White Paper Security

ORANGE BUSINESS

CLOUD AVENUE DYNAMIC

Version : 2.0
Date : 22/01/2026

Business

Description du document

Propriétés				
Titre document	White Paper Security – Cloud Avenue Dynamic			
Version	2.0			
Rédacteur	Business Security Officer (BSO) Cloud Avenue Dynamic			
Statut	❑ En cours	❑ Revue	■ Validé	❑ Approuvé
Date	Jeudi 22 janvier 2026			

Classification du document

Classification	
Confidentialité	Diffusion libre

Diffusion

Société	Fonction	Diffusion
Global Delivery & Operations (GDO) Sales		Lecture
	BM-GDO Sales	Approbation
		Lecture
Ob/Global Delivery & Operations (GDO) / Global Platforms & Service (GPS)	Chief Information Security Officer (CISO) GDO/GPS	Lecture
	BSO Cloud Avenue Dynamic	Rédaction

Historique des versions

Version	Opération	Nom	Date
1	Création du document	BSO Cloud Avenue Dynamic	Janvier 2026

Sommaire

White Paper Security

1. Introduction

1.1. Objet du document

Le présent document constitue le White Paper Security d'Orange Business pour la fourniture du service Cloud Avenue Dynamic aux clients. Il décrit les principales mesures de sécurité techniques et organisationnelles appliquées par Orange Business pour garantir la sécurité de ses offres.

Ce document s'applique aux offres Cloud professionnelles commercialisées par Orange Business à destination des entreprises. Les offres traitées dans ce document sont :

- Cloud Avenue Dynamic

1.2. Organisation du document

Le présent document suit l'organisation par chapitres de l'ISO 27002:2022 :

- Le chapitre 1 constitue l'introduction du document ;
- Le chapitre 2 constitue une synthèse des atouts de Cloud Avenue Dynamic sur les aspects sécurité ;
- Le chapitre 3 liste les mesures de sécurité organisationnelles mises en œuvre ;
- Le chapitre 4 détaille les mesures de sécurité applicables aux personnes ;
- Le chapitre 5 concerne les mesures de sécurité physique implémentées ;
- Le chapitre 6 liste les mesures de sécurité technologiques mises en œuvre ;
- Les annexes.

2. Forces de l'offre Cloud Avenue Dynamic sur la sécurité

Ce chapitre liste les principaux atouts de l'offre Cloud Avenue Dynamic sur les aspects sécurité.

2.1. Gouvernance & Conformité :

La sécurité de Cloud Avenue Dynamic repose sur une gouvernance rigoureuse et une conformité certifiée. L'offre bénéficie d'un cadre normatif complet, fondé sur de nombreuses certifications comme les normes ISO 27001, SOC2 et CISPE, qui garantissent la mise en œuvre de bonnes pratiques internationales en matière de gestion de la sécurité de l'information et de protection des données dans le cloud.

Enfin, la conformité au RGPD est assurée par la localisation et le traitement intégral des données au sein du territoire français, sous juridiction nationale.

2.2. Hébergement

L'ensemble des données est hébergé dans des datacenters situés exclusivement en France, à Val-de-Reuil et Chartres. Ces infrastructures appartiennent et sont exploitées directement par Orange.

Les datacenters d'Orange sont conçus pour offrir un très haut niveau de résilience, avec redondance énergétique, supervision continue et capacités de basculement entre sites, que le client doit souscrire pour garantir une continuité de service même en cas de sinistre majeur.

2.3. L'architecture

L'architecture technique de Cloud Avenue Dynamic repose sur des fondations robustes, construites autour des technologies VMware vCloud Director et NSX-T. Cette base permet de garantir une isolation stricte entre les clients grâce à une segmentation réseau avancée et à la virtualisation sécurisée des ressources.

Chaque client dispose d'environnements distincts et contrôlables, avec la possibilité d'opter pour des infrastructures dédiées via l'offre vCenter On Demand. Ces options assurent un cloisonnement logique et physique des données et des charges de travail.

Les connexions sont protégées par des dispositifs de sécurité réseau intégrés, tels que les pare-feux distribués, le filtrage de flux, le VPN IPsec et la connectivité MPLS certifiée EAL2+. En complément, des mécanismes de protection anti-DDoS et des options de filtrage avancé viennent renforcer la disponibilité et la défense périmétrique des environnements clients.

2.4. Support et accompagnement

Au-delà de la technologie, Cloud Avenue Dynamic se distingue par la qualité de son accompagnement. Le support est assuré par des équipes d'experts cloud et sécurité, disponibles en continu. Orange Business met à disposition un vaste ensemble de ressources documentaires, de guides techniques et de bonnes pratiques accessibles via le wiki Cloud Avenue Dynamic, favorisant l'autonomie des clients tout en garantissant un cadre sécurisé : https://cloud.orange-business.com/offres/infrastructure-iaas/cloud-avenue/wiki-cloud-avenue/accueil/presentation-de-cloud-avenue/

L'accompagnement à la migration et à la sécurisation des environnements fait également partie de l'offre, avec des conseils adaptés aux enjeux spécifiques de chaque organisation.

3. Mesures de sécurité organisationnelles

Ce chapitre correspond à la thématique 5 de l'ISO 27002 version 2022.

3.1. Politique de sécurité

Les politiques de sécurité sont alignées sur les normes ISO 27001 et ISO 27002. L'offre Cloud Avenue Dynamic suit les politiques de sécurité et réglementations d'Orange Groupe.

3.2. Organisation de la sécurité

Cette partie décrit d'un point de vue « sécurité » l'organisation de l'offre Cloud Avenue Dynamic.

3.2.1. Relations avec les partenaires technologiques pour la gestion des vulnérabilités et l'optimisation de l'infrastructure

Nous entretenons des partenariats technologiques structurés avec des éditeurs et intégrateurs de référence — notamment VMware — afin d'accélérer et sécuriser la gestion des correctifs et l'analyse continue de nos infrastructures. Ces partenaires nous donnent accès aux avis de sécurité, bonnes pratiques et canaux d'escalade éditeur.

L'objectif est d'assurer un maintien en condition de sécurité et d'opérationnalité mesurable, tout en réduisant les délais de traitement des vulnérabilités et l'empreinte de risque pour nos clients.

3.2.2. Business Security Officer

Le client peut choisir une prestation BSO client supplémentaire au moment de la signature du contrat. Dans ce cadre, Orange Business nomme un Business Security Officer (BSO) pour piloter la sécurité sur tout ou partie de la durée de la prestation.

Par défaut, ses missions sont :

- Un contact privilégié au sein du département sécurité avec un Business Security Officer pour le suivi de la sécurité de la prestation et les conseils sécurité ;
- La collecte d'indicateurs de sécurité prédéfinis et un reporting périodique sous forme de tableau de bord sécurité et d'un comité de sécurité ;
- Apporte sa contribution pour la coordination et la priorisation des actions de correction des incidents de sécurité ;
- Accompagne l'infrastructure lors de ses audits et suit les plans d'actions de correction ;
- La mise à jour annuelle de la documentation sécurité et d'un Plan d'Assurance Sécurité personnalisé.

Le Business Security Officer, dans le cadre de sa relation avec Cloud Avenue Dynamic, s'assure du respect de la ségrégation des tâches et de la bonne application de la politique du SMSI et fournira ainsi les indicateurs correspondants. Il respecte et est garant des mesures de sécurité de l'information mises en œuvre au cours de la prestation. Il prend en compte dans son analyse les exigences du client et les spécificités réglementaires (certification HDS, GDPR) pour proposer d'éventuels ajustements voire de nouveaux services.

Les missions du Business Security Officer peuvent être étendues en fonction des prestations contractualisées (fréquence de reporting, indicateurs du tableau de bord, fréquence des audits, de la mise à jour de la documentation sécurité, gestion de la sécurité d'infrastructure dédiée telle que des locaux, IT et personnels dédiés etc.)

3.2.2.1. Comités de sécurité

Le « Comité Sécurité » est une instance qui permet de suivre régulièrement l'avancement du niveau de sécurité de la solution client. Il est organisé et animé par le Business Security Officer.

SW01 - COSEC (Comité de sécurité)		
Périmètre de la prestation couvert	Ensemble de la prestation	
Ordre du jour type	Pour la période écoulée ▪ Revue des alertes de sécurité ▪ Revue des indicateurs de sécurité ▪ Revue du PAS	
Fréquence	1 COSEC trimestriel	
Participants	Orange Business Security : - BSO	Orange Business : - Cloud Avenue Dynamic
Documents en entrée	Documents supports du comité	
Documents en sortie	Compte rendu	

Cette fréquence peut être ajustée par le Business Security Officer selon les besoins de Cloud Avenue Dynamic.

Indicateurs et tableaux de bord

La SSI du Contrat sera pilotée au travers d'indicateurs qui seront tous produits par le BSO et analysés en détail lors du comité sécurité.

Ci-après, la liste des éléments applicables au contrat et leur fréquence de reporting.

