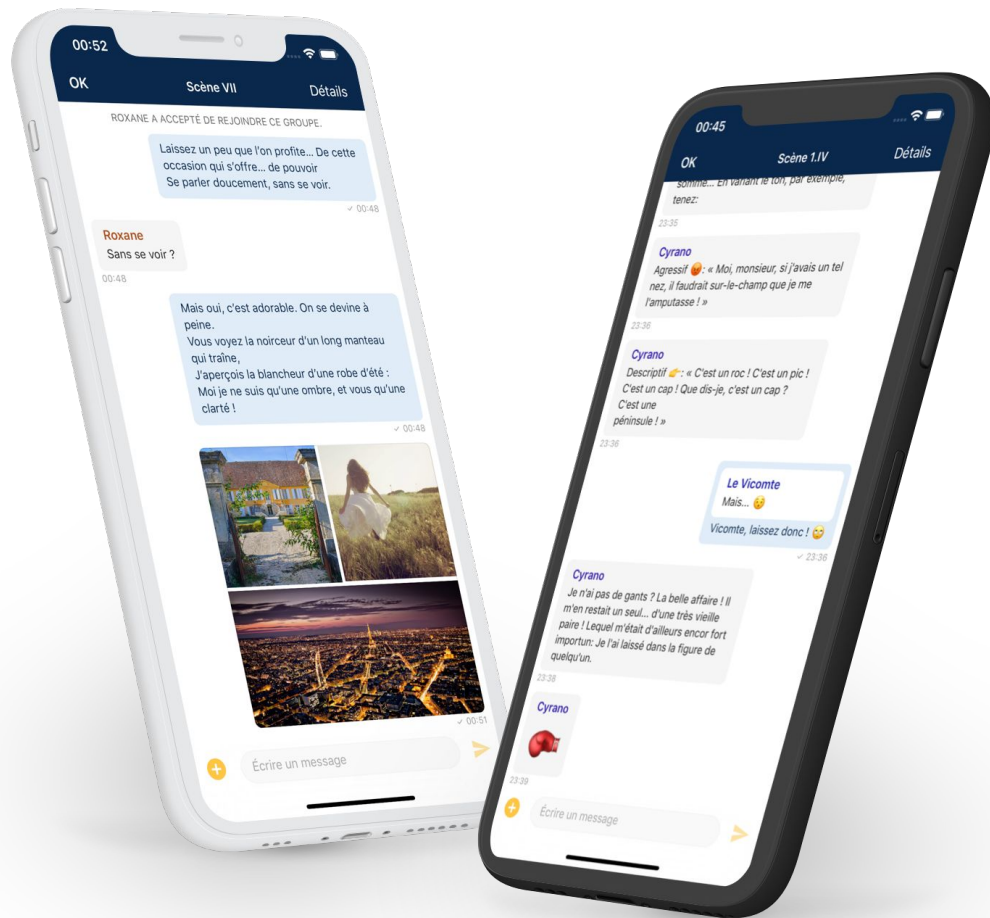




**La messagerie instantanée
la plus sûre du monde**



L'équipe Olvid.



Thomas Baignères

CEO

Docteur en cryptographie (EPFL)



Matthieu Finiasz

CTO

Docteur en cryptographie (ENS - X - UC Berkeley - INRIA)

Co-fondateur  CybelAngel



Cédric Sylvestre

Business Development

ESCP



Jacques-André Bondy

Product, Support & Marketing

ISG International



EPFL

informatiques mathématiques
inria

Reconnaisances



PRIX DU JURY
FIC 2020



PRIX DU PUBLIC
LES ASSISES 2020



**PRIX DE
L'INNOVATION**
LES ASSISES 2020



Olvid est la première messagerie instantanée certifiée CSPN par l'ANSSI.



**I-LAB
WINNER**
BPI 2020



Un écosystème fantastique.



CRYPTO
EXPERTS 



WILCO

SHAKE UP
BY WAVESTONE

platform58
l'incubateur de La Banque Postale

bpi**france**

Generate 
S'unir pour innover

W*i*
 BNP PARIBAS



LA
PLACE
STRATÉGIQUE

Sources des fuites de données en entreprises.



