
ORACLE®

Le Règlement Général sur la Protection des Données de l'Union européenne :

Comment les solutions de sécurité Oracle peuvent aider

Jérôme CHAGNOUX
Industry Architect / Security Expert
Oracle France TSBU
16 mai 2017

Déclaration de mise en garde

Ce qui suit est destiné à décrire l'orientation générale pour nos produits. Il est conçu uniquement à des fins d'information et ne peut-être incorporé dans un contrat. Il ne s'agit pas d'un engagement à fournir du matériel, du code ou des fonctionnalités, et ne ne doit pas être utilisé pour prendre des décisions d'achat. Le développement, la publication et le calendrier des caractéristiques ou fonctionnalités décrites pour les produits Oracle reste à la seule discrétion de Oracle. Les technologies identifiées ne sont pas disponibles pour tous les services Cloud.

Avertissement

Les informations contenues dans ce document ne doivent pas être interprétées ni utilisées comme un avis juridique sur le contenu, l'interprétation ou l'application de toute législation, réglementation ou directive réglementaire. Les clients existants et potentiels doivent s'adresser à leur propre conseiller juridique pour comprendre l'applicabilité de toute loi ou réglementation relative à leur traitement de données personnelles, y compris par l'intermédiaire des produits ou services de tout fournisseur.

ORACLE

Présentation du règlement

- Le Règlement Général sur la Protection des Données (« RGPD ») remplace une Directive européen de Protection des Données vieille de plus de 15 ans.
- Nouvelles exigences légales pour les responsables du traitement (ou contrôleurs) et les sous-traitants (ou processeurs).
- Les exigences comprennent un nouveau régime de responsabilités et de sanctions.
- Dates clefs :
  - Publication : 4 mai 2016
  - Application : 25 mai 2018[1]

Journal officiel **L 119**

de l'Union européenne

Édition de langue française — Législation — 59e année, 4 mai 2016

Sommaire — *I Actes législatifs* — page

RÈGLEMENTS

* **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([1])** 1

DIRECTIVES

* **Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil** 89

* **Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière** 132

([1]) Texte présentant de l'intérêt pour l'EEE

FR

Les actes dont les titres sont imprimés en caractères maigres sont des actes de gestion courante pris dans le cadre de la politique agricole et ayant généralement une durée de validité limitée.

Les actes dont les titres sont imprimés en caractères gras et précédés d'un astérisque sont tous les autres actes.

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

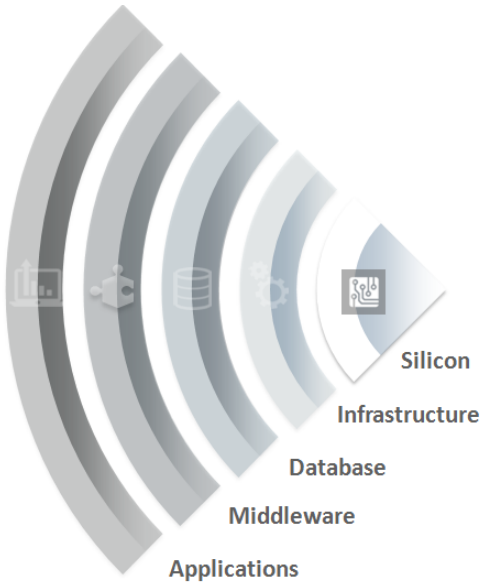
Certains aspects clés du Règlement

Harmonisation des lois sur la confidentialité des données	Le patchwork de 28 lois existantes se transforme en un règlement global (à quelques exceptions)
Applicabilité globale	Les organisations établies dans l'UE ainsi que les organisations extérieures à l'UE offrant des biens et des services à des personnes basées dans l'UE
Droits renforcés pour les individus	Droit de retrait/d'effacement/à l'oubli – que l'utilisateur peut demander à tout moment
Notification obligatoire des failles	Dans les 72 heures aux autorités de contrôle, « sans délai » aux personnes concernées
Responsabilité conjointe	Entre responsables de traitement et sous-traitants
Consentement explicite	Usage des données personnelles conformément à l'accord obtenu explicitement avec propriétaire des données (la personne concernée)
Transferts de données	Les droits de confidentialité sont attachés aux données et suivent globalement les données dans leur transfert
Recours collectifs	Ouvre la possibilité de poursuites collectives de la part des individus
Mise en application commune	Les autorités de contrôle appliqueront le règlement en se consultant entre elles
Amendes augmentées	Jusqu'à 4% du chiffre d'affaires global ou 20 000 000€, selon la valeur la plus élevée
Besoin de protection des données	Exigence explicite de protection des données, par conception et par défaut, ainsi que la sécurisation des traitements

