LIVRE BLANC · SÉCURITÉ DE LA SOLUTION

Livre blanc sécurité de REVIEWIT

Comment REVIEWIT protège la plateforme, les connexions à vos systèmes et vos données : identité, isolation, chiffrement, preuve, assistant RITA, exploitation et continuité. Ce livre blanc décrit les mesures en service à la date de publication et dit clairement celles qui sont prévues.

VERSION
1.0 · Novembre 2026

PÉRIMÈTRE
REVIEWIT SAS · solution SaaS REVIEWIT, toutes régions

DIFFUSION
Public

SOMMAIRE

01 REVIEWIT en bref
02 Principes de sécurité
03 Responsabilité partagée
04 Identité et accès
05 Isolation et résidence des données
06 Chiffrement, clés et secrets
07 Preuve et piste d'audit
08 Connexions aux systèmes du client
09 Assistant RITA
10 Développement et exploitation
11 Incidents et continuité
12 Vie privée, rétention et conformité
13 Contact et documents

OBJET

REVIEWIT est une solution SaaS de revue et de certification des accès. Pour l'exercer, elle collecte des métadonnées d'identité et de droits dans les systèmes de ses clients et produit la preuve des décisions prises. Ce livre blanc s'adresse aux responsables de la sécurité, aux équipes achats et conformité ; il présente l'architecture de sécurité de la solution, sans détail qui en affaiblirait la protection.

LECTURE

Chaque mesure porte un état. **En service** : en fonctionnement à la date de publication. **Limite connue** : en service, avec la limite décrite. **Prévu** : inscrit à la trajectoire de REVIEWIT, sans engagement de date. **Engagement** : obligation contractuelle de REVIEWIT. La référence contractuelle est l'annexe 1 de l'accord de traitement des données (mesures techniques et organisationnelles) ; en cas d'écart, elle prévaut sur le présent document.

SECTION 01 REVIEWIT en bref

REVIEWIT réunit dans une même boucle la découverte des accès, leur revue par des personnes désignées et la preuve des décisions. La solution se raccorde aux suites collaboratives, aux annuaires d'identité et aux applications métier du client, par des connexions dédiées ou par import de fichiers.

MÉTADONNÉES

Des métadonnées, pas des contenus

Identités, comptes, groupes, appartenances, rôles, ressources et permissions. Ni le contenu des messages, des documents ou des fichiers, ni les mots de passe.

CONTRÔLES NATIFS

Vos contrôles restent maîtres

REVIEWIT ne remplace ni l'authentification ni les autorisations des plateformes connectées : il les lit, en lecture seule, avec les permissions que vous lui accordez.

DÉCISION HUMAINE

Une personne décide

Chaque décision de revue est prise par une personne nommée et tracée. L'assistant RITA ne prend, ne recommande ni ne rédige aucune décision.

PREUVE

Une preuve qui se vérifie

Piste d'audit chaînée et scellée chaque jour, exportable avec ses empreintes et ses sceaux pour être vérifiée hors de REVIEWIT.

SECTION 02 Principes de sécurité

PRINCIPE	CE QUE CELA SIGNIFIE CHEZ REVIEWIT
Confiance zéro	Aucun utilisateur, service, connexion ni réseau n'est réputé sûr : chaque appel est authentifié, et la souscription qu'il vise est celle de son jeton d'accès, contrôlée à l'entrée.
Moindre privilège	Rôles propres à REVIEWIT, avec une échéance obligatoire pour les rôles nominatifs ; connexions en lecture seule ; chaque composant n'accède qu'aux secrets nécessaires à sa fonction.
Défense en profondeur	Contrôles superposés : identité, autorisation, isolation des bases, réseau privé, chiffrement, coffre de secrets, piste d'audit scellée.
Sécurité par défaut	L'assistant RITA fonctionne par défaut en mode déterministe, sans modèle d'IA ; le mode IA générative n'est actif que sur décision du client.
Minimisation	Requêtes restreintes aux attributs utiles ; chaque plan de collecte porte sur une seule ressource choisie par le client ; RITA ne reçoit que des agrégats.

Maîtrise par le client	Le client choisit ses connexions et les périmètres collectés, sa région d'hébergement, son profil de rétention, l'activation de RITA et les destinations de sa piste d'audit.
Rien d'annoncé sans vérification	Une mesure n'est dite en service qu'une fois constatée ; ce qui est prévu est dit prévu.

SECTION 03 Responsabilité partagée

La sécurité de la solution se répartit entre quatre acteurs.

