intouch
to be and to stay

Security & Privacy

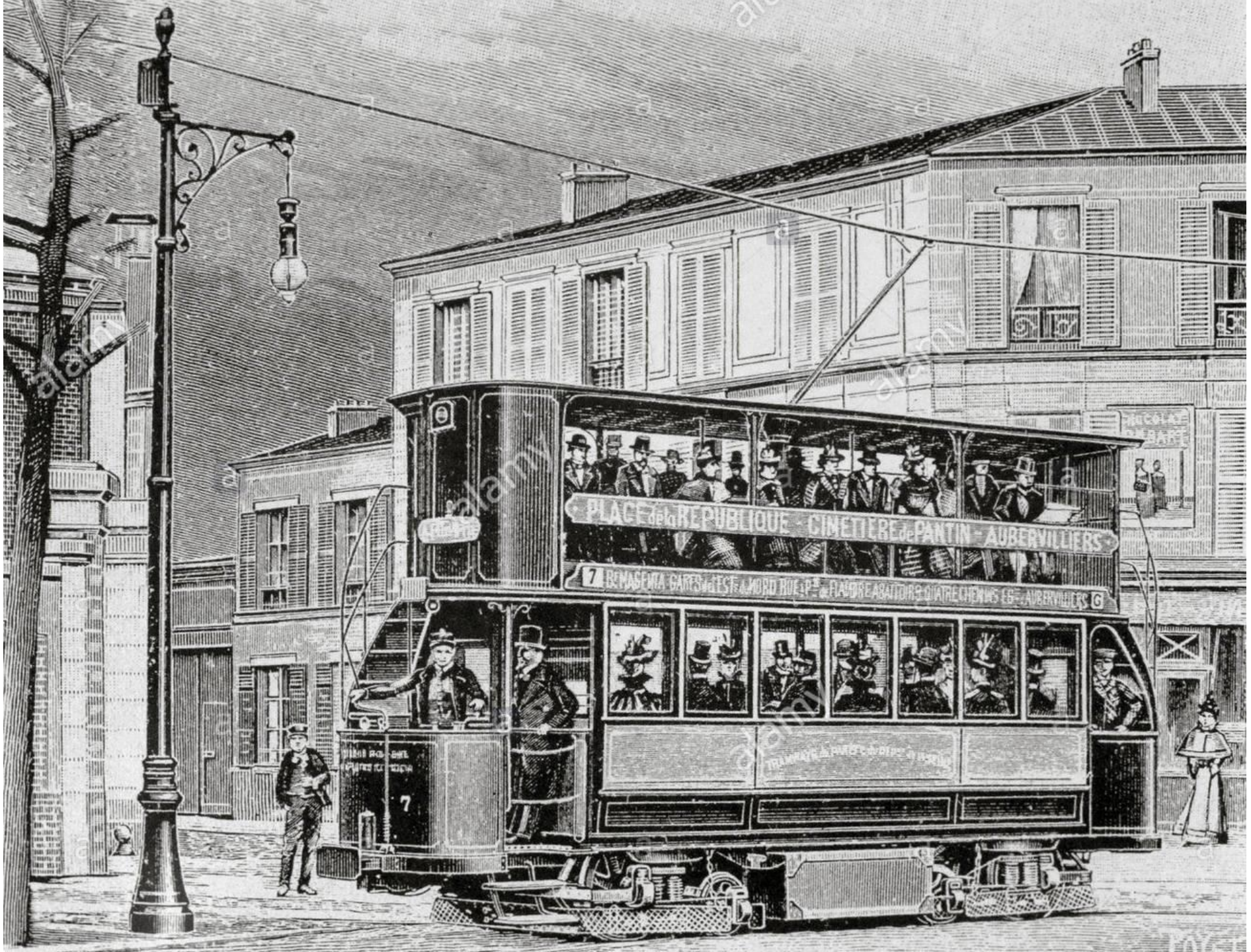
In Web apps, Mobile apps & the Cloud

Victor Sawma . *co-founder* . *cto*

Cyberchisel

Index

Privacy Defined


PLACE de la REPUBLIQUE - CIMETIERE de PANTIN - AUBERVILLIERS
7


gettyimages
Universal History Archive
630042762

Almost ZERO Privacy existed


intouch
to be and to stay
Cyberchisel

How can one get a fresh start?

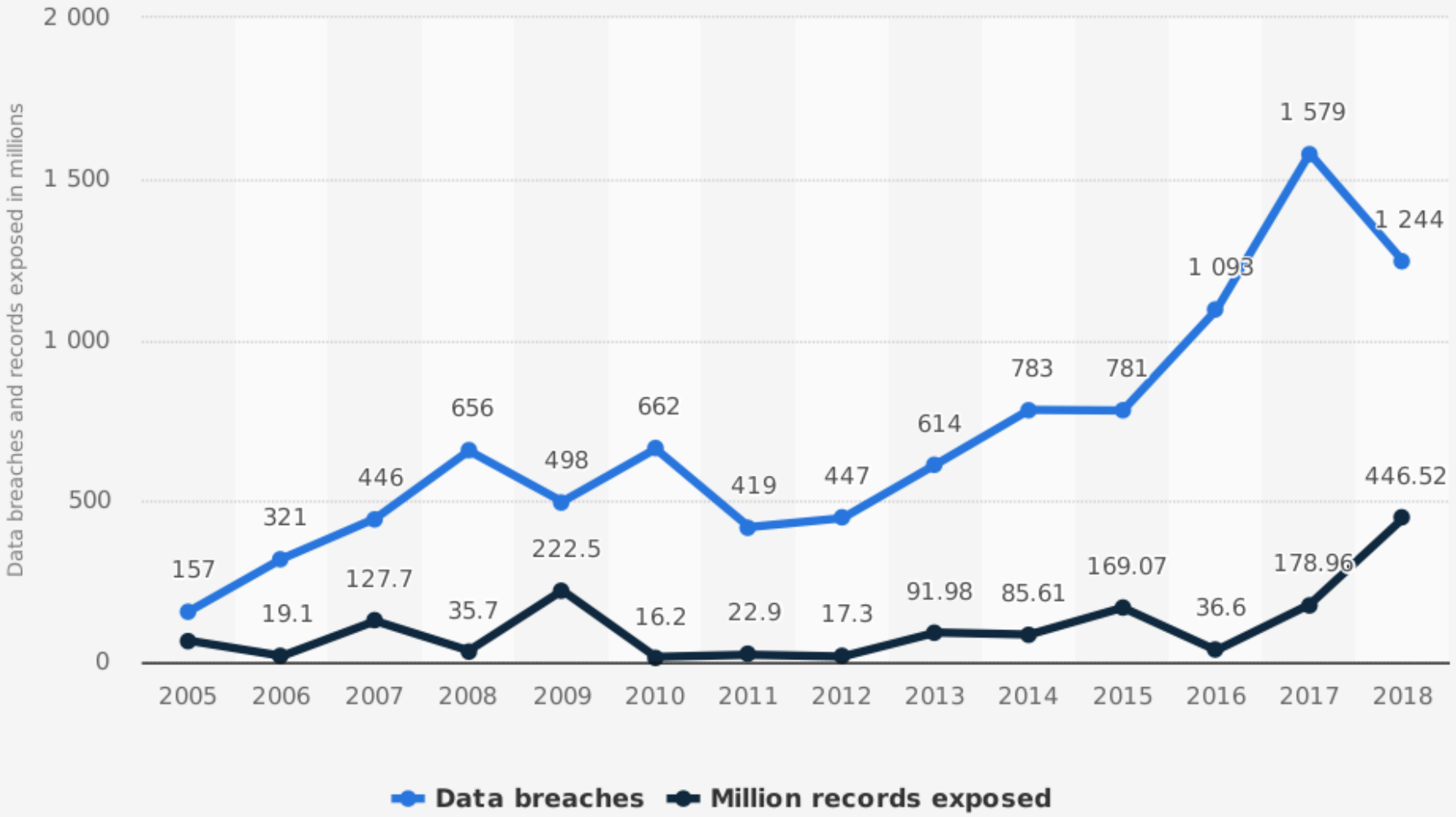
Privacy Defined

"a state in which one is not observed or disturbed by other people"

"the state of being free from public attention"

