



LA VOIE SÛRE VERS UN USAGE DE L'IA À GRANDE ÉCHELLE

Comment les entreprises peuvent tirer parti de l'IA moderne sans compromettre la souveraineté des données ni la conformité.






Autonomie totale sur les données pour un avenir numérique sûr

Autonomie totale sur les données pour un avenir numérique sûr Dans un monde multi-cloud et SaaS, les données sensibles circulent bien au-delà du périmètre de l'entreprise. Alors que les cyberattaques, les ransomwares et les menaces internes se multiplient, la simple défense périmétrique ne suffit plus. Les entreprises doivent s'assurer que toute donnée compromise demeure inexploitée et sans valeur pour les attaquants.

Les données constituent aujourd'hui l'actif le plus précieux des entreprises. Grâce à Centraya AI, elles gardent une autonomie complète sur leurs informations : possession des clés, choix du lieu d'hébergement et contrôle direct du chiffrement. Ce modèle garantit la conformité, supprime les dépendances technologiques et rend toute donnée dérobée inexploitée – un socle de confiance et de résilience pour une transformation numérique sûre et durable.

 swiss made software

e3 en bref

Data Ownership. Digital Confidence. Lasting Security.

Chez e3, nous sommes convaincus que les organisations doivent garder en tout temps une autonomie totale sur leurs données – qu'elles soient stockées, traitées ou partagées via des services cloud ou d'intelligence artificielle. C'est à cette condition que la transformation numérique peut révéler tout son potentiel.

Depuis plus de 25 ans, nous accompagnons les entreprises dans la protection des données, le respect de la conformité et la gestion proactive des cyberrisques. Partenaire de confiance de secteurs variés – santé, assurances, services financiers et industrie – nous contribuons à renforcer leur résilience numérique.

Grâce à une expertise approfondie en cybersécurité et en conformité, nous aidons nos clients à réduire les risques tout en construisant une base digitale solide et durable pour l'avenir.



Les risques d'entreprise, moteur du chiffrement

Avec le développement du cloud, du SaaS et de l'intelligence artificielle, les données sensibles franchissent les limites classiques de la sécurité. Pour répondre à cette évolution, le principe du Zero Trust doit s'appliquer jusqu'à la donnée elle-même : seul un chiffrement constant et une gestion stricte des accès assurent une conformité et une confiance durables.



Exigences légales

Afin de répondre aux exigences du RGPD et aux réglementations propres à leur secteur, les organisations doivent assurer une gestion rigoureuse de leurs données sensibles, même dans des environnements hybrides et multi-cloud.



Protection des données & confidentialité

Protéger les informations personnelles et sensibles est indispensable pour maintenir la confiance et assurer la protection des données tout au long des processus digitaux.



Cyberrésilience

Les attaques d'aujourd'hui déjouent les défenses traditionnelles. En rendant les données dérobées inutilisables grâce au chiffrement, Centraya AI remet en cause le modèle économique du ransomware et place la maîtrise des données au cœur de la cyberrésilience moderne.



Intelligence artificielle

Maîtriser de façon fiable la qualité et la confidentialité des modèles d'IA devient un enjeu central. Mais les entreprises qui renoncent à utiliser l'IA prennent du retard. Centraya AI permet un usage sécurisé de l'IA, où création de valeur et confidentialité restent garanties à parts égales.

Chez e3, nous sommes convaincus que la conformité et le Zero Trust commencent au niveau des données. Avec Centraya AI, les organisations étendent leur autonomie dans l'ère du cloud et de l'intelligence artificielle – tout en garantissant le respect des réglementations, la maîtrise des risques et la protection de l'innovation.





Autonomie des données = stratégie de sécurité + technologie

Centraya AI offre aux organisations la liberté d'utiliser le cloud, le SaaS et l'intelligence artificielle sans compromettre la sécurité. Grâce à la combinaison d'une approche stratégique, du chiffrement et de la tokenisation, la solution assure la conformité, préserve l'indépendance technologique et protège les données partout.



