Bodet Software

RGPD et édition logicielle

Mars 2018

Sommaire

Le DPO

BODET Software

Les problématiques

Sommaire

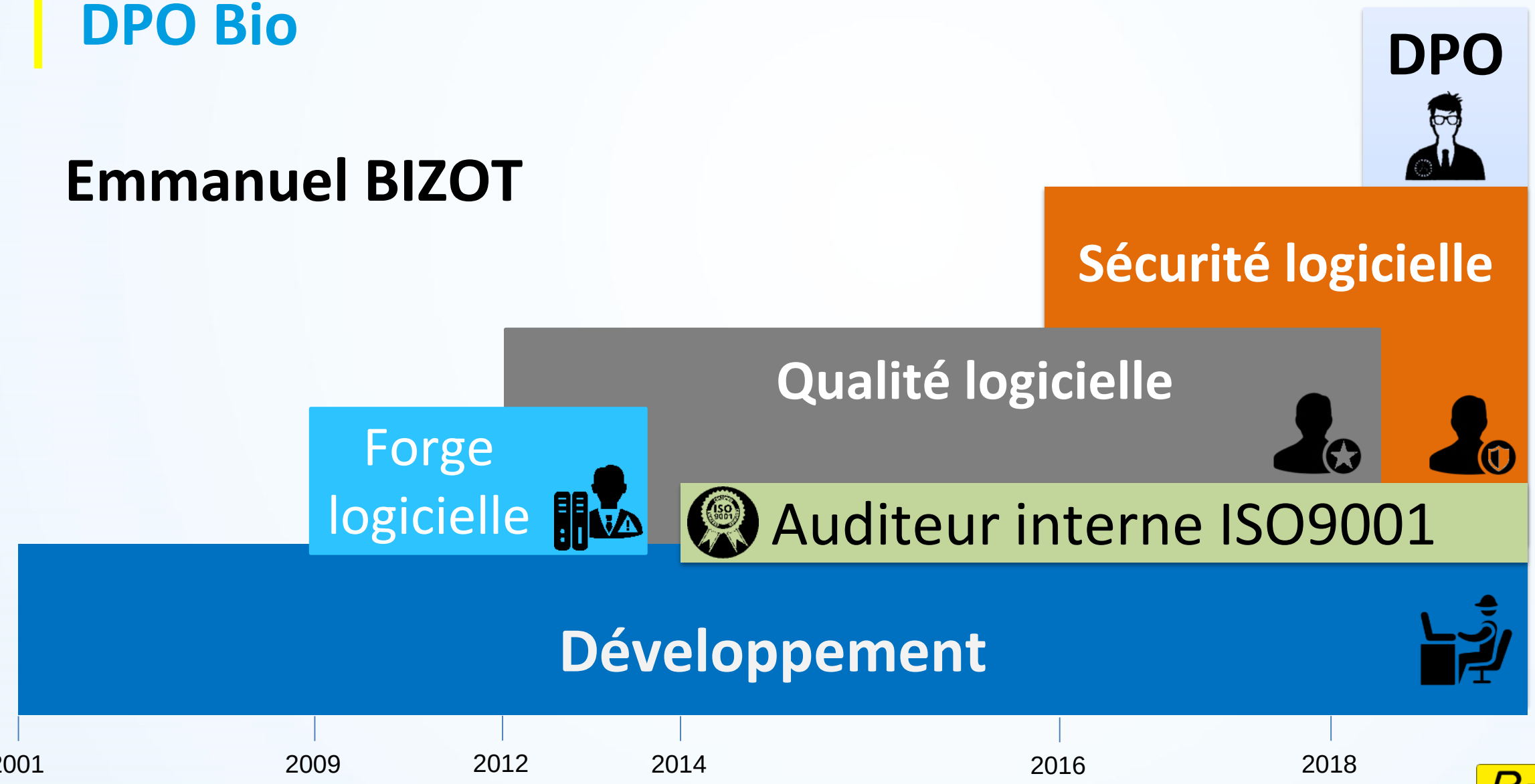
→ **Le DPO**

BODET Software

Les problématiques

DPO Bio

Emmanuel BIZOT



Bodet Software

Sommaire

Le DPO

→ **BODET Software**

Les problématiques

Groupe Bodet - Des chiffres

88
M € de CA

720
collaborateurs

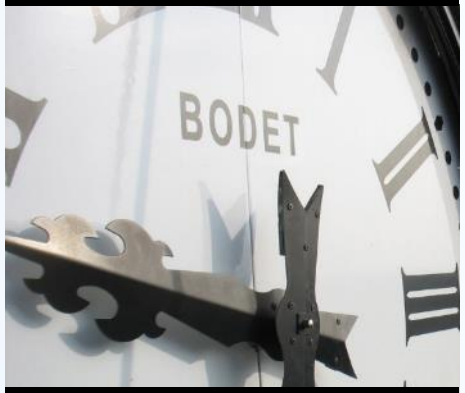
150 ans d'expertise

Bodet Software

Groupe Bodet - Des métiers multiples

Bodet Campanaire

Bodet Campanaire



Horlogerie d'édifice
Équipement du clocher

Bodet Time

Bodet Time

Horlogerie industrielle
Sonneries
Affichage

Bodet Sport

Bodet Sport

Affichage sportif
Affichage vidéo LED
Affichage piscine

Bodet Software

Bodet Software

Gestion des temps
Contrôle d'accès
SIRH

Bodet Software

Bodet Software - Des chiffres

41
M € de CA

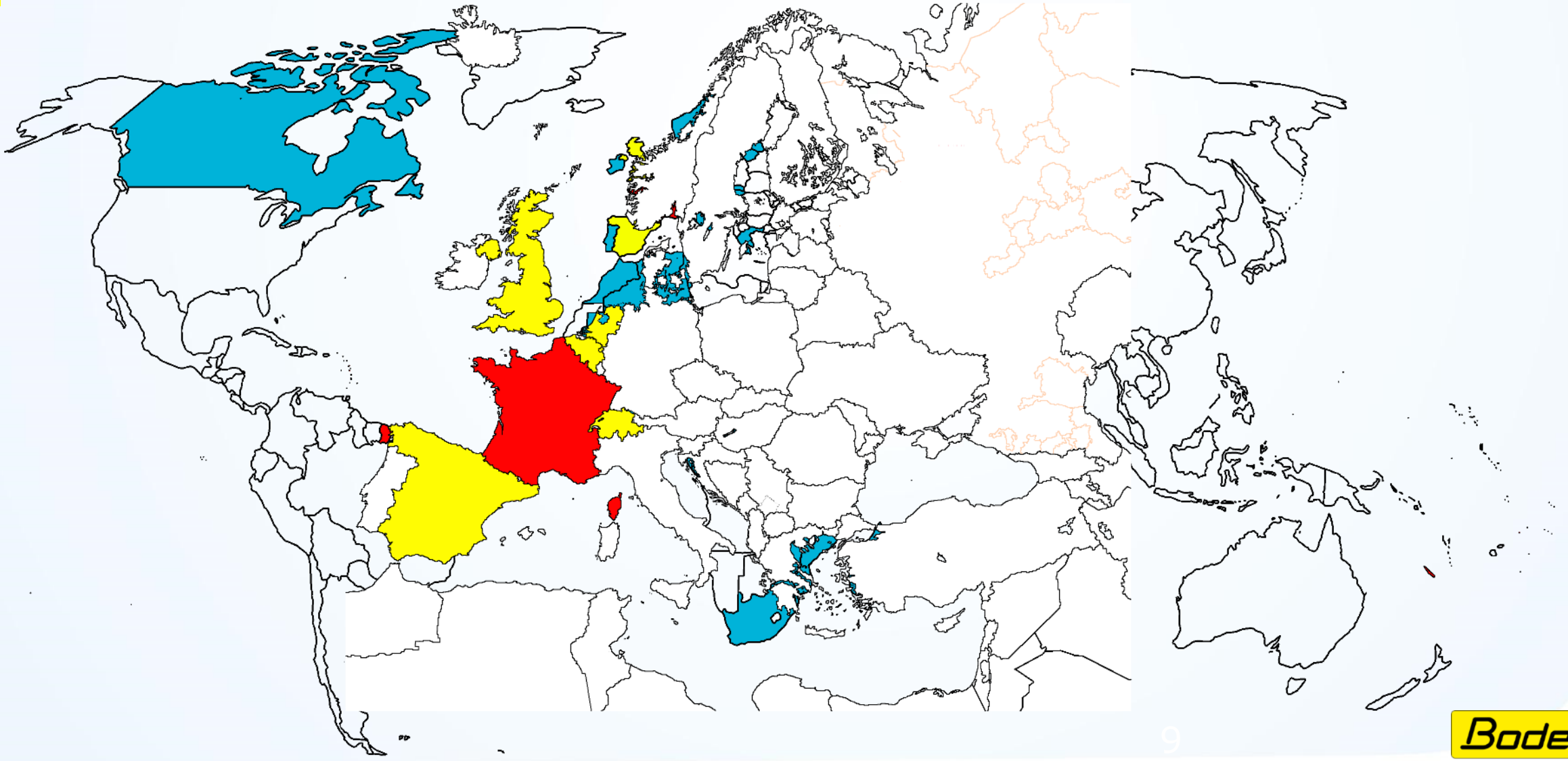
330
collaborateurs

35 000
clients

4 000 000
d'utilisateurs

Bodet Software

En France, en Europe et ailleurs



Bodet Software

Les facettes du logiciel Kelio

SI RH

Contrôle d'accès

Bodet Software

Les facettes du logiciel Kelio

Mode Licence

Kelio OnPremise

Mode SaaS

Kelio OnDemand

Bodet Software

Les facettes RGPD d'un éditeur

RT		Entreprise = Salariés
		Système informatique
		Créer
		Vendre
ST		Installer / Former
		Supporter
ST Tiers		Héberger

