Equalis OpsReg

Vue d'ensemble de l'architecture de sécurité

Version 1.0 · 2 novembre 2026 · EqualisTech OpsReg Limited, CRO 814298

Comment Equalis OpsReg lit les abonnements Azure d'un client, où la plateforme s'exécute, quelles mesures protègent les données des clients et comment les preuves sont conservées. Rédigé à partir du centre de confiance et des pages produit publiés ; aucun nom de système interne.

1. Modèle d'accès

La plateforme est en lecture seule dès sa conception. Elle reçoit trois rôles Azure intégrés en lecture seule sur les abonnements choisis et ne dispose d'aucun droit en écriture. Elle ne déploie aucune stratégie, ne modifie aucune ressource, et aucune fonction ne peut être activée pour lui en donner la capacité.

Elle lit des métadonnées de configuration et de sécurité via Azure Resource Manager et Azure Resource Graph, y compris les recommandations et alertes de sécurité qu'Azure expose pour ces ressources. Les rôles ne donnent aucun accès aux données de vos bases de données, comptes de stockage ou machines virtuelles. Le rôle Reader permet aussi d'interroger les données de journaux des espaces de travail Log Analytics de ces abonnements.

L'accès est révocable à la demande depuis votre propre locataire, en supprimant les attributions de rôles et l'application d'entreprise.

Rôles	Reader, Security Reader, Cost Management Reader
Droits en écriture	Aucun
Données lues	Métadonnées uniquement, jamais le contenu des charges de travail
Informations d'identification Azure stockées	Aucune

2. Architecture

Où s'exécute chaque composant, et comment circulent les données : la configuration est lue dans votre locataire, en lecture seule, et les constats ne partent que vers les outils que vous connectez.

Votre locataire Azure

Abonnements
De 1 à 50, chaque abonnement est un périmètre d'audit

Attributions de rôles (lecture seule)
Reader, Security Reader, Cost Management Reader

Application multilocataire
Consentement administrateur ; accès révocable à la demande depuis votre propre locataire

Azure Resource Manager et Azure Resource Graph, en lecture seule

Equalis OpsReg · Azure North Europe, sauvegardes dans West Europe

Moteur de règles
437 règles versionnées, cinq référentiels

Stockage des preuves
Écriture unique, conservation sept ans pendant l'abonnement

Tableaux de bord et exports PDF
Par référentiel et par abonnement

Connecteurs

Microsoft Teams, Slack, e-mail, Jira, ServiceNow, PagerDuty, Webhook

Les constats sont envoyés vers les outils de vos équipes

3. Rôles accordés

Trois rôles de lecture intégrés, sans aucun droit d'écriture sur vos ressources, limités aux abonnements que vous choisissez.

Rôle	Utilité
Reader	Lire la configuration de toutes les ressources.
Security Reader	Lire les recommandations, alertes et états de sécurité qu'Azure expose pour vos ressources.
Cost Management Reader	Attribué par le même modèle en vue d'une capacité ultérieure ; la version actuelle ne lit aucune donnée de coût. Comme les deux autres rôles, il ne donne aucun droit d'écriture sur vos ressources.

4. Hébergement et localisation des données

Élément	Localisation
Régions Azure	North Europe (Irlande) ; sauvegardes géo-redondantes dans West Europe (Pays-Bas)
Transferts hors EEE	Aucun par EqualisTech, en dehors des constats envoyés aux outils que vous connectez. Microsoft documente des cas limités dans lesquels les services Microsoft que nous utilisons (Microsoft Azure, y compris le réseau périphérique d'Azure Front Door, Microsoft Entra External ID, Azure Communication Services et Microsoft 365) peuvent traiter des données ou y accéder hors de l'UE, par exemple pour l'accès à distance par le personnel de Microsoft, les opérations de sécurité mondiales et le support ; voir l'accord de traitement des données.
Entité juridique	EqualisTech OpsReg Limited, Dublin, Irlande (CRO 814298)
Droit applicable	Droit irlandais

5. Mesures de sécurité

Isolation des clients

Sécurité au niveau des lignes dans la base de données. Chaque requête sur les données clients est filtrée sur l'identifiant client issu du jeton d'accès, jamais du corps de la requête.

Réseau

Azure Front Door Premium avec un pare-feu applicatif web utilisant les jeux de règles gérés de Microsoft (Default Rule Set et Bot Manager), en mode Prévention en production. En production, bases de données et stockage sont derrière des points de terminaison privés.

Identité

Microsoft Entra External ID pour la connexion des utilisateurs, identités managées entre les services de la plateforme. L'accès à vos abonnements passe par l'application multilocataire à laquelle vous consentez, qui s'authentifie avec une identité managée comme information d'identification fédérée : aucun secret client, certificat ni information d'identification Azure n'est stocké.

Intégrité des preuves

Preuves en écriture unique, conservation pendant sept ans tant que votre abonnement à Equalis OpsReg est actif, rapports scellés par empreinte cryptographique et journaux d'audit dont toute altération est détectable.

Lecture seule dès la conception

Le code ne contient aucun appel qui écrit dans vos abonnements Azure. Le principe précède la première ligne de code : informer, ne jamais agir.

Comptes professionnels uniquement

L'inscription exige une adresse sur le domaine de votre organisation. Les messageries personnelles sont refusées.

6. Intégrité et conservation des preuves

Les preuves sont écrites une seule fois et ne peuvent être modifiées ni par l'application ni par ses utilisateurs. Elles sont conservées sept ans tant que votre abonnement à Equalis OpsReg est actif, et les rapports de preuves sont scellés par une empreinte cryptographique : toute modification ultérieure est détectable.

Les exports sont produits par référentiel et par abonnement : le périmètre d'un rapport correspond toujours à celui de l'audit.

Conservation	Sept ans pendant l'abonnement
Stockage	Écriture unique
Intégrité des rapports	Scellés par empreinte cryptographique
Périmètre des exports	Un référentiel, un abonnement
Format	PDF

7. Sous-traitants ultérieurs

Sous-traitants ultérieurs de la plateforme Equalis OpsReg à sa disponibilité générale. Les clients sont informés au moins 30 jours avant l'ajout ou le remplacement d'un sous-traitant ultérieur et peuvent s'y opposer. Les services utilisés par ce site web sont indiqués dans la politique de confidentialité.

Sous-traitant ultérieur	Service	Localisation
Microsoft Ireland Operations Limited	Hébergement de la plateforme (Microsoft Azure), authentification (Microsoft Entra External ID), e-mails de notification (Azure Communication Services) et messagerie du support (Microsoft 365)	Union européenne (plateforme en Irlande, sauvegardes aux Pays-Bas ; autres services Microsoft dans des centres de données de l'UE, sous réserve des exceptions limitées documentées par Microsoft)

8. Signaler une vulnérabilité

Si vous pensez avoir identifié une vulnérabilité dans Equalis OpsReg, écrivez à security@equalistech.com en décrivant le problème. Nous accusons réception de chaque signalement et vous tenons informé jusqu'à sa résolution.

Merci de ne pas accéder à des données qui ne vous appartiennent pas et de ne pas perturber le service pendant vos recherches.