AYI NEDJIMI Consultants

SIEM Cloud-Native vs On-Premise : Comparatif Complet 2026

Catégorie : SOC et Detection Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Comparatif détaillé SIEM cloud-native versus on-premise en 2026 : coûts, performances, souveraineté, scalabilité et critères de choix pour votre SOC.

Résumé exécutif

Ce comparatif analyse en profondeur les avantages et inconvénients des SIEM cloud-native versus on-premise en 2026 : modèles de coûts avec TCO détaillé sur 3 ans, performances de recherche et d'ingestion, enjeux de souveraineté des données face au Cloud Act américain, scalabilité et élasticité, compétences requises pour chaque modèle, et critères de décision objectifs pour choisir l'architecture adaptée à votre SOC. Le marché est polarisé entre des solutions cloud-native comme Microsoft Sentinel et Google Chronicle, et des solutions on-premise comme Splunk Enterprise et Elastic Security auto-hébergée. Nous démontrons que l'approche hybride combinant les forces du cloud et du on-premise est souvent la stratégie optimale, et nous fournissons un framework décisionnel basé sur le volume d'ingestion, les contraintes réglementaires et les compétences disponibles.

Le choix entre un **SIEM cloud-native** et un **SIEM on-premise** est l'une des décisions architecturales les plus structurantes pour un SOC en 2026. Ce choix engage l'organisation sur plusieurs années et impacte profondément les coûts, les compétences requises, la souveraineté des données et la capacité d'évolution de la plateforme de détection. Le marché est aujourd'hui polarisé entre des solutions cloud-native comme Microsoft Sentinel et Google Chronicle qui misent sur l'élasticité du cloud et l'absence de gestion d'infrastructure, et des solutions on-premise ou hybrides comme Splunk Enterprise et Elastic Security auto-hébergée qui offrent un contrôle total sur les données et l'infrastructure. La réalité est que la majorité des organisations en 2026 adoptent une approche hybride, combinant des composants cloud et on-premise en fonction de leurs contraintes spécifiques. Ce comparatif objectif vous fournit les éléments d'analyse nécessaires pour faire un choix éclairé, en examinant chaque dimension critique avec des données chiffrées et des retours d'expérience concrets, tout en évitant les biais marketing qui favorisent systématiquement l'un ou l'autre modèle selon les intérêts de l'éditeur.

Retour d'expérience : Un groupe de distribution (15 000 utilisateurs, 85 sites) a migré d'un Splunk on-premise vers Microsoft Sentinel en 18 mois. Le coût mensuel est passé de 35 000 EUR (infrastructure + licences + 2 ETP admin) à 22 000 EUR (ingestion Sentinel + 0,5 ETP admin). Cependant, la migration a nécessité 6 mois de réécriture des règles de détection de SPL vers KQL et la perte temporaire de certaines fonctionnalités avancées non disponibles nativement dans Sentinel.

Modèles de coûts comparés

L'analyse des **coûts** est souvent le premier critère de décision et celui qui génère le plus de confusion. Le modèle on-premise repose sur des coûts d'investissement initiaux (serveurs, stockage, licences) et des coûts récurrents de maintenance (administration, mises à jour, remplacement matériel). Le modèle cloud-native repose sur des coûts opérationnels récurrents basés principalement sur le *volume d'ingestion* en Go par jour. La comparaison directe est trompeuse si elle n'inclut pas le **TCO (Total Cost of Ownership)** complet sur 3 à 5 ans. Le TCO on-premise doit inclure : les serveurs et leur amortissement, les licences logicielles, le stockage et sa croissance, l'alimentation électrique et le refroidissement, le coût des administrateurs systèmes dédiés (1 à 2 ETP pour un cluster de taille moyenne) et les coûts de mises à jour et de migration de versions. Le TCO cloud-native doit inclure : les frais d'ingestion mensuels, les frais de stockage des données (qui peuvent être significatifs pour les rétentions longues), les coûts de sortie de données (egress fees), les frais de requêtes sur les données archivées et le temps humain de gestion (réduit mais non nul).

En pratique, le **point de bascule économique** se situe généralement autour de 200 à 300 Go par jour d'ingestion. En dessous, le cloud-native est généralement plus économique car il évite les investissements d'infrastructure et réduit les besoins en administration. Au-dessus, le on-premise devient souvent plus intéressant car les coûts d'ingestion cloud croissent linéairement tandis que les coûts d'infrastructure on-premise bénéficient d'économies d'échelle. Les **commitment tiers** des solutions cloud (réductions pour engagement de volume) et les options de **Basic Logs / Archive Logs** à tarif réduit compliquent la comparaison mais peuvent rendre le cloud-native compétitif à des volumes plus élevés. Pour les organisations utilisant déjà massivement Azure ou AWS, les crédits cloud et les remises globales peuvent significativement avantager le modèle cloud-native. Consultez les recommandations de l'ANSSI pour les considérations de souveraineté qui impactent ce choix.