Bodet Software

Sommaire

Le DPO

La société BODET

→ **Problématiques**

Bodet Software

RGPD – Le cadre

Droit d'accès
Droit à l'oubli
Droit de rectification
…

Protection de l'individu

Entreprises / Economie numérique

Responsabilité
Confidentialité
Sécurité
Documentation
Gestion de risques
Assistance
Notification
DPO

Pouvoirs politiques

Loi Européenne au dessus des lois nationales
Sanctions conséquentes (max 4% CA monde / 20M€)
Date d'application: mai 2018

Bodet Software

Les guides chez Bodet Software

CNIL - Guide du ST

Sécurité - ANSSI / Audits

Nouveau Monde Avocats (Me Lamon)

Différentes problématiques

L’engagement

Les registres

Notification

Privacy by design / default

Sécurité

Droits des personnes

Bodet Software

Différentes problématiques

- **L’engagement**
- Les registres
- Notification
- Privacy by design / default
- Sécurité
- Droits des personnes

Bodet Software

L’engagement d’entreprise

Nomination d’un DPO

Politiques de protection

Révision des Contrats

Bodet Software

Engager les sous traitants

Clauses contractuelles

Garanties suffisantes du SST *(responsabilité du ST)*

Validation par le client

Bodet Software

Démontrer le respect des DP

Documentation (SMDCP / Registres)

Rapports d’audit (Logiciel / SI)

Label CNIL

Auditabilité (logiciel / sites)

Bodet Software

Différentes problématiques

L’engagement

→ **Les registres**

Notification

Privacy by design / default

Sécurité

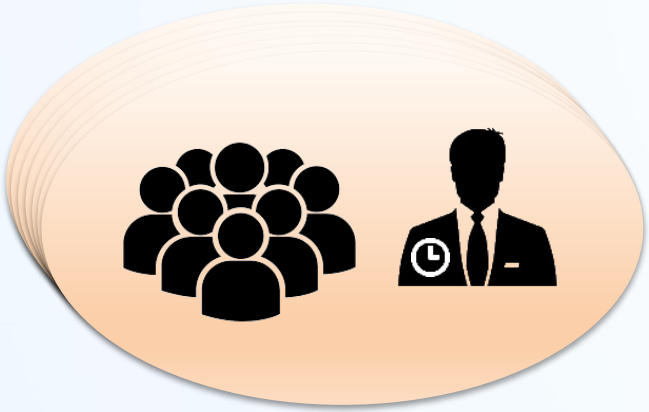
Droits des personnes

Bodet Software

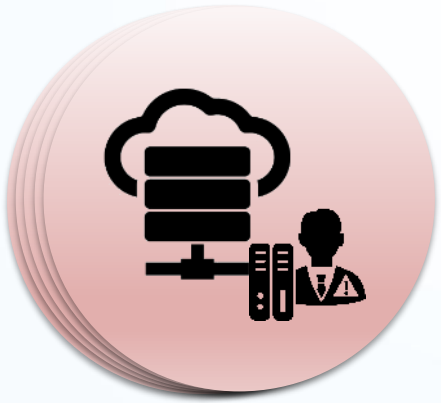
Deux registres distincts

Registre Kelio

Registre de traitements



Clients

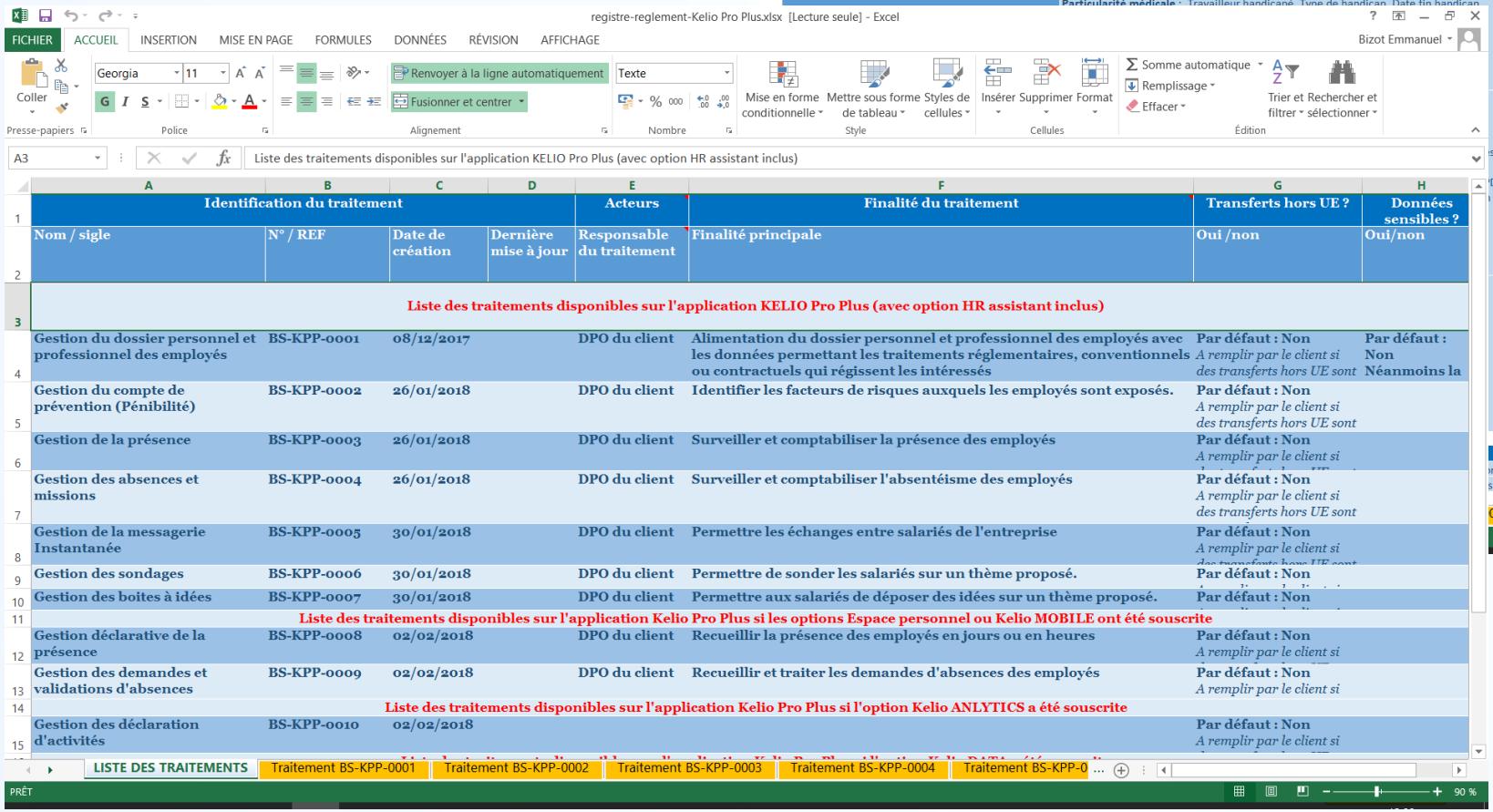


SaaS

Registre des catégories d'activité de traitement

Registre de traitements

Exemple



Bodet Software

Différentes problématiques

L’engagement

Les registres

→ **Notification**

Privacy by design / default

Sécurité

Droits des personnes

Bodet Software

Notification en tant que sous-traitant

Devoir de notification

Procédure liée au registre CAT

Client 72h : signalement ‘au plus tôt’