Privacy Does Matter

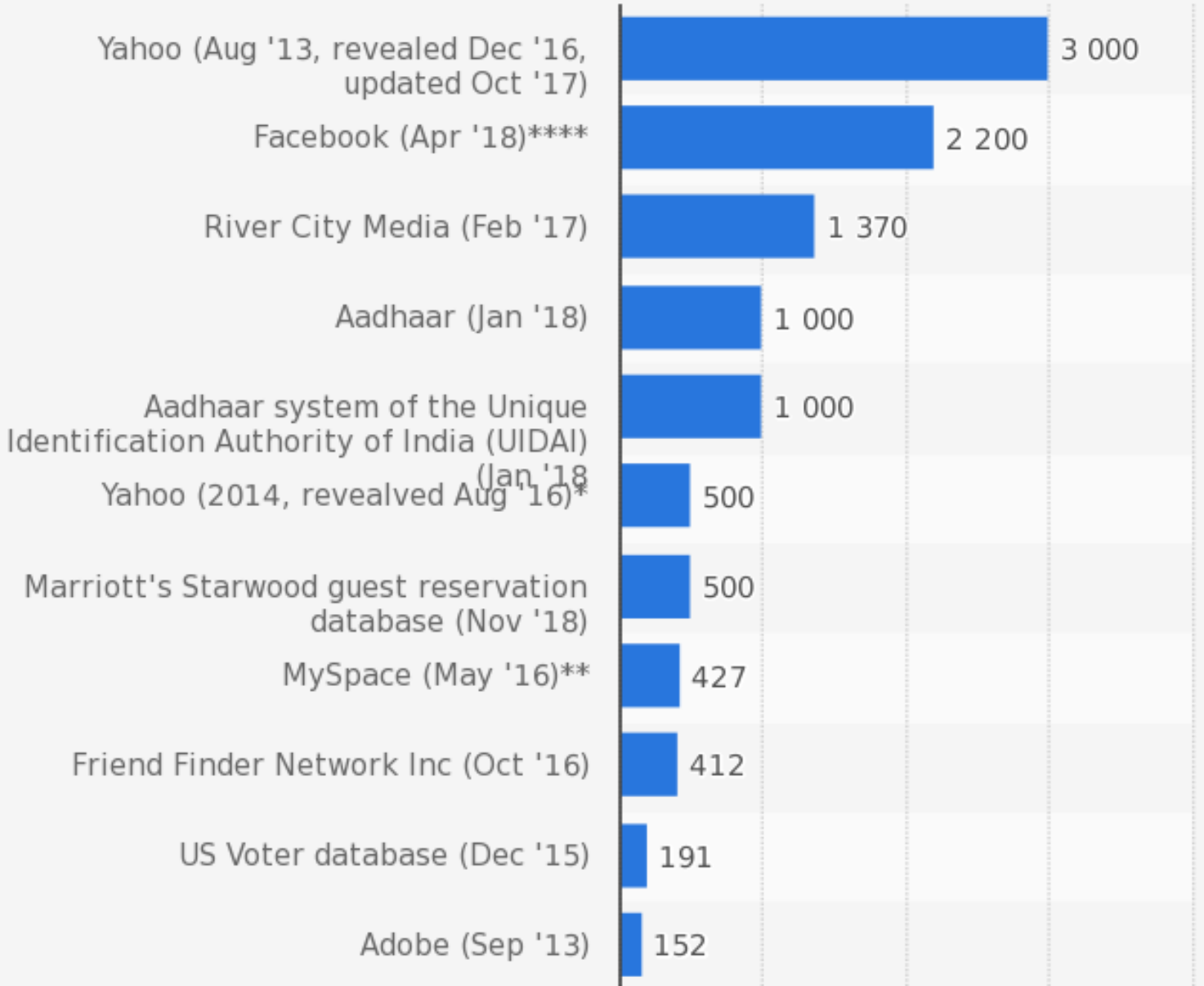
Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)



Source
Identity Theft Resource Center
© Statista 2019

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2018

Number of compromised data records in selected data breaches as of November 2018 (in millions)



Number of U.S. data breaches 2014-2018, by industry

	Business	Medical/Healthcare	Banking/Credit/Financial	Government/Military	Educational
2014	258	333	43	92	57
2015	312	277	71	63	58
2016	495	376	52	72	98
2017	870	374	134	74	127
2018	571	363	135	99	76

