Session 1

Atelier Technique Futur ERP Aareon

Bénédicte Callens, Cédric Farina,
Mohamed Elmachtani Idrissi

Vos interlocuteurs Aareon durant cette session

Bénédicte CALLENS
Directrice Développement

Cédric FARINA
Responsable Application Delivery

Mohamed ELMACHTANI IDRISSI
Responsable Etudes
& Architecture Logicielle

AGENDA

14:00-14:15 : Introduction

01

14:15-14:40 : L'ARCHITECTURE TECHNIQUE & SES COMPOSANTS

Notre approche, nos partenaires, les fondements, l'approche DevOps par l'I.a.C.

02

14:40-15:00 : LES SERVICES DANS LE CLOUD

Définitions, planning PIH-PRH, matrice métiers

03

15:00-15:20 : L'ARCHITECTURE API

O.R.D.S.

15:20-15:35 : Pause

04

15:35-16:15 : L'ACCES AUX DONNEES

La Sécurisation, les flux, les expositions, l'accès C.R.U.D.

16:15-16:55 : Session d'échanges

16:55-17:00 : Conclusion

Aareon

Introduction

Objectifs

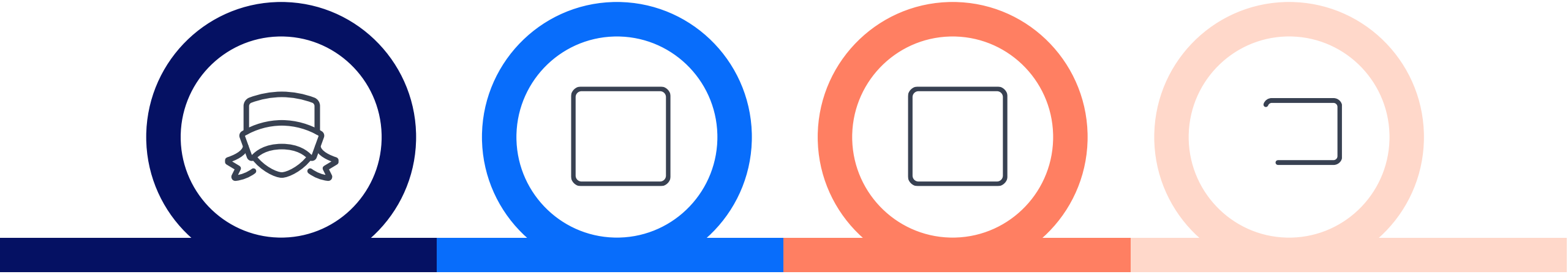
Echanger ensemble autour de l'architecture cible dans un contexte cloud et la confronter à vos organisations actuelles.

Nous assurer de bien prendre en compte l'intégralité de vos besoins dans le cadre de ce projet.

01 L’Architecture Technique & ses composants

Nos solutions en mode hébergé

Une expérience de longue date



Depuis 1999

Démarrage des premiers environnements en mode hébergé.

PRH

HBL Habitat, Noisy-le-Sec Habitat, Harmonie Habitat, OPAC de l'Indre, Rives de Seine Habitat, etc.

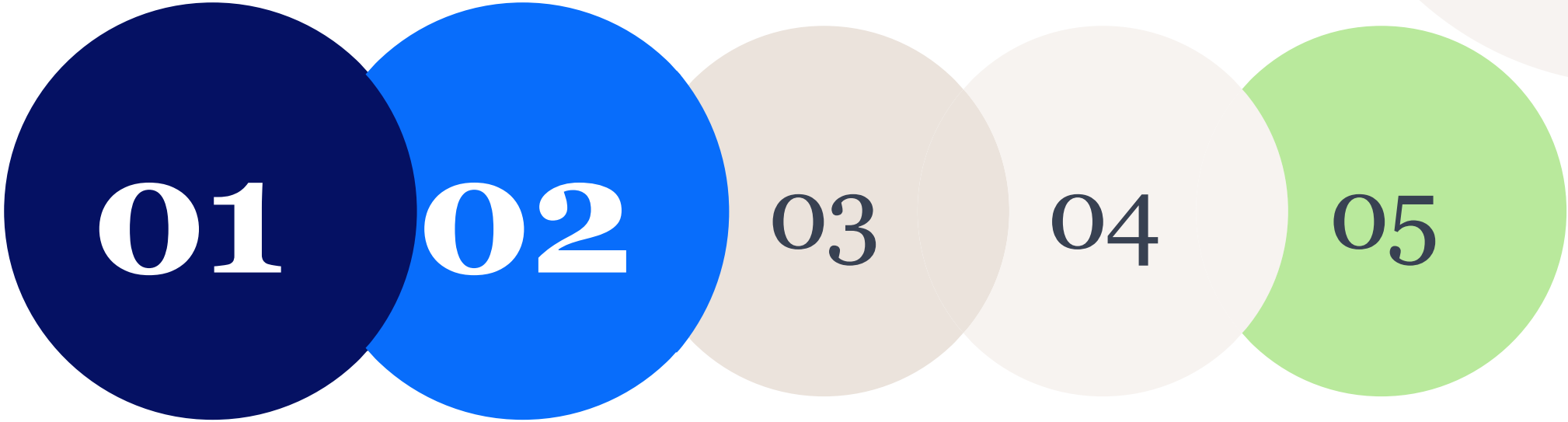
PIH

Troyes Aubes Habitat, Semisap, OPH Levallois, OPH Terre Du Sud, OPH Famille Provence, ARPE Logements Étudiants, Semaba, etc.

SD

Plus de **120** clients dont : Valophis, Société Immobilière Grand Hainaut, 1001 Vies Habitat, 13 Habitat, Erilia, Promologis, Domnis, Espace Habitat.

Notre approche technique en 5 points



Conception

Collecter les exigences métier.
Et adapter l'infrastructure cible pour prendre en charge les exigences.

Construire

La conception de l'infrastructure dictera la construction initiale requise, ainsi que les besoins en maintenance et en adaptation ultérieurs.

Déployer

Configurer les installations.
Tester.
Ajuster.
Migrer les données du client vers le cloud.

Maintenir

Maitriser et ajuster les paramètres des services en fonction de l'usage.
Maintenir les activités des services.

Exploiter

Surveiller pour garantir une utilisation, et une sécurisation optimale des services.

Aareon

Nos partenaires

ORACLE

Service de cloud computing

DIGORA

Spécialistes Oracle Expert - bases de données, accompagnement au cloud computing

THELYS

Spécialistes Oracle - Experts APEX, FOEX, etc.

INSUM

Spécialistes Oracle - Experts APEX, etc.