Stratégie de sécurité

- » **Gouvernance des données:** Fixe les règles de propriété des clés, de localisation du stockage et de gestion du chiffrement.
- » **Conformité :** Garantit que la protection des données répond aux exigences réglementaires et aux normes propres à chaque secteur.
- » **Politiques et processus:** Établissent un cadre clair pour la manipulation, le chiffrement et le contrôle d'accès aux informations sensibles.
- » **Atténuation des risques :** Garantit que les données dérobées restent inutilisables.



Technologie

- » **Chiffrement & tokenisation:** Protègent les données sur toutes les plateformes et auprès de tous les fournisseurs.
- » **Gestion des clés :** La possession de vos propres clés assure une maîtrise complète et prévient toute dépendance envers les fournisseurs.
- » **Intégration cloud & SaaS:** Permet une utilisation sûre et fluide du cloud, des environnements hybrides, multi-cloud et de l'intelligence artificielle.

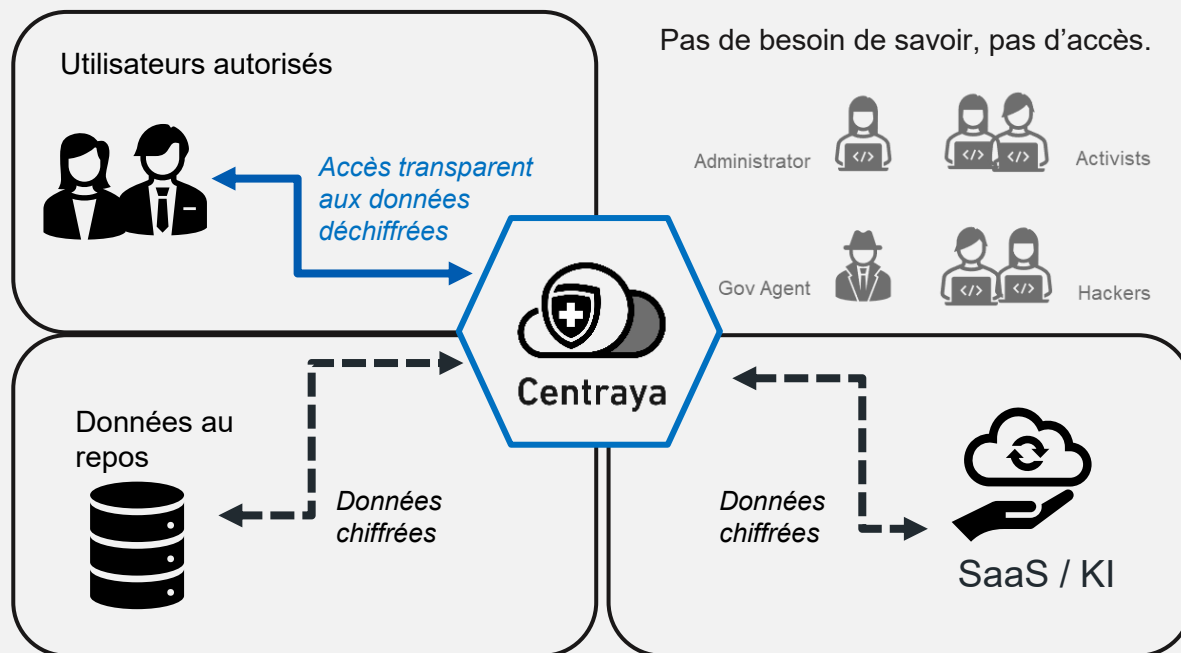
Centraya AI : faire de la sécurité un levier de croissance

Centraya AI remet la protection des données entre les mains de l'organisation. Grâce à une autonomie complète sur les clés, le lieu de stockage et le chiffrement, la sécurité cesse d'être une contrainte pour devenir un accélérateur de croissance. Centraya AI lève ainsi les freins à l'innovation et permet d'exploiter tout le potentiel du cloud, du SaaS et de l'intelligence artificielle.



Le gardien fiable de vos données

Centraya AI joue le rôle d'une couche de sécurité transparente entre votre organisation, vos dépôts de données et les services cloud ou SaaS externes. Il veille à ce que les informations sensibles ne sortent de votre environnement que sous forme chiffrée, et que seules les personnes disposant des droits nécessaires puissent les consulter.



