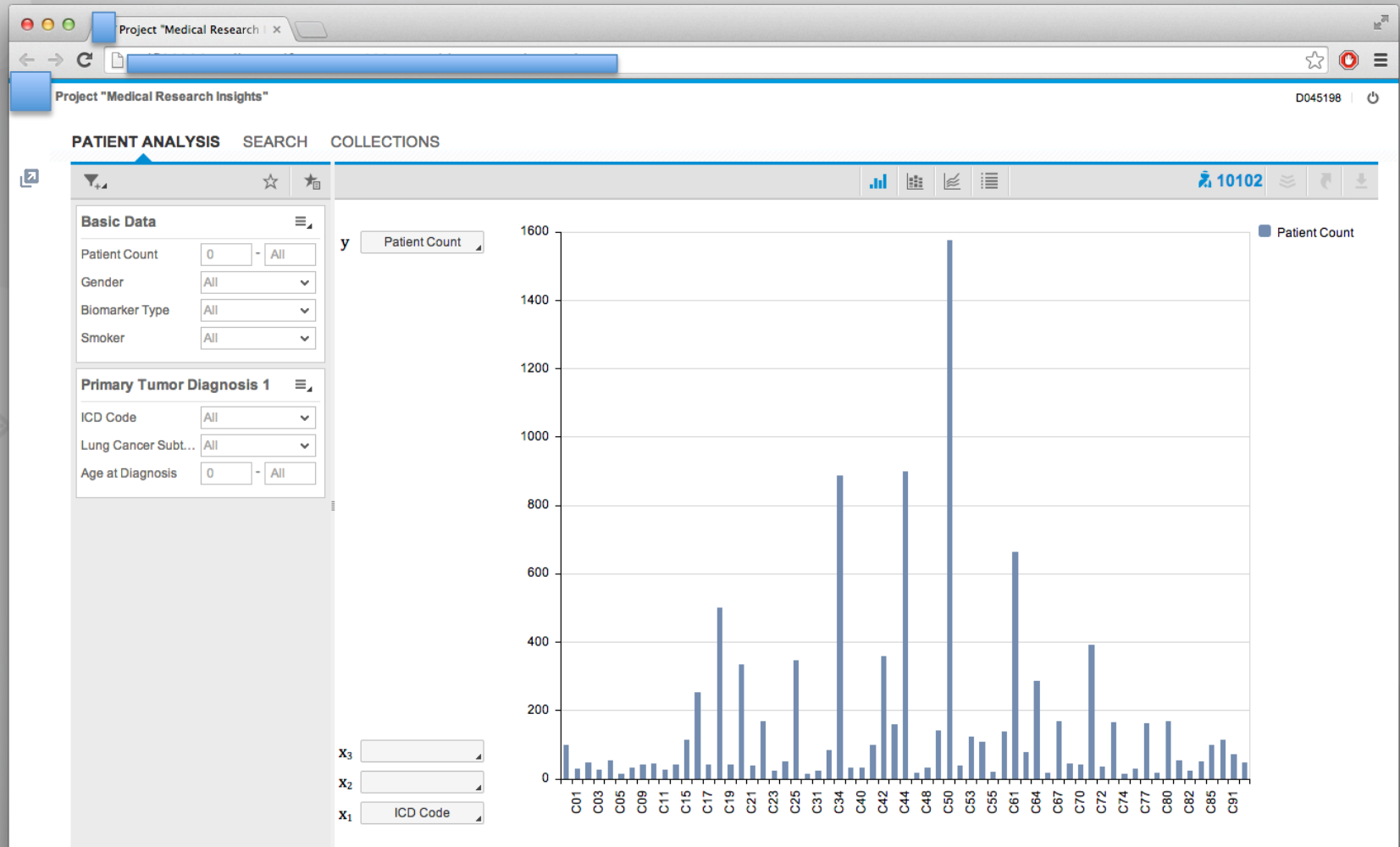
LEARN.

GROW.

Advantages	Disadvantages
Sandbox	Browser-specific
Lightweight client	Key management
	Simple queries (only textual values)



Healthcare Application



Healthcare Application

- Only JOIN and simple WHERE conditions

CONNECT.

LEARN.