Les fondements de notre architecture CLOUD

Architecture en compartiments

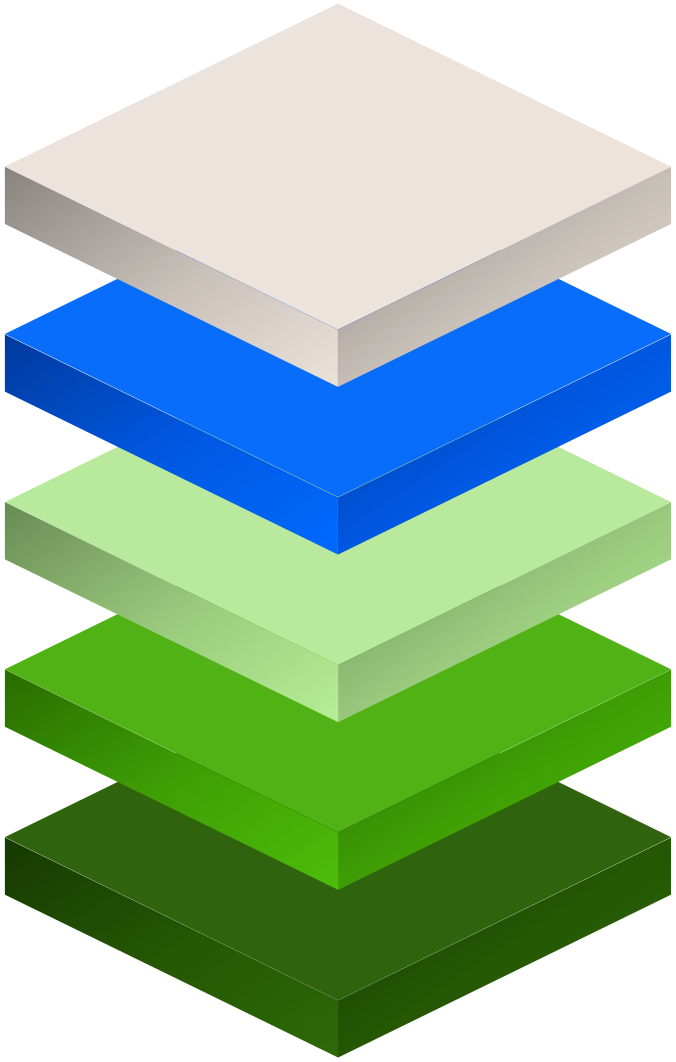
Un compartiment de production
Un compartiment de test
Un compartiment de PRA
Un compatiment d'administration (Aareon)

Accès

Modèle de sécurité à confiance zéro (ZTA)
Un virtual cloud network (VCN) par compartiment
un subnet propre à chaque client
Web Application Firewal(WAF) par compartiment

Infrastructure

3 Fault Domains (FD) par cloud
Les FD permettant de repartir les ressources de sorte qu'elles ne se trouvent pas sur le même matériel physique au sein d'un même datacenter



Architecture multi site

Site de PARIS (Production et Test)
Site de MARSEILLE (PRA)

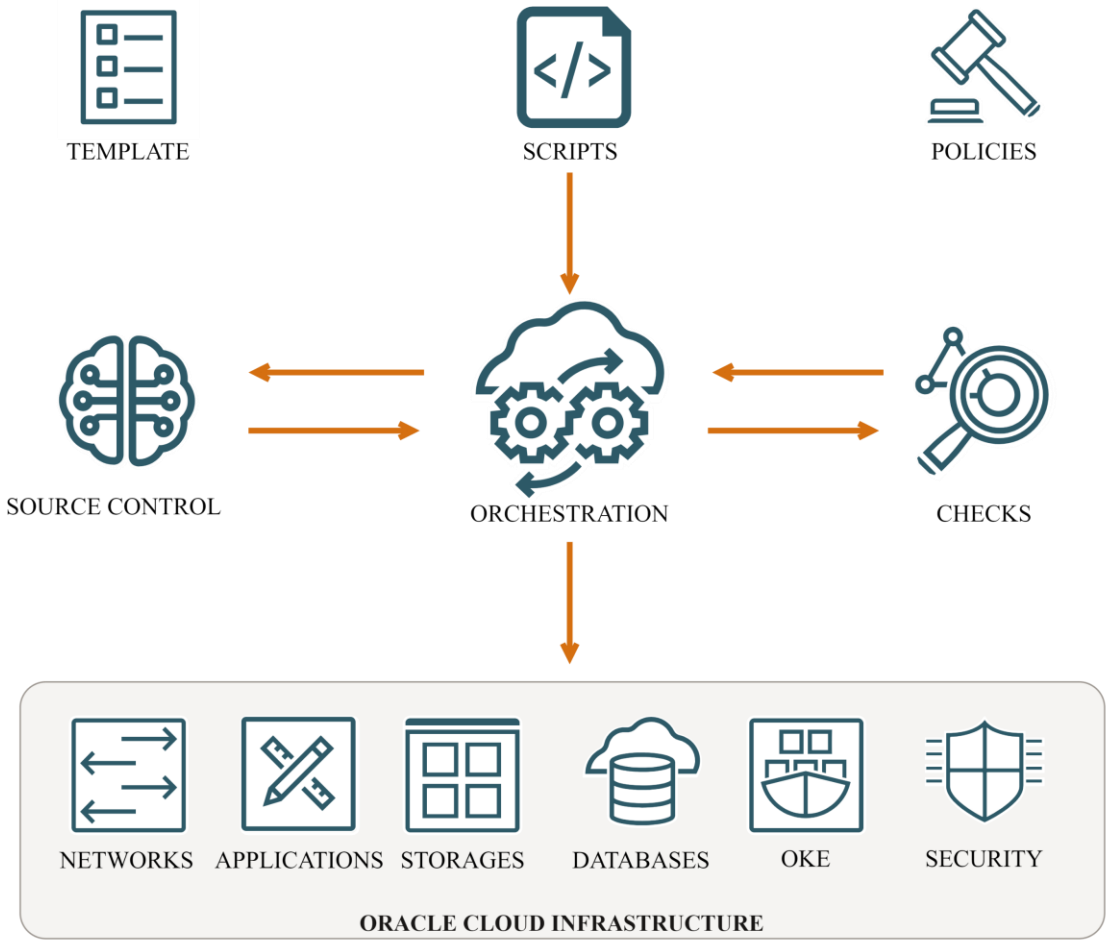
Infrastructure As Code

Standardisation des installations
Reduction des risques (mauvaise manipulation, mauvaise configuration, workflow de validation, etc.)
Rapidité d'exécution

Une orientation « Infrastructure as Code (IaC) »