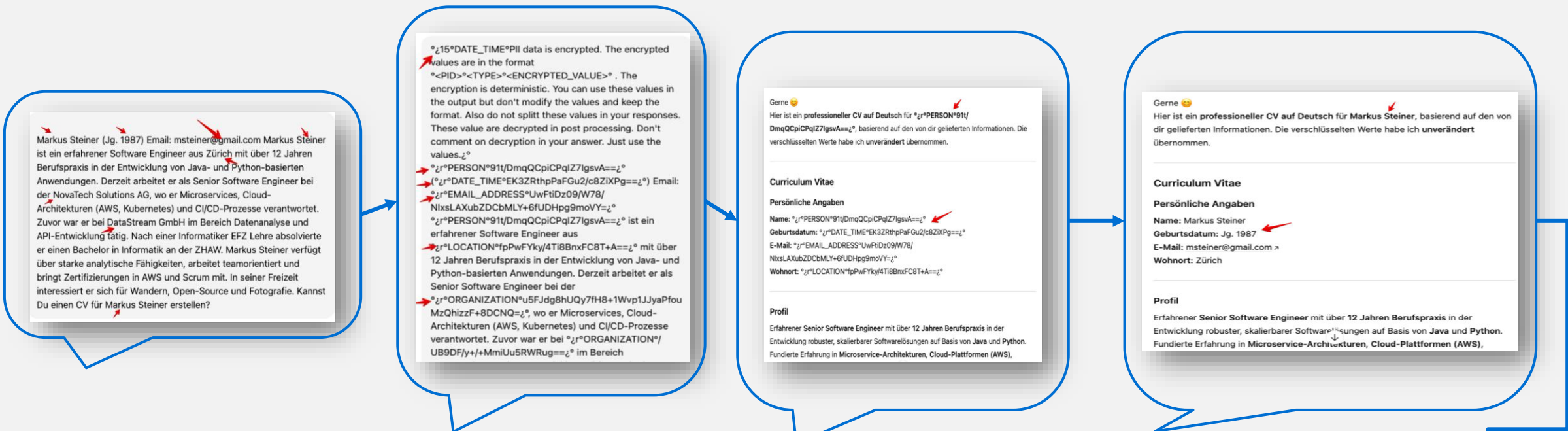
En protégeant les données sensibles par chiffrement, Centraya AI assure que la conformité et la responsabilité sur les données sont maintenues à tout moment. Mais le chiffrement n'est qu'un début : Centraya AI transforme le cloud en un espace de confiance pour l'innovation et donne aux organisations la liberté d'exploiter pleinement les solutions SaaS, d'intelligence artificielle ou internes.



Utiliser l'IA de manière sûre et en toute confiance



Centraya AI analyse les prompts (entrées), identifie les informations sensibles – notamment les données personnellement identifiables (PII) – et les chiffre. L'IA est alors informée que le texte contient des éléments chiffrés ainsi que du type d'information auquel ils correspondent, par exemple une personne. Elle peut ainsi comprendre le contexte et accomplir sa tâche sans identifier la personne.



