

SELINE

Sovereign - Ethical - Local Intelligence, Natively Encrypted

W H I T E P A P E R

Intelligence artificielle souveraine, chiffrée et conforme

A propos de ce document

Ce livre blanc présente l'architecture, les fondements éthiques, le cadre de conformité réglementaire et la proposition de valeur stratégique de SELINE - solution d'intelligence artificielle souveraine conçue pour les organisations européennes qui opèrent dans des environnements sensibles, critiques ou régulés.

SELINE s'adresse aux RSSI, DPO, DSI, juristes et décideurs d'organisations qui ne peuvent pas se permettre de déléguer leur souveraineté numérique à des tiers hors de leur contrôle.

Version	1.1 - Février 2026
Classification	Public
Auteur	Equipe SELINE - EVI SAS
Contact	contact@evi.biz
Site web	www.evi.biz

Sommaire

1. Résumé exécutif	3
2. Le contexte : pourquoi la souveraineté est devenue urgente	4
3. Présentation de SELINE	5
4. Architecture technique	6
5. Sécurité et chiffrement	7
6. Conformité réglementaire	9
7. Souveraineté numérique : les six piliers	11
8. Comparatif concurrentiel	12
9. Cas d'usage et secteurs cibles	13
10. Feuille de route	14
11. Conclusion	15

1. Résumé exécutif

Dans un contexte où l'adoption de l'intelligence artificielle s'accélère dans tous les secteurs économiques et institutionnels, une question fondamentale émerge : à qui appartiennent vos données lorsque vous utilisez une IA ? Pour une grande partie des solutions disponibles sur le marché - ChatGPT, Copilot, Gemini - la réponse dépend de l'offre choisie, mais un point demeure central : vos données sont traitées via des infrastructures cloud opérées par des acteurs soumis à des cadres juridiques extra-européens (ex. Cloud Act), ce qui peut réduire votre maîtrise de la localisation, des accès et des garanties contractuelles.

SELINE apporte une réponse radicale à cette problématique : une intelligence artificielle conçue dès sa fondation pour être déployée sur votre infrastructure, avec zéro transfert de données hors de votre périmètre, une conformité native au RGPD, des mécanismes de préparation à l'EU AI Act, et une architecture de chiffrement conçue pour des environnements sensibles.

La proposition SELINE en quatre points

1. Souveraineté totale : vos données ne quittent jamais votre datacenter ou cloud souverain.
2. Conformité réglementaire intégrée : RGPD, NIS2, exigences ANSSI - mécanismes de préparation à l'EU AI Act dès la conception.
3. Chiffrement systématique : AES-256-GCM au repos, TLS 1.3 en transit, HSM pour la gestion des clés.
4. Indépendance technologique : aucun lock-in fournisseur, modèles à poids ouverts (open-weight) ou sous licences auditable, pas de Cloud Act.

Ce livre blanc détaille l'architecture technique, le cadre de conformité et la proposition de valeur stratégique de SELINE pour les organisations qui opèrent dans des environnements sensibles, régulés ou critiques.

2. Le contexte : pourquoi la souveraineté est devenue urgente

2.1 L'expansion incontrôlée des IA cloud

En 2024 et 2025, l'adoption massive des IA conversationnelles dans les entreprises et administrations européennes a révélé une faille structurelle : la quasi-totalité des solutions disponibles reposent sur une infrastructure appartenant à des entreprises américaines - Microsoft, Google, OpenAI/Microsoft, Amazon - soumises à la juridiction extraterritoriale des Etats-Unis.

Le Cloud Act (Clarifying Lawful Overseas Use of Data Act), adopté en 2018, permet aux autorités américaines d'ordonner à tout fournisseur de cloud américain de livrer des données stockées n'importe où dans le monde - y compris en Europe - sans en informer le propriétaire des données ni passer par les voies judiciaires bilatérales habituelles.

Constat

Dans la pratique, une part majeure des déploiements d'IA générative en Europe s'appuie sur des infrastructures cloud opérées par des acteurs extra-européens. Les estimations varient selon le périmètre étudié et la méthodologie ; l'enjeu principal reste la maîtrise de la localisation des données, des accès et des obligations légales applicables.