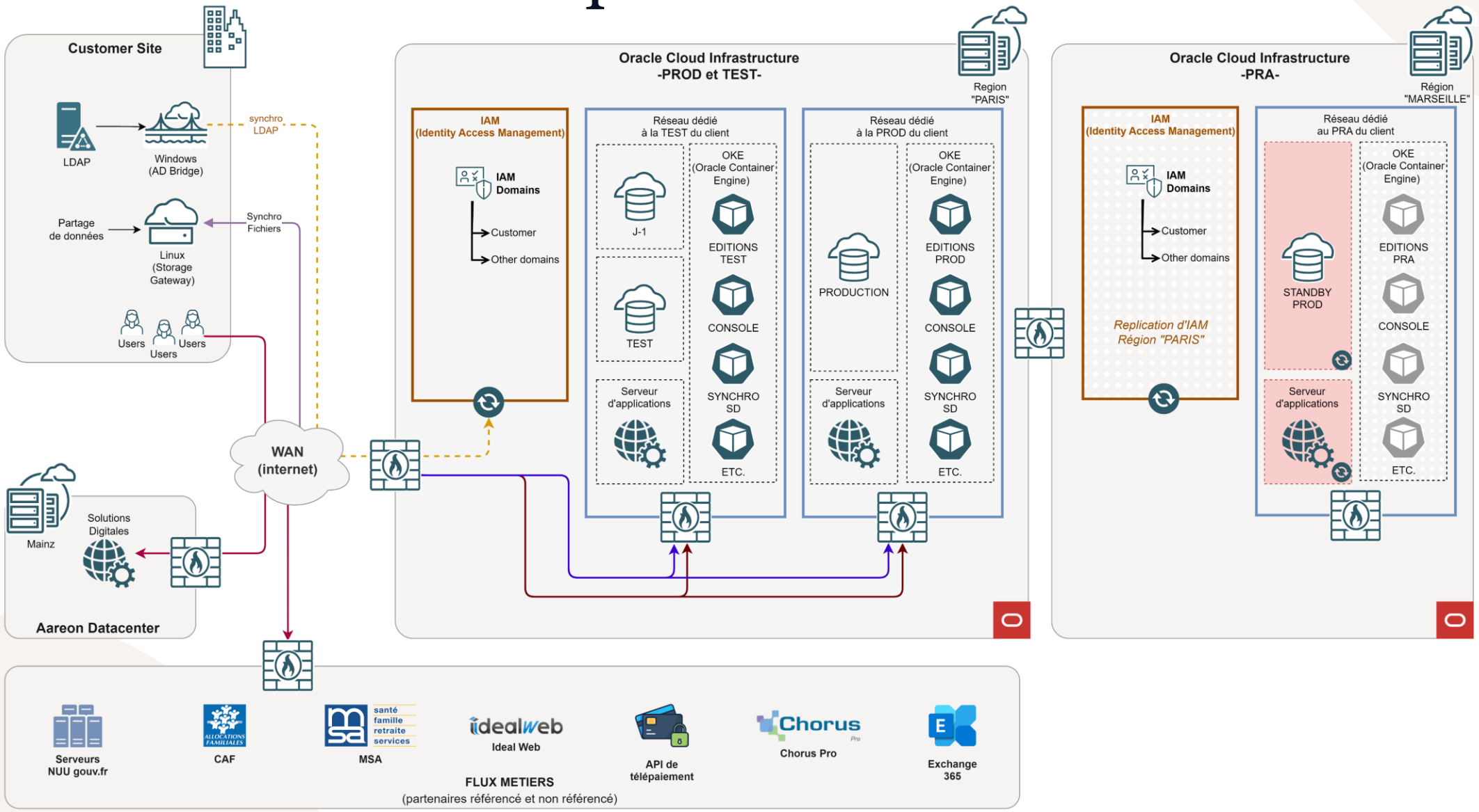
- **Définition :**
  - L'Infrastructure as code (IaC) est un ensemble de mécanismes permettant de gérer, par des fichiers, une infrastructure.

- **Les avantages principaux de « l'infrastructure as Code » sont :**
  - La traçabilité des actions
  - Une uniformisation
  - La réduction des risques
  - La rapidité d'exécution