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

14,717,618,286

ONLY **4%** of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY

6,360,250

Records

EVERY HOUR

265,010

Records

EVERY MINUTE

4,417

Records

EVERY SECOND

74

Records

intouch
to be and to stay

Cyberchisel

The average total cost
of a data breach is

$3.86 MILLION

The average cost per
lost or stolen record in a
data breach is

$148

Yahoo holds the record for
largest data breach ever with

3 BILLION

compromised accounts


39 SECONDS
is how often a cyber
attack occurs


22%
of data breaches involved the
use of stolen credentials


The cost of lost business after
a breach for US organizations is
$4.2 MILLION

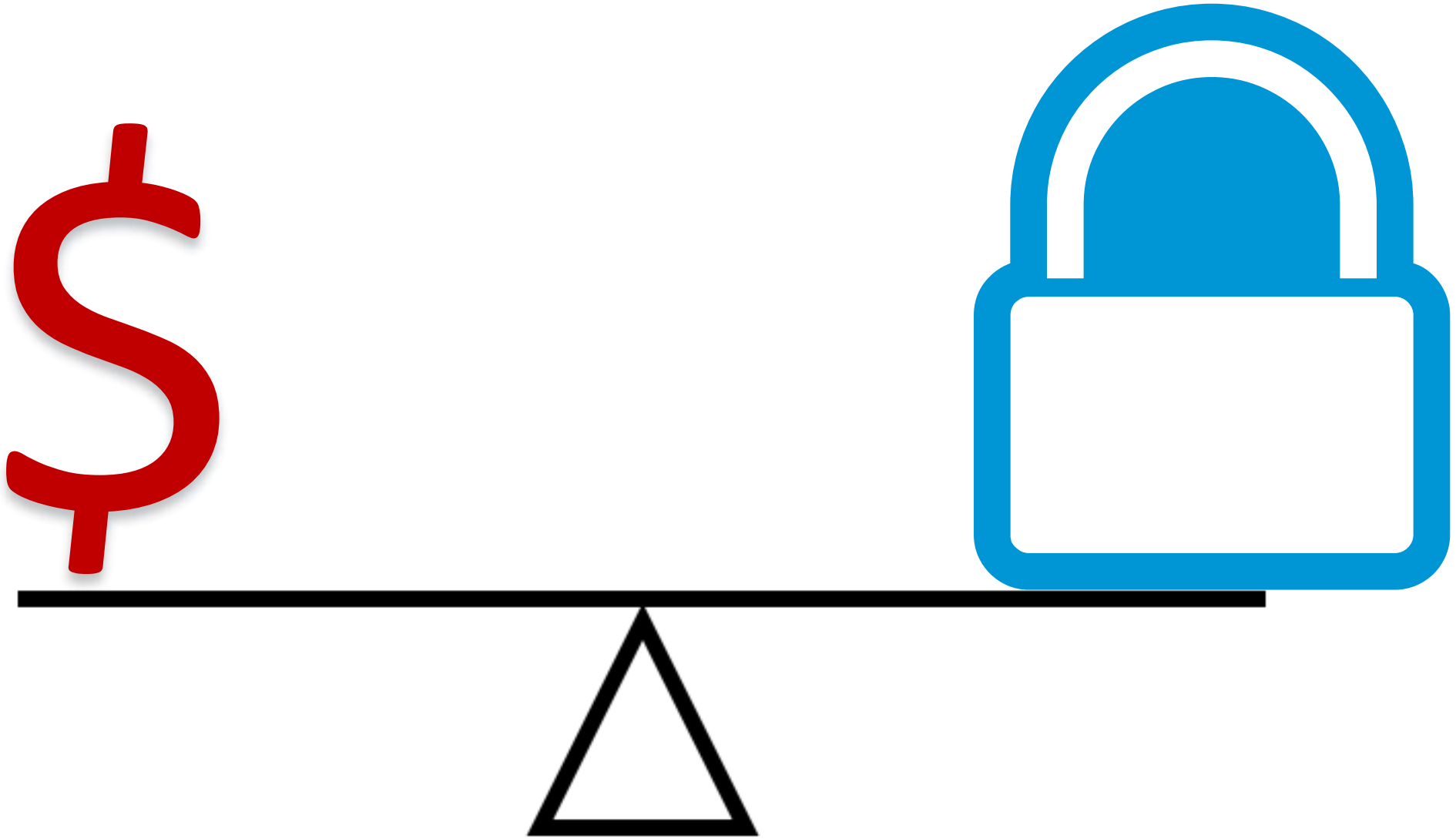
Privacy Breach Risks

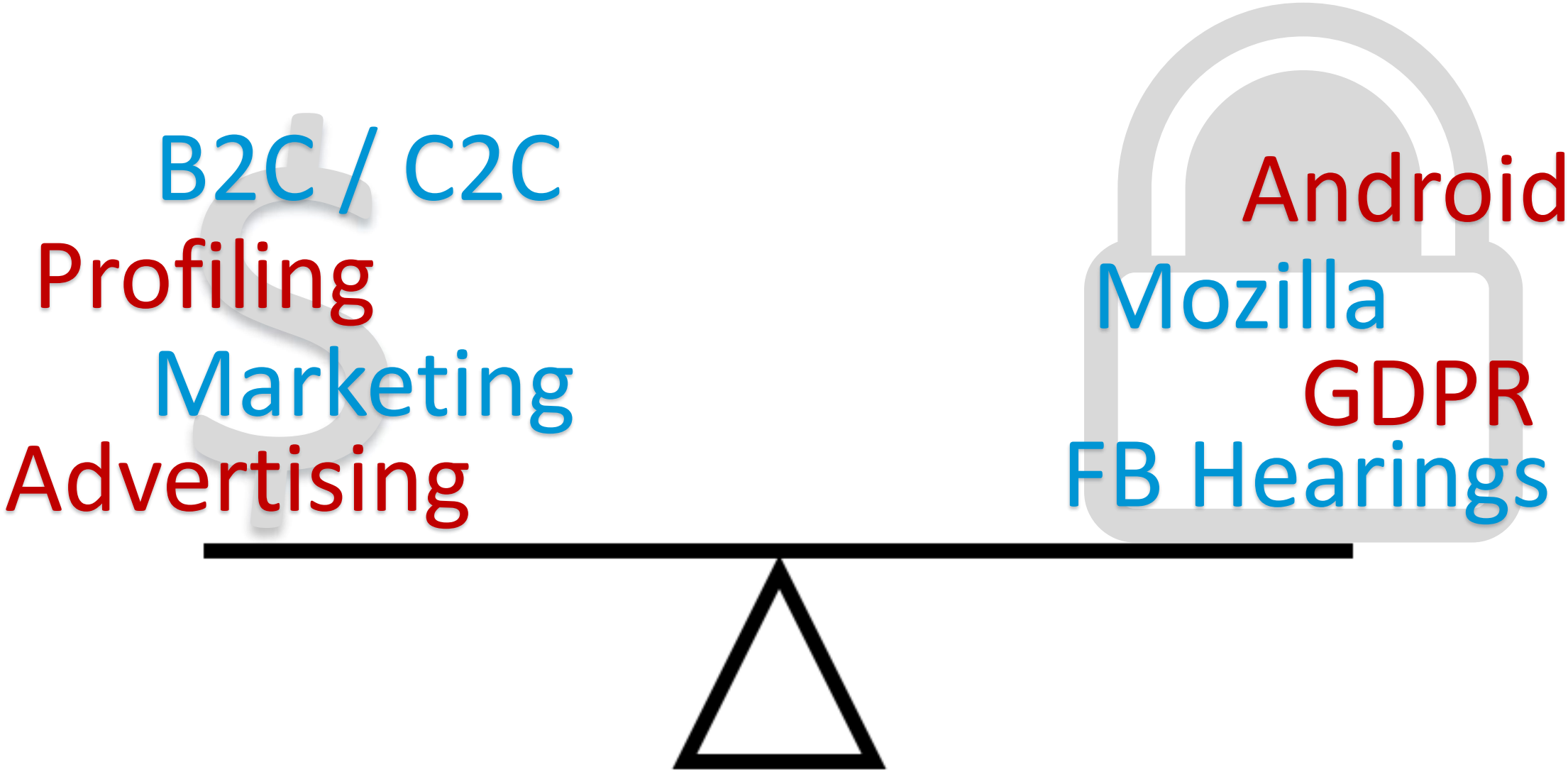
"22% of data breached in 2017 involved stolen credentials (Verizon)"

"36% of compromised data was personal info like name, birthday, and gender (Verizon)"

"27% of breaches caused by human error (IBM)"

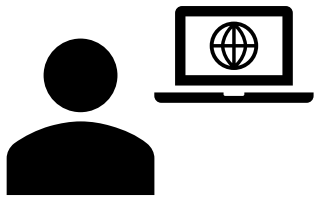
The Battle

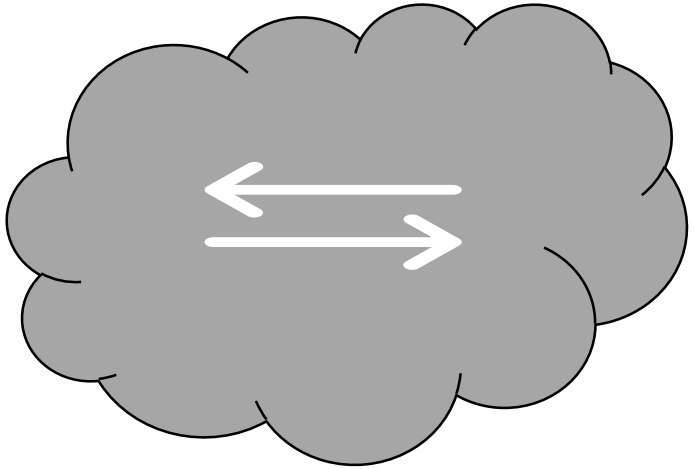


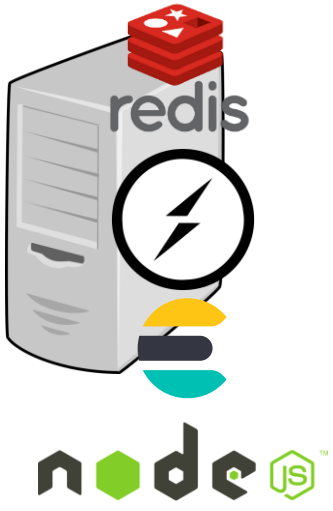

B2C / C2C
Profiling
Marketing
Advertising
Android
Mozilla
GDPR
FB Hearings

Privacy in Web Apps

A Typical Web Environment







Core Requirements

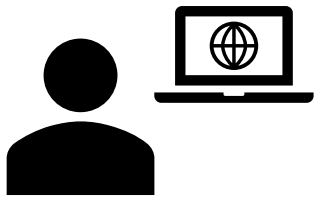
Privacy by Design

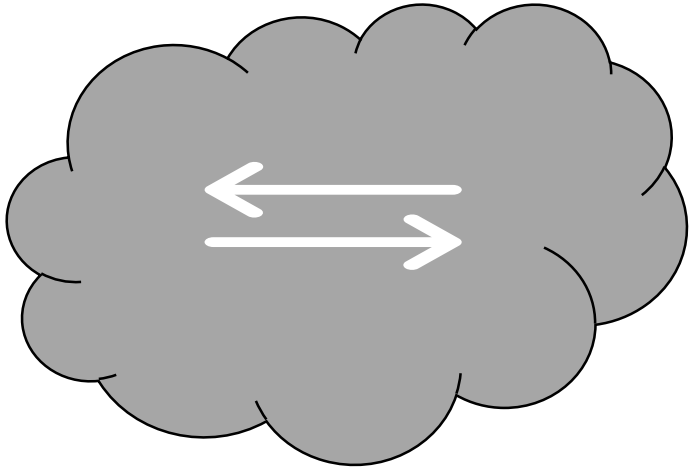
Ask for Explicit Consent

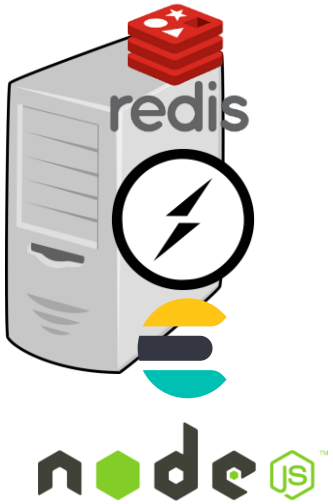
The Right to Be Forgotten

Providing Visibility and Transparency

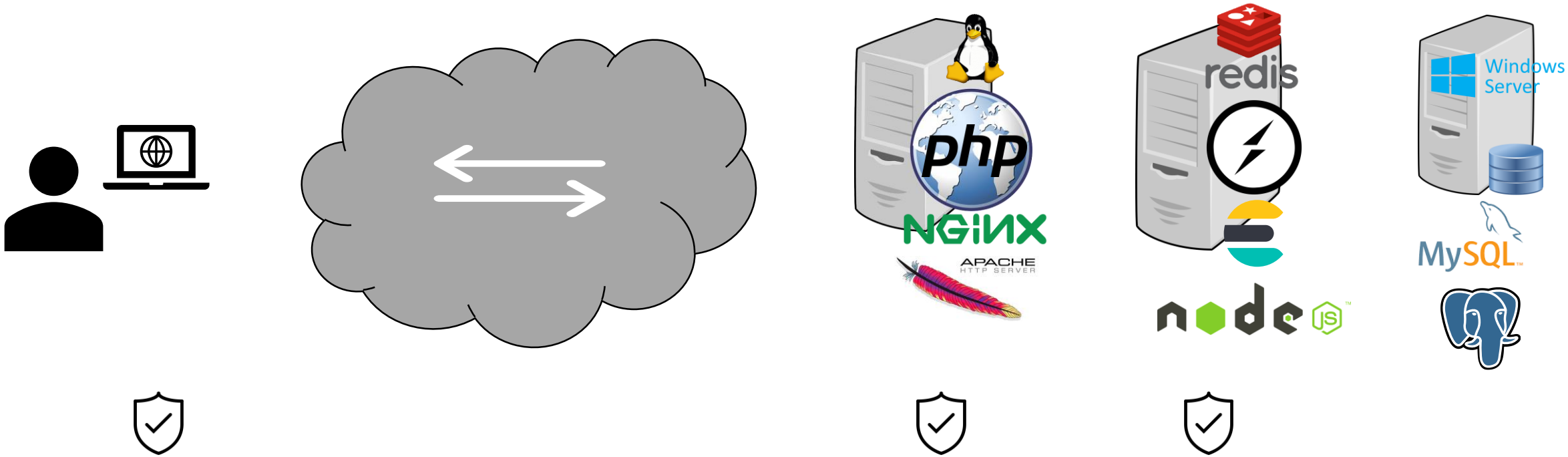
“Determine whether the web app really needs all the requested personal data”



