

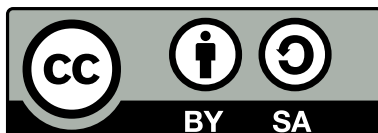
# *Étude de l'autonomie stratégique autour du poste de travail bureautique*

*De la dépendance technologique à la maîtrise opérationnelle :  
analyse et scénarios de migration.*

---

Cette étude est un livrable du projet de fin d'études de six étudiants de l'ECE, sous le pilotage d'EDE, au bénéfice d'EDF ; sa publication se fait dans le cadre de ce partenariat.

Cet ouvrage a pour vocation d'analyser les enjeux de la souveraineté numérique et de l'autonomie stratégique autour du poste de travail bureautique et de fournir aux décideur-euses une méthodologie d'évaluation rigoureuse pour piloter la transition des infrastructures bureautiques vers une maîtrise opérationnelle durable.



Mise à disposition selon les termes de la  
**Licence Creative Commons Attribution - Partage dans les Mêmes Conditions**  
Les fichiers sources utilisés pour compiler ce document sont disponibles via ce [lien](#).

## **Auteurs :**

Luca Soler, Antoine Grenouillet, Matteo Demichele, Naël Michot, Alexis Lulin, Evane Lipou

24/02/2026

## Table des matières

---

1. Remerciements .....	5
2. Résumé exécutif .....	6
2.1. Contexte .....	6
2.1.1. Du logiciel propriétaire à l'hégémonie politique .....	6
2.1.2. L'insécurité juridique : remise en question du dogme de la localisation physique .....	6
2.1.3. La technologie comme arme de coercition diplomatique .....	7
2.1.4. Enjeux RSE .....	7
2.2. Diagnostic du poste de travail bureautique .....	8
2.3. La sécurité par la transparence : un changement de paradigme .....	8
2.4. Méthodologie d'évaluation .....	8
2.5. Stratégie de mise en œuvre .....	9
3. Contexte de l'étude .....	10
3.1. Le constat des dépendances .....	10
3.2. L'ambition de souveraineté, pourquoi maintenant ? .....	10
3.3. Exemples de réussites .....	11
3.3.1. En France .....	11
3.3.2. À l'international .....	11
3.4. Projets en cours et dynamiques collectives .....	12
3.5. Problématique .....	13
4. Méthodologie d'évaluation et de notation .....	14
4.1. Définition des notions clés .....	14
4.1.1. Souveraineté numérique et autonomie stratégique .....	14
4.1.2. Logiciel libre, open source et propriétaire .....	14
4.2. Construction de l'Indice d'Autonomie Stratégique (IAS) .....	15
4.3. Les six piliers de l'Indice d'Autonomie Stratégique .....	16
4.4. Interprétation et limites : distinguer souveraineté et performance .....	26
5. État des lieux de l'architecture du poste de travail bureautique .....	27
5.1. Cartographie des briques actuelles .....	27
5.2. Découpage en briques fonctionnelles .....	28
5.2.1. Identité & Conformité .....	28
5.2.2. Gestion de parc et maintien en condition opérationnelle .....	28
5.2.3. Socle réseau .....	30
5.2.4. Stockage distant .....	30
5.2.5. Applications (outillage métier) .....	31
5.2.6. Sécurité .....	31
5.2.7. Collaboration .....	32
5.3. Évaluation et conclusion .....	34
5.4. Périmètre de l'étude : Définition du « poste de travail bureautique » .....	34
6. Approche théorique d'un projet de migration .....	35
6.1. Opportunités et modèles économiques .....	35
6.1.1. De la dépense de licence à l'investissement humain .....	35
6.1.2. Le piège de la réduction des coûts comme objectif unique .....	36

6.1.3. Financement et pérennité de l'écosystème libre .....	36
6.2. Cadrage stratégique et alignement de la gouvernance .....	37
6.3. Utilisation d'un socle applicatif commun .....	37
6.4. Gestion de projet .....	37
6.5. Gestion du capital humain et traitement des résistances .....	38
6.6. Trajectoire de migration .....	39
6.6.1. Sanctuarisation du socle applicatif commun et indépendance des formats .....	39
6.6.2. Validation par la preuve .....	39
6.6.3. Extension du périmètre et qualification des usages .....	39
6.6.4. Industrialisation par opportunité de renouvellement .....	40
6.6.5. Inversion de la norme et gestion des exceptions .....	40
6.7. Accessibilité numérique .....	40
6.8. Continuité de service et blocages techniques résiduels .....	41
7. Analyse comparative des alternatives .....	43
7.1. Systèmes d'exploitation pour les postes utilisateur-rices .....	43
7.1.1. Debian .....	43
7.1.2. openSUSE .....	45
7.1.3. Fedora .....	46
7.1.4. Ubuntu .....	47
7.1.5. Synthèse et recommandation .....	49
7.2. Environnements de bureau .....	50
7.2.1. KDE Plasma .....	50
7.2.2. GNOME .....	51
7.2.3. Cinnamon .....	52
7.2.4. Synthèse et recommandation .....	53
7.3. Approvisionnement des terminaux .....	54
7.3.1. iPXE + Preseed + scripts .....	55
7.3.2. FAI (Fully Automated Install) .....	55
7.3.3. Foreman + Katello .....	56
7.3.4. FOG Project .....	56
7.3.5. Synthèse et recommandation .....	57
7.4. Configuration .....	58
7.4.1. Ansible .....	58
7.4.2. Puppet Enterprise .....	59
7.4.3. OpenVox (Vox Pupuli) .....	60
7.4.4. Rudder .....	61
7.4.5. Synthèse et recommandation .....	62
7.5. Navigateur Web .....	63
7.5.1. Firefox (Mozilla) .....	64
7.5.2. Brave .....	64
7.5.3. Synthèse et recommandation .....	65
7.6. Suite Bureautique .....	65
7.6.1. Only Office .....	66
7.6.2. LibreOffice .....	67
7.6.3. Apache OpenOffice .....	68

7.6.4. Synthèse et recommandation .....	69
7.7. Collaboration .....	69
7.7.1. Private Discuss .....	70
7.7.2. Element (Matrix) .....	70
7.7.3. Nextcloud Talk .....	71
7.7.4. Synthèse et recommandation .....	72
7.8. Stockage et partage .....	73
7.8.1. Nextcloud .....	73
7.8.2. Twake .....	74
7.8.3. La Suite Numérique .....	75
7.8.4. Synthèse et recommandation .....	76
7.9. Sécurité des terminaux .....	77
7.9.1. Wazuh .....	77
7.9.2. HarfangLab .....	78
7.9.3. Elastic Security .....	79
7.9.4. Synthèse et recommandation .....	79
8. Déclinaison opérationnelle de la migration .....	81
8.1. Socle commun et formats ouverts .....	81
8.1.1. Brique fonctionnelle : Stockage et partage .....	81
8.2. Gestion de l'héritage MPIP .....	82
8.2.1. Gestion des politiques de classification et de chiffrement des documents .....	82
8.2.2. Stratégie de migration progressive : Le modèle du Ministère Autrichien (BMWET) .....	83
8.2.3. Socle commun applicatif .....	83
8.2.4. Nécessité d'interopérabilité .....	85
8.3. Transition au niveau du système d'exploitation .....	86
8.3.1. Phase 2 : Validation technique (POC) .....	86
8.3.2. Phase 2 : Validation technique et socle (POC) .....	86
8.3.3. Phase 3 : Pilote et confrontation aux métiers .....	86
8.3.4. Phase 4 : Industrialisation et automatisation .....	87
8.3.5. Phase 5 : Inversion de la norme et gestion de l'héritage .....	87
9. Conclusion .....	88
Glossaire .....	89
Bibliographie .....	92

# 1. Remerciements

---

La réalisation de cet ouvrage est le fruit d'une réflexion collective et d'un engagement partagé en faveur de la souveraineté numérique et de l'autonomie stratégique. Nous tenons à exprimer notre profonde gratitude à toutes les personnes qui ont permis de porter ce projet et d'en faire valoir les enjeux.

Nos remerciements s'adressent tout d'abord à l'équipe projet de l'ECE, qui nous a accordé sa confiance en autorisant ce sujet et en nous offrant le cadre nécessaire pour le développer. Nous remercions également chaleureusement Romaric Sichler, qui a suivi et encadré avec attention l'évolution de nos travaux durant ces six derniers mois.

Nous tenons à exprimer notre reconnaissance envers EDF pour son soutien et l'autorisation de mener ces recherches, avec une pensée particulière pour Loïc Bouchet, Ludovic Burg, Jean-Michel Chareyron et Yves Gacogne. Nous saluons les convictions et l'initiative portée par Laurent Leroy, dont l'impulsion a été déterminante pour concrétiser ces recherches.

Une gratitude toute singulière est adressée à Kent Brudey, dont l'implication a grandement contribué à l'ancrage, l'affûtage et l'affinage des thématiques abordées, ainsi qu'à la force des arguments déployés au fil des pages.

De plus, nous souhaitons remercier l'ensemble des contributeurs et contributrices de l'écosystème du libre ayant pris part aux diverses conférences, billets de blog, interviews et tables rondes accessibles sur le web. Ce document n'aurait pu voir le jour sans la richesse de vos interventions, la générosité de vos témoignages et la finesse de vos analyses sur les enjeux des logiciels libres, de la souveraineté numérique et de l'autonomie stratégique.

Enfin, nous remercions nos lecteurs et lectrices, ainsi que toutes celles et ceux qui, par leurs relectures attentives et leurs encouragements, ont contribué à parfaire la pertinence de cet ouvrage. Que ce travail puisse servir de guide et d'inspiration pour de futures trajectoires de transformation numérique.

## 2. Résumé exécutif

---

Le poste de travail bureautique constitue aujourd'hui la porte d'entrée principale du système d'information de toute organisation et le réceptacle de son patrimoine intellectuel. Pourtant, la majorité de ces environnements repose sur des écosystèmes technologiques dont la maîtrise technologique échappe aux organisations.

Cette étude dresse un état des lieux des dépendances technologiques qui pèsent sur l'outil de travail quotidien. Elle analyse comment l'hégémonie d'éditeurs monopolistiques, couplée à l'évolution des cadres juridiques internationaux (comme le *CLOUD Act* américain), transforme un choix technique en un risque stratégique, juridique et environnemental pour les organisations.

L'objectif de ce rapport est de proposer une trajectoire de migration vers un environnement maîtrisé, évalué à partir de l'Indice d'Autonomie Stratégique (IAS), où l'organisation peut exercer son autonomie stratégique, afin de garantir la pérennité et la maîtrise opérationnelle de ses postes de travail.

### 2.1. Contexte

Pour comprendre les enjeux de la souveraineté, il est nécessaire de hiérarchiser les mécanismes qui entravent aujourd'hui la liberté de choix des organisations. Cette dépendance repose sur un triptyque conceptuel : le caractère **propriétaire** des outils, la structure **monopolistique** du marché et l'**hégémonie** politique qui en découle.

#### 2.1.1. Du logiciel propriétaire à l'hégémonie politique

Le **logiciel propriétaire** se définit comme une solution dont l'usage est régi par une licence restrictive interdisant l'étude, la modification ou la redistribution du logiciel. Cette opacité technique crée un enfermement propriétaire (aussi appelé *vendor lock-in*). À terme, la dépendance contractuelle et technique devient telle que le coût financier et opérationnel d'une sortie du système devient prohibitif pour l'organisation.

Lorsque ces solutions sont portées par un nombre restreint d'acteurs, le marché devient **monopolistique**. Cette concentration de pouvoir n'est pas qu'économique : elle devient **hégémonique** lorsqu'un État utilise la domination de ses entreprises nationales pour imposer ses normes juridiques et sa vision stratégique au reste du monde. Si cette hégémonie est aujourd'hui principalement le fait des États-Unis, les multinationales comme Alphabet (Google), Amazon, Méta (Facebook), Apple et Microsoft font partie des plus grandes capitalisations boursières mondiales [1], le risque est structurel : une dépendance similaire envers des solutions venant d'Allemagne ou de Chine poserait les mêmes défis d'autonomie.

#### 2.1.2. L'insécurité juridique : remise en question du dogme de la localisation physique

L'idée qu'héberger des données sur le sol européen suffit à les protéger est une illusion juridique. L'arsenal législatif américain, à travers le *CLOUD Act* et les procédures *Foreign Intelligence Surveillance Act (FISA)*, notamment la section 702 [2], implique l'extraterritorialité du droit.

Dès lors qu'une entreprise (ou sa filiale) tombe sous la juridiction américaine, elle a l'obligation légale de fournir les données demandées par les agences de renseignement, peu importe le lieu de stockage physique. Ainsi, la doctrine du *Cloud First*, qui a guidé les décisions des directions informatiques de la dernière décennie, se heurte à une réalité nouvelle : l'incapacité juridique des prestataires américains à garantir la confidentialité absolue des données face à leur propre gouvernement [3].

### 2.1.3. La technologie comme arme de coercition diplomatique

La vulnérabilité n'est pas seulement juridique, elle est opérationnelle. Dans un contexte géopolitique instable, les infrastructures numériques sont utilisées comme des leviers de politique étrangère.

Les sanctions technologiques peuvent paralyser instantanément une organisation. L'exemple récent du juge français Nicolas Guillou, de la Cour Pénale Internationale, dont les accès personnels et professionnels ont été visés par des sanctions américaines, illustre qu'aucun acteur n'est à l'abri d'une restriction de service arbitraire. Faire reposer la continuité d'activité sur des acteurs soumis à des aléas diplomatiques constitue un risque systémique pour l'organisation.

### 2.1.4. Enjeux RSE

L'activité humaine a déjà dépassé 7 des 9 limites planétaires définies par le Stockholm Resilience Centre [4], illustrant une pression croissante sur les équilibres écologiques mondiaux. Des points de tension se cristallisent de plus en plus entre différents secteurs, dont le numérique, dépendant des mêmes ressources. Le secteur numérique, en particulier, est connu pour son utilisation de 50 à 70 substances minérales du tableau périodique des éléments [5]. Il fait face à des défis majeurs liés à l'accès aux matières premières, ainsi qu'aux ressources en eau et en électricité. Dans ce contexte, les impératifs de sobriété et d'adaptation s'imposent.

Pourtant, la dépendance numérique actuelle place les organisations en contradiction directe avec leurs engagements Responsabilité Sociétale des Entreprises (RSE). La transition forcée vers Windows 11 illustre cette dérive, en rendant obsolètes près de 400 millions de terminaux pourtant parfaitement fonctionnels [6], cette décision génère une pollution numérique [7] massive, aux antipodes des impératifs de sobriété. Ce mécanisme démontre que l'absence de maîtrise logicielle (évoquée précédemment) se traduit par une incapacité à gérer durablement le cycle de vie du matériel.

Le numérique repose sur une base matérielle dont le coût humain est dévastateur. L'extraction massive de minerais (cobalt, coltan, lithium) pour les puces et l'infrastructure *cloud* alimente, notamment en République Démocratique du Congo, un système de travail forcé et de travail des enfants sous le contrôle de groupes armés [8], [9]. Au-delà de l'extractivisme, la porosité entre intérêts privés et politiques répressives aggrave ce bilan éthique. Cette dérive est manifeste, comme le montre l'implication des infrastructures d'Amazon (AWS), de Google ou de Palantir dans les opérations de l'ICE (Immigration and Customs Enforcement) aux États-Unis facilitant le profilage, la localisation et l'expulsion massive de populations migrantes [10], [11].

À l'opposé de ces logiques extractivistes et répressives, l'usage de logiciels libres constitue un levier de responsabilité concret. En permettant l'usage de systèmes plus légers, il prolonge la durée de vie des équipements et brise le cycle de l'obsolescence programmée. Cette approche offre également l'opportunité de réallouer les budgets, substituant à la rente logicielle versée aux monopoles un investis-

sement stratégique dans le capital humain et la montée en compétences interne, garantissant ainsi une cohérence entre RSE et autonomie stratégique.

## 2.2. Diagnostic du poste de travail bureautique

L'analyse de l'architecture actuelle du poste de travail bureautique révèle que la stratégie des organisations dépend désormais étroitement des outils de Microsoft, dont l'hégémonie (plus de 70 % des parts de marché mondiales) permet d'imposer une stratégie d'hybridation vers le cloud.

Ce verrouillage technologique opère un transfert de maîtrise significatif : les identités, les données et les clés de chiffrement échappent progressivement au contrôle direct de l'entité pour basculer dans l'écosystème de l'éditeur. En conséquence, l'autonomie stratégique de l'organisation autour du poste de travail Windows est aujourd'hui jugée fortement compromise, car elle se retrouve conditionnée par les évolutions et les exigences imposées par les solutions cloud de Microsoft.

## 2.3. La sécurité par la transparence : un changement de paradigme

L'un des préjugés les plus tenaces à l'encontre du logiciel libre réside dans l'idée que l'accessibilité du code source publiquement faciliterait le travail des attaquants. Pourtant, la recherche en sécurité informatique et la pratique opérationnelle démontrent l'inverse, la sécurité par l'obscurité (propre aux logiciels propriétaires) est une stratégie fragile qui ne fait que retarder la découverte des failles sans les empêcher.

Le logiciel libre s'appuie sur le principe de Kerckhoffs [12], postulant que la robustesse d'un système doit résider dans sa conception et non dans la dissimulation de ses mécanismes [13]. Cette transparence permet une auditabilité continue et indépendante, transformant le code source en un bien commun supervisé par une multitude d'acteurs.

## 2.4. Méthodologie d'évaluation

Si plusieurs initiatives ont émergé aux niveaux national et européen, elles restent souvent fragmentées. L'indice de résilience numérique (IRN) [14] se focalise sur la chaîne de valeur, tandis que les réglementations de l'UE [15] privilégient la protection des données et la concurrence. Face à ce constat, nous avons décidé de concevoir un cadre d'analyse global capable de comparer les solutions technologiques entre elles sous l'angle spécifique de l'autonomie stratégique. C'est pour répondre à ce besoin que nous avons développé l'Indice d'Autonomie Stratégique (IAS). Fondé sur une méthodologie rigoureuse et sur des critères mesurables, cet indice permet d'évaluer chaque alternative sur 100 points, articulés autour de six piliers :

1. **AS1 | Maîtrise des données & Juridiction** : Sommes-nous protégés contre l'ingérence d'acteurs tiers ? (Analyse de la nationalité, de l'hébergement et du chiffrement).
2. **AS2 | Gouvernance** : Qui décide du futur de nos outils ? (Structure de l'éditeur, transparence de la feuille de route et contrôle de l'actionnariat).
3. **AS3 | Licence & Ouverture** : Avons-nous le droit de voir, modifier et repartir avec les sources ? (Nature de la licence et accessibilité du code source).
4. **AS4 | Interopérabilité & Réversibilité** : Pouvons-nous changer de solution sans douleur ? (Usage de standards ouverts, qualité des API et facilité d'export des données).
5. **AS5 | Coût & Support** : Maîtrisons-nous les coûts totaux de la solution ? (Modèle de facturation et existence d'un écosystème d'experts autour de la solution).

6. **AS6 | Pérennité & Sobriété** : La solution est-elle durable et responsable ?  
(Dynamisme de la communauté, diversité des financements et éco-conception).

## 2.5. Stratégie de mise en œuvre

La trajectoire de migration proposée s'appuie sur la sélection des solutions ayant obtenu les meilleurs scores d'IAS et tire les enseignements des précédents historiques, qu'il s'agisse des succès (Gendarmerie nationale française) ou des échecs (Ville de Munich).

L'analyse de ces retours d'expérience met en lumière une condition *sine qua non* de réussite : la nécessité d'un **sponsor fort** au niveau de la **direction générale**.

Par direction générale, nous entendons ici le **pouvoir politique de l'organisation** (PDG, Comex, élu, ou mandataires sociaux). Ce portage est indispensable car une migration vers un environnement souverain est une transformation culturelle plus que technique ; elle exige un portage politique inébranlable pour légitimer la démarche.

Fort de ce soutien, le déploiement opérationnel d'un poste de travail souverain se doit d'écarter toute approche brutale au profit d'une stratégie progressive sur le temps long, structurée en quatre phases :

1. **Sanctuarisation du socle applicatif commun** : Découplage des usages et du système d'exploitation par le déploiement prioritaire des logiciels à haut score IAS (Firefox, Thunderbird, LibreOffice) sur le parc Windows existant.
2. **Validation par la preuve (POC)** : Montée en compétence des équipes techniques, validation de l'intégration du poste et des logiciels sélectionnés au sein du système d'information.
3. **Politique de déploiement volontariste** : Mise à disposition du poste sur un périmètre d'utilisateur·rices volontaires. Cette étape permet de valider l'intégration technique du poste souverain.
4. **Industrialisation par opportunité** : Déploiement du système souverain avec le cycle naturel de renouvellement du matériel, rendant la transition techniquement fluide et budgétairement neutre. Il est toujours possible de demander à conserver un poste Windows.
5. **Inversion de la norme** : Le poste souverain devient le standard par défaut de l'organisation. L'attribution d'un poste Windows devient une exception, qui doit être formellement justifiée par des impératifs métiers bloquants.

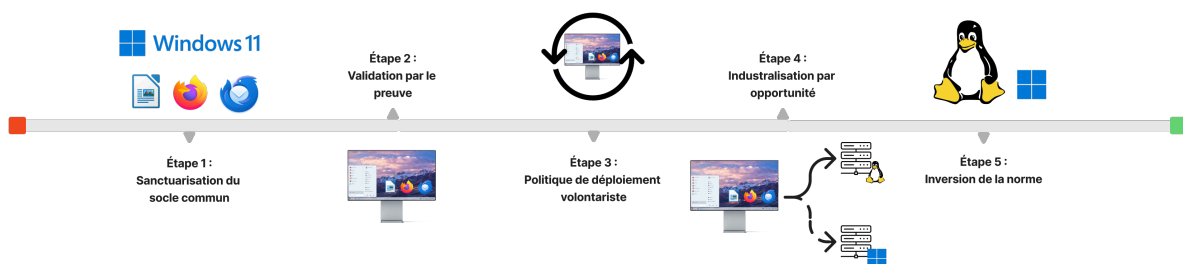


Fig. 1. - Schéma de la stratégie de déploiement d'un poste bureautique souverain

## 3. Contexte de l'étude

---

L'hégémonie exercée par les géants du numérique, conjuguée à l'accélération des contraintes géopolitiques et environnementales, impose désormais une révision profonde de la stratégie relative au poste de travail bureautique.

Cette étude vise à dresser un état des lieux de la dépendance technologique actuelle liée au poste de travail Windows.

Elle propose ensuite une trajectoire de migration vers un environnement numérique souverain, en s'appuyant sur des alternatives éprouvées afin de garantir l'autonomie stratégique de l'organisation.

### 3.1. Le constat des dépendances

La dépendance aux technologies **propriétaires monopolistiques**, aujourd'hui majoritairement américaines, ne relève plus d'un simple arbitrage technique mais constitue un risque avéré pour les organisations européennes.

Ce déséquilibre se traduit par une fuite massive de capitaux. 265 milliards d'euros de dépenses numériques des entreprises européennes, soit près de **80%**, sortent de l'Union européenne. À trajectoire constante, ce montant pourrait atteindre 500 milliards d'euros par an d'ici 2030 [16], [17], [18], [19].

Au-delà de l'aspect économique, cette dépendance s'articule autour de trois axes :

Le marché technologique actuel est structurellement verrouillé par un **oligopole** d'éditeurs (Microsoft, Google, Amazon). Cette hégémonie impose des cycles de renouvellement matériel contraints, les évolutions logicielles devenant systématiquement plus énergivores et exigeantes en ressources, rendant le parc informatique existant prématurément obsolète.

L'usage massif de solutions *Software as a Service (SaaS)* et *cloud* expose les données européennes au droit américain. Des dispositifs comme le *Clarifying Lawful Overseas Use of Data Act* [20] permettent aux autorités américaines d'accéder aux données hébergées par leurs entreprises, quelle que soit leur localisation géographique. En effet, des incidents récents (comme les sanctions technologiques touchant l'Iran [21], les restrictions d'accès à des services *cloud* pour certaines institutions internationales [22], ou encore le témoignage édifiant d'un juge de la Cour Pénale Internationale, expliquant l'impact des mesures restrictives américaines sur la vie courante [23]) démontrent que les infrastructures numériques (système d'exploitation, *cloud*, systèmes de paiement) peuvent être utilisées comme des leviers de politique étrangère, menaçant la continuité d'activité des entités dépendantes.

De plus, ce modèle entraîne des coûts récurrents élevés (licences, abonnements) sur lesquels les organisations n'ont presque pas de levier de négociation.

### 3.2. L'ambition de souveraineté, pourquoi maintenant ?

Tout d'abord, au niveau de la stratégie de RSE, l'urgence écologique impose une gestion durable du parc informatique. Il s'agit de limiter la production massive de déchets électroniques [7], notamment ceux induits par les politiques des éditeurs propriétaires comme le montre le renouvellement forcé de millions de machines suite à la fin du support de Windows 10.

D'autre part, la souveraineté numérique est devenue une préoccupation partagée par les citoyen·nes et les professionnel·les français. Pour toute organisation, s'aligner sur des valeurs de transparence, de collaboration et d'indépendance (propres au logiciel libre) est un gage de responsabilité ; et même une question de cohérence avec la mission de service public pour les organisations concernées.

Enfin, la quête de résilience impose un changement de paradigme vers la low-tech. Face à la vulnérabilité croissante des chaînes d'approvisionnement et aux crises énergétiques, le simple remplacement d'un logiciel par un autre ne suffit plus. Comme le souligne le rapport du Cigref [24], l'organisation doit intégrer l'approche low-tech comme un levier de résilience numérique basée sur trois axes :

- **Utilité** : questionner le juste besoin pour éliminer les fonctionnalités superflues en cherchant à maximiser l'utilité sociale des solutions.
- **Accessibilité** : garantir des technologies réparables et maîtrisables en interne. Ce qui favorise la transmission des savoirs, le partage des compétences et le renforcement du lien social.
- **Durabilité** : privilégier des systèmes d'exploitation sobres, capables de tourner sur du matériel ancien ou reconditionné, réduisant ainsi drastiquement la dépendance aux renouvellements matériels imposés par les géants du marché.

### 3.3. Exemples de réussites

La migration vers un poste de travail souverain n'est pas une utopie ; elle a été réalisée avec succès par diverses organisations en France et à l'international.

#### 3.3.1. En France

- **La Gendarmerie nationale (GendBuntu)** : Il s'agit de la référence majeure avec 85 000 postes migrés sous une version dérivée d'Ubuntu. Initié pour des raisons d'indépendance numérique, ce projet a permis une réduction des coûts (baisse de 40% du Total Cost of Ownership (TCO) constatée entre 2008 et 2015). Cette migration a prouvé la faisabilité d'une transition massive et industrielle. Elle a permis une maîtrise totale du cycle de vie des logiciels et une indépendance vis-à-vis des éditeurs.
- **Les Villes de Fontaine et d'Échirolles** : Ces collectivités ont mené une migration basée sur une volonté politique forte d'autonomie stratégique et de service public. Le retour d'expérience montre une très forte satisfaction des utilisateur·rices (notée 4,5/5) et une simplification de l'administration technique du parc (mises à jour facilitées, meilleure sécurité). La stratégie de changement progressif et non forcé a été un facteur clé de leur succès.

#### 3.3.2. À l'international

L'élan vers l'indépendance technologique dépasse les frontières françaises, souvent motivé par des stratégies de défense nationale et de souveraineté numérique :

- **Danemark et Allemagne** : Diverses administrations européennes, notamment au Danemark et en Allemagne, ont engagé des processus de migration vers des standards ouverts et des systèmes libres pour réduire leur dépendance aux fournisseurs américains.
- **Iran** : Face aux sanctions technologiques et aux restrictions d'accès aux services cloud internationaux, le pays a dû adapter ses infrastructures pour garantir sa continuité d'activité, illustrant la nécessité de maîtriser ses dépendances.

- **Venezuela (Canaima)** : Dans une optique d'indépendance nationale forte, le gouvernement a favorisé le développement et l'adoption d'une distribution GNU/Linux nationale (Canaima) pour ses administrations publiques, afin de s'affranchir des licences propriétaires étrangères.
- **Russie (Astra Linux)** : Dans un contexte de tensions géopolitiques accrues, la Russie a accéléré sa transition vers Astra Linux, un système d'exploitation sécurisé initialement conçu pour l'armée. Cette démarche vise à remplacer Microsoft Windows par une infrastructure souveraine capable de supporter les secteurs critiques et les administrations de l'État.
- **Chine (Kylin)** : À travers son programme de substitution technologique, la Chine déploie massivement Kylin. Basé sur le noyau Linux, ce système d'exploitation est au cœur de la stratégie nationale visant à éliminer la dépendance aux technologies étrangères au sein des infrastructures gouvernementales et financières. Il possède actuellement 90% de part de marché dans le secteur gouvernemental chinois.
- **Cuba (Nova Linux)** : Pour répondre à l'embargo technologique et garantir son autonomie numérique, Cuba a développé Nova Linux pour remplacer Microsoft Windows. Cette distribution est un pilier de la politique de migration vers les logiciels libres de l'île, favorisant ainsi la maîtrise du code source et la sécurité nationale.

### 3.4. Projets en cours et dynamiques collectives

La quête d'autonomie stratégique numérique se traduit aujourd'hui par des réalisations concrètes. Une véritable dynamique collective peut émerger, portée par la conviction que la souveraineté ne s'atteint pas en solitaire, mais par la mutualisation des ressources et des compétences.

- **Le modèle danois** : Le Danemark engage une démarche de transition avec son réseau **OS2** (Offentligt digitaliseringsfællesskab). Ce collectif regroupe plus de 80 % des municipalités danoises pour co-développer des solutions libres. En 2025, le pays a franchi une première étape en amorçant une transition globale de ses administrations vers LibreOffice pour s'affranchir de la dépendance aux éditeurs américains.
- **Métropole de Lyon** : À l'échelle locale, la ville et la métropole de Lyon amorcent une transformation. À travers le projet Territoire Numérique Ouvert (TNO), co-développé avec le SITIV, elles déploient une suite collaborative souveraine. L'objectif est de réduire la dépendance technologique et stimuler l'économie locale, 100% des marchés du projet étant attribués à des entreprises françaises de la région Auvergne Rhône Alpes.
- **Hauts-de-France** : Un collectif de professeur·es a lancé la démarche **NIRD** (Numérique, Inclusif, Responsable, Durable) et l'utilisation de la distribution **PrimTux** [25]. Cette démarche est soutenue par le ministère de l'Éducation nationale, cela montre qu'un environnement souverain peut être un levier d'inclusion scolaire et de réemploi de matériel informatique.
- **L'État français** : Le 26 janvier 2026 a été annoncée la généralisation de Visio. Développée par la Direction interministérielle du numérique (DINUM), cette solution de visioconférence sécurisée et souveraine deviendra obligatoire pour l'ensemble des services de l'État d'ici 2027. Cette initiative vise à remplacer les outils propriétaires extra-européens par une alternative intégrée à « La Suite Numérique », garantissant ainsi que les échanges administratifs restent sous contrôle technologique national.

Ces projets mettent en lumière des **synergies** qui vont se construire, en mutualisant les coûts, le développement de communs numériques permet de partager l'effort financier entre plusieurs acteurs. Tout en impliquant une diversité de parties prenantes (collectivités, entreprises, associations, ...) dans une

vision partagée. En choisissant des standards ouverts, ces acteurs facilitent les coopérations futures et évitent l'enfermement propriétaire. L'ambition n'est plus seulement de remplacer un outil par un autre, mais de bâtir un écosystème résilient où chaque partie prenante devient garante de la pérennité et de la souveraineté de la ressource commune.

### 3.5. Problématique

Cette étude cherche à répondre à la problématique suivante :

*Comment garantir l'autonomie stratégique pour la souveraineté numérique de l'organisation en articulant la réflexion autour du poste de travail, tout en conciliant les impératifs de sobriété numérique, de maîtrise budgétaire et de maintien de la performance métier ?*

## 4. Méthodologie d'évaluation et de notation

---

Cette section détaille le cadre théorique et les métriques utilisées pour évaluer l'autonomie stratégique numérique des solutions auditées. Bien que plusieurs initiatives aient été lancées, tant au niveau national qu'europpéen, elles se concentrent souvent sur des segments spécifiques comme l'indice de résilience numérique (IRN) [14] qui analyse l'intégralité de la chaîne de valeur, ou les réglementations de l'UE qui traitent de la protection des données et de la concurrence [15].

Dans notre cas, nous avons besoin d'un cadre d'évaluation permettant de comparer des solutions technologiques entre elles sous le prisme de l'autonomie stratégique. C'est dans cette optique que nous avons développé l'Indice d'Autonomie Stratégique (IAS).

### 4.1. Définition des notions clés

La précision terminologique est sensible dans un contexte où le terme « souveraineté » est de plus en plus souvent utilisé comme un argument marketing, du « sovereign washing » [26].

#### 4.1.1. Souveraineté numérique et autonomie stratégique

Il est impératif de distinguer la posture politique de la capacité opérationnelle, distinction soulignée par les travaux récents sur la géopolitique du numérique [27].

- **Souveraineté numérique** : Capacité de l'État ou de l'organisation à faire respecter ses droits et sa législation dans le cyberspace. Elle s'oppose à l'extra-territorialité du droit (ex: *CLOUD Act* [20]). C'est une notion juridique.
- **Autonomie stratégique** : Capacité à agir librement, à choisir ses dépendances et à ne pas être soumis à la coercition d'un tiers (fournisseur ou état). L'objectif n'est pas l'autarcie, mais la maîtrise des dépendances critiques. L'objectif est de disposer de la capacité de choisir ses dépendances et de transformer l'interdépendance en levier de puissance plutôt qu'en vulnérabilité. C'est une notion opérationnelle.

#### 4.1.2. Logiciel libre, open source et propriétaire

Chaque logiciel est soumis à une licence qui définit le pouvoir de l'utilisateur·rice sur le logiciel. Si l'accès au code source est une condition *sine qua non* de l'auditabilité, c'est bien la nature juridique de la licence qui accorde (ou non) les **quatre libertés** fondamentales.