Ce que l'on voit à travers



CybelAngel

Négligence

90%

La malveillance est
rare

Tiers

95%

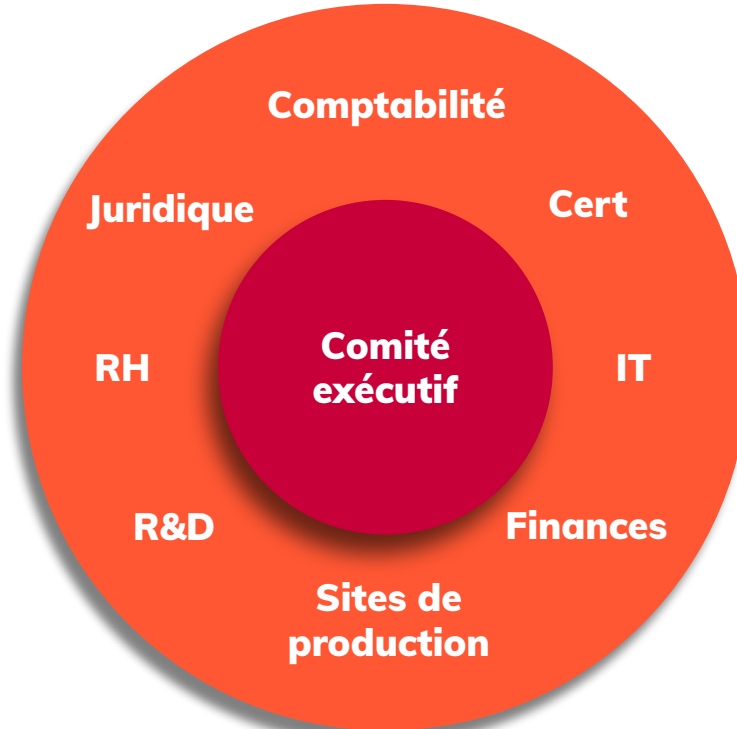
Sous-traitants,
partenaires,
avocat, etc.