2.2 La montée des obligations réglementaires

L'Union Européenne a réagi à cette problématique avec une accélération législative sans précédent :

- Le RGPD (2018) impose des règles strictes sur le traitement des données personnelles, dont l'interdiction de principe de transfert hors UE sans garanties adéquates.
- L'EU AI Act (2024, applicable progressivement jusqu'à 2027) crée le premier cadre légal mondial réglementant les systèmes d'intelligence artificielle, avec des obligations de transparence, de traçabilité et de gestion des risques.
- La directive NIS2 (2022) renforce considérablement les obligations de cybersécurité pour les entités essentielles et importantes, y compris celles qui utilisent des systèmes IA.
- La qualification SecNumCloud de l'ANSSI définit les exigences pour les services cloud utilisables par les administrations et OIV français.

Face à ces évolutions, les organisations ne peuvent plus se permettre d'ignorer la question de la souveraineté de leurs outils IA. Les amendes potentielles sont substantielles : jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires mondial pour les violations les plus graves de l'EU AI Act.

2.3 Le vide du marché

Malgré l'urgence de la situation, l'offre en IA souveraine reste fragmentée et souvent inadaptée aux besoins opérationnels des grandes organisations. Les solutions disponibles souffrent de compromis inacceptables : performance insuffisante, manque de conformité certifiée, dépendance à des éditeurs étrangers, ou absence de support pour les environnements air-gap.

SELINE comble ce vide en proposant une solution industrielle complète, auditable et conforme, conçue pour les exigences les plus élevées.

3. Présentation de SELINE

3.1 Qu'est-ce que SELINE ?

SELINE - Sovereign, Ethical, Local Intelligence, Natively Encrypted - est une plateforme d'intelligence artificielle de nouvelle génération conçue pour les organisations européennes qui placent la souveraineté numérique au cœur de leur stratégie. SELINE n'est pas un simple modèle de langage : c'est une infrastructure complète d'IA, déployable dans votre datacenter ou sur un cloud souverain qualifié, qui intègre nativement les mécanismes de sécurité, de conformité et de gouvernance.

3.2 Les valeurs fondatrices

Souveraineté (S)

Vos données, vos modèles, votre infrastructure. SELINE n'a aucun accès à votre environnement depuis l'extérieur. Les mises à jour sont sous votre contrôle exclusif.

Ethique (E)

L'IA de SELINE est conçue pour être explicable, équitable et auditable. Nous appliquons les principes de l'OCDE sur l'IA éthique et les recommandations de l'Union Européenne.

Localité (L)

Traitement local, inférence locale, stockage local. Zéro communication avec des services tiers non autorisés. Compatible mode air-gap pour les environnements totalement isolés.

Chiffrement natif (NE)

AES-256-GCM, TLS 1.3, HSM, chiffrement homomorphique en option. La sécurité n'est pas une couche ajoutée - elle est intégrée à chaque couche de l'architecture.

3.3 Les marchés ciblés

SELINE s'adresse prioritairement aux secteurs où la souveraineté et la sécurité des données ne sont pas négociables :

- Défense et renseignement - traitement de données classifiées, analyses opérationnelles, aide à la décision en environnement contraint ;
- Santé - dossiers patients, imagerie médicale, recherche clinique, télémédecine sécurisée ;
- Finance - analyse de risque, lutte contre le blanchiment, données clients sensibles, secret bancaire ;
- Administration publique - services régaliens, collectivités, ministères, opérateurs d'importance vitale ;
- Industrie critique - Energie, eau, télécommunications, transport, industrie de défense ;
- Cabinets juridiques et d'audit - secret professionnel, confidentialité des mandats.

4. Architecture technique

4.1 Vue d'ensemble

L'architecture de SELINE est conçue autour du principe de défense en profondeur (Défense in Depth) : chaque couche du système applique des mécanismes de sécurité indépendants, de sorte que la compromission d'une couche n'entraîne pas la compromission de l'ensemble.

