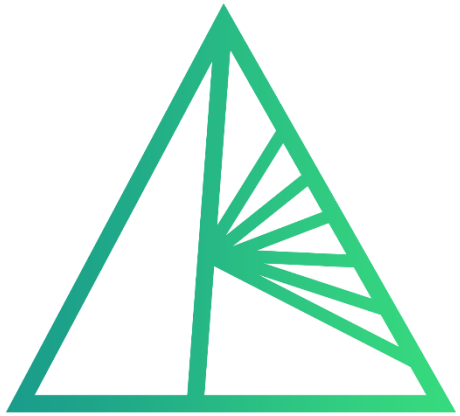


PRISME

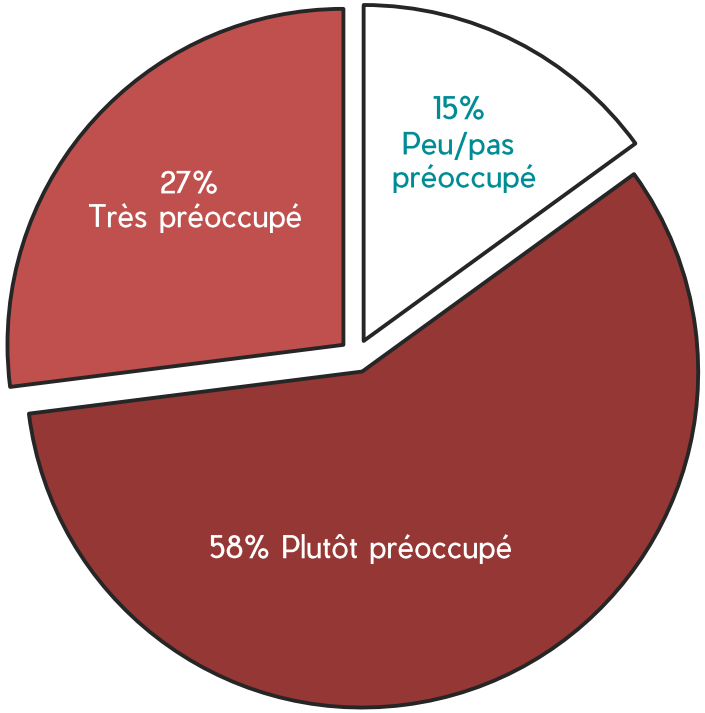
Une solution pour reprendre le contrôle des données personnelles sur son smartphone

La collecte de données massive est problématique pour les usagers

On assiste à un "siphonage" des données personnelles (navigation web, capteurs de géolocalisation, IoT...) (1)

Un sujet de préoccupation majeur, en hausse pour les Français (2)

Qui se traduit par une défiance des usagers sur l'usage de leurs données personnelles.



ETAT DES LIEUX

- Entreprises : 1ère étape RGPD (traité au minimum aujourd'hui)
- Usagers :
  - Peu / Pas d'outils permettant de se protéger
  - Hausse des Addblockers / cookies blockers...
  - 3/5 des usagers sont « Résignés » (3)

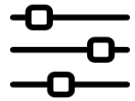
L'usager subit et ne peut choisir

https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare
https://www.csa.eu/fr/survey/les-fran%C3%A7ais-et-la-protection-de-leurs-donnees-personnelles
https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&context=asc_papers

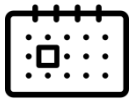
Or la principale source de collecte des données est le Smartphone

Navigation web
(profiling & retargeting)

Géolocalisation
(GPS / Tracking Wifi /Tracking Bluetooth)



Collecte capteurs
(données de santé et assurances,,,)



Collecte système
(agenda / contacts / messages / carte SD)

Caméra
(activation à distance, captation visuelle)

Microphone
(activation à distance)

Prisme, un ensemble App + Cloud qui protège le smartphone sans changer les habitudes du consommateur

En permettant à l'usager de maitriser la confidentialité des données issues de son smartphone

Choix des données partagées

Hiérarchisation des données transmises

Réglage de la sensibilité des données (ex: géolocalisation, Identifiant Web)

Créations de fake datas

Sans modifier les habitudes de l'usager

(la plus simple et la plus transparente possible)

Le client peut continuer à utiliser ses Apps favorites

Protection de l'usager

- Informer l'usager pour la prise de conscience (sans lui faire peur)
- Lui laisser le choix, la maîtrise de la situation
- Ne pas changer ses habitudes
- Maintenir aux mieux les services de ses applications

Différentes techniques de protection
Phasage de l'offre (voir détails en annexe)