Aareon

Architecture technique cible

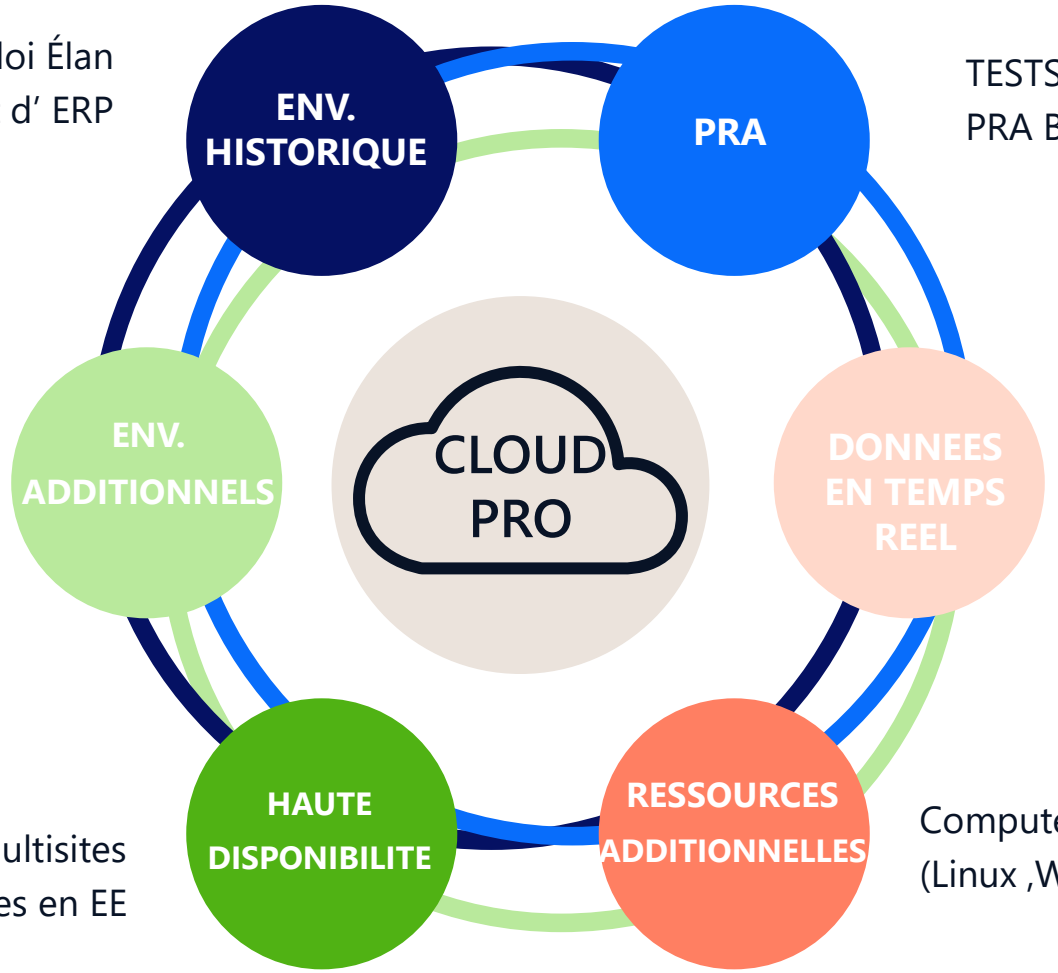


Composition des Serveurs BDD et APPLICATION / environnement

			0 - 8000	8 001 - 20 000	20 001 - 50 000	50 001 - 70 000	70 001- 100 000	100 001 - 120 000
BDD	PROD	SERVEUR	1	1	1	1	1	1
	RECT - PROJ	SERVEUR	1	2	2	2	2	2

			0 - 8000	8 001 - 12 000	12 001 - 20 000	20 001 - 50 000	50 001- 100 000	100 001 - 120 000
APPLI	PROD	SERVEUR	1	1	1	2	2	2
	RECT - PROJ	SERVEUR	1	2	2	2	2	2

Les options spécifiques individualisables



Fusion loi Élan
Changement d' ERP

TESTS PRA MÉTIERS
PRA BASE J-1

Formation, Dev, Etc.

Base de données en EE
Base décisionnelle (copie partielle Goldengate)

Gestion en multisites
Base de données en EE

Compute, Stockage, services, etc. (Linux ,Windows)

Aareon

02 Les services dans le CLOUD

Modèle Cloud « as a Service »

Responsabilité CLIENT

Responsabilité AAREON

I (Infrastructure)

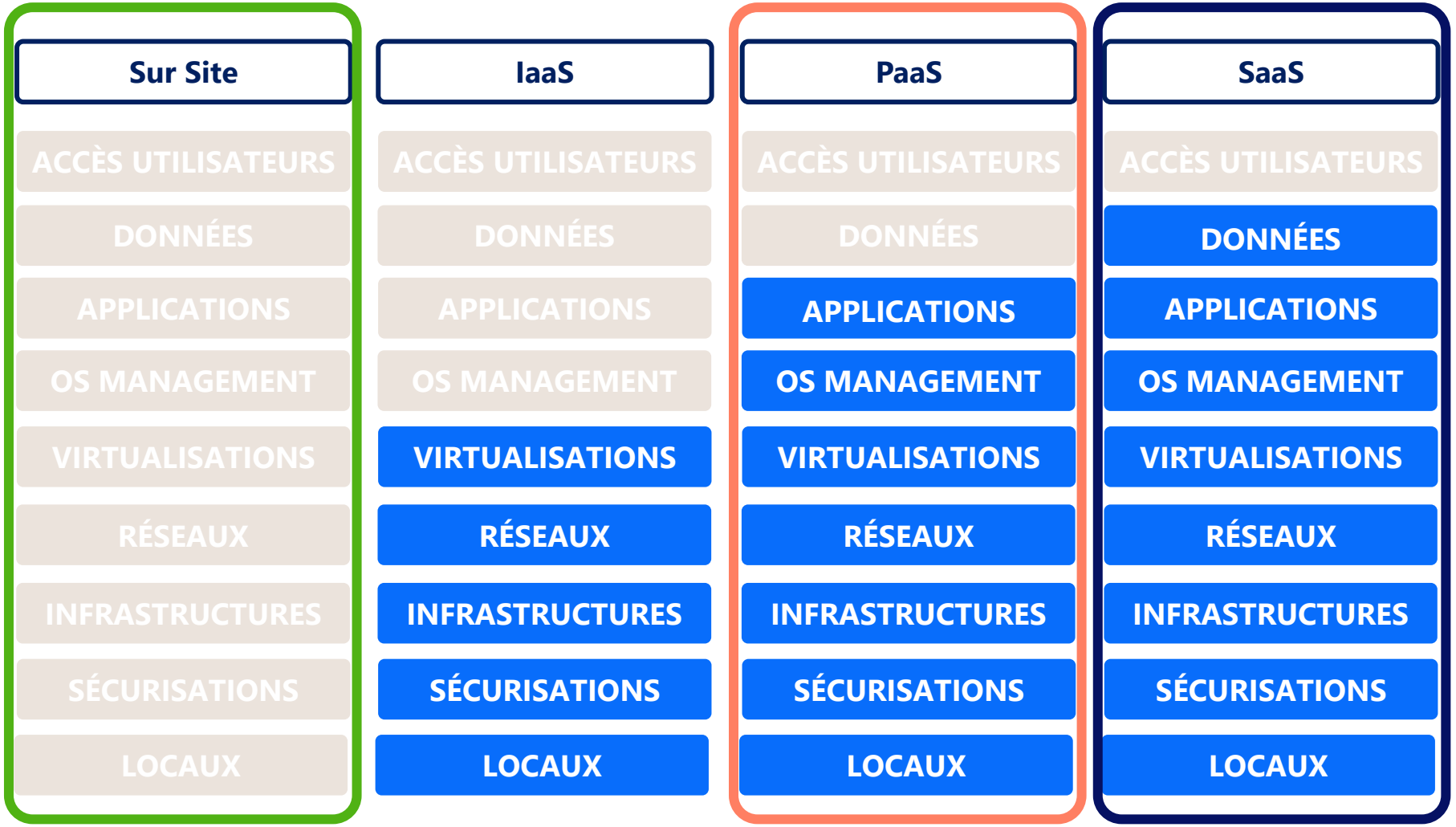
Le fournisseur CLOUD gère les matériels (serveurs, virtualisation, stockage, réseaux).

P (Plateforme)

Le fournisseur CLOUD maintient les applications

S (Service)

Le fournisseur CLOUD prend en charge l'ensemble des couches techniques



Aareon

Plan de migration PIH (scénarios)

ENVIRONNEMENT ACTUEL

CLIENTS
(Sur Site)

Chacun est propriétaire de son environnement.

Serveurs SGBD
Serveurs d'applications
Solutions tierces

PHASE DE TRANSITION

PHASE HÉBERGEMENT

CLIENTS HÉBERGÉS
(PaaS)

AAREON propose de centraliser les environnements ERP courant.