Tous les niveaux

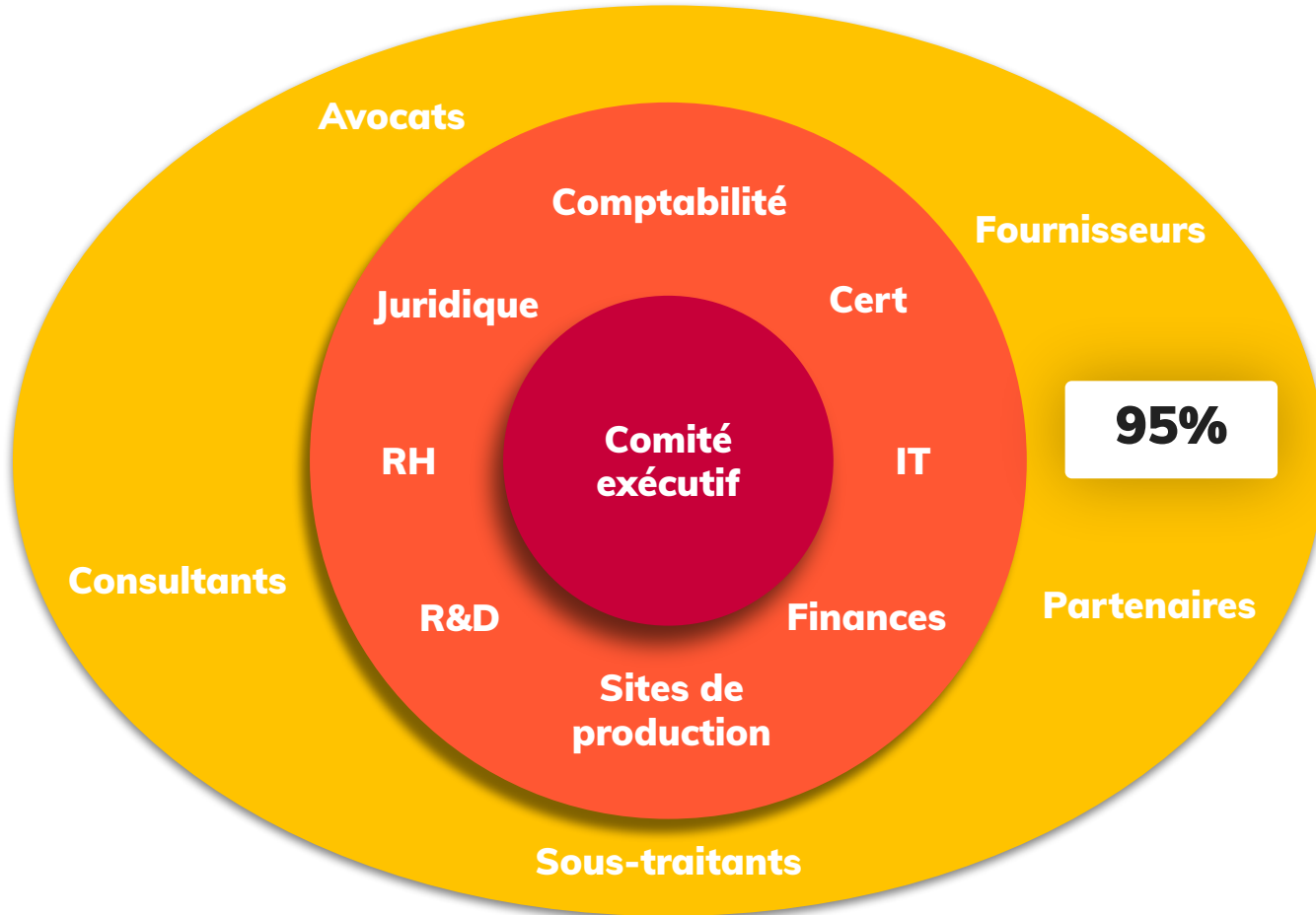
Top management,
consultants, RH, R&D

Et tout ce que l'on ne voit pas...

Cas d'usage.



Cas d'usage.



Messageries : plutôt WhatsApp à Matignon et Telegram à l'Elysée

Fidèles à leurs habitudes de juppéistes, Édouard Philippe et ses collaborateurs continuent à échanger par WhatsApp alors qu'Emmanuel Macron et ses ministres utilisent Telegram.



Emmanuel Macron a commencé à utiliser Telegram alors qu'il était à Bercy pour préparer sa campagne en toute discrétion. Olivier Thomas - AFP/Philippe Lopez



?!?!

Cas particulier de la messagerie instantanée

**Pouvez-vous faire confiance à
WhatsApp, Telegram, Signal ?**

Executive Summary.



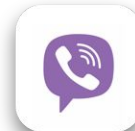
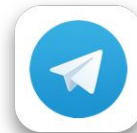
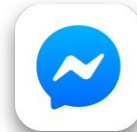


Non

Messageries proposant du chiffrement de bout-en-bout.

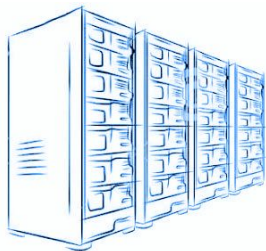


Chiffrement systématique



Chiffrement optionnel

Une sécurité centralisée.



Serveur de
distribution
des messages

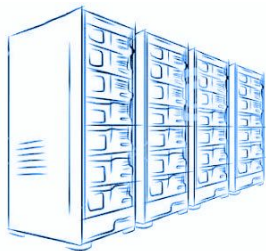
Distribue les messages

- Disponibilité
- Qualité de service
- Tolérance aux pannes

Aucun rôle dans la sécurité

- Chiffrement de bout en bout

Une sécurité centralisée.