29 autorités : CNIL =autorité chef de file

Bodet Software

Différentes problématiques

L’engagement

Les registres

Notification

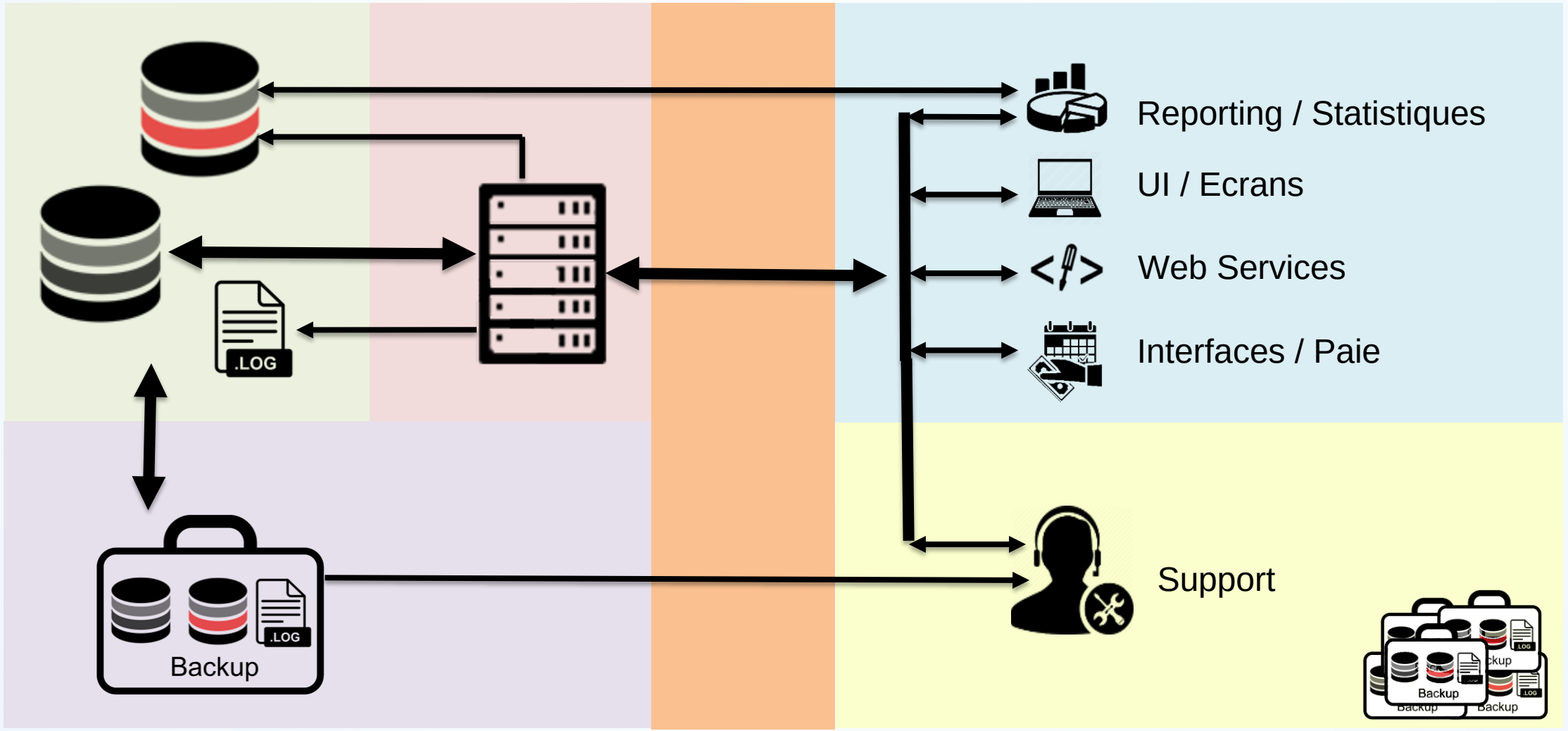
→ **Privacy by design / default**

Sécurité

Droits des personnes

Bodet Software

Les zones de sécurité d'un logiciel



Privacy en tant qu'éditeur

Authentification / pas de user anonyme

Gestion de droit / Politique de mots de passe

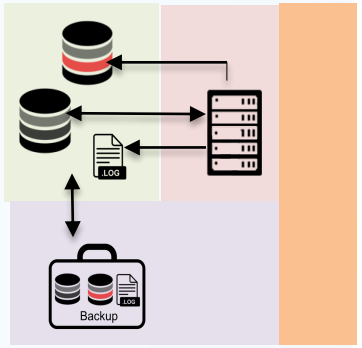
Support : délégation de pouvoir + validation du client

Peu de saisie obligatoire (Minimisation)

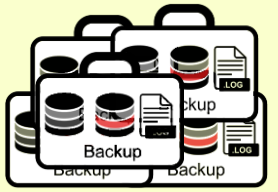
Purge automatique préréglée

Transferts chiffrés

Privacy en tant que sous-traitant



- Hébergeur ISO27001 / ISAE3402
- Engagement et sensibilisation du personnel
- Politique de sécurité / Restriction des accès
- Suppression des données de support
- Anonymisation des données de support



Bodet Software

Différentes problématiques

L’engagement

Les registres

Notification

Privacy by design / default

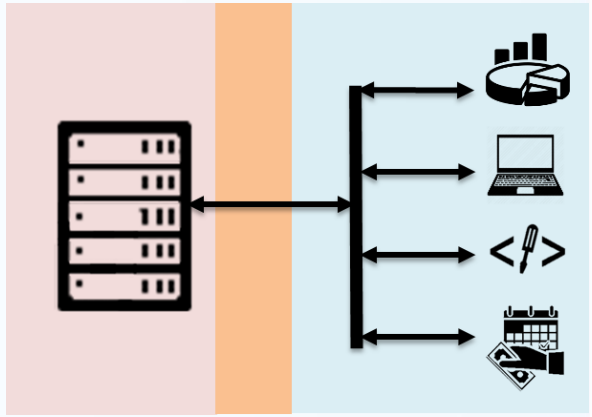
→ **Sécurité**

Droits des personnes

Bodet Software

Sécuriser le logiciel – Des moyens

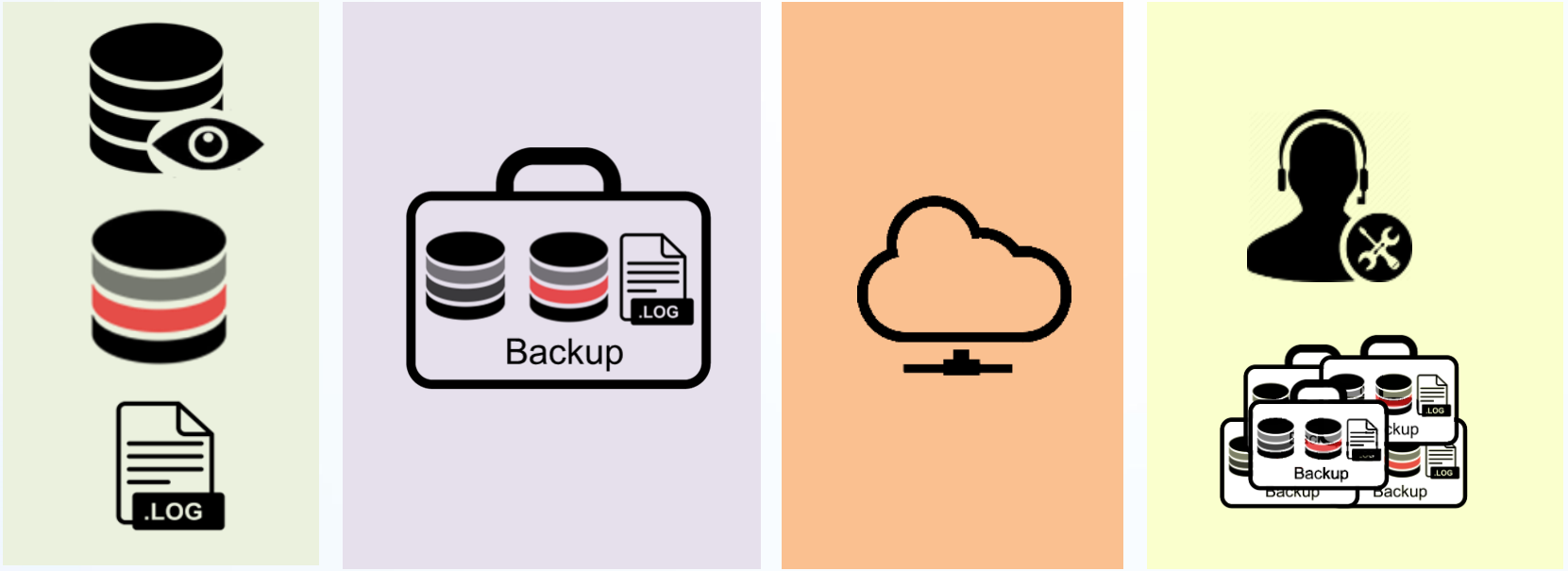
- Ingénieur qualité
- Ingénieur sécurité
- Audits externes (Kereval / Clients)
- Budget R&D
- Chiffrer la source, working on it