3.2.2.1.1. Indicateurs Primaire (Run)

Security Weather and Reporting

01

Security Governance

La gouvernance Sécurité est un comité de pilotage continu de la posture de sécurité de l'offre, en coordination avec les équipes Global Platforms & Services. Son périmètre couvre la mise à jour des analyses de risques, la veille et la remédiation des vulnérabilités, l'exécution et le suivi des plans d'actions, la gestion des incidents et des changements à impact sécurité, ainsi que la conformité/audits, les tests de sécurité et la continuité d'activité.

02

Security Committee

Présenté en comité de sécurité, le tableau de bord sécurité contient les différents indicateurs du présent Plan d'Assurance Sécurité et relate plus généralement l'état de santé de la solution Global Platforms & Services Cloud.

Vulnerability Review

01

Vulnerabilities Management

Le Business Security Officer réalise une veille des vulnérabilités pouvant affecter les machines de la solution. Un rapport est formalisé sous forme d'indicateurs et rapporté en comité de sécurité.

02

Vulnerability Health

Une attention particulière est apportée aux vulnérabilités de niveau 4 (Haute) et 5 (Critique). Cet indicateur est revu en comité de sécurité. Un rapport est formalisé et rapporté en comité de sécurité.

3.2.2.1.2. Indicateurs Complémentaires (Run)

Security Review

01

Accounts Access Review

Le Business Security Officer fait une revue de l'ensemble des comptes de la plate-forme et valide les accès. Il rend compte en comité de sécurité.

02

Password Policy and Rotation Review

Le Business Security Officer vérifie la politique des mots de passe mis en place sur l'ensemble des comptes de l'offre et la bonne rotation de ces derniers. Il rend compte en comité de sécurité.

Technical Review

05

System Configuration Review

Le Business Security Officer suit l'évolution des configurations système pour identifier tout changement susceptible de baisser le niveau de sécurité et/ou identifier les opportunités de durcissement.

06

Operation System Obsolescence

Le Business Security Officer met en évidence et suit l'évolution de l'Obsolescence des systèmes d'exploitation, équipements et applicatives qui composent le parc du contrat.

Physical Security Review

Sur demande du client, une visite annuelle de nos centres d'hébergement peut être organisée dans le cadre d'un audit pour vérifier la bonne mise en œuvre des mesures décrites dans le présent document.

3.2.2.1.3. RACI

Cloud Avenue Dynamic est une infrastructure de type IaaS (Infrastructure As A Service). Le modèle de responsabilité suivant est appliqué :

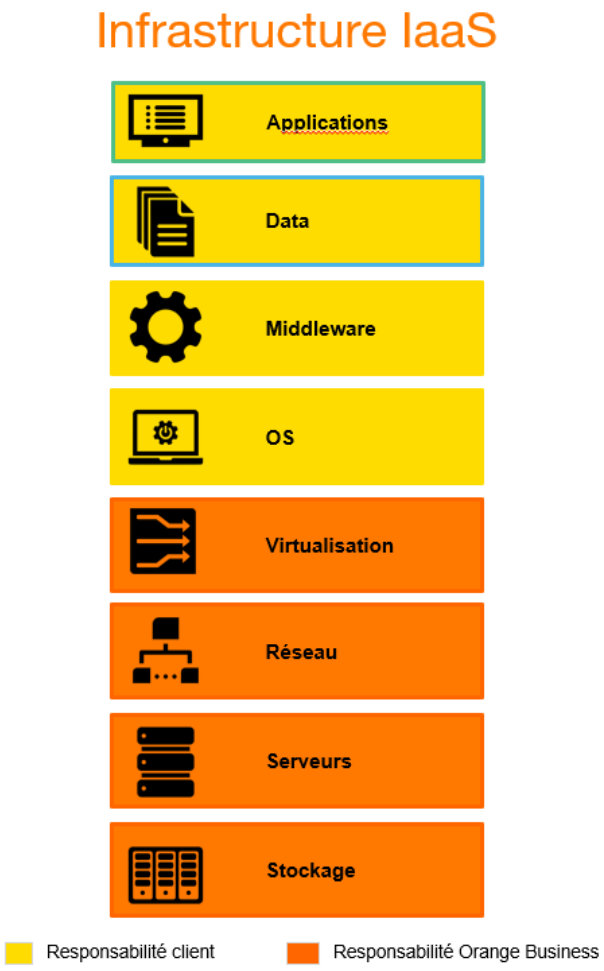

Figure 1 : Infrastructure IaaS

3.3. Gestion des actifs

3.3.1. Inventaire des actifs

La liste des actifs supports (routeurs, commutateurs, pare-feux, baies de stockage, serveurs, machines virtuelles, logiciels…) des offres Cloud est maintenue dans des outils de cartographie internes Orange. Ces outils tracent à la fois les composants de l'infrastructure de Cloud Avenue Dynamic et les composants des environnements clients (ex : Virtual Machine, pare-feux virtuels …).

Ces inventaires sont mis à jour dans le cadre du processus de gestion des changements.

3.3.2. Mesures de protection des actifs supports

Classification des ressources d'infrastructure

Les ressources d'infrastructures sont classifiées sur une échelle à 4 niveaux, définie dans la Global Security Policy d'Orange, et permettant de qualifier le préjudice pour Orange et ses clients en cas d'incident sur la ressource :

- **Niveau 4** : impact vital, enjeux très importants (voire vitaux) correspondant à des risques inadmissibles ;
- **Niveau 3** : impact critique, enjeux importants correspondant à des risques dont les effets doivent être limités ;
- **Niveau 2** : impact sensible, enjeux modérés et risques maîtrisés avec un tort limité pour l'entreprise ;
- **Niveau 1** : impact nul ou quasi-nul.

Toutes les ressources de Cloud Avenue Dynamic hébergées dans nos datacenters (routeurs, commutateurs, baies de stockage et de sauvegarde, serveurs, …) sont considérées au minimum de **niveau 3** (soit niveau 3 ou niveau 4). Les mesures associées à la protection de ces ressources critiques sont décrites tout au long de ce document.

Classification, marquage et protection de la documentation

La documentation est classifiée puis marquée, conformément aux règles internes Orange définies dans le document « Marquage des documents ». Quatre niveaux y sont définis : **diffusion libre**, **restreint Orange**, **confidentiel Orange** et **Souverain Orange.**

Les documents opérationnels des projets / offres Cloud Avenue Dynamic sont stockés sur des serveurs de fichier. L'accès est protégé par un contrôle d'accès nominatif et une gestion des droits gérée selon le principe du besoin d'en connaître.

Classification des informations clientes

La classification des informations clientes hébergées sur l'offre Cloud Avenue Dynamic est sous la responsabilité des clients.

3.3.3. Effacement des données

Protection des données clientes désallouées

Les données clients sur des ressources désallouées sont protégées contre l'accès par d'autres clients. Les produits utilisés par Orange, comme VMWARE, garantissent que, par exemple, si des ressources de stockage sont réaffectées, le nouveau client ne peut pas voir les données de l'ancien.

Suppression des données clientes en fin de contrat

En fin de contrat, l'ensemble des ressources affectées aux clients sont désallouées, et les données clientes deviennent inexploitables, comme évoqué dans le paragraphe précédent.

Seules les sauvegardes sont conservées quelques mois par Orange après la fin de contrat. Passé ce délai, Orange ne détient plus aucune donnée du client.

3.4. Contrôle d'accès

Orange assure le contrôle d'accès sur les environnements qui sont contractuellement sous sa responsabilité. Le contrôle d'accès sur les systèmes et applications managés par le client est sous sa responsabilité.

3.4.1. Contrôle d'accès pour les exploitants d'Orange

Moyens d'accès

Les exploitants d'Orange administrent l'infrastructure Cloud Avenue Dynamic (serveurs, baies de stockage, équipements réseaux, équipements de sécurité…) de la manière suivante :

Remarque : pour certaines offres, les VM clientes peuvent être managées par Orange, on parle alors d'offre managées ou co-managées. Ce mode d'administration spécifique n'est pas décrit dans ce paragraphe mais dans les spécificités de chaque offre (qui font l'Objet de white paper spécifique à ces offres).

- **1 – Accès depuis le réseau interne Orange.** L'administration de l'infrastructure Cloud n'est possible que depuis le réseau interne Orange et à partir des bastions hautement sécurisés.
- **2 – Filtrage et authentification nominative en entrée de la plateforme d'administration.** La plateforme Cloud Avenue Dynamic est protégée du réseau interne Orange par une zone de sécurité intermédiaire, appelée plateforme d'administration, laquelle héberge des serveurs de rebonds. Cette étape permet d'assurer :
  - Du filtrage réseau ;
  - De l'authentification nominative et du traçage des accès ;
  - De la journalisation des sessions sur un serveur de log centralisé ;
  - De l'autorisation : l'administrateur ne peut accéder qu'aux ressources autorisées pour son profil.
- **3 – Filtrage supplémentaire sur la plateforme Cloud.** Il s'agit d'un jeu de règles supplémentaire (pare-feu/ACL/groupes de sécurité) ajoutées à l'existant pour que seuls les accès d'administration de l'infrastructure Cloud proviennent de la plateforme d'administration.
- **4 - Authentification des exploitants sur les environnements Cloud.** L'administrateur habilité s'authentifie sur le composant qu'il souhaite administrer :
  - Authentification avec des comptes centralisés (AD, TACACS+) ou locaux ;
  - Journalisation des sessions sur un serveur de log centralisé ;

- Autorisation : l'administrateur ne peut accéder qu'aux ressources autorisées par son profil.
- Traçabilité : traçage des actions administrateurs, renouvellement automatique des mots de passe des serveurs.