Serveur de
distribution
des messages

Distribue les messages

- Disponibilité
- Qualité de service
- Tolérance aux pannes

Aucun rôle dans la sécurité

- Chiffrement de bout en bout



Annuaire
centralisé
des utilisateurs

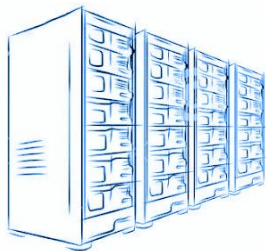
Distribue les identités numériques

- Usurpation d'identité
- Déchiffrement ciblé
- Espionnage de masse
- Exploitation des données personnelles

Clé de voûte de toute la sécurité

- Nécessite de faire confiance à l'opérateur

Une sécurité centralisée.



Serveur de
distribution
des messages

Annuaire
centralisé
des utilisateurs



Distribue les messages

- Disponibilité
- Qualité de service
- Tolérance aux pannes

Aucun rôle dans la sécurité

- Chiffrement de bout en bout

Distribue les identités numériques

- Usurpation d'identité
- Déchiffrement ciblé
- Espionnage de masse
- Exploitation des données personnelles

Clé de voûte de toute la sécurité

- Nécessite de faire confiance à l'opérateur



Toutes les solutions reposent sur un annuaire central.

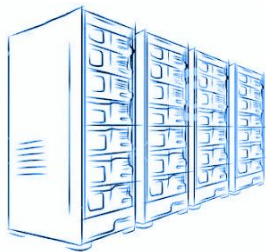


Chiffrement systématique

Toutes ces solutions ont le même **modèle de sécurité**.

Elles imposent un **annuaire central** sur lequel vous n'avez aucun contrôle.

Olvid : une solution sans annuaire centralisé.



Serveur de
distribution
des messages

Annuaire
centralisé
des utilisateurs

**Cryptographie
de pointe**

**Aussi simple que
WhatsApp**

**Pas de données
personnelles**

**Pas de fuites
de données**

**Pas d'usurpation
d'identité**

« Zero Trust »

**Pas de
métadonnées**

A user centric app with a B2B business model.



Free App

Messages
Attachments
Photos & videos
Secure group chat



Paid Features

Secure calls
Video conferencing
IT Integration
Desktop version

Professional communication tools.



Email

**Microsoft
365**

Proxies

**Google
Workspace**

Antivirus

VPN

PGP

Firewall

?

Professional communication tools.



Email

**Microsoft
365**

Proxies

**Google
Workspace**

Antivirus

VPN

PGP

Firewall

WhatsApp
ㄥ(ツ)ㄥ



Why WhatsApp.



Easy to use

**One App for
Friends & Family
Colleagues**

“Free”

Les grandes questions.



Où les données
sont-elles stockées ?

Comment l'utilisateur
accède-t-il à ses
données ?

Comment sont-elles
chiffrées ?
Qui détient les clés ?

Une attaque de
masse est-elle
possible ?

Contre qui veut-on se
protéger ?

Une attaque ciblée
est-elle facile ?

Contre qui veut-on se protéger ?



Les utilisateurs

Un concurrent

Un hacker

Un état

Globalement identique

À quel point l'utilisateur
risque-t-il se tromper ?

Pourra toujours faire une
attaque ciblée

Où les données sont-elles stockées ?



Cloud US

Cloud
« souverain »

On premise

On device

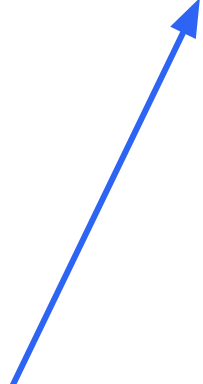
Sujet au Cloud Act, etc.



À éviter (cher et peu sûr)



Pas applicable à tous
les cas d'usage



Comment sont-elles chiffrées ? Qui détient les clés ?



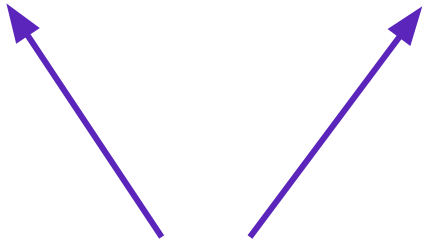
Pas de chiffrement

Chiffrement de
disque

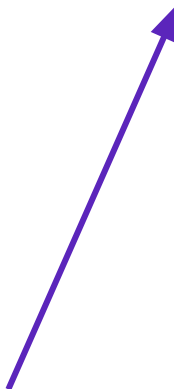
Chiffrement par
mot de passe

Chiffrement par
une clé utilisateur

N'apporte pas de sécurité



Illusion de sécurité



Comment l'utilisateur accède-t-il à ses données ?