Bodet Software

Sécuriser – Une question de risque

Des données à travers une chaîne humaine



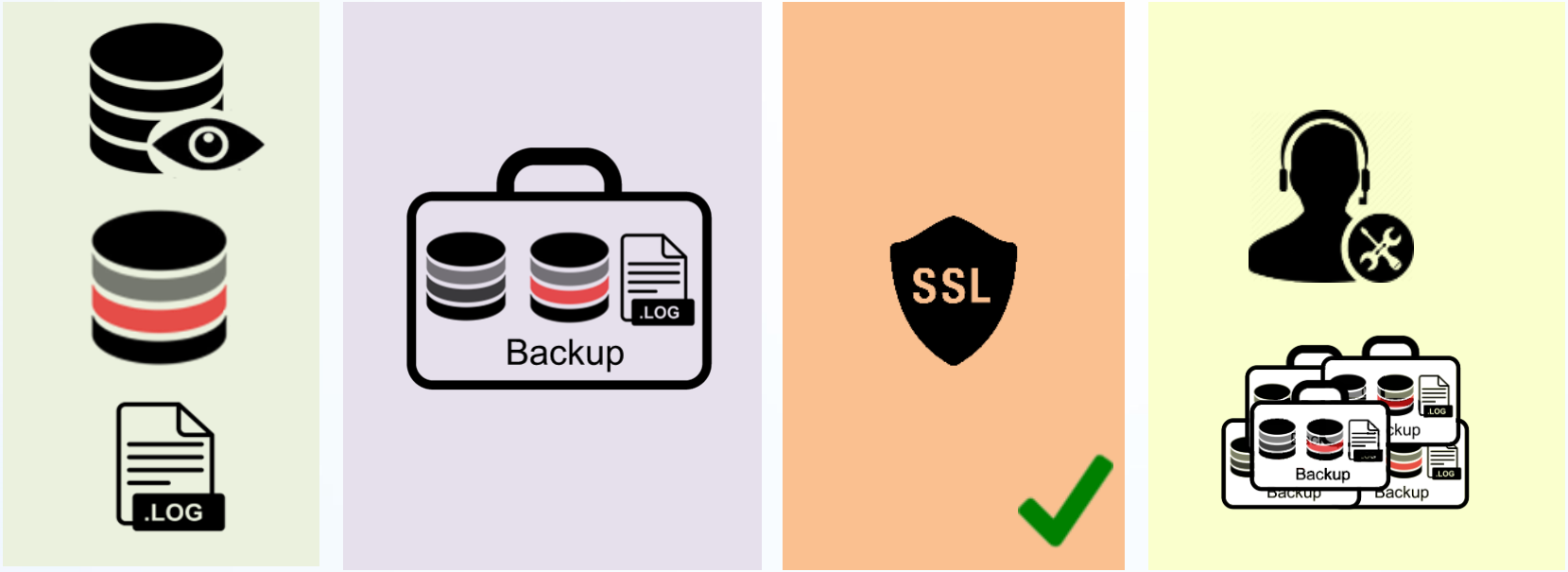
1 client

Inconnu

1000 clients

Bodet Software

Sécuriser – Les transferts : SSL



1 client

1000 clients

Bodet Software

Sécuriser la base– Chiffrement natif

Bases privées vs Bases publiques

Des bases hétérogènes

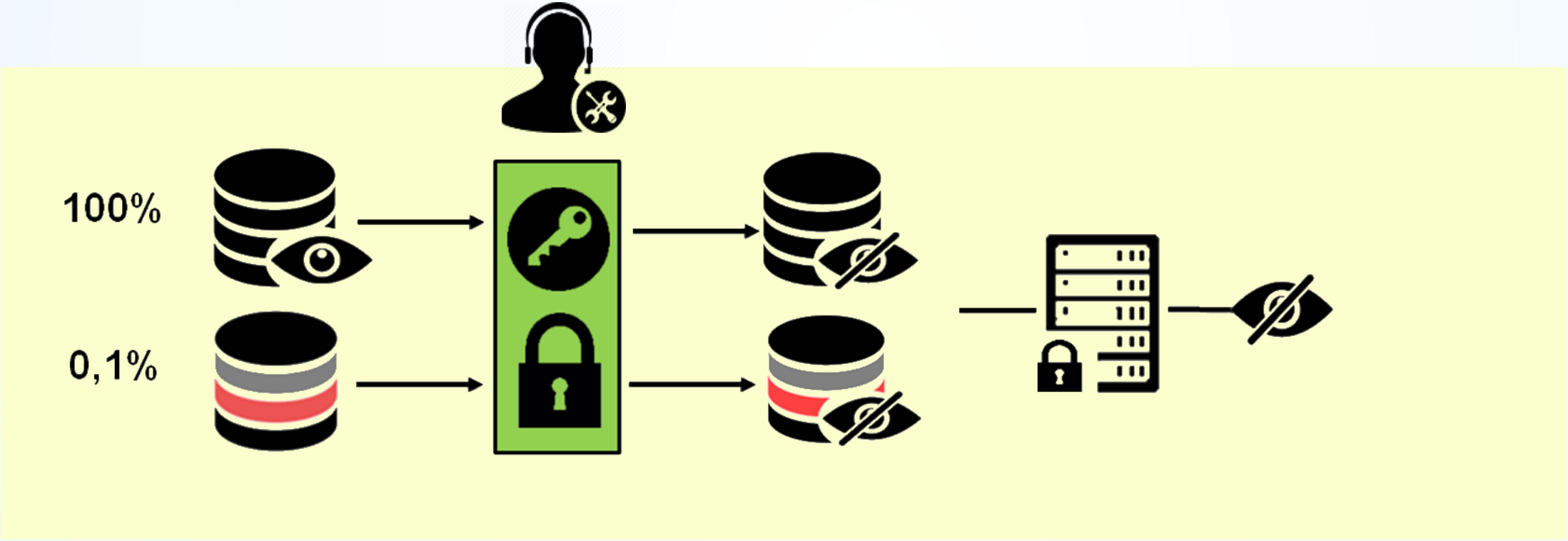
Paramétrages hétérogènes et parc existant