- **Launcher** (évolution de l'application DataRespect)

  Information permissions et facilitation de leurs désactivations

- **Filtrage cloud (proxi)**

  Filtrage des flux non prévus/désirés

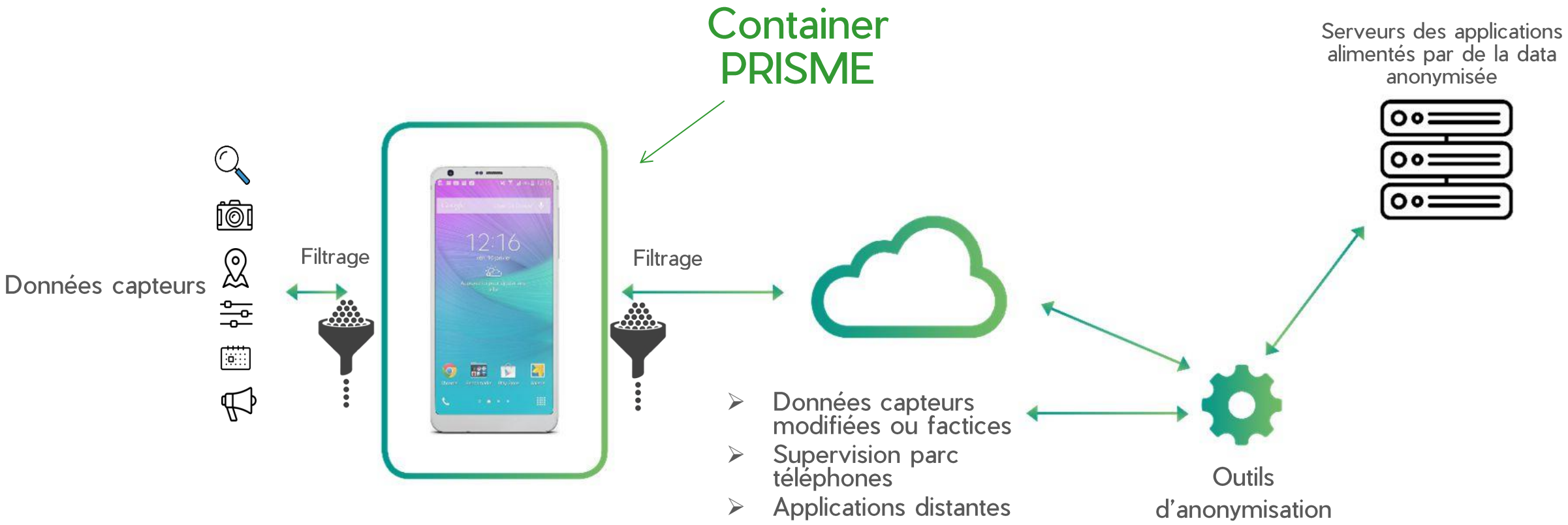
- **Miroir d'application distante**

  Emulation de l'application sur un serveur dans le cloud (possibilité de Fake Data)

- **Containerisation OS**

  Filtrage des données en entrée et en sortie de l'OS

Technologie cible: Container OS Android + Cloud



Modèle économique
Cible commerciale

Produits vendus

Vente abonnement à gestionnaires de flotte

Vente solutions à opérateurs ou constructeur

Cibles et phasage

Phase 1 : B2B

- Flottes entreprises

(aéronautique/armement/nucléaire/grandes entreprises)

Phase 2 : B2C

- **Flotte familiale (ex. privacy pour les enfants)**

Eventuellement avec partenaire «tiers de confiance» type assurance

SWOT

FORCES	FAIBLESSES
• Equipe expérimentée • Disponibilité des briques d'anonymisation DataRespect • Rapidité et agilité dans l'exécution et la prise de décision • Expérience Android / administration serveurs	• Taille critique pour traiter avec des grands groupes • Exigence élevée contre les failles • Importance dépôt Propriété Intellectuelle • Couverture Internationale • Hors Marché IOS (Apple) • Marché téléphonique saturé d'offres
OPPORTUNITES	**MENACES**
• Prise de conscience usagers en hausse • Communication autour de la nouvelle réglementation européenne • Millénials conscients et impliqués dans le rapport à la donnée personnelle • Paranoïa des entreprises sur leur confidentialité	• Etre sorti du marché par un gros acteur • Ne pas avoir assez de moyens financiers pour se développer rapidement • Dépendance aux performances des solutions cloud choisies

PRISME

Nous contacter :

Philippe MICHEL

06 45 42 79 25

phil@prisme.mobi