Login &
mot de passe

Double
authentification

Client web

Application dédiée
& cryptographie

Simple contrôle d'accès :
Nécessite de faire
confiance au service

Vol de clé « facile »

Une attaque est-elle facile ?



Attaque de masse

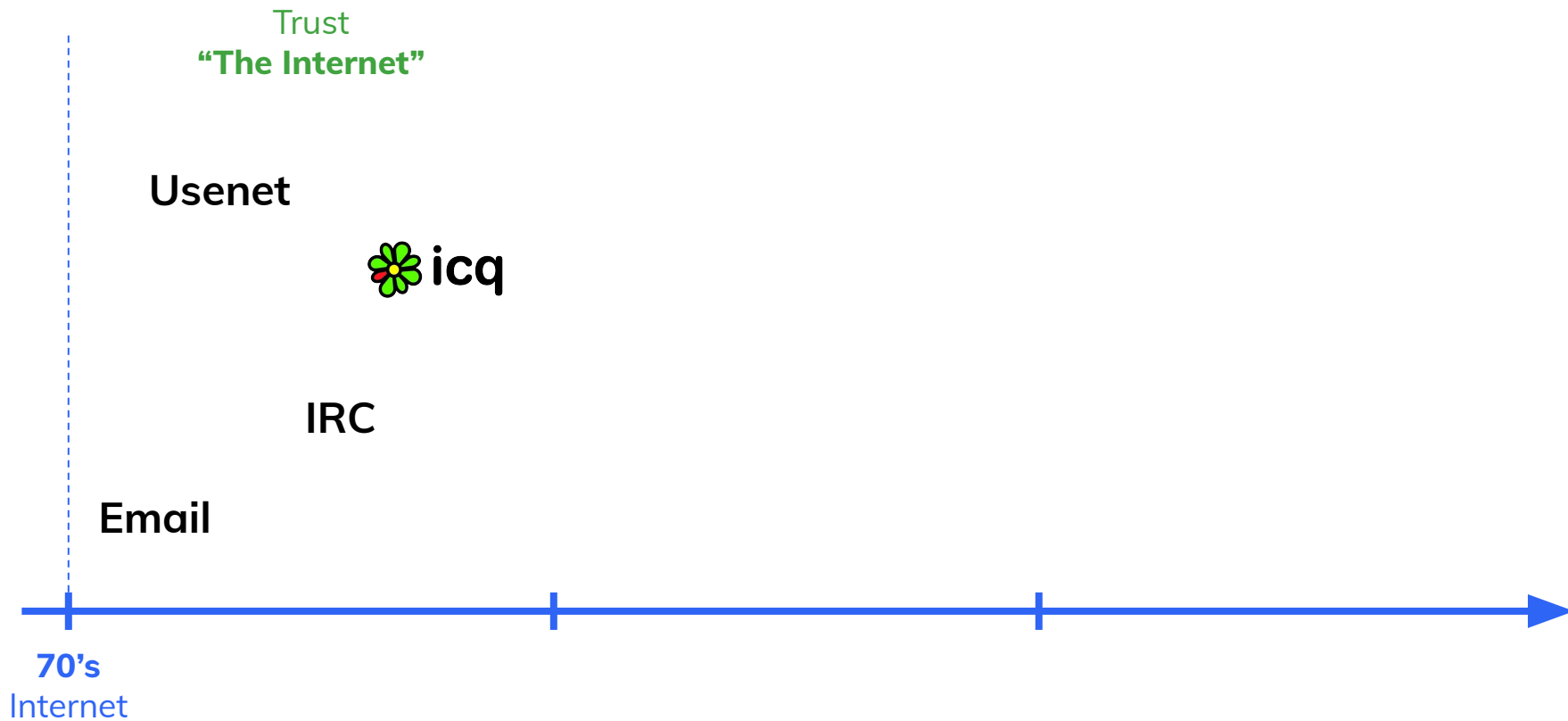
- Données centralisées
- Niveau de protection des serveurs
- Contrôle d'accès (configuration)