- **Liberté 0** : Utiliser le logiciel. La liberté d'exécuter le programme, pour tous les usages (professionnel, personnel, éducatif) et sans aucune restriction.
- **Liberté 1** : Étudier le logiciel. La liberté d'accéder au code source pour comprendre comment il fonctionne et de l'adapter à ses besoins.
- **Liberté 2** : Redistribuer le logiciel. La liberté de copier le programme et de le partager avec d'autres (gratuitement ou non) pour aider son prochain.
- **Liberté 3** : Améliorer le logiciel. La liberté de modifier le code et de publier les améliorations pour que l'ensemble de la communauté en profite.

Type	Caractéristiques	Impact
<b>Propriétaire</b>	Code fermé (« Boîte noire »). Interdiction de modification, droit d'usage révocable.	<b>Dépendance totale.</b> Audit de sécurité impossible par un tiers de confiance.
<b>Open Source</b>	Code ouvert. Octroie la capacité d'étudier le code source du logiciel.	<b>Transparence partielle.</b> Des briques propriétaires peuvent être cachées. Ce mode ne permet pas de garantir la pérennité d'accès et d'utilisation du logiciel.
<b>Logiciel Libre</b>	Code libre. Liberté d'exécuter, étudier, modifier et de redistribuer le logiciel.	<b>Maîtrise totale.</b> Garantie de pérennité ( <u>fork</u> possible) et d'indépendance.

Tableau 1. - Comparaison des modèles de distribution logicielle

Dans cette perspective, le logiciel libre s'impose comme le seul levier technologique capable de concrétiser l'autonomie stratégique d'une organisation. Contrairement au modèle propriétaire, qui maintient l'organisation dans une dépendance contractuelle et technique vis-à-vis de l'éditeur, ou à certaines formes d'Open Source conservant des verrous commerciaux, le logiciel libre transfère la maîtrise intégrale de l'outil à l'organisation. En garantissant juridiquement les libertés d'étude, de modification et de redistribution, il offre une assurance contre l'obsolescence programmée ou l'abandon d'un produit par son éditeur grâce à la possibilité de créer une dérivation (*fork*). Cette capacité à auditer le code et à en maintenir l'évolution en interne ou via un tiers constitue la condition *sine qua non* pour s'affranchir de toute coercition extérieure et choisir ses dépendances sans les subir.

De plus l'écosystème libre propose désormais des briques technologiques matures, robustes et éprouvées pour le poste de travail (navigateurs, suites bureautiques, outils de collaboration), rendant la transition techniquement réaliste.

L'évaluation qui suit vise donc à mesurer l'**autonomie stratégique** de l'organisation au travers du choix de ses outils numériques, afin d'assurer une maîtrise des dépendances critiques.

## 4.2. Construction de l'Indice d'Autonomie Stratégique (IAS)

Dans un contexte géopolitique instable, la dépendance technologique constitue un risque critique pour les organisations européennes. Inspiré par les travaux du Cigref [28], du « Cloud Sovereignty Framework » [15] de l'UE, du référentiel SecNumCloud [29] de l'ANSSI, et principalement du travail de l'aDRI qui a créé l'Indice de Résilience Numérique (IRN) [14], nous avons construit l'**Indice d'Autonomie Stratégique (IAS)**.

Une distinction méthodologique fondamentale justifie la création de l'IAS en complément de l'IRN. Là où l'IRN agit comme un indicateur **macroscopique** destiné aux directions générales pour mesurer la vulnérabilité globale de l'organisation (culture du risque, processus, part globale des dépenses), l'IAS se positionne comme son pendant **opérationnel et microscopique**.

L'IAS ne note pas l'entreprise, mais la solution technique elle-même. Il constitue le levier d'action permettant aux directions des systèmes d'informations de concrétiser les objectifs de résilience fixés par

l'IRN, en descendant au niveau de granularité nécessaire pour arbitrer factuellement entre deux logiciels concurrents.

Cet indice permet de choisir des alternatives en se basant sur des faits mesurables, il est structuré autour de six piliers. Afin d'assurer une analyse granulaire et précise, chaque pilier est subdivisé en plusieurs critères, permettant d'identifier avec exactitude les forces et les dépendances de chaque solution auditée.

Cet indice permet ainsi de fonder le choix d'alternatives sur des critères mesurables selon six piliers.

Nous avons fait le choix méthodologique d'une échelle discrète, interdisant les notes intermédiaires (comme 2 ou 4) lors de l'évaluation unitaire des critères. Ce parti pris permet de :

- **Forcer la décision** : Cette contrainte oblige l'auditeur à arbitrer.
- **Valoriser les sauts qualitatifs** : L'échelle 0-1-3-5 permet de pondérer plus lourdement les progrès qu'une échelle linéaire classique. Le passage du statut « Insatisfaisant » (1) au statut « Satisfaisant » (3) représente un saut de maturité qui mérite d'être mathématiquement valorisé.

Contrairement à une approche par coefficients fixes, l'IAS utilise une pondération dynamique basée sur la pertinence : si un critère est jugé « Non Concerné » pour une brique logicielle donnée, il est exclu du calcul. Cette exclusion recalibre automatiquement le poids relatif des autres critères, garantissant que la note finale ne reflète que les enjeux réels de la solution auditée.

La note d'un pilier  $P$  est définie par la moyenne des notes des critères  $C$  jugés pertinents ( $m$  étant le nombre de critères dont l'état est différent de « Non Concerné ») :

$$\text{Note}_P = \frac{1}{m} \sum_{i=1}^m C_i$$

Où chaque  $C_i$  représente la valeur d'un critère applicable au sein du pilier. Ainsi  $\text{Note}_P \in [0, 5]$ .

L'indice final est ramené sur une base 100 afin de permettre une comparaison homogène entre différentes catégories de produits.

$$\text{Score d'une solution étudiée par l'IAS} = \left( \frac{1}{n} \sum_{i=1}^n \left( \frac{1}{m_i} \sum_{j=1}^{m_i} C_{i,j} \right) \right) \times 20$$

Où :

- $n = 6$  représente le nombre de piliers de l'indice ;
- $m_i$  est le nombre de critères applicables dans le pilier  $i$  ;
- $C_{i,j} \in [0, 5]$  est la note obtenue pour le critère  $j$  du pilier  $i$ .

Le coefficient 20 permet de transposer la moyenne pondérée (initialement sur 5) vers une échelle sur 100.

### 4.3. Les six piliers de l'Indice d'Autonomie Stratégique

La présentation des six piliers est accessible ici : Chapitre 2.4

L'évaluation des solutions du marché pour chaque brique logicielle repose sur l'analyse croisée de six piliers fondamentaux. La grille d'évaluation est trouvable et téléchargeable ici [30].

## AS1 : Maîtrise des données & Juridiction

Objectif : Évaluer l'exposition aux lois extra-européennes et le contrôle technique sur les données.

### AS1-1 : Nationalité et implantation du siège de l'éditeur

Évaluation de l'exposition de l'entité responsable (éditeur ou mainteneur) aux lois extra-européennes. L'analyse porte sur le siège social et l'assujettissement aux lois à portée extraterritoriale (ex: CLOUD Act, FISA).

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Siège social hors UE et/ou soumis à des lois extra-territoriales intrusives sans garanties de protection des données.	Siège hors UE mais bénéficiant d'une <u>décision d'adéquation</u> .	Siège social et centre de décision effectif en Union européenne.	Siège social et gouvernance situés en France.

### AS1-2 : Localisation de l'hébergement

Pays où les serveurs sont situés.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Hébergement hors UE.	Hébergement UE via <u>hyper-scaler</u> non souverain.	Hébergement UE (non certifié SecNumCloud [29]).	Hébergement certifié SecNumCloud [29] ou auto-hébergement possible.

### AS1-3 : Confidentialité technique et maîtrise du chiffrement

Évaluation de la protection des données contre les accès non autorisés, y compris par le fournisseur ou l'hébergeur. Mesure l'étanchéité technique de la solution face à l'espionnage industriel ou aux réquisitions extra-territoriales.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Pas de chiffrement au repos ou chiffrement partiel des flux. Les données circulent ou sont stockées de manière lisible par l'hébergeur.	Données chiffrées au repos et en transit, mais l'hébergeur détient et gère les clés. La confidentialité repose uniquement sur un engagement contractuel ou juridique.	L'organisation apporte ou gère ses propres clés de chiffrement. L'hébergeur y accède pour le traitement, mais n'en a pas la garde permanente.	Chiffrement de bout en bout. L'hébergeur n'a jamais accès aux clés ni aux données en clair. Seul l'utilisateur final peut déchiffrer les informations.

### AS1-4 : Conformité réglementaire et protection des données

Évaluation de l'aptitude du produit à respecter le cadre légal (ex: RGPD) et à protéger l'utilisateur-riche contre les risques juridiques. Mesure l'engagement de l'entité responsable dans la veille et l'application des normes de protection de la vie privée.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Le produit ne respecte pas les principes de base. L'entité responsable décline toute responsabilité quant à la conformité.	L'entité reconnaît les réglementations sans proposer d'outils d'aide. L'implémenteur doit configurer manuellement et à ses risques les mécanismes de protection.	Toutes les réglementations applicables au produit en matière de protection des données et de confidentialité ont été analysées pour le marché cible. Le produit comprend des mesures visant à faciliter et à garantir la conformité de	Le produit dispose d'un cadre de conformité robuste, comprenant une analyse complète de toutes les réglementations applicables en matière de protection des données et de confidentialité pour le marché cible. Il aide active-

		l'utilisateur-riche, mais il ne surveille pas systématiquement les mises à jour ou les modifications apportées à la réglementation.	ment le responsable de la mise en œuvre à maintenir la conformité et suit systématiquement les mises à jour des exigences ou des réglementations afin de garantir une conformité continue.
--	--	---	--

## AS2 : Gouvernance

Objectif : Évaluer la stabilité de l'éditeur et l'influence de l'utilisateur sur le futur du produit.

### AS2-1 : Structure juridique et finalité de l'entité

Évalue la nature juridique de l'organisation responsable du produit et l'alignement de ses intérêts avec ceux de l'utilisateur-riche. L'objectif est de mesurer le risque de changement de stratégie lié à des impératifs financiers (recherche de profit maximal, rachat, sortie de bourse).

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Acteur privé lucratif sous contrôle d'actionnaires externes (société cotée, fonds d'investissement). La priorité est la rentabilité financière, induisant un risque élevé de captivité ou de pivot commercial.	Acteur privé lucratif de type TPE/PME/ETI. Bien que plus agile, la structure reste vulnérable à un rachat ou à une faillite, avec une gouvernance centrée sur les propriétaires.	Acteur privé avec des mécanismes de protection (ex: agrément ESUS, coopérative/SCOP, ou État) ou communauté de bénévoles non constituée. L'intérêt métier prime, mais la structure peut manquer de garanties contractuelles fortes.	Organisation à but non lucratif (fondation, association) dont les statuts sanctuarisent le développement du produit comme un bien commun. Absence constitutionnelle de recherche de profit, garantissant une stabilité des objectifs à long terme.

### AS2-2 : Transparence de la feuille de route

Mesure de la capacité des utilisateur-rices à anticiper, auditer et orienter les évolutions fonctionnelles. L'analyse porte sur la publicité des développements et l'ouverture des processus décisionnels de l'entité responsable.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Absence de visibilité, aucune feuille de route publique.	Feuille de route publique, mais informative uniquement. Les décisions sont prises de manière unilatérale par l'éditeur sans mécanisme de retour utilisateur-riche.	Gouvernance consultative, feuille de route à jour avec un canal de recueil des besoins (ex: ticketing, forum). Les priorités sont affichées mais l'arbitrage final reste fermé.	Gouvernance ouverte et contributive, processus de hiérarchisation transparent. L'utilisateur-riche ou la communauté peut influencer directement les priorités via un système de vote ou de financement de fonctionnalités (co-construction).

### AS2-3 : Souveraineté de l'actionariat et contrôle

Analyse de l'origine des capitaux et des droits de vote pour identifier les risques d'ingérence.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Contrôle majoritaire par des entités extra-UE.	Influence significative ou minorité de blocage hors-UE.	Actionariat majoritairement européen mais sans protection contre un rachat.	Capital 100% souverain ou verrouillé (fondation, association, coopérative, état, ou capital distribué).

### AS2-4 : Participation à la prise de décision de la solution

Évaluation de la structure de commandement du produit. Mesure la capacité de l'utilisateur-riche ou d'un collègue d'acteurs de confiance à exercer un contrôle sur les orientations stratégiques et à s'opposer à des décisions unilatérales (minorité de blocage).

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Gouvernance opaque ou inexistante. Le développement est piloté exclusivement par une entité privée sans droit de regard externe.	Il n'existe aucune structure de gouvernance communautaire pour diriger le développement continu de l'outil numérique.	Il existe certains processus informels de gestion communautaire visant à orienter le développement continu de l'outil numérique.	Des structures communautaires existent et sont mises en œuvre de manière transparente, avec des rôles et des responsabilités documentés, et sont utilisées pour orienter le développement continu de l'outil numérique.

## AS3 : Licence & Ouverture

Objectif : Évaluer le droit d'usage, d'audit et de modification du code source.

### AS3-1 : Disponibilité du code

La mesure dans laquelle le produit est convivial pour les développeur-euses, de sorte qu'une personne technique qui ne connaît pas le produit puisse y contribuer. Cela inclut la mesure dans laquelle le code source est organisé et documenté, ainsi que la mesure dans laquelle d'autres documents destinés aux développeur-euses facilitent le processus d'intégration.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Code source non accessible au public.	Le code source existe dans un référentiel nécessitant une habilitation ou un accord spécifique.	Le code source existe dans un référentiel accessible au public.	Le code source est disponible dans un référentiel accessible au public. Le logiciel est structuré de manière à permettre des personnalisations locales et l'ajout de nouveaux modules et fonctionnalités sans nécessiter la création d'une branche du code principal.

### AS3-2 : Nature de la licence et protection contre la fermeture

Analyse du régime juridique du code et des garanties de maintien de l'ouverture. L'objectif est d'évaluer la protection contre le *relicensing* (changement de licence) et la capacité de la solution à rester un bien commun numérique sur le long terme.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Propriétaire et fermé. L'usage, la modification et la redistribution sont interdits. L'organisation est totalement dépendante du bon vouloir de l'éditeur pour la survie du produit.	Licence Open Source permissive (ex: MIT, Apache 2.0). Le code est libre, mais l'absence de copyleft permet à l'éditeur ou à un tiers de créer une version propriétaire dérivée. Risque de détournement de la valeur sans retour à la communauté (ex: Redis, Valkey).	Licence libre à réciprocité (Copyleft type GPL, AGPL) avec propriété intellectuelle détenue par un acteur privé. La licence protège contre la fermeture des contributions, mais l'éditeur peut décider de changer la licence des versions futures (relicensing) s'il possède tous les droits (ex: MySQL -> MariaDB).	Licence libre à réciprocité (Copyleft type GPL, AGPL) avec propriété intellectuelle détenue par une fondation ou un organisme public. Toute fermeture est juridiquement impossible. Le caractère bien commun est sanctuarisé par l'impossibilité pour un acteur unique de changer la licence (ex: Linux, WordPress, ...).

### AS3-3 : Transparence et accessibilité du cycle de développement

Évalue la disponibilité réelle du code source et la capacité de l'utilisateur·rice à auditer le produit en continu. L'objectif est de distinguer la publication d'instantanés, du développement ouvert permettant une correction immédiate des vulnérabilités.

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Code fermé. L'audit est impossible ou strictement réservé à des tiers choisis et rémunérés par l'éditeur. Aucun contrôle indépendant n'est permis.	Accessibilité restreinte ou différée. Le code est consultable sous accord de confidentialité ou publié périodiquement après la sortie des versions (ex: modèle RHEL ou Android AOSP). Le processus de développement reste privé.	Code source public et auditable à tout moment. Le code est accessible dans un dépôt public, mais le processus de décision et les correctifs en cours de préparation (staged) ne sont pas visibles avant leur publication officielle.	Développement ouvert. Le code est développé publiquement en temps réel (dépôt de code public). L'utilisateur·rice peut auditer les correctifs avant même leur publication et suivre les discussions techniques des développeur·reuses.

## AS4 : Interopérabilité & Réversibilité

Objectif : Éviter l'enfermement propriétaire et garantir la fluidité des données.

### AS4-1 : Standards de données

Utilisation de formats ouverts et documentés garantissant l'interopérabilité des données (ex: JSON, XML, ODF).

0 - Non-Autonome	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Formats propriétaires fermés. Lecture impossible sans le logiciel.	Export limité à des formats pauvres (PDF, CSV mal structuré).	Formats ouverts structurés et documentés (JSON, SQL, XML).	Normes internationales natives (ODF, IFC, ISO) garantissant la pérennité.

**AS4-2 : Qualité de l'API**

Utilisation de normes ouvertes et conception modulaire afin de permettre la réversibilité. Les données peuvent être facilement exportées depuis le système.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Aucune API disponible (saisie manuelle ou scraping requis). Formats propriétaires fermés. Lecture impossible sans le logiciel.	L'extraction ou l'importation de données dans le système nécessite généralement de consulter le code source et/ou d'accéder directement à la base de données.	Certaines API sont disponibles pour accéder aux données et les gérer. Il existe des interfaces utilisateur-riche permettant d'exporter les données de base et les métadonnées du système (par exemple au format CSV).	Une API robuste est disponible pour répondre aux besoins clés en matière d'échange de données et de métadonnées.

**AS4-3 : Multi-plateforme**

Capacité à s'exécuter sur différents environnements sans dépendance exclusive.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Verrouillage de la solution à un système d'exploitation spécifique (ex: Windows).	Dépendance à un moteur d'exécution ou un framework propriétaire.	Support de plusieurs systèmes d'exploitation via conteneurisation ou clients dédiés.	Agnostique : client universel garantissant une expérience identique partout.

**AS4-4 : Capacité d'ingestion et de reprise de l'existant**

Évalue la capacité de la solution à importer et à intégrer les données provenant des outils externes. L'objectif est de mesurer la disponibilité d'outils de migration permettant de conserver l'historique, les structures et les métadonnées lors du changement de plateforme.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Aucun outil d'import n'est disponible. La reprise des données doit se faire manuellement ou via des saisies fastidieuses, induisant un risque de perte d'information.	La solution supporte l'import de fichiers bruts, mais nécessite des scripts de conversion pour traiter les formats spécifiques (ex: .pst, .ost). Les relations entre les données (calendriers, droits d'accès) sont perdues.	Il existe des connecteurs ou des procédures documentées pour les sources les plus courantes. Le transfert est fonctionnel mais peut demander des ajustements manuels post-migration.	La solution dispose d'outils de migration automatisés et certifiés pour les standards du marché. L'intégralité des données et métadonnées est réintégréable dans la nouvelle solution.

**AS4-5 : Facilité d'extraction et réversibilité**

Existence d'une procédure outillée et documentée pour exporter l'intégralité des données.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Données prisonnières. Aucun export global possible.	Export complexe nécessitant un développement technique.	Procédure d'export complète mais manuelle et chronophage.	Réversibilité automatisable nativement comprenant les données et métadonnées).

### AS4-6 : Architecture modulaire et composabilité

Mesure le degré de modularité et d'extensibilité de la solution. Une architecture découpée en briques interchangeable garantit l'agilité, la réutilisation et l'indépendance vis-à-vis d'un fournisseur unique.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Architecture monolithique. Les composants sont étroitement liés. Toute modification locale nécessite un 'fork' ou une altération directe du code source principal.	Modularité limitée. L'architecture permet l'ajout de quelques extensions ou plugins via des interfaces pré-définies, mais le cœur reste rigide et indissociable.	Conception orientée services. La solution est composée de modules fonctionnels indépendants et interchangeables (Microservices ou API-first), facilitant l'adaptation aux besoins métiers.	Écosystème composable et standardisé. Architecture nativement modulaire utilisant des standards ouverts. Chaque composant peut être remplacé ou maintenu par des entités distinctes sans compromettre l'intégrité de l'ensemble.

## AS5 : Coût & Support

Objectif : Garantir la maîtrise financière et l'existence d'un écosystème de services indépendants.

### AS5-1 : Modèle de facturation

Prédictibilité des coûts et absence de frais cachés ou de sortie.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
SaaS captif avec métriques imprévisibles et frais de sortie.	Abonnement avec historique de hausses unilatérales fréquentes.	Licence perpétuelle ou abonnement avec prix fixe contractuel.	TCO maîtrisé. Modèle stable sans frais de sortie ni captivité.

### AS5-2 : Transparence et capacité de projection budgétaire

Évalue la capacité de l'organisation à modéliser le coût total de possession (TCO) de manière autonome. L'objectif est de mesurer la disponibilité de données chiffrées (besoins en serveurs, ressources humaines d'exploitation, infrastructure) permettant d'anticiper les dépenses sans subir les hausses unilatérales d'un fournisseur.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Opacité tarifaire et dépendance. Le modèle repose sur des licences SaaS ou propriétaires avec des métriques de facturation variables et imprévisibles. Historique de hausses unilatérales ou frais cachés (frais de sortie, API payantes) empêchant toute projection fiable.	Visibilité budgétaire limitée. Seuls les coûts directs (licences) sont connus. Les coûts indirects d'infrastructure et de maintenance sont peu documentés, rendant le calcul du TCO complexe et sujet à des erreurs d'estimation importantes.	Directives budgétaires basées sur l'usage. Existence de retours d'expérience (REX) de déploiements actifs fournissant des ratios de haut niveau (ex: nombre d'utilisateur-rires par serveur). Permet de planifier un budget de fonctionnement cohérent mais encore approximatif.	Modélisation capacitaire exhaustive. Disponibilité de données détaillées et publiques couvrant l'intégralité des coûts : dimensionnement matériel (CPU/RAM/Stockage), temps humain nécessaire à l'exploitation (ETP), et coûts de formation. L'organisation peut bâtir un business plan précis et indépendant pour un déploiement à grande échelle.

### AS5-3 : Indépendance et ouverture de l'écosystème de maintenance

Évalue la diversité des acteurs capables d'assurer le support technique et la maintenance corrective. L'objectif est de mesurer le risque de dépendance économique vis-à-vis d'un prestataire unique et la liberté de l'organisation à changer de partenaire de support.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Monopole éditeur. Seul l'éditeur détient les droits et les capacités techniques pour corriger les bugs ou assurer le support. L'organisation subit unilatéralement les tarifs et les délais imposés.	Marché fermé ou captif. Le support est délégué à un réseau restreint de partenaires strictement contrôlés par l'éditeur. La concurrence est limitée et les méthodes d'intervention restent opaques ou propriétaires.	Marché concurrentiel régulé. Plusieurs prestataires indépendants et certifiés sont présents sur le marché. L'organisation peut changer de partenaire de support, bien que l'accès aux correctifs de bas niveau (bugs critiques) dépende encore d'une validation finale de l'éditeur.	Écosystème ouvert et souverain. Le code étant libre et la documentation publique, n'importe quelle ESN ou l'équipe interne peut assurer la maintenance complète (y compris corrective). La concurrence est large, garantissant une maîtrise des coûts et une pérennité indépendante de l'éditeur d'origine.

### AS5-4 : Qualité de la documentation et autonomie d'exploitation

Évalue la richesse des ressources techniques permettant l'installation, la configuration et le maintien en condition opérationnelle (MCO) de la solution. L'objectif est de mesurer la capacité des équipes internes à devenir autonomes sans dépendre systématiquement du support éditeur.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Documentation inexistante ou cryptique. Le fonctionnement interne de la solution est une 'boîte noire'. Toute intervention technique nécessite l'appel à l'éditeur, créant une dépendance opérationnelle totale.	Documentation sommaire, fragmentée ou obsolète. Les procédures critiques (mise à jour, sauvegarde, debug) sont peu documentées ou nécessitent une ingénierie inverse.	Documentation technique complète et structurée par l'éditeur (Guides AdminSys, API, schémas d'architecture). Elle permet une exploitation efficace.	Patrimoine de connaissances exhaustif, public et contributif (Wiki, documentation officielle détaillée, FAQ communautaire). Présence de ressources d'automatisation et de forums d'entraide actifs permettant de résoudre les incidents complexes en totale autonomie.

### AS5-5 : Disponibilité des compétences sur le marché

Mesure la facilité pour l'organisation de recruter des profils qualifiés ou de trouver des prestataires externes maîtrisant la solution. Un score élevé garantit que l'organisation ne sera pas bloquée par une pénurie de main-d'œuvre spécialisée.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Expertise confidentielle ou de niche. Très peu de professionnels maîtrisent l'outil. Le départ d'un seul collaborateur ou la défaillance d'un prestataire unique met en péril le maintien en condition opérationnelle.	Compétences rares et coûteuses. Quelques experts identifiés, mais le marché est en tension. Le recrutement est long et nécessite souvent des formations spécifiques lourdes après l'embauche.	Expertise établie et accessible. La solution est enseignée dans certains cursus ou maîtrisée par de nombreuses ESN. Il est possible de recruter ou de sous-traiter dans des délais raisonnables.	Standard du marché. La compétence est largement répandue (ex: administrateur Debian, développeur Python). Abondance de profils certifiés et de prestataires en concurrence, garantissant une flexibilité maximale et des coûts de prestation maîtrisés.

### AS5-6 : Ergonomie du produit

Évalue la qualité de l'interface et la proximité avec les standards de l'industrie. Un score élevé permet de réduire les besoins en formation et les risques de rejet de la solution par les collaborateurs.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Interface austère ou obsolète. Ergonomie non conforme aux standards actuels du Web ou du bureau. Nécessite une formation systématique pour chaque nouvel utilisateur-riche sous peine d'incapacité de travail.	Interface complexe ou contre-intuitive. Les flux de travail sont sensiblement différents des habitudes acquises. Risque élevé de baisse de productivité initiale et de forte résistance au changement.	Interface moderne et fonctionnelle. L'ergonomie est soignée et respecte les conventions usuelles. Un utilisateur-riche standard retrouve ses marques avec un temps d'adaptation minimal (auto-formation possible).	Expérience utilisateur-riche de premier plan. L'interface est jugée supérieure ou équivalente aux solutions propriétaires hégémoniques du marché. Intègre des fonctions d'accessibilité (RGAA) et d'aide à la prise en main qui facilitent une adoption immédiate sans formation préalable.

### AS6 : Pérennité & Sobriété

Objectif : Assurer la survie à long terme de la solution et minimiser son impact environnemental.

#### AS6-1 : Vitalité et résilience de l'écosystème

Mesure la pérennité technique à travers l'activité de développement et la diversité des contributeur-rices. Un score élevé garantit que le logiciel évolue face aux menaces de sécurité et ne dépend pas d'un groupe restreint d'individus (facteur de bus).

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Projet moribond. Aucune mise à jour de sécurité depuis plus de 6 mois. La dette technique accumulée rend la solution vulnérable et obsolète à court terme.	Dépendance critique (Facteur de bus = 1). Le développement repose sur un individu seul ou une micro-équipe sans relais. Tout arrêt de leur part entraîne l'arrêt immédiat du support technique.	Communauté active et structurée. Présence de contributeur-rices régulières et cycles de publication documentés. La maintenance est assurée, mais le projet reste majoritairement porté par une seule entité ou un petit noyau de développeur-euses.	Pluralité d'acteurs indépendants (entreprises, fondations, bénévoles) contribuant au code. La gouvernance du développement est décentralisée, garantissant la survie du projet même en cas de retrait d'un-e contributeur-riche majeur-e.

#### AS6-2 : Diversité du financement

Stabilité économique et dépendance financière du projet.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Dépendance critique à un seul donateur ou un seul gros client.	Financement par dette ou capital-risque à court terme (risque de pivot stratégique).	Modèle économique diversifié (services, licences, fondations).	Financement pérenne, distribué et indépendant d'un seul acteur.

**AS6-3 : Éco-conception et efficacité matérielle**

Mesure l'optimisation du logiciel et son empreinte sur les ressources (CPU, RAM, stockage). Une solution sobre permet de retarder le renouvellement du matériel (limitation des déchets électroniques) et réduit la consommation énergétique globale.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Logiciel obèse. Consommation de ressources disproportionnée par rapport aux fonctionnalités. Exige systématiquement du matériel de dernière génération pour fonctionner de manière fluide.	Optimisation limitée. Pas de prise en compte des principes d'éco-conception. La consommation énergétique est élevée et le logiciel présente des fuites de ressources (ex: fuites mémoire) non corrigées.	Code optimisé et stable. La solution fonctionne correctement sur du matériel standard ou reconditionné. L'éditeur communique sur l'optimisation des performances et la réduction de l'empreinte carbone du produit.	Sobriété native. Logiciel conçu pour une efficacité maximale. Capacité à s'exécuter sur des configurations anciennes sans dégradation de l'expérience utilisateur-riche.

**AS6-4 : Conformité et accessibilité numérique**

Évalue l'accessibilité de l'interface pour les personnes en situation de handicap (visuel, auditif, moteur). Un score élevé garantit l'inclusivité de l'outil et la conformité aux obligations légales (RGAA en France, EN 301 549 en Europe).

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Inaccessible. L'interface ne supporte aucun outil d'assistance (lecteurs d'écran, navigation clavier seule). Absence totale de contraste ou d'alternatives textuelles.	Accessibilité partielle et non documentée. Quelques efforts sur les contrastes, mais les flux de travail critiques (formulaires, menus complexes) restent bloquants pour de nombreux-se utilisateur-rices.	Bon niveau d'accessibilité. La solution respecte les principes de base des WCAG ou du RGAA. L'interface est largement compatible avec les technologies d'assistance, bien que quelques fonctions avancées nécessitent des ajustements.	Exemplarité et conformité totale. La solution dispose d'une déclaration de conformité (VPAT ou audit RGAA) avec un taux proche de 100%. L'accessibilité est intégrée dès la conception et l'interface est nativement inclusive.

**AS6-5 : Rétro-compatibilité**

Mesure la capacité du produit à maintenir son fonctionnement sur des infrastructures existantes et à garantir la stabilité des interfaces lors des mises à jour. Une forte rétro-compatibilité protège contre l'obsolescence subie et réduit les coûts de migration forcée.

0 - Non-Autonomie	1 - Risque Élevé	3 - Risque Mitigé	5 - Contrôlé
Obsolescence rapide : Pas de support des versions antérieures. Les mises à jour imposent systématiquement une montée de version matérielle ou une rupture des interfaces (API/données).	Support court terme : Rétro-compatibilité limitée à la version immédiatement précédente. Cycle de vie des versions inférieur à 2 ans, forçant des migrations fréquentes et coûteuses.	Stabilité garantie : Existence de versions à support étendu garanties sur plusieurs années. Compatibilité ascendante maintenue pour les fonctions critiques.	Continuité et sobriété : Engagement de compatibilité sur le matériel ancien (Low-tech) et maintien strict de la compatibilité des API/données sur le très long terme (10 ans+).

## 4.4. Interprétation et limites : distinguer souveraineté et performance

Il est fondamental de dissocier la note IAS de la qualité intrinsèque d'une solution. L'IAS mesure l'autonomie stratégique que peut exercer l'organisation vis-à-vis de l'utilisation d'une solution, et non la performance fonctionnelle ou l'expérience utilisateur-rice.

Une note faible ne signifie pas que le produit est mauvais ou inefficace. Elle signale une dette d'indépendance.

Cette distinction est cruciale pour la lecture des résultats :

- **Le cas du standard du marché** : Une solution propriétaire dominante sur le marché (type Microsoft 365) peut offrir des fonctionnalités supérieures ou une meilleure ergonomie, tout en obtenant un score IAS quasi nul. Cela indique que l'usage de cet outil, bien que confortable, place l'organisation dans une situation de dépendance forte, qu'elle soit subie ou consentie.
- **Le choix éclairé** : L'objectif de l'IAS n'est pas d'interdire dogmatiquement les solutions ayant un score faible, mais de transformer une dépendance invisible en un risque géré. Si une solution à faible score est retenue pour des raisons opérationnelles impératives (absence d'alternative crédible), ce choix devient une **prise de risque acceptée** qui devra être documentée et potentiellement compensée par d'autres mesures de sécurité en s'attardant sur la lecture approfondie du score selon chaque pilier.

Ainsi, l'IAS ne juge pas la pertinence métier de l'outil, mais calcule le coût politique et stratégique de son adoption pour une organisation.

## 5. État des lieux de l'architecture du poste de travail bureautique

Ce chapitre vise à dresser un bilan technique et fonctionnel de l'architecture de gestion classique autour d'un poste de travail bureautique. Il cherche à identifier les dépendances critiques et les mécanismes structurants, permettant de comprendre le mode de gestion du parc informatique afin de pouvoir identifier les dépendances et explorer des alternatives permettant de garantir l'autonomie stratégique de l'organisation.

L'analyse se focalise ici sur l'environnement Windows car c'est le système d'exploitation bureautique le plus représenté sur le marché. Sa position est estimée à plus de 70 % des parts de marché mondiales, ce qui permet à l'éditeur d'imposer ses choix stratégiques aux organisations. Cette domination ne se limite pas au système d'exploitation en lui-même, mais structure l'intégralité de l'écosystème de gestion de parc et de collaboration, rendant l'étude de son architecture indispensable pour identifier les leviers d'actions.

### 5.1. Cartographie des briques actuelles

L'infrastructure généralement mise en place s'inscrit de plus en plus dans une logique d'hybridation imposée par Microsoft. Entre les composants historiques On-Premise (Active Directory, SCCM, DFS) et les services cloud de l'écosystème (Microsoft Entra ID, Microsoft Intune, ...).

Cette configuration matérialise la stratégie de transition vers le modèle Cloud First imposée par l'éditeur.

Le schéma ci-dessous modélise l'architecture en distinguant deux sphères logiques :

- **La zone d'administration** : matérialisant l'environnement géré par les administrateur-rices (identité, mécanismes de gouvernance, ...).
- **La zone poste de travail** : matérialisant l'environnement numérique manipulé par les utilisateur-rices (applications, suite bureautique, collaboration, ...).