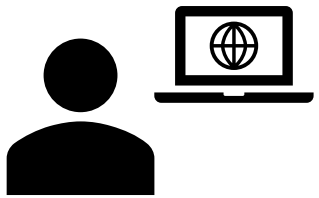


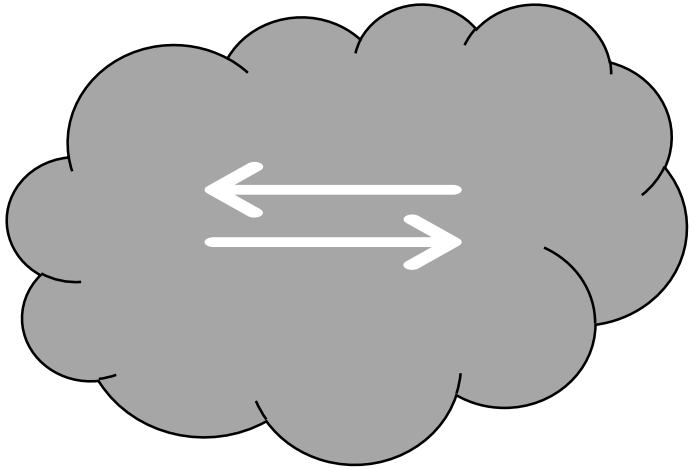


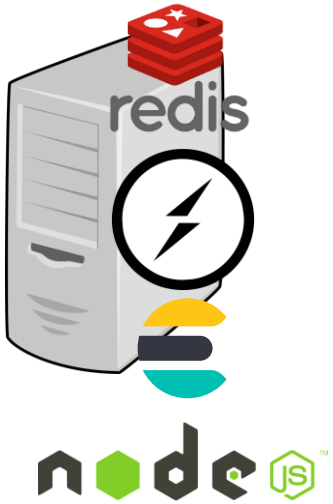
“Make sure sessions and cookies expire and are destroyed after logout”



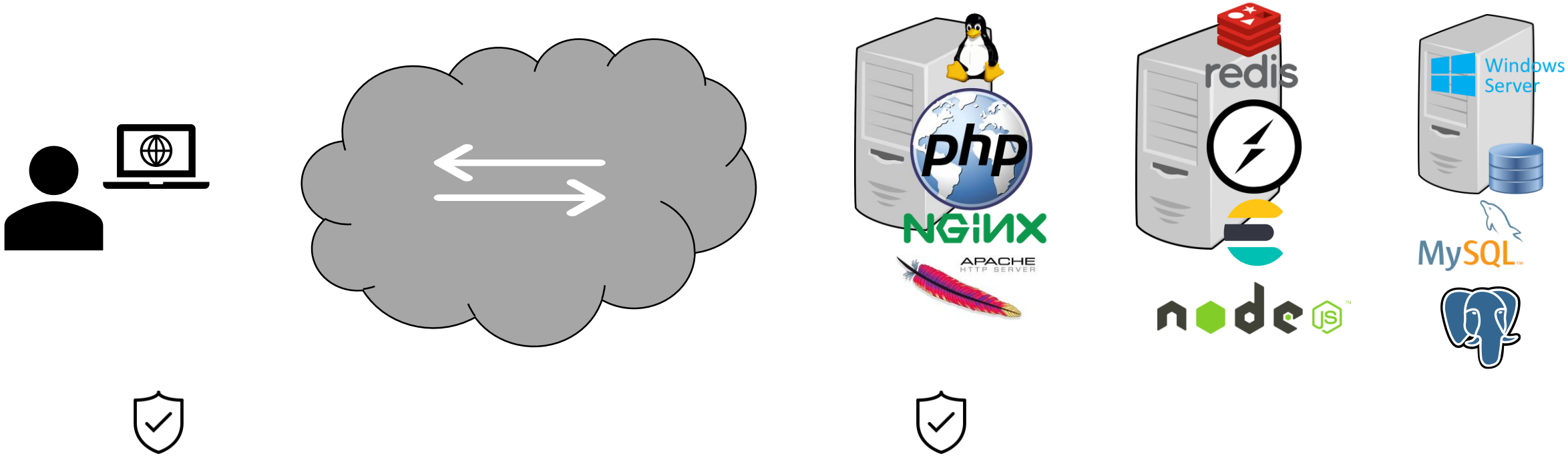
“Do not track user activity without their explicit approval / opt-in”



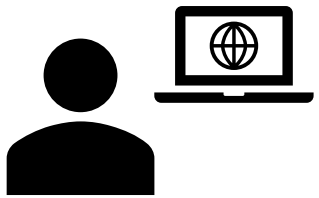


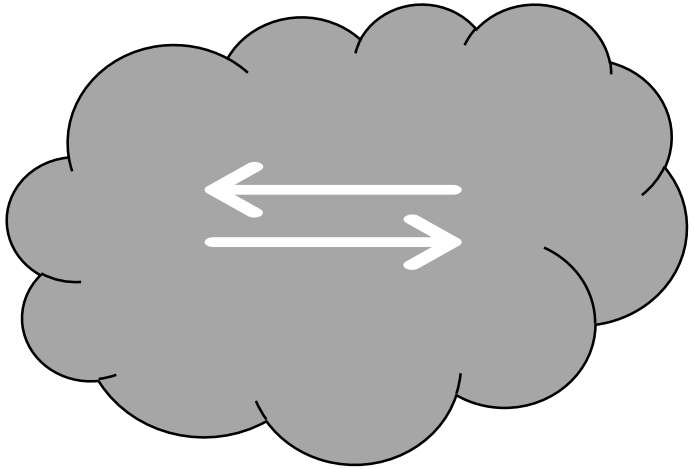


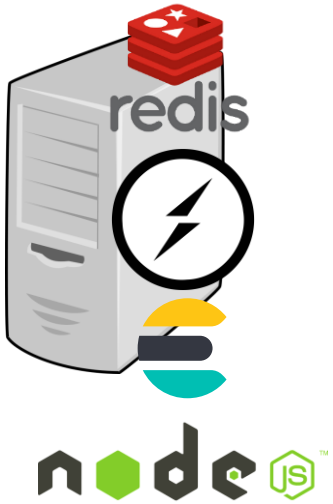
"Tell users about logs that save location or IP addresses"



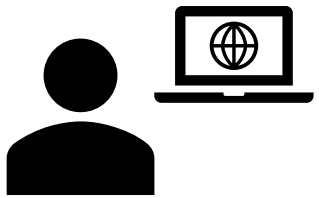
“Create a clear and easy-to-read terms & conditions and privacy policy”