Oracle développe des fonctions de Sécurité renforcée

Principe du moindre privilège

Défense en profondeur



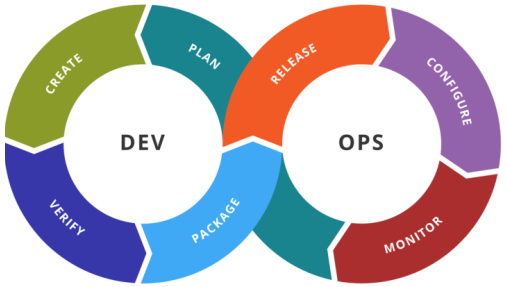
Pour toutes vos données sensibles, incluant Propriétés Intellectuelles, Données Business et Informations Personnelles

ORACLE

Les outils de Sécurité Oracle qui peuvent être utiles pour le RGPD

Sécurité des Personnes

Sécurité des Applications



Sécurité des Données

Depuis plusieurs années, les clients Oracle utilisent plusieurs de ces outils pour les aider à se conformer à la Directive de 1995 de l'Union européenne sur la Protection des Données

ORACLE

Les outils de Sécurité Oracle qui peuvent être utiles pour le RGPD

Sécurité des Personnes

Authentification

Gestion des identités

Gouvernance

Single Sign-On

Audit

Self-Service

Conformité

Gestion des accès

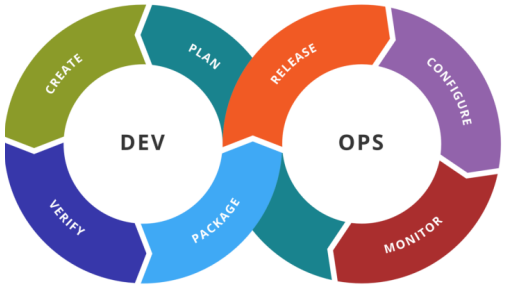
Habilitations

Sécurité des API

Sécurité des Applications

Configuration des applications et des services

Conformité IT



Sécurité des API

Patching

Audit

Performance des applications et des services

Sécurité des Données

Contrôles préventifs

Chiffrement

Séparation des pouvoirs

Data Masking

Gestion des clefs

Contrôles d'administration

Contrôles par investigation

Audit

Surveillance des menaces, Analyse des logs et des utilisateurs, Réponse aux incidents

ORACLE

Les produits de Sécurité Oracle

Utilisables pour protéger les données personnelles (ou toutes autres données sensibles de l'entreprise)

Systèmes existants

- ❑ Devraient être retro-paramétrés pour améliorer la sécurité de leurs bases de données (impact minimal sur la base de données)
- ❑ Devraient évaluer, scorer et corriger les violations en utilisant des métriques standard de l'industrie en plus de règles personnalisées
- ❑ Devraient analyser le comportement des utilisateurs et des entités dans les applications et les services afin de détecter les anomalies/intrusions et y répondre
- ❑ Peuvent être modifiés pour utilisé une infrastructure d'authentification et de contrôle d'accès partagée
- ❑ Devraient être administrés de façon à ce que les personnes ayant changé de fonction ou quitté l'organisation n'aient plus d'accès aux applications

Nouveaux systèmes

- ❑ Devraient avoir leurs bases de données paramétrées de façon sécurisée grâce aux outils appropriés de sécurisation de la base de données
- ❑ Comme pour les systèmes existant, avec un focus sur les services Cloud hétérogènes (Oracle, AWS, Azure, ...)
- ❑ Doivent avoir des APIs protégées par défaut
- ❑ Devraient profiter d'une infrastructure commune de Gestion des Identités et des Accès