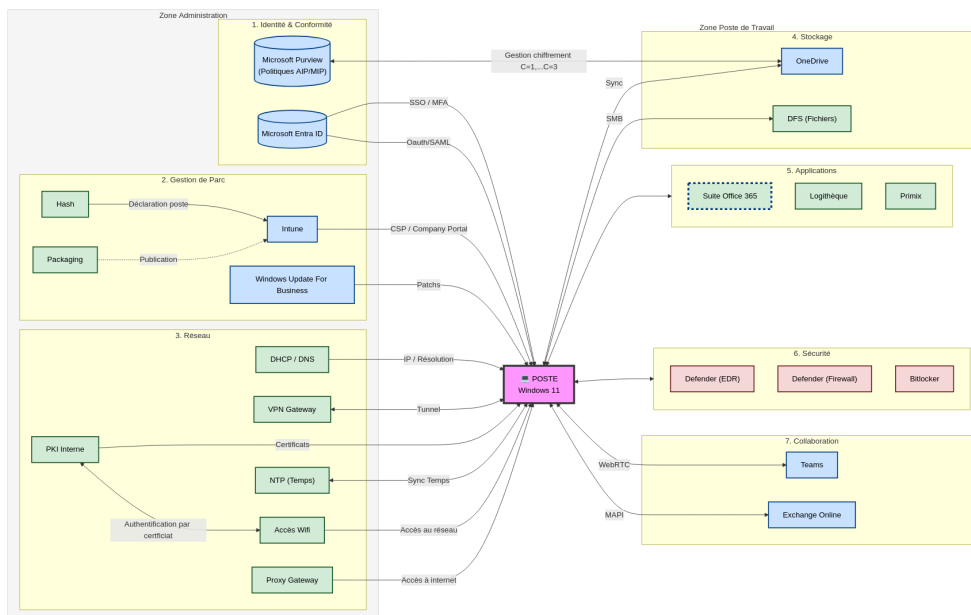


Fig. 2. - Schéma d'architecture global du poste de travail Windows

## 5.2. Découpage en briques fonctionnelles

Nous pouvons identifier sept blocs logiques permettant de représenter les briques fonctionnelles essentielles s'architecturant autour d'un poste de travail.

### 5.2.1. Identité & Conformité

Ce bloc a pour rôle de :

- **Authentifier** les utilisateur-rices et les machines.
- **Autoriser** l'accès aux ressources
- **Gouverner la donnée** en appliquant des étiquettes de sensibilité qui suivent l'information partout où elle transite.

#### Microsoft Entra ID

IAS : 39 / 100

Origine : USA 🇺🇸

Licence : Propriétaire

Modèle Économique : SaaS (Abonnement)

#### Analyse IAS :

- **Données (0,7/5)** : Soumis au droit américain (*CLOUD Act*, *FISA*). Hébergement sur *Azure*. Les clés de l'identité sont gérées par l'éditeur.
- **Gouvernance (1/5)** : Entreprise états-unienne. Feuille de route décidée unilatéralement, évolutions parfois subies et forcées.
- **Licence (0/5)** : Code fermé. Aucun audit indépendant possible.
- **Interopérabilité (3,5/5)** : Basé sur des standards ouverts (*SAML*, *OIDC*), mais réversibilité complexe (enfermement propriétaire fort).
- **Coût (3/5)** : Modèle *SaaS* captif. Les fonctions de sécurité avancées nécessitent des licences coûteuses.
- **Pérennité (3,5/5)** : Solide financièrement.

*Entra ID est l'outil d'authentification et d'autorisation de Microsoft. Son score IAS est critique : en effet, confier les clés de chiffrement des identités numériques à un acteur soumis à une juridiction extra-européenne expose tout le système d'information.*

### 5.2.2. Gestion de parc et maintien en condition opérationnelle

Ce bloc assure le cycle de vie technique du poste de travail. Il remplit trois fonctions clés :

- L'**enrôlement** initial du matériel dans le système d'information.
- La **configuration** des paramètres du système d'exploitation (stratégies de sécurité, réglages).
- La **distribution** des mises à jour logicielles et des correctifs de sécurité (patch management).

## Microsoft Windows 11

**IAS : 38 / 100****Origine :** USA 🇺🇸**Licence :** Propriétaire**Modèle Économique :** Coût par machine (Abonnement)

### Analyse IAS :

- **Données (0,34/5)** : Collecte native de données télémétriques et diagnostiques vers les serveurs de l'éditeur. Soumission au cadre légal américain (*FISA*, *CLOUD Act*) permettant l'accès aux données par les autorités fédérales.
- **Gouvernance (0,34/5)** : Contrôle unilatéral des évolutions par une société cotée. Les mises à jour de fonctionnalités et l'intégration de services tiers (publicité, IA) sont souvent imposées sans consentement explicite de l'utilisateur·rice.
- **Licence (0/5)** : Système au code source fermé. Interdiction totale d'audit indépendant approfondi, de modification du noyau ou de redistribution d'une version allégée.
- **Interopérabilité (2,5/5)** : Écosystème applicatif conséquent mais non portable, créant une forte captivité (enfermement propriétaire).
- **Coût (3,67/5)** : Coûts d'acquisition souvent masqués ou prévisibles. L'écosystème de support est largement implanté, facilitant la maintenance malgré la complexité du système.
- **Pérennité (1,5/5)** : Obsolescence matérielle programmée via des prérequis stricts (CPU récents, *TPM 2.0*) excluant un parc informatique fonctionnel. Consommation élevée de ressources système par rapport aux alternatives légères.

*Windows est le système d'exploitation bureautique leader sur le marché. Cependant, son adoption impose une télémétrie active, et une dépendance envers les décisions stratégiques de Microsoft, comme par exemple pour l'obsolescence de millions de terminaux lors de la bascule vers Windows 11.*

## Microsoft Intune

**IAS : 38 / 100****Origine :** USA 🇺🇸**Licence :** Propriétaire**Modèle Économique :** SaaS (Abonnement)

### Analyse IAS :

- **Données (0,7/5)** : Soumis au droit américain (*CLOUD Act*). Hébergement sur Azure (non souverain). Télémétrie des terminaux et clés de chiffrement gérées par l'éditeur.
- **Gouvernance (1/5)** : Stratégie décidée unilatéralement. Dépendance aux cycles de vie Microsoft.
- **Licence (0/5)** : Code fermé, impossible à auditer indépendamment.
- **Interopérabilité (3/5)** : Pilotage possible via l'API Microsoft Graph. La réversibilité implique souvent la réinitialisation des appareils (enfermement propriétaire).

- **Coût (3/5)** : Modèle de rente, les licences sont souvent incluses dans les abonnements (E3/E5) liés aux postes.
- **Pérennité (3,5/5)** : Solide financièrement.

*Intune est la solution centralisée préconisée par Microsoft pour la gestion des terminaux sous système d'exploitation Windows. La gestion via Intune implique une télémétrie forcée. Le contrôle sur les mises à jour est limité, réduisant l'autonomie opérationnelle.*

### 5.2.3. Socle réseau

Il s'agit des services de bas niveau indispensables à la communication.

- Les services de **résolution et d'adressage** (DNS/DHCP) permettent au poste de se connecter au réseau.
- La **gestion du temps** (NTP) est nécessaire pour la coordination des services d'authentification ainsi que pour la traçabilité des actions
- La **cryptographie** (PKI) fournit les certificats nécessaires au chiffrement des flux et à l'authentification forte.

### 5.2.4. Stockage distant

Ce bloc gère la conservation du patrimoine informationnel. L'architecture actuelle tend à scinder ce rôle en deux :

- Le **stockage personnel synchronisé**, permettant la mobilité de l'utilisateur·rice (accès aux fichiers depuis n'importe quel terminal).
- Le **stockage partagé**, structurant les dossiers d'équipe et les archives de l'organisation.

#### Microsoft OneDrive

IAS : 42 / 100

**Origine** : USA 🇺🇸

**Licence** : Propriétaire

**Modèle Économique** : SaaS (Abonnement + Stockage)

#### Analyse IAS :

- **Données (0,7/5)** : Soumis au droit américain (CLOUD Act). Hébergement sur l'infrastructure Azure. Chiffrement géré par Microsoft.
- **Gouvernance (1/5)** : Stratégie produit décidée unilatéralement par Microsoft. Intégration forcée avec Teams, SharePoint.
- **Licence (0/5)** : Code fermé.
- **Interopérabilité (4/5)** : La récupération des fichiers peut être automatisable, mais la réversibilité des métadonnées (partages, historique) peut s'avérer complexe.
- **Coût (3/5)** : Modèle de rente, abonnement via licences individuelles.
- **Pérennité (3,5/5)** : Pérennité financière. Impact environnemental fort (réplication des données).

*OneDrive est la solution de stockage et partage des données de Microsoft. Le stockage des données sur des clouds publics (Microsoft) pose des problèmes majeurs de juridiction et de confidentialité (chiffrement géré par l'hébergeur).*

### 5.2.5. Applications (outillage métier)

Ce bloc représente la couche de productivité. Son rôle est de mettre à disposition les exécutables nécessaires au travail quotidien.

#### Suite bureautique Microsoft

**IAS : 39 / 100**

**Origine :** USA 🇺🇸

**Licence :** Propriétaire

**Modèle Économique :** SaaS (Abonnement)

#### Analyse IAS :

- **Données (0,67/5) :** Assujettissement de l'éditeur au CLOUD Act, FISA. Même en usage local, la télémétrie et l'incitation forte au stockage cloud (OneDrive) exposent les données aux juridictions américaines.
- **Gouvernance (0,34/5) :** Pilotage commercial unilatéral sans droit de regard des utilisateur·rices. Les choix d'interface et de fonctionnalités sont imposés, parfois au détriment des habitudes de travail établies.
- **Licence (0/5) :** Code source fermé et propriétaire.
- **Interopérabilité (2,5/5) :** Formats de fichiers techniquement ouverts mais dont la complexité et les spécificités d'implémentation compliquent la compatibilité parfaite avec les suites alternatives. Forte adhérence technique liée aux macros (VBA).
- **Coût (3,67/5) :** Bascule progressive vers un modèle de rente (abonnement) augmentant le coût sur le long terme. Le marché du support est néanmoins très étendu et mature.
- **Pérennité (2/5) :** L'inflation des besoins en ressources matérielles et l'intégration de fonctionnalités d'intelligence artificielle alourdissent l'empreinte environnementale de ces produits.

*La suite bureautique de Microsoft propose une gamme de produits complète pour l'édition de documents, cependant son adoption entérine une dépendance forte aux formats de données propriétaires (VBA).*

### 5.2.6. Sécurité

Ce bloc agit directement sur le poste. Il assure :

- L'**intégrité du système** via le chiffrement du disque (protection contre le vol physique).
- La **surveillance comportementale** (Endpoint Detection and Response (EDR)) pour détecter et bloquer les processus malveillants en temps réel.
- Le **filtrage des flux** entrants et sortants (*firewall* local).

## Microsoft Defender

IAS : 40 / 100

Origine : USA 🇺🇸

Licence : Propriétaire

Modèle Économique : SaaS (Abonnement)

### Analyse IAS :

- **Données (0,7/5)** : Soumis au droit américain (*CLOUD Act*, *FISA*). Hébergement sur Azure. La télémétrie de sécurité (fichiers suspects, métadonnées) est analysée dans le *cloud* Microsoft.
- **Gouvernance (1/5)** : Stratégie unilatéralement décidée par l'éditeur.
- **Licence (0/5)** : Code fermé. Impossible de vérifier comment le moteur traite les données sensibles.
- **Interopérabilité (3/5)** : L'API *Microsoft Graph* est très complète pour l'orchestration. Cependant, les politiques de détection et les règles d'exclusion sont propriétaires : la migration vers un autre EDR nécessite de tout reconstruire.
- **Coût (3/5)** : Modèle basé sur la rente (abonnement).
- **Pérennité (3,5/5)** : Solide financièrement. Impact écologique notable dû à l'analyse comportementale effectuée par les modèles d'intelligence artificielle hébergés sur le *cloud* de Microsoft.

*Microsoft Defender est l'outil de sécurisation des postes proposé par Microsoft. Son score IAS est faible : l'analyse des menaces en temps réel implique l'envoi de métadonnées critiques vers une infrastructure sous juridiction américaine.*

## 5.2.7. Collaboration

Ce bloc fonctionnel est devenu le point d'entrée principal de l'environnement de travail numérique. Il agrège :

- **Les échanges synchrones** : Messagerie instantanée, visioconférence et téléphonie.
- **Les échanges asynchrones** : Messagerie électronique classique (courriel) et gestion de temps (agenda/calendrier).
- **La co-édition** : Capacité à travailler à plusieurs en temps réel sur le même document.

## Microsoft Teams

IAS : 30 / 100

Origine : USA 🇺🇸

Licence : Propriétaire

Modèle Économique : SaaS (Abonnement)

### Analyse IAS :

- **Données (0,67/5)** : Soumission aux lois extra-territoriales américaines (*CLOUD Act*, *FISA*). Le chiffrement est géré par la plateforme, exposant les métadonnées et contenus aux requêtes administratives tierces.
- **Gouvernance (0,33/5)** : Stratégie produit décidée unilatéralement par l'éditeurs

- **Licence (0/5)** : Architecture fermée et code source inaccessible.
- **Interopérabilité (3/5)** : L'API (Microsoft Graph) permet de nombreuses intégrations, contrebalancée par une forte complexité d'extraction des données (conversations, wikis) hors de l'écosystème.
- **Coût (3/5)** : Modèle de rente, coût par licence.
- **Pérennité (2/5)** : Solide financièrement. Le client est gourmand en ressources matérielles accélérant l'obsolescence du parc informatique.

*Microsoft Teams est une plateforme de messagerie instantanée et de collaboration, cependant son adoption implique une dépendance technologique forte et une exposition à l'extraterritorialité du droit américain.*

## Microsoft Exchange Online

IAS : 41 / 100

**Origine** : USA 🇺🇸

**Licence** : Propriétaire

**Modèle Économique** : SaaS (Abonnement)

### Analyse IAS :

- **Données (0,67/5)** : Soumission directe au droit extra-territorial américain (CLOUD Act, FISA). Le chiffrement est géré par l'éditeur, permettant techniquement l'accès ou l'indexation des contenus hébergés.
- **Gouvernance (0,3/5)** : Pilotage centralisé par une société cotée. Les choix d'évolution sont unilatéraux, incluant l'arrêt de protocoles historiques sans validation communautaire.
- **Licence (0/5)** Code source inaccessible. Pas de possibilité d'audit de sécurité indépendant, de modification ou de redistribution autonome.
- **Interopérabilité (4/5)** : Support étendu des standards de messagerie (SMTP, IMAP) et API complète (Microsoft Graph). L'export complet des données reste néanmoins complexe (formats propriétaires PST).
- **Coût (3,67/5)** : Modèle de rente (SaaS) sujet aux évolutions tarifaires. L'écosystème de maintenance est cependant vaste et ouvert, permettant une mise en concurrence des prestataires de support.
- **Pérennité (3,67/5)** : Stabilité financière de l'éditeur assurée. La politique de cycle de vie impose des mises à jour régulières des clients et des protocoles de sécurité.

*Microsoft Exchange Online est une solution de messagerie structurellement inadaptée au traitement de données souveraines en raison de sa juridiction et de son modèle d'hébergement dans le cloud, où les clés de chiffrements ne sont pas gérées par le client.*

### 5.3. Évaluation et conclusion

L'application de notre grille d'évaluation via l'IAS aux briques déployées révèle un score de souveraineté globalement **critique**.

La bascule vers le *Cloud First* opère un transfert de maîtrise significatif vers l'éditeur américain Microsoft, concernant à la fois les identités, les données et les clés de chiffrement.

La dépendance identifiée est double :

1. **Dépendance technologique** : Une adhérence structurelle rendant complexe la reconstruction de l'infrastructure sans briques Microsoft.
2. **Dépendance opérationnelle** : La nécessité quasi-obligatoire d'un accès aux services *cloud* pour administrer le poste au quotidien.

L'autonomie stratégique du poste de travail actuel est, par conséquent, fortement compromise.

### 5.4. Périmètre de l'étude : Définition du « poste de travail bureautique »

Afin de garantir la faisabilité et la pertinence de la recherche d'alternatives, il est nécessaire de circonscrire strictement le périmètre du « poste de travail bureautique ».

L'étude se concentrera sur les composants logiciels en interaction directe avec l'utilisateur·rice ou nécessaires à la maintenance du terminal :

L'étude se concentrera sur les composants logiciels en interaction directe avec l'utilisateur·rice ou nécessaires à la maintenance du terminal :

- **Systeme d'exploitation (OS)** : L'environnement d'exécution (remplacement de Windows).
- **Sécurité du poste** : Protection résidente (EDR) et mécanismes de durcissement.
- **Suite bureautique** : Traitement de texte, tableur et présentation.
- **Collaboration & Communication** : Messagerie (courriel/agenda) et outils de travail collaboratif (chat/visioconférence).
- **Gestion de parc** : Outils de déploiement, de configuration et de maintien en condition opérationnelle.

## 6. Approche théorique d'un projet de migration

---

Le constat de dépendance ayant été établi, la question n'est plus de savoir pourquoi migrer, mais comment piloter cette transformation. Ce chapitre propose une synthèse analytique des retours d'expérience relatifs à la migration vers un poste de travail souverain, basé sur GNU/Linux. Il s'appuie sur la réalisation d'entretiens et l'étude de retours d'expérience d'acteurs ayant réalisé une migration d'un parc informatique Windows vers GNU/Linux. Nous allons nous concentrer ici sur l'analyse des méthodes appliquées au sein d'organisations d'envergure, notamment la Gendarmerie nationale [31], diverses collectivités territoriales françaises, telles que les villes de Fontaine, d'Échirolles [32], de Saint-Martin d'Uriage [33], différentes administrations européennes (Danemark, Allemagne, ...) [34], ainsi que la gestion du parc informatique GNU/Linux chez EDF [35]. Au-delà de l'identification de facteurs clés de succès, cette analyse s'attache spécifiquement à isoler les déterminants structurels et humains qui permettent de prémunir le projet contre l'échec [36], [37], [38], [39], [40].

### 6.1. Opportunités et modèles économiques

L'analyse économique d'une migration vers des solutions libres ne saurait se limiter à la simple soustraction des coûts de licences propriétaires. Si la réduction des dépenses de fonctionnement est une réalité constatée dans la quasi-totalité des organisations ayant franchi le pas, elle doit être appréhendée à travers le prisme du coût total de possession (TCO). L'économie réalisée n'est pas une fin en soi, mais le résultat d'une réallocation stratégique des ressources : le budget quitte la rente logicielle pour investir dans le capital humain et la pérennité du système d'information.

#### 6.1.1. De la dépense de licence à l'investissement humain

Les retours d'expérience, notamment celui de la Gendarmerie nationale, font état d'une baisse significative du TCO, estimée à environ 40 % sur la durée. La collectivité d'Échirolles estime quant à elle une économie de plus de 400.000€ par an pour environ 1000 agent-es. Cette économie structurelle repose sur deux leviers principaux. Le premier : la suppression des coûts de licences (système d'exploitation, antivirus, suite bureautique) génère une marge de manœuvre budgétaire immédiate. Le second est lié à la sobriété numérique : la moindre exigence matérielle des distributions GNU/Linux permet d'allonger la durée de vie des postes de travail, réduisant ainsi la fréquence de renouvellement du parc et l'empreinte carbone associée.

Cependant, cette « gratuité » du code ne signifie pas l'absence de coûts. La migration implique un transfert de charges vers l'investissement intellectuel. Les économies réalisées sur les licences doivent être réinjectées, au moins partiellement, dans l'expertise technique. L'administration d'un parc Linux, bien que souvent plus stable et automatisable, requiert des compétences pointues qui peuvent être plus onéreuses sur le marché du travail que celles liées aux environnements Microsoft standardisés. Le modèle économique bascule donc d'une logique de consommation de produits, dites dépenses d'exploitation (OpEx), vers une logique de construction de compétences et de maîtrise interne, dites dépenses d'investissement (CapEx).

## 6.1.2. Le piège de la réduction des coûts comme objectif unique

Il est primordial de souligner qu'une migration dont le moteur principal serait la réduction budgétaire s'expose à un risque élevé d'échec. Si l'économie est un effet de bord bénéfique de l'opération, elle ne doit pas en constituer la genèse.

Une approche purement comptable tend à sous-estimer les coûts cachés de la conduite du changement (formation, accompagnement, baisse temporaire de productivité) et à négliger l'investissement nécessaire dans l'écosystème. Les organisations qui réussissent leur transition sont celles qui visent avant tout la souveraineté, la sécurité et l'adaptabilité de leur système d'information. L'argument économique sert alors à justifier la viabilité du projet auprès des décideurs financiers, mais ne dicte pas la stratégie opérationnelle.

## 6.1.3. Financement et pérennité de l'écosystème libre

L'adoption de logiciels libres par des organisations d'envergure pose inévitablement la question de la pérennité de ces solutions. Contrairement au modèle des logiciels propriétaires où le financement est garanti par la rente, via la vente de licences, le modèle de financement des logiciels libres repose sur des logiques de contribution et de communs. Pour garantir la qualité et la sécurité des outils qu'elle utilise, l'organisation doit passer du statut de consommateur à celui de contributeur.

Ce financement de l'écosystème peut prendre plusieurs formes, qui doivent être intégrées au budget de la DSI :

1. La contribution : Détacher du temps de travail des développeur·euses et administrateur·rices internes pour contribuer au code source, à la documentation ou au rapport de bugs des projets amonts utilisés au sein du SI. Cette contribution directe permet non seulement d'améliorer les outils utilisés, mais aussi de renforcer la communauté autour de ces projets.
2. Le financement : Souscrire à des contrats de support auprès de sociétés de services spécialisées ou à des éditeurs de logiciels libres. Même si le support n'est pas systématiquement sollicité, ce financement agit comme une assurance et permet à ces entreprises de rémunérer les développeur·euses qui maintiennent le code.
3. Le mécénat et les dons : Soutenir financièrement les fondations ou les associations qui portent les projets critiques de l'infrastructure. Une initiative très intéressante à ce sujet est [Copie Publique](#). Ce dispositif propose aux organisations de sanctuariser une part de leur budget informatique pour la redistribuer aux écosystèmes du logiciel libre. La sélection des projets soutenus repose sur des mécanismes de démocratie participative, impliquant directement les salarié·es dans la valorisation du patrimoine numérique qu'ils et elles utilisent au quotidien.

En adoptant cette posture, l'organisation ne se contente pas de réaliser des économies ; elle investit dans la résilience de sa propre chaîne d'approvisionnement logiciel et participe à la consolidation d'un patrimoine numérique en commun. En contribuant à ce patrimoine, l'organisation mutualise les efforts et les coûts de développement (car partagés avec d'autres acteurs), ce qui permet *in fine* de rationaliser et d'optimiser les investissements.

## 6.2. Cadrage stratégique et alignement de la gouvernance

La migration vers un poste de travail GNU/Linux, ne peut être réduite à une substitution technologique ; elle constitue une transformation culturelle majeure qui exige un alignement strict entre la vision politique de l'organisation et sa mise en œuvre opérationnelle. Les nombreux retours d'expérience, démontrent quasi unanimement que le succès de l'opération repose avant tout sur un portage et un sponsor fort de la part de la direction des systèmes d'informations (DSI) et de la présidence et direction générale (PDG) de l'organisation. Cette implication au plus haut niveau est indispensable pour légitimer la démarche de maîtrise des dépendances technologiques visée par l'organisation et éventuellement neutraliser les pressions externes des éditeurs de logiciels propriétaires [41].

## 6.3. Utilisation d'un socle applicatif commun

Si la migration vers un système d'exploitation souverain constitue l'objectif final de l'autonomie technique, la véritable bataille se joue au niveau de la couche applicative. L'analyse des différents projets de migration vers des systèmes d'exploitation permettant de garantir l'autonomie stratégique de l'organisation, comme GNU/Linux, montre qu'il est impératif de dissocier la trajectoire des usages de celle du système, en priorisant la mise en œuvre d'un socle logiciel commun et agnostique sur l'environnement Windows existant. Cette stratégie de découplage ne doit pas être considérée comme une phase préparatoire, mais comme le pivot central de la réduction des risques du projet.

L'unanimité des retours d'expérience démontrent que l'adhérence des utilisateur·rices réside majoritairement dans leurs outils quotidiens - navigateur web, suite bureautique, client de messagerie - plutôt que dans le système d'exploitation lui-même. En généralisant proactivement des solutions libres, respectant des formats interopérables et multiplateformes telles que Firefox, LibreOffice, Thunderbird sur le parc Windows, l'organisation neutralise la dépendance fonctionnelle à Windows bien en amont de la migration technique vers GNU/Linux. Cette approche permet de lisser la courbe d'apprentissage sur plusieurs années et de traiter les problématiques d'interopérabilité (formats de fichiers, macros, polices) sans les cumuler avec les ruptures liées à l'environnement de bureau.

Dès lors, la bascule ultérieure vers un système d'exploitation souverain change de nature : elle cesse d'être une rupture d'usage pour devenir une opération quasi transparente pour un·e utilisateur·rice retrouvant instantanément ses logiciels de travail habituel. La priorité de la DSI doit donc porter sur la standardisation de ce socle applicatif, qui constitue à lui seul le garant de la réversibilité et de l'autonomie stratégique, le système d'exploitation n'étant in fine que le vecteur d'exécution de ces outils.

## 6.4. Gestion de projet

En matière de gouvernance de projet, l'analyse des précédents historiques commande de s'affranchir des indicateurs de performance purement quantitatifs et des calendriers rigides. L'expérience démontre qu'imposer des objectifs chiffrés, tels que des volumes de postes à migrer à date fixe ou des seuils d'économies à court terme, constitue un facteur de risque élevé d'échec du projet. Cette approche dirigiste, souvent déconnectée de la réalité opérationnelle, a été identifiée comme le dénominateur commun de plusieurs échecs de migration ou de surcoûts importants, comme observé dans le cas de la ville de Munich où les pressions temporelles ont conduit à des dérapages budgétaires puis à un retour en arrière vers Windows [42].

La stratégie éprouvée privilégie une cinétique de déploiement sur le temps long. Ce changement de paradigme permet de synchroniser le rythme d'industrialisation avec la maturité numérique des

utilisateur-rices, plutôt que de tenter de forcer l'adoption sous la contrainte d'un planning arbitraire. En laissant le système GNU/Linux devenir la norme par un phénomène de diffusion sociale et de preuve par l'usage au sein des équipes, l'organisation s'assure une transition pérenne où le nouveau standard s'impose de lui-même par sa pertinence opérationnelle et non par la coercition [43].

Pour donner un ordre d'idée de l'inertie de tels projets, dans le cas de la ville d'Échirolles, bien que l'impulsion politique date de 2021 avec le changement de mandature, le déploiement auprès des agent-es n'a débuté qu'en septembre 2024. Ces trois années de maturation ont permis de valider la viabilité technique (choix de la distribution GNU/Linux Zorin OS) au sommet de la hiérarchie, le Directeur Général des Services étant le premier utilisateur dès 2021, avant de l'étendre aux différents services de la commune.

À une échelle plus vaste, la Gendarmerie Nationale a mis près de 10 ans pour stabiliser son parc de plus de 80 000 postes sous GendBuntu. Le projet a été entamé dès 2005 par l'adoption de Firefox et OpenOffice, la migration vers leur propre système (GendBuntu) a été annoncée en 2008 pour atteindre 80% du parc vers 2013-2015. Cependant, il faut bien avoir en tête que l'objectif de ces transitions n'est pas nécessairement d'atteindre le 100% de postes GNU/Linux, certains logiciels métiers spécifiques pouvant encore nécessiter Windows, mais bien de renverser le rapport de force. En démontrant qu'une alternative solide existe et qu'elle est déployable à grande échelle, l'organisation retrouve sa liberté de choix, sa maîtrise budgétaire et, surtout, une indépendance technologique réelle. L'outil informatique redevient un moyen au service de la performance métier, et non plus une contrainte dictée par des intérêts privés.

## 6.5. Gestion du capital humain et traitement des résistances

L'analyse des différents retours révèle que la résistance au changement la plus critique ne provient pas nécessairement des utilisateur-rices finaux, mais paradoxalement des équipes techniques. Le passage à un environnement à base de logiciels libres peut être perçu par les administrateur-ice-s système comme une obsolescence de leurs compétences acquises sur les écosystèmes propriétaires, générant un sentiment de mise en danger professionnelle. La conduite du changement doit donc intégrer un volet ressources humaines (RH) prioritaire, visant à valoriser la montée en compétence sur les technologies libres et à adapter les profils de recrutement pour soutenir cette nouvelle trajectoire technologique.

L'acceptation du changement par les utilisateur-rices finaux ne se décrète pas ; elle se construit par une stratégie de marketing interne visant à rendre le nouvel environnement désirable plutôt que subi. Les retours d'expérience confirment que l'un des leviers d'adhésion les plus efficaces consiste à synchroniser la migration logicielle avec un renouvellement matériel. Cette association psychologique positive permet de présenter le passage à Linux comme une montée en gamme de l'environnement de travail global, et non comme une régression ou une contrainte technique.

Au-delà de l'aspect matériel, l'adhésion se renforce par la démonstration des gains fonctionnels intrinsèques au nouveau système, qui se traduisent par une amélioration directe de la qualité de vie numérique de l'agent-e. La communication doit mettre en exergue des avantages concrets tels que la vitesse supérieure de l'indexation et de la recherche de fichiers au sein de l'explorateur de fichier, ou encore la gestion transparente des mises à jour système qui, contrairement aux environnements Windows, s'exécutent rapidement et ne requièrent que très ponctuellement un redémarrage.

De plus, cette approche pragmatique gagne à être complétée par une dimension porteuse de sens, mobilisant des arguments de responsabilité sociétale et stratégique. La sensibilisation aux enjeux de souveraineté numérique, à la rationalisation des deniers publics (économies de licences, contribution et efforts mutualisés) et à l'impact écologique (allongement de la durée de vie du matériel grâce à la légèreté

du système) permet d'inscrire l'effort individuel d'adaptation dans un projet collectif valorisant. Toutefois, il est impératif que ces arguments de valeurs ne supplantent jamais la finalité première : la capacité du poste de travail à servir le métier. La migration ne peut être considérée comme un succès que si elle garantit, *in fine*, le maintien ou l'amélioration de la capacité opérationnelle des services.

## 6.6. Trajectoire de migration

La méthodologie de déploiement préconisée, issue de l'analyse des pratiques éprouvées par la Gendarmerie nationale et les collectivités de Fontaine et d'Échirolles, s'articule autour d'une progression séquentielle. Cette approche temporelle, qui s'étend sur plusieurs années, est conçue pour atténuer les risques opérationnels et diluer la résistance au changement. Elle se décompose en cinq phases distinctes, allant de l'harmonisation applicative à la généralisation du système d'exploitation GNU/Linux par défaut.

### 6.6.1. Sanctuarisation du socle applicatif commun et indépendance des formats

Comme expliqué précédemment, avant toute trajectoire de migration vers un poste de travail GNU/Linux, une étape préliminaire indispensable consiste à harmoniser le socle logiciel applicatif sur les postes Windows existants. L'idée est de déployer les solutions permettant de garantir l'autonomie stratégique choisies par l'organisation. Ainsi, la bascule définitive du système d'exploitation devient quasiment transparente, ce qui permet de réduire le choc cognitif.

Cette première étape vise à découpler l'environnement de travail de l'utilisateur-riche de la couche système sous-jacente. Il s'agit de permettre à l'organisation de recouvrer la maîtrise de ses données en s'affranchissant des formats de documents propriétaires. En basculant vers des standards ouverts, l'organisation neutralise les adhérences techniques (macros, polices, mises en page) qui constituent habituellement les points de blocage majeurs lors d'une migration de système d'exploitation. La neutralisation de l'adhérence technique sera abordé dans le chapitre 7. Cette étape rend la transition future quasiment transparente pour les utilisateur-rices, dont les outils quotidiens demeurent inchangés quel que soit l'environnement d'exécution.

### 6.6.2. Validation par la preuve

S'ensuit la phase initiale de déploiement effectif de poste de travail GNU/Linux, en se concentrant sur un périmètre restreint. L'objectif est de cibler prioritairement les populations disposant d'une forte appétence technique et d'un rôle décisionnel, comme le management. Cette phase cherche à valider techniquement l'intégration de la distribution GNU/Linux choisie au sein du système d'information et à vérifier son ergonomie. C'est durant cette période que les équipes de la DSI acquièrent la compétence nécessaire à l'administration du nouveau parc et procèdent aux ajustements fins de l'interface pour garantir une expérience optimale.

### 6.6.3. Extension du périmètre et qualification des usages

Suite à la validation technique, le déploiement s'étend à un panel de volontaires, cela peut représenter jusqu'à environ 10% du parc. Cette étape est cruciale pour confronter le poste de travail GNU/Linux à la réalité diversifiée des métiers de l'organisation. En exposant le système à un échantillon représentatif, la DSI est en mesure d'identifier les cas d'usage complexes, les incompatibilités logicielles périphériques

ou les besoins spécifiques non détectés lors du cadrage initial. Cette phase permet de consolider les stratégies de remédiation et de rassurer les futur-es utilisateur-rices grâce à l'existence d'une base installée fonctionnelle et visible au sein de chaque service.

#### 6.6.4. Industrialisation par opportunité de renouvellement

L'industrialisation du déploiement ne s'opère pas par une bascule massive, mais s'inscrit dans le cycle de vie naturel du matériel informatique. Durant cette période, qui dure généralement quatre ans ou plus selon les cycles d'amortissement, chaque renouvellement de poste physique est l'occasion de proposer systématiquement la machine sous GNU/Linux. La stratégie repose ici sur l'incitation plutôt que la contrainte : l'utilisateur-riche conserve la possibilité de refuser et de demander un poste Windows, mais l'association de GNU/Linux avec un matériel neuf et performant favorise son adoption. Cette approche permet de faire monter la charge progressivement, d'atteindre une couverture significative du parc sans heurts, et de mesurer précisément la résistance au changement résiduelle.