Attaque ciblée

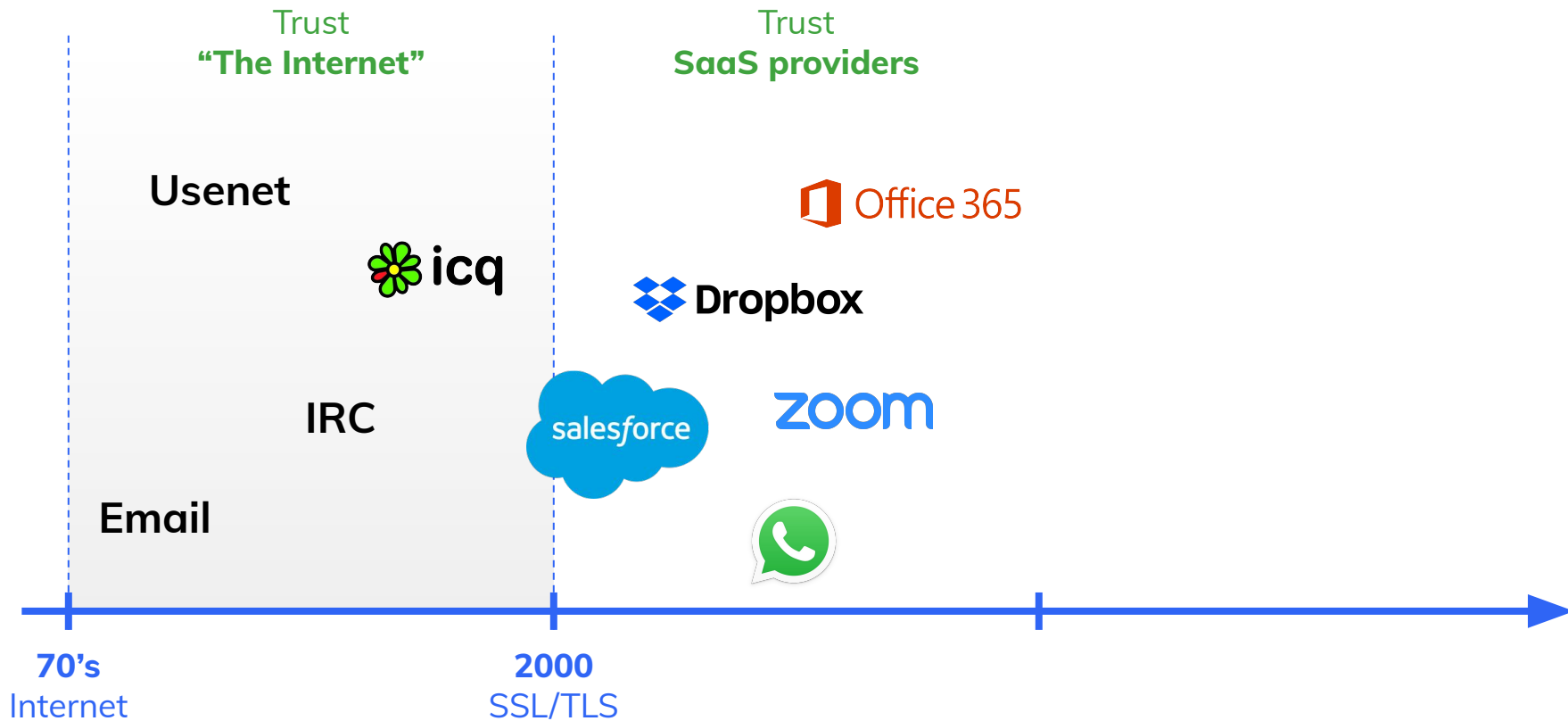
- Vol de mot de passe
- Interception de SMS
- Phishing ciblé
- Intrusion sur un ordinateur ou un téléphone
- Vol de device

Quel coût ? Quel ROI pour un adversaire ?