PHASE HYBRIDE

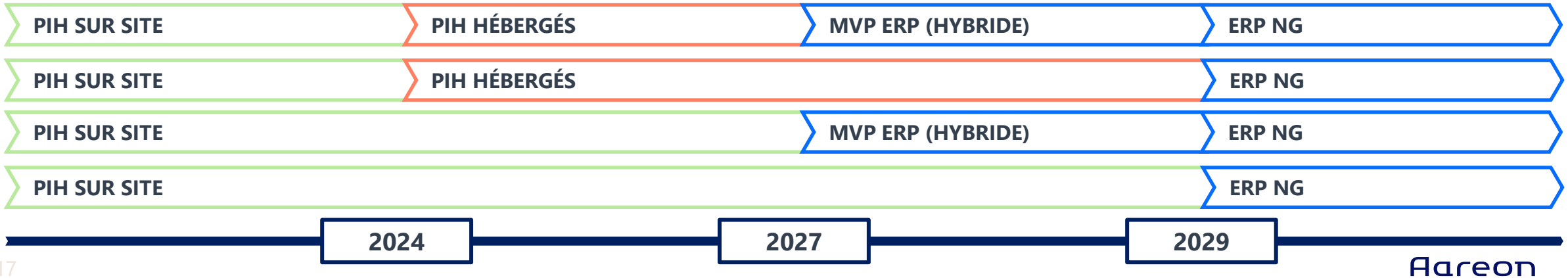
CLIENTS
(SaaS)

AAREON met à disposition une solution hybride (FORMS-APEX).

ERP NG

CLIENTS
(SaaS)

AAREON met à disposition une solution entièrement sous APEX.



Aareon

Matrice métiers PIH

SITE CLOUD HÉBERGÉ | HÉBERGÉ | SITE ou HÉBERGÉ

= **Flux (Sortant)** (https / sftp / smtp (ssl/tls) / pop3 (ssl) / imap (ssl) / ssh / sip)

= **Consommation par fichiers.**

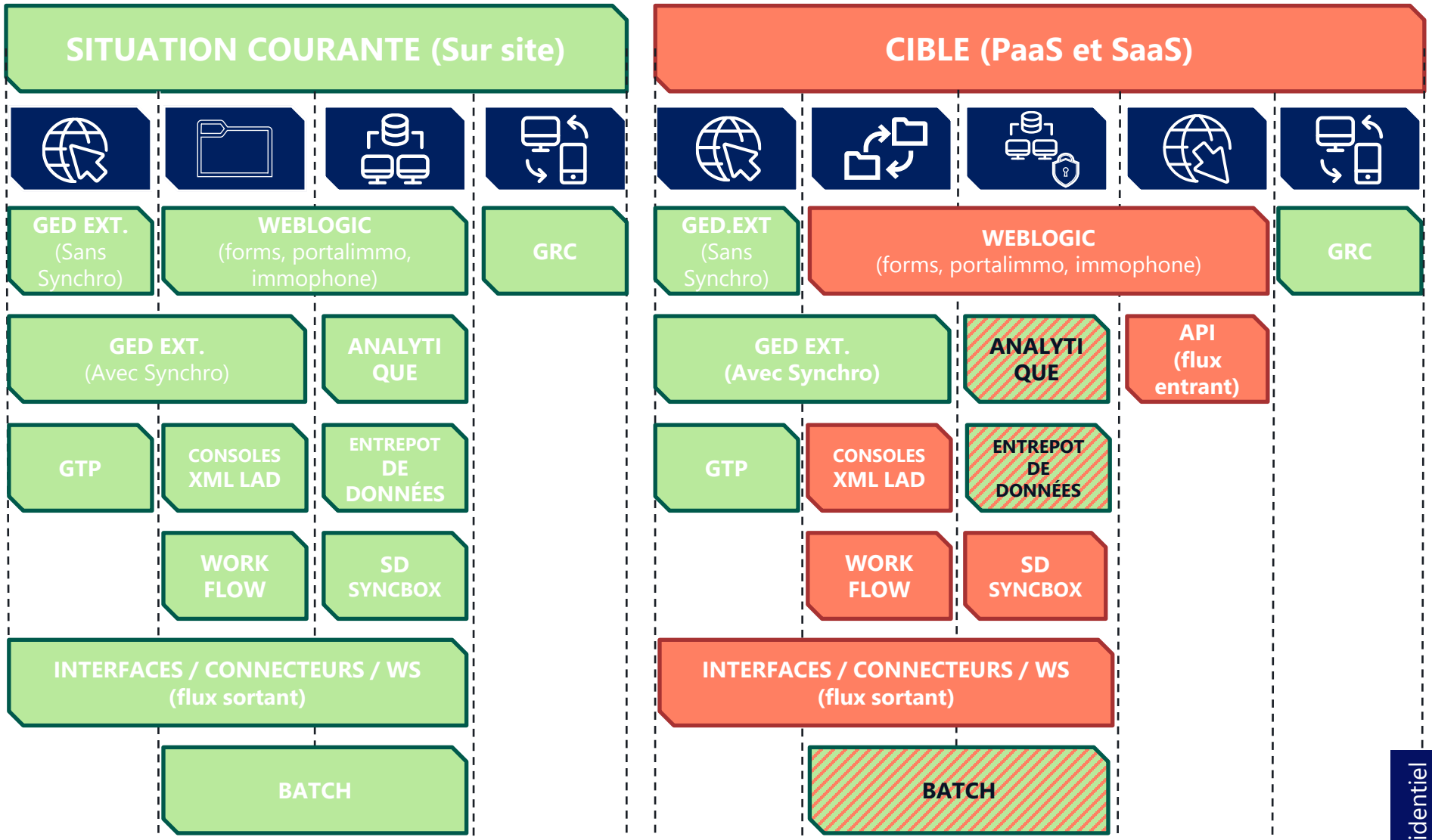
= **Connexion directe en base.**

= **Couplage téléphonique**

= **Consommation par fichiers.** (Synchronisé site <-> cloud)

= **Connexion distante directe en base** (site <-> cloud)

= **Flux (Entrant)** (https)