Critère	SIEM Cloud-Native	SIEM On-Premise	Avantage
Coût initial	Faible (pas d'infrastructure)	Élevé (serveurs, licences)	Cloud
Coût récurrent (< 200 Go/j)	Modéré et prévisible	Élevé (admin + maintenance)	Cloud
Coût récurrent (> 500 Go/j)	Élevé (ingestion linéaire)	Modéré (économies d'échelle)	On-Premise
Scalabilité	Élastique et instantanée	Planification et achat requis	Cloud
Souveraineté données	Données chez le cloud provider	Contrôle total localisation	On-Premise
Compétences requises	Focus sécurité	Sécurité + infrastructure	Cloud
Personnalisation	Limité par la plateforme	Contrôle total	On-Premise
Mises à jour	Automatiques par l'éditeur	Manuelles, planification requise	Cloud

Comment évaluer les enjeux de souveraineté ?

La **souveraineté des données** est un critère de décision de plus en plus important en 2026, notamment pour les organisations soumises à des réglementations strictes (OIV, opérateurs de services essentiels, secteur public, santé, défense). Les données de sécurité ingérées par le SIEM contiennent des informations sensibles : identifiants de connexion, adresses IP internes, topologie réseau, activité des utilisateurs, et potentiellement des données personnelles soumises au RGPD. Avec un SIEM cloud-native, ces données sont stockées dans l'infrastructure du cloud provider, généralement dans des data centers situés dans la région choisie mais sous la juridiction de l'éditeur (américain pour Microsoft, Google et Splunk Cloud). Le *Cloud Act* américain permet aux autorités US de demander l'accès aux données stockées par des entreprises américaines, même si les données sont physiquement situées en Europe. Pour les organisations sensibles, cette exposition juridique est un risque inacceptable.

Plusieurs **stratégies** permettent de concilier les avantages du cloud avec les exigences de souveraineté. L'approche **SecNumCloud** en France certifie des cloud providers qui garantissent l'immunité aux lois extraterritoriales, mais les solutions SIEM disponibles sur ces cloud qualifiés sont encore limitées en 2026. L'approche **hybride** consiste à conserver les données les plus sensibles on-premise tout en utilisant le cloud pour les données moins critiques ou pour les capacités d'analyse avancées (ML, threat intelligence cloud). L'approche **open source auto-hébergée** avec Elastic Security déployée sur une infrastructure souveraine offre le meilleur compromis entre fonctionnalités modernes et contrôle total des données, au prix d'un investissement en compétences d'administration. Pour les exigences spécifiques au secteur défense, consultez notre article sur le Zero Trust et ses implications architecturales. Pour les environnements Active Directory, notre livre blanc AD détaille les exigences de monitoring on-premise.

Pourquoi la scalabilité change-t-elle la donne ?

La **scalabilité** est l'avantage le plus significatif du modèle cloud-native et celui qui justifie souvent à lui seul le choix du cloud pour les organisations à forte croissance. Avec un SIEM cloud-native, l'augmentation du volume de données est transparente : il suffit d'augmenter le budget pour ingérer davantage de données, sans planification d'infrastructure, sans achat de serveurs et sans migration de données. Cette élasticité est particulièrement précieuse lors des pics d'activité (période de soldes pour le retail, campagnes de phishing massives, incidents de sécurité majeurs qui multiplient le volume de logs) et lors de la croissance organique (acquisitions, ouverture de nouveaux sites, déploiement de nouvelles applications). Avec un SIEM on-premise, chaque augmentation significative de volume nécessite une planification en amont (dimensionnement, commande de matériel, installation, migration), un processus qui prend typiquement 2 à 4 mois et qui peut laisser le SOC en situation de sous-capacité pendant cette période. Le risque est de manquer des détections critiques parce que le SIEM rejette des logs faute de capacité d'ingestion ou de stockage.

En contrepartie, la scalabilité cloud-native a un **coût linéaire** qui peut devenir prohibitif à très grand volume. Les organisations ingérant plus de 1 To par jour doivent évaluer soigneusement le TCO cloud versus on-premise. Les architectures **hybrides** offrent un compromis intéressant :

un SIEM cloud-native pour les sources de données cloud et les données à volume variable, couplé à un stockage on-premise ou data lake pour les données à haut volume et faible valeur temps réel (logs de flux réseau, logs web). Cette architecture combine la flexibilité du cloud avec la maîtrise des coûts de l'on-premise pour les gros volumes. Consultez notre article sur le threat hunting avec Sentinel pour voir comment les capacités analytiques cloud apportent de la valeur au-delà du simple stockage.