Couche 1 - Interface	API REST / GraphQL, authentification OAuth2 / SAML / SSO, rate limiting, WAF intégré
Couche 2 - Orchestration	LLM Gateway, routage des requêtes, gestion du contexte, isolation des sessions
Couche 3 - Inférence	Moteur de modèles (GPU on-premise), sandboxing par session, zéro mémoire inter-utilisateurs
Couche 4 - RAG & Données	Vectorisation locale, base de données vectorielle chiffrée, corpus métier privés
Couche 5 - Stockage	AES-256-GCM, HSM pour clés, journaux immuables cryptographiquement signés
Couche 6 - Réseau	TLS 1.3, micro-segmentation, zero-trust networking, mode air-gap disponible

4.2 Modèles supportés

SELINE supporte nativement plusieurs familles de modèles à poids ouverts (open-weight) ou sous licences auditées, en privilégiant des modèles européens ou dont la gouvernance et la chaîne d'approvisionnement sont documentées :

- Mistral AI (Mistral 7B, Mistral Large, Mixtral) - modèles français, architecture ouverte ;
- Meta LLaMA 3 et versions ultérieures - modèles ouverts et auditables ;
- Falcon (UAE / TII) - modèle à poids ouverts haute performance ;
- Modèles spécialisés métier (légal, médical, financier) - fine-tuning sur vos données locales.

4.3 Options de déploiement

- On-premise complet - datacenter propre, GPU dédié, isolation maximale ;
- Cloud souverain - OVHcloud, Outscale (Dassault), Scaleway - hébergement SecNumCloud ;
- Hybride - traitement local, archivage souverain, réplication chiffrée ;
- Air-gap - déploiement totalement hors réseau pour les environnements DR/SDI.

5. Sécurité et chiffrement

5.1 Principes fondamentaux

La sécurité de SELINE repose sur trois principes fondamentaux : le chiffrement ubiquitaire (toutes les données sont chiffrées en permanence, au repos comme en transit), l'isolation stricte (chaque session d'inférence est cloisonnée et ne peut accéder aux données d'une autre session), et la traçabilité totale (chaque action est journalisée de manière immuable et audité). Le modèle de menace pris en compte inclut notamment l'exfiltration de données, la compromission d'identités, les attaques de chaîne d'approvisionnement et les attaques spécifiques aux LLM (prompt injection).

5.2 Architecture de chiffrement

AES-256-GCM - chiffrement au repos

Toutes les données stockées par SELINE - corpus documentaires, historiques de sessions, journaux de requêtes, configurations - sont chiffrées avec l'algorithme AES-256-GCM (Galois/Counter Mode), qui assure à la fois la confidentialité et l'intégrité des données. Il s'agit d'un standard cryptographique largement reconnu et aligné avec les bonnes pratiques de sécurité (chiffrement + authentification).

Gestion des clés - HSM (Hardware Security Module)

Les clés cryptographiques ne sont jamais stockées en clair sur le système de fichiers. Elles sont protégées par un HSM certifié FIPS 140-2 Level 3 ou CC EAL4+, physiquement présent dans votre datacenter. La rotation des clés est automatisée selon une politique configurable, et le mécanisme de récupération (key escrow) est entièrement sous votre contrôle.

TLS 1.3 avec Perfect Forward Secrecy

Toutes les communications - entre les composants SELINE, entre les clients et l'API, et entre les microservices internes - utilisent TLS 1.3 avec Perfect Forward Secrecy (PFS). Cela garantit que même si une clé privée est compromise ultérieurement, les communications passées ne peuvent pas être déchiffrées.

Isolation des sessions d'inférence

Chaque session d'inférence s'exécute dans un contexte mémoire isolé (sandboxing). Les données d'un utilisateur A ne peuvent jamais fuir vers la session d'un utilisateur B - même en cas d'attaque de type prompt injection ou de comportement anormal du modèle. Ce cloisonnement est appliqué au niveau du kernel Linux via des namespaces et des cgroups.

Chiffrement homomorphique (option avancée)

Pour les cas d'usage nécessitant un niveau de confidentialité extrême, SELINE propose un mode d'inférence sur données chiffrées par chiffrement homomorphique partiel (PHE). Le modèle d'IA effectue certains calculs sans accéder aux données en clair. Cette option s'applique à un périmètre fonctionnel restreint et implique un surcoût de calcul ; elle est généralement réservée à des traitements ciblés ou à des POC soumis à des contraintes réglementaires ou contractuelles fortes.

5.3 Journalisation immuable

Chaque évènement du cycle de vie de SELINE est enregistré dans un journal cryptographiquement signé et infalsifiable : requêtes utilisateurs (hachées), décisions d'inférence, accès aux ressources, erreurs système, modifications de configuration, et tentatives d'accès non autorisées.

Ces journaux sont conformes aux exigences de l'ANSSI (PSSIE) et peuvent être exportés vers votre SIEM (Splunk, ElasticSearch, QRadar) pour l'analyse de sécurité. Un rapport automatique hebdomadaire est généré pour votre DPO et votre RSSI.