Les accès d'administration sont toujours réalisés de manière sécurisée via le protocole SSL/TLS (exemples de flux : HTTPS, SSH).

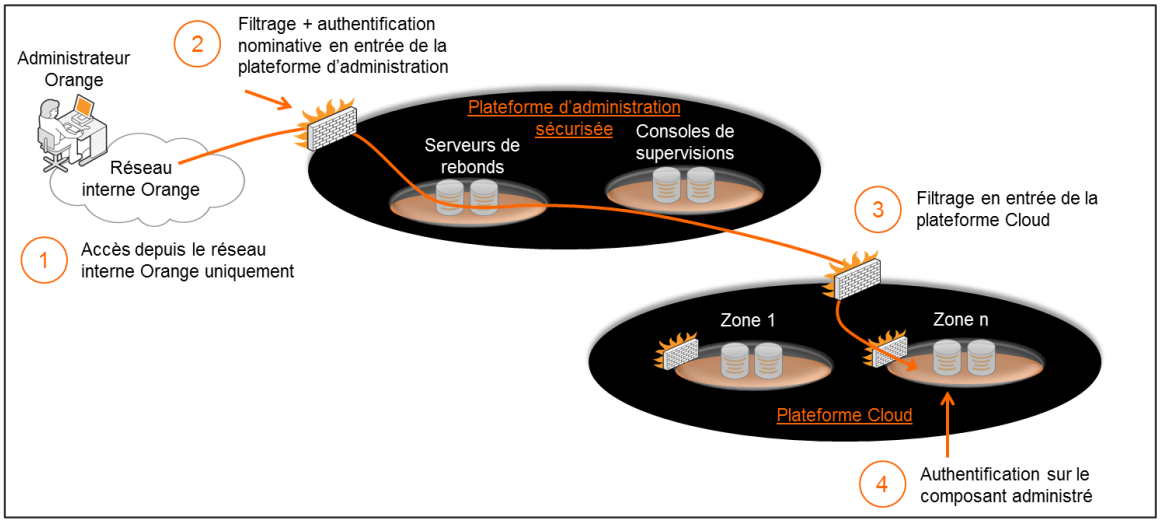

Figure 2 : Accès administration Cloud Avenue Dynamic

Authentification et gestion des mots de passe

Les connexions avec les comptes d'exploitation respectent les politiques internes de gestion de mot de passe.

Pour les personnels, un token disposant d'un certificat est fourni par le système de PKI (public key infrastructure) du groupe Orange est stocké sur ce token pour assurer une authentification multi facteurs renforcée.

Procédure d'attribution et de révocation des droits pour les exploitants d'Orange

La procédure d'attribution/révocation d'un compte et des droits associés est appliquée et contrôlée. Cette procédure est une mesure de sécurité du SMSI (Systèmes de Management de la Sécurité de l'Information) certifié ISO 27001, mis en place par Orange.

Les comptes partagés ne sont autorisés que de manière exceptionnelle sous forme de dérogation. Ils doivent être listés et justifiés.

Revue des droits pour les exploitants d'Orange

Une revue des habilitations et des droits est effectuée périodiquement et fait l'objet d'un compte rendu. L'activité consiste à extraire la liste des personnes ayant un compte opérationnel sur Cloud Avenue Dynamic. Cette liste est recoupée par manager qui va définir si le compte doit être maintenu ou non. Si le compte opérationnel n'est pas plus nécessaire il est alors supprimé. En cas de découverte de droits illégitimes, les mesures adéquates sont appliquées :

- Suspension du compte ;
- Examen des traces d'utilisation pour révéler d'éventuels incidents ;
- Prise de mesures correctrices (mise à jour des procédures, sensibilisation du management…).

3.4.2. Contrôle d'accès pour les clients d'Orange

Les clients se connectent aux environnements Cloud Avenue Dynamic à des fins d'administration ou d'accès aux services applicatifs. Les accès sont réalisés via Internet et/ou un réseau privé (VPN client) en fonction des offres et des options sélectionnées par le client.

Les accès clients sont toujours réalisés de manière sécurisée via le protocole SSL/TLS 1.3 (exemples de flux : HTTPS, SSH) :

- L'authentification serveur (portails d'administration, serveurs applicatifs) est systématiquement réalisée via un certificat X.509 « serveur » délivré par une autorité de certification reconnue.
- L'authentification client est réalisée sur la base d'un login/mot de passe transmis préalablement de manière sécurisée à chaque client. Pour certaines offres, il est possible de mettre en œuvre une authentification forte (usage de token logiciel générant un mot de passe à usage unique, usage de certificat X.509 « client »).
- Les flux réseaux sont systématiquement chiffrés selon l'état de l'art.

Le client porte la responsabilité de la sécurité des éléments d'authentification qui lui sont communiqués par Orange. Dans la mesure des possibilités offertes par les outils, Orange impose une complexité minimale sur tous les mots de passe manipulés par le client.

Pour certaines offres, le client a la possibilité de créer lui-même des comptes d'accès (profils utilisateur, administrateur). Les identifiants et les droits d'accès associés sont sous la responsabilité du client.

L'ensemble des connexions client est tracée dans des journaux d'événements (logs) qui sont archivés conformément à la législation en vigueur.

4. Mesures de sécurité applicables aux personnes

Ce chapitre correspond à la thématique 6 de l'ISO 27002 version 2022.

4.1. Maîtrise des intervenants

Une liste des intervenants sur Cloud Avenue Dynamic est maintenue à jour dans le cadre du processus de gestion des entrées/sorties. Cette liste est notamment utilisée comme référentiel pour effectuer la revue des habilitations logiques (cf. 3.4 - Contrôle d'accès). Les droits d'accès des intervenants sont modifiés/supprimés dès qu'ils changent de fonction ou qu'ils quittent la société.

4.2. Sélection des candidats

Les candidats sélectionnés à l'embauche sur la base de CV et lettre de motivation sont soumis à de multiples vérifications dans le respect de la réglementation locale de l'embauche comprenant sans s'y limiter à une vérification de la carte d'identité, la récupération des diplômes ou attestations de réussites (certifications, recommandations...).

Le contrôle des intervenants par les autorités s'effectue dans le cadre de la réglementation locale au lieu de l'embauche.

4.3. Sensibilisation

Des actions de sensibilisation à la sécurité des Systèmes d'Information ont principalement lieu au travers de formations dispensées à tout le personnel Orange.

D'autres actions sont régulièrement menées pour maintenir le niveau de sensibilité au travers messages de communication sur les bonnes pratiques de sécurité, et d'intervention d'experts sécurité dans les réunions d'équipe. En cas de menace plus imminente, des messages d'alerte sécurité sont envoyées à l'intégralité du personnel (ex : campagne de phishing).

Des sensibilisations plus spécifiques aux risques sécurité sont réalisées semestriellement sur la population des top managers, notamment aux risques légaux et réglementaires.

Un espace est mis à disposition du personnel sur le réseau social de l'entreprise pour retrouver les supports de formation, des guides spécifiques, et pour pouvoir poser des questions aux experts sur le forum.

4.4. Engagement écrit des intervenants

4.4.1. Engagement de confidentialité des intervenants

Les salariés ont une obligation générale de discrétion inscrite dans leur contrat de travail et/ou dans leur convention collective. Ci-après un extrait d'un contrat de travail Orange :

> « Article 10 : Secret professionnel et devoir de discrétion
>
> Comme l'ensemble du personnel d'Orange, Madame/Monsieur _____ est tenu(e) au secret professionnel absolu. Cette prescription s'applique pendant l'exécution et la suspension du contrat de travail ainsi qu'après sa rupture et concerne notamment les techniques mises en œuvre par Orange, ainsi que toutes études et travaux exécutés dans l'entreprise.
>
> Elle s'applique également à toute information ayant un caractère confidentiel, en particulier celles qui ne sont pas habituellement communiquées au public, que Madame/Monsieur _____ pourrait recueillir à l'occasion de ses fonctions ou du seul fait de sa présence à Orange.
>
> Le non-respect de cette prescription de secret constituerait une faute et pourrait faire l'Objet de poursuites civiles et/ou pénales. »

4.4.2. Charte de bon usage des ressources informatiques

De même, tout salarié doit, par le règlement intérieur, respecter la charte de bon usage des ressources informatiques.