#### 6.6.5. Inversion de la norme et gestion des exceptions

La dernière phase intervient lorsque la masse critique d'utilisateur-rices est atteinte et que la maturité de la solution est avérée. La logique de mise à disposition du poste s'inverse alors pour instituer le poste de travail GNU/Linux comme le standard par défaut de l'organisation. Dès lors, l'attribution d'un poste Windows ne relève plus d'un choix mais devient une exception qui doit être formellement justifiée par des impératifs métiers bloquants ou des incompatibilités logicielles insolubles. Généralement les besoins métiers spécifiques nécessitent un maintien autour de 10 % à 15 % des postes Windows pour des usages spécifiques.

Cette méthode de déploiement progressive permet de migrer la majorité de l'organisation vers un environnement GNU/Linux tout en assurant la continuité opérationnelle sans contraindre ni brusquer les utilisateur-rices.

### 6.7. Accessibilité numérique

Cette partie est constituée d'éléments extraits de « Poste de travail Linux : Annexe Accessibilité » écrit par Atos, un livrable de l'activité de veille du marché de support logiciel libre sous le pilotage de la DGFIP disponible [ici](#) utilisé sous licence CC BY-SA 4.0.

L'accessibilité numérique consiste à permettre à toutes et tous, y compris aux personnes en situation de handicap, d'accéder aux services numériques. Ici, cela va concerner la capacité pour les personnes en situation de handicap d'utiliser les environnements de travail GNU/Linux et ainsi de pouvoir utiliser les mêmes logiciels et outils que leurs collègues.

L'aménagement du poste de travail au besoin des personnes en situation de handicap est un aspect fondamental de l'insertion professionnelle. Un aménagement « raté » a des impacts bien plus grands pour une personne en situation de handicap, car il peut l'empêcher de travailler efficacement, de remplir l'intégralité de ses missions ou d'être autonome. L'aménagement des postes de travail pour ce public est régulièrement voir trop souvent négligé.

Il existe plusieurs possibilités pour aménager un poste de travail :

1. L'utilisateur-riche connaît ses besoins et indique les logiciels dont il a besoin ;

2. L'utilisateur-riche et l'entité ont besoin d'être accompagnés, il est possible de faire appel à un tiers. Le tiers peut-être la mission handicap, une entreprise spécialisée, un ergothérapeute, etc.
  - Dans le cas de la Gendarmerie Nationale, par exemple, l'entreprise [Hypra](#) a été sollicitée.

L'adoption d'un poste de travail [GNU/Linux](#) ne saurait se faire au détriment de l'inclusion. Si la migration répond à des impératifs de souveraineté et d'écologie dans le cadre de la responsabilité sociétale des entreprises (RSE), elle doit également garantir l'accessibilité numérique pour toutes et tous. Les environnements de bureau [GNU/Linux](#) modernes intègrent nativement des technologies d'assistance conformes aux standards internationaux (lecteur d'écran [Orca](#), gestion des contrastes élevés, loupe, navigation au clavier). De plus, la nature ouverte des solutions retenues constitue un atout majeur par rapport aux solutions propriétaires : elle offre la possibilité technique d'adapter ou de modifier le code des interfaces pour répondre à des besoins spécifiques de handicap, sans dépendre du bon vouloir ou de la feuille de route d'un éditeur tiers.

Nous vous invitons à lire l'étude d'Atos sur l'accessibilité numérique qui travaille en profondeur cette thématique [44].

Nous pouvons affirmer que l'accessibilité sur Linux a atteint un seuil de maturité permettant son déploiement en milieu professionnel. Cependant, le fonctionnement des technologies d'assistance ne se limite pas au niveau du système d'exploitation, et concerne toute la chaîne applicative : leur disponibilité au niveau du système n'emporte pas nécessairement leur fonctionnement au sein des diverses applications utilisées. Ainsi si les applications les plus communes et utilisées bénéficient d'un bon niveau de support, ce n'est pas le cas de logiciels moins courants, pour lesquels aucune attention particulière n'a été apportée par les éditeurs de ces solutions. En particulier, si l'accessibilité des navigateurs web est globalement satisfaisante, c'est très loin d'être le cas pour les applications et contenus accédés via ces navigateurs.

## 6.8. Continuité de service et blocages techniques résiduels

L'approche dogmatique visant une éradication totale des systèmes propriétaires est à proscrire au profit d'un pragmatisme technique garantissant la continuité des opérations. Il est nécessaire de reconnaître que certaines applications métiers spécifiques, ne disposent pas d'équivalents libres. Pour ces périmètres incompressibles, la DSI peut mettre en œuvre des solutions de virtualisation ou d'accès distant ([VDI](#), usage de protocoles [RDP](#) via des clients comme [Remmina](#)), permettant aux utilisateur-rices d'accéder à leurs applications Windows critiques depuis leur environnement [GNU/Linux](#) de manière transparente.

Cette architecture hybride permet de contourner les blocages techniques sans remettre en cause la stratégie globale de migration. Parallèlement, l'organisation, pour palier ces différents blocages peut arbitrer entre le développement interne de solutions, la collaboration avec les communautés du logiciel libre ou le recours au support d'éditeurs spécialisés. Cette gestion au cas par cas assure que la souveraineté technologique ne se construit pas au détriment de la qualité de service informatique.



Fig. 3. - Feuille de route de la conduite du changement

## 7. Analyse comparative des alternatives

---

La stratégie de migration ayant été définie, sa mise en œuvre opérationnelle nécessite une évaluation rigoureuse des solutions techniques disponibles. Ce chapitre détaille une analyse comparative des différentes familles d'outils, allant du système d'exploitation aux suites collaboratives, afin d'identifier les solutions les plus pertinentes au regard de l'indice IAS.

### 7.1. Systèmes d'exploitation pour les postes utilisateur-rices

Le système d'exploitation est le socle de la pile logicielle d'un poste utilisateur. C'est le composant dont le choix mérite le plus de considération, car la migration de tout un parc informatique est une opération souvent trop coûteuse pour être effectuée plus d'une fois.

L'élément principal de tout OS est son noyau. Dans l'écosystème des OS libres, il existe trois principales familles de noyaux monolithiques : Linux, BSD, et Solaris. Il existe également des noyaux avec une architecture micro-kernel, tel que GNU Hurd. Dans cette section, nous considérons uniquement des OS basés sur le noyau Linux, car il dispose de l'écosystème le plus riche et mature, avec la plus large compatibilité matérielle.

Chaque distribution Linux se distingue par la vision et les choix de ses mainteneurs :

- la façon dont sont articulés l'ensemble des paquets logiciels peut différer ;
- certains paquets logiciels peuvent être nativement installés, parfois avec des personnalisations importantes ;
- les configurations par défaut sont souvent très différentes ;
- les garanties données en termes de stabilité des mises à jour et d'interopérabilité des paquets sont variables.

Concernant ce dernier point, nous avons choisi d'écarter les distributions suivant un modèle de mise à jour continue par rolling release, notamment toutes celles basées sur Arch Linux. Le risque d'instabilité non maîtrisé de cette approche nous semble être trop coûteux opérationnellement pour envisager des déploiements à grande échelle. Inversement, les distributions suivant un modèle de mises à jour ponctuelles par releases versionnées paraissent appropriées. Ce fonctionnement permet de concentrer temporellement les risques et efforts liés aux montées de versions, et de bénéficier de stabilité le reste du temps. Ce modèle n'empêche pas de continuer à recevoir les correctifs de sécurité des différents paquets logiciels, car ceux-ci sont typiquement rétroportés par les mainteneurs des distributions Linux. Dans ce cas de figure, un facteur de décision important est la durée pendant laquelle chaque version de l'OS est maintenue et continue de recevoir des correctifs. Selon les éditeurs et les versions, cette durée peut s'étendre de plusieurs mois à plusieurs années. Plus elle est longue, plus la stabilité du parc informatique et la marge de manœuvre pour les montées de version sont grandes.

#### 7.1.1. Debian

Debian est une distribution Linux créée en 1993, réputée pour sa stabilité et son adhésion stricte aux principes du logiciel libre. Elle est développée par le projet Debian, une communauté internationale financée par des dons et constituée intégralement de bénévoles.

## Debian

IAS : 93 / 100

**Éditeur** : The Debian Project

**Origine** : Internationale 🌐

**Licence** : DFSG

**Modèle Économique** : Dons

### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (3/5)** : Le projet Debian n'est pas soumis à une juridiction précise : il s'agit d'une communauté distribuée internationalement. Ses seules racines juridiques sont celles des organisations à but non lucratif à travers lesquelles les dons sont perçus (par exemple Debian France ou Software in the Public Interest, Inc). Ces organisations n'ont pas d'influence sur la gouvernance [45]. Les infrastructures de construction et de distribution des paquets logiciels sont également répartis internationalement, avec une bonne partie localisée aux États-Unis, mais aussi en Europe, et plusieurs miroirs existent en France [46]. La nature internationale du projet Debian lui donne les moyens de se prémunir contre les pressions légales d'un état spécifique. Debian n'envoie pas de télémétrie, il n'y a pas de traitement de quelconques données utilisateur.
- **AS2 | Gouvernance (5/5)** : Le projet Debian est une communauté sans motivation financière gérée par des bénévoles. Le projet suit un modèle démocratique dans lequel les décisions sont prises collectivement par ses membres, et documentées publiquement [45]. N'importe qui peut devenir contributeur [47]. Le projet ne sert les intérêts d'aucune entreprise spécifique.
- **AS3 | Licence & Ouverture (5/5)** : Les composants de Debian sont tous placés sous des licences libres suivants les Debian Free Software Guidelines (DFSG) [48]. Les sources sont auditables, modifiables, et redistribuables, sans restrictions. Les processus sont également transparents : les développements et les suivis des vulnérabilités sont publiquement accessibles.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : Le format deb utilisé pour la gestion des paquets logiciels est le format le plus vaste de l'écosystème Linux. Il est souvent supporté nativement par les éditeurs tiers qui fournissent des logiciels compatibles avec Linux. Les miroirs Debian qui servent des paquets sont accessibles gratuitement.
- **AS5 | Coût & Support (5/5)** : Debian a toujours été gratuit et a pour objectif de le demeurer [48]. La documentation officielle est riche [49], et se présente sous différentes formes : manuels, wiki, forum. C'est une distribution Linux mature et répandue, rendant sa maintenance très accessible via du personnel interne, ou avec du support tiers chez toute ESN compétente.
- **AS6 | Pérennité & Sobriété (5/5)** : Le projet Debian est très dynamique et possède plus de mille contributeurs actifs [50]. Le projet est soutenu financièrement et matériellement [51] par de nombreuses entreprises et individus. Les paquets logiciels sont maintenus à jour. Les versions majeures de l'OS sont maintenues pendant trois ans, avec deux ans supplémentaires en LTS. Il est également possible de payer les prestations d'une entreprise tierce française, Freexian, qui propose une offre appelée Extended LTS allongeant la durée de vie des versions majeures de cinq ans supplémentaires [52]. Debian a une très large compatibilité matérielle, permettant l'exploitation d'ordinateurs âgés, notamment via la prise en charge des architectures CPU 32 bits [53]. Une

installation avec environnement de bureau nécessite 2 Go de mémoire (2x moins que Windows 11), et 10 Go de stockage (6x moins que Windows 11) [54].

*Debian est le choix de la stabilité et du logiciel libre. C'est l'un des OS les plus indépendants politiquement et commercialement. Les infrastructures actuelles de construction des paquets logiciels sont partiellement localisées dans des pays hors de l'Union Européenne, mais n'en sont pas dépendantes pour autant. Debian a une très vaste compatibilité matérielle, lui permettant d'étendre la durée de vie des machines. C'est un système très généraliste, qui demande donc un effort initial de configuration pour lisser l'expérience utilisateur. C'est l'OS idéal pour un parc géré par une équipe technique compétente.*

## 7.1.2. openSUSE

openSUSE est une distribution Linux communautaire parrainée par l'entreprise allemande SUSE Software Solutions Germany GmbH. Elle possède plusieurs déclinaisons : stable, rolling release, avec ou sans immutabilité. L'entreprise propose sa propre alternative non communautaire payante, appelée SUSE Linux Enterprise, donnant accès à des services et support professionnels.

### openSUSE

IAS : 84 / 100

**Éditeur** : SUSE Software Solutions

**Origine** : Allemagne 🇩🇪 / Suède 🇸🇪

**Licence** : GPLv2

**Modèle Économique** : Parrainage

#### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (3/5)** : La politique du projet openSUSE impose que son président soit un employé de l'entreprise SUSE [55]. Les infrastructures de construction et de distribution des paquets logiciels appartiennent à SUSE et sont principalement localisées en Allemagne, avec des miroirs à l'international, dont en France [56]. L'OS n'envoie pas de télémétrie, il n'y a pas de traitement de quelconques données utilisateur.
- **AS2 | Gouvernance (2.7/5)** : Bien que le projet openSUSE soit communautaire et sans but lucratif, il est très dépendant de SUSE, qui est une entreprise privée. Cette dépendance est présente aussi bien au niveau des infrastructures qu'au niveau du conseil d'administration du projet, partiellement constitué de membres de SUSE [55]. L'entreprise est détenue par EQT AB [57], un fonds d'investissement suédois coté en bourse. Ces liens ont un impact sur le soutien financier du projet, mais n'influencent pas les décisions guidant la direction du projet, qui sont prises de façon communautaire et démocratique [58], et sont publiquement documentées. N'importe qui peut devenir nouveau contributeur.
- **AS3 | Licence & Ouverture (5/5)** : openSUSE est sous licence GPLv2 [59], garantissant que ses sources sont auditables, modifiables, et redistribuables, sans restrictions.

- **AS4 | Interopérabilité & Réversibilité (5/5)** : Le format RPM utilisé pour la gestion des paquets logiciels est un format très répandu dans l'écosystème Linux, développé par Red Hat. Les miroirs openSUSE qui servent ces paquets sont accessibles gratuitement.
- **AS5 | Coût & Support (5/5)** : openSUSE a toujours été gratuit et a pour objectif de le demeurer [55]. Plusieurs sources de documentation sont disponibles sous différentes formes : wiki, manuels, forum. L'accessibilité de ces ressources permet à n'importe quel technicien ou ESN d'acquérir les compétences nécessaires au maintien de cet OS. De plus, l'entreprise SUSE propose sa propre alternative payante avec support professionnel, appelée SUSE Linux Enterprise.
- **AS6 | Pérennité & Sobriété (4.5/5)** : Le projet openSUSE possède une grande base communautaire contribuant à son développement, ainsi qu'une participation continue de l'entreprise SUSE. Le projet est parrainé matériellement et financièrement par neuf entreprises dont SUSE [60]. Les individus peuvent aussi faire des dons matériels. Les paquets logiciels sont maintenus à jour. De nouvelles versions de l'OS sortent tous les ans, et sont toutes maintenues pendant 2 ans. Les ressources recommandées officiellement pour une installation openSUSE avec environnement de bureau sont 2 Go de mémoire (2x moins que Windows 11) et 8 Go de stockage (8x moins que windows 11) [61].

*openSUSE est un choix qui va dans le sens du logiciel libre et européen, accompagné d'une ouverture sur une alternative payante avec support professionnel. L'OS se distingue aussi par la présence native d'outils d'administration uniques au projet : YaST, qui offre une interface d'administration graphique, et Snapper, qui facilite la prise et restauration de snapshots.*

### 7.1.3. Fedora

Fedora est une distribution Linux communautaire parrainée par l'entreprise américaine Red Hat. Elle possède plusieurs déclinaisons, dont certaines immutables (les éditions Atomic Desktop). Red Hat propose sa propre alternative commerciale basée sur Fedora, appelée Red Hat Enterprise Linux (RHEL), donnant accès à du support professionnel étendu.

#### Fedora

IAS : 69 / 100

**Éditeur** : Red Hat

**Origine** : États-Unis 🇺🇸

**Licence** : MIT

**Modèle Économique** : Parrainage

#### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (0/5)** : Le projet Fedora est parrainé par l'entreprise Red Hat, elle-même détenue par IBM. Les infrastructures de construction des paquets logiciels sont celles de Red Hat, et sont donc principalement localisées aux États-Unis. Des miroirs existent dans le monde et notamment en France, mais cela ne change pas l'origine des paquets. Le système n'envoie aucune télémétrie par défaut.

- **AS2 | Gouvernance (1.7/5)** : Le projet Fedora est communautaire, mais il est très dépendant de Red Hat, une entreprise privée détenue par IBM, qui est coté en bourse. Cette dépendance est très forte au niveau des finances et des infrastructures, et elle est partielle au niveau de la gouvernance. Le charte du Conseil de Fedora impose que la position de chef et quelques autres positions du conseil soient occupées par des employés de Red Hat [62]. Néanmoins, D'autres positions du conseil sont tenues par des membres de la communauté, et les décisions guidant le projet sont prises de façon collective et transparente. Les nouveaux contributeurs sont les bienvenus [63].
- **AS3 | Licence & Ouverture (5/5)** : Fedora est sous licence MIT [64], garantissant que ses sources soient auditables, modifiables, et redistribuables, sans restrictions.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : Fedora utilise le format RPM pour ses paquets logiciels. Ce format a été créé par Red Hat, et a une grande couverture dans l'écosystème Linux. Les miroirs distribuant ces paquets logiciels sont accessibles gratuitement.
- **AS5 | Coût & Support (5/5)** : Fedora est gratuit, et a pour objectif de le rester [65]. Des ressources et documentations en tout genre sont disponibles : wiki, manuels, forum. De plus, il s'agit d'une distribution dont l'utilisation est répandue. Ces éléments en font une distribution pour laquelle il n'est pas difficile de trouver du personnel ou des ESN qualifiées pour la maintenir. En outre, l'entreprise Red Hat propose sa propre alternative payante avec support professionnel, appelée Red Hat Enterprise Linux (RHEL).
- **AS6 | Pérennité & Sobriété (4/5)** : Le projet Fedora a une communauté large et active de contributeurs, soutenue par la participation continue de l'entreprise Red Hat. Le projet est parrainé par une dizaine d'entreprises, dont la plus impliquée est naturellement Red Hat [66]. Les paquets logiciels sont maintenus à jour. Une nouvelle version majeure de Fedora sort tous les 6 mois, et chacune d'entre elles est maintenue pendant 13 mois [67]. Les ressources matérielles minimum recommandées pour une installation Fedora sont 2 Go de mémoire (2x moins que Windows 11) et 15 Go de stockage (4x moins que Windows 11) [68].

*Fedora, et son alternative payante RHEL, sont des distributions réputées de qualité pour les entreprises. Fedora possède certains avantages intéressants par rapport à d'autres distributions, notamment sa prise en charge native des politiques de sécurité SELinux. Ses cycles de release relativement courts donnent l'avantage des logiciels plus récents, mais au coût d'une certaine stabilité. De façon générale, les points forts de cet OS sont à pondérer avec les coûts non négligeables en matière de souveraineté causés par ses racines juridiques américaines.*

## 7.1.4. Ubuntu

Ubuntu est une distribution Linux basée sur Debian. Elle est développée par l'entreprise britannique Canonical Ltd, avec des contributions communautaires. Canonical propose des services payants donnant accès à du support étendu et à du conseil professionnel.

### Ubuntu

IAS : 52 / 100

Éditeur : Canonical

Origine : Royaume-Uni 

**Licence :** Multiples

**Modèle Économique :** Freemium

**Analyse IAS :**

- **AS1 | Maîtrise Données & Juridiction (0/5) :** Ubuntu est développé par l'entreprise britannique Canonical Group Ltd. Le Royaume-Uni est concerné par le «US-UK Data Access Agreement», un accord conclu en 2022 sous l'égide du CLOUD Act américain. L'entreprise possède une filiale appelée « Canonical USA Inc. » qui est basée aux États-Unis, ce qui renforce ses liens avec la juridiction américaine. Les infrastructures de construction des paquets logiciel au format deb sont celles de leur service appelé Launchpad, principalement localisé au Royaume-Uni. Les infrastructures du Snap Store dépendent quant à elles lourdement de fournisseurs cloud publics américains.
- **AS2 | Gouvernance (1.3/5) :** Ubuntu est développé par Canonical, une entreprise privée qui n'appartient à aucune organisation parente, et qui est donc en pleine possession de ses finances et arbitrages. Les décisions faisant avancer Ubuntu sont prises collectivement au sein de différents comités communautaires [69], et leurs échanges sont publiquement accessibles. Néanmoins, Canonical se réserve le droit d'arbitrage final, et a déjà imposé des décisions unilatérales par le passé, comme l'intégration à Ubuntu du service propriétaire Snap Store.
- **AS3 | Licence & Ouverture (4.3/5) :** Ubuntu est une distribution sous licence globale libre : seuls les paquets logiciels assemblés par Ubuntu ont des licences devant être respectées [70].
- **AS4 | Interopérabilité & Réversibilité (1/5) :** Ubuntu utilise deux formats de paquets logiciels : deb et snap. Le format deb est le plus répandu dans l'écosystème Linux. Les serveurs distribuant ces paquets sont accessibles librement en HTTP, et ont de nombreux miroirs. En revanche, le Snap Store est un service propriétaire de Canonical : son implémentation et ses API ne sont pas documentées.
- **AS5 | Coût & Support (5/5) :** Ubuntu est une distribution open source, documentée, et dont l'utilisation est répandue. Canonical propose aussi des services payant de support étendu et de conseil professionnel. En outre, il est possible de trouver facilement du personnel ou des ESN compétentes pour avoir du support tiers ou interne.
- **AS6 | Pérennité & Sobriété (4/5) :** Canonical, qui possède plus de 1 200 employés, consacre une grande part de ses efforts dans le développement d'Ubuntu [71]. L'entreprise soutien son développement matériellement et financièrement. Elle génère aussi des revenus avec des services de conseil sur des sujets indépendants d'Ubuntu. Les individus peuvent aussi faire des dons pour soutenir le développement de la distribution. Les versions LTS d'Ubuntu sortent tous les 2 ans, et sont prises en charge pendant 5 ans. Le service payant Ubuntu Pro, commercialisé par Canonical, permet d'ajouter 5 ans de prise en charge supplémentaire. Les ressources minimum recommandées pour une installation sur une machine physique sont 4 Go de mémoire (comme Windows 11) et 25 Go de stockage (2,5x moins que Windows 11) [72].

*Ubuntu constitue une alternative à Debian qui se veut plus axée sur des problématiques d'entreprise. Les configurations par défaut offrent une expérience moins généraliste mais plus lisse. Les offres payantes de Canonical donnent accès à du conseil et à du support de longue durée sans passer par des prestataires tiers. En contrepartie, le projet a des liens juridiques avec les États-Unis, sa gouvernance est moins communautaire, et l'intégration grandissante du Snap Store propriétaire pose des questions sur les directions futures.*

### 7.1.5. Synthèse et recommandation

**Recommandation :** La nature communautaire, libre et robuste de Debian lui confère l'indice d'autonomie stratégique le plus élevé. C'est le choix à privilégier pour une équipe technique compétente, capable de s'investir dans la configuration des systèmes et dans la résolution d'éventuels incidents opérationnels. En revanche, s'il est jugé indispensable d'avoir une proximité professionnelle avec l'éditeur du système d'exploitation, alors openSUSE est un choix pertinent. Cette alternative allie souveraineté européenne et ouverture vers une solution professionnelle en cas de besoin grâce à SUSE Enterprise Linux. Enfin, les deux derniers choix, Fedora et Ubuntu, présentent des désavantages conséquents en matières de souveraineté et de gouvernance, mais bénéficient d'un écosystème plus répandu que celui d'openSUSE. Ce dernier point peut potentiellement augmenter la quantité de documentation communautaire en ligne, ou faciliter la recherche d'employé-es internes compétent-es familiarisé-es avec ces distributions. Ubuntu est le choix le moins recommandé, accusant d'une intégration progressive avec le Snap Store propriétaire, et d'une démarcation plus floue entre gouvernance communautaire et gouvernance commerciale.

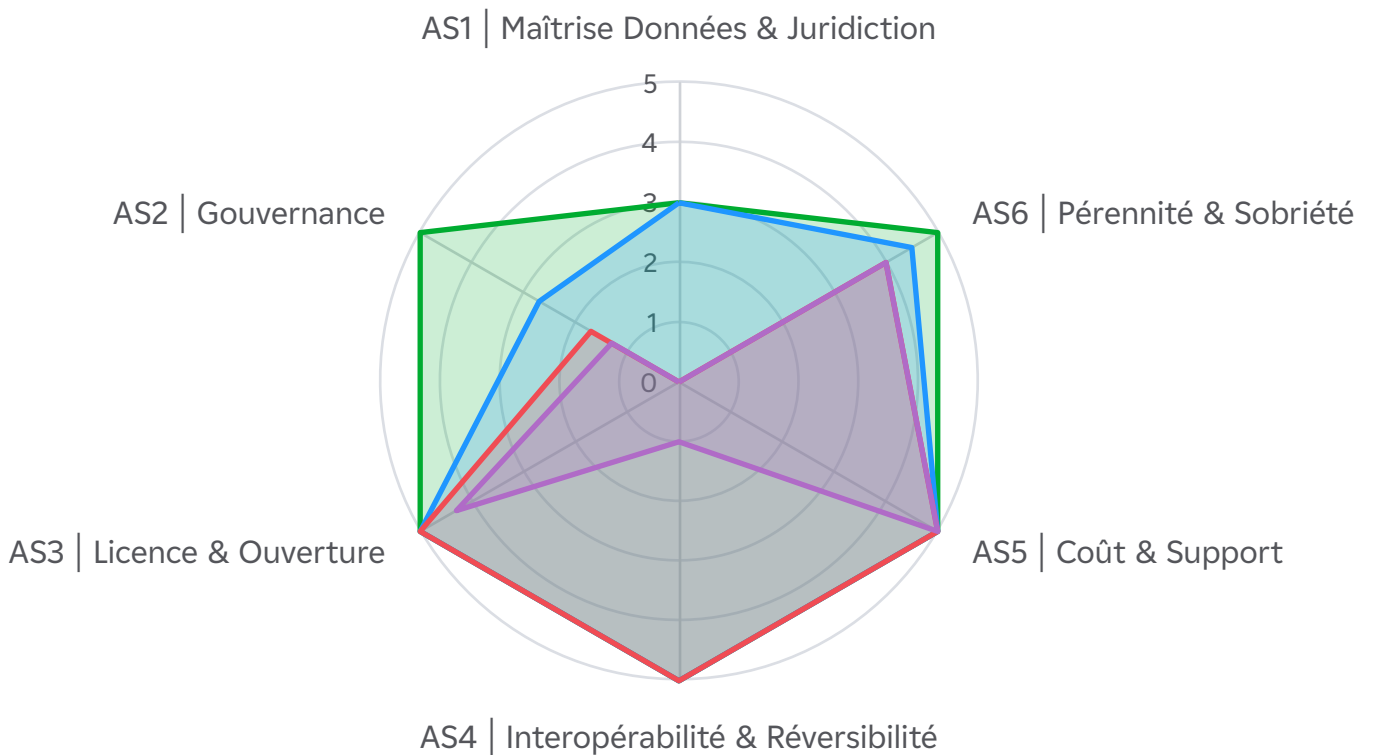


Fig. 4. - Comparatif des systèmes d'exploitation pour les postes utilisateur-rices

## 7.2. Environnements de bureau

L'environnement de bureau est l'élément qui fait le lien entre l'utilisateur·ice et le système d'exploitation. C'est l'interface graphique qui gère les fenêtres, la barre des tâches, le menu de démarrage, les icônes et les préférences d'affichage.

Dans le cadre d'une migration depuis Windows, le choix de l'environnement de bureau est un facteur critique d'acceptation du changement. Les utilisateur·ice·s ont des réflexes musculaires et visuels qui se sont ancrées sur plusieurs années. Par exemple, ils ont l'habitude de trouver le menu « Démarrer » en bas à gauche, la zone de notification en bas à droite, et une gestion des fenêtres spécifique à Windows. Une rupture trop brutale avec ces habitudes peut entraîner une perte de productivité et un rejet de la solution choisie pour la migration.

Nous avons sélectionné des environnements de bureau de l'écosystème Linux qui sont capables d'adopter une interface similaire à celle de Windows, certains nativement, d'autres avec de la configuration.

### 7.2.1. KDE Plasma

KDE Plasma est l'un des environnements de bureau les plus anciens et matures de l'écosystème libre. Il est développé par une communauté internationale, ancrée légalement dans une organisation à but non lucratif basée en Allemagne. Plasma est réputé pour sa modularité : il peut ressembler à Windows, à macOS, ou à quelque chose d'unique.

#### KDE Plasma

**IAS : 88 / 100****Origine :** Allemagne **Licence :** GPLv2**Modèle Économique :** Dons

#### Analyse IAS :

- **Maîtrise des données & Juridiction (3/5)** : Le projet KDE est représenté légalement par l'association à but non lucratif KDE e.V. basée en Allemagne.
- **Gouvernance (5/5)** : KDE e.V. est une association à but non lucratif, et n'a donc pas d'actionnaires. Le développement de KDE Plasma est communautaire et transparent. Les décisions sont prises collectivement par la communauté.
- **Licence (5/5)** : KDE Plasma est sous licence libre GPLv2. Son code source est accessible publiquement, et la GPL garantit le droit de le modifier et de le redistribuer librement.
- **Interopérabilité (5/5)** : KDE Plasma fonctionne sur la plupart des distributions Linux, et sur les distributions BSD. Il repose sur le framework graphique Qt, qui offre des API documentées et stables pour le développement d'outils pouvant interagir avec l'environnement graphique.
- **Coût (5/5)** : KDE Plasma est gratuit et vise à le rester. Il est publiquement documenté sous plusieurs formes : manuels, pages sur le wiki KDE UserBase, et catégorie dédiée sur le forum de KDE. Le framework graphique Qt sur lequel repose Plasma, est documenté et très répandu. Une ESN quelconque peut facilement être capable de développer des widgets spécifiques pour Plasma.
- **Pérennité (3,5/5)** : La communauté KDE est un regroupement international de plusieurs milliers de membres, développant activement leurs différents produits, dont Plasma. Le projet KDE est

financé par des dons individuels, ainsi que par le parrainage de plusieurs entreprises telles que Canonical, Google, et SUSE, sans dépendance unique sur un sponsor spécifique. Malgré sa richesse visuelle, Plasma a une consommation de ressources relativement bien optimisée. Il peut tourner sur du matériel ancien. Les versions majeures n'ont plus de LTS depuis la version 6, ce sera désormais aux distributions GNU/Linux d'en assurer la maintenance, il faudra donc regarder ce paramètre en fonction de la distribution GNU/Linux choisie. Les versions mineures quant à elles ne sont maintenues que pendant 4 mois chacune par KDE.

*KDE Plasma est un bon choix en matière de souveraineté européenne, car représenté par une organisation siégeant en Allemagne. Pour la migration, c'est un produit flexible : il est possible de lui donner une apparence visuelle très similaire à Windows 10 ou 11, afin de familiariser rapidement les utilisateur-ice-s. L'un de ses possibles défauts est la multiplicité des options, qui peut perdre un-e utilisateur-ice s'aventurant profondément dans les menus de configuration. Cet aspect peut être mitigé par la fonctionnalité Kiosk, permettant de verrouiller l'accès à certaines configurations.*

## 7.2.2. GNOME

GNOME est l'environnement de bureau par défaut de la plupart des grandes distributions Linux d'entreprise (RHEL, SLES, Ubuntu, Debian). Il propose une approche ergonomique unique, axée sur la simplicité. Son apparence par défaut est différente de celle de Windows, mais cela peut être remédié par son système d'extensions, permettant de modifier son interface.

### GNOME

IAS : 77 / 100

**Origine :** États-Unis 🇺🇸

**Licence :** GPLv2

**Modèle Économique :** Dons

#### Analyse IAS :

- **Maîtrise des données & Juridiction (0/5) :** Le projet GNOME est porté par la fondation GNOME, basée aux États-Unis.
- **Gouvernance (5/5) :** La fondation GNOME est une organisation à but non lucratif, et n'a donc pas d'actionnaires. La gouvernance est transparente. La plupart des décisions sont prises de façon informelle et collaborative entre les contributeurs. Ces derniers ont aussi un droit de vote dans les élections des membres du conseil d'administration, conférant à chacun un pouvoir d'influence la direction globale du projet.
- **Licence (5/5) :** GNOME est sous licence libre GPLv2. Son code source est accessible publiquement, et la GPL permet sa modification et sa redistribution.
- **Interopérabilité (5/5) :** GNOME fonctionne sur la plupart des distributions Linux, et il est même l'environnement de bureau par défaut de la plupart des distributions majeures. Il repose sur le framework graphique GTK, qui dispose d'API documentées et stables permettant d'interagir avec les éléments graphiques.

- **Coût (5/5)** : GNOME est gratuit et vise à le rester. Sa documentation est large et publiquement accessible. La communauté d'entraide est également active sur le forum officiel. GNOME étant l'environnement de bureau le plus utilisé dans les distributions Linux professionnelles, il est maîtrisé par les ESN.
- **Pérennité (3/5)** : Le projet GNOME reçoit annuellement des contributions d'environ 1 000 contributeur·rices réparti·es internationalement. Il est financé par des dons individuels, ainsi que par plusieurs organisations via son programme d'adhésion au conseil consultatif, comprenant entre autres Canonical, Debian, Google, Red Hat, SUSE, sans dépendance unique sur une organisation donnée.