Personne utilisatrice
(1)
Saisie



Centraya AI
(2)
Chiffrement



IA
(3)
Traitement et sortie



Centraya AI
(4)
Déchiffrement



Personne utilisatrice
(5)
Résultat

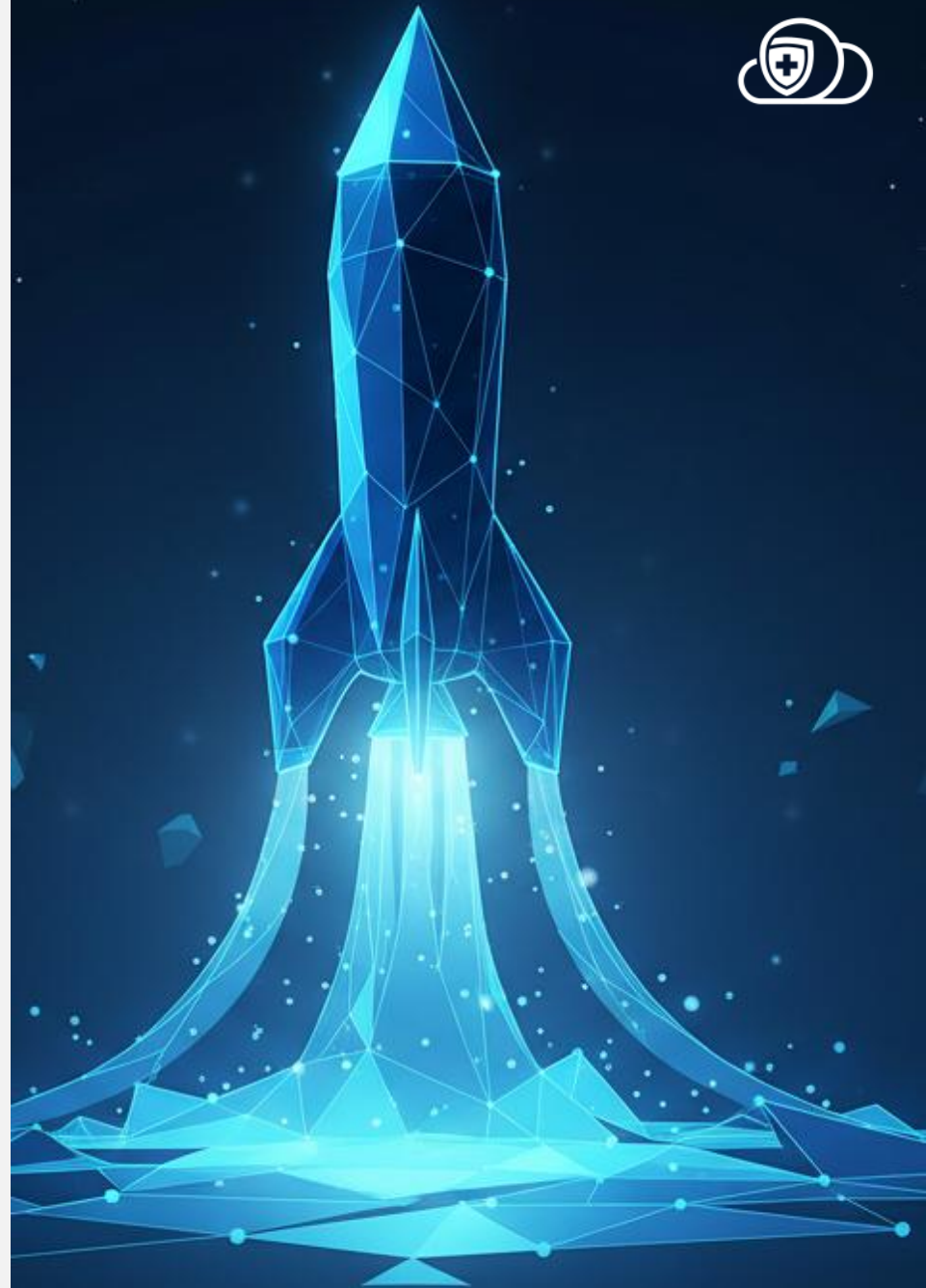


FAITES-VOUS VOTRE PROPRE OPINION

Trop beau pour être vrai ? C'est le moment idéal pour en parler.

Avec Centraya AI, ces possibilités deviennent concrètes.

À découvrir dès maintenant sur
e3ag.ch/fr/centraya-ai





Construisons ensemble votre avenir numérique en toute sécurité !

Depuis 25 ans, e3 aide les organisations à garder le contrôle total sur leurs données. Grâce à une approche Zero Trust, à une indépendance vis-à-vis des fournisseurs et à une expertise approfondie, nous réduisons la complexité et renforçons la résilience numérique.

Nos solutions assurent une protection complète contre les cybermenaces et les pertes de données, garantissent la conformité et renforcent la préparation de votre entreprise face aux enjeux numériques de demain.

e3 AG Suisse – Zurich

Binzstrasse 24
CH-8045 Zurich

- » engage@e3ag.ch
- » +41 44 400 46 56

e3 AG Suisse – Berne

Falkenplatz 3
CH-3012 Berne

- » engage@e3ag.ch
- » +41 31 305 46 56

Présence internationale

- » Brésil
- » Allemagne
- » Pays-Bas



e3ag.ch/fr/



[LinkedIn](#)