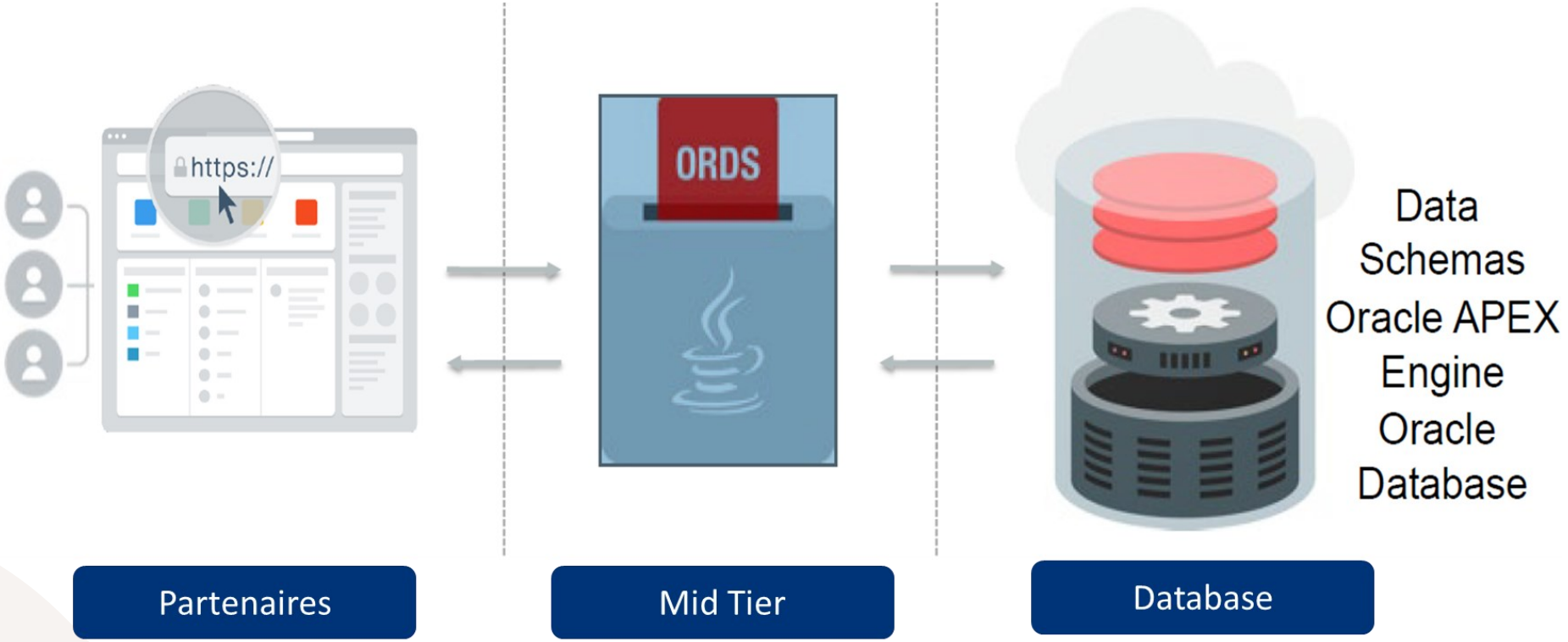


Aareon

03 L’Architecture API

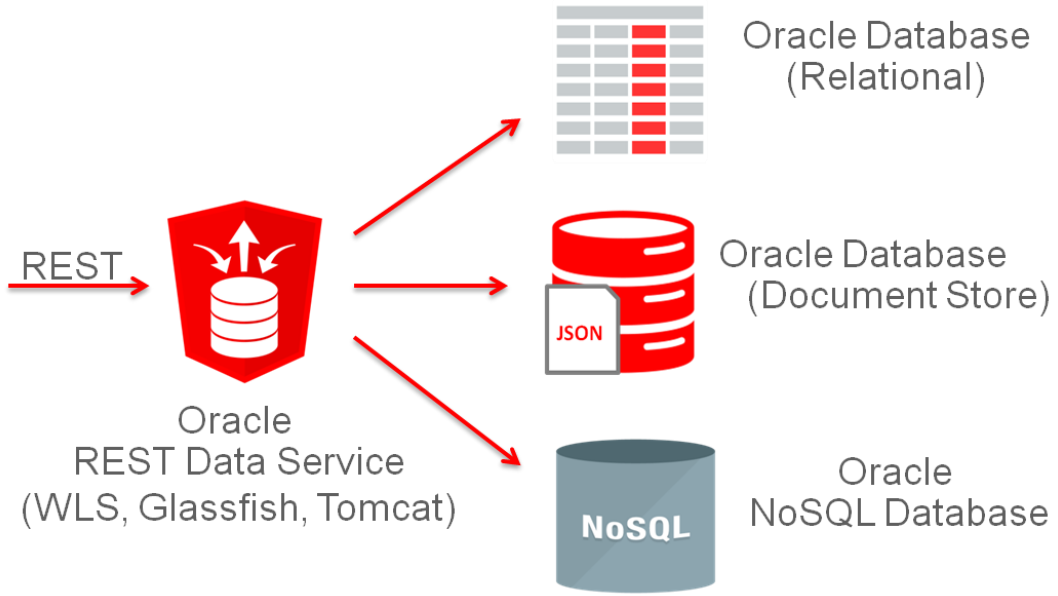
L’architecture API (Interface de Programmation d’Application)

Stack Technique
ORDS : Oracle REST Data Services : Une architecture Trois tiers



ORDS : Oracle REST Data Services

- Permet de capturer ou d'exposer des données dans une base de données Oracle en utilisant le protocole REST.
- Réponses au format standard {json}
- Livré sous forme d'application Java qui peut fonctionner de manière autonome ou dans un conteneur J2EE (Apache Tomcat, Oracle WebLogic).
- Support l'authentification OAuth2.0.
- Utilisation de la logique métier (PL/SQL Packages).
- Résultats paginés pour gérer les performances.
- Documentation Open API (pour partenaires).



04 L’accès aux données

Sécurisation

Identité et Access Management IAM

Gestion unique des identités (SSO).
Authentification des identités (MFO, CYCLE DE VIE).
Accès aux ressources.