4.4.3. Fin de contrat

Dans le cadre de la fin de contrat chez Orange Business, le processus est mené conformément aux politiques et procédures groupe. L'ensemble des matériels est blanchi (effacement sécurisé), tous les accès révoqués, et les données afférentes effacées de manière définitive. Les contrôles de conformité et les preuves associées (journaux de révocation, certificats d'effacement) sont dûment archivés.

4.4.4. Travail à distance

Conformément au contrat de travail et à la charte de télétravail d'Orange Business, les administrateurs comme l'ensemble des collaborateurs peuvent exercer leurs activités en télétravail, dans les limites et conditions prévues (éligibilité, quotité hebdomadaire, accord managérial, droit à la déconnexion, règles HSE). Les modalités pratiques (équipement fourni, prise en charge, support) sont définies et communiquées via les canaux officiels Orange Business.

Le télétravail est, par défaut, encadré par des règles de sécurité obligatoires : usage exclusif d'équipements gérés et chiffrés (MDM, correctifs à jour), connexion via VPN avec MFA, accès de production uniquement via bastion/PAM selon le principe du moindre privilège. Les politiques de confidentialité et de protection des données s'appliquent en tout lieu, avec verrouillage de session, environnement de travail sécurisé et obligation de signaler tout incident. Des contrôles et audits vérifient le respect de ces mesures, avec des exigences renforcées pour les fonctions sensibles (administrateurs, accès privilégiés).

5. Mesures de sécurité physique

Ce chapitre correspond à la thématique 7 de l'ISO 27002 version 2022.

La sécurité physique et environnementale vise à protéger le système d'information d'Orange et de ses clients contre :

- Les menaces environnementales et les sinistres : explosion, séisme, incendie, dégât des eaux, panne de courant, panne de la climatisation, panne télécoms…
- Les menaces d'intrusions physiques : accès en salle d'une personne non habilitée, vol de disques durs contenant des informations sensibles…

5.1. Sécurité physique et environnementale de nos centres d'hébergement

Notre offre Cloud Avenue Dynamic (infrastructures, sauvegardes…) est hébergée sur plusieurs centres d'hébergement (« datacenters »). Les sites d'hébergement de Cloud Avenue Dynamic sont Val-De-Reuil et Chartres. Le site de principal est celui de Val-De-Reuil, Chartres est le site de backup.

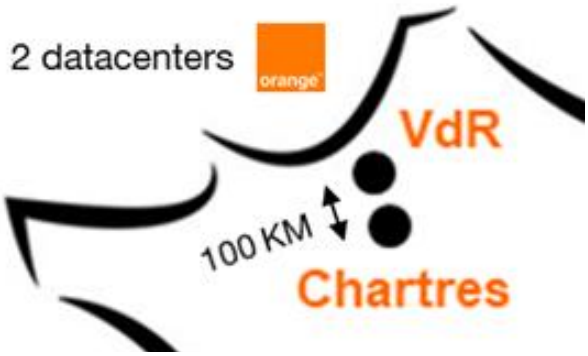

Figure 3 : Localisation des datacenters Cloud Avenue Dynamic

Les mesures de sécurité suivantes sont mises en œuvre au niveau de ces centres d'hébergement d'Orange :

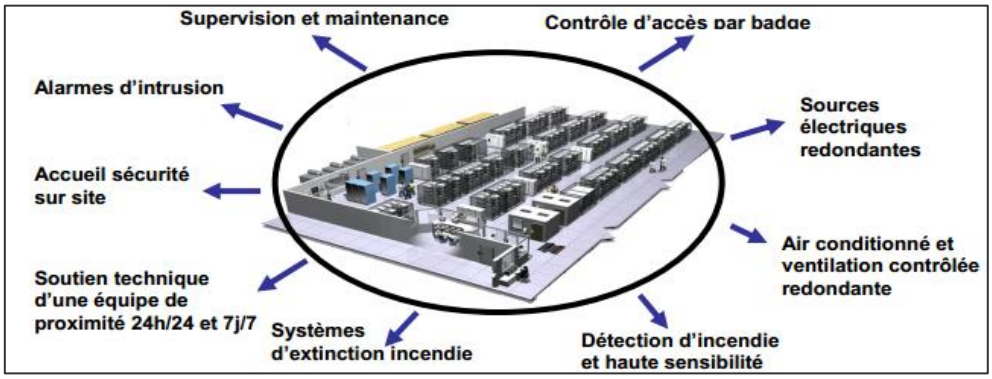

Figure 4 : Mesures de sécurité Datacenter

ISAE 3402 - Tous les centres d'hébergement mentionnés ci-dessus sont certifiés ISAE 3402 Type II (ex. SAS 70). ISAE 3402 est le standard permettant aux clients qui externalisent d'Obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de service. Depuis le 15 juin 2011, il se substitue au standard SAS 70 et est applicable aux engagements internationaux. À ce titre, des auditeurs indépendants se sont livrés à des contrôles rigoureux au cours d'une période de test de 12 mois pour valider la qualité, la fiabilité et l'intégrité des processus et contrôles opérationnels d'Orange. Ce rapport d'audit indépendant assure aux clients d'Orange Business que les services dont ils bénéficient répondent aux exigences de la loi Sarbanes-Oxley aux États-Unis et respectent des **objectifs clés de sécurité**, de gestion du changement et de continuité des services.

Classification TIER - Les datacenters de l'offre Cloud Avenue Dynamic sont construits et opérés pour satisfaire aux exigences TIER IV. Le niveau TIER IV est le niveau le plus performant de la classification TIER.

Tolérance aux pannes et à la maintenance - Les architectures techniques mises en œuvre permettent de répondre aux contraintes d'exploitation suivantes :

- Absence d'impact sur la charge lors du premier défaut.
- Grande tolérance aux pannes, jusqu'à 2 défauts majeurs sans impact.
- Absence d'interruption de service lors d'une intervention de maintenance.

Le mode de gestion et les processus mis en œuvre permettent d'assurer la sécurité des personnes, des bâtiments et des équipements hébergés.

L'architecture mise en place pour Cloud Avenue Dynamic comprend la répartition sur les 2 sites (Val-De-Reuil et Chartres) en mode actif/actif au niveau serveur. L'accès Internet pour sa part doublé en mode actif/passif sur les 2 sites.

Spécifications détaillées dans les livrets de site[1] - Les spécifications de nos centres d'hébergement sont détaillées dans des livrets de site qui abordent les thématiques suivantes :

- Energie (redondance des adductions, redondance des tableaux généraux de distribution de la basse tension, groupe électrogène d'une autonomie minimale de 72 heures, onduleurs …) ;
- Climatisation (redondance N+1, c'est-à-dire que la panne d'une climatisation n'a aucun impact sur la chaîne de production de froid) ;
- Urbanisation (allées, faux-planchers …) ;
- Protection incendie (détection, extinction, centrale de supervision, …) ;
- Protection dégâts des eaux (détection, pompes …) ;
- Protection contre les intrusions (barrières/murs de sécurité, contrôle d'accès, vidéo-surveillance, gardiens, rondes, détection d'intrusion, gestion des invités …) ;
- Organisation de la sécurité sur les sites (responsables, surveillance 24/7, réactivité, …) ;
- Sécurité de l'environnement (absence de risque naturel …).

[1] Livrets de site : ces livrets sont confidentiels, mais consultables dans les locaux d'Orange après signature d'un engagement de confidentialité.

5.2. Sécurité physique et environnementale de nos plateaux d'exploitation

Les plateaux d'exploitation sont les locaux depuis lesquels sont exploitées par Orange Business les offres Cloud Avenue Dynamic. Les différents plateaux sont :

- MSC Inde, Egypte et Pologne : support niveau 1 et niveau 2 des infrastructures supportant les offres Cloud (firewall, serveurs, réseau…) ;
- Site Orange/France : support niveau 3 de Cloud Avenue Dynamic.

Les centres d'exploitation suivants, situés à Cesson-Sévigné, en Inde en Égypte et en Pologne, disposent d'une certification de sécurité ISO 27001 délivrée par l'AFNOR, dont l'adresse des sites est indiquée sur les certificats. Le périmètre fonctionnel de la certification est la mise en œuvre, la fourniture et le support de services infogérés et de solutions de communication.

Dans le cadre de la fourniture des services cloud, Orange Business peut avoir à transférer des données du client en dehors de l'Union Européenne vers les MSCs mentionnés ci-dessus. Au sein du groupe, un "Agreement for the transfer of customer personal data" est en vigueur depuis le 2 janvier 2013. Selon cet « Agreement », les données personnelles que les clients (en tant que responsables de traitement) transfèrent à Orange Business (en tant que sous-traitant ou sous-traitant ultérieur) bénéficient d'un niveau de protection adéquat tel qu'exigé par la Commission Européenne. Chaque entité légale d'Orange Business située en dehors de l'Union Européenne dans un pays n'assurant pas un niveau de protection adéquat tel qu'exigé par la Commission Européenne, s'est engagée, en signant cet « Agreement », à respecter la Directive Européenne 95/46/EC, et a ainsi accepté d'être liée par les clauses standards de la Commission Européenne.