ACTEUR	RESPONSABILITÉ
REVIEWIT	Application, connexions, interfaces de programmation, isolation des souscriptions, données stockées, chiffrement et coffre de secrets, piste d'audit, développement et publication, gestion des vulnérabilités, notification des incidents, accès de son personnel.
Notre hébergeur cloud	Centres de données et leur sécurité physique ; infrastructure de calcul, de stockage et de réseau ; disponibilité des services gérés. Sa sécurité est attestée par ses certifications ISO/IEC 27001 et ses rapports SOC.
Plateformes connectées	Authentification et autorisations natives, interfaces exposées, application des permissions accordées à REVIEWIT, disponibilité de leur service.
Client	Choix des systèmes connectés et des périmètres ; permissions accordées aux connexions ; fournisseur d'identité et sa politique d'authentification forte ; attribution des rôles REVIEWIT ; désignation des réviseurs ; protection de ses propres identifiants et de la clé qu'il importe.

SECTION 04 Identité et accès

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Authentification fédérée	Autorité d'identité propre à REVIEWIT (OpenID Connect), raccordée au fournisseur d'identité du client, dont les politiques d'authentification s'appliquent.	EN SERVICE
Authentification forte des administrateurs	Exigée sur les consoles d'administration et vérifiée au retour du fournisseur d'identité.	EN SERVICE
Authentification des réviseurs	Non imposée par REVIEWIT sur la console de revue : sa force dépend de la politique du fournisseur d'identité du client.	LIMITE CONNUE
Rôles et autorisations	Rôles propres à REVIEWIT, attribués dans REVIEWIT : opérateur de plateforme, administrateur de souscription, rôles de workspace, auditeur en lecture seule. Échéance obligatoire des rôles nominatifs.	EN SERVICE
Validation à quatre yeux	Les opérations sensibles sont approuvées par deux personnes distinctes ; c'est le cas de l'export et de la suppression des bases d'une souscription en fin de contrat.	EN SERVICE

Accès du personnel de REVIEWIT	Limité au besoin, tracé dans la piste d'audit et, hors urgence, réalisé à la demande du client.	EN SERVICE
Fédération SAML	Raccordement des fournisseurs d'identité par SAML 2.0.	PRÉVU

SECTION 05 Isolation et résidence des données

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Bases dédiées	Chaque souscription dispose de ses propres bases, avec des rôles d'accès propres à chacune et aucun droit de connexion accordé par défaut.	EN SERVICE
Contrôle de souscription	La souscription visée par un appel est celle que porte son jeton d'accès, vérifiée à l'entrée de la plateforme.	EN SERVICE
Résidence	Données stockées et traitées dans la région d'hébergement choisie par le client (Paris par défaut) ; sauvegardes conservées dans cette région.	EN SERVICE
Aucune copie hors région	Aucune copie dans une autre région, sauf instruction écrite du client pour une copie des sauvegardes dans une seconde région de la même géographie.	EN SERVICE
Bases non exposées	Aucune base accessible depuis Internet ; aucune adresse IP publique sur les sous-réseaux ; administration par un bastion, sans SSH ni adresse IP publique.	EN SERVICE
Réseau	Réseau privé virtuel réparti sur deux zones de disponibilité ; filtrage en chaîne entre le point d'entrée, les services et les bases.	EN SERVICE
Pare-feu applicatif	Pare-feu applicatif, journaux de flux réseau et filtrage des flux sortants.	PRÉVU

SECTION 06 Chiffrement, clés et secrets

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
En transit	TLS 1.2 et 1.3 sur les points d'entrée, redirection vers HTTPS, HSTS dans les consoles ; TLS imposé vers les bases de données.	EN SERVICE
Au repos	Bases chiffrées au niveau du stockage ; archives chiffrées sur une clé dédiée à rotation annuelle ; coffre de signature sur une clé à rotation ; états de l'infrastructure chiffrés (AES-GCM).	EN SERVICE
Secrets de la plateforme	Aucun secret dans la configuration ni dans les journaux ; gestionnaire de secrets de notre hébergeur cloud ; autorité de certification interne qui renouvelle les identités des services et tient une liste de révocation des appelants.	EN SERVICE
Identifiants des connexions	Sous la garde de REVIEWIT SEAL : chiffrés sous une clé maître dédiée à chaque client et liés à leur détenteur ; aucune fonction, même d'administration, ne permet d'en lire la valeur.	EN SERVICE