5.4 Protection contre les attaques spécifiques aux LLM

SELINE implémente l'intégralité des recommandations de l'OWASP LLM Top 10, incluant la protection contre les vecteurs d'attaque spécifiques aux modèles de langage :

- Prompt injection - filtrage et validation multicouche des entrées, détection comportementale ;
- Data leakage - prévention de l'exfiltration de données d'entraînement par des requêtes adversariales ;
- Insecure output handling - sanitisation systématique des sorties, protection contre les injections dans les workflows downstream ;
- Supply chain attacks - vérification cryptographique des poids de modèles, SBOM (Software Bill of Materials) certifiée ;
- Model denial of service - rate limiting avance, détection d'anomalies, circuit breakers.

6. Conformité réglementaire

6.1 Le tableau de conformité SELINE

SELINE a été architecturée avec une approche « compliance by design » : chaque exigence réglementaire identifiée a été traduite en contrôle technique ou organisationnel natif du produit, et non en post-traitement ou en documentation annexe.

Référentiel	Statut	Couverture SELINE
RGPD (2016/679)	En vigueur	Privacy by design, minimisation, droit à l'effacement, registre des traitements automatisé
EU AI Act (2024/1689)	Applicable progressivement 2025-2027	Risque maîtrise, traçabilité, XAI, supervision humaine, marquage CE IA
NIS2 (2022/2555)	Obligatoire OES/OIV	Segmentation réseau, gestion vulnérabilités, notification ANSSI sous 72h
ANSSI SecNumCloud	Recommandé	Compatible hébergement qualifié, politique de sécurité documentée
ISO 27001	En préparation	SMSI complet, contrôles Annexe A, audits internes planifiés
ISO 42001 (IA)	Alignement natif	Management des systèmes d'IA, éthique, biais, équité algorithmique
SOC 2 Type II	En préparation	Disponibilité, confidentialité, intégrité des traitements
OWASP LLM Top 10	Implémenté	Protection prompt injection, data leakage, insecure output, supply chain

6.2 RGPD - conformité approfondie

Le RGPD constitue le socle juridique sur lequel repose toute l'architecture de SELINE. Les six principes du RGPD (licéité, limitation des finalités, minimisation, exactitude, limitation de conservation, intégrité et confidentialité) sont implémentés techniquement :

- Privacy by Design & by Default : aucune donnée personnelle n'est collectée au-delà du strict nécessaire. Les options de confidentialité les plus restrictives sont activées par défaut ;
- Droit à l'effacement : mécanisme d'effacement sécurisé (aligné sur NIST SP 800-88 Rev.2 : Clear/Purge/Destroy, incluant crypto-erase lorsque applicable) déclenché automatiquement à la demande, avec certificat d'effacement ;
- Portabilité : export des données personnelles en formats standards ouverts (JSON, CSV) sur demande de l'utilisateur ou du DPO ;
- Registre des traitements : généré automatiquement en temps réel, prêt pour présentation à la CNIL ou à toute autorité de contrôle ;
- Notification de violation : système d'alerte automatique vers le DPO en cas de détection d'incident, avec rapport préformaté pour notification à la CNIL dans le délai légal de 72h.

6.3 EU AI Act - positionnement de SELINE

L'EU AI Act classe les systèmes d'IA selon leur niveau de risque. SELINE, utilisée comme outil d'assistance dans des secteurs professionnels, relève selon les cas d'usage de la catégorie « haut risque » ou « risque limité ». Dans tous les cas, SELINE offre les mécanismes requis pour la conformité :

- Système de gestion des risques : intégré nativement, avec évaluation continue et alertes configurables ;
- Qualité des données : traçabilité des jeux de données d'entraînement, documentation des biais potentiels ;
- Transparence et explicabilité (XAI) : chaque réponse peut être accompagnée d'une explication de son origine et des sources mobilisées ;
- Supervision humaine (Human-in-the-Loop) : mécanismes natifs de validation humaine avant exécution d'actions critiques ;
- Robustesse et précision : tests de régression automatisés, métriques de performance documentées ;
- Documentation technique : package de conformité prêt pour soumission à l'autorité nationale de surveillance.