ORACLE

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Protection des données dès la conception et protection des données par défaut - Art. 25 (suite)	Comment la technologie Oracle peut aider	Produits/Services Cloud de sécurité Oracle correspondant
… le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. …	**Sécurité des Données** Protéger les *données personnelles* dans les applications nouvelles ou existantes par le déploiement des produits de sécurisation des bases de données appropriés. Masquer (pseudonymiser) les copies des *données personnelles* de production dans les environnements de développement et de qualification pour réduire le risque d'exposition des *données personnelles*. Réécrire à la volée les données personnelles (par exemple réécrire une date de naissance en **-**-1985) pour minimiser l'accès aux *données personnelles* via les applications.	Oracle Database Security Oracle DBCS High/extreme performance Oracle Data Masking Oracle Advanced Security

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Protection des données dès la conception et protection des données par défaut - Art. 25 (suite)	**Comment la technologie Oracle peut aider**	**Produits/Services Cloud de sécurité Oracle correspondant**
… par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. …	**Sécurité des Personnes** Fournir uniquement aux **bonnes** personnes (employés, sous-traitants, clients, partenaires) des accès aux **bonnes** *données personnelles* au **bon** moment.	Oracle Identity Governance Suite Oracle Access Management Suite Oracle Identity Cloud Service
	Sécurité des Applications Assurer la visibilité, la configuration et la protection contre les menaces pour les services Cloud.	Oracle CASB Cloud Service
	Protéger les API des utilisations abusives.	Oracle API Platform Cloud Service
	S'assurer que les applications et services Cloud soit correctement configurés.	Oracle Compliance Cloud Service
	Garantir que les applications et services Cloud qui gèrent des *données personnelles* soient sous surveillance contre les intrusions/utilisations abusives (y compris internes à l'entreprise).	Oracle Security Monitoring and Analytics Cloud Service

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Sécurité du traitement - Art. 32	Comment la technologie Oracle peut aider	Produits/Services Cloud de sécurité Oracle correspondant
… le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :	**Sécurité des Données**	
	Masquer les *données personnelles* en dehors des bases de production.	Oracle Data Masking
	Chiffrer les *données personnelles* lors du stockage et des transferts vers ou depuis des bases de données Oracle.	Oracle Advanced Security
a) la pseudonymisation et le chiffrement des données à caractère personnel;	Gérer les clefs utilisées pour chiffrer les bases contenant des *données personnelles*.	Oracle Key Vault
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;	Se protéger des utilisateurs à privilèges	Oracle Database Vault
	Se protéger des attaques par injection SQL sur les bases contenant des *données personnelles*.	Oracle Audit Vault Database Firewall
	Répliquer des *données personnelles*.	Oracle Data Guard
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; …	Activer la disponibilité à chaud des *données personnelles*.	Oracle Real Application Clusters
	Activer la résilience des traitement	Oracle Zero Data Loss Recovery Appliance
	Protéger les bases de données sur le Cloud Oracle	Oracle DBCS High/extreme performance

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Sécurité du traitement - Art. 32	Comment la technologie Oracle peut aider	Produits/Services Cloud de sécurité Oracle correspondant
… le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : a) la pseudonymisation et le chiffrement des données à caractère personnel; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; …	**Sécurité des Personnes** Gérer le cycle de vie des utilisateurs qui accèdent aux *données personnelles*. Centraliser l'authentification des utilisateurs qui accèdent aux *données personnelles*. **Sécurité des Applications** Assurer la visibilité, la configuration et la protection contre les menaces pour les services Cloud. Protéger les API qui fournissent des accès aux *données personnelles*. Surveiller la configuration des applications et des services. Surveiller et répondre aux comportements anormaux dans les applications traitant des *données personnelles*.	Oracle Identity Governance Oracle Access Management Oracle Directory Services Oracle Identity Cloud Service Oracle CASB Cloud Service Oracle API Platform Cloud Service Oracle Compliance Cloud Service Oracle Security Monitoring and Analytics Cloud Service