Des performances altérées

Un handicap pour la maintenance

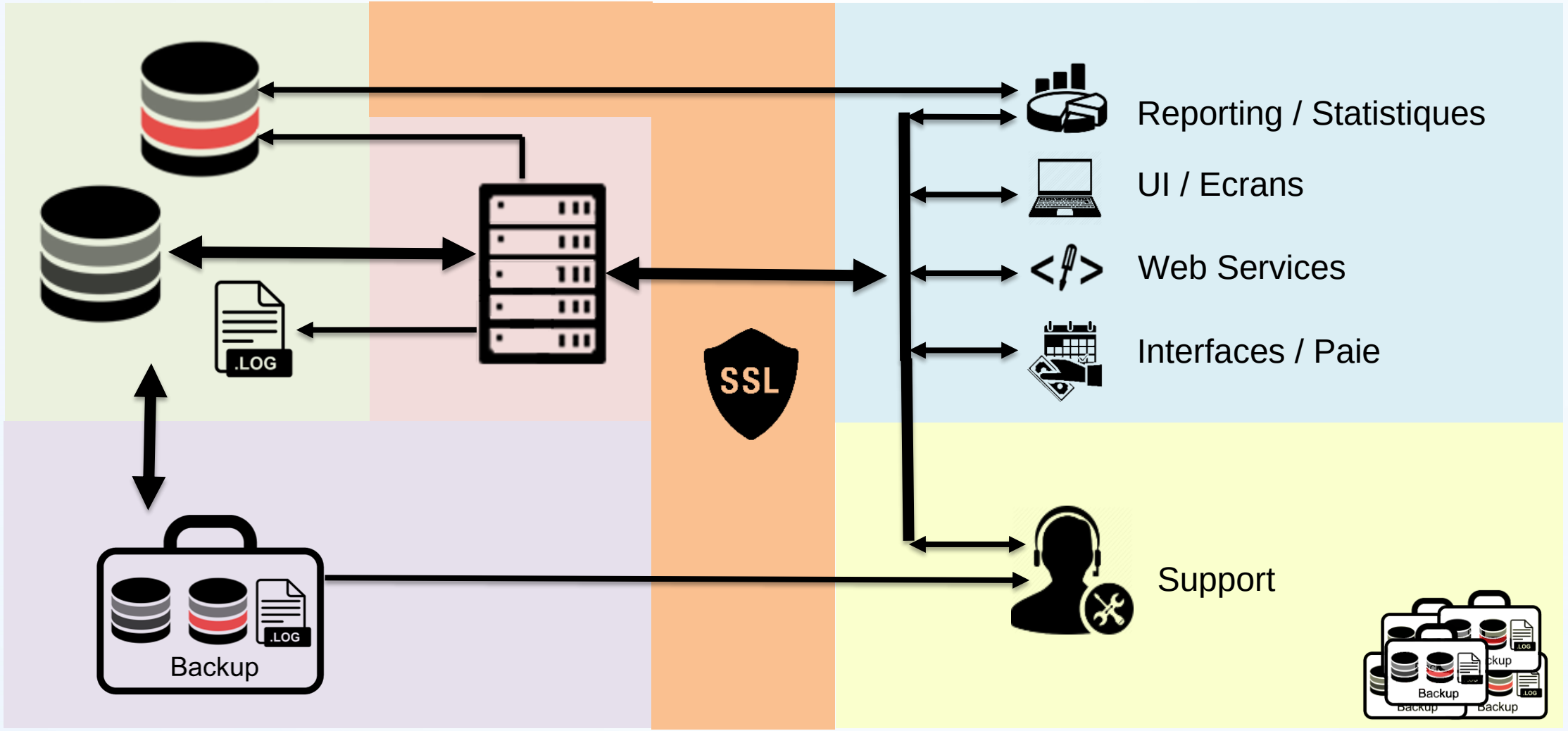
Bodet Software

Sécuriser la maintenance – Anonymisation



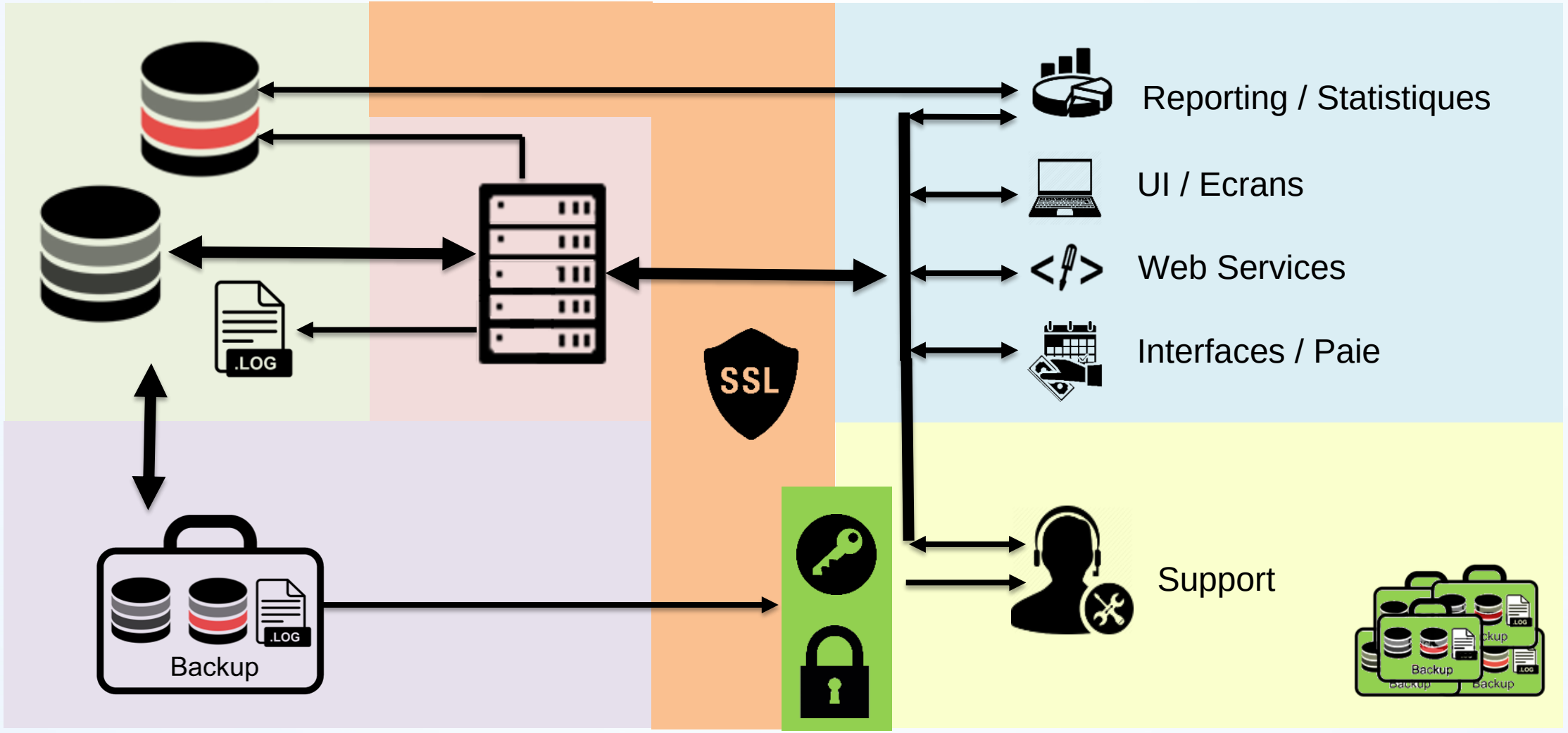
Bodet Software

Sécuriser la maintenance – Anonymisation



Bodet Software

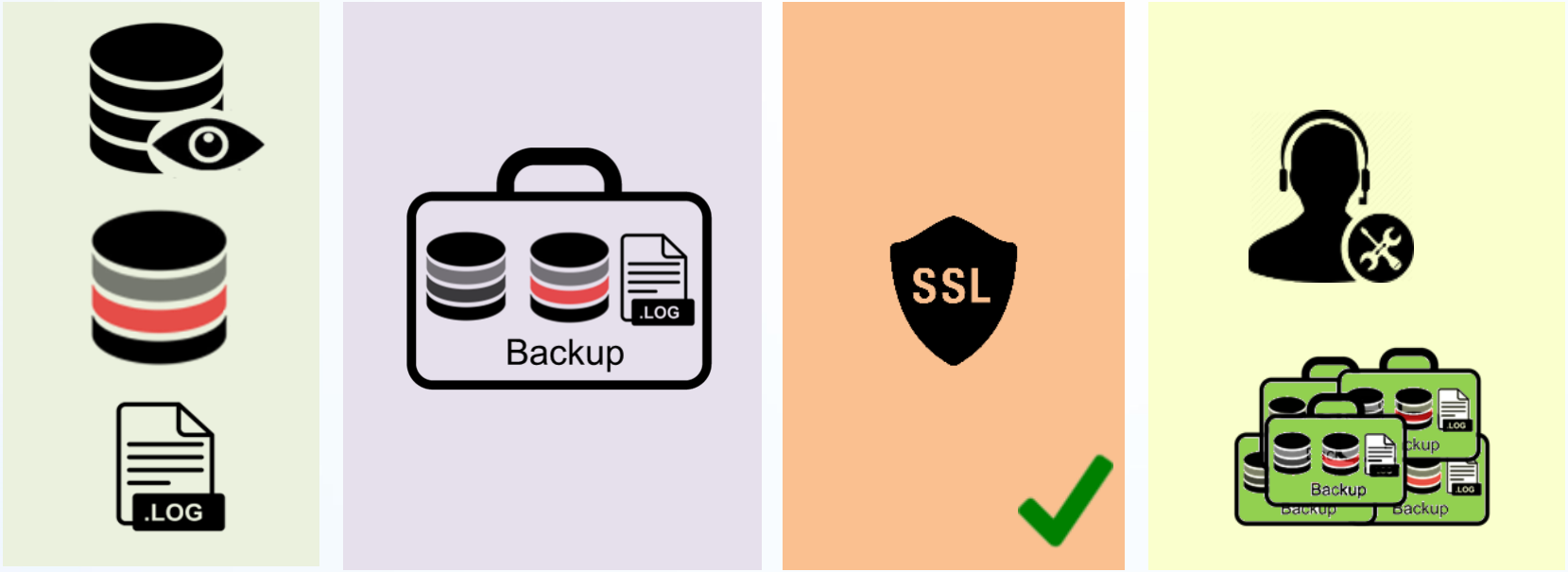
Sécuriser la maintenance – Anonymisation