*GNOME est le choix du standard industriel, massivement déployé dans l'écosystème Linux. Par défaut, son ergonomie est déroutante pour un·e utilisateur·ice de Windows. Cependant, il existe des extensions, comme "Dash to Panel", "Arc Menu", ou les extensions de ZorinOS, qui permettent de transformer GNOME pour offrir une expérience proche de celle de Windows. Cela ajoute malgré tout une dépendance sur des extensions tierces qui se doivent d'être maintenues sur le long terme par leurs développeur·euse·s, sous peine de problèmes de compatibilité avec les nouvelles versions majeures de GNOME.*

### 7.2.3. Cinnamon

Cinnamon est un environnement de bureau issu d'un fork de GNOME 3. Il a été créé par l'équipe de la distribution Linux Mint, avec comme objectif de conserver une ergonomie traditionnelle de bureau, comme c'était le cas pour GNOME avant la refonte de son interface.

#### Cinnamon

IAS : 85 / 100

**Origine** : Irlande 🇮🇪

**Licence** : GPLv2

**Modèle Économique** : Dons

#### Analyse IAS :

- **Maîtrise des données & Juridiction (3/5)** : Cinnamon est porté par Linux Mint, une communauté ouverte et indépendante, qui perçoit ses dons à travers l'entreprise irlandaise Linux Mint Ltd.
- **Gouvernance (4/5)** : Linux Mint est un projet communautaire indépendant, soutenu par des dons perçus à travers Linux Mint Ltd. Le projet n'a pas d'actionnaires. Les développements sont pilotés par les contributeurs du projet, en tenant compte des idées de la communauté.
- **Licence (5/5)** : Cinnamon est sous licence libre GPLv2. Son code source est accessible publiquement, et la GPL permet de le modifier et de le redistribuer.
- **Interopérabilité (5/5)** : Cinnamon fonctionne sur la plupart des distributions Linux, et aussi sur les distributions BSD. En tant que fork de GNOME, il est construit avec le framework graphique GTK, qui offre des API documentées et stables pour interagir avec les éléments graphiques.
- **Coût (5/5)** : Cinnamon est gratuit et a pour but de le rester. Sa documentation est moins étoffée que celles de GNOME et KDE Plasma, mais elle reste présente et publiquement accessible. Le forum

de Linux Mint possède aussi des catégories dédiées à Cinnamon. Moins d'ESN sont spécialisées sur Cinnamon que sur GNOME et Plasma, mais la base technologique reste standard (GTK), et la documentation est présente.

- **Pérennité (3,5/5)** : L'équipe de développement de Cinnamon ne comporte qu'une dizaine de membres, mais elle est active et les mises à jour sont régulières. La communauté apporte aussi ses contributions au projet. Linux Mint reçoit environ 40 000\$ de dons mensuels de la part de nombreux individus, et de la part de plusieurs organisations via son programme de parrainage, comprenant entre autres Datadog et eukhost, sans dépendance à un donateur spécifique. La consommation de ressources de Cinnamon est relativement faible, mais il existe malgré tout des alternatives encore plus légères. Les nouvelles versions de Cinnamon sont alignées avec celles de Linux Mint, et sont donc maintenues en LTS pendant 3 ans.

*Cinnamon est un choix pragmatique disposant de plusieurs avantages : son ergonomie est proche de celle de Windows, ses menus de configurations sont moins riches et plus épurés que ceux de KDE Plasma, et sa stabilité est exemplaire, plus forte que celle de GNOME et Plasma. Ces avantages sont nuancés par une présence un peu moins prononcée dans l'écosystème Linux, avec une documentation moins étoffée, une équipe de développement plus petite, et des financements moins conséquents.*

#### 7.2.4. Synthèse et recommandation

**Recommandation** : KDE Plasma est la solution recommandée. Son score IAS est le plus élevé. Côté souveraineté, son siège est en Allemagne, sa juridiction est donc européenne. Côté technique, c'est l'une des propositions les plus légères et configurables. Plasma peut être configuré nativement pour avoir une interface semblable à celle de Windows, ce qui est un point non négligeable dans le contexte d'une migration. Si la problématique prioritaire est la stabilité et la possibilité de déploiement sans configuration, alors Cinnamon est une bonne alternative. Elle est aussi européenne et légère en ressources. Enfin, si la standardisation avec facilité de support entreprise est nécessaire, alors GNOME peut être un choix pertinent. Bien que son siège soit américain, sa robustesse lui a permis de s'imposer comme la solution la plus répandue dans l'écosystème. Il faudra néanmoins prévoir un effort de configuration via des extensions pour adapter son ergonomie aux habitudes des utilisateur·rices venant de Windows.

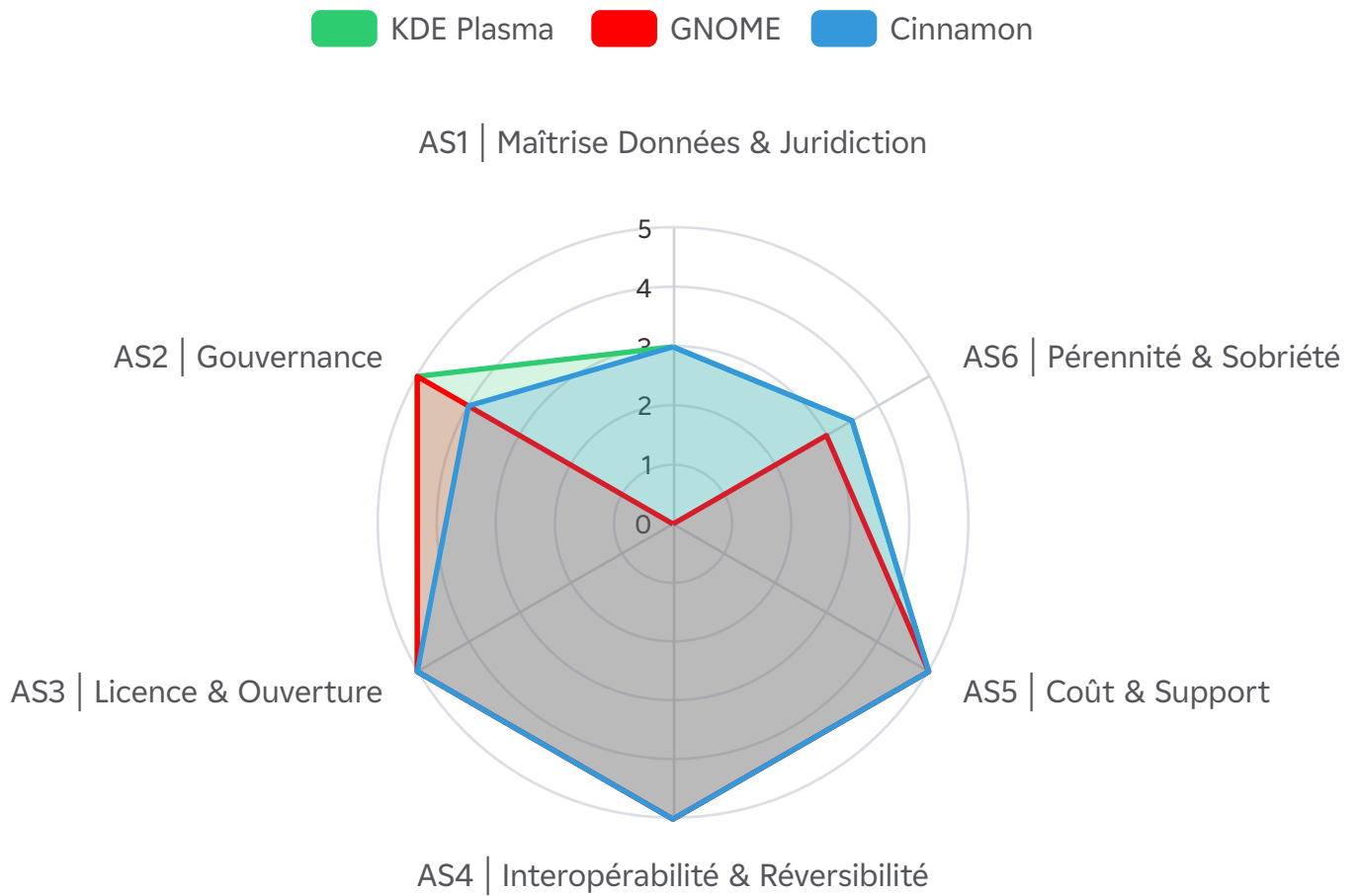


Fig. 5. - Comparatif des environnements de bureau

Dans le cadre de la transition des postes de travail vers un écosystème GNU/Linux, l'abandon des outils Microsoft (MECM/SCCM, Intune) nécessite une refonte des mécanismes de gestion du parc.

Cette brique couvre l'ensemble des mécanismes permettant d'industrialiser le cycle de vie des postes de travail. À savoir, le déploiement initial (approvisionnement), la configuration continue, ainsi que le maintien en condition opérationnelle et conformité.

La grille d'évaluation IAS détaillée est accessible ici : [73]

### 7.3. Approvisionnement des terminaux

L'approvisionnement correspond à la phase initiale du cycle de vie du poste de travail. Il regroupe l'ensemble des mécanismes permettant de déployer automatiquement un poste GNU/Linux, depuis un état vierge, sans intervention manuelle.

Cette étape couvre le démarrage via le réseau (PXE / iPXE [74]), l'installation automatisée du système, l'application des premières configurations et l'intégration du poste dans les briques centrales du système d'information (annuaire, inventaire, configuration).

Contrairement à la configuration continue, le provisioning est une opération ponctuelle qui vise à produire un poste conforme, reproductible et prêt à être pris en charge par les outils de gestion du parc.

Dans une logique d'Autonomie stratégique et de maîtrise de la chaîne technique, cette partie propose d'étudier des logiciel libre, standards et auto-hébergeable.

### 7.3.1. iPXE + Preseed + scripts

Une chaîne iPXE + Preseed + scripts de post-installation permet d'automatiser intégralement l'installation du système d'exploitation : boot réseau, installation non interactive, configuration initiale, puis intégration aux briques centrales (IAM, inventaire, durcissement).

#### iPXE + Preseed + scripts

**IAS : 94 / 100**

**Origine** : Communautaire

**Licence** : Libre (standards PXE/DHCP/TFTP/HTTP + outils GPL)

**Modèle Économique** : Communautaire

#### Analyse IAS :

- **Données (5/5)** : Déploiement entièrement On-Premise. Aucun flux vers un cloud tiers. Contrôle total des images, scripts et artefacts.
- **Gouvernance (5/5)** : Outils standards et communautaires, gouvernance ouverte et transparente.
- **Licence (5/5)** : Chaîne basée sur des composants libres et auditable. Aucune dépendance à un outil propriétaire.
- **Interopérabilité (4/5)** : Excellente compatibilité Debian-like. Intégration facilitée avec IAM et inventaire via scripts/CLI/API.
- **Coût (5/5)** : Licence 0€. Coût limité à l'infrastructure (PXE/HTTP) et à l'exploitation.
- **Pérennité (4/5)** : Socle simple, durable et sobre. Risque limité, mais dépendance à l'ingénierie interne pour maintenir les templates.

*Cette chaîne constitue le socle le plus cohérent pour un provisioning souverain : légère, maîtrisable et reproductible. Elle permet d'industrialiser rapidement le déploiement tout en gardant une maîtrise totale de la chaîne technique.*

### 7.3.2. FAI (Fully Automated Install)

FAI est un outil historique Debian permettant des installations totalement automatisées via des classes de configuration. Très flexible, il demande en contrepartie une expertise plus élevée.

#### FAI (Fully Automated Install)

**IAS : 89 / 100**

**Origine** : Communautaire

**Licence** : GPLv2

**Modèle Économique** : Communautaire

**Analyse IAS :**

- **Données (5/5)** : Déploiement On-Premise, contrôle total.
- **Gouvernance (4/5)** : Projet stable, mais moins “mainstream” que d'autres outils.
- **Licence (5/5)** : GPLv2, audit complet.
- **Interopérabilité (4/5)** : Très adapté Debian. Intégration possible avec IAM/inventaire via scripts.
- **Coût (5/5)** : Licence 0€, coût d'exploitation lié à la complexité.
- **Pérennité (4/5)** : Durable, mais dépend fortement de la compétence interne.

*FAI est un excellent complément pour des déploiements avancés, mais sa complexité opérationnelle le rend moins adapté comme socle initial si l'objectif prioritaire est la simplicité et la montée en charge rapide.*

### 7.3.3. Foreman + Katello

Foreman est une plateforme de provisioning et de gestion de cycle de vie (dashboard, API, orchestration). Très complète, mais plus lourde à opérer dans un contexte de poste Debian-like.

#### Foreman + Katello

**IAS : 86 / 100**

**Origine** : International

**Licence** : GPLv3

**Modèle Économique** : Communautaire. Support pro disponible.

**Analyse IAS :**

- **Données (5/5)** : Déploiement On-Premise possible.
- **Gouvernance (4/5)** : Projets structurés, roadmaps actives.
- **Licence (5/5)** : GPLv3, audit complet.
- **Interopérabilité (4/5)** : Puissant via API, mais orientation forte “fleet/infra” et intégration Debian à cadrer.
- **Coût (3/5)** : Licence 0€ mais coûts d'exploitation plus élevés (stack lourde).
- **Pérennité (4/5)** : Projets pérennes, mais complexité et dépendances plus importantes.

*Foreman est très pertinent pour des besoins d'orchestration et de gestion de parc à grande échelle, mais il peut être surdimensionné pour un provisioning orienté sobriété et maîtrise opérationnelle.*

### 7.3.4. FOG Project

FOG Project est une solution libre de clonage et de déploiement de postes via le réseau. Elle s'appuie sur PXE/iPXE pour amorcer les machines, puis orchestre l'imaging (capture/déploiement d'images disque), avec des fonctionnalités de gestion (inventaire, tâches planifiées, multicast).

## FOG Project

IAS : 72 / 100

**Origine** : Communautaire

**Licence** : GPL (logiciel libre)

**Modèle Économique** : Communautaire

### Analyse IAS :

- **Données (5/5)** : Déploiement entièrement On-Premise. Contrôle total des images, scripts et flux de provisioning.
- **Gouvernance (4/5)** : Projet communautaire structuré, mais avec une communauté plus restreinte que les standards Debian.
- **Licence (5/5)** : Logiciel libre, code auditable et modifiable.
- **Interopérabilité (3.5/5)** : Très pertinent pour l'imaging et le déploiement via PXE/iPXE, mais moins intégré nativement à Debian/Preseed qu'une chaîne dédiée (nécessite cadrage des workflows et du post-install).
- **Coût (5/5)** : Licence 0€. Coûts limités à l'infrastructure (stockage, réseau) et à l'exploitation.
- **Pérennité (3/5)** : Solution éprouvée pour l'imaging, mais l'approche "images disque" peut devenir plus coûteuse à maintenir à grande échelle qu'un provisioning déclaratif (templates + post-install).

*FOG est une alternative crédible lorsqu'un besoin fort d'imaging (clonage, multicast) est prioritaire. Dans un contexte Debian orienté sobriété et maîtrise, il reste cependant moins naturel qu'une chaîne iPXE + Preseed + scripts, car il recentre la logique sur des images à maintenir plutôt que sur des templates déclaratifs.*

### 7.3.5. Synthèse et recommandation

**Recommandation** : la chaîne **iPXE + Preseed + scripts** est retenue comme solution cible. Elle maximise la maîtrise de bout en bout, reste parfaitement compatible Debian et limite la complexité opérationnelle. **FAI** est une alternative crédible pour des scénarios avancés. **Foreman** est à considérer uniquement si un besoin fort de plateforme centralisée (dashboard/API) devient prioritaire. **FOG** constitue une option pertinente lorsque l'imaging (clonage, multicast) est prioritaire, au prix d'une maintenance accrue des images par rapport à une approche déclarative.

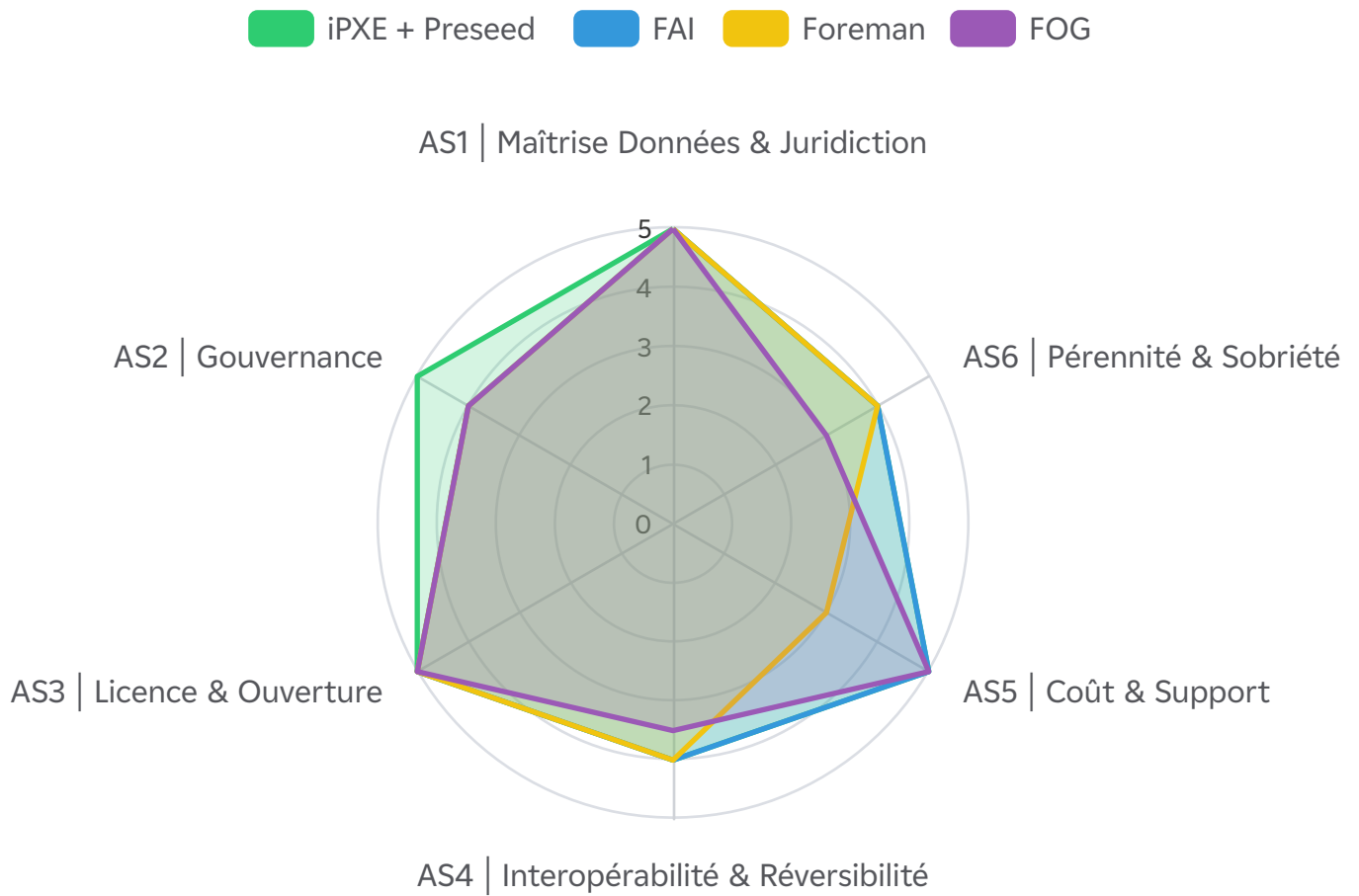


Fig. 6. - Comparatif des solutions de provisioning

## 7.4. Configuration

Tout au long du cycle de vie du poste de travail, la configuration continue, ainsi que le maintien en condition opérationnelle sont des besoins essentiels pour assurer la sécurité et la conformité du poste de travail.

Dans ce contexte, l'adoption d'approches de type **Infrastructure as Code** (IaC) permet de garantir la reproductibilité, la traçabilité et la cohérence des configurations à grande échelle.

Cette section évalue les solutions majeures du marché pour la configuration et l'orchestration du parc (**Ansible, Puppet, OpenVox, et Rudder**), à l'aune de l'Indice d'Autonomie Stratégique.

### 7.4.1. Ansible

Ansible est une solution libre sans-agent pour l'automatisation de la configuration d'ordinateurs.

**Ansible (Red Hat / IBM)**

**IAS : 73 / 100**

**Origine :** États-Unis 🇺🇸

**Licence :** GPLv3 (ansible-core) / Propriétaire (Ansible Automation Platform)

**Modèle Économique :** Support Entreprise disponible

#### Analyse IAS :

- **Maîtrise des données & Jurisdiction (3.34/5) :** Solution auto-hébergeable fonctionnant sans agent (réduction de la surface d'attaque). La confidentialité des données dépend de l'implémentation (ex: utilisation d'Ansible Vault pour les secrets) et de la sécurisation du nœud de contrôle.
- **Gouvernance (1/5) :** Projet sponsorisé par Red Hat (IBM), qui détient la marque et salarie la majorité de la « Core Team ». Bien que les décisions techniques soient ouvertes et supervisées par un Steering Committee élu, l'influence de l'éditeur reste prépondérante sur la feuille de route stratégique. Risque de souveraineté lié à un éditeur américain, bien que le code soit ouvert.
- **Licence (5/5) :** Le moteur ansible-core est entièrement libre (GPLv3). Les « Collections » (modules) peuvent avoir leurs propres licences (généralement permissives type BSD/Apache), favorisant la réutilisation.
- **Interopérabilité (4.5/5) :** S'appuie sur des standards ouverts (YAML pour les playbooks, JSON pour les retours modules) et des protocoles standards (SSH, WinRM). Aucune installation spécifique requise sur les cibles (« Agentless »), garantissant une absence de verrouillage technique. Il existe également la possibilité de configurer les nœuds en mode « pull » afin d'approcher un fonctionnement de type agent.
- **Coût (4.33/5) :** Version communautaire (ansible-core + interface web AWX) gratuite. La version entreprise (AAP) avec support Red Hat est onéreuse (modèle de souscription par nœud géré).
- **Pérennité & Sobriété (3.5/5) :** Communauté active, avec de nombreux experts présents sur le marché. Côté sobriété : l'exécution en Python et le mode de connexion SSH (ouvertures de sessions multiples) peuvent être plus consommateurs en ressources CPU/réseau que des agents compilés (type Go/Rust), mais cela évite la maintenance d'agents sur les postes.

*Ansible s'impose comme un outil puissant d'automatisation, alliant une architecture robuste sans agent à un moteur entièrement libre (ansible-core sous GPLv3). Cependant, la prépondérance de Red Hat (IBM) dans sa gouvernance expose l'organisation à un risque et à une stratégie produit à deux vitesses. L'usage de la version communautaire constitue un excellent levier d'indépendance technologique et économique, à condition d'internaliser la compétence technique pour pallier l'absence de support contractuel et assurer la maintenance de l'outillage périphérique (AWX).*

## 7.4.2. Puppet Enterprise

Puppet est une solution basée sur des agents installés sur les machines.

**Puppet (Perforce Software)**

**IAS : 47 / 100**

**Origine** : États-Unis 🇺🇸

**Licence** : Apache 2.0 (Puppet Open Source) / Propriétaire (Puppet Enterprise)

**Modèle Économique** : Support Entreprise. Modèle souscription par nœud (PE).

#### Analyse IAS :

- **Maîtrise des données & Juridiction (2.67/5)** : Solution hébergeable On-Premise fonctionnant sur une architecture Client-Serveur (Agents). Bien que les données (catalogues, facts) restent en local, la sécurité dépend de la gestion de la PKI (certificats SSL) et du durcissement du Puppet Master.
- **Gouvernance (0.34/5)** : Détenu par Perforce Software (fonds de Private Equity américains Clearlake et Francisco Partners). Depuis le rachat en 2022, la roadmap est devenue opaque et fortement orientée vers la rentabilité de l'offre commerciale, au détriment de l'animation communautaire. Risque élevé d'enfermement propriétaire.
- **Licence (2.33/5)** : Modèle Open Core :
  - **Puppet Open Source** : Licence Apache 2.0. Moteur robuste mais livré « nu » (ligne de commande).
  - **Puppet Enterprise** : Licence propriétaire. Verrouille les fonctionnalités essentielles à l'exploitation à l'échelle (Console Web unifiée, RBAC, Orchestrator, Reporting de conformité). Contrairement à Ansible, il n'y a pas d'équivalent officiel « upstream » complet pour l'interface graphique (nécessite l'intégration complexe d'outils tiers).
- **Interopérabilité (3/5)** : Repose sur un DSL (Domain Specific Language) propriétaire basé sur Ruby. Bien que puissant pour la gestion d'état, ce langage crée une barrière à l'entrée et une dette technique (compétences rares). L'intégration nécessite souvent des modules spécifiques ou des développements en Ruby.
- **Coût (3/5)** :
  - **Enterprise** : Coûteux, tarification par nœud.
  - **Open Source** : Gratuit en licence, mais TCO élevé. La maintenance de la stack technique (Java/Jetty, PuppetDB, PostgreSQL) et l'écriture du code Puppet demandent une expertise rare sur le marché du travail et donc coûteuse.
- **Pérennité (2.5/5)** : Il existe une communauté développée, cependant les compétences métiers sont rare sur le marché du travail.

*Puppet reste une référence pour le maintien de conformité en continu sur des parcs massifs, là où son architecture basée sur des agents excelle. Toutefois, son modèle Open Core restrictif et son rachat par un fonds d'investissement (Perforce) signalent une stratégie de rente plutôt que d'innovation ouverte. L'usage de la version Open Source est viable mais incertaine : elle impose une courbe d'apprentissage raide (langage DSL) et l'intégration d'outils tiers pour obtenir une visibilité graphique, rendant le ticket d'entrée technique beaucoup plus élevé que ses concurrents .*

### 7.4.3. OpenVox (Vox Pupuli)

OpenVox est un fork communautaire de Puppet, lancé officiellement fin 2024 / début 2025 par l'organisation Vox Pupuli. Il a été créé pour assurer la survie d'une version totalement libre du moteur de gestion de configuration, suite à l'arrêt du développement public et à la fermeture progressive du code par l'éditeur propriétaire Perforce. Il vise une compatibilité avec l'écosystème Puppet existant.

## OpenVox (Vox Pupuli)

IAS : 73 / 100

**Origine** : Mondial / Communautaire 

**Licence** : Apache 2.0

**Modèle Économique** : Gratuit. Support via partenaires communautaires.

### Analyse IAS :

- **Maîtrise des données & Juridiction (4/5)** : Solution strictement identique à Puppet sur le plan technique (Architecture Agent/Serveur). Auto-hébergeable sans aucune dépendance à un service Cloud ou SaaS. Aucune télémétrie commerciale forcée.
- **Gouvernance (5/5)** : Piloté par Vox Pupuli, un collectif d'experts et de mainteneurs reconnus, fonctionnant sur un modèle communautaire. Contrairement au projet original désormais piloté par les intérêts financiers d'un fonds (Perforce), OpenVox garantit que la roadmap sert les intérêts des opérateurs techniques et non des actionnaires.
- **Licence (5/5)** : Apache 2.0. Le code est libre, sans clause « Open Core » restrictive. L'objectif est de maintenir tout l'outillage nécessaire (y compris les paquets serveurs et agents) sous licence permissive, là où l'éditeur historique tend à ne plus distribuer la version libre de binaires prêts à l'emploi.
- **Interopérabilité (1.75/5)** : Repose sur un DSL (Domain Specific Language) propriétaire basé sur Ruby. Bien que puissant pour la gestion d'état, ce langage crée une barrière à l'entrée et une dette technique (compétences rares). L'intégration nécessite souvent des modules spécifiques ou des développements en Ruby.
- **Coût (3.67/5)** : Totalement gratuit. Le coût se reporte sur l'expertise humaine (comme pour toute solution libre).
- **Pérennité (2.5/5)** : Projet jeune (créé en réaction à l'abandon de facto de la version libre par l'éditeur). Bien que porté par des experts historiques (les « anciens » de la communauté Puppet), il doit encore faire ses preuves sur la durée pour garantir le maintien des paquets de sécurité sur le long terme sans le financement d'une entreprise marraine majeure.

*OpenVox incarne la résilience de la communauté DevOps face à la stratégie de la terre brûlée de Perforce. En forkant le moteur Puppet pour le placer sous la gouvernance neutre de Vox Pupuli, le projet offre une porte de sortie vitale aux organisations massivement investies dans le langage Puppet mais refusant le verrouillage commercial. C'est la solution de continuité par excellence pour pérenniser un parc Legacy sans subir de chantage à la licence.*

## 7.4.4. Rudder

Rudder est une solution française de « Continuous Configuration », conçue spécifiquement pour l'audit et la conformité. Contrairement à Puppet et Ansible, Rudder adopte une approche différente. Plutôt que d'apprendre un langage, il propose une interface web graphique où les serveurs peuvent être configurés à la souris. En sélectionnant le résultat attendu (installer un package, configurer un service...), en ajoutant les paramètres, Rudder s'occupe du reste.

## Rudder (Normation)

IAS : 68 / 100

**Origine** : France / Union Européenne 

**Licence** : Apache 2.0 / Propriétaire (plugins)

**Modèle Économique** : Souscription par nœud avec support & plugins supplémentaires.

### Analyse IAS :

- **Maîtrise des données & Jurisdiction (4.34/5)** : Rudder est une solution éditée par une PME française. Le déploiement est réalisé On-Premise. Rudder n'envoie pas de télémétrie, il n'y a pas de traitement de quelconques données utilisateur.
- **Gouvernance (4.34/5)** : Bien que le projet soit sous licence libre, il est très dépendant de l'entreprise éditrice Normation. Toutefois, la prise de décision est tournée vers la communauté. La roadmap est publique et il existe de nombreux échanges actifs entre l'éditeur et la communauté.
- **Licence (2.34/5)** : Solution Open-Core avec des plugins commerciaux sous licence propriétaire. Le modèle économique repose sur le support, l'expertise et les services.
- **Interopérabilité (3.5/5)** : Rudder possède une API REST complète et documentée permettant de d'automatiser de nombreuses actions actionables habituellement via l'interface graphique de l'outil. L'agent Rudder est multiplateformes (compatible GNU/Linux et Windows).
- **Coût (3/5)** : L'entreprise propose plusieurs versions selon les besoins de l'organisation (orientation sécurité, conformité réglementaire, ...), la tarification se calcule par noeud à l'année et donne accès à un support dédié.
- **Pérennité (3/5)** : Le projet est développé depuis plus de 10 ans. Il est maintenu de façon continue par l'entreprise Normation. Cependant, la taille de la communauté est bien plus restreinte qu'Ansible ou Puppet.

*Rudder se distingue comme une alternative française de référence pour la gestion de configuration et l'audit en continu (Continuous Compliance). Contrairement à ses concurrents qui séparent souvent moteur et interface, Rudder offre nativement une console Web complète dans sa version libre. Son développement piloté par l'éditeur français Normation garantit une immunité juridique face aux réglementations extraterritoriales. Si sa communauté est plus restreinte que celle d'Ansible, Rudder compense par une spécialisation forte sur la conformité et une architecture technique légère (l'agent est écrit en C), en faisant un choix stratégique pour les Secteurs Régulés.*

### 7.4.5. Synthèse et recommandation

L'analyse des différentes solutions de configuration du poste de travail met en évidence des solutions correspondant à des besoins différents.

**Recommandation** : L'analyse croisée des solutions d'orchestration révèle l'absence de leader hégémonique sur l'ensemble des piliers de l'Indice d'Autonomie Stratégique. Le choix final de la brique dépendra donc d'un arbitrage entre maturité technologique et impératifs de souveraineté. Ansible s'impose comme le choix de la standardisation opérationnelle. Son architecture sans agent et l'omniprésence de ses compétences sur le marché facilitent une intégration rapide et garantissent une excellente interopérabilité. Toutefois, sa gouvernance centralisée aux États-Unis impose une acceptation du risque lié aux législations

extraterritoriales. À l'inverse, Rudder se distingue par son adéquation aux enjeux de Maintien en Condition de Sécurité (MCS). En tant que solution française, elle offre les meilleures garanties en matière de souveraineté juridique. Son interface graphique constitue un levier d'adoption pertinent pour les équipes moins familières avec l'approche « Infrastructure as Code », bien que son modèle de tarification par nœud doive être mis en perspective avec les volumes du parc à gérer. Enfin, pour les infrastructures privilégiant une autonomie totale vis-à-vis des éditeurs commerciaux, OpenVox représente une alternative résiliente. En tant que fork libre, il permet de pérenniser les environnements basés sur Puppet tout en s'affranchissant des risques de fermeture de l'écosystème.