Protection et Intégrité de la donnée

Base de données encrypté par défaut (TDE)
Accès par IAM et Certificat (nominatif)
Encryptions de bout en bout

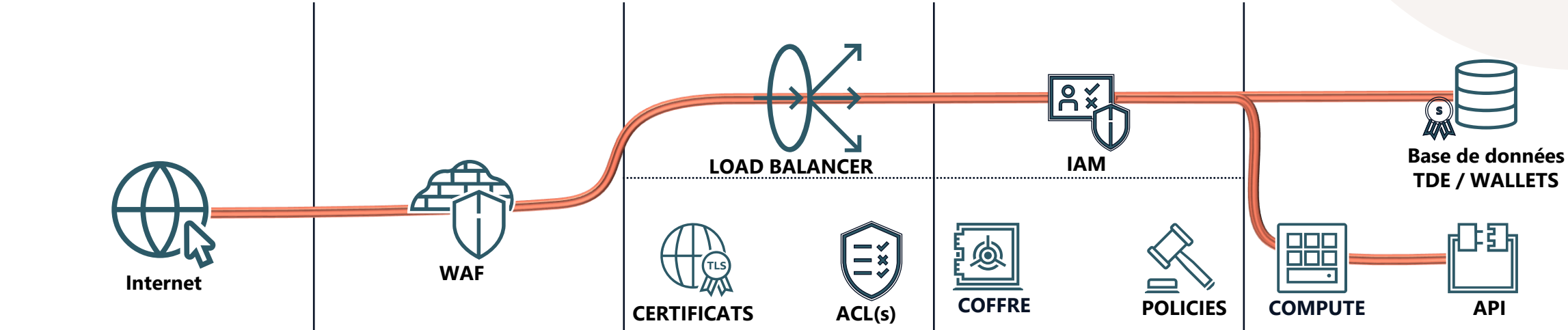
PRA

Perte de données maximale admissibles de 10 à 30 min max
Durée maximale d'interruption admissible de 48h max

Gestion des Systèmes

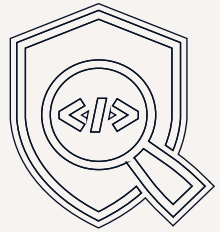
Monitoring , Optimisation
Analyse des logs et traçabilité (SIEM)
OS management

Le cheminement des flux



Communications entre les clients et les serveurs sont sécurisés par le protocole **HTTPS** qui chiffre les données échangées	**WAF** dispositif de sécurité qui protège les applications contre les attaques.	**LOAD BALANCER** pour répartit les requêtes sur les serveurs d'applications ou serveurs de donnée	**IAM** mécanisme d'authentification permettant l'accès aux ressources	Ressources clients dédiées dans un **SUBNET PRIVÉ**.

Exposition des applications



Pour assurer la sécurité et la performance des applications

- Les serveurs applicatifs sont installés dans un **subnet privé**, qui ne sont pas accessibles depuis internet.
- Pour gérer le trafic des clients, un **load balancer** est utilisé, pour répartit les requêtes sur les serveurs d'applications.
- Les communications entre les clients et les serveurs d'applications sont sécurisés par le protocole https, qui chiffre les données échangées.
- Mise en œuvre d'un WAF, c'est un dispositif de sécurité qui protège les applications web contre les attaques malveillantes. Il analyse le trafic entrant et sortant et bloque les requêtes suspectes ou dangereuses.

  Ci-dessous une liste non exhaustive des protections :
  - Protection contre les Attaques par Force Brute
  - Filtrage des Payloads Malveillants
  - Protection contre les Attaques par Déni de Service (DDoS)
  - Listes Blanches et Noires d'Adresses IP
  - Filtrage par Réputation d'Adresse IP
  - Protection contre les Attaques Cross-Site Scripting (XSS).
  - Protection contre les Attaques Cross-Site Request Forgery (CSRF).

Exposition des bases

Pour assurer la sécurité et l’accès aux données

Exposition Indirecte

- Les bases sont installées dans un subnet privé , qui ne sont pas accessibles depuis internet.
- Les base de données sont encryptées.
- Pour gérer le trafic des clients, un load balancer est utilisé, pour aiguiller les requêtes sur les serveurs de données,
- Les communications entre les clients et les serveurs de données sont sécurisés par le protocole https, qui chiffre les données échangées..
- Pour renforcer la sécurité entre les bases de données et les clients, nous utiliserons le mécanisme d'authentification par certificat sur le LISTENER. Ce mécanisme permet de vérifier l'identité des clients.

Echange de données automatisées

Pour assurer les ETL* entre les solutions restantes sur SITE et notre offre CLOUD

- Pour les ETL nous proposons une passerelle de stockage (Storage Gateway fourni par ORACLE et demandé dans nos prés requis technique) afin de faciliter l'intégration des données entre les progiciels restant sur SITE et notre offre CLOUD.

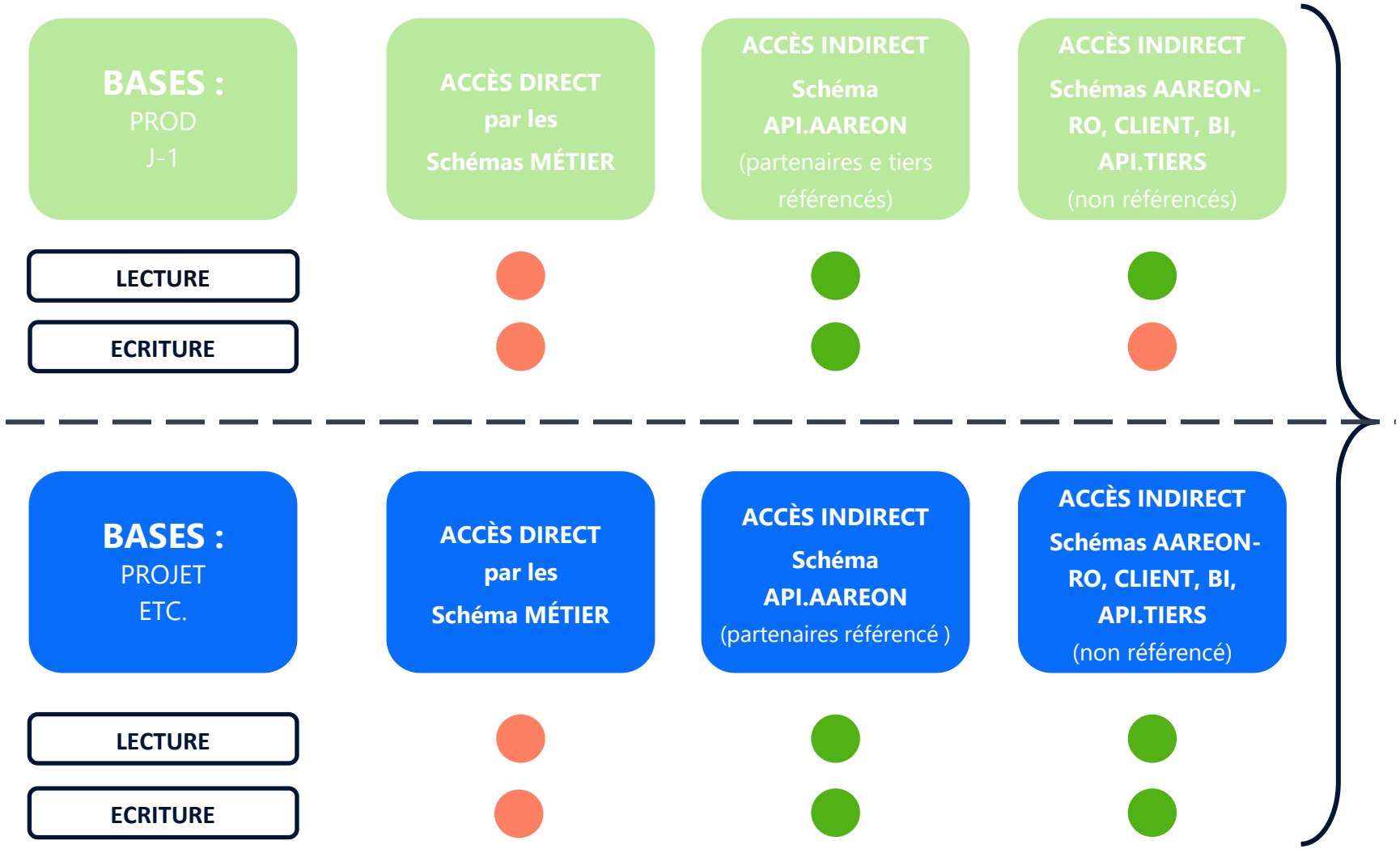
- Cette solution permet de transférer les données par fichier, en respectant les formats et les normes de chaque système. Ainsi, vous pouvez bénéficier de la performance et de la sécurité de notre offre CLOUD, tout en conservant vos applications existantes sur SITE.

