LENA

Stockage cloud & risques humains

12 juin 2018

Pourquoi Lena ?

Qu’est-ce que Lena ?

Lena est un service cloud de stockage et partage de fichiers avec des fonctionnalités de protection contre les fuites de données.

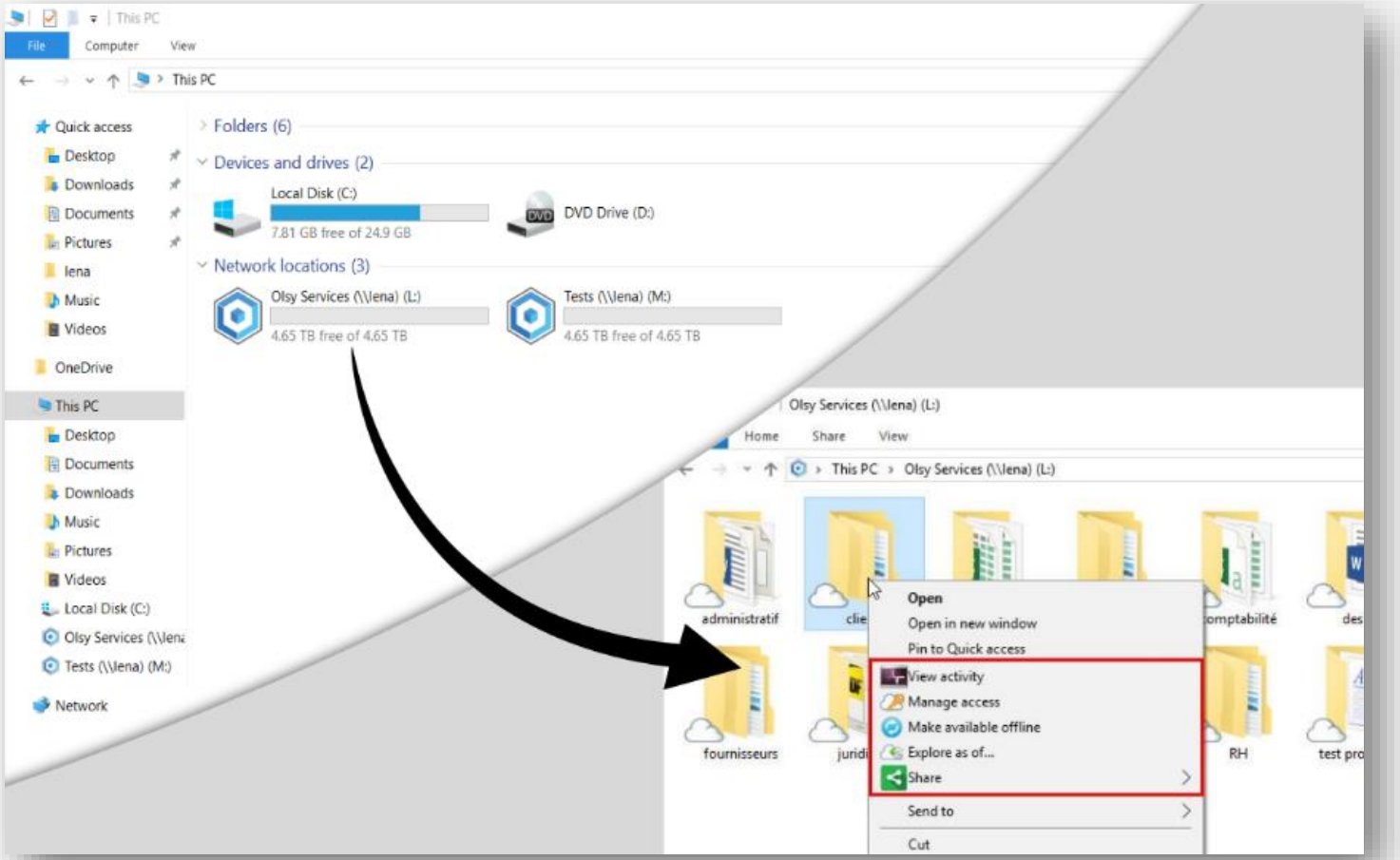
⇨ Fichiers accessibles de partout

⇨ Backup distant en continu

⇨ Protège contre les ransomwares

⇨ Empêche les fichiers sensibles de « sortir »

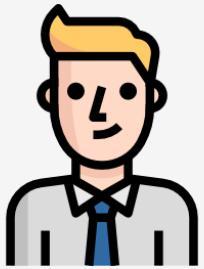
Comment ça se présente ?