■ Ansible
 ■ Puppet
 ■ Rudder
 ■ OpenVox

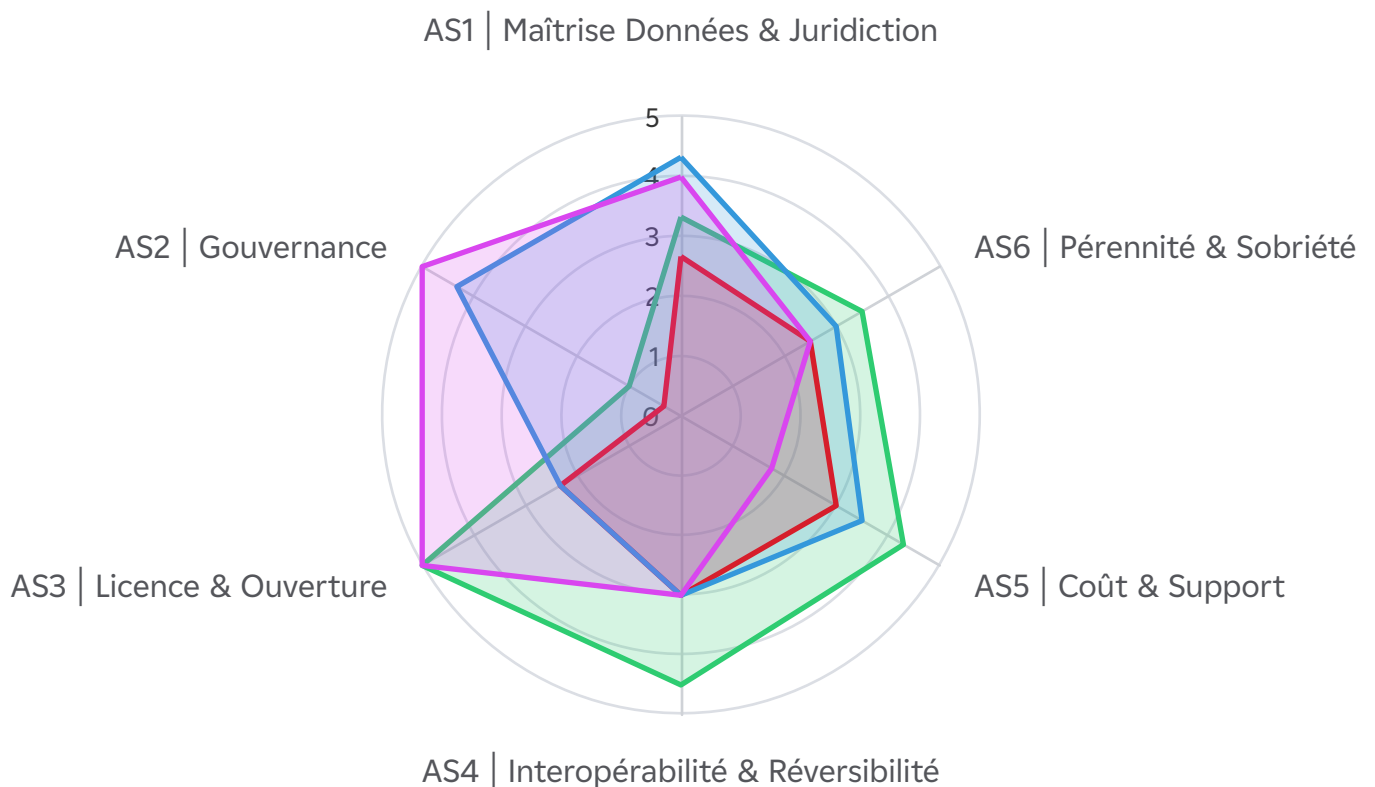


Fig. 7. - Comparatif des solutions de configuration des postes

## 7.5. Navigateur Web

Le navigateur web est devenu l'interface principale d'accès au Système d'Information, centralisant les applications métiers (SaaS), les outils collaboratifs et l'accès aux ressources documentaires. Dans un contexte de souveraineté, le choix du navigateur est critique, il est le premier rempart contre la fuite de métadonnées, le pistage publicitaire et l'exploitation de vulnérabilités par des entités tierces.

L'enjeu majeur réside dans la diversification du moteur de rendu pour éviter un monopole technologique de Chromium (Google), tout en garantissant une compatibilité avec les standards du Web moderne.

### 7.5.1. Firefox (Mozilla)

Firefox est le seul navigateur majeur indépendant n'utilisant pas le moteur de rendu Chromium. Développé par la fondation Mozilla, il place la vie privée et les standards ouverts au centre de sa conception.

#### Firefox

**IAS : 73 / 100**

**Éditeur :** Mozilla Foundation

**Origine :** États-Unis 🇺🇸

**Licence :** MPL 2.0

**Modèle Économique :** Dons

#### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (4/5) :** La Mozilla Foundation est basée aux États-Unis. Bien que soumise au droit américain, sa structure à but non lucratif et sa mission d'intérêt public limitent les risques de coopération commerciale pour l'exploitation des données. Firefox ne pratique pas de collecte de données intrusive et permet de désactiver toute télémétrie.
- **AS2 | Gouvernance (1.5/5) :** Mozilla est une organisation à but non lucratif dont la gouvernance est transparente. Les décisions sont prises pour garantir un Web ouvert, sans pression d'actionnaires. Les utilisateur·rices peuvent influencer les évolutions via la communauté de développement.
- **AS3 | Licence & Ouverture (4/5) :** Le code source est intégralement libre (MPL 2.0). Firefox est l'un des logiciels les plus audités au monde. Sa nature open-source permet la création de versions dérivées « durcies » (hardened) pour des besoins de haute sécurité.
- **AS4 | Interopérabilité & Réversibilité (5/5) :** Firefox soutient activement les standards du W3C. Son moteur de rendu Gecko assure une alternative saine à l'hégémonie de Google, évitant un verrouillage technologique où un seul acteur dicterait les normes du Web.
- **AS5 | Coût & Support (4/5) :** Firefox propose une version ESR (Extended Support Release), idéale pour les déploiements en entreprise. Elle garantit une stabilité des fonctionnalités et un support de sécurité étendu sur plus d'un an, facilitant la maintenance par les équipes IT.
- **AS6 | Pérennité & Sobriété (3.5/5) :** Le projet est extrêmement dynamique avec des mises à jour de sécurité mensuelles. Sa légèreté par rapport aux navigateurs basés sur Chromium permet de limiter la consommation de mémoire vive sur les postes de travail.

*Firefox est la solution de référence pour l'autonomie stratégique. C'est le seul navigateur qui permet de rompre la dépendance technique vis-à-vis du moteur de Google tout en offrant des outils d'administration centralisée (via fichiers de politiques JSON) permettant de verrouiller les paramètres de sécurité sur l'ensemble du parc.*

### 7.5.2. Brave

Brave est un navigateur basé sur Chromium qui se distingue par son blocage natif et agressif de la publicité et des traqueurs. Il offre une compatibilité totale avec les extensions Chrome tout en supprimant les composants de télémétrie de Google.

## Brave

IAS : 73 / 100

**Éditeur** : Brave Software, Inc.

**Origine** : États-Unis 🇺🇸

**Licence** : MPL 2.0

**Modèle Économique** : Freemium

### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (1.5/5)** : Société basée aux États-Unis. Brave se distingue par un modèle « Privacy by Design » où aucun traitement de données personnelles n'est effectué sur leurs serveurs.
- **AS2 | Gouvernance (4/5)** : Société privée, ce qui peut poser des questions sur la stratégie à long terme (notamment l'intégration de services de cryptomonnaies par défaut), bien que le modèle économique soit centré sur le respect de la vie privée.
- **AS3 | Licence & Ouverture (4/5)** : Code source ouvert sous licence MPL 2.0. La transparence est élevée, permettant de vérifier que les fonctions de pistage de Google ont bien été neutralisées dans le moteur Chromium.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : Basé sur Chromium, il offre la meilleure compatibilité possible avec les applications web complexes développées spécifiquement pour l'écosystème Google.
- **AS5 | Coût & Support (3/5)** : Support communautaire robuste. L'administration centralisée est possible via les mêmes outils que pour Chrome/Chromium (GPO ou fichiers de configuration).
- **AS6 | Pérennité & Sobriété (4.5/5)** : Projet très actif bénéficiant des mises à jour de sécurité rapides du projet Chromium, tout en y ajoutant ses propres couches de protection.

*Brave constitue une alternative pragmatique pour les utilisateur-rices ou les applications exigeant absolument le moteur Chromium. Sa force réside dans sa capacité à offrir une navigation « propre » sans configuration complexe, bien que sa dépendance au moteur de Google reste un point de vigilance stratégique.*

### 7.5.3. Synthèse et recommandation

**Recommandation** : Firefox ESR est retenu comme le navigateur cible par défaut pour l'ensemble du parc. Il est le seul à garantir une véritable indépendance technologique via son moteur Gecko. Son cycle de support étendu (ESR) est parfaitement adapté aux contraintes de stabilité d'une organisation d'envergure. Brave pourra être proposé comme solution de secours pour des cas d'usage spécifiques où une compatibilité stricte avec Chromium est requise pour certaines applications métiers.

### 7.6. Suite Bureautique

Cette section analyse les solutions de suite bureautique compatibles avec un poste de travail GNU/Linux. L'objectif est de fournir aux utilisateur-rices une suite de bureautique complète (éditeur de texte, tableur, présentation), capable de remplacer les solutions propriétaires telles que **Word**, **Excel** ou **PowerPoint**.

Cette brique est critique pour l'adoption du poste Linux, car elle impacte directement l'expérience utilisateur-riche quotidienne, la continuité des usages bureautiques, la qualité des documents générés ainsi que la productivité des collaborateur-rices.

L'analyse se concentre sur la capacité des solutions à gérer le format des documents existants, à présenter une interface moderne et familière pour faciliter le changement de logiciel et à garantir l'interopérabilité via des standards ouverts.

### 7.6.1. Only Office

OnlyOffice est une suite bureautique développée par [Ascensio System SIA](#), qui se positionne comme l'alternative la plus proche de Microsoft Office en termes d'interface. Elle utilise nativement les formats [OOXML](#) (docx, xlsx, pptx), ce qui facilite la transition immédiate pour les utilisateur-rices venant d'un environnement Windows.

#### OnlyOffice

**IAS : 73 / 100**

**Éditeur :** Ascensio System SIA

**Origine :** Europe / Lettonie 🇱🇻

**Licence :** AGPLv3

**Modèle Économique :** Souscription

#### Analyse IAS :

- **AS1 | Maîtrise Données & Jurisdiction (4/5) :** Bien que le siège social soit situé en Lettonie (Union Européenne), la structure de l'entreprise est complexe avec une holding située à Singapour. Cette fragmentation géographique peut poser des questions de souveraineté à long terme, bien que l'hébergement puisse être réalisé entièrement On-Premise, garantissant ainsi le contrôle des données.
- **AS2 | Gouvernance (1.5/5) :** La gouvernance est majoritairement privée et centralisée par l'éditeur. Le développement est piloté par l'entreprise, bien que le code soit ouvert aux contributions communautaires. La feuille de route reste à la discrétion d'Ascensio System.
- **AS3 | Licence & Ouverture (4/5) :** Le cœur de la solution est placé sous licence AGPLv3, garantissant l'accès au code source et la liberté de modification. Cependant, certains modules avancés et les solutions mobiles/professionnelles sont régis par des licences commerciales propriétaires.
- **AS4 | Interopérabilité & Réversibilité (5/5) :** C'est le point fort de la solution : elle est conçue pour une compatibilité maximale avec les formats Microsoft. En revanche, son utilisation par défaut des formats OOXML peut être perçue comme un frein à l'adoption des standards ouverts comme l'ODF (OpenDocument Format).
- **AS5 | Coût & Support (4/5) :** Une version communautaire gratuite est disponible, tandis que le support professionnel et les fonctionnalités « Entreprise » nécessitent une souscription payante. La documentation est complète et l'écosystème est en forte croissance.
- **AS6 | Pérennité & Sobriété (3.5/5) :** La solution est largement adoptée et fréquemment mise à jour. Son interface moderne et ses fonctionnalités de co-édition en temps réel en font un outil pérenne pour les organisations.

*OnlyOffice est la solution idéale pour minimiser le choc cognitif lors de la migration. Son interface en ruban et sa gestion de la mise en page des fichiers Microsoft garantissent la continuité métier. C'est un choix pragmatique pour les services ayant une forte interdépendance documentaire avec des partenaires externes sous environnement Windows.*

## 7.6.2. LibreOffice

LibreOffice est la suite bureautique libre la plus aboutie, issue du projet communautaire The Document Foundation. Elle est le porte-étendard des formats ouverts et de l'indépendance technologique.

### LibreOffice

IAS : 97 / 100

**Éditeur** : The Document Foundation

**Origine** : Allemagne 

**Licence** : LGPLv3

**Modèle Économique** : Dons

#### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (5/5)** : Porté par [The Document Foundation](#), basée en Allemagne, le projet bénéficie d'une protection juridique européenne robuste et d'une immunité vis-à-vis des législations extraterritoriales.
- **AS2 | Gouvernance (5/5)** : La gouvernance est méritocratique et transparente, pilotée par une fondation à but non lucratif. Aucune entreprise ne possède de contrôle unilatéral sur la feuille de route.
- **AS3 | Licence & Ouverture (5/5)** : Entièrement sous licence LGPLv3 (libre), le code source est auditable et modifiable sans aucune restriction. C'est le garant de la pérennité numérique des archives de l'organisation.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : LibreOffice est le logiciel de référence pour le format ODF (ISO/IEC 26300). Bien qu'il lise et écrive les formats Microsoft, des ruptures de mise en page peuvent apparaître sur des documents complexes. Il intègre toutefois un support croissant des macros VBA. [75]
- **AS5 | Coût & Support (4/5)** : Gratuit par défaut, le support peut être contractualisé via un vaste écosystème de prestataires. La documentation communautaire est la plus vaste du marché.
- **AS6 | Pérennité & Sobriété (5/5)** : Le projet dispose d'une base de contributeurs massive et de financements diversifiés. Sa légèreté lui permet de fonctionner sur du matériel ancien, favorisant la sobriété numérique.

*LibreOffice est le choix de l'autonomie stratégique et de l'interopérabilité à long terme. S'il demande un effort d'adaptation pour les utilisateur·rices habitués au ruban Microsoft (malgré l'interface « Tabbed » optionnelle), il est le seul à garantir que les données ne resteront jamais captives d'un format propriétaire.*

### 7.6.3. Apache OpenOffice

Apache OpenOffice est une suite bureautique libre historique, issue du code source d'OpenOffice.org. Bien qu'elle ait été la référence mondiale durant la décennie 2000, son développement est aujourd'hui plus lent que celui de son dérivé LibreOffice, se concentrant principalement sur la maintenance et la stabilité de son interface.

#### OpenOffice

**IAS : 73 / 100**

**Éditeur :** The Apache Software Foundation

**Origine :** États-Unis 🇺🇸

**Licence :** Apache 2.0

**Modèle Économique :** Dons

#### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (1.5/5) :** Le projet est hébergé par la Apache Software Foundation, une organisation à but non lucratif basée aux États-Unis. Bien que la fondation offre une protection contre les intérêts purement commerciaux, le projet reste soumis au cadre juridique américain.
- **AS2 | Gouvernance (4/5) :** La gouvernance est assurée par un comité de gestion de projet au sein de la fondation Apache. Les décisions sont prises de manière collégiale par des bénévoles, garantissant une certaine neutralité, bien que le dynamisme du projet soit en net recul par rapport aux standards actuels du marché.
- **AS3 | Licence & Ouverture (4/5) :** La suite est distribuée sous la licence Apache License 2.0. Cette licence libre est moins restrictive que la licence Copyleft (GPL), permettant une réutilisation large du code, mais elle n'impose pas la redistribution des améliorations sous la même licence, contrairement à l'AGPL ou la GPL.
- **AS4 | Interopérabilité & Réversibilité (5/5) :** OpenOffice utilise nativement le format standard ODF (OpenDocument Format). Cependant, sa capacité à gérer les formats Microsoft récents (.docx, .xlsx) est limitée : s'il peut lire ces fichiers, il ne peut pas toujours les enregistrer avec une fidélité de mise en page optimale, créant une rupture d'interopérabilité pour les échanges externes.
- **AS5 | Coût & Support (3/5) :** La solution est entièrement gratuite. Le support repose exclusivement sur une communauté de bénévoles via des forums et des wikis. Le manque de prestataires professionnels proposant un support commercial (LTS) sur cette solution spécifique rend son adoption risquée pour un parc informatique de grande échelle.
- **AS6 | Pérennité & Sobriété (4.5/5) :** La pérennité du projet est une source de préoccupation. Avec un nombre de contributeurs actifs en baisse et des cycles de mise à jour très espacés, la solution peine à corriger rapidement les vulnérabilités de sécurité ou à s'adapter aux nouvelles exigences matérielles, contrairement aux projets plus dynamiques.

*Apache OpenOffice représente un choix conservateur dont l'intérêt s'estompe face à LibreOffice. Si sa stabilité et sa légèreté peuvent convenir à des parcs de machines anciennes, son manque de compatibilité native avec les formats OOXML modernes et son cycle de développement constituent une dette technique pour l'organisation.*

### 7.6.4. Synthèse et recommandation

**Recommandation :** L'analyse comparative des solutions de productivité conduit à une stratégie de déploiement différenciée selon les phases de la migration et les besoins métiers. OnlyOffice est retenu comme la solution cible pour la transition utilisateur-riche. Son interface en ruban et sa gestion native des formats OOXML minimisent le choc cognitif et garantissent la continuité des échanges avec l'écosystème Windows externe. LibreOffice est préconisé comme le standard de souveraineté à long terme. Il est le seul outil capable de garantir l'indépendance totale des données via le format ouvert ODF et de s'affranchir des logiques de formats propriétaires. Il constitue le socle indispensable pour la pérennité du patrimoine documentaire. Apache OpenOffice est écarté pour un déploiement industriel. Bien qu'historiquement stable, son manque de dynamisme, son cycle de mise à jour ralenti et sa compatibilité limitée avec les formats Microsoft récents en font une solution inadaptée aux exigences d'un système d'information moderne.

■ LibreOffice 
 ■ OnlyOffice 
 ■ OpenOffice

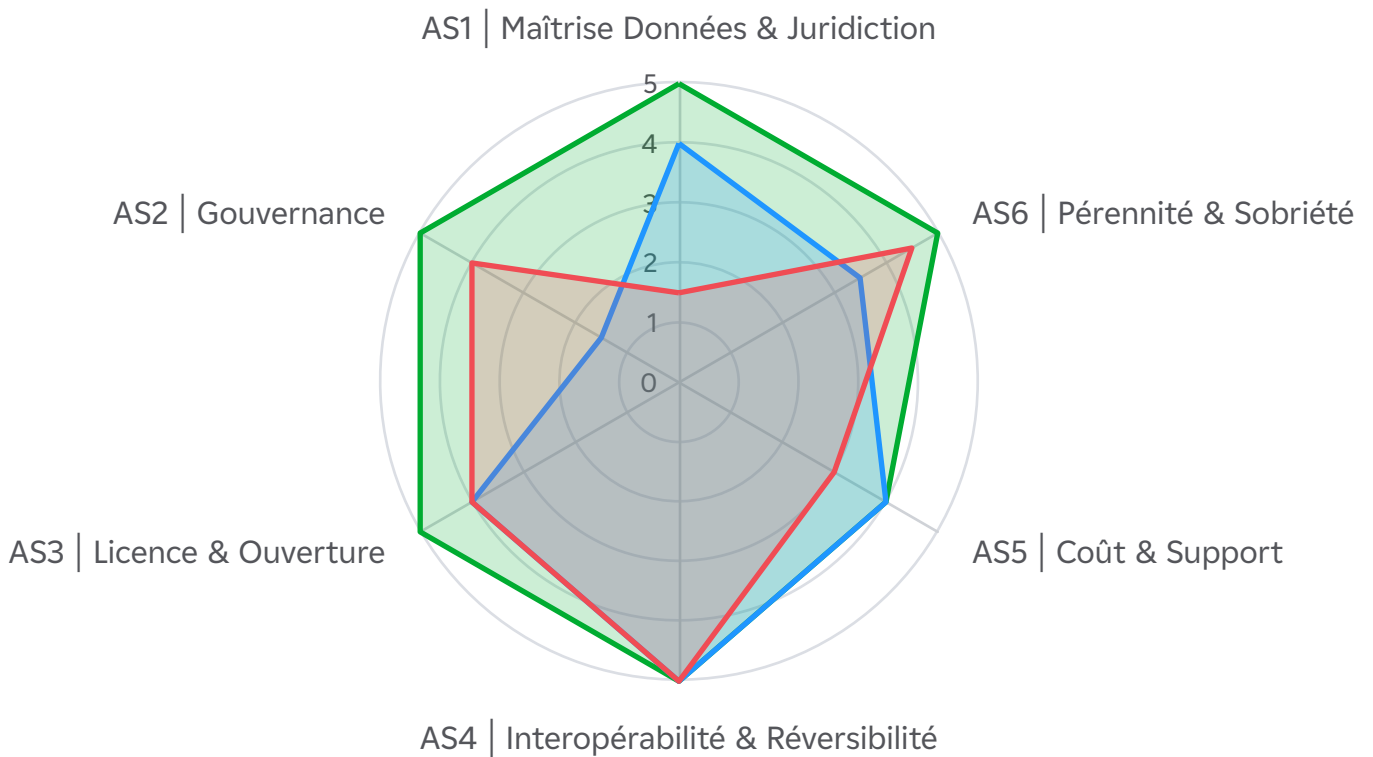


Fig. 8. - Comparatif des suites bureautiques

### 7.7. Collaboration

Cette section analyse les solutions de collaborations libres sous Linux. Elle vise à trouver des alternatives à Teams ou Slack.

Cette brique est critique car son bon fonctionnement est essentiel pour la productivité de l'ensemble des équipes et son choix définit en grande partie le niveau de confidentialité et la sécurité des données échangées au quotidien.

L'analyse se portera donc sur le fonctionnement, la facilité de prise en main, la qualité des appels audio et vidéo ainsi que la sécurité des données.

### 7.7.1. Private Discuss

Private Discuss est une solution propriétaire française. Il s'agit d'une solution axé sur la sécurité. Sa nature de produit propriétaire en fait une solution clé en main qui évite la difficulté d'avoir à mettre en place et gérer une solution open source. Cependant, cela implique une certaine dépendance à l'éditeur.

#### Private Discuss

**IAS : 59 / 100****Origine** : France**Licence** : Propriétaire**Modèle Économique** : Licence SaaS

#### Analyse IAS :

- **Données (5/5)** : Hébergement On-Premise ou chez un hébergeur français. La sécurité des données est le coeur de la solution.
- **Gouvernance (2,5/5)** : Société française mais gouvernance purement privée et roadmap à la discrétion de l'éditeur.
- **Licence (0/5)** : Il s'agit d'une solution propriétaire et donc fermée.
- **Interopérabilité (4/5)** : L'éditeur fournit des API REST documentées, la solution est agnostique en terme d'OS et il existe une procédure d'export manuelle des données.
- **Coût (2,5/5)** : Cette solution est payante sous forme de licences classiques aux prix fixes.
- **Pérennité (4/5)** : L'éditeur maintient et continue de développer le produit, ils disposent d'un nombre suffisant de contracts et de gros comptes pour assurer la pérennité de l'entreprise.

*Private Discuss est une solution intéressantes pour les entreprises ayant des besoins de confidentialité importants (OIV, secteur Défense, COMEX). Cependant, dans l'optique d'une migration vers Linux et l'open source, elle présente une limite majeure : sa nature de logiciel propriétaire la rend dépendante de son éditeur*

### 7.7.2. Element (Matrix)

Element est le client pour le protocole d'échange de données Matrix développé par les développeurs de Matrix eux-mêmes. Il s'agit d'une solution open source au design moderne et aux fonctionnalités complètes. Le fait qu'il repose sur le protocole Matrix le rend particulièrement sûr.

#### Element

**IAS : 87 / 100**

**Origine :** Royaume-Uni 🇬🇧

**Licence :** Open source

**Modèle Économique :** Licence support entreprise

**Analyse IAS :**

- **Données (3,5/5) :** Hébergement On-Premise ou chez un hébergeur au choix, chiffrement, mais éditeur anglais.
- **Gouvernance (3,5/5) :** Société basée au Royaume-Uni mais développement participatif et possibilité de fork.
- **Licence (5/5) :** Il s'agit d'une solution open source libre.
- **Interopérabilité (5/5) :** L'interopérabilité est le but premier de la solution : pouvoir communiquer avec n'importe qui, peu importe la messagerie qu'il utilise.
- **Coût (4,5/5) :** La version entreprise est une licence payante qui donne accès au support.
- **Pérennité (4,5/5) :** L'éditeur maintient et continue de développer le produit, ils disposent d'un nombre suffisant de contracts et de gros comptes pour assurer la pérennité de l'entreprise. De plus, la solution est open source, collaborative, et il existe déjà un grand nombre de forks.

*Element (Matrix) privilégie l'ouverture et l'interopérabilité : c'est la solution reine pour les organisations qui doivent communiquer de manière sécurisée et décentralisée avec des partenaires externes ou d'autres entités.*

### 7.7.3. Nextcloud Talk

Nextcloud Talk est une solution de communication open source qui étend la workplace Nextcloud. Il s'agit d'une excellente solution particulièrement simple à mettre en place si Nextcloud est déjà la solution choisie pour la brique « workplace » ou « stockage ».

#### Nextcloud Talk

IAS : 94 / 100

**Origine :** Allemagne

**Licence :** Open source

**Modèle Économique :** Licence support entreprise

**Analyse IAS :**

- **Données (4,5/5) :** Hébergement On-Premise ou chez un hébergeur au choix, chiffrement, éditeur européen.
- **Gouvernance (4,5/5) :** Société basée en Allemagne, développement très participatif et communauté très active.
- **Licence (5/5) :** Il s'agit d'une solution open source libre.
- **Interopérabilité (5/5) :** Agnostique et nativement intégrée à Nextcloud.
- **Coût (5/5) :** La version entreprise est une licence payante qui donne accès au support et est optionnelle.

- **Pérennité (4,5/5)** : L'éditeur maintient et continue de développer le produit, ils disposent d'un nombre suffisant de contracts et de gros comptes pour assurer la pérennité de l'entreprise. De plus, la solution est open source et collaborative.

*Nextcloud Talk est le choix de la proximité et de l'intégration : si l'équipe utilise déjà Nextcloud pour ses fichiers, Talk s'impose naturellement pour centraliser les échanges internes sans multiplier les outils*

#### 7.7.4. Synthèse et recommandation

**Recommandation** : Nextcloud Talk est retenue comme la solution cible privilégiée pour l'organisation. Bien qu'Element constitue une alternative d'excellence pour les besoins de communication décentralisée et inter-entités, Nextcloud Talk s'impose par sa capacité à unifier l'expérience utilisateur au sein d'une plateforme unique.

En s'appuyant sur l'infrastructure de stockage déjà identifiée comme souveraine, Nextcloud Talk permet de centraliser les échanges internes sans multiplier les outils tiers, garantissant ainsi une adoption fluide et une maîtrise totale des métadonnées sous juridiction européenne. Private Discuss demeure une option spécialisée pour les périmètres exigeant un niveau de confidentialité, bien que sa nature propriétaire limite l'autonomie stratégique globale visée par ce projet.

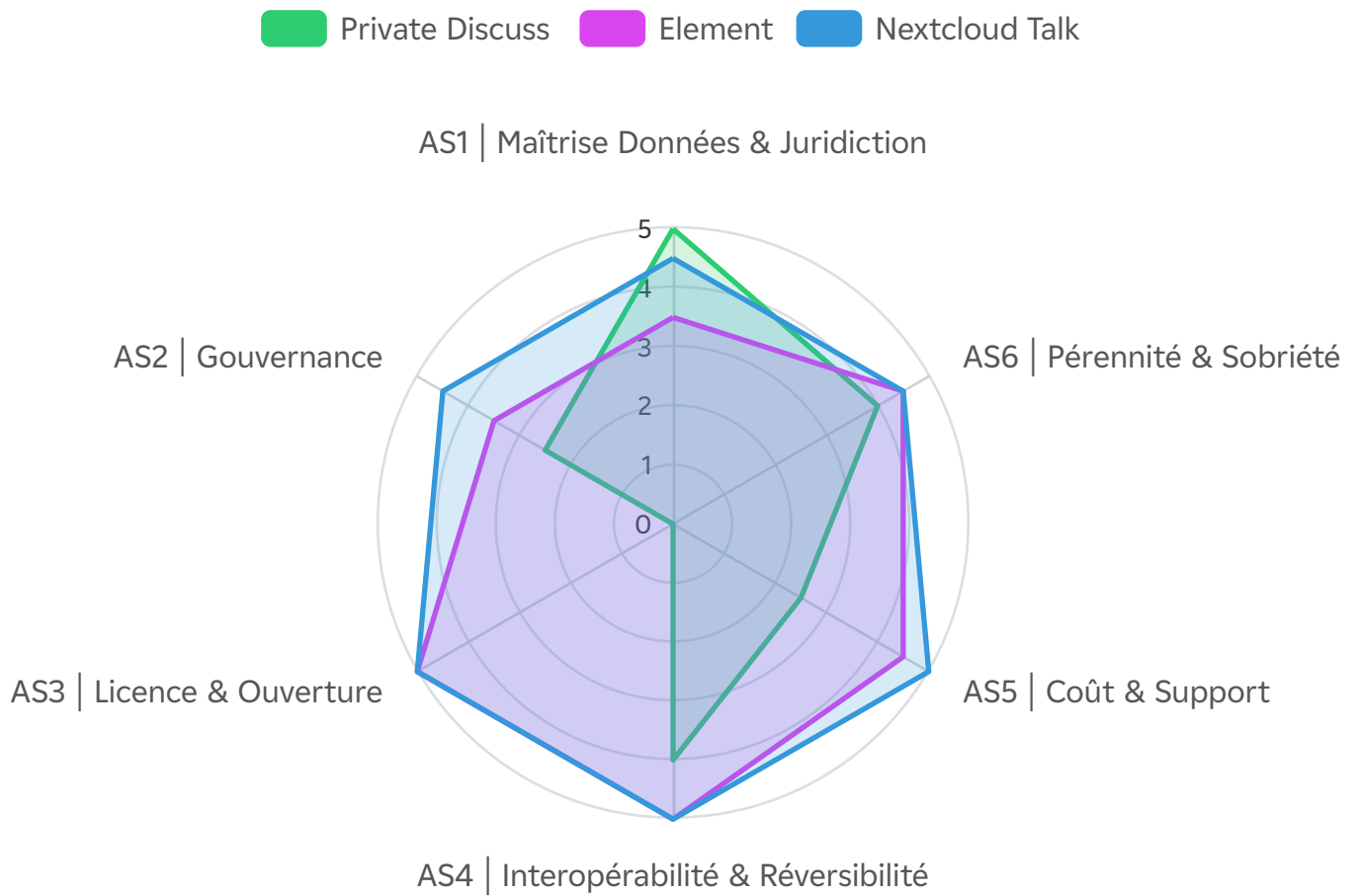


Fig. 9. - Comparatif des solutions de collaboration

## 7.8. Stockage et partage

Cette section analyse les solutions de stockage et de partage de fichiers destinées à un poste de travail GNU/Linux à grande échelle. L'objectif est de fournir aux utilisateur-rices un espace de stockage centralisé, sécurisé et synchronisé, tout en remplaçant les solutions propriétaires telles que OneDrive et SharePoint

Cette brique est critique pour l'adoption du poste GNU/Linux, car elle impacte directement l'expérience utilisateur-riche quotidienne, la continuité des usages bureautiques, la collaboration ainsi que la souveraineté et la sécurité des données.

### 7.8.1. Nextcloud

Nextcloud est une plateforme collaborative libre permettant le stockage, la synchronisation et le partage de fichiers, avec une interface web moderne et une intégration avancée des services collaboratifs. Elle s'est imposée comme le standard européen pour les organisations publiques et privées cherchant à s'affranchir des solutions cloud extra-européennes.

## Nextcloud

IAS : 90 / 100

Éditeur : Nextcloud

Origine : Allemagne 🇩🇪

Licence : AGPLv3

Modèle Économique : Support

### Analyse IAS :

- **AS1 | Maîtrise Données & Juridiction (5/5)** : L'éditeur est basé en Allemagne, garantissant une conformité stricte au RGPD et une immunité totale face au *CLOUD Act* américain. L'hébergement peut être réalisé *On-Premise*, offrant un contrôle intégral sur les données et les clés de chiffrement.
- **AS2 | Gouvernance (4/5)** : Nextcloud GmbH maintient une gouvernance ouverte et transparente, avec une communauté de développeur-euses très active à travers l'Europe. La feuille de route est publique et les décisions stratégiques sont partagées avec l'écosystème.
- **AS3 | Licence & Ouverture (4/5)** : Le cœur de la solution est placé sous licence AGPLv3. Bien que certains modules avancés soient proposés sous licence commerciale pour les besoins spécifiques des entreprises, la nature libre du produit garantit une auditabilité permanente.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : La solution supporte nativement les standards WebDAV et dispose d'une API REST complète. Son intégration avec les annuaires LDAP/SSO et les suites bureautiques (OnlyOffice, LibreOffice) en fait une pierre angulaire du poste de travail *GNU/Linux*.
- **AS5 | Coût & Support (4/5)** : Il existe un écosystème mature de prestataires certifiés en Europe capables d'assurer le support de niveau 3 et l'infogérance. La documentation officielle est exhaustive et disponible pour les administrateur-rices.
- **AS6 | Pérennité & Sobriété (5/5)** : Bénéficiant d'une adoption massive dans le secteur public (notamment en France et en Allemagne), la pérennité du projet est assurée par des financements diversifiés et une base installée solide.

*Nextcloud constitue la solution de référence pour le stockage et le partage souverain. Sa maturité fonctionnelle, son ancrage européen et sa capacité à remplacer nativement des services comme OneDrive en font un choix pertinent pour une migration à grande échelle.*

## 7.8.2. Twake

Éditée par l'entreprise française Linagora, Twake se présente comme une plateforme collaborative moderne tout-en-un, incluant une brique de stockage de fichiers conçue pour la souveraineté française.

## Twake

IAS : 83 / 100

Éditeur : Linagora

Origine : France 🇫🇷

Licence : AGPLv3

Modèle Économique : Souscription

**Analyse IAS :**

- **AS1 | Maîtrise Données & Juridiction (4/5)** : Solution de droit français portée par un acteur historique de l'Open Source en France. Elle garantit une protection juridique contre les ingérences étrangères et s'inscrit dans les démarches de certification de sécurité nationales.
- **AS2 | Gouvernance (3/5)** : Pilotée par Linagora, la gouvernance est stable et ancrée dans l'écosystème numérique français. L'entreprise collabore étroitement avec les administrations pour adapter le produit aux besoins spécifiques du secteur public. Cependant, il n'y a pas de gouvernance communautaire et très peu de contribution hors des employés de Linagora.
- **AS3 | Licence & Ouverture (4/5)** : Le code source est disponible sous licence AGPLv3, favorisant la transparence et permettant des audits de sécurité approfondis.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : Twake propose une architecture modulaire et des API documentées. Elle facilite l'intégration des flux de travail et propose des connecteurs pour les outils de collaboration courants.
- **AS5 | Coût & Support (4/5)** : Le support est directement assuré par l'éditeur en France, offrant une proximité opérationnelle et linguistique pour des équipes localisées en France.
- **AS6 | Pérennité & Sobriété (5/5)** : Le projet est soutenu par une entreprise qui exerce depuis plus de 25ans désormais, et qui s'inscrit dans la stratégie de souveraineté numérique portée par l'État français via de nombreux partenariats public-privé.