* ETL (Extract Transform Load) pour l'automatisation des échanges de données entre progiciels par fichier.

Accès aux données

- **La base de PRODUCTION est sanctuarisée**
  - Accès sous conditions (R, R-W) (Slide 37-38) et depuis OCI (~~non sur site~~)
- **Accès à une base J-1 / PROJET**
  - Accès sous conditions (R, RW) (Slide 37-38) et depuis OCI et/ou sur site.
- **Accès à une base se fait par les outils fournis par AAREON**
  - Accès indirect type Sql Dev Web.
  - Accès direct par SqlNet (HTTPS,TLS, WALLET Oracle) / WAN ou VPN

Matrice des accès aux données sur solution standard



LES ACCÈS SONT :

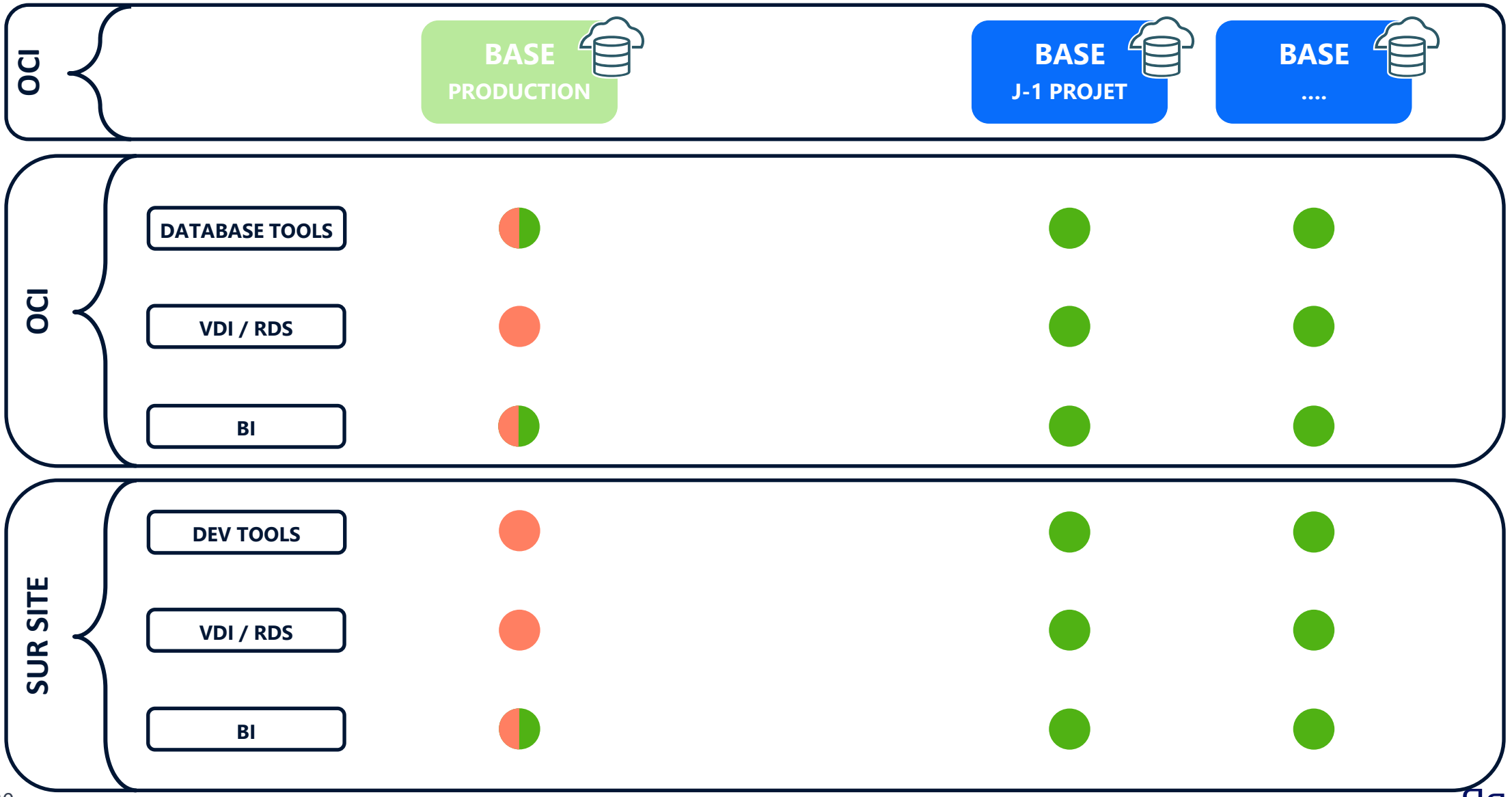
1. Gérés par le IAM via des certificats nominatifs
2. Durée de vie limitée des certificats
3. Schéma dédié Client pour accès indirect.
4. Schéma dédié pour Produits/ Solutions (BI, tiers non référencés) .

Schémas Oracle
(LOGI, HLMWIN, PORTAL, H/L/Sxxxx_GL_00, etc.)
RO : Lecture **RW** : Lecture et Écriture

Aareon

ACCÈS SOUS CONDITIONS ACCÈS KO ACCÈS OK

Matrice des accès aux données par les outils et le lieu



Aareon

Merci pour votre participation !

Rendez-vous pour la Session 2
le mardi 19 mars 2024 de 14h00 à 17h00