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

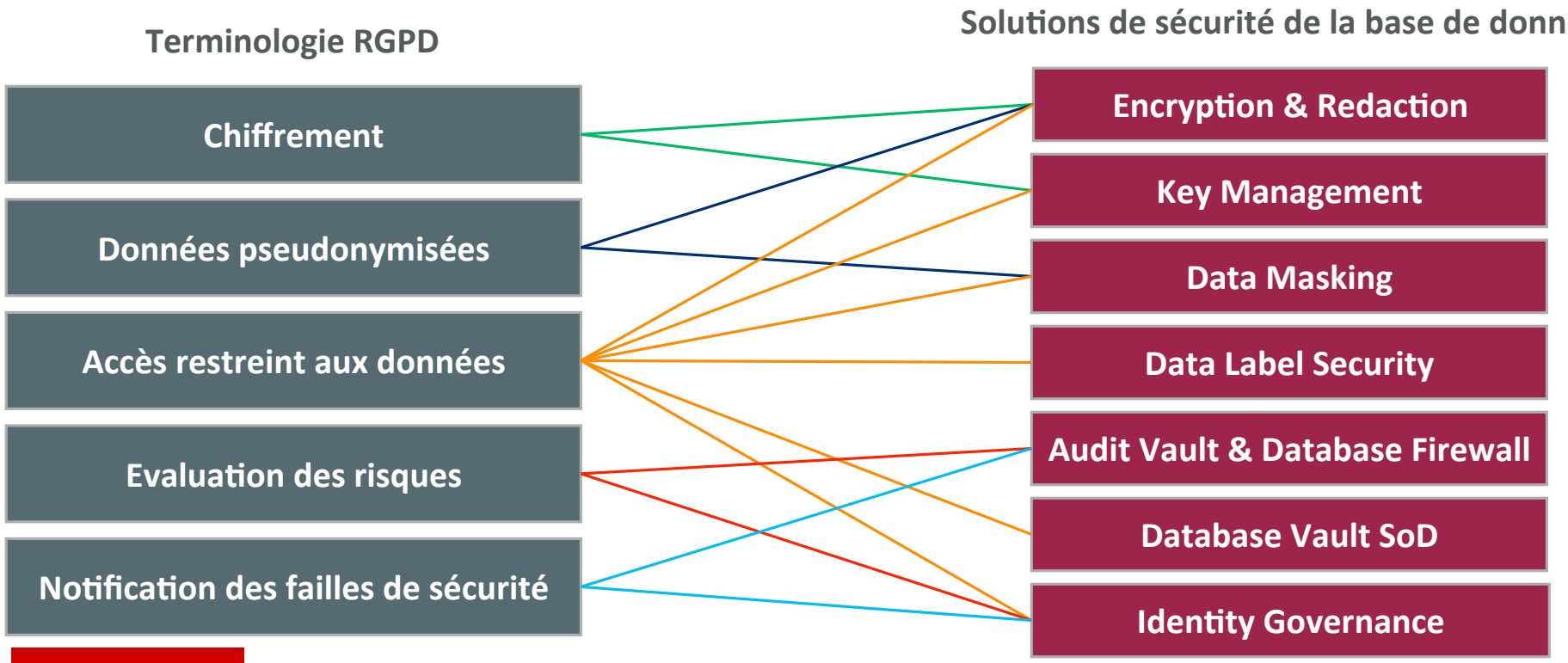
Communication à la personne concernée d'une violation de données - Art. 34	Comment la technologie Oracle peut aider	Produits/Services Cloud de sécurité Oracle correspondant
… La communication à la personne concernée (…) n'est pas nécessaire si (…) : a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées (…), en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ; b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées (…) n'est plus susceptible de se matérialiser ; …	**Sécurité des Données** Protéger les bases de données **Sécurité des Personnes** Protéger le parc applicatif Gérer les accès des utilisateurs **Sécurité des Applications** Assurer la visibilité, la configuration et la protection contre les menaces pour les services Cloud. Surveiller/corriger les configurations. Gestion de la sécurité DevOps. Analyse des logs de sécurité.	 Oracle Advanced Security Oracle Key Vault Oracle Database Vault Oracle Audit Vault & Database Firewall Oracle Access Management Oracle Identity Governance Oracle Directory Services Oracle CASB Cloud Service Oracle API Platform Cloud Service Compliance Cloud Service Security Monitoring and Analytics Cloud Service

Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Conditions générales pour imposer des amendes administratives - Art. 83	**Comment la technologie Oracle peut aider**	**Produits/Services Cloud de sécurité Oracle correspondant**
… Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants: (…) f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ; …	Voir les technologies Oracle relatives aux articles 25 et 32 citées précédemment	

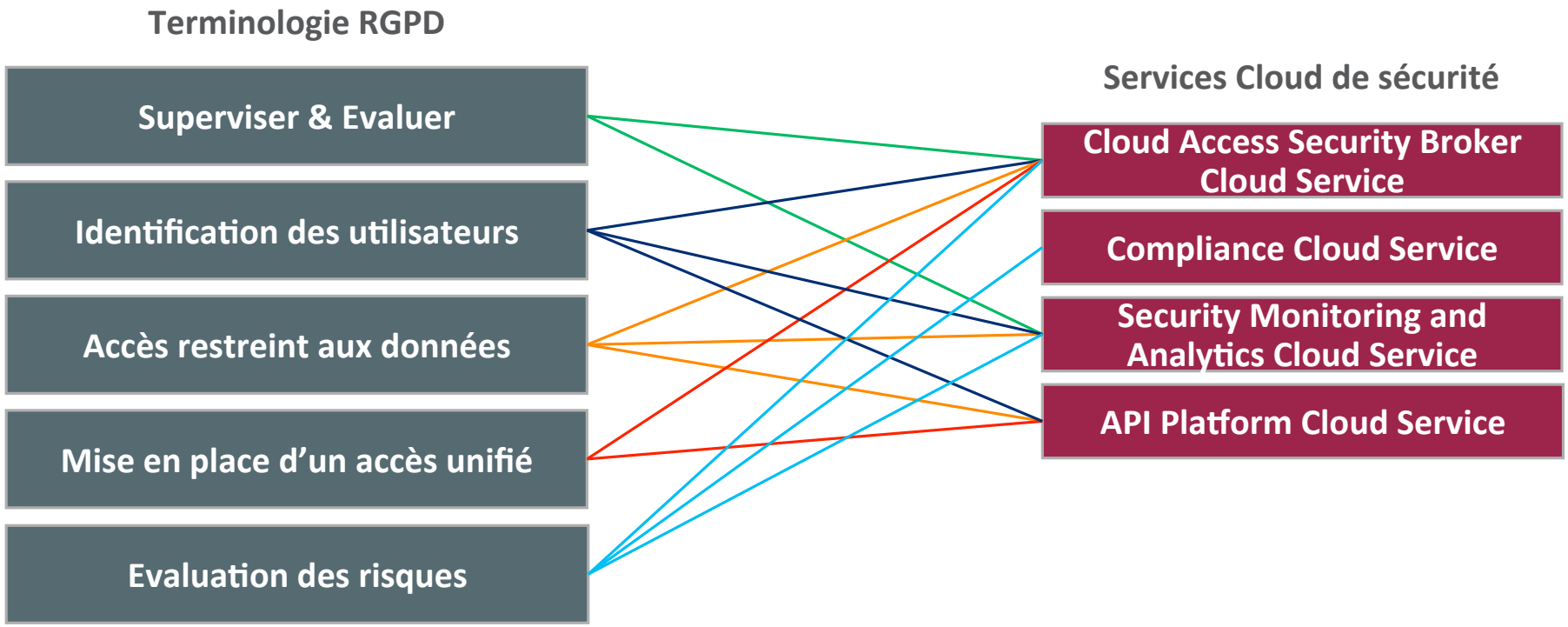
Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Sécurité des Données