Objectifs de sécurité

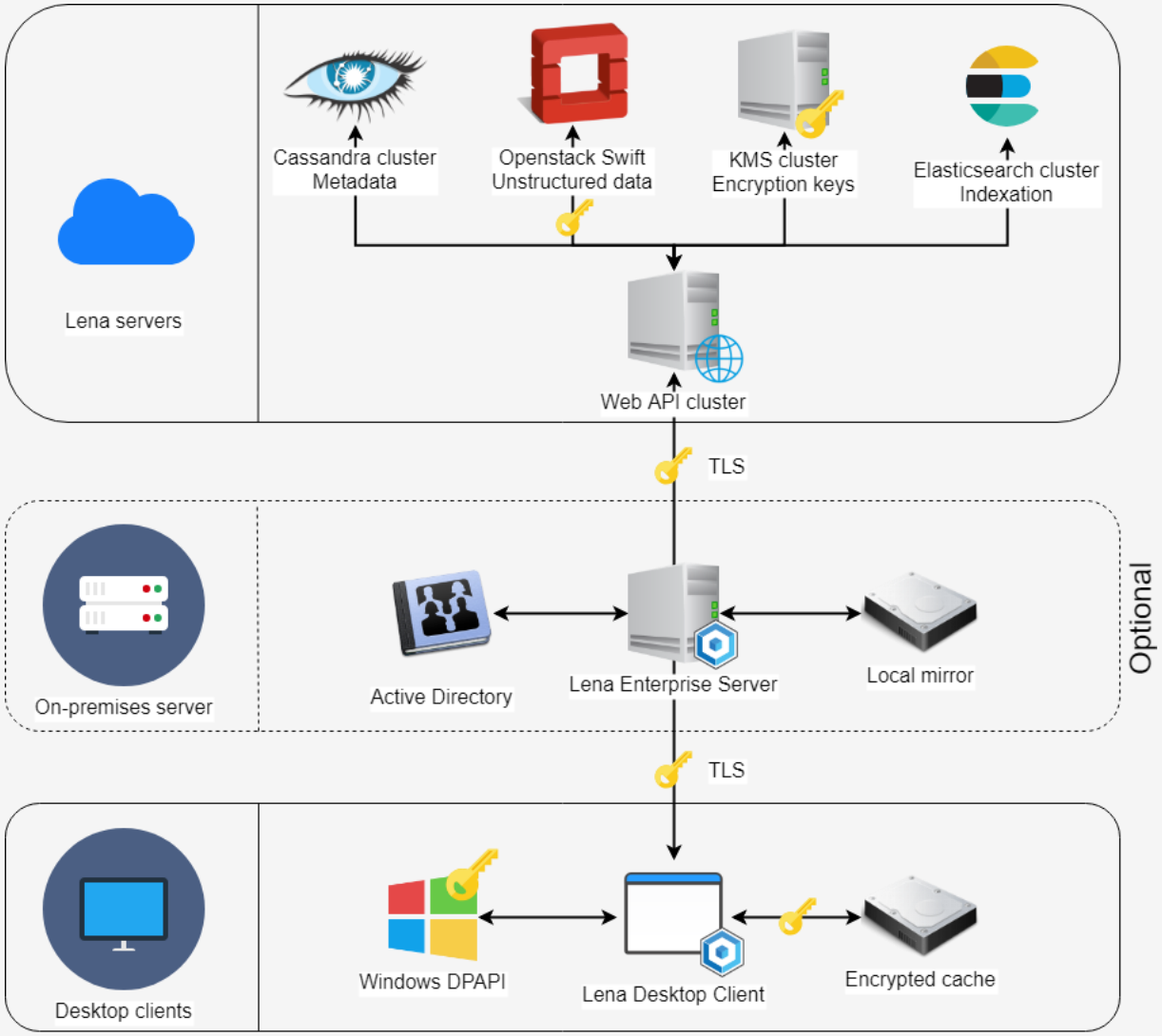
Intégrité des données

Confidentialité des fichiers sensibles



Non-administrateur

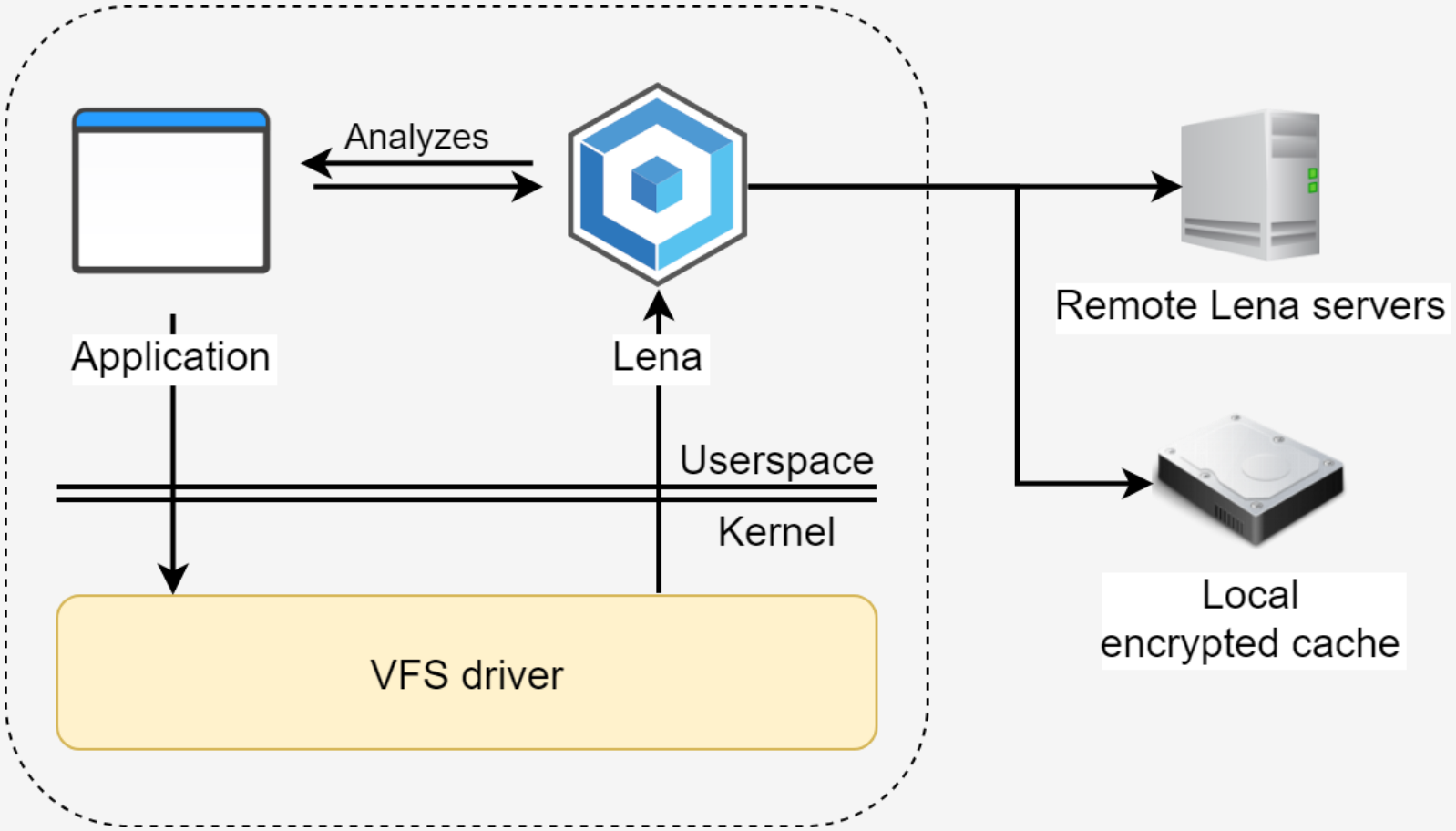
Vue d'ensemble



Stockage des données côté serveur

- Stockage séparé des données non-structurées et des métadonnées.
- Triple réplication sur des machines distinctes dans les deux cas.
- Structure de données « à la git » avec :
  - une base immutable et « append-only » contenant les données non-structurées ;
  - un index variable contenant toutes les informations sur l'arborescence de fichiers.

Accès aux données côté client



Contrôle d’accès côté client

Grâce à cette position de « proxy filtrant » d’accès aux données, Lena peut effectuer un contrôle d’accès strict, à la fois sur :

L’utilisateur qui accède aux données

L’application qui accède aux données

Blocage de comportements illégitimes type envoi par mail, upload sur service cloud, etc.