*Twake est une alternative française sérieuse Elle est particulièrement pertinente pour les organisations cherchant un support éditeur national fort.*

### 7.8.3. La Suite Numérique

La Suite Numérique est l'ensemble collaboratif piloté par la Direction interministérielle du numérique (DINUM). Initialement conçue pour les agent-es de l'État, sa nature modulaire basée sur des briques Open Source permet son déploiement en autonomie complète. Dans ce scénario, l'organisation assure elle-même l'hébergement et l'administration des briques (Nextcloud pour le stockage, Element/Matrix pour la messagerie, Jitsi pour la visio), garantissant une autonomie stratégique élevée.

#### La Suite

IAS : 88 / 100

**Éditeur** : DINUM

**Origine** : France 

**Licence** : MIT

**Modèle Économique** : Public

**Analyse IAS :**

- **AS1 | Maîtrise Données & Juridiction (5/5)** : L'entité responsable (DINUM) est de nationalité française. En choisissant l'auto-hébergement, l'organisation s'assure que les serveurs sont situés physiquement sous son contrôle direct. Cette configuration offre une protection contre le CLOUD

Act et les réquisitions extra-territoriales, car aucune entité tierce n'intervient dans la chaîne de traitement des données.

- **AS2 | Gouvernance (3.5/5)** : La structure juridique est un acteur public (État français), dont les intérêts sont alignés sur la souveraineté nationale et non sur le profit. La feuille de route est transparente et contributive pour les acteurs publics, mais pas pour les acteurs privés, ne permettant pas d'influencer les priorités.
- **AS3 | Licence & Ouverture (4/5)** : Toutes les briques de La Suite sont issues du logiciel libre, principalement sous licences à sans réciprocité (MIT). Le code source est public, auditable et téléchargeable sans restriction, garantissant un droit de fork total. En cas d'arrêt du support par la DINUM, l'organisation conserve la capacité technique et légale de maintenir son instance de manière autonome.
- **AS4 | Interopérabilité & Réversibilité (5/5)** : La solution utilise des formats ouverts issus de normes internationales (ODF, Matrix, XMPP). L'architecture est nativement modulaire (microservices) : chaque brique (stockage, édition, messagerie) peut être mise à jour ou remplacée indépendamment sans compromettre l'intégrité de l'ensemble. Des API robustes facilitent l'automatisation de la réversibilité des données.
- **AS5 | Coût & Support (4/5)** : L'auto-hébergement permet de s'affranchir de tout abonnement captif. Le TCO est maîtrisé et repose sur les coûts d'infrastructure interne et de RH. Le marché du support est ouvert, n'importe quelle ESN compétente en logiciel libre peut intervenir sur le code ou la maintenance, brisant tout monopole d'éditeur.
- **AS6 | Pérennité & Sobriété (5/5)** : Le dynamisme est assuré par les acteurs de l'états principaux contributeurs de la solution. Le financement est pérenne et distribué, car adossé aux budgets de l'État et des grandes administrations. L'engagement de rétro-compatibilité sur le matériel existant favorise une démarche de sobriété numérique.

*Le déploiement de « La Suite » en auto-hébergement élimine les dépendances aux fournisseurs de cloud et place la responsabilité de la donnée entre les seules mains de l'organisation. Si elle exige une expertise technique interne plus forte pour l'exploitation, elle garantit une résilience juridique et opérationnelle face aux aléas géopolitiques.*

## 7.8.4. Synthèse et recommandation

**Recommandation** : Nextcloud est retenu comme la solution cible privilégiée pour l'architecture du poste de travail souverain.

Son score IAS élevé (90/100) et son adoption massive par les administrations européennes garantissent une réduction drastique des risques de migration. Cependant, les solutions françaises Twake et La Suite constituent des alternatives de premier plan, notamment pour les organisations exigeant un accompagnement éditeur localisé en France.

Bien que Nextcloud demeure la solution cible, l'émergence de l'initiative Open Buro, cofondée par les acteurs de Twake et La Suite, va être intéressante à suivre.

Cette alliance vise à briser les silos de données en définissant un standard d'interopérabilité ouvert, garantissant que le courrier électronique, la collaboration documentaire et la visioconférence fonctionnent comme une plateforme unifiée et non comme une collection d'outils déconnectés. L'objectif est d'offrir

à chaque organisation la liberté de composer sa propre *workplace* à partir de logiciels interopérables, garantissant ainsi une expérience utilisateur-rice fluide et intégrée.

Nextcloud La Suite Twake

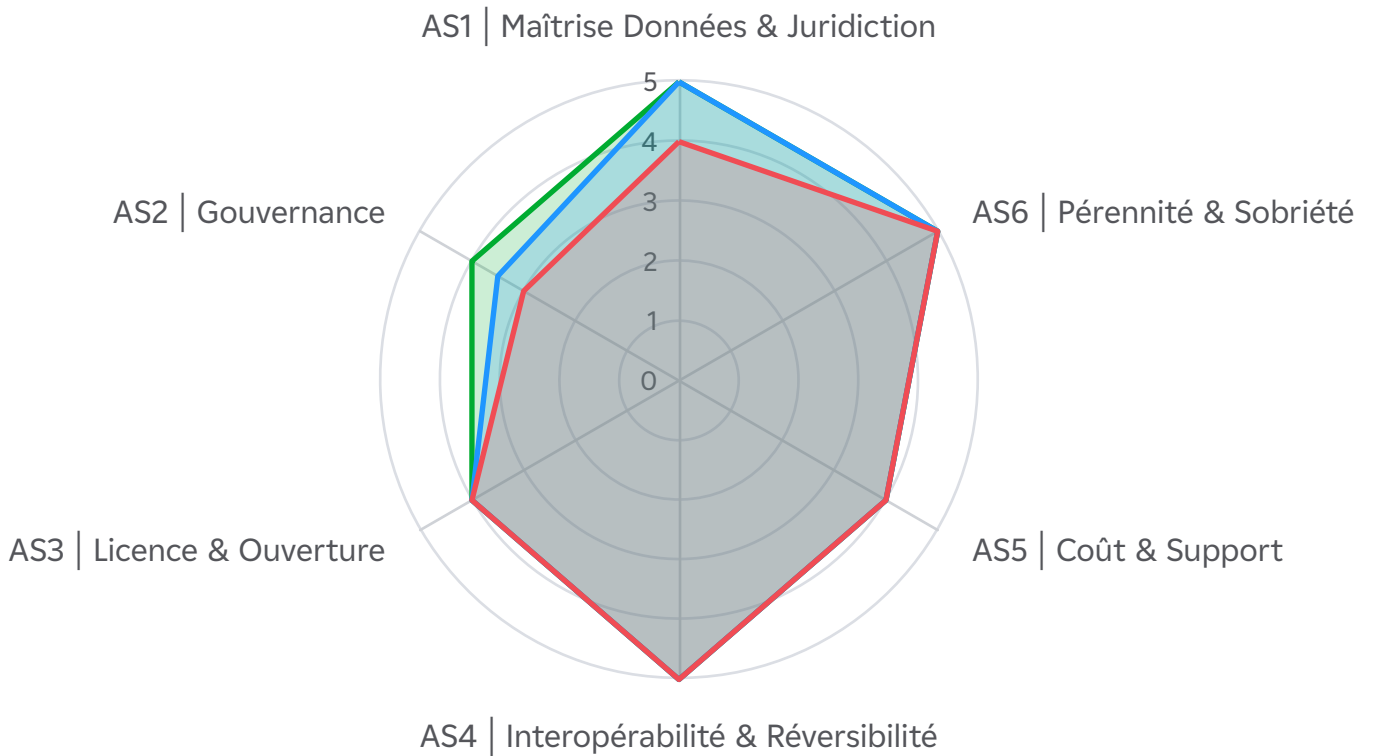


Fig. 10. - Comparatif des systèmes de stockage et partage

## 7.9. Sécurité des terminaux

Cette section analyse les solutions de détection et de réponse aux incidents (EDR/XDR). L'objectif est de remplacer des solutions propriétaires comme Microsoft Defender ou CrowdStrike par une solution assurant une télémétrie transparente et une maîtrise totale des données.

L'analyse se base sur la capacité des outils à répondre aux fonctions principales (FIM, détection comportementale, réponse active) tout en respectant les contraintes de ressources et de compatibilité Linux.

### 7.9.1. Wazuh

Wazuh est une plateforme de sécurité unifiée (XDR/SIEM) née d'un fork d'OSSEC. C'est le standard de facto de l'Open Source.

## Wazuh

IAS : 80 / 100

**Origine** : International / USA (Siège) 🇺🇸

**Licence** : GPLv2 (100% Libre)

**Modèle Économique** : Communautaire. Support pro disponible.

### Analyse IAS :

- **Données (3,33/5)** : Architecture On-Premise totale. L'organisation possède toute la chaîne, de l'agent au stockage. Aucune télémétrie sortante.
- **Gouvernance (1,66/5)** : Piloté par Wazuh Inc (USA). Bien que le code soit ouvert, la gouvernance reste privée.
- **Licence (5/5)** : GPLv2. Logiciel libre strict. Toutes les fonctionnalités (même Enterprise) sont incluses.
- **Interopérabilité (4,5/5)** : Utilise JSON et une API REST complète. Intégration aisée avec TheHive, Cortex, Grafana.
- **Coût (5/5)** : Licence 0€. Modèle économique basé sur le service. TCO maîtrisé.
- **Pérennité (4,5/5)** : Communauté massive, releases fréquentes.

*Wazuh représente le choix rationnel pour concilier sécurité avancée et souveraineté. Sa note de 80/100 reflète une adéquation quasi-parfaite, ne concédant des points que sur la nationalité US de l'entité support, risque mitigé par la licence GPLv2 qui sanctuarise le code.*

## 7.9.2. HarfangLab

HarfangLab est un EDR français certifié par l'ANSSI, conçu pour l'excellence technique et une faible empreinte en ressource mémoire et CPU.

## HarfangLab

IAS : 57.5 / 100

**Origine** : France 🇫🇷

**Licence** : Propriétaire

**Modèle Économique** : Commercial (Abonnement)

### Analyse IAS :

- **Données (5/5)** : Société de droit français. Hébergement On-Premise ou Cloud SecNumCloud. Immunité au Cloud Act.
- **Gouvernance (3/5)** : PME européenne indépendante. Roadmap claire mais gouvernance privée.
- **Licence (0/5)** : Code fermé. L'audit complet est impossible sans accord spécifique. Pas de libertés logicielles.
- **Interopérabilité (2,75/5)** : API documentée et connecteurs, mais pas de standards ouverts intrinsèques.
- **Coût (3/5)** : Licence commerciale récurrente (OpEx). Coût non négligeable comparé au libre.

- **Pérennité (3,5/5)** : Entreprise en croissance (Scale-up), mais ne dispose pas de la communauté massive d'un projet historique.

*HarfangLab est le choix 'Performance & Souveraineté'. Techniquement très abouti (Agent Rust, inspection mémoire). Cependant, son caractère propriétaire et son coût le placent en second choix derrière Wazuh pour un projet priorisant le Logiciel Libre.*

### 7.9.3. Elastic Security

Elastic Security est le module de sécurité de la suite Elastic (ELK), passant de la gestion de logs au XDR.

#### Elastic Security

IAS : 65 / 100

**Origine** : États-Unis 🇺🇸

**Licence** : Source Available (SSPL / ELv2)

**Modèle Économique** : Freemium / Licence Entreprise

#### Analyse IAS :

- **Données (3,33/5)** : Hébergement On-Premise possible. Contrôle total des index.
- **Gouvernance (1,33/5)** : Société cotée (NYSE). Pressions financières dictant la roadmap.
- **Licence (2,33/5)** : N'est plus Open Source (OSI). Licence "Source Available" restrictive sur l'usage commercial.
- **Interopérabilité (5/5)** : Standard de marché (Elastic Common Schema (ecs)). Écosystème de connecteurs immense.
- **Coût (3/5)** : Modèle complexe. Fonctions avancées (Machine Learning (Apprentissage Automatique) (ml)) souvent payantes.
- **Pérennité (4,5/5)** : Référence mondiale incontournable dans la gestion de données.

*Un challenger technique puissant pour l'investigation (Threat Hunting). Toutefois, son statut de société cotée et sa licence non-libre constituent des freins pour l'autonomie stratégique absolue.*

### 7.9.4. Synthèse et recommandation

L'analyse comparative inclut également les leaders du marché (Microsoft Defender, CrowdStrike) pour illustrer l'écart en matière de souveraineté.

**Recommandation** : **Wazuh** est retenu comme la solution cible (Note 80/100). Il offre le meilleur compromis entre couverture fonctionnelle (File Integrity Monitoring (FIM), réponse active), maîtrise des coûts et indépendance technologique. **HarfangLab** (58/100) reste une alternative crédible pour des besoins de performance ou s'il y a nécessité d'une certification ANSSI.

Microsoft Defender Wazuh HarfangLab Elastic Security

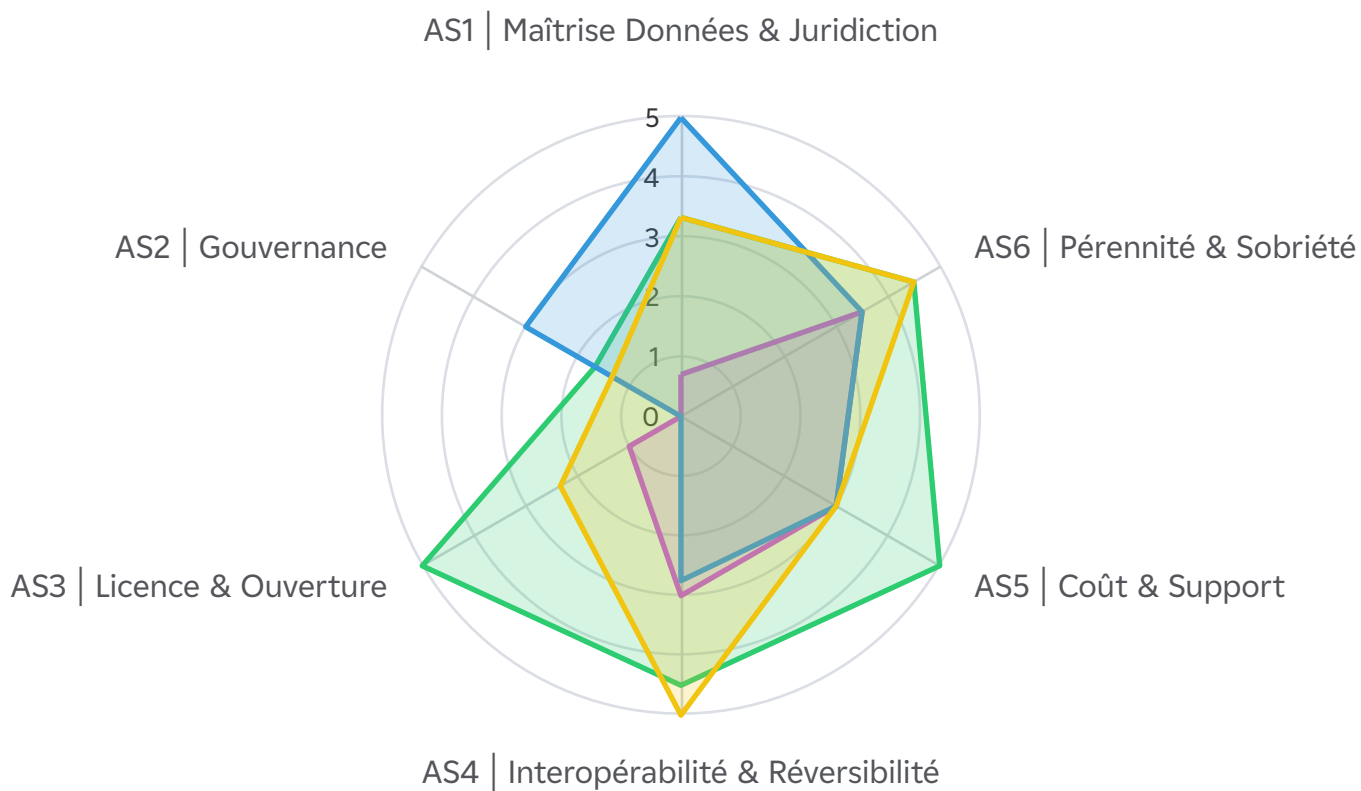


Fig. 11. - Comparatif des solutions EDR

## 8. Déclinaison opérationnelle de la migration

L'identification des solutions les plus pertinentes selon le contexte et les besoins de l'organisation permet désormais de structurer la trajectoire de déploiement effectif. Ce dernier chapitre décline de manière opérationnelle les phases de transition, en accordant une attention particulière au traitement de l'héritage technologique et à la continuité des usages métiers.

Il est essentiel de souligner que cette transition peut ne pas s'effectuer pas de manière isolée. L'adossement à des communautés d'expert-es et de pair-es partageant ces enjeux est un facteur clé de succès.

Plusieurs réseaux de référence peuvent être sollicités :

- **France Numérique Libre** : un collectif de responsables informatiques dédié à la promotion du logiciel libre dans le secteur public.
- **Adullact** et **l'April** : des associations incontournables qui sauront vous orienter vers les ressources et les compétences mutualisées les plus pertinentes.
- **PLOSS-RA** : pour identifier les entreprises du numérique libre, notamment en région Auvergne-Rhône-Alpes.

Enfin, pour une approche plus locale et événementielle, l'**Agenda du Libre** recense les rassemblements et ateliers techniques à proximité de votre organisation.

### 8.1. Socle commun et formats ouverts

La première étape consiste à sanctuariser un socle applicatif commun entre les postes Windows et le futur système d'exploitation GNU/Linux. L'objectif est d'habituer les utilisateur-rices à des outils libres, et de basculer les formats de fichiers vers des formats ouverts et interoperables.

En prenant le besoin de classification en termes de confidentialité suivant :

Niveaux	C0	C1	C2	C3
<b>Confidentialité</b>	Information « Libre »	Information « Interne »	Information « Restreinte »	Information « Confidentielle »
Description	Peut être rendue publique sans risque.	Peut être diffusée au périmètre de l'entreprise.	Limitée à un projet ou une mission particulière.	Accessible uniquement aux personnes nommément désignées.
<b>Protection</b>	Marquage	Marquage du document et corps du message	Marquage + Chiffrement	Marquage + Chiffrement qualifié ANSSI

Tableau 2. - Matrice de confidentialité pour échanger des données

#### 8.1.1. Brique fonctionnelle : Stockage et partage

Nextcloud ayant obtenu le meilleur score IAS pour la brique fonctionnelle stockage et partage, nous basons notre scénario de migration sur cet outil. Au-delà du stockage, la solution offre une réponse

native aux exigences de la Politique de Marquage et de Protection de l'Information (Microsoft Purview Information Protection (MPIP)).

## 8.2. Gestion de l'héritage MPIP

L'obstacle technique le plus critique lors d'une migration hors de Onedrive et Sharepoint concerne la gestion des étiquettes de sensibilité Microsoft MPIP (Microsoft Purview Information Protection) [76]. Ce dispositif, qui couple classification et chiffrement, crée une adhérence forte à l'écosystème Azure Active Directory : les documents chiffrés deviennent techniquement illisibles en dehors de la suite MS Office et sans authentification Microsoft.

Dans une stratégie de migration vers des solutions souveraines et open source (LibreOffice, Nextcloud), cette protection constitue un point de blocage majeur, rendant les archives inaccessibles.

Pour garantir la pérennité et l'interopérabilité du patrimoine documentaire, il est impératif lors de la migration de procéder à une opération de retrait complet des étiquettes de confidentialité et du chiffrement associé afin de pouvoir les transférer vers Nextcloud.

Des solutions techniques d'automatisation existent pour traiter les volumes importants de données sans intervention manuelle :

- L'utilisation de scripts PowerShell administrateur permet d'itérer sur l'ensemble des bibliothèques SharePoint et OneDrive pour retirer programmatiquement les étiquettes [77].
- Les retours d'expérience communautaires confirment la faisabilité de cette désactivation globale pour préparer l'export des données brutes vers le nouveau système [78], [79].

Une fois cette opération réalisée, les documents retrouvent un format ouvrable en dehors de l'écosystème Microsoft, prêts à être ingérés par Nextcloud et re-classifiés selon la politique interne de l'organisation.

### 8.2.1. Gestion des politiques de classification et de chiffrement des documents

Nextcloud intègre également des mécanismes permettant de décliner opérationnellement les niveaux de confidentialité (C0 à C3) définis précédemment. Cette implémentation s'appuie sur :

- **Les Étiquettes Système** : Si l'utilisateur·rice peut définir le niveau de confidentialité (C0 à C3) comme il-elle le faisait via MPIP, Nextcloud introduit des étiquettes gérées de manière centralisée par l'administration. Grâce au module *Automated Tagging* [80], le système peut marquer automatiquement un fichier selon son contenu (ex: détection de mots-clés, de formats de données sensibles) ou son emplacement. Ces étiquettes peuvent être rendues invisibles pour l'utilisateur·rice final, garantissant que le marquage reste intègre et ne soit pas supprimé par erreur.
- **Le Contrôle d'Accès aux Fichiers (File Access Control)** : Ce moteur de règles permet d'appliquer des restrictions dynamiques basées sur les étiquettes (ex: interdire le partage public d'un document marqué « C3 » ou bloquer l'accès depuis une IP hors du réseau sécurisé) [81].

## 8.2.2. Stratégie de migration progressive : Le modèle du Ministère Autrichien (BMWET)

Une stratégie de migration progressive est préconisée. Cette approche s'inspire du retour d'expérience du Ministère Fédéral Autrichien de l'Économie, de l'Énergie et du Tourisme (BMWET), qui a migré ses 1 200 collaborateur·ice·s vers Nextcloud pour garantir sa souveraineté numérique [82].

### 8.2.2.1. Le découplage interface / infrastructure de stockage

La stratégie mise en œuvre par le BMWET repose sur une architecture hybride transitoire. L'objectif est de dissocier l'interface utilisateur·rice de l'infrastructure de stockage des données.

Dans cette configuration, les utilisateur·rices conservent initialement leurs interfaces habituelles (Microsoft Outlook, Microsoft Teams) pour limiter la friction cognitive et le besoin de formation immédiat. Tandis que le stockage dans le cloud propriétaire (OneDrive, SharePoint) est progressivement désactivé et remplacé par Nextcloud, hébergé sur les infrastructures propres de l'organisation (On-Premise).

Cette intégration est rendue possible, par des connecteurs tiers (tels que **Sendent** [83] utilisé par le ministère autrichien) qui s'interfaçent directement dans les menus d'Outlook, de Teams et des applications Microsoft (Word, Powerpoint, ...). Concrètement, lorsqu'un·e utilisateur·rice envoie une pièce jointe ou partage un fichier dans une conversation Teams, le fichier est stocké de manière transparente sur le serveur Nextcloud sécurisé de l'organisation, et non sur le cloud public américain.

Par ailleurs, leur retour d'expérience souligne que l'accompagnement direct par les équipes de Nextcloud et de Sendent a été déterminant pour résoudre les points de blocage techniques. Cette approche permet d'établir une feuille de route de migration sur le temps long, où chaque phase renforce l'autonomie de l'organisation sans bloquer la production.

## 8.2.3. Socle commun applicatif

Dans le même temps, il est préconisé de déployer une offre de logiciels libres sur les postes de travail Windows existants, sans pour autant retirer immédiatement les outils propriétaires habituels. Cette stratégie vise à acculturer les utilisateur·rices en douceur, en laissant temporairement le choix de l'outil.

L'objectif est de démontrer la valeur ajoutée des solutions libres par la preuve et l'usage quotidien, plutôt que par la contrainte administrative.

### 8.2.3.1. Navigateur Web

La première étape consiste à préinstaller et configurer **Mozilla Firefox** comme alternative à **Google Chrome** ou **Edge**. Pour inciter à la bascule, la Direction des Systèmes d'Information (DSI) peut configurer Firefox avec des avantages immédiats pour les utilisateur·rices :

- Installation native de bloqueurs de publicités et de traqueurs (ex: <https://addons.mozilla.org/fr/firefox/addon/ublock-origin/> uBlock Origin), rendant la navigation plus fluide et rapide.
- Paramétrage par défaut des moteurs de recherche respectueux de la vie privée.
- Synchronisation des marque-pages sécurisée.

L'utilisateur·rice conserve la liberté d'utiliser Chrome, mais l'expérience nettoyée et optimisée de Firefox agit comme un levier naturel d'adoption.

### 8.2.3.2. Collaboratif

Une fois la bascule réussie de la brique « Stockage et Partage » vers Nextcloud l'organisation peut basculer vers un système de messagerie électronique hébergée en interne (Open-Xchange par exemple), s'affranchissant ainsi progressivement des serveurs Microsoft Exchange Online.

Il est préconisé de favoriser une transition douce. Comme montré par l'exemple de la migration plus de 30.000 boîtes mail, effectué par l'état germanique Schleswig-Holstein [84] le montre, **Mozilla Thunderbird** peut être déployé et configuré par défaut sur les postes Windows. Dans un premier temps ce dernier est relié à Microsoft Exchange Online ce qui permet d'habituer les utilisateur·rices à son interface. Une fois la bascule vers une messagerie internalisée, la configuration de **Mozilla Thunderbird** sera adaptée afin de pouvoir se connecter de manière transparente au nouvel environnement mail.

La stratégie de migration technique de Microsoft Exchange Online vers Open-Xchange, telle qu'illustrée par le retour d'expérience du SITPI [85] est graduelle. La migration s'appuie sur les travaux de la DINUM, qui a développé une suite d'outils d'automatisation (disponibles sur le dépôt dimail-infra) permettant un déploiement industrialisé et reproductible de l'infrastructure Open-Xchange. Tout d'abord une première phase synchronisation initiale, à l'aide d'outils comme Imapsync ou des connecteurs API spécifiques, permet de répliquer le contenu des boîtes mails (arborescences de dossiers, courriels et métadonnées de lecture) en arrière-plan depuis les serveurs Microsoft vers l'instance auto-hébergée. Ce processus s'effectue sans interruption pour l'utilisateur·rice, qui continue de travailler sur son environnement habituel. Ensuite, le jour de la migration effective, une dernière passe de synchronisation (« delta ») est effectuée pour récupérer les messages reçus depuis la phase initiale. Une fois cette cohérence de données assurée, la migration se concrétise au niveau du poste de travail, le client Mozilla Thunderbird, déjà déployé et maîtrisé par les utilisateur·rices, voit sa configuration de serveur modifiée. Ce changement permet de basculer de manière transparente vers la messagerie internalisée, dans un environnement technique désormais maîtrisé.

### 8.2.3.3. Messagerie instantanée

Dans la même veine, en remplacement des solutions de discussion propriétaires (Microsoft Teams), l'organisation va basculer ses échanges temps réel vers Element (s'appuyant sur le protocole de communication décentralisé et ouvert Matrix).

D'un point de vue opérationnel, cette transition repose sur l'internalisation du service via le déploiement de son propre **homeserver** (généralement via l'implémentation Synapse). Cette internalisation garantit que l'intégralité de la base de données (messages, fichiers partagés et surtout les métadonnées) reste sous la juridiction technique et juridique de l'entité. Sur le plan de la sécurité, l'architecture bascule vers un modèle où le chiffrement de bout en bout (E2EE), activé par défaut, rend les échanges techniquement inaccessibles aux administrateur·ice·s eux-mêmes. Enfin, la fluidité des interconnexions est assurée par le mécanisme de fédération, qui permet de collaborer directement avec d'autres entités externes compatibles sans la lourdeur administrative de la gestion des comptes invités.

### 8.2.3.4. Suite bureautique

Sur le volet production documentaire, l'objectif est d'habituer les équipes à l'interface et aux formats libres avant la migration du système d'exploitation.

- **Format par défaut : LibreOffice** est installé sur tout le parc et défini comme programme par défaut pour les formats ouverts (ODF), ce guide [75] rédigé par The Document Foundation est intéressant à suivre.
- **Ergonomie adaptative** : L'interface à onglets est activée pour offrir une expérience visuelle proche du ruban Microsoft, réduisant la friction pour les habitués.
- **Cohabitation** : La suite Microsoft Office reste disponible dans un premier temps pour traiter les documents hérités complexes, mais n'est plus l'outil privilégié pour les nouveaux documents.

Cette phase de tuilage permet aux équipes de valider l'adhésion aux interfaces libres (Thunderbird, Firefox, LibreOffice) sur le parc Windows actuel. Elle permet de réduire considérablement le choc cognitif lors de la future bascule vers un système d'exploitation GNU/Linux, l'environnement applicatif étant déjà familier et maîtrisé.

### 8.2.3.5. Gestion de la transition et problématique des macros

Concernant l'usage de macros VBA (Visual Basic for Applications) au sein de la suite Microsoft Office, d'un point de vue systémique, la prolifération de macros complexes dans les services est souvent le signe que le système d'information n'a pas su répondre aux besoins métiers. L'utilisateur-riche, faute d'outil adapté, bricole une automatisation sur Microsoft Excel. L'objectif stratégique est donc de remplacer ces tableaux fragiles par des outils pérennes (applications web dédiées, formulaires Nextcloud, ou intégrations API), rendant la macro obsolète par conception.

Pour les documents qui ne peuvent être immédiatement remplacés par un outil métier, trois trajectoires peuvent être définies :

1. **Compatibilité native** : LibreOffice a réalisé des progrès significatifs dans l'exécution du code VBA [86]. Pour les macros simples, la transition est transparente.
2. **Réécriture** : Pour les macros critiques, un projet de portage vers LibreOffice Basic ou Python (mieux intégré et plus puissant) peut être engagée. C'est l'occasion d'assainir le code et d'en assurer la maintenance future. Ce travail de portage peut être assuré par des prestataires qualifiés comme l'entreprise OpenGo. OpenGo accompagne les organisations pendant toute la durée de la migration, leurs services couvrent toute la chaîne de déploiement allant de la formation au portage des documents.
3. **Abandon** : Si le coût de réécriture est supérieur à la valeur métier, le processus est simplifié ou abandonné. C'est un levier de réduction de la dette technique.

### 8.2.4. Nécessité d'interopérabilité

L'impératif d'interopérabilité, rigoureusement documenté par la Direction Interministérielle du Numérique (DINUM) est un enjeu de souveraineté et de pérennité patrimoniale. L'adoption systématique du format standardisé ODF (Open Document Format, norme ISO/IEC 26300) permet de rompre la dépendance imposée par les formats propriétaires, dont l'opacité et les variations de spécifications au fil des versions induisent une obsolescence des archives numériques. D'un point de vue structurel, l'indépendance de la donnée vis-à-vis de son outil de traitement garantit que les documents produits par l'organisation restent exploitables sur le temps long, indépendamment des évolutions commerciales ou des changements unilatéraux de licences des éditeurs hégémoniques. Cette approche, alignée sur les préconisations du Référentiel Général d'Interopérabilité [87], transforme la donnée d'un format captif en un actif universel

et ouvert, neutralisant ainsi les coûts de sortie de l'écosystème propriétaire tout en sécurisant l'accès à l'information pour les décennies à venir.

### 8.3. Transition au niveau du système d'exploitation

Une fois le découplage entre le système d'exploitation et les logiciels effectué, et le socle applicatif commun adopté par la majorité des utilisateur·rices, la migration du système d'exploitation peut s'engager. Cette transition doit être pilotée comme un projet critique, en suivant une méthodologie itérative.

#### 8.3.1. Phase 2 : Validation technique (POC)

Cette étape initiale cible un périmètre restreint (volontaires + management). C'est également ici l'occasion pour les équipes techniques de monter en compétences sur les logiciels qui ont été choisis pour infogérer le parc informatique GNU/Linux.

Cette phase de montée en compétence est une réponse directe aux résistances techniques. En valorisant l'expertise sur des technologies libres et auditables, l'organisation transforme la crainte de l'obsolescence professionnelle en une opportunité de montée en gamme des profils RH. La DSI devient ainsi capable d'assurer la maintenance de l'outillage de manière autonome, garantissant la pérennité du système d'information.

#### 8.3.2. Phase 2 : Validation technique et socle (POC)

Cette étape initiale cible un périmètre restreint (volontaires + management stratégique). L'objectif est surtout politique, il faut montrer la viabilité de la solution par l'exemplarité de la hiérarchie et en levant les potentiels blocages techniques critiques.

Sur le plan technique, ce POC (Proof of Concept) doit valider :

- **L'intégration au réseau et à l'annuaire** : Authentification centralisée (LDAP), montage des partages réseaux, application des politiques de sécurité.
- **La compatibilité matérielle** : Validation des pilotes pour l'ensemble du parc cible (imprimantes, docking stations, gestion de l'énergie sur les portables).
- **La pile de sécurité** : Fonctionnement du VPN, chiffrement des disques (LUKS), et des solutions EDR/Antivirus.

C'est également l'occasion pour les équipes techniques de monter en compétences sur l'administration du parc GNU/Linux (gestion de paquets, scripting). La DSI doit sortir de cette phase avec une première version du poste fonctionnel, et l'infrastructure de Maintenance en Condition Opérationnelle (MCO) du parc informatique maîtrisée et déployée garantissant ainsi l'autonomie du service.

#### 8.3.3. Phase 3 : Pilote et confrontation aux métiers

Le périmètre est étendu à un échantillon représentatif de la diversité des métiers, sur la base du volontariat, incluant des profils « nomades » et « sédentaires ».

L'objectif est d'identifier les **frictions opérationnelles** non détectées pendant la phase de POC. Un canal de support dédié est mis en place afin de garantir une résolution rapide des incidents et une collecte précise des retours d'expérience.