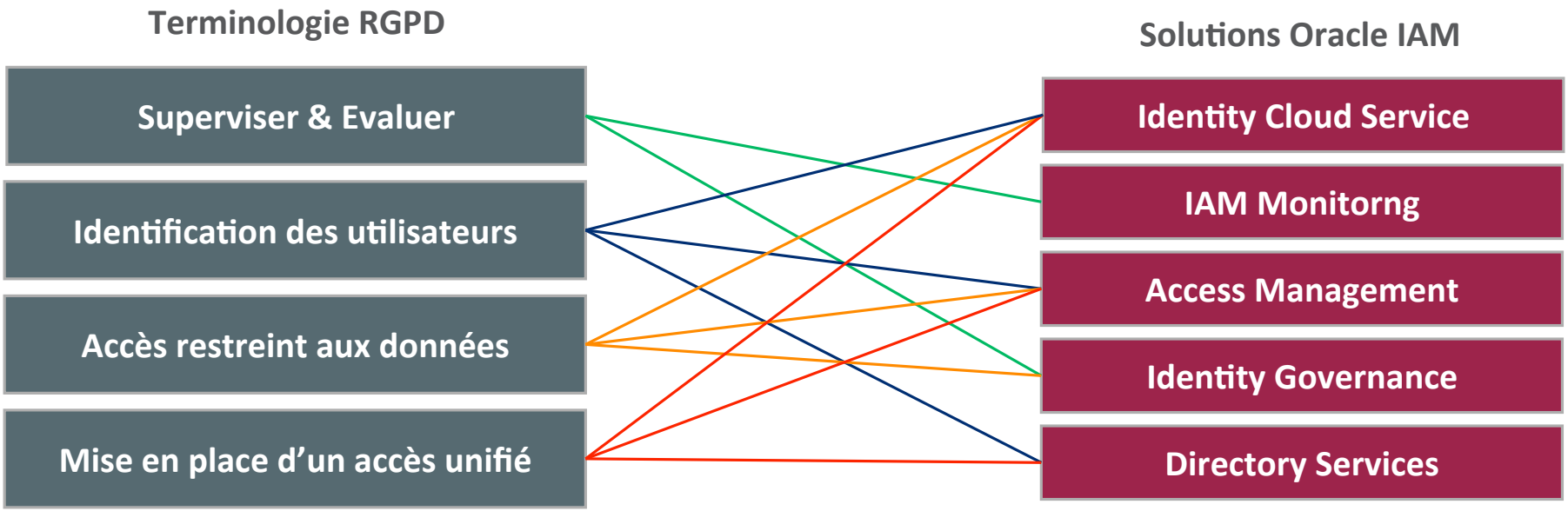
Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Sécurité des Applications



Les solutions Oracle qui peuvent aider à la mise en conformité RGPD

Sécurité des Personnes



Synthèse des capacités des produits Oracle Security

- **Sécurité de la base de données**
  - Oracle Advanced Security
    - Chiffrement des données au repos
    - Réécriture de données à la volée
  - Oracle Key Vault
    - Gestion des clés de chiffrement (création, renouvellement, répudiation…)
  - Oracle Database Vault
    - Protection contre les utilisateurs à privilèges (par exemple DBA)
  - Oracle Audit Vault & Database Firewall
    - Entrepôt pour la centralisation des traces d'activités pour les bases de données de différents éditeurs ou d'autres produits
    - Protection contre les attaques par injection SQL (pour les bases de données de différents éditeurs)
  - Oracle Label Security
    - Protection supplémentaire pour les lignes d'enregistrement très importantes
  - Data Masking
    - Masquage (ou pseudonymisation) des données sensibles pour les environnement hors production

- **Gestion des Identités et des Accès**
  - Oracle Identity Governance
    - Gestion du cycle de vie des utilisateurs (arrivées, mutations, départs)
  - Oracle Access Management
    - Single Sign On, authentification double-facteurs
  - Oracle Directory Services
    - Offre d'annuaires LDAP (incluant la virtualisation d'annuaire)

- **Services Cloud de Sécurité**
  - DB Cloud peut utiliser les fonctionnalités/options de sécurité de la base de données
    - Certaines options peuvent se déployer sur site (on-premise)
  - Oracle Identity Cloud Service
  - Oracle Cloud Access Security Broker (CASB) Cloud Service
  - Oracle Security Monitoring and Analytics Cloud Service
  - Oracle Compliance Cloud Service
  - Oracle API Platform Cloud Service

Alors, par où commencer…

Faites un Security Risk Assessment

Livre blanc sur la Sécurité des Bases de Données et le RGPD

(chaque voyage démarre là où vous êtes)

ORACLE

Integrated Cloud

Applications & Platform Services


ORACLE®