Bodet Software

Sécuriser – Anonymisation

SSL / VPN



1 client

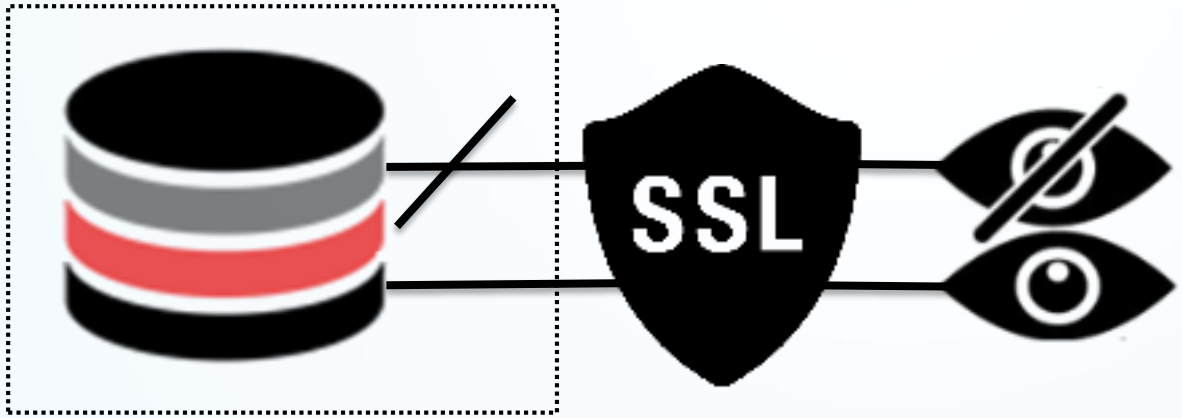
Inconnu

1000 clients

Bodet Software

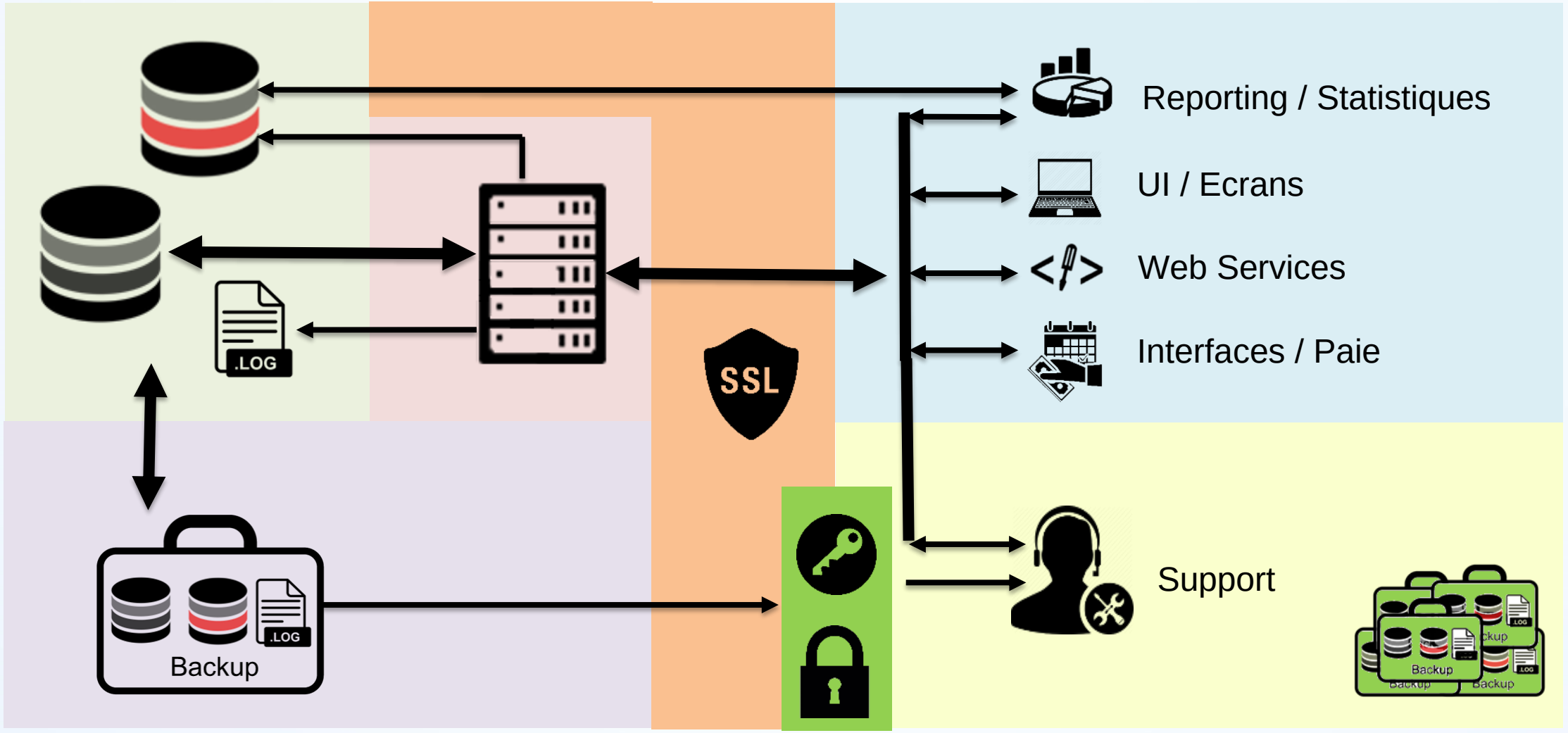
Sécuriser la base statistique

Bases publiques : SSL + Data Masking



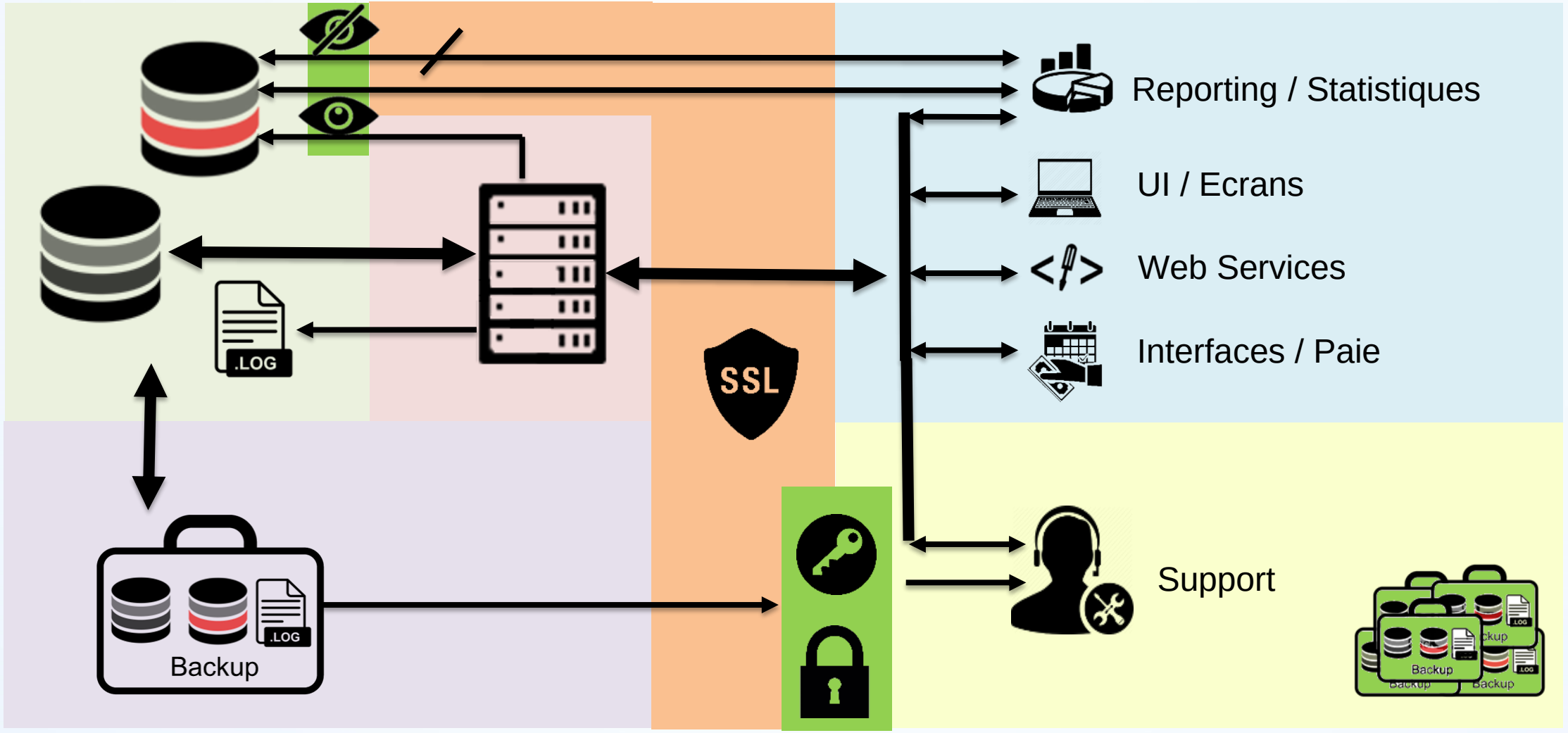
Bodet Software

Sécuriser la base statistique



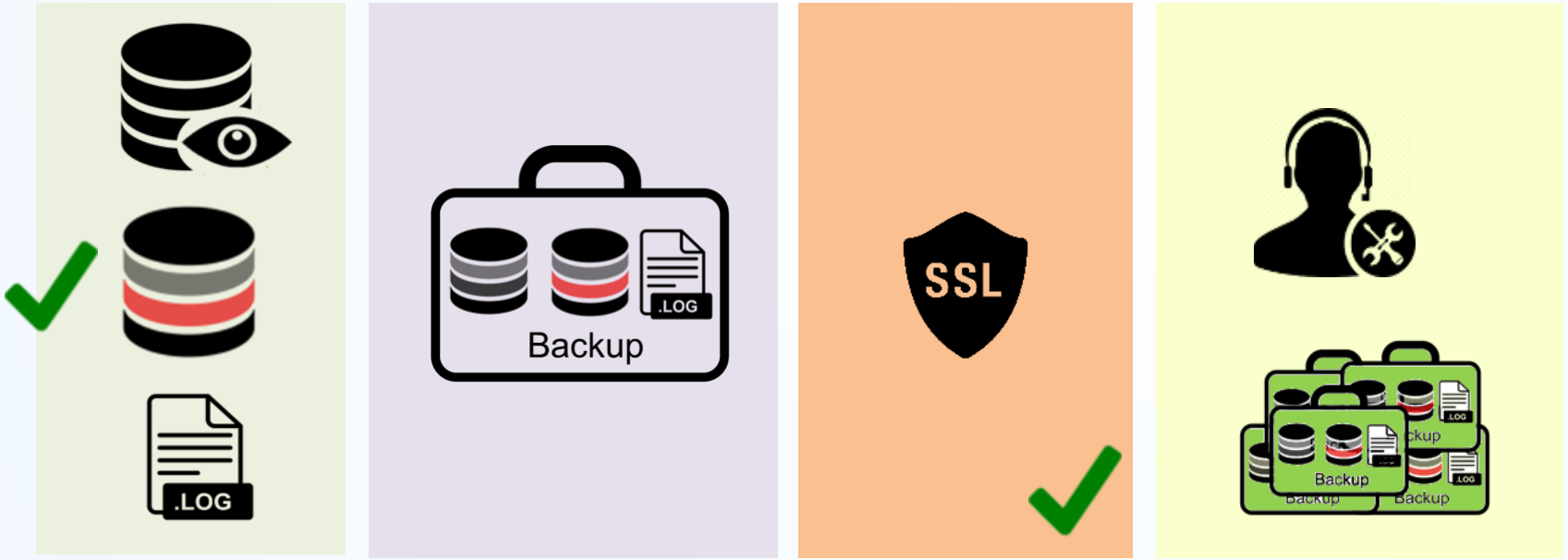
Bodet Software

Sécuriser la base statistique



Sécuriser la base statistique

SSL / VPN



1 client

Inconnu

1000 clients

Bodet Software

Sécuriser la base privée – En production

Le serveur chiffre

Les clés de chiffrement sont spécifiques à chaque client