6. Mesures de sécurité technologiques

Ce chapitre correspond à la thématique 8 de l'ISO 27002 version 2022.

6.1. Cryptographie

Suites cryptographiques - Toutes les suites cryptographiques utilisées sur les offres Cloud Avenue Dynamic (ex : AES 256, SHA-256, TLS 1.3) sont basées sur les standards du marché dont le niveau de sécurité est éprouvé. L'étude technique de l'ENISA[2], « Algorithms, Key Size and Parameters Report, 2013 Recommendations » a en particulier été prise en compte pour choisir les suites cryptographiques. Les flux d'administration sont systématiquement chiffrés en utilisant le protocole SSL/TLS.

Gestion des certificats – Les certificats d'authentification des serveurs se basent sur des autorités de certifications (ex : VeriSign, Thawte…) reconnues par les principaux navigateurs Web. Les certificats d'authentification pour nos services d'administration internes (accessibles uniquement par les exploitants Orange) peuvent se baser sur des certificats X.509 générés par l'autorité PKI de certification interne d'Orange.

Chiffrement des disques durs des exploitants Orange – Pour la sécurisation des données sensibles, les exploitants Orange disposent d'une solution de chiffrement supplémentaire avec authentification par token (ZoneCentral de Prim'X). Cette solution a été certifiée EAL3+ sur sa version 3.1 par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

KMS : Une cérémonie des clés a été menée sur Cloud Avenue Dynamic conformément à notre politique de gestion cryptographique et aux bonnes pratiques ISO/IEC 27001 (gestion des clés). Cela inclue un pilotage par la sécurité avec séparation des rôles et double contrôle, la génération et l'initialisation des clés dans un HSM certifié, une traçabilité complète (charte d'engagement signée, liste de présence, enregistrement et numéros de scellés), des vérifications techniques réussies (KCV, tests de chiffrement/déchiffrement), ainsi que la mise en place d'un cycle de vie maîtrisé (ex. rotation planifiée et procédures de révocation).

[2] ENISA : European Network and Information Systems Agency

6.2. Sécurité opérationnelle

6.2.1. Gestion des procédures opérationnelles

Certification ISO 20000 et ITIL

La gestion des services par Orange Business est certifiée ISO 20000[3]. Les exigences de la certification ISO 20000 sont alignées avec les meilleures pratiques de la dernière version d'ITIL (v4 2019) pour les processus tels que la fourniture des services, la gestion des relations, la résolution de problèmes, le contrôle et la mise en production, les exigences de sécurité renforcées.

Gestion des changements

La gestion des changements est réalisée selon le modèle ITILv4 ; cela concerne notamment les changements relatifs à la sécurité. La gestion des changements est opérée sous la responsabilité d'un « change manager ».

- Les changements « standards », c'est-à-dire pré-identifiés dans un catalogue, suivent un processus simplifié, et ne nécessitent pas une étude préalable par un expert sécurité.
- Les changements identifiés comme étant "non-standard" (évolutions) sont formalisés dans des RFC (Request For Change) avec un passage en réunion CAB (Change Advisory Board). Les RFC font l'Objet d'une étude sécurité préalable par un expert sécurité du « Centre de Compétence Sécurité Cloud » qui donne son avis sur celle-ci. La sécurité est donc représentée au CAB ; elle a autorité pour interdire un changement jugé dangereux ou non conforme à la politique de sécurité, et elle peut le faire en toute indépendance.
  Les CAB ont lieu de manière hebdomadaire. Pour des changements à caractère urgent (exemple : mise à jour de sécurité critique), il est possible de traiter immédiatement la demande de changement dans le cadre d'une réunion ECAB (Emergency Change Advisory Board).

La gestion des changements mis en œuvre par Orange Business permet ainsi de :

- Minimiser l'impact des changements sur les services opérationnels et utilisateurs ;
- Disposer de méthodes standardisées, procédures et mécanismes de contrôle ;
- Identifier les interlocuteurs habilités à demander un changement ;
- Contrôler les changements afin qu'ils correspondent à la politique de sécurité ;
- Formaliser l'évaluation correcte de l'impact, la priorité, les avantages et le risque d'un changement ;
- Définir des catégories de changements et de temps d'implémentation associés ;
- Gérer les priorités des changements en fonction des risques et impacts ;
- Améliorer la qualité de l'information et de la communication :
  - Assurer que toutes les parties concernées ont été impliquées pour limiter les incidents liés aux changements ;
  - Alimenter la base de données de configuration en informations correctes ;
  - Faire en sorte que tous les changements soient documentés ;
  - Communiquer proactivement les indisponibilités planifiées aux utilisateurs/clients.

[3] Certificat associé : https://certificats-attestations.afnor.org/certification=335171233155

Gestion des capacités

La gestion des capacités est réalisée selon le modèle ITILv4 sous la responsabilité d'un « capacity manager ». L'objectif est d'assurer un niveau de service constant pour les clients. La gestion des capacités permet d'anticiper les futurs besoins des clients en analysant les mesures et les tendances de consommations sur les ressources composant l'infrastructure Cloud.

La gestion des capacités surveille et agit principalement sur :

- Les ressources CPU/RAM ;
- Les ressources réseaux (bande passante, espace d'adressage) ;
- Les ressources stockage et sauvegarde ;
- Les licences logicielles.

Pour Cloud Avenue Dynamic, le « capacity manager » établit régulièrement des statistiques avec différents indicateurs (mesures techniques, prévisions commerciales).

6.2.2. Protection contre les codes malveillants

Environnement client

L'offre Cloud Avenue Dynamic inclut un service antivirus dédié (Trend Micro) pour les environnements client (si le client a déjà son propre anti-virus, il n'est pas nécessaire de l'installer).

L'agent antivirus installé sur les systèmes met à jour ses composants toutes les heures (version de l'agent, la base de signature virale pour la détection des menaces en temps réel, l'analyse comportementale des fichiers, l'inspection mémoire, etc.) auprès d'un serveur de mise à jour spécifique situé dans une zone de sécurité dédiée aux mises à jour des machines des clients. Ce serveur de base de signature antivirus est lui-même mis à jour en temps-réel sur des serveurs publics mis à disposition sur internet par l'éditeur de la solution antivirus.

6.2.3. Gestion des sauvegardes

Environnement client

Les données des environnements clients sont sauvegardées selon la politique de sauvegarde Cloud Avenue Dynamic et en fonction des options sélectionnées par le client. De manière générale, les données clients sont sauvegardées automatiquement et de manière périodique avec une durée rétention qui dépend des offres.

Les sauvegardes peuvent être de différentes natures en fonctions des offres et des options. Exemple :

- Sauvegarde en mode fichier (« file level »), notamment pour les données applicatives ;
- Sauvegarde en mode image (« image level ») pour les machines virtuelles ;
- Sauvegarde de données brutes (serveur de fichiers).

Les modalités de restauration varient selon les offres :

- Restauration réalisée par le client de manière autonome ;
- Restauration réalisée par Orange Business sur demande de changement via le portail d'administration.

Infrastructure Orange Business

Toutes les configurations des équipements des infrastructures Cloud Avenue Dynamic sont sauvegardées régulièrement. Cela concerne notamment :

- Les serveurs : Windows, Linux, données applicatives (notamment les bases de données) ;
- Les équipements réseau (routeurs, switchs) ;
- Les équipements de sécurité (UTM firewall, Appliance VPN) ;
- Les équipements de stockage.

Pour les configurations statiques, les sauvegardes sont réalisées à chaque évolution de configuration. L'opération de sauvegarde est encadrée par le processus de gestion des changements.

Pour les configurations dynamiques, des agents réalisent des sauvegardes automatiques de manière périodique. La rétention des données de configuration est à minima de 14 jours (plusieurs versions de sauvegardes sont conservées).

Toutes les sauvegardes de configuration sont stockées sur des sites tiers (datacenters distincts) afin de garantir la disponibilité des données de configuration en cas de sinistre majeur sur le site de production. Les sauvegardes sont stockées de manière sécurisée (cloisonnement logique) en fonction du besoin d'en connaitre.

6.2.4. Journalisation et supervision sécurité

Orange assure une supervision systématique de ses infrastructures et services Cloud, notamment d'un point de vue sécurité. Une journalisation des évènements (logs) est mise en œuvre sur l'ensemble des composants, notamment les composants sécurité. Cette journalisation a plusieurs objectifs :

- Détecter et analyser les incidents de sécurité ;
- Répondre aux obligations légales ;
- Permettre le troubleshooting.

Tous les composants sont supervisés en 24/7 et des astreintes sont mises en place pour intervenir sur des incidents critiques, notamment lorsque la sécurité est impactée.