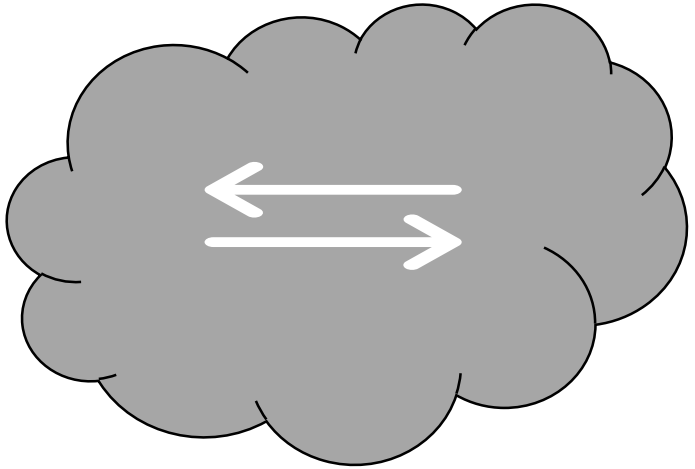


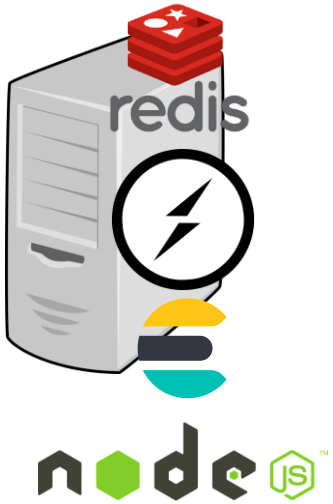




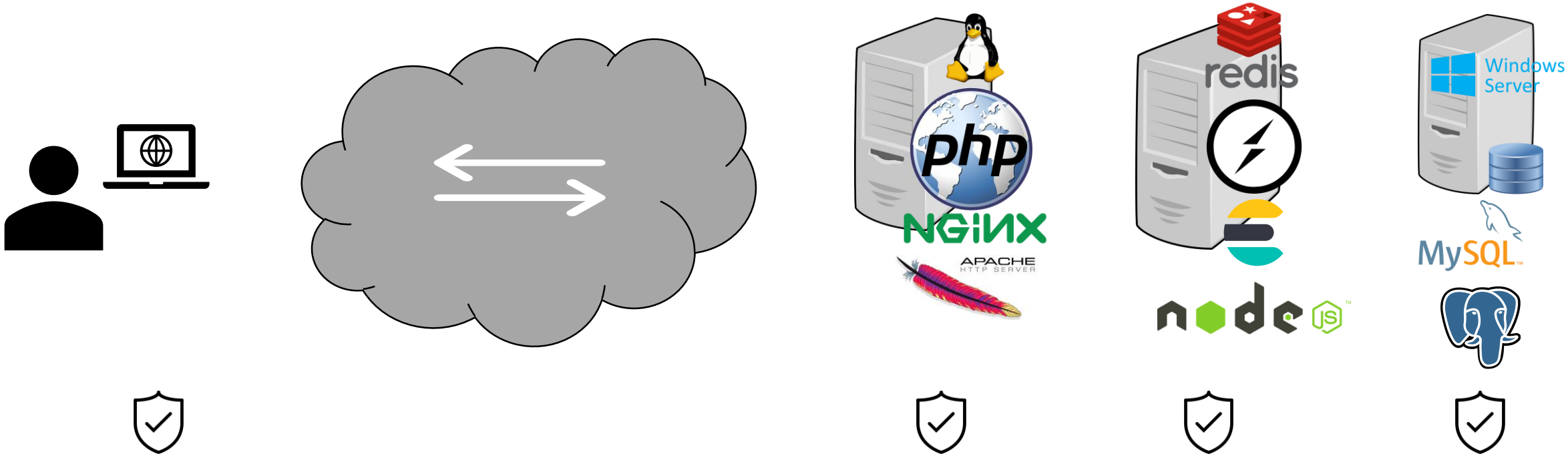
“Explicitly inform users about any data sharing with 3rd parties”



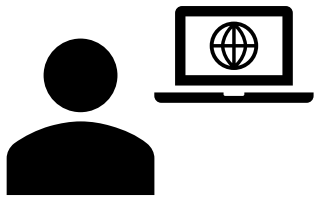


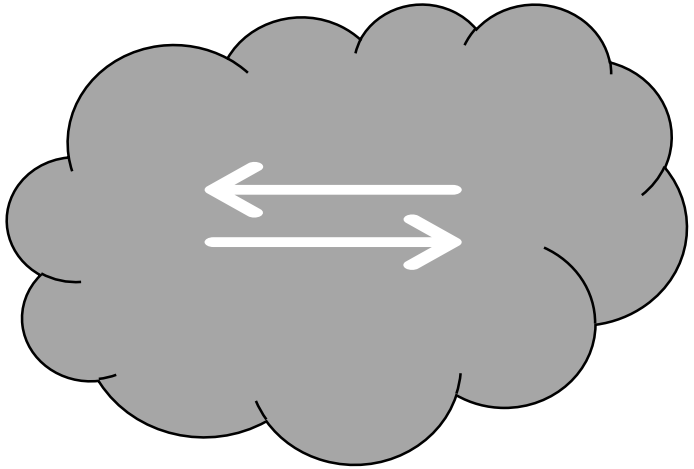


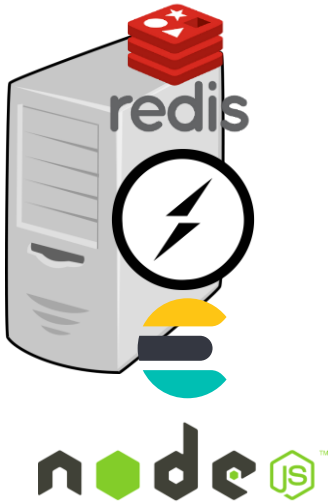
“Create clear policies for data breaches”



“Delete data of users who cancel their service”







Use OAUTH / SSO for data portability

“Enforce secure communications through HTTPS & HSTS”

“Encrypt all personal data and inform users about it”

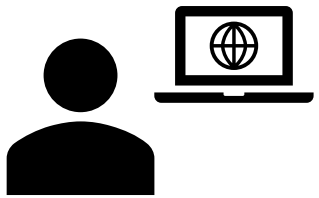
“Encrypt personal data from ‘web forms’ and inform users about it”

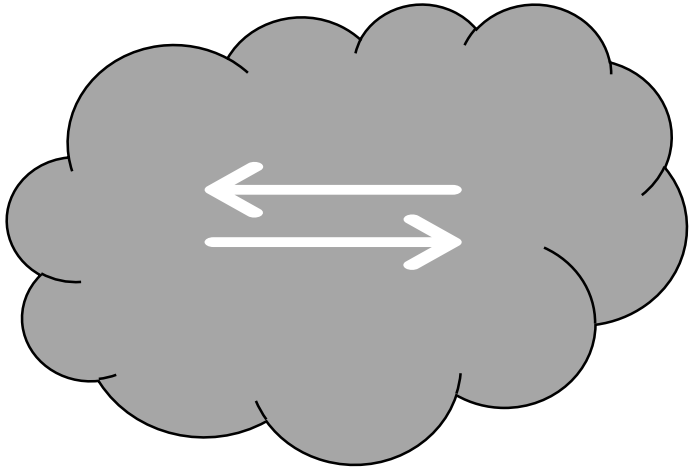
"Store logs in a safe place, preferably encrypted"

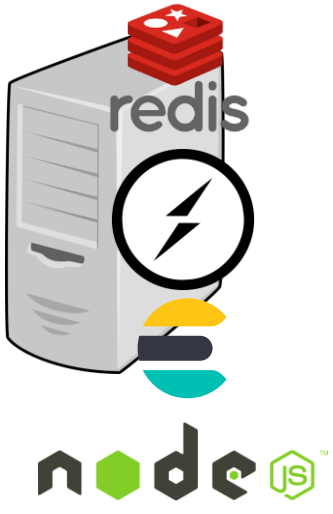
"Replace Security Questions with 2-Factor authentication"

“Patch web vulnerabilities asap”