7. Souveraineté numérique : les six piliers

La souveraineté numérique n'est pas un argument commercial - c'est une posture stratégique qui engage la sécurité nationale, la compétitivité économique et la liberté démocratique. SELINE la structure autour de six piliers opérationnels :

Pilier 1 - Hébergement souverain

SELINE s'exécute exclusivement sur votre infrastructure propre ou chez des hébergeurs certifiés SecNumCloud (Outscale/Dassault, OVHcloud HDS, Scaleway). La localisation des données est garantie contractuellement et techniquement. Aucune donnée ne quitte le territoire de l'UE sans votre accord explicite et documenté.

Pilier 2 - Contrôle des modèles

Les poids des modèles d'IA sont physiquement déposés dans votre environnement et signés cryptographiquement. Vous décidez des mises à jour. Aucune modification à distance n'est possible. La chaîne d'approvisionnement des modèles est documentée (Model Bill of Materials).

Pilier 3 - Indépendance des GAFAM

L'architecture de SELINE n'utilise aucun service cloud américain (AWS, Azure, GCP, OpenAI API). Le Cloud Act américain ne s'applique donc pas à l'infrastructure SELINE. Les modèles utilisés sont européens ou à poids ouverts / sous licences auditées, sans dépendance contractuelle envers les grands acteurs technologiques américains.

Pilier 4 - Gouvernance des données

Vous définissez qui peut utiliser l'IA, sur quelles données, avec quel niveau d'accès. La politique de rétention, le droit à l'oubli, le cloisonnement par classification de données (Public, Interne, Confidentiel, Secret) sont tous configurables et appliqués techniquement.

Pilier 5 - Résilience opérationnelle

Le mode air-gap de SELINE permet un fonctionnement complet sans connexion Internet. Indispensable pour les environnements Diffusion Restreinte (DR), les systèmes d'information sensibles (SIS) ou les infrastructures critiques isolées. SELINE intègre également des mécanismes de haute disponibilité (HA) et de reprise après sinistre (PRA).

Pilier 6 - Transparence algorithmique

Le code source et les composants de SELINE peuvent être audités (sous NDA ou par un tiers de confiance). L'architecture des modèles est documentée. La chaîne d'approvisionnement logicielle est tracée via une SBOM (Software Bill of Materials). Vous savez exactement ce que fait votre IA, pourquoi elle produit tel ou tel résultat, et quels composants tiers sont intégrés.

8. Comparatif concurrentiel

Le tableau ci-dessous compare SELINE aux principales solutions IA d'entreprise disponibles sur le marché européen, selon les critères de souveraineté, de sécurité et de conformité réglementaire :

Critère	SELINE	ChatGPT Ent.	Copilot M365
Déploiement 100% on-premise	Natif	Cloud (SaaS)	Cloud (SaaS)
Données jamais hors UE	Garanti	Selon région/tenant - non garanti	Selon région/tenant - non garanti
Non-entraînement sur vos données	Oui (par design)	Oui par défaut (selon politique éditeur)	Oui par défaut (selon documentation Microsoft)
Cloud Act américain inapplicable	Oui	Applicable	Applicable
Chiffrement AES-256 + HSM	Natif	Partiel	Partiel
Mode air-gap / réseau isolé	Disponible	Non	Non
EU AI Act conforme	Préparation (mécanismes)	Dépend des usages	Dépend des usages
Code source auditable	Audit possible	Fermé	Fermé
Indépendance modèles à poids ouverts	Oui	Non	Non
Journaux immuables / ANSSI	Natif	Limité	Limité

Note méthodologique

Les informations relatives aux solutions concurrentes sont basées sur leurs documentations publiques, politiques de confidentialité et conditions générales d'utilisation disponibles à la date de publication de ce document (février 2026). Ces informations et statuts peuvent évoluer. Les lignes relatives au non-entraînement reflètent les politiques publiques des offres business/entreprise ; elles ne constituent pas une garantie contractuelle de SELINE pour des offres tierces.

9. Cas d'usage et secteurs cibles

9.1 Secteur public et administration

Les ministères, collectivités territoriales et opérateurs de services publics font face à une triple contrainte : exigences de la CADA sur la transparence, obligations NIS2 sur la cybersécurité, et réglementation sur les données à caractère personnel. SELINE permet de déployer des assistants intelligents pour la gestion documentaire, la rédaction administrative, l'analyse juridique ou le support aux agents - avec la garantie que les délibérations sensibles, les données citoyennes et les informations à diffusion restreinte ne quittent jamais l'infrastructure de l'Etat.