Nature des logs sécurité

Les évènements journalisés sont définis composant par composant, selon deux critères :

- Les exigences légales : En France, la LCEN[4] et CPCE[5].
- Les exigences de sécurité :
  - Évènements liés aux activités d'administration pour l'ensemble des composants ;
  - Évènements des composants de sécurité (exemple : les logs firewall).

En France, la journalisation et la supervision des journaux sont réalisées en respectant la Loi Informatique et Libertés.

[4] LCEN : Loi pour la Confiance dans l'Economie Numérique
[5] CPCE : Code des Postes et des Communications Electroniques

Centralisation des logs sécurité

Tous les composants des infrastructures Cloud remontent leurs logs périodiquement ou en temps réel sur des serveurs de collecte situés dans des zones de sécurité spécifiques. Les logs sécurité sont protégés en intégrité et uniquement accessibles par les administrateurs en charge de la sécurité. La rétention des logs est de 3 mois par défaut (troubleshooting et sécurité) et d'un an pour les logs légaux.

Référence unique de temps

L'horodatage des logs, notamment les logs sécurité, est réalisé avec une référence de temps unique pour tous les composants de Cloud Avenue Dynamic. Le service de temps est fourni par différents serveurs NTP installés dans des zones de sécurité spécifiques. La référence de temps est fournie par un serveur physique dédié (serveur racine avec antenne GPS) installé dans les zones de services internes d'Orange Business.

Consultation des logs par le client

Dans Cloud Avenue Dynamic, le client a la possibilité d'accéder aux logs de son environnement, notamment les logs des applicatifs et firewalls. Les accès aux logs sont sécurisés et restreints à chaque environnement client.

6.2.5. Gestion des vulnérabilités techniques

La gestion des vulnérabilités a pour principal objectif le maintien en condition de sécurité des infrastructures et des services de Cloud Avenue Dynamic. Les vulnérabilités sont identifiées dans le cadre d'une veille sécurité et de scans de vulnérabilités. Elles sont ensuite qualifiées avec un correctif à déployer en production.

La veille sécurité, le suivi du déploiement des correctifs et le reporting sont la responsabilité des « Responsables Sécurité Opérations » et du « BSO ».

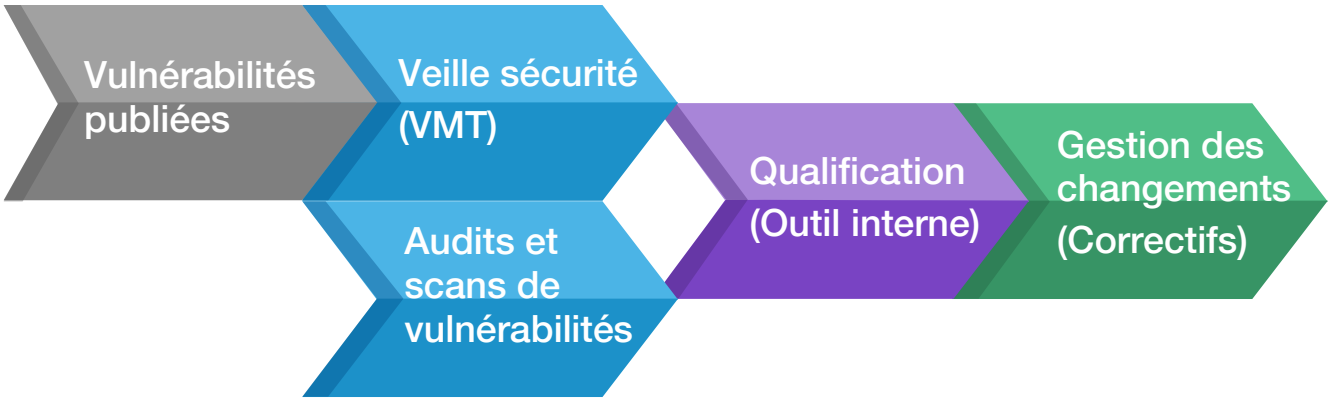

Figure 5 : Gestion des vulnérabilités

Veille sécurité

L'ensemble des composants fait l'objet d'une veille sécurité permanente qui a pour but d'identifier les vulnérabilités techniques pouvant impacter la sécurité des infrastructures et des services de Cloud Avenue Dynamic.

La veille sécurité est alimentée par différents canaux :

- Les bulletins sécurité des éditeurs de produits (hyperviseur de virtualisation, équipements réseau et sécurité, OS…) ;
- Les rapports de veille : VMT, CVE, NIST NVD, CERT-FR … ;
- Les remontées des clients ;
- Les remontées de nos audits et de nos scans de vulnérabilités.

Audits et scans de vulnérabilités

Des audits réguliers (ou permanents sur les infrastructures les plus critiques) sont lancés sur nos plateformes de production pour à la fois mesurer l'état des vulnérabilités de nos plateformes et potentiellement identifier des vulnérabilités n'ayant pas été analysées par la veille. Pour cela, Orange utilise des solutions de tiers leaders sur le marché des scans de vulnérabilités.

Des tests d'intrusion indépendants sont réalisés systématiquement avant chaque mise en production des nouvelles fonctionnalités de Cloud Avenue Dynamic, et les évolutions majeures des fonctionnalités existantes sont également pentestées afin de rester conformes aux exigences de sécurité. Lorsqu'une vulnérabilité critique est identifiée, un processus de contre-pentest est déclenché après remédiation pour valider l'efficacité des correctifs et l'absence de régression. Le BSO est responsable du suivi de la correction des vulnérabilités, jusqu'à la clôture sur preuve.

Mise à jour des VMWare Tools :

Dans le cadre du modèle de responsabilité partagée, **la mise à jour des VMware Tools incombe exclusivement au client**. Tout défaut d'application de correctifs ou de mises à jour pouvant exposer des vulnérabilités **demeure sous sa responsabilité**. En conséquence, Orange Business ne saurait être tenue responsable des incidents, compromissions ou attaques exploitant une telle vulnérabilité au sein des environnements du client. En cas d'impact sur les services d'Orange Business ou sur ceux d'autres clients imputables à ce défaut de mise à jour, **des mesures de remédiation** (ex. isolation des VMs) **et des pénalités financières** pourront être appliquées au client, conformément aux conditions contractuelles et aux SLA en vigueur.

Reporting

Le BSO réalise un reporting mensuel interne de la veille sécurité et des vulnérabilités traitées sur la période. Ce dernier est ensuite présenté lors des COSEC et n'est pas transmis aux clients pour des raisons de confidentialité.

En cas de vulnérabilité critique et susceptible d'impacter fortement ses clients, Orange Business communique directement avec ses clients à des fins d'information.

6.3. Sécurité des communications

6.3.1. Sécurité des architectures Cloud Orange

Principes généraux

Les architectures des différentes zones de Cloud Avenue Dynamic sont validées par un responsable sécurité Ingénierie placé sous la gouvernance du Chief Security, Risk and Compliance Officer. Ce dernier est garant de la cohérence des différentes architectures d'un point de vue sécurité.

Cette démarche basée sur un modèle prédéfini d'architecture offre plusieurs avantages :

- Simplification de la mise en œuvre d'une nouvelle offre Cloud ;
- Homogénéité des pratiques et des architectures entre les différentes offres ;
- Mutualisation de certains équipements ;
- Garantie sur la sécurité des offres : les modèles sont validés puis leur mise en œuvre est contrôlée par le Centre de Compétence Sécurité Cloud. Le niveau de sécurité de chaque nouvelle offre est également évalué par des audits et des tests d'intrusions avant toute mise en production. Il en est de même pour toute évolution majeure. Les résultats des audits et des tests d'intrusions internes ne sont pas diffusés aux clients pour des raisons de confidentialité ;
- Simplification du maintien en condition de sécurité.

Une analyse de risque systématique à chaque nouvelle offre complète la validation sécurité de l'architecture. Ces 2 actions constituent les bases de la démarche « Security By Design » garantissant la prise en compte de la sécurité dans le design des offres.

Domaines de confiance et Zones de sécurité

L'architecture de Cloud Avenue Dynamic applique le même modèle consistant à séparer les domaines de confiances, notamment le Back-end (interne Orange) et le Front End qui supporte les services Cloud exposés aux clients. Le cloisonnement back-end/front-end est physique, c'est-à-dire que des serveurs sont dédiés au back-end et d'autres dédiés au front-end.

Au sein de chaque domaine de confiance, des zones de sécurité assurent un cloisonnement logique par la mise en œuvre de certaines fonctionnalités telles que :

- La virtualisation (machines virtuelles, firewall virtuels, Load-balancer virtuels, routeurs virtuels/VRF) ;
- Les VLAN (802.1Q) ;
- Les réseaux virtuels VPN (IPSec, SSL) ;
- Le stockage virtuel (disques virtuels).

Ce cloisonnement logique garantit notamment l'isolation des différents environnements client.

Les communications entre les différentes zones de sécurité sont systématiquement contrôlées. La configuration locale des différents composants est également réalisée de manière à renforcer le cloisonnement et la sécurité.