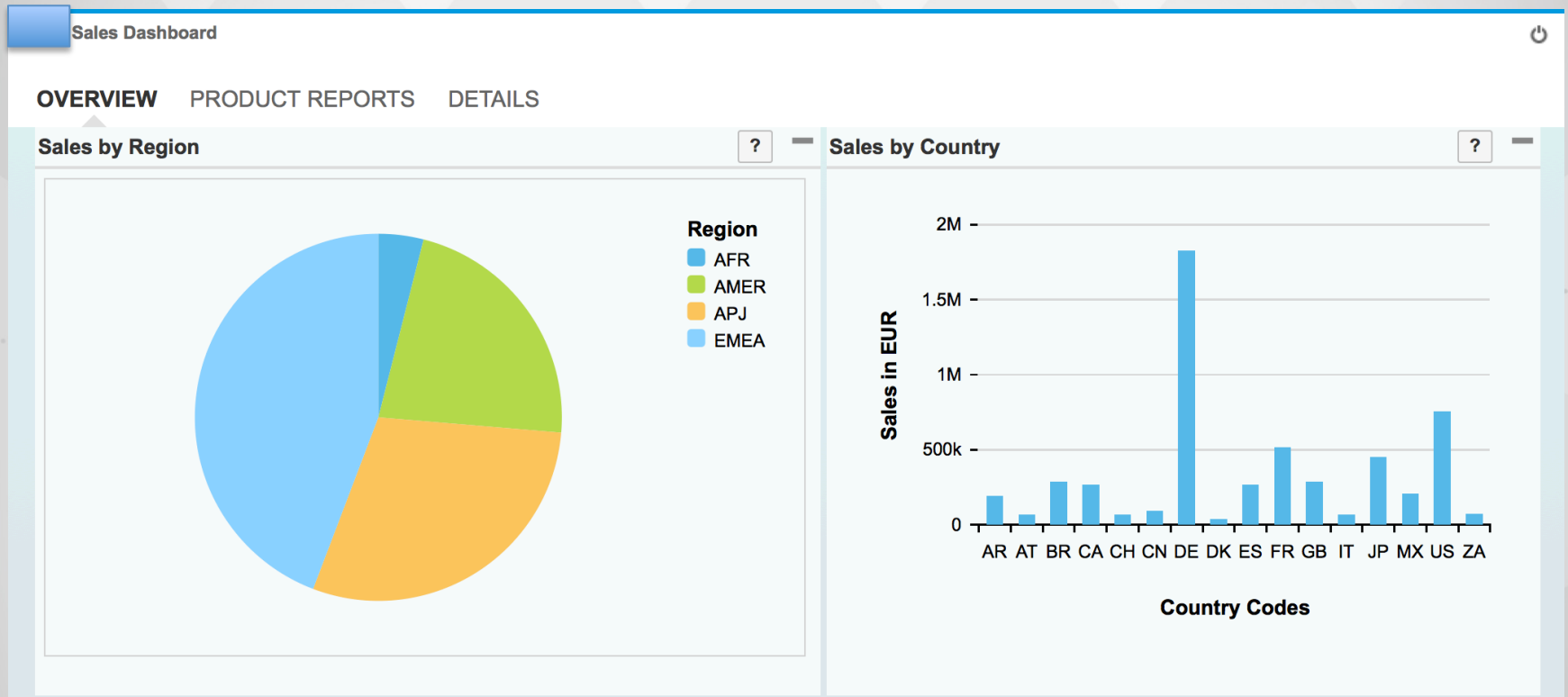
GROW.

ENCRYPT ALL THE THINGS



OWASP
Open Web Application
Security Project

Sales Dashboard



Sales Dashboard

- Complex queries with SUM and ORDER BY SUM (not supported on encrypted data)

ENCRYPT SOME OF THE THINGS



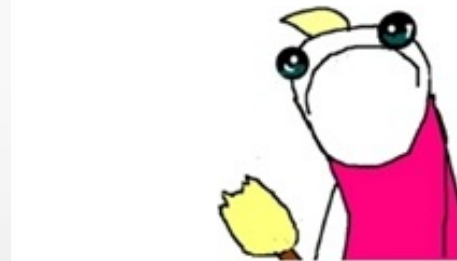
Sales Dashboard

- Complex queries with SUM and ORDER BY SUM (not supported on encrypted data)

ENCRYPT ALL THE THINGS



CHANGE ALL YOUR CODE



OWASP
Open Web Application
Security Project

Challenges

- Not supported functions:
 - ORDER BY SUM
 - LIKE/FUZZY search queries
- Business logic on the server:
TOTAL = SUM(PRICE);
IF TOTAL > 200 THEN TOTAL *= 0.9;
-> move it to the client?



Final Words – Trade-off

CONNECT.

LEARN.

Security



Performance

Functionality



OWASP
Open Web Application
Security Project

Thanks for your attention

CONNECT.

LEARN.

GROW.

Questions/remarks?

walter.tighzert@sap.com



OWASP
Open Web Application
Security Project

Sources

- Mint: https://www.mint.com/images/rd/features/overview_hero.png
- CryptDB: <http://css.csail.mit.edu/cryptdb/cryptdbdiag.jpg>
- Cloud scenario: benny@fuhry.de