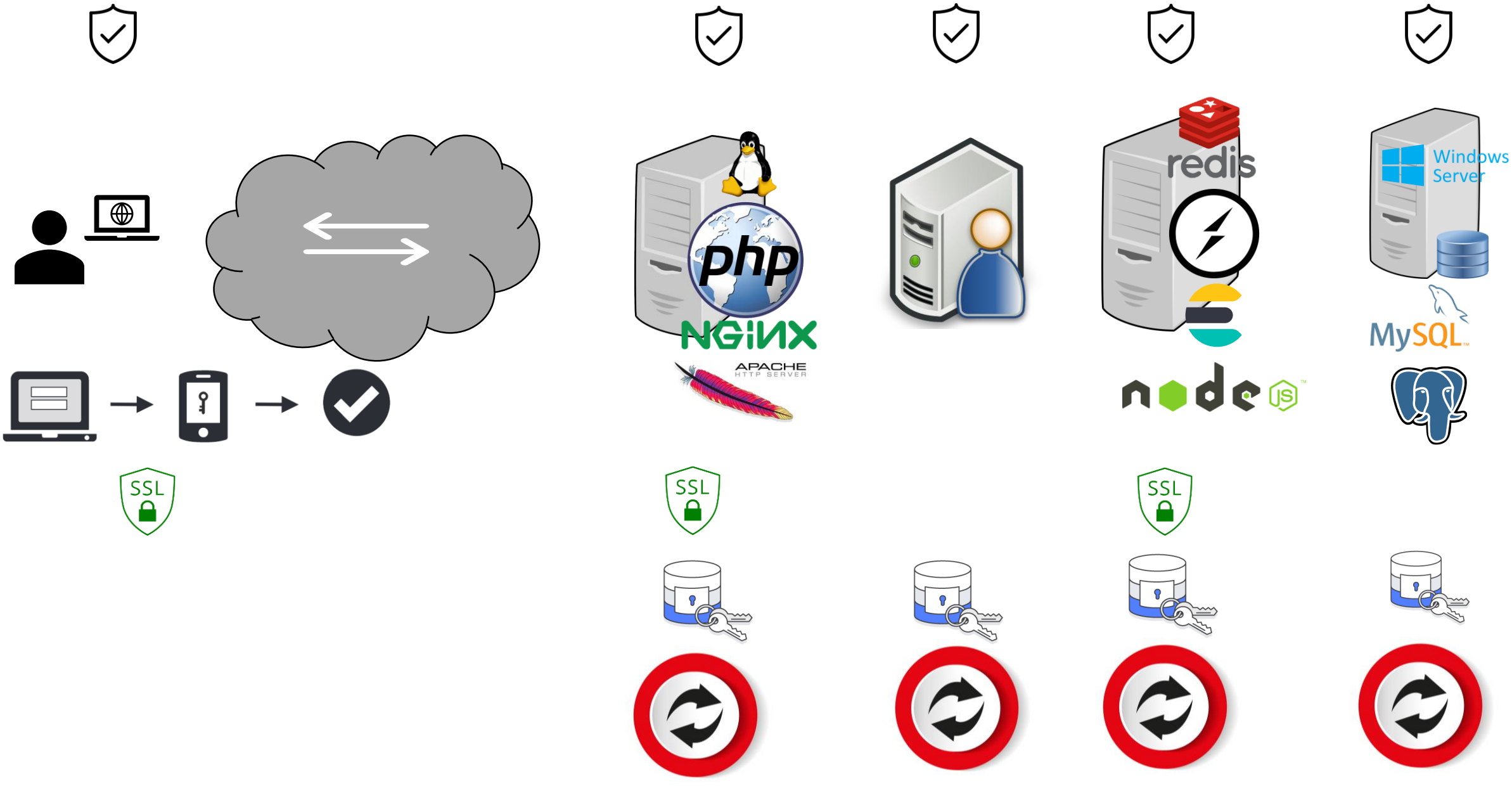
We must move from this setup…



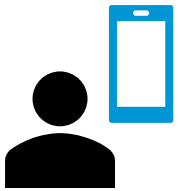


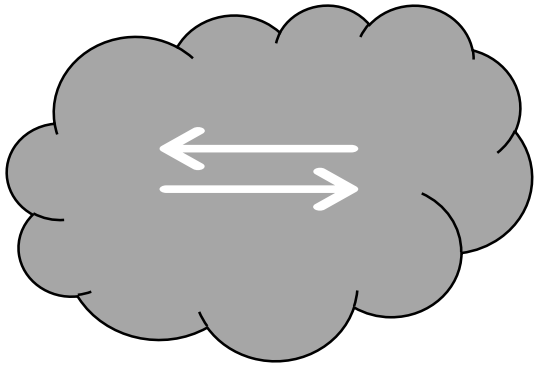


To this setup…

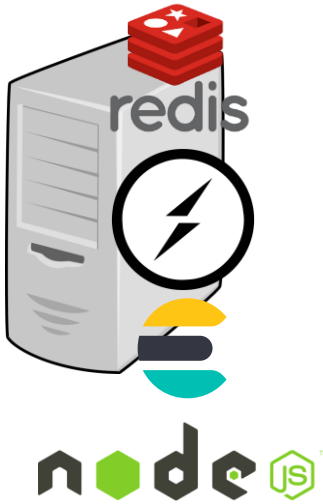


Then, we add Mobile Apps



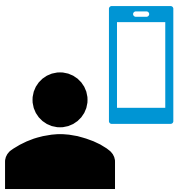


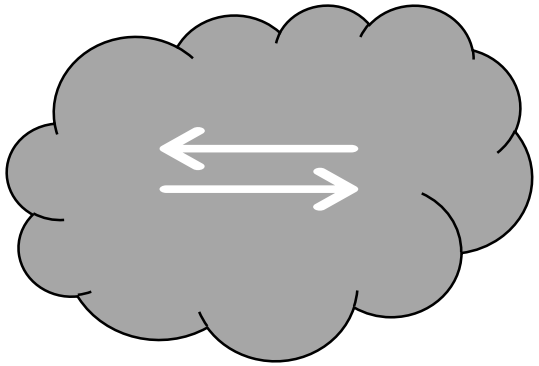

php
NGINX
APACHE
HTTP SERVER

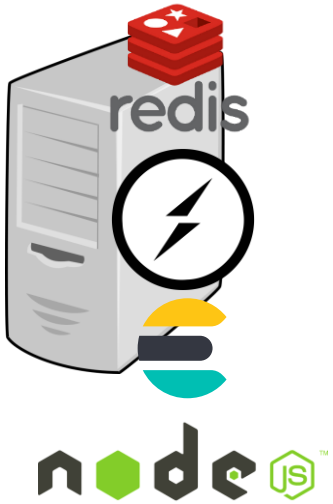

redis
node
JS


Windows
Server
MySQL

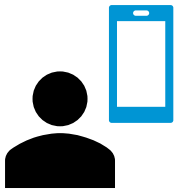
Ask for permissions on first need and only when needed

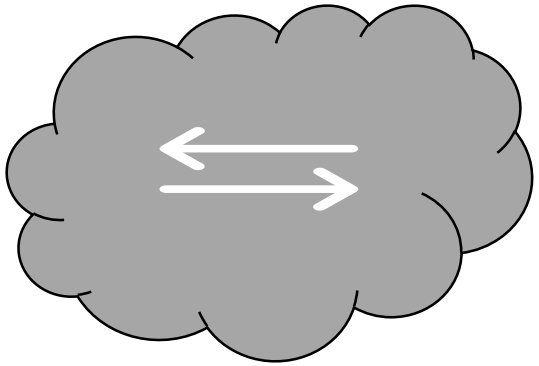


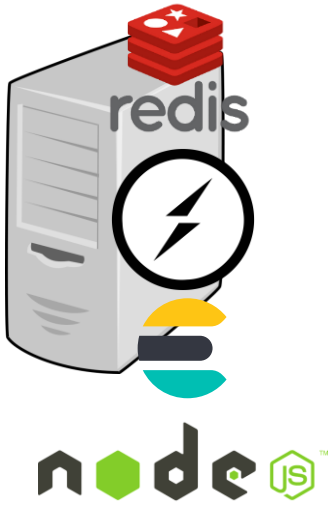




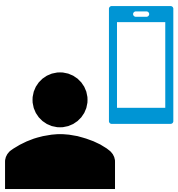
Don't store secrets in application code

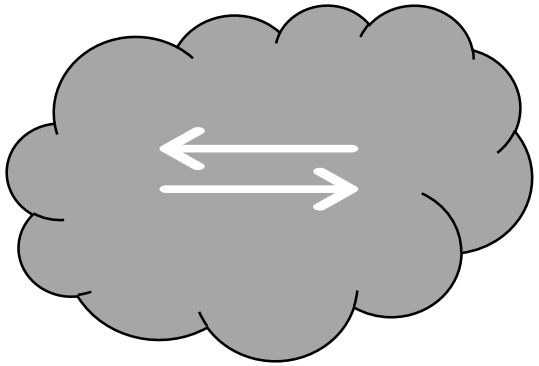


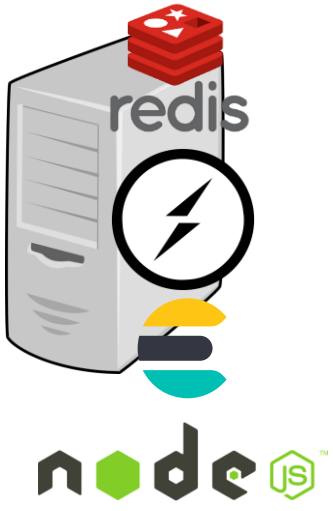




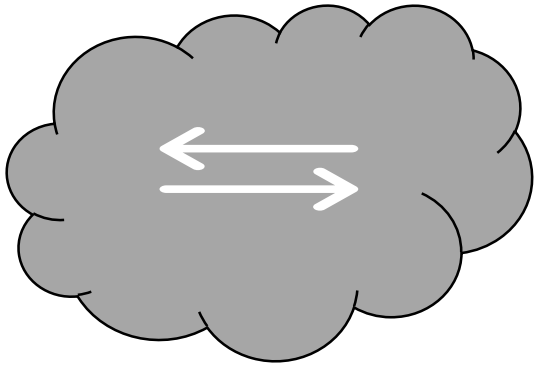
Check authenticity of SSL Certificates

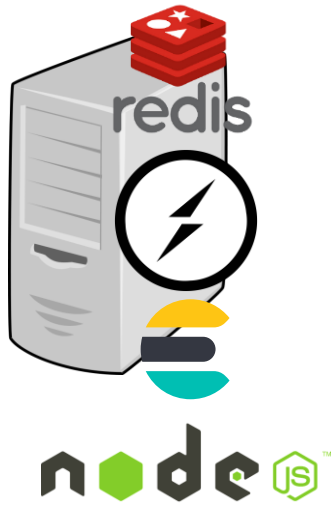




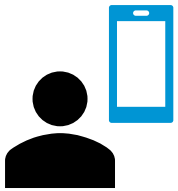


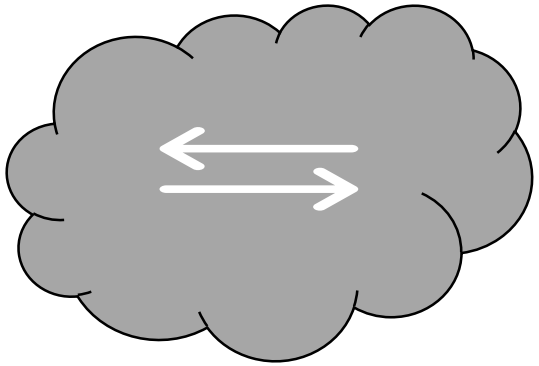
Use & enforce secure *session tokens*

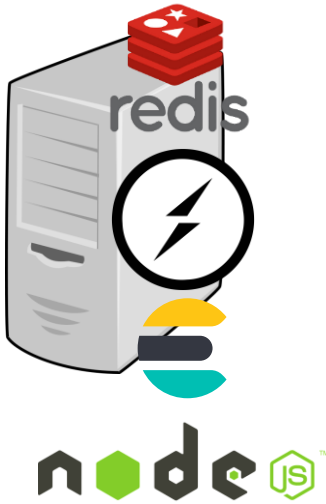




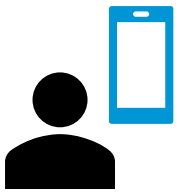
Use time stamps to avoid *replay attacks*