Infrastructure Orange Business

Les serveurs d'infrastructure sont regroupés par zones de sécurité selon leur fonction (serveur d'administration, serveur frontal utilisé par les clients), leur nature (base de données, serveurs web) et leur niveau d'exposition (par exemple accessible ou non par les clients). Ainsi, des zones de sécurité sont dédiées aux outils d'exploitation d'Orange Business.

De manière générale, tous les serveurs disposent d'une interface dédiée aux flux de données et d'une interface technique dédiée aux flux de service (administration notamment).

Tous les composants des infrastructures cloud (serveurs, firewall, routeurs, baies de stockage…) sont configurés sur la base de guides de configuration sécurisés (guidelines) établis par les différentes ingénieries avec le concours d'experts sécurité du groupe Orange Business.

Environnements clients

L'isolation entre les environnements clients est basée sur les fonctions de virtualisation décrites précédemment. Au sein de Cloud Avenue Dynamic, le client a la possibilité de gérer des fonctions de sécurité (firewall virtuel notamment). Les fonctions fournies aux clients varient selon les options sélectionnées.

Tous les détails concernant les environnements clients, les documents contractuels ou les certificats de la plateforme sont répertorié suivant ce lien.

6.3.2. Sécurité des échanges

Sécurité des flux internes Orange

Les moyens suivants sont mis en place pour sécuriser les échanges internes Orange :

- Réseaux : Les réseaux d'interconnexion entre les plateformes Cloud et les plateaux d'exploitation sont protégés par une ou plusieurs des solutions suivantes :
  - VPN MPLS ;
  - Tunnels chiffrés (IPSec, TLS) ;
  - Réseau de fibres dédié.
- Messagerie : A la demande des clients, les échanges de données sensibles effectués par mail entre les clients et Ob peuvent être chiffrés par un outil tiers convenu avec le client (ex : Orange recommande zed).
- Flux d'administration : Les flux d'administration sont protégés conformément à l'état de l'art avec des connexions de type SSL/TLS (SSH, HTTPS).

Les échanges entre les différentes zones de sécurité sont systématiquement contrôlés par des firewalls appliquant le principe élémentaire « tout ce qui n'est pas explicitement autorisé est interdit ».

Sécurité des flux client

Les clients se connectent aux environnements Cloud Avenue Dynamic à des fins d'administration ou d'accès aux services. Les flux d'administration des clients sont systématiquement sécurisés par des protocoles garantissant l'authentification, la confidentialité et l'intégrité (TLS, AES256…). Les méthodes d'accès varient selon les options sélectionnées par le client.

Les échanges sont sécurisés avec des connexions de type SSL/TLS qui respectent l'état de l'art du moment.

6.3.3. Protection contre les dénis de service et les intrusions

Orange Business dispose de protections pour protéger ses clients contre les attaques de type « déni de service » :

- **Sondes anti DDOS déployées au cœur du réseau du Groupe Orange**
  Cloud Avenue Dynamic bénéficie du système de protection avancée « CleanPipe » contre les attaques massives en déni de service provenant d'Internet. Ce système est déclenché par le Security Operating Center (SOC) d'Orange en s'appuyant sur des sondes déployées en cœur du réseau opérateur du Groupe Orange.

- **Pare-feux situés à l'entrée des plateformes Cloud Orange**
  Le trafic en entrée de plate-forme est supervisé par des pare-feux qui filtrent certains paquets jugés suspects par simple analyse protocolaire.

6.4. Acquisition, développement et maintenance des systèmes d'information

6.4.1. Analyse de risques

L'analyse de risques EBIOS RM est la base du système de gestion de la sécurité de Global Delivery & Operations. Le principe de fonctionnement de ces dernières est détaillé ci-dessous :

- Analyse de risques annuelle du système de management de la sécurité (SMSI) : dans le cadre de la certification ISO27001, une analyse de risque globale des principaux services, processus et outils de Global Platforms and Services est réalisée, avec un plan de traitement de risque validé par le directeur général de Global Platforms and Services ;
- Analyse de risques « haut-niveau » (HLRA : High-Level Risk Analysis) avant chaque démarrage de nouveau service/solution : cette analyse de risques permet d'évaluer les principaux risques (données personnelles, etc.) et orienter en amont les équipes projet vers des solutions sécurisées ;
- Analyse de risques de sécurité (Security Risk Analysis) : selon les résultats du HLRA, une analyse de risque complète de sécurité est menée ou non. Cette analyse de risque permet d'identifier les risques liés à l'architecture, au modèle opérationnel et à l'organisation ;
- Analyse de risques dans le cas d'une « due diligence » : vérification de la sécurité d'un fournisseur de solution ou de sous-traitance, voire en cas d'acquisition de société.

Les analyses de risques proposent systématiquement des mesures de sécurité à mettre en place pour limiter les risques identifiés. Ces documents ne sont pas transmis aux clients pour des raisons de confidentialité.

6.4.2. Bonnes pratiques de développement et d'intégration

Cloud Avenue Dynamic applique systématiquement le processus de sécurité dès la conception à tout nouveau composant et à toute évolution majeure.

Bonnes pratiques de développement

Les développements spécifiques réalisés par Orange Business ou par un sous-traitant respectent le guide interne Orange de bonnes pratiques de développement sécurisé.

Bonnes pratiques d'intégration / renforcement de la sécurité des configurations

Les systèmes et logiciels sous la responsabilité d'Orange Business sont configurés avec un niveau de sécurité renforcé par l'application d'un « guide de hardening ». Par exemple pour les environnements VMware vSphere, Orange Business se base sur les guides de hardening sécurité fournis par VMware (https://www.vmware.com/security/hardening-guides.html).

Certification sécurité des composants critiques

Le Centre de Compétence Sécurité Cloud d'Orange Business veille à ce que les composants critiques aient des certifications de sécurité reconnues sur un périmètre approprié avant d'être intégrés dans nos offres Cloud. Ainsi, le Centre de Compétence Sécurité Cloud s'appuie généralement sur les certifications « Critères Communs » (ISO 15408) et vérifie leur pertinence en contrôlant les paramètres suivants :

- Niveau d'assurance : EAL4 souhaité au minimum.

- Cible de sécurité couvrant des domaines fonctionnels suffisamment larges : support cryptographique, identification et authentification, étanchéité des machines virtuelles...

A titre d'exemple, les composants critiques suivants sont certifiés critères communs :

- VMWare: https://www.vmware.com/fr/security/certifications/common-criteria.html
- Pare-feu Juniper : EAL4.

6.4.3. Recette de sécurité

Validation sécurité des composants

Les composants les plus critiques de la plateforme de Cloud Avenue Dynamic font l'objet de tests de sécurité (revue de configuration/code et/ou tests d'intrusion) afin de valider leur niveau de sécurité.

A titre d'exemple, les portails d'administration ont déjà fait plusieurs fois l'objet de plusieurs tests d'intrusion et d'une revue de configuration/code.

Tous les templates (OS ou applicatifs) fournis par Orange Business font également l'objet d'une validation et sont régulièrement testés et mis à jour pour prendre en compte les dernières vulnérabilités et patchs.

Plateforme de non-production

Des plateformes de développement/qualification/préproduction existent, notamment pour valider la sécurité des évolutions ou pour mener des audits complets d'intrusion.

En cas de déploiement de patch ou de nouveaux services, ces derniers suivent le processus de sécurité by design et sont testés sur ces plateformes de non-production afin de valider le bon fonctionnement et les non-régressions du patchs et/ou des nouveaux services.

Absence de données clientes sur les plateformes de non-production

Aucune donnée cliente n'est présente sur les plateformes de non-production qui sont complètement disjointes des plates-formes de production.

6.5. Gestion des sous-traitants

6.5.1. Sécurité dans les contrats avec nos sous-traitants

Dans le cadre du référencement, Orange Business évalue la gestion de la sécurité de ses principaux fournisseurs avec notamment la fourniture d'un plan d'assurance sécurité détaillant les mesures prises par l'entreprise pour garantir la sécurité de la prestation réalisée pour Orange Business.

L'acceptation des équipes de la sécurité interne fait partie des prérequis au référencement.

Nos prestataires/fournisseurs s'engagent dans nos contrats sur la confidentialité et l'intégrité des données qu'ils auront à leur connaissance durant la prestation.

Les sous-traitants intégrés aux équipes internes Orange Business utilisent les mêmes outils et processus que les personnels Orange Business, et respectent donc par défaut les bonnes pratiques explicitées dans ce document : sensibilisation, contrôle d'accès physique et logiques …

6.5.2. Suivi de la sécurité des services fournis par nos sous-traitants

Orange Business prévoit la possibilité d'auditer ses sous-traitants afin de vérifier le respect des engagements sécurité prévus dans les contrats. Ces audits débouchent sur des plans d'actions sécurité permettant d'améliorer le niveau de sécurité des sous-traitants.

6.6. Gestion des incidents de sécurité

La politique de gestion des incidents de sécurité est décrite dans la politique de sécurité Orange Business.