Identifiants antérieurs à la garde	Les identifiants déposés avant la mise en service de la garde sont repris sous la clé maître de leur client, détenteur par détenteur ; jusqu'à leur reprise, ils ne sont protégés que par le chiffrement au repos des bases.	LIMITE CONNUE
Clé du client pour la signature	Le client peut importer sa propre clé privée de connexion dans le coffre SEAL, qui signe avec elle ; la clé n'est jamais exportée.	EN SERVICE
Chiffrement par clé du client	Chiffrement sous une clé maître détenue ou importée par le client.	PRÉVU
Rotation des clés	Clé maître de chaque souscription : rotation automatique annuelle. Clés de chaque client dans le coffre SEAL : rotation annuelle. Clé de signature de SEAL : échéance fixée, alerte avant son terme. Identités des services : renouvellement automatique.	EN SERVICE

La **Fiche sécurité SEAL** (publique) et l'**annexe « Gestion des clés et des secrets »** (clients et prospects sous accord de confidentialité) détaillent les modèles de clé, la révocation et la suppression des secrets.

SECTION 07 Preuve et piste d'audit

La valeur d'une revue d'accès tient à sa preuve. REVIEWIT la construit pour qu'un auditeur puisse la vérifier lui-même, sans devoir faire confiance à REVIEWIT.

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Contenu des événements	Horodatage UTC, acteur, rôle effectif, action, résultat.	EN SERVICE
Chaînage et sceaux	Événements canonisés et chaînés par empreinte SHA-256 ; chaque chaîne est scellée chaque jour par l'autorité de scellement REVIEWIT SEAL ; toute altération devient détectable.	EN SERVICE
Purge	Par segment scellé entier, jamais ligne à ligne ; le registre des purges est protégé contre la modification et la suppression.	EN SERVICE
Diffusion vers votre SIEM	Événements diffusés vers le SIEM du client (BEACON).	EN SERVICE
Export vérifiable	Piste d'audit exportable avec sa séquence, ses empreintes chaînées et ses sceaux signés ; le client en vérifie l'intégrité selon une procédure documentée.	EN SERVICE

SECTION 08 Connexions aux systèmes du client

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Lecture seule	La collecte se fait en lecture seule : aucune écriture vers Microsoft 365 ni vers Google Workspace.	EN SERVICE

Permission plus large que la lecture	Lorsqu'une plateforme n'offre pas de permission de lecture suffisante, comme pour lire les permissions des sites SharePoint, la permission demandée n'est exercée qu'en lecture.	EN SERVICE
Périmètre choisi	Chaque plan de collecte porte sur une seule ressource choisie par le client ; les requêtes sont restreintes aux attributs utiles.	EN SERVICE
Reflet à jour	Reflet rafraîchi à chaque collecte : un compte disparu de la source disparaît du reflet.	EN SERVICE
Identifiants sous garde	Identifiants des connexions sous la garde de SEAL (section 06) ; le client peut à tout moment retirer son consentement auprès de la plateforme source.	EN SERVICE

SECTION 09 Assistant RITA

RITA aide à lire les accès et les campagnes. Elle ne prend, ne recommande ni ne rédige aucune décision de revue.

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Maîtrise par le client	Désactivable par souscription et par fournisseur ; mode déterministe par défaut, sans appel à un modèle d'IA ; aucun outil d'écriture.	EN SERVICE
Mode IA générative	Actif seulement si le client l'active par un avenant de traitement IA ; routes limitées à la géographie de la région (européenne pour l'Union européenne) ; toute autre route est refusée côté serveur.	EN SERVICE
Pas d'entraînement	Ni REVIEWIT ni ses fournisseurs n'utilisent les données du client pour entraîner des modèles.	ENGAGEMENT
Conservation	Conversations jamais conservées ; empreinte de chaque question conservée 12 mois dans la piste d'audit ; journal des questions de données purgé à 30 jours.	EN SERVICE
Filtrage	Secrets filtrés avant tout envoi au modèle ; version de modèle figée ; RITA ne reçoit que des agrégats.	EN SERVICE

SECTION 10 Développement et exploitation

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Analyse statique	Analyseurs de code exécutés à chaque compilation.	EN SERVICE
Tests automatisés	Suites de tests automatisés, dont des tests négatifs d'accès aux consoles.	EN SERVICE
Chaîne de publication	Images de conteneurs à étiquettes immuables, analysées à la poussée et déployées par empreinte ; manifeste de version scellé, exigé pour le canal stable.	EN SERVICE