Pour chaque blocage métier identifié, une réponse technique standardisée est définie :

- **Virtualisation locale ou applicative** : Pour les besoins ponctuels d'outils Windows spécifiques. Wine permet d'exécuter des logiciels Windows directement sur un poste Linux, sans avoir besoin d'installer le système Windows lui-même. Il sert de traducteur pour que les applications métiers spécifiques, qui n'existent pas encore en version libre ou web, continuent de fonctionner normalement. C'est une solution beaucoup plus légère et rapide qu'une machine virtuelle, permettant d'assurer la continuité du travail sans alourdir le matériel.
- **Bureaux distants (VDI/RDP)** : Cette solution permet d'accéder à distance à un environnement Windows complet ou à une application spécifique hébergée sur un serveur centralisé. Le logiciel ne s'exécute pas sur le poste de l'utilisateur-riche, mais sur le serveur de la DSI, seule le flux vidéo s'affiche à l'écran. C'est la solution pour les outils métiers complexes, incompatibles avec GNU/Linux, tout en permettant de conserver un poste de travail local sécurisé et souverain.
- **Alternatives Web** : La stratégie consiste ici à remplacer les logiciels par des applications accessibles via un navigateur web. Qu'il s'agisse de solutions internes ou de services en ligne.

Cette phase ne se conclut que lorsque tous les incidents bloquants sont levés.

### 8.3.4. Phase 4 : Industrialisation et automatisation

C'est la phase critique de massification. Elle s'appuie sur l'automatisation pour absorber la charge sans dépasser les capacités de support. Elle s'adosse au cycle naturel de renouvellement du matériel (10 à 15% du parc par an).

Tout-e collaborateur-ice éligible au renouvellement de son ordinateur se voit proposer par défaut un modèle sous GNU/Linux. L'accession à poste Windows reste possible, mais uniquement sur demande explicite, inversant ainsi la charge de l'inertie.

Le déploiement manuel est proscrit. L'utilisation d'outils de gestion de configuration est impérative pour garantir l'homogénéité du parc. Le provisionnement des postes doit tendre vers l'automatisation via l'installation réseau (PXE) et des configurations automatique.

Pour faciliter la transition, il faut prévoir un utilitaire permettant de migrer les données locales du poste de travail Windows vers le poste de travail GNU/Linux. Pour ce qui est des logiciels du socle commun applicatif, l'utilisateur-riche retrouvera les mêmes outils que sur son poste Windows.

### 8.3.5. Phase 5 : Inversion de la norme et gestion de l'héritage

Une fois la masse critique atteinte (généralement après deux à quatre ans), le poste GNU/Linux devient le standard unique.

L'attribution d'un poste Windows dérogatoire obéit à un processus strict :

1. **Justification métier** : Preuve d'incompatibilité logicielle sans contournement (virtualisation/web) possible.
2. **Validation hiérarchique** : Accord de la direction pour assumer le surcoût de support associé.

## 9. Conclusion

---

Cette étude démontre que la souveraineté numérique du poste de travail ne peut plus être considérée comme une option technique, mais s'impose comme un impératif de résilience stratégique, juridique et environnementale pour les organisations européennes. L'analyse approfondie des briques logicielles actuelles, majoritairement structurées autour de l'écosystème Microsoft, révèle une dépendance critique caractérisée par une exposition aux lois extraterritoriales américaines et un verrouillage propriétaire limitant l'autonomie décisionnelle.

Face à ce constat, l'Indice d'Autonomie Stratégique a permis d'identifier des alternatives robustes issues du logiciel libre, telles que Debian pour le système d'exploitation, Nextcloud pour le stockage collaboratif et Libre Office pour la productivité bureautique, offrant des garanties de transparence et de maîtrise technique supérieures. La réussite d'une telle transition repose moins sur la substitution brutale des outils que sur une trajectoire de migration progressive et pilotée, débutant par la sanctuarisation d'un socle applicatif commun et l'adoption de formats ouverts.

En définitive, le passage vers un environnement souverain nécessite un portage politique fort au plus haut niveau de l'organisation afin de transformer la dépense en licences propriétaires en un investissement stratégique dans le capital humain et la maîtrise opérationnelle interne. Cette démarche, bien que complexe, permet de réaligner l'outil informatique avec les engagements RSE tout en garantissant la pérennité du patrimoine informationnel face aux aléas géopolitiques mondiaux.

## Glossaire

---

**DSI - Direction des Systèmes d'Information:** Organe stratégique d'une organisation chargé de concevoir, de mettre en œuvre et de maintenir l'ensemble des ressources informatiques (matériel, logiciels, réseaux). [83](#), [86](#), [87](#)

**EDR - Endpoint Detection and Response:** Solution de sécurité installée sur les terminaux (postes de travail) assurant la surveillance comportementale pour détecter et bloquer les processus malveillants en temps réel. [31](#), [34](#), [77](#), [78](#), [89](#)

**FIM - File Integrity Monitoring:** Technologie de surveillance de l'intégrité des fichiers permettant de détecter en temps réel toute modification, création ou suppression non autorisée de fichiers critiques du système. Cette fonctionnalité est une composante essentielle des solutions de sécurité de type **EDR**, pour assurer la conformité et détecter les tentatives d'intrusion ou de corruption du système. [79](#)

**IAS - Indice d'Autonomie Stratégique:** Méthodologie d'évaluation quantitative élaborée dans le cadre de cette étude pour mesurer le niveau de souveraineté d'une solution numérique. Noté sur 100, cet indice évalue la solution selon six piliers fondamentaux : la maîtrise des données & la juridiction, la gouvernance de l'éditeur, l'ouverture de la licence, l'interopérabilité technique, la maîtrise des coûts & la pérennité. Il sert d'outil d'aide à la décision pour sélectionner les alternatives logicielles minimisant les risques de dépendance technologique. [6](#), [8](#), [9](#), [9](#), [14](#), [15](#), [15](#), [26](#), [26](#), [26](#), [26](#), [26](#), [43](#), [88](#)

**MPIP - Microsoft Purview Information Protection:** Technologie propriétaire de classification et de chiffrement des documents liée à Azure Active Directory, créant une adhérence forte qui rend les fichiers illisibles en dehors de l'écosystème Microsoft sans opération de déchiffrement préalable. [82](#), [82](#)

**TCO - Total Cost of Ownership:** Coût Total de Possession. Indicateur financier intégrant non seulement le coût d'acquisition des licences, mais aussi les coûts de maintenance, de formation, de support et de matériel sur l'ensemble du cycle de vie. [11](#), [22](#), [35](#), [35](#), [60](#), [76](#), [78](#)

**Autonomie stratégique - autonomie stratégique:** Capacité opérationnelle à agir librement, à choisir ses dépendances et à ne pas être soumis à la coercition d'un tiers (fournisseur ou état étranger). L'objectif n'est pas l'autarcie, mais la maîtrise des dépendances critiques. [5](#), [5](#), [8](#), [8](#), [8](#), [14](#), [55](#), [91](#)

**CapEx - dépenses d'investissement:** Investissements destinés à créer une valeur durable ou à acquérir des actifs à long terme. La migration vers le logiciel libre permet de transformer une part de l'OpEx en CapEx en investissant dans le capital humain, l'expertise interne et la pérennité du système d'information. [35](#)

**cloud - Infrastructure nuagique:** Modèle permettant d'accéder à des ressources informatiques (serveurs, stockage, applications) via [Internet](#), sans avoir à gérer l'infrastructure physique locale. [7](#), [8](#), [8](#), [10](#), [10](#), [10](#), [31](#), [32](#), [32](#), [73](#), [76](#)

**CLOUD Act - Clarifying Lawful Overseas Use of Data Act:** Loi fédérale américaine permettant aux autorités des États-Unis d'accéder aux données hébergées par leurs entreprises, quelle que soit la localisation géographique des serveurs (y compris en Europe), créant un risque d'ingérence étrangère [20]. [6](#), [6](#), [10](#), [14](#), [17](#), [28](#), [29](#), [29](#), [30](#), [31](#), [32](#), [32](#), [33](#), [48](#), [74](#), [76](#), [90](#), [90](#), [91](#), [91](#)

**Cloud First - priorité au nuage:** Stratégie informatique consistant à privilégier systématiquement les solutions de cloud computing lors du déploiement de nouveaux services ou de la modernisation d'infrastructures, avant d'envisager des solutions hébergées localement, On-Premise. [7](#), [27](#), [34](#)

**communs numériques:** Ressources numériques produites et gérées collectivement par une communauté selon des règles d'auto-gouvernance. Ils se caractérisent par un accès ouvert et l'absence d'appropriation exclusive (ex: Wikipédia, logiciels libres, OpenStreetMap). [12](#)

**ecs - Elastic Common Schema:** Spécification de format de données open source définissant un ensemble commun de champs à utiliser lors du stockage de données de journaux (logs) et de métriques dans Elasticsearch. Ce standard facilite l'interopérabilité et l'analyse croisée des données provenant de sources hétérogènes au sein d'un écosystème de sécurité. [79](#)

**extraterritorialité - Extraterritorialité:** Capacité d'une loi nationale à s'appliquer en dehors de ses frontières (ex: le Clarifying Lawful Overseas Use of Data Act américain s'appliquant aux données stockées en Europe par des entreprises US). [6](#), [90](#)

**FISA - Foreign Intelligence Surveillance Act:** Loi fédérale américaine de 1978 encadrant la surveillance du renseignement étranger. Sa section 702 (ajoutée en 2008) est particulièrement critique pour la souveraineté numérique européenne : elle autorise les agences de renseignement américaines (NSA, FBI) à exiger des fournisseurs de services numériques américains (tels que Microsoft, Google ou AWS) la communication des données de communication de personnes non-américaines situées hors des États-Unis. Ce dispositif, qui fonctionne sans mandat judiciaire individualisé, constitue avec le CLOUD Act l'un des principaux vecteurs de l'extraterritorialité du droit américain, exposant les données hébergées par ces prestataires à un risque légal de captation. [6](#), [17](#), [28](#), [29](#), [31](#), [32](#), [32](#), [33](#)

**fork:** Action de dérivation d'un dépôt de code source pour pouvoir y apporter des modifications indépendantes sans affecter le projet original. [15](#), [15](#), [60](#), [76](#)

**GNU/Linux:** Linux est un système d'exploitation libre et open source de type Unix, basé sur le noyau Linux créé en 1991 par Linus Torvalds. De nombreuses distributions Linux ont depuis vu le jour et constituent un important vecteur de popularisation du mouvement du logiciel libre. À l'origine, le terme Linux ne désignait que le noyau de système d'exploitation Linux. Puis, par métonymie, l'usage du terme Linux s'est répandu pour décrire tant le noyau Linux que le système d'exploitation au sens large, qui contenait plus de logiciels issus du projet GNU que du projet Linux. Le nom GNU/Linux a été initié par Debian à la demande de Richard Stallman, pour créditer à la fois les développeurs de GNU (les logiciels système) et de Linux (le noyau). [35](#), [35](#), [35](#), [35](#), [37](#), [37](#), [37](#), [38](#), [38](#), [38](#), [38](#), [39](#), [39](#), [39](#), [39](#), [39](#), [40](#), [40](#), [40](#), [40](#), [40](#), [41](#), [41](#), [41](#), [51](#), [51](#), [54](#), [65](#), [73](#), [73](#), [74](#), [86](#), [86](#), [87](#), [87](#), [87](#), [87](#)

**logiciel libre - logiciels libres:** Logiciel dont la licence garantit juridiquement les libertés d'utiliser, étudier, modifier et redistribuer le code. Contrairement à l'Open Source qui est un modèle de développement, le Logiciel Libre est une approche garantissant le transfert de maîtrise intégrale de l'outil à l'organisation. [5](#), [7](#), [8](#), [8](#), [11](#), [55](#)

**ml - Machine Learning (Apprentissage Automatique):** Champ d'étude de l'intelligence artificielle qui s'appuie sur des approches mathématiques et statistiques pour permettre aux ordinateurs d'apprendre à partir de données. Dans le contexte des solutions de sécurité comme Elastic Security, ces fonctions avancées sont utilisées pour la détection d'anomalies comportementales, mais font souvent l'objet d'une tarification spécifique. [79](#)

*On-Premise* - **On-Premise**: Mode d'hébergement où les logiciels et les données sont installés sur les infrastructures locales propres de l'organisation, garantissant un contrôle total des données et des clés de chiffrement, par opposition au SaaS ou au Cloud public. [27](#), [66](#), [70](#), [74](#), [83](#), [90](#), [91](#)

*OpEx* - **dépenses d'exploitation**: Charges courantes nécessaires au fonctionnement quotidien d'une organisation. Dans le modèle informatique propriétaire, l'OpEx inclut les abonnements SaaS et les rentes de licences logicielles, souvent caractérisés par une absence de levier de négociation et une captivité vis-à-vis de l'éditeur. [35](#), [78](#)

**OS - système d'exploitation**: Ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs (ex: Windows, macOS, Linux, Android). [10](#), [12](#), [39](#), [39](#), [39](#)

**RSE - Responsabilité Sociétale des Entreprises**: Intégration volontaire par les entreprises de préoccupations sociales et environnementales à leurs activités commerciales et à leurs relations avec les parties prenantes. C'est la contribution des entreprises aux enjeux du développement durable. [7](#), [8](#), [10](#), [88](#)

**SaaS - Software as a Service**: Modèle de distribution où le logiciel est hébergé et opéré par le fournisseur sur ses propres infrastructures. Dans le cadre de cet audit, ce modèle est souvent qualifié de « captif » et identifié comme un risque pour l'Autonomie stratégique en raison de l'exposition juridique (CLOUD Act) et de l'impossibilité pour l'organisation de maîtriser totalement ses données, par opposition au modèle On-Premise. [10](#), [22](#), [22](#), [28](#), [33](#), [63](#), [91](#)

*Souveraineté numérique* - **souveraineté numérique**: Capacité de l'État ou de l'organisation à faire respecter ses droits et sa législation dans le cyberspace. Elle s'oppose à l'extra-territorialité du droit (ex: CLOUD Act). C'est une notion juridique distincte de l'autonomie stratégique. Cette distinction est critique pour éviter le « sovereign washing », une pratique consistant à utiliser le terme souveraineté comme un simple argument marketing pour masquer des dépendances technologiques réelles [26]. [5](#), [5](#), [14](#)

## Bibliographie

---

- [1] Café de la bourse, « TOP 10 des plus grandes sociétés au monde par capitalisation boursière en 2026 ». [En ligne]. Disponible sur: <https://www.cafedelabourse.com/actualites/societes-plus-grandes-capitalisations-boursieres>
- [2] D. Bradbury, « Le débat sur la réautorisation de la section 702 de la FISA a des implications transatlantiques ». [En ligne]. Disponible sur: <https://fr.isms.online/data-protection/fisa-section-702-reauthorization-debate-carries-transatlantic-implications/>
- [3] Sénat, « Commande publique : audition de Microsoft », 2025. [En ligne]. Disponible sur: [https://www.youtube.com/watch?v=\\_psdHMc16cM&t=1633s](https://www.youtube.com/watch?v=_psdHMc16cM&t=1633s)
- [4] Stockholm Resilience Center, « Planetary boundaries ». [En ligne]. Disponible sur: <https://www.stockholmresilience.org/research/planetary-boundaries.html>
- [5] A. Stephant, « Les Métaux de la Révolution 4.0 ». [En ligne]. Disponible sur: <https://www.systext.org/node/1568>
- [6] P. Marissal et E. Polselli, « Fin de Windows 10 : un immense gâchis économique et écologique », 2025, [En ligne]. Disponible sur: <https://web.archive.org/web/20250928180441/https://www.humanite.fr/social-et-economie/microsoft/fin-de-windows-10-un-immense-gachis-economique-et-ecologique>
- [7] Greenpeace, « La pollution numérique, qu'est-ce que c'est ? ». [En ligne]. Disponible sur: <https://www.greenpeace.fr/la-pollution-numerique/>
- [8] ONU, « Le chef des droits de l'homme de l'ONU dénonce l'exploitation illégale des minerais dans l'Est de la RDC ». [En ligne]. Disponible sur: <https://news.un.org/fr/story/2024/10/1149526>
- [9] Amnesty, « Alimenter le changement ou le statu quo ? ». [En ligne]. Disponible sur: <https://www.amnesty.org/fr/latest/news/2023/09/drc-cobalt-and-copper-mining-for-batteries-leading-to-human-rights-abuses/>
- [10] factually, « Did Microsoft or Amazon end contracts with ICE and when? ». [En ligne]. Disponible sur: <https://factually.co/fact-checks/business/did-microsoft-or-amazon-end-ice-contracts-when-0ce9c9>
- [11] J. Washington, « Google Fulfilled ICE Subpoena Demanding Student Journalist's Bank and Credit Card Numbers ». [En ligne]. Disponible sur: <https://theintercept.com/2026/02/10/google-ice-subpoena-student-journalist/>
- [12] Wikipédia, « Principe de Kerckhoffs ». [En ligne]. Disponible sur: [https://fr.wikipedia.org/wiki/Principe\\_de\\_Kerckhoffs](https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs)
- [13] ANSSI, « Posture générale et actions de l'ANSSI sur l'open-source ». [En ligne]. Disponible sur: <https://cyber.gouv.fr/enjeux-technologiques/open-source/>
- [14] aDRI, « IRN ». [En ligne]. Disponible sur: <https://resiliencenumerique.com/>

- [15] Commission Européenne, « Cloud Sovereignty Framework », technical report, 2025. [En ligne]. Disponible sur: [https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113\\_en?filename=Cloud-Sovereignty-Framework.pdf](https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf)
- [16] Cigref, « La dépendance technologique aux softwares & cloud services américains : une estimation des conséquences économiques en Europe ». [En ligne]. Disponible sur: <https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe>
- [17] European Commission, « State of the Digital Decade 2025 report ». [En ligne]. Disponible sur: <https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report>
- [18] Eurostat, « Cloud computing - statistics on the use by enterprises ». [En ligne]. Disponible sur: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud\\_computing\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises)
- [19] ecdpm, « Tech sovereignty and a new EU foreign economic policy ». [En ligne]. Disponible sur: <https://ecdpm.org/work/tech-sovereignty-and-new-eu-foreign-economic-policy>
- [20] N. Verliac, « CLOUD Act : législation américaine sur l'accès extraterritorial aux données », 2025, [En ligne]. Disponible sur: <https://blog.ostraca.fr/blog/cloud-act-legislation-extraterritoriale-donnees/>
- [21] N. Verliac, « Souveraineté numérique : quand les infrastructures américaines deviennent des armes géopolitiques », 2025, [En ligne]. Disponible sur: <https://blog.ostraca.fr/blog/souverainete-numerique-controle-americain-infrastructures/#cinq-cas-r%C3%A9v%C3%A9lateurs-de-d%C3%A9pendance-technologique>
- [22] M. Clavey, « Sanctions US : un juge de la CPI n'a plus accès aux services numériques américains », *Next*, 2025, [En ligne]. Disponible sur: <https://next.ink/206366/sanctions-us-un-juge-de-la-cpi-na-plus-acces-aux-services-numeriques-americains/>
- [23] ISC-PIF, « Juge Guillou, Cour Pénale Internationale - Soirée ISC-PIF #20Janvier 2026 », 2026. [En ligne]. Disponible sur: <https://vimeo.com/1158584868>
- [24] Cigref, « L'approche low-tech au service de la résilience numérique des organisations ». [En ligne]. Disponible sur: <https://www.cigref.fr/wp/wp-content/uploads/2026/02/Rapport-Lapproche-low-tech-au-service-de-la-resilience-numerique-des-organisations-Fevrier-2026-Cigref.pdf>
- [25] Underscore\_, « L'emprise inquiétante de Microsoft sur les écoles françaises », 2026. [En ligne]. Disponible sur: <https://www.youtube.com/watch?v=rdRDGjOGiUM>
- [26] Hanna, « "Nuage souverain" ou "lavage souverain" ? Un cheval de Troie aux portes de l'Europe numérique. », 2025, [En ligne]. Disponible sur: <https://tuta.com/fr/blog/sovereign-washing>
- [27] O. Coelho, *Géopolitique du numérique - L'impérialisme à pas de géants*. Éditions de l'Atelier, 2025.
- [28] Cigref, « Communiqué de Presse : Indice de Résilience Numérique ». Consulté le: 24 novembre 2025. [En ligne]. Disponible sur: <https://assets.rte-france.com/prod/public/2025-07/2025-07-04-cp-indice-resilience-numerique.pdf>
- [29] ANSSI, « SecNumCloud - Référentiel d'exigences ». 2022. [En ligne]. Disponible sur: <https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf>

- [30] L. Soler, « Grille d'évaluation de l'indice d'autonomie stratégique ». [En ligne]. Disponible sur: [https://gitlab.com/pfe25-t-507/rapport/-/raw/main/data/ias/questionnaire-ias-v1.0-template.ods?ref\\_type=heads&inline=false](https://gitlab.com/pfe25-t-507/rapport/-/raw/main/data/ias/questionnaire-ias-v1.0-template.ods?ref_type=heads&inline=false)
- [31] Libre à vous !, « Gendarmerie nationale et logiciels libres », 2019, [En ligne]. Disponible sur: <https://www.librealire.org/libre-a-vous-radio-cause-commune-transcription-de-l-emission-du-3-septembre-2019#Gendarmerie-nationale-et-logiciels-libres>
- [32] N. Vivant, « Passer au libre, c'est changer de monde ! », 2025, [En ligne]. Disponible sur: <https://www.librealire.org/passer-au-libre-c-est-changer-de-monde>
- [33] C. Chassagne, *Migrer son système d'information vers les logiciels libres - Un défi politique et technique pour les collectivités*. Territorial éditions, 2024. [En ligne]. Disponible sur: <https://boutique.territorial.fr/migrer-systeme-information-logiciels-libres.html>
- [34] Schleswig Holstein, « Open Innovation and Open Source Strategy of Land Schleswig-Holstein ». [En ligne]. Disponible sur: [https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Service/Downloads/\\_dateien/open-source-strategy\\_EN.pdf?\\_\\_blob=publicationFile&v=3](https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Service/Downloads/_dateien/open-source-strategy_EN.pdf?__blob=publicationFile&v=3)
- [35] M. Dogguy, « Scibian, a distro for industrial R&D and engineering », Debconf, 2017. [En ligne]. Disponible sur: <https://debconf17.debconf.org/talks/145/>
- [36] Atos, « Études de veille 2021-2024 : Le poste de travail Linux », 2022, [En ligne]. Disponible sur: <https://gitlab.adullact.net/marche-sll/etudes-de-veille#le-poste-de-travail-linux>
- [37] Atos, « Poste de travail Linux : Annexe Retour d'expérience », 2022, [En ligne]. Disponible sur: [https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package\\_files/360/download](https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package_files/360/download)
- [38] Atos, « Poste de travail Linux : État de l'art et conduite du changement », 2022, [En ligne]. Disponible sur: [https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package\\_files/361/download](https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package_files/361/download)
- [39] Commission Européenne, « Declaration of Independence: The LiMux Project in Munich », 2011, [En ligne]. Disponible sur: <https://interoperable-europe.ec.europa.eu/sites/default/files/document/2011-12/IDABC.OSOR.casestudy.LiMux.pdf>
- [40] Commission Européenne, « Towards the freedom of the operating system: The French Gendarmerie goes for Ubuntu », 2012, [En ligne]. Disponible sur: <https://interoperable-europe.ec.europa.eu/sites/default/files/document/2012-02/IDABC.OSOR.casestudy.Gendarmerie.10.pdf>
- [41] ZDNET, « Microsoft moins cher que l'Open Source ? Non rétorque la ville de Munich », 2013, [En ligne]. Disponible sur: <https://www.zdnet.fr/actualites/microsoft-moins-cher-que-l-open-source-non-retorque-la-ville-de-munich-39787057.htm>
- [42] V. Rieß-Marchive, « Peter Hofmann, LiMux : « l'adoption était essentielle » », 2014, [En ligne]. Disponible sur: <https://web.archive.org/web/20250808143035/https://www.lemagit.fr/reponse/Peter-Hofmann-LiMux-ladoption-etait-essentielle>
- [43] Le MagIT, « La stratégie gagnante d'une migration du poste de travail sous Linux », 2021, [En ligne]. Disponible sur: <https://web.archive.org/web/20250613064051/https://www.lemagit.fr/etude/La-strategie-gagnante-dune-migration-du-poste-de-travail-sous-Linux>
- [44] Atos, « Poste de travail Linux : Annexe Accessibilité », 2022, [En ligne]. Disponible sur: [https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package\\_files/358/download](https://gitlab.adullact.net/marche-sll/etudes-de-veille/-/package_files/358/download)

- [45] The Debian Project, « Constitution for the Debian Project ». [En ligne]. Disponible sur: <https://www.debian.org/devel/constitution>
- [46] The Debian Project, « Debian Mirrors (worldwide) ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://www.debian.org/mirror/list>
- [47] The Debian Project, « Diversity Statement ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://www.debian.org/intro/diversity>
- [48] The Debian Project, « Debian Social Contract ».
- [49] The Debian Project, « Documentation ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://www.debian.org/doc/>
- [50] The Debian Project, « Debian Contributors list ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://contributors.debian.org/>
- [51] The Debian Project, « Debian partners ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://www.debian.org/partners/>
- [52] The Debian Project, « Extended Long Term Support ». [En ligne]. Disponible sur: <https://wiki.debian.org/LTS/Extended>
- [53] The Debian Project, « Debian ports ». [En ligne]. Disponible sur: <https://www.debian.org/ports/>
- [54] The Debian Installer team, « Debian GNU/Linux Installation Guide ». [En ligne]. Disponible sur: <https://www.debian.org/releases/stable/installmanual>
- [55] The openSUSE project, « Guiding principles ». [En ligne]. Disponible sur: [https://en.opensuse.org/openSUSE:Guiding\\_principles](https://en.opensuse.org/openSUSE:Guiding_principles)
- [56] The openSUSE project, « Mirrors Report ». [En ligne]. Disponible sur: <https://mirrors.opensuse.org/>
- [57] SUSE, « EQT Private Equity Announces Voluntary Public Purchase Offer and Intention to Delist SUSE », août 2023, [En ligne]. Disponible sur: <https://www.suse.com/news/eqt-announces-voluntary-public-purchase-offer-and-intention-to-delist-suse/>
- [58] The openSUSE project, « Members ». [En ligne]. Disponible sur: <https://en.opensuse.org/openSUSE:Members>
- [59] The openSUSE project, « License ». [En ligne]. Disponible sur: <https://en.opensuse.org/openSUSE:License>
- [60] The openSUSE project, « Sponsors ». [En ligne]. Disponible sur: <https://en.opensuse.org/Sponsors>
- [61] The openSUSE project, « Hardware requirements ». [En ligne]. Disponible sur: [https://en.opensuse.org/Hardware\\_requirements](https://en.opensuse.org/Hardware_requirements)
- [62] The Fedora Project, « Fedora Council Charter ». [En ligne]. Disponible sur: <https://docs.fedoraproject.org/en-US/council/>
- [63] The Fedora Project, « Get Involved ». [En ligne]. Disponible sur: <https://docs.fedoraproject.org/en-US/project/join/>
- [64] The Fedora Project, « License of Fedora Linux ». [En ligne]. Disponible sur: <https://docs.fedoraproject.org/en-US/legal/fedora-linux-license/>

- [65] The Fedora Project, « Fedora's Mission and Foundations ». [En ligne]. Disponible sur: <https://docs.fedoraproject.org/en-US/project/>
- [66] The Fedora Project, « Fedora Sponsors ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://fedoraproject.org/en/sponsors/>
- [67] The Fedora Project, « Fedora Linux Release Life Cycle ». [En ligne]. Disponible sur: <https://docs.fedoraproject.org/en-US/releases/lifecycle/>
- [68] The Fedora Project, « Hardware Overview ». [En ligne]. Disponible sur: [https://docs.fedoraproject.org/en-US/fedora/latest/release-notes/hardware\\_overview/](https://docs.fedoraproject.org/en-US/fedora/latest/release-notes/hardware_overview/)
- [69] Ubuntu, « Project Governance ». [En ligne]. Disponible sur: <https://ubuntu.com/community/docs/governance>
- [70] Ubuntu, « Ubuntu open-source licences ». [En ligne]. Disponible sur: <https://canonical.com/legal/open-source-licences>
- [71] Ubuntu, « Canonical ». Consulté le: janvier 2026. [En ligne]. Disponible sur: <https://ubuntu.com/community/docs/governance/canonical>
- [72] Ubuntu, « Installation/SystemRequirements ». [En ligne]. Disponible sur: <https://help.ubuntu.com/community/Installation/SystemRequirements>
- [73] L. Soler, « Grille d'évaluation IAS outil de configuration poste ». [En ligne]. Disponible sur: [https://gitlab.com/pfe25-t-507/rapport/-/raw/main/data/ias/questionnaire-ias-solution-configuration-poste.ods?ref\\_type=heads&inline=false](https://gitlab.com/pfe25-t-507/rapport/-/raw/main/data/ias/questionnaire-ias-solution-configuration-poste.ods?ref_type=heads&inline=false)
- [74] Wikipédia, « Preboot Execution Environment », [En ligne]. Disponible sur: [https://en.wikipedia.org/wiki/Preboot\\_Execution\\_Environment](https://en.wikipedia.org/wiki/Preboot_Execution_Environment)
- [75] LibreOffice, « Libreoffice Migration Protocol ». [En ligne]. Disponible sur: <https://www.documentfoundation.org/media/tdf-migrationprotocol-v2.pdf>
- [76] Microsoft, « Learn about Microsoft Purview ». [En ligne]. Disponible sur: <https://learn.microsoft.com/en-us/purview/purview>
- [77] Andrew et Windows Management Experts, « Automating Sensitivity Label and Encryption Removal in SharePoint Online with PowerShell ». [En ligne]. Disponible sur: <https://windowsmanagementexperts.com/encryption-removal-in-sharepoint-powershell/>
- [78] Microsoft, « How to remove a sensitivity label and encryption app ». [En ligne]. Disponible sur: <https://learn.microsoft.com/en-us/answers/questions/5623877/how-to-remove-sensitivity-label-and-encryption-app>
- [79] Reddit, « How to remove a sensitivity label applied to files if the policy has been deleted? ». [En ligne]. Disponible sur: [https://www.reddit.com/r/Office365/comments/17rnym9/how\\_to\\_remove\\_a\\_sensitivity\\_label\\_applied\\_to/](https://www.reddit.com/r/Office365/comments/17rnym9/how_to_remove_a_sensitivity_label_applied_to/)
- [80] Nextcloud, « Automated tagging of files ». [En ligne]. Disponible sur: [https://docs.nextcloud.com/server/stable/admin\\_manual/file\\_workflows/automated\\_tagging.html](https://docs.nextcloud.com/server/stable/admin_manual/file_workflows/automated_tagging.html)
- [81] Nextcloud, « File access control ». [En ligne]. Disponible sur: [https://docs.nextcloud.com/server/stable/admin\\_manual/file\\_workflows/access\\_control.html](https://docs.nextcloud.com/server/stable/admin_manual/file_workflows/access_control.html)

- [82] Nextcloud, « From Microsoft to digital sovereignty: Practical steps for your organization », Nextcloud, 2025. [En ligne]. Disponible sur: <https://nextcloud.com/blog/recording/vavfvoq2grtghqqppergerg/>
- [83] Sendent, « Sendent homepage ». [En ligne]. Disponible sur: <https://sendent.com/>
- [84] S. Rudra, « Good News! Germany's Schleswig-Holstein Completes Massive Migration to Open Source Email Systems ». [En ligne]. Disponible sur: <https://itsfoss.com/news/schleswig-holstein-email-system-migration/>
- [85] SITPI, « AlpOSS 2026 - Déploiement de la messagerie OpenXchange au SITPI : RETEX de la migration de la ville de Claix ». [En ligne]. Disponible sur: <https://video.echiroilles.fr/w/p/7CPFbyKwNmWZBVbnMo2rmk?playlistPosition=17&resume=true>
- [86] LibreOffice, « Working with VBA Macros ». [En ligne]. Disponible sur: <https://help.libreoffice.org/latest/lo/text/sbasic/shared/vbasupport.html>
- [87] Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat, « Référentiel Général d'Interopérabilité ». [En ligne]. Disponible sur: [https://s3.eu-west-par.io.cloud.ovh.net/numerique-gouv-website/numerique-gouv-website/documents/Referentiel\\_General\\_Interoperabilite\\_V2.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=83d53d2d1ca64211b6b9581adffa67ce%2F20260220%2Feu-west-par%2Fs3%2Faws4\\_request&X-Amz-Date=20260220T153221Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=79b1d1fd607711b49a631b4fb5cf02bd6871b588888cd6da6445ac5e577bfa5d](https://s3.eu-west-par.io.cloud.ovh.net/numerique-gouv-website/numerique-gouv-website/documents/Referentiel_General_Interoperabilite_V2.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=83d53d2d1ca64211b6b9581adffa67ce%2F20260220%2Feu-west-par%2Fs3%2Faws4_request&X-Amz-Date=20260220T153221Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=79b1d1fd607711b49a631b4fb5cf02bd6871b588888cd6da6445ac5e577bfa5d)

## Liste des figures

---

Fig. 1	Schéma de la stratégie de déploiement d'un poste bureautique souverain .....	9
Fig. 2	Schéma d'architecture global du poste de travail Windows .....	27
Fig. 3	Feuille de route de la conduite du changement .....	42
Fig. 4	Comparatif des systèmes d'exploitation pour les postes utilisateur-rices .....	49
Fig. 5	Comparatif des environnements de bureau .....	54
Fig. 6	Comparatif des solutions de provisioning .....	58
Fig. 7	Comparatif des solutions de configuration des postes .....	63
Fig. 8	Comparatif des suites bureautiques .....	69
Fig. 9	Comparatif des solutions de collaboration .....	73
Fig. 10	Comparatif des systèmes de stockage et partage .....	77
Fig. 11	Comparatif des solutions EDR .....	80

## Liste des tableaux

---

Tableau 1	Comparaison des modèles de distribution logicielle .....	15
Tableau 2	Matrice de confidentialité pour échanger des données .....	81