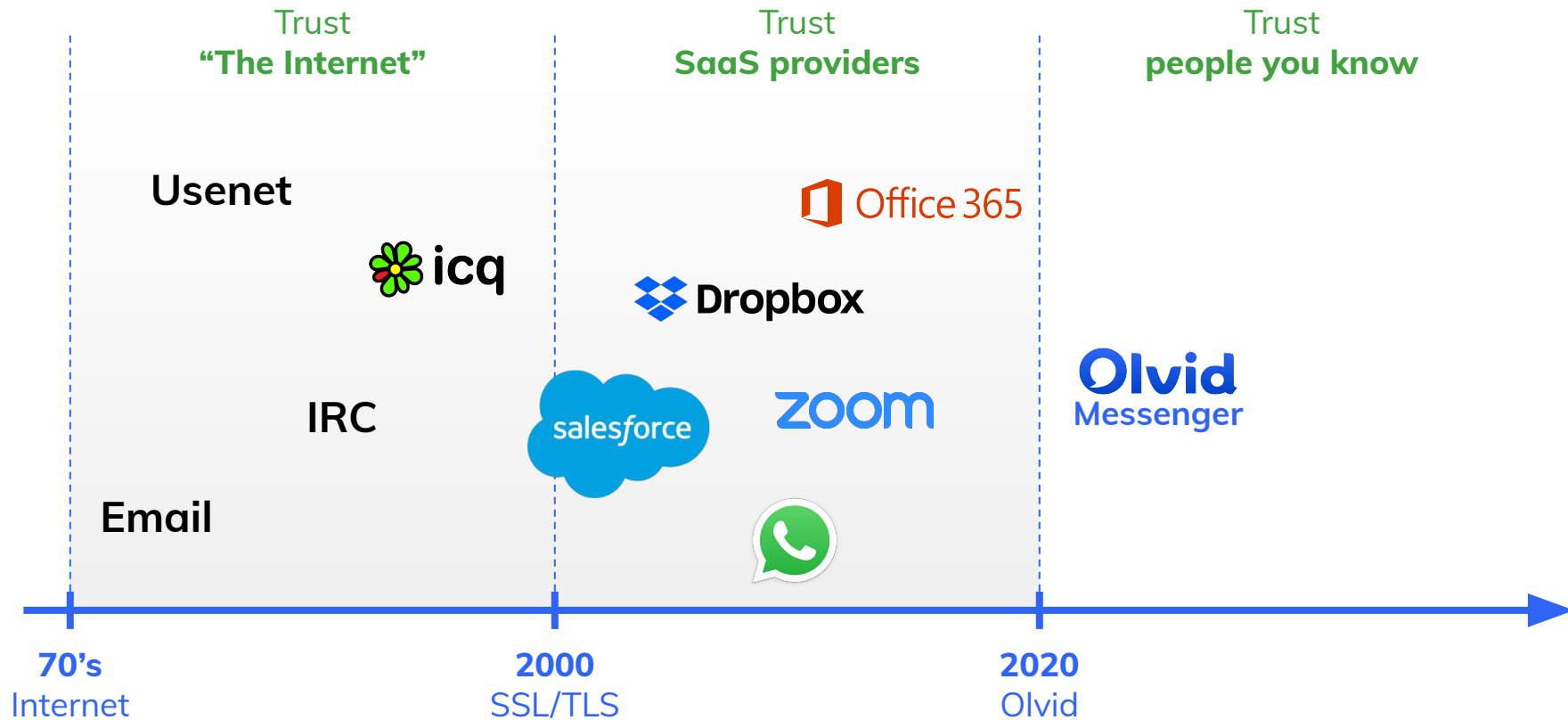
What's Old.



What's Up.



What's Next.



Nous contacter.



Olvid - WAI BNP Paris
19 Boulevard Poissonnière
75002 Paris
France



Assistance Olvid



contact@olvid.io



+33 6 61 57 64 51