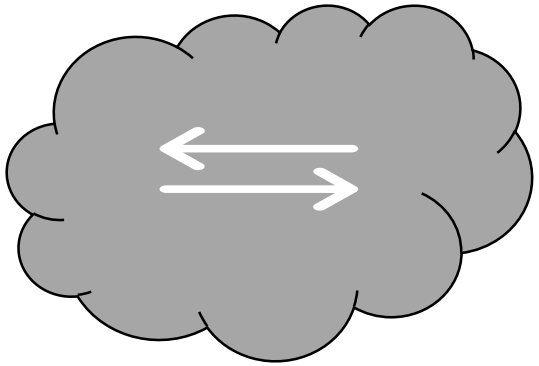


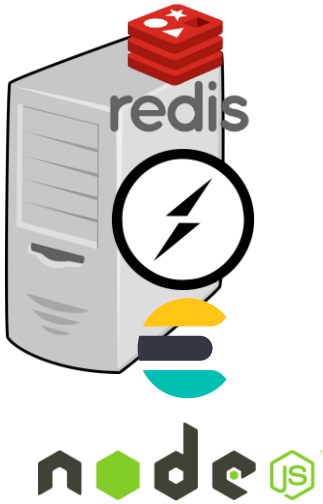




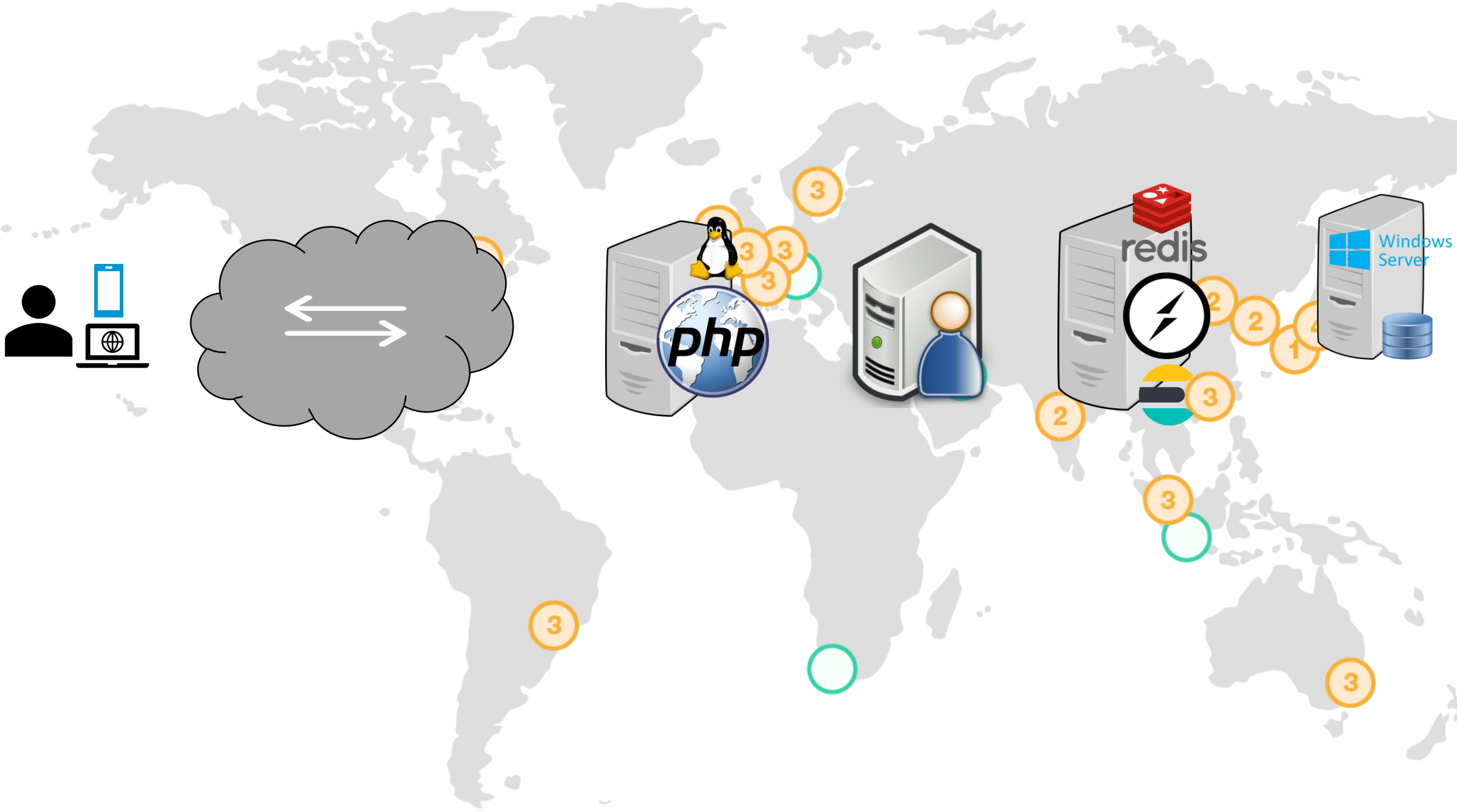
Encrypt data on local phone storage



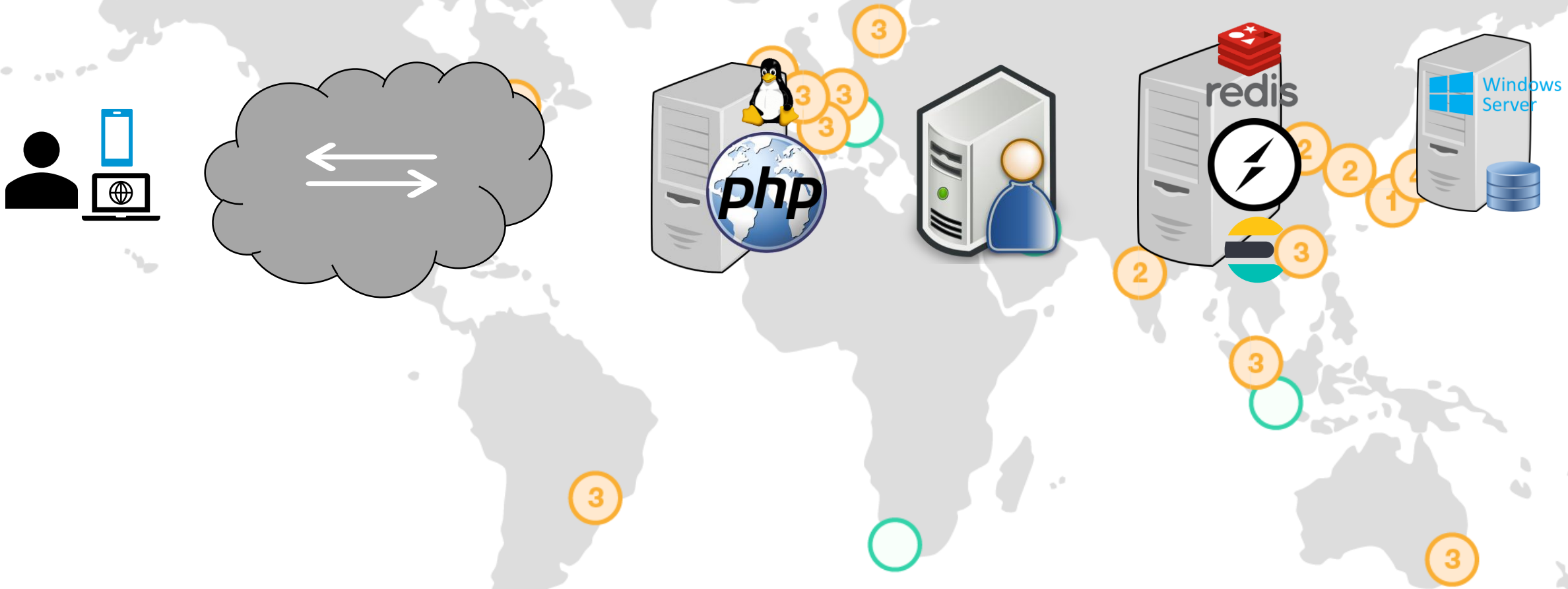




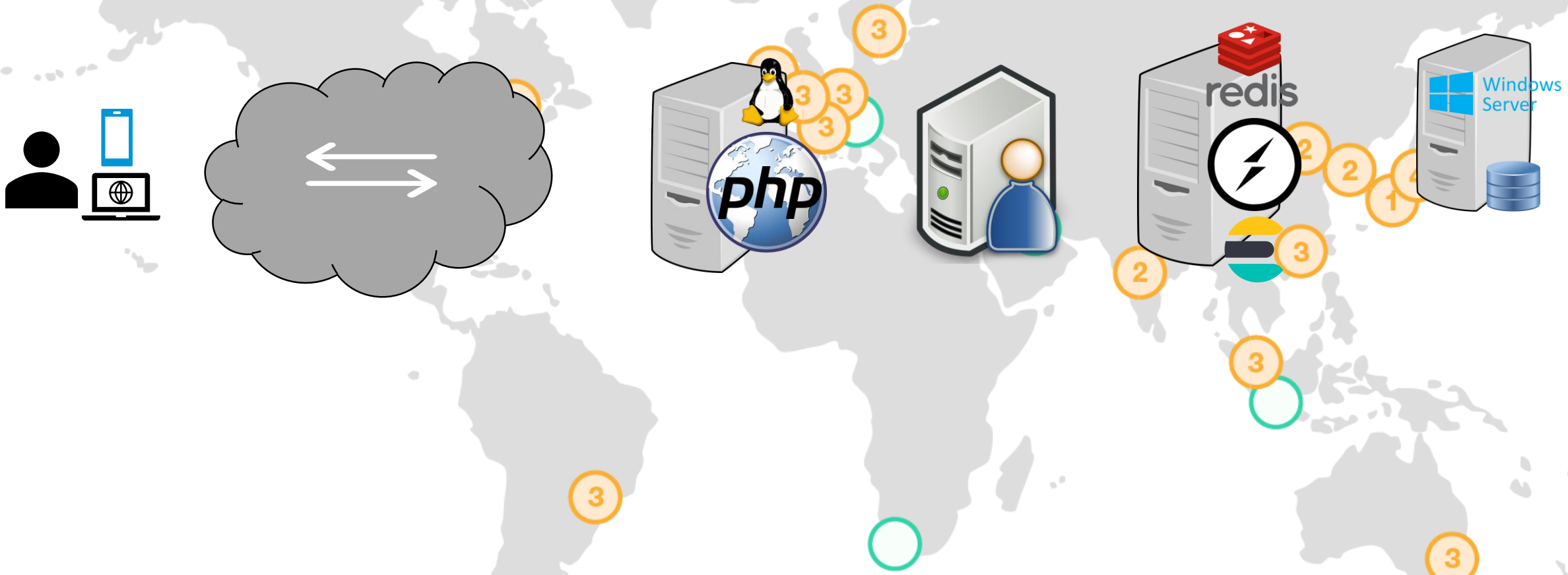
Then, we go On Cloud


redis
Windows
Server
php

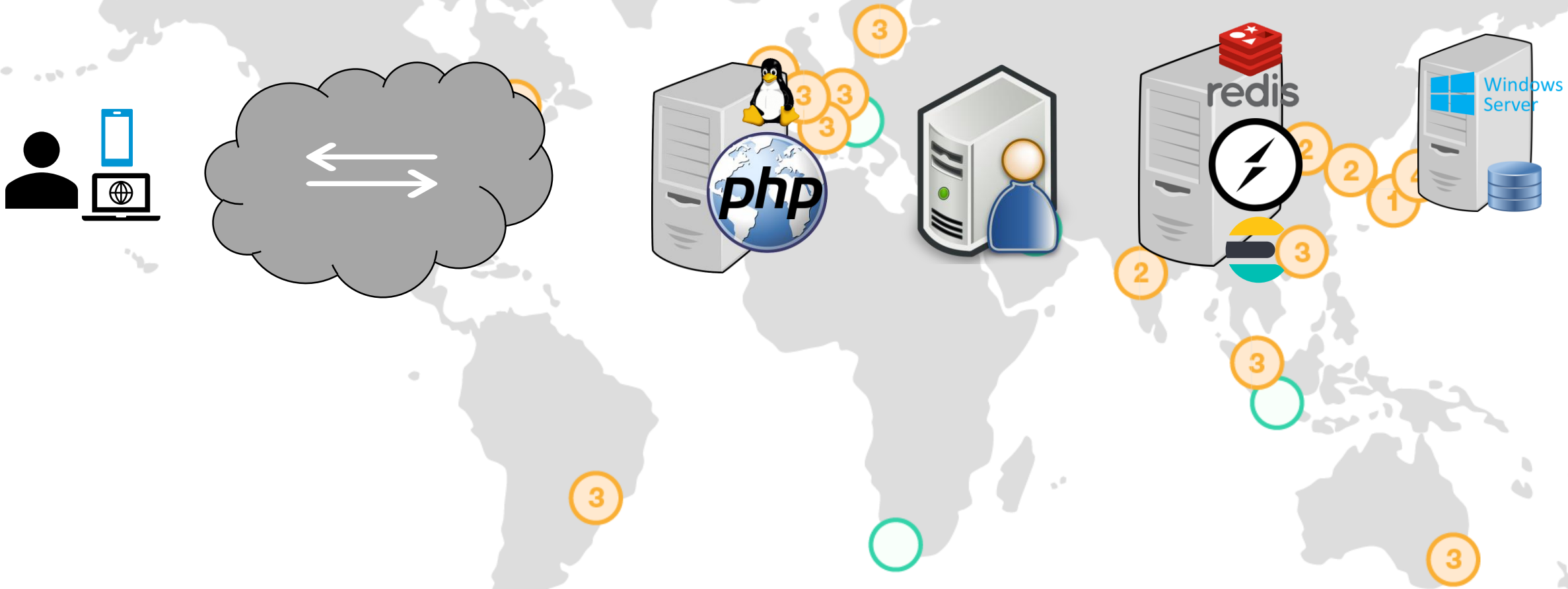
Be careful with cloud instance locations



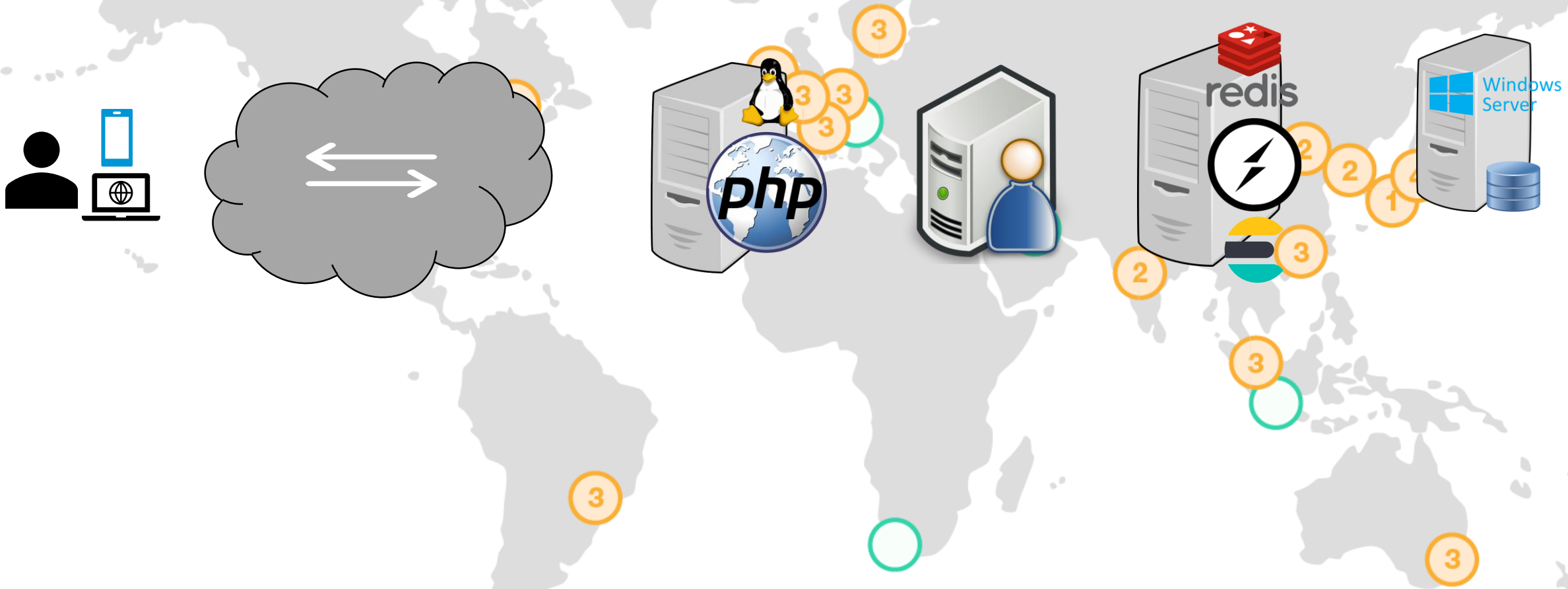
Wipe Out data before *Dumping Instances*



Use Private & Hybrid clouds for sensitive data



Check Cloud Providers for PCI Compliance



In conclusion…

It is NOT hard

It is just delicate

Build your checklist

And Always Check it!

we're always happy to help

get intouch with us today

intouch
to be and to stay

Cyberchisel

hibrid

ripply

Qatar
Office 04. 11° floor, Corniche Tower
Old salata, Doha, Qatar
P.O. Box: 37595

Lebanon (HQ)
3rd Floor. Bayada 11. Bayada
Metn. Lebanon

UAE
Office 507. 5th floor. Gateway Building - Bloc B
Dubai Media City. Dubai. UAE
P.O. Box: 502819

Kuwait
Panasonic Tower . 29th Floor . Fahad Al Salem St.
Kuwait City . Kuwait

Ukraine
Povitriana 10A . Lviv
Lviv Oblast . Ukraine