9.2 Défense et renseignement

Pour les environnements de niveau DR et au-dessus, SELINE propose une déclinaison spécifique en mode air-gap, homologable selon les référentiels de l'ANSSI. Aucune connexion externe, aucune télémétrie, aucun canal de mise à jour automatique - seul l'administrateur système accrédité peut interagir avec l'infrastructure. Les cas d'usage incluent l'analyse de documents opérationnels, la veille sur sources ouvertes (OSINT) traitée en local, et l'aide à la rédaction de rapports classifiés.

9.3 Santé et sciences de la vie

Les données de santé constituent la catégorie de données personnelles la plus sensible aux yeux du RGPD (article 9). SELINE permet aux établissements de santé, aux laboratoires pharmaceutiques et aux organismes de recherche de déployer des IA pour l'analyse de dossiers patients, le codage médical, l'aide au diagnostic ou la recherche clinique - sans jamais exposer les données patients à des serveurs tiers, tout en garantissant la conformité HDS (Hébergeur de Données de Santé).

9.4 Services financiers

Les établissements financiers opèrent sous la supervision de l'ACPR et sont soumis au secret bancaire, au RGPD, et à la directive DORA sur la résilience opérationnelle numérique. SELINE permet le déploiement d'IA pour la détection de fraudes, l'analyse KYC/AML, la revue de contrats, ou les recommandations de gestion d'actifs - avec une traçabilité totale exigible par les régulateurs.

9.5 Industrie et infrastructures critiques

Les opérateurs d'importance vitale (OIV) et les entreprises industrielles gérant des informations techniques sensibles (plans, brevets, procédés) peuvent déployer SELINE pour l'assistance à la maintenance, la documentation technique, ou l'analyse de données de production - sans risque d'exposition de leurs propriétés intellectuelles ou de leurs systèmes de contrôle industriel (OT/ICS).

10. Feuille de route

2026 - Disponibilité générale

- Version 1.0 - déploiement on-premise avec modèles Mistral et LLaMA 3
- Certification ISO 27001 et engagement SOC 2 Type II
- Module RAG (Retrieval-Augmented Generation) local haute performance
- Interface web et API REST documentée (OpenAPI 3.0)
- Connecteurs natifs : SharePoint, Confluence, S3-compatible, PostgreSQL

2026 T3 - Fonctionnalités avancées

- Fine-tuning supervise sur corpus client - modèles métier personnalisés
- Module d'analyse multimodale (texte + images + documents PDF/Office)
- Dashboard de conformité temps réel pour DPO et RSSI
- Support des environnements air-gap avec mise à jour par médias amovibles chiffrés

2027 - Ecosystème et certifications

- Certification EU AI Act - marquage CE pour systèmes à haut risque
- Qualification SecNumCloud (en coopération avec hébergeurs qualifiés)
- Module de chiffrement homomorphe - option avancée (périmètre ciblé)
- Marketplace de modèles sectoriels certifiés (santé, droit, finance, défense)
- API multi-agents pour orchestration de tâches complexes

11. Conclusion

Nous sommes à un tournant. Les organisations européennes qui adoptent aujourd'hui des solutions IA sans considérer la question de la souveraineté construisent une dépendance structurelle dont les conséquences - juridiques, stratégiques, économiques - se feront sentir pendant des années.

L'enjeu n'est pas uniquement technique. Il est politique, économique et philosophique : à qui faisons-nous confiance pour traiter nos informations les plus sensibles ? Qui contrôle les infrastructures de décision que nous déployons au cœur de nos organisations ?

Le choix de SELINE, c'est le choix de reprendre le contrôle

SELINE n'est pas une alternative au cloud : c'est une alternative à la dépendance. Une IA qui reste chez vous, qui travaille pour vous, qui n'appartient qu'à vous. Dans un monde où les données sont le nouvel actif stratégique, la souveraineté n'est plus une option - c'est une nécessité.

EVI SAS met à disposition son équipe d'experts pour accompagner votre organisation dans l'évaluation de vos besoins, la démonstration technique et le déploiement de SELINE dans votre environnement.

Demander une démonstration

contact@evi.biz
www.evi.biz

Documentation technique

Accès développeur disponible
Environnement de test sandbox

© 2026 EVI SAS - Tous droits réservés. Ce document est fourni à titre d'information uniquement. Les caractéristiques du produit sont susceptibles d'évoluer. SELINE est une marque d'EVI SAS.