Quelles compétences sont nécessaires pour chaque modèle ?

Les **compétences requises** diffèrent significativement entre les deux modèles et ce facteur est souvent sous-estimé dans la décision. Le modèle on-premise exige des compétences doubles : des compétences d'**administration d'infrastructure** (systèmes Linux/Windows, virtualisation, stockage, réseau, haute disponibilité, sauvegarde) et des compétences de **sécurité opérationnelle** (écriture de règles, investigation, threat hunting). Trouver des profils combinant ces deux expertises est difficile et coûteux. Le modèle cloud-native réduit significativement les besoins en compétences infrastructure mais nécessite des *compétences cloud spécifiques* (gestion des ressources cloud, optimisation des coûts, IAM cloud) en plus des compétences de sécurité. L'avantage du cloud est que l'équipe SOC peut se concentrer sur son cœur de métier (détection et réponse) plutôt que sur la maintenance de l'infrastructure. Pour les organisations qui peinent à recruter des profils infrastructure, le cloud-native est souvent le choix pragmatique. Consultez notre comparatif DFIR pour les compétences d'investigation qui restent nécessaires quel que soit le modèle.

Mon avis : En 2026, le dogmatisme est l'ennemi du bon choix. Ni le tout-cloud ni le tout-on-premise ne conviennent à la majorité des organisations. L'approche hybride qui place les données cloud dans un SIEM cloud-native et les données sensibles on-premise dans un SIEM open source est souvent la meilleure stratégie. Si vous êtes une PME de moins de 5 000 utilisateurs sans contrainte de souveraineté, le cloud-native (Sentinel ou Splunk Cloud) est le choix rationnel. Si vous êtes un OIV ou un acteur du secteur défense, l'on-premise ou le SecNumCloud est une nécessité. Entre les deux, analysez objectivement votre TCO sur 3 ans et vos contraintes de compétences avant de décider.

Migration d'un modèle à l'autre : défis et bonnes pratiques

La **migration** d'un SIEM on-premise vers le cloud (ou inversement) est un projet complexe qui doit être soigneusement planifié. Les principaux défis incluent la **réécriture des règles de détection** (les langages de requête diffèrent entre solutions : SPL, KQL, Lucene), la **migration des données historiques** (coûteuse en bande passante et en temps d'importation pour les volumes importants), la **reconfiguration des sources de collecte** (remplacement ou reconfiguration des agents, des connecteurs et des pipelines de traitement) et la **formation des équipes** (prise en main du nouvel outil, apprentissage du nouveau langage de requête). Les bonnes pratiques recommandent une migration progressive avec une **période de fonctionnement parallèle** de 3 à 6 mois pendant laquelle les deux SIEM coexistent, permettant de valider la couverture de détection du nouveau système avant de désactiver l'ancien.

Commencez par migrer les sources les plus simples et les règles les plus critiques, puis étendez progressivement. Consultez notre article sur les détections Azure AD pour des exemples de règles à prioriser lors d'une migration vers Sentinel.

À retenir : Le choix entre SIEM cloud-native et on-premise dépend de trois facteurs clés : le volume d'ingestion (le cloud est avantageux sous 200-300 Go/jour), les exigences de souveraineté (l'on-premise est nécessaire pour les données les plus sensibles) et les compétences disponibles (le cloud réduit le besoin en administration d'infrastructure). L'approche hybride est souvent le meilleur compromis, combinant la flexibilité du cloud avec le contrôle de l'on-premise pour les données critiques.

Avez-vous chiffré le TCO réel de votre SIEM actuel sur 3 ans en incluant tous les coûts cachés, ou prenez-vous vos décisions architecturales sur des estimations approximatives ?

Sources et références : MITRE ATT&CK · MITRE CAR

Perspectives et prochaines étapes

La frontière entre cloud et on-premise va continuer de s'estomper avec l'émergence de solutions hybrides natives qui s'adaptent automatiquement au placement optimal des données. Les solutions SIEM as a Service souveraines vont se développer en Europe sous l'impulsion des certifications SecNumCloud et des exigences NIS 2. Pour prendre votre décision, réalisez un TCO détaillé sur 3 ans pour les deux modèles en incluant tous les coûts directs et indirects, évaluez vos contraintes de souveraineté avec votre DPO et votre RSSI, et conduisez un POC de 2 mois avec la solution cloud-native la plus pertinente pour votre écosystème avant de vous engager.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.