Gestion des vulnérabilités	Surveillance du code, des dépendances, des images et de la configuration ; correction ou atténuation sous 14 jours pour une vulnérabilité critique, sous 30 jours pour une vulnérabilité élevée, dans le cycle normal de publication pour les autres.	ENGAGEMENT
Page de statut publique	Sondes externes lancées depuis plusieurs régions sur chaque région provisionnée ; historique de disponibilité et incidents publiés.	EN SERVICE
Test d'intrusion	Test d'intrusion annuel par un tiers indépendant.	PRÉVU
Détection centralisée	Journalisation des appels d'administration, détection des menaces et centralisation des alertes chez l'hébergeur ; astreinte.	PRÉVU

SECTION 11 Incidents et continuité

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Violation de données	Notification au client au plus tard 24 heures après la prise de connaissance, y compris lorsque la violation survient chez un sous-traitant ultérieur ; compléments au fil de l'enquête.	ENGAGEMENT
Incident de sécurité (NIS 2, DORA)	Pour les clients concernés : alerte sous 24 heures, mise à jour sous 72 heures, rapport final sous un mois ; en cas de doute, l'incident est notifié.	ENGAGEMENT
Sauvegardes	Sauvegardes automatiques des bases, conservées 35 jours en production ; base répartie sur deux zones de disponibilité.	EN SERVICE
Export vérifié	Export d'une souscription vérifié par une restauration réelle.	EN SERVICE
Objectifs de reprise	Perte de données maximale (RPO) de 24 heures et délai maximal de rétablissement (RTO) de 48 heures, pour un service désigné comme soutenant une fonction critique ou importante (DORA).	ENGAGEMENT
Test de restauration chronométré	Test chronométré vérifiant ces objectifs.	PRÉVU

La synthèse **« Stratégie de sauvegarde et de reprise »** (publique) détaille ces mesures.

SECTION 12 Vie privée, rétention et conformité

MESURE	MISE EN ŒUVRE CHEZ REVIEWIT	ÉTAT
Rôles au sens du RGPD	Le client est responsable du traitement et REVIEWIT sous-traitant, dans le cadre d'un accord de traitement des données (article 28) ; traitement sur instruction documentée du client.	EN SERVICE

Sous-traitants ultérieurs	Accord de traitement de chaque fournisseur archivé et évalué ; tout ajout ou remplacement notifié trente jours à l'avance, avec droit d'opposition.	EN SERVICE
Conservation limitée	Catalogue de 37 catégories de données avec des durées ratifiées ; profil de rétention choisi par le client ; purge par le produit ; registre de suppression hors sauvegarde ; mesures de gel tracées.	EN SERVICE
Droits des personnes	Recherche d'une personne dans les bases d'une souscription, export et effacement, sous la référence de la demande.	EN SERVICE
Fin de contrat	Export vérifié de la souscription, remise d'un paquet de restitution, effacement des bases, attestation de suppression ; aucun frais de changement de fournisseur.	EN SERVICE
Certification de REVIEWIT	REVIEWIT ne détient pas encore de certification propre et n'en revendique aucune avant de l'avoir obtenue ; la démarche ISO/IEC 27001 est engagée.	PRÉVU

La solution aide ses clients à produire les preuves de revue des accès attendues par le RGPD, l'ISO/IEC 27001, NIS 2, DORA ou SOC 2 ; cela ne fait pas de REVIEWIT une entité certifiée au titre de ces référentiels.

SECTION 13 Contact et documents

Questions de sécurité et signalement de vulnérabilités : **security@we-reviewit.com**. REVIEWIT accuse réception de chaque signalement et le traite selon sa politique de divulgation responsable. Nous demandons aux chercheurs de ne consulter, modifier ni conserver aucune donnée de client.

DOCUMENT	ACCÈS
Politique de divulgation responsable des vulnérabilités	Public
Fiche sécurité SEAL (scellement, gestion des clés)	Public
Stratégie de sauvegarde et de reprise — synthèse	Public
Annexe « Gestion des clés et des secrets »	Clients et prospects sous accord de confidentialité
Mesures techniques et organisationnelles (annexe 1 du DPA)	Clients · accès authentifié
Accord de traitement des données et ses annexes	Clients · accès authentifié
Prestataires informatiques de REVIEWIT	Clients · accès authentifié

REVIEWIT SAS · Sécurité : security@we-reviewit.com · Protection des données : dpo@we-reviewit.com.
Document revu annuellement et après tout changement majeur de la solution. La version française fait foi.