Préparation des équipes opérationnelles

Cette phase a pour but de préparer chaque intervenant au traitement des incidents : excellence opérationnelle (sensibilisation, entrainements réguliers à la gestion des différents types d'incidents…) et accès rapide à une documentation à jour (inventaire des actifs, schéma réseau, documentation technique, journaux…).

Lors de cette préparation, les opérationnels sont sensibilisés à l'identification d'incidents de sécurité potentiels. Le principe est que lorsqu'un incident opérationnel est identifié alors l'opérationnel en charge puisse identifier de manière raisonnable si l'incident peut entrainer un problème de sécurité (typiquement si un système de protection tombe en panne) ou si l'origine de l'incident peut être liée à la sécurité (malware, botnet, tentative d'intrusion, déni de service ...).

Détection des incidents de sécurité

Les moyens de détection mis en œuvre pour détecter un incident de sécurité sont :

- Outils de supervision standards (Patrol, Zabbix) ou spécifiques à la sécurité (SIEM[6], sondes anti-DDOS) ;
- Personnel en charge de la supervision des journaux (IDS, log FW, log systèmes, log applicatifs…) ;
- Cellule de veille ;
- Equipe sécurité (ex : Centre de Compétence Sécurité Cloud) ;
- Alertes remontées par le client.

Cette supervision s'effectue sur les composants sous la responsabilité directe d'Orange Business (portail, hyperviseur, environnements clients dont la sécurité est managée par Orange Business…).

Enregistrement et qualification des incidents de sécurité

Orange Business dispose d'un outil de gestion des incidents de sécurité.

Les alertes sont saisies dans l'outil sous forme d'un ticket d'incident par deux types d'acteurs :

- Les acteurs techniques en charge de l'exploitation / supervision du service ;
- Les acteurs du centre de support, alertés par un appel ou un mail du client.

Les alertes sont qualifiées selon leur nature et leur gravité.

[6] SIEM : Security Information Event Management, outil permettant de corréler les logs, c'est-à-dire de relier des évènements différents à une même cause.

Nature de l'incident - L'outil de gestion des incidents distingue quatre catégories d'incidents :

- Intrusion ;
- Dysfonctionnement ;
- Vulnérabilité ;
- Légal (incident de nature réglementaire faisant intervenir des acteurs particuliers).

Gravité de l'incident - Le tableau ci-dessous synthétise les niveaux de gravité des incidents ainsi que les actions à mener :

Niveau	Description
1	**Critique** Perte complète des services pour plusieurs utilisateurs, ou incident ayant un impact critique sur les activités du client. Nécessite une prise en compte immédiate et la mise à disposition en urgence de ressources dédiées jusqu'à résolution de l'incident.
2	**Majeur** Services dégradés. Les utilisateurs peuvent accéder aux services mais connaissent des difficultés ou subissent des délais significatifs. Nécessite une prise en compte immédiate et la mise à disposition de ressources pour une résolution rapide de l'incident.
3	**Mineur** Services fournis avec des délais ou des difficultés mineurs. L'activité de l'entreprise n'est pas significativement entravée. Nécessite une prise en compte programmée pour éviter toute dégradation significative du service.

Réponse à l'incident de sécurité

Les réponses suivantes peuvent être apportées :

- Mesures d'urgence (mise en quarantaine, …) ;
- Activation de la cellule de crise ;
- Communications aux clients, aux partenaires, aux exploitants ;
- Application d'un correctif ;
- Restauration d'un système ;
- …

Revue et actions post-incident

Une fois l'incident de sécurité traité, le Centre de Compétence Sécurité Cloud analyse la nature de l'incident et la qualité de la réponse apportée par Orange Business. Si besoin, le Centre de Compétence Sécurité Cloud met à jour les procédures de gestion des incidents de sécurité dans une démarche d'amélioration continue.

Communication vers les clients

Pour les incidents ayant pu avoir un impact sur la sécurité des clients d'Orange Business, une communication est faite vers les clients selon les modalités prévues au contrat. Pour les clients ayant opté pour un Business Security Officer dédié, la communication se fera directement vers le RSSI du client.

6.7. Sécurité de la gestion de la continuité d'activité

Les taux de disponibilité sont précisés dans les descriptions de services.

Toutes nos offres Cloud ont leur infrastructure entièrement redondée sur plusieurs sites (ou par exception temporaire sur plusieurs salles informatiques), avec des mécanismes de haute disponibilité de manière à rendre transparent les pannes locales : réseau (accès Internet, accès VPN, pare-feu), portail d'administration, virtualisation, stockage…

Toutes les sauvegardes (configuration, sauvegardes clients) sont répliquées sur des sites distants afin de garantir la disponibilité des données en cas de sinistre majeur sur le site de production.

Les offres Cloud Avenue Dynamic sont exploitées depuis plusieurs plateaux d'exploitation. Ainsi, en cas d'indisponibilité total d'un site d'exploitation, la continuité de l'administration des offres Cloud Avenue Dynamic est assurée.

La continuité de l'exploitation est régulièrement testée au travers de simulations.

Des clauses de réversibilité sont présentes dans les contrats des offres Cloud Avenue Dynamic. En cas de résiliation du Service, à l'exception de la résiliation pour faute du Client, le Client pourra demander à Orange Business le déclenchement de la réversibilité et mettra alors en œuvre les moyens raisonnablement nécessaires pour assurer la continuité du Service, afin que le client dispose, à l'issue de la Période de Réversibilité, des capacités lui permettant de continuer à satisfaire ses besoins (cf. contrat plus de détails).

6.8. Conformité

6.8.1. Respect des exigences légales et contractuelle

Dans le cadre de la démarche d'analyse de risques propre à tout projet d'Orange Business, une revue des obligations légales et contractuelles est effectuée et un plan d'action est proposé. Le livrable produit s'appelle le LOA (Legal Obligation Assessment). Les points abordés sont :

- Le respect des clauses contractuelles (licences, propriétés industrielles, engagements spécifiés dans la description de service…) ;
- Le respect des réglementations spécifiques issues du domaine d'activité d'Orange Business (LCEN[7] et CPCE[8]) ;
- La tenue d'un registre des traitements de données à caractère personnel, conformément au Règlement général sur la protection des données (RGPD). Orange Business Services a nommé un DPO (Data Protection Officer, ou délégué à la protection des données) qui assure la tenue du registre. Le DPO est un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable des traitements de ces données, que dans les rapports de ce dernier avec la CNIL (Commission Nationale de l'Informatique et des Libertés), autorité administrative indépendante chargée de veiller au respect du RGPD. Le DPO occupe ainsi une place centrale dans le développement sécurisé des nouvelles technologies de l'information et de la communication et assure, au sein de l'entreprise, la diffusion

[7] LCEN : Loi pour la Confiance dans l'Economie Numérique
[8] CPCE : Code des Postes et des Communications Electroniques

de la culture informatique et libertés et la maîtrise des risques sur les données à caractère personnel.

Toujours dans ce même cadre d'analyse de risques, une revue des données personnelles est proposée. Le livrable produit s'appelle le PRA (Privacy Risk Assessment).

6.8.2. Contrôle du respect des politiques de sécurité

Le Centre de Compétence Sécurité Cloud a la charge de contrôler l'application de la Politique de Sécurité pour chaque offre Cloud. Il réalise donc un contrôle continu et pilote des audits organisationnels et techniques périodiquement.

- Exemple d'audit organisationnel : contrôle de la gestion des habilitations ;
- Exemple d'audit technique : tests d'intrusions, réalisation de scan Nessus ou Qualys, audit de configuration…

En complément, Orange Business est soumis à des audits réguliers (AFNOR, ISAE 3402) réalisés par des organismes externes et menant à des contrôles du niveau de sécurité.

6.8.3. Certifications liées à la sécurité

Orange Business possède les certifications suivantes adhérentes au périmètre des offres Cloud :

- ISAE 3402 pour les centres d'hébergement
  - Les centres d'hébergement d'Orange sont certifiés ISAE 3402 Type II (ex SAS70).
- Certification sécurité ISO 27001
  - Orange Business possède une certification sécurité ISO 27001 sur le périmètre de la « mise en œuvre, la fourniture et le support de services en infogérance et de solutions de communications » pour les sites de Cesson-Sévigné, d'Egypte, de l'île Maurice, d'Inde et de Pologne[9].
- Certification SOC1 et SOC2
- Certification ISO 27017
- Certification ISO 27018
- Certification ISO 9001
- Certification ISO 14001
- Certification ISO 20000-1
- Certification CISPE (Cloud Infrastructure Service Providers Europe – Protection des données)
- Certification Critères Communs EAL 2+ (ISO 15408) sur la sécurité du réseau international IP-VPN en 2008
- Certification Critères Communs (ISO 15408) des équipements de sécurité et les équipements de virtualisation utilisés sur nos offres :
  - VMWare : https://www.vmware.com/security/certifications/common-criteria.html
  - Pare-feu Juniper : EAL4.

[9] Certificat associé : https://certificats-attestations.afnor.org/certification=335181233155