Contrôle des programmes légitimes

Lena isole les programmes légitimes à accéder à un document en « hookant » les appels systèmes de ces programmes qui pourraient constituer des vecteurs de fuite.

Blocage des vecteurs de fuite type « Enregistrer sous », presse-papier, impression, capture d'écran, etc.

Et côté serveur

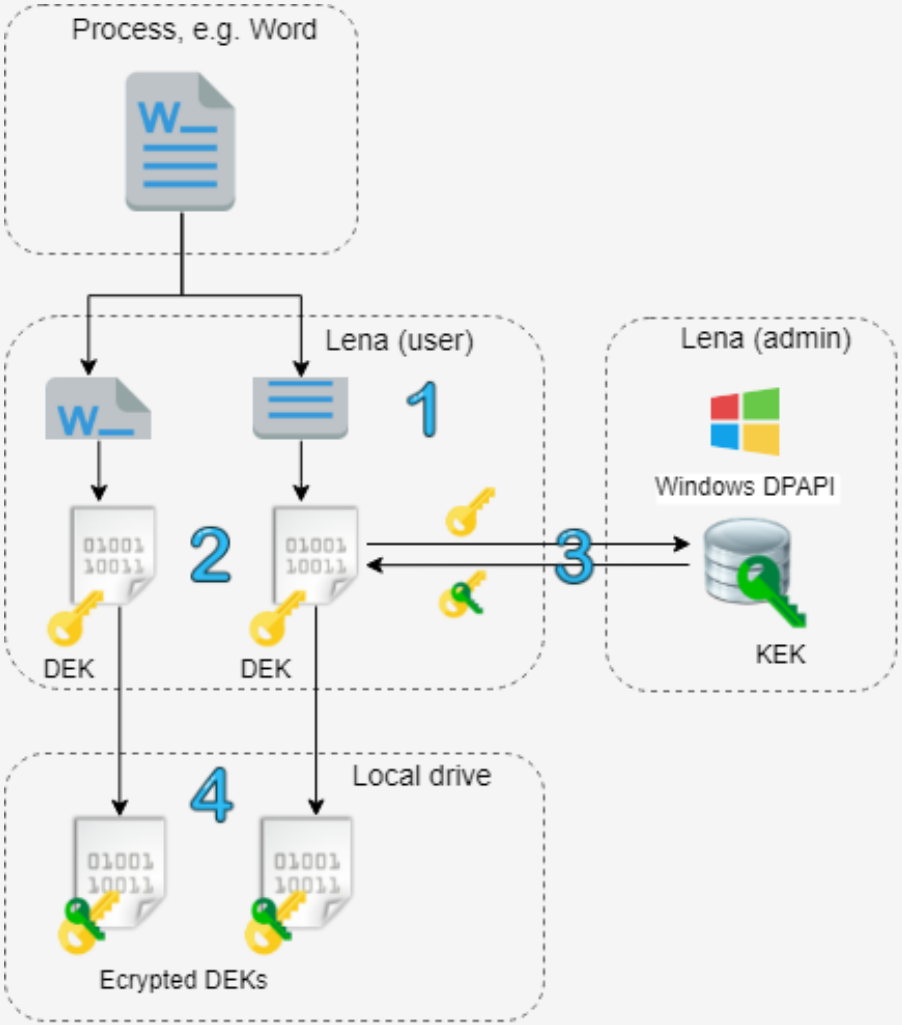
Dans le cas général, les données ne sont pas présentes côté client et doivent être téléchargées depuis les serveurs.

Le comportement de l'utilisateur est évalué côté serveur et peut être bloqué s'il est suspect (activité inhabituelle, lecture de trop de données sensibles...).

À terme, utilisation de machine learning pour la détection de comportements suspects.

Protection des données côté client

- Chiffrement DEK via AES-256-CBC
- Chiffrement KEK via AES-256-CBC
- Protection KEK via DPAPI
- Rotation des KEK tous les 90 jours, expirent au bout de 5ans.



Protection des données côté serveur

Même principe mais :

- Les KEK sont propres à chaque drive.
- Les KEK ne quittent jamais des serveurs spécifiques dédiés à leur gestion (KMS).
- À terme, délégation de la gestion des clés aux clients et utilisation de HSM.

Merci de votre attention

Questions ?