Bodet Software

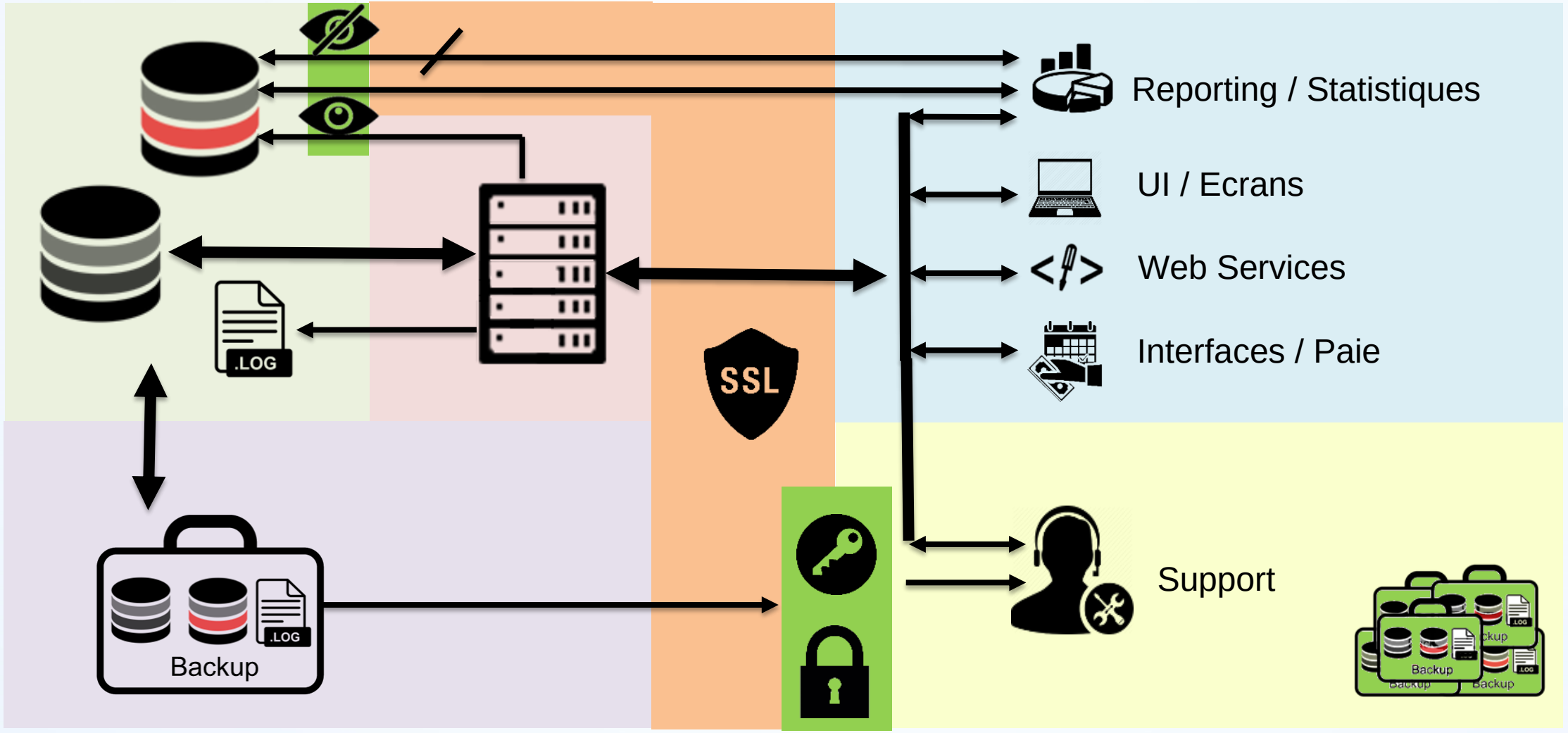
Sécuriser la base privée – En support

Le serveur n’a pas la clé, la donnée est anonyme

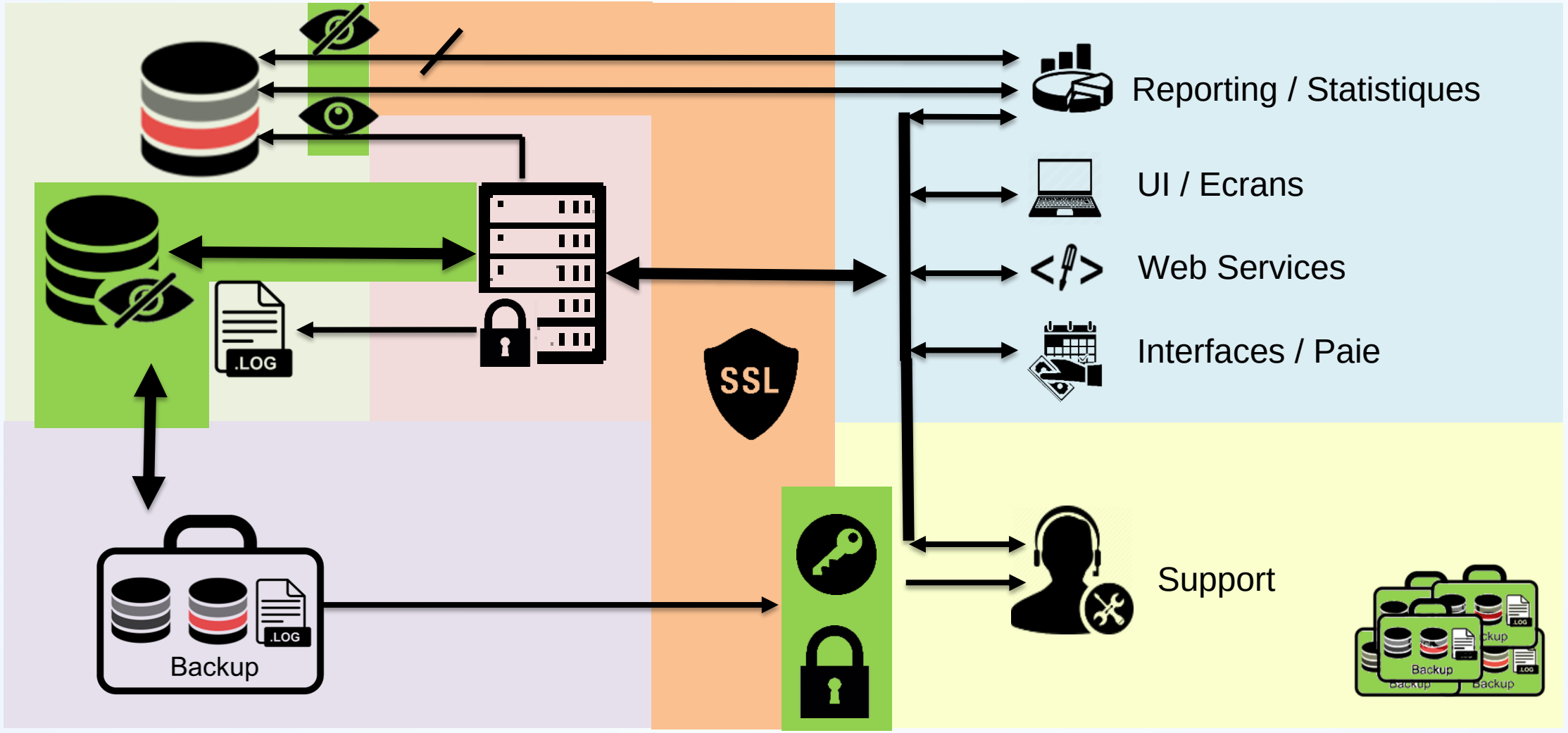
Répond à 99% des cas d’analyse

Bodet Software

Sécuriser la base privée - Avant

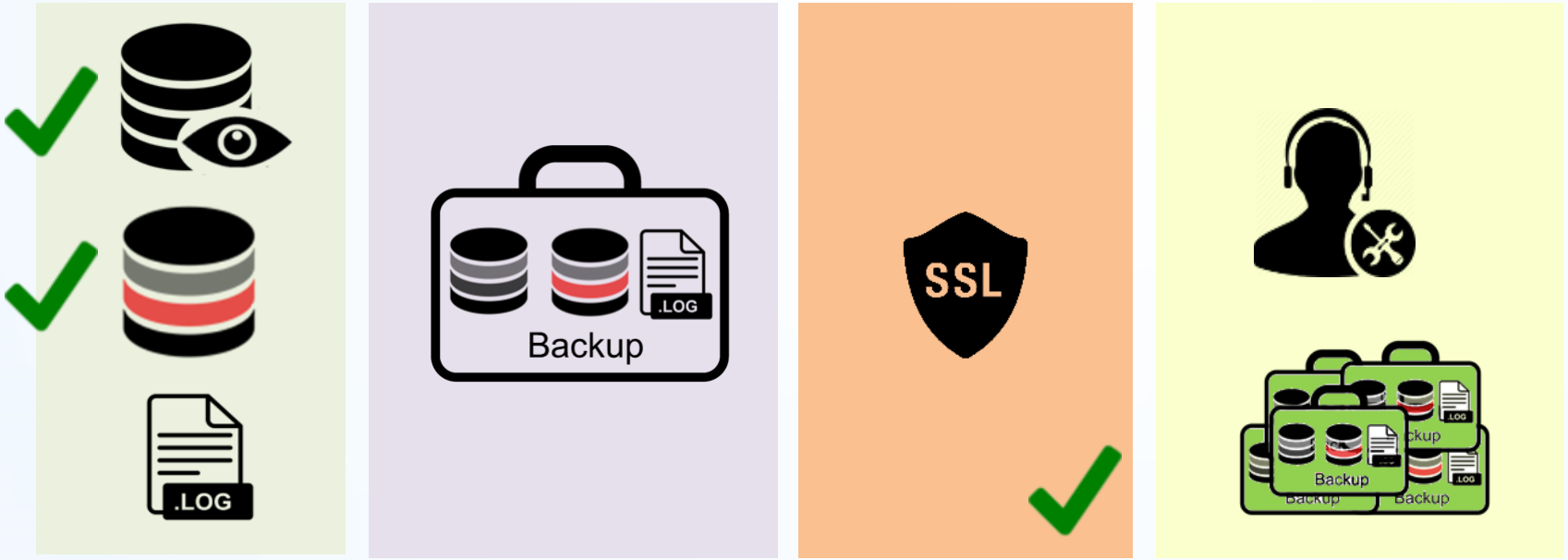


Sécuriser la base privée - Après



Sécuriser la base privée - Après

SSL / VPN



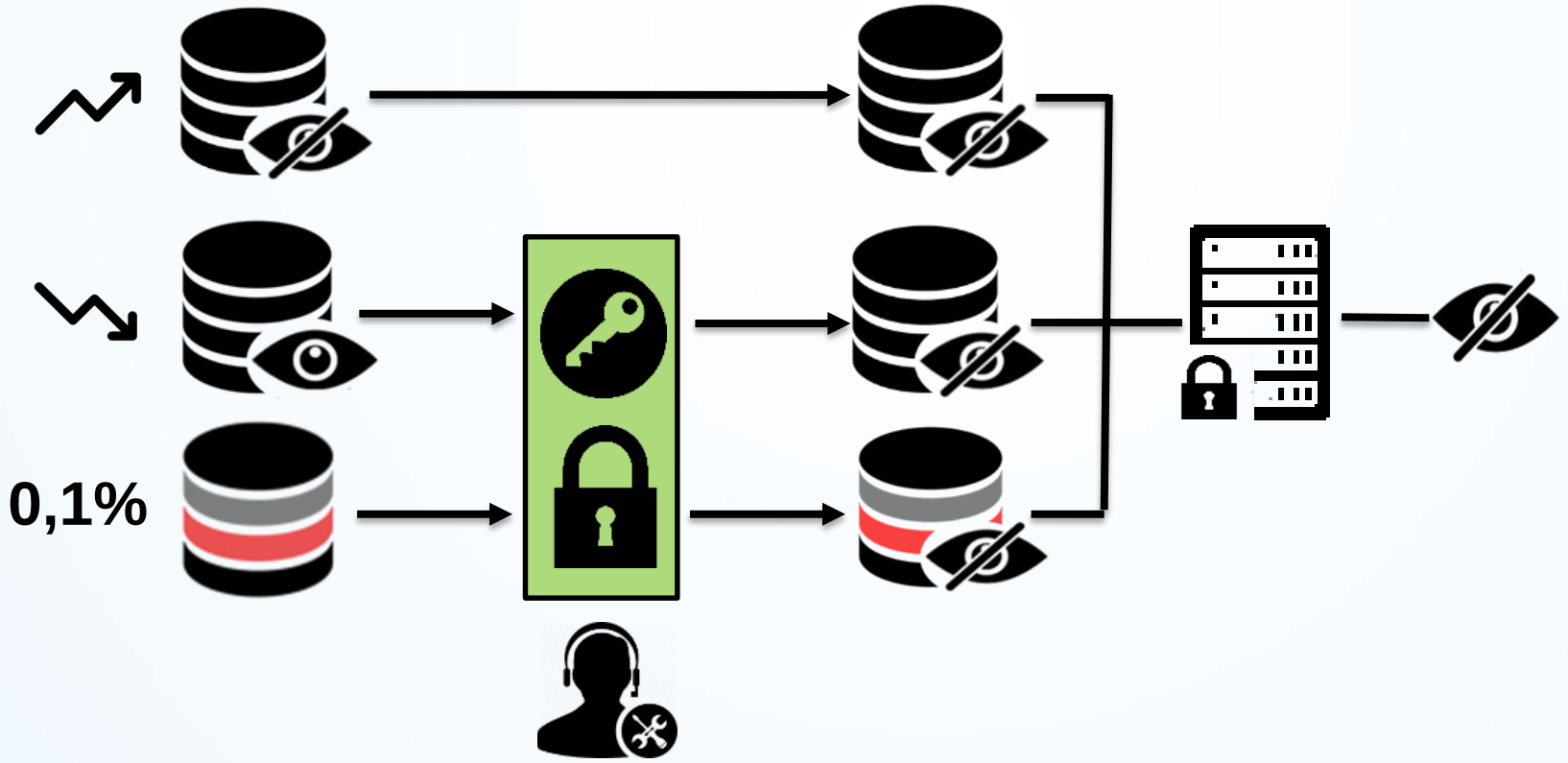
1 client

Inconnu

1000 clients

Bodet Software

Sécuriser la base – Un support anonyme



Bodet Software

Différentes problématiques

L’engagement

Les registres

Notification

Privacy by design / default

Sécurité

→ **Droits des personnes**

Bodet Software

Les droits (oublier/consulter/rectifier)

Voie hiérarchique vs voie logicielle

Masquer vs supprimer ?

Droit à l’oubli vs devoir de conservation

Un ticket au support

Bodet Software

L’oubli, le défi du SI

BDD clientes

BDD commerciale / support

Des supports multiples

Des formats multiples

Mails : problèmes de privé / public

Bodet Software

L’actualité

Un système de management

Une horde de questionnaires

Une FAQ et des réponses types

Registre de traitement et PIA pour le client

Diffuser le RGPD

Bodet Software

Des questions ?

RGPD
au-delà du cadre
une opportunité de s’améliorer

Bodet Software