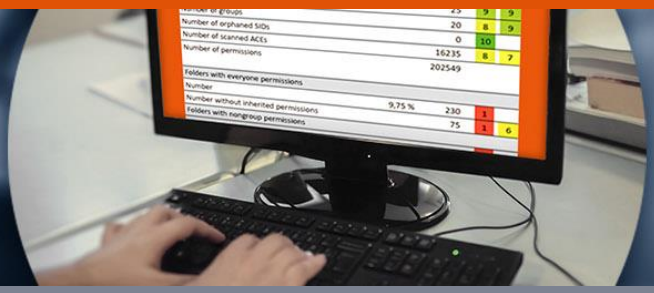
betasystems

GARANCY DATA ACCESS GOVERNANCE

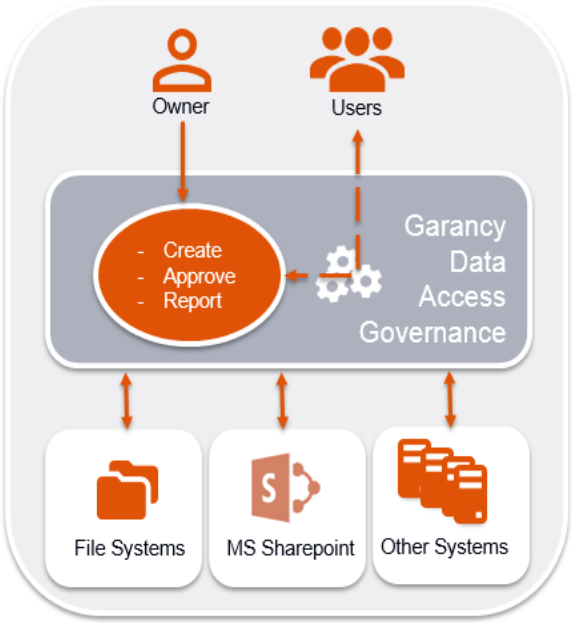


Gestion sûre des accès aux données non structurées

- *Qui donnent les droits d'accès aux données sensibles non structurées dans votre entreprise ?*
- *Savez-vous qui est responsable de ces données ?*
- *Savez-vous si votre gestion des accès respecte les exigences de conformité ?*

Meilleure sécurité et précision améliorée

Les entreprises traitent un volume de données non structurées toujours plus grand dans leur quotidien, entre les documents, les tableaux, les présentations ou les e-mails. Les serveurs de fichiers et les autorisations sont de plus en plus difficiles à gérer. La sécurité des informations est menacée notamment par des accumulations de droits et des droits d'accès non supprimés pour les salariés ayant quitté l'entreprise. Il est important de clairement savoir qui a accès à quoi, qui autorise l'accès et de déceler les faiblesses structurelles dans les serveurs de fichiers qui peuvent entraîner des fuites de données involontaires.



Les départements métiers qui ont produit l'information délivrent les autorisations
Grâce à GARANCY Data Access Governance (DAG), les départements métiers sont responsables des informations qu'ils stockent :

- Les propriétaires de données déterminent rapidement et facilement « qui devrait avoir accès à telles ressources de données, quand, où et de quelle manière ». Cela se fait sans intervention directe de l'administration informatique et sous une forme compréhensible par tous.
- GARANCY DAG permet de gérer les permissions à un niveau inférieur aux groupes « Active Directory » tels que les serveurs de fichiers, les services SharePoint ou d'autres systèmes de gestion des documents.
- Des workflows de permission intégrés ou encore le portail en libre-service connectent automatiquement les propriétaires de données ou les responsables de projets concernés au processus d'attribution.

GARANCY DAG permet ainsi une gestion autonome des données, ressources et droits d'accès par les départements métiers en accord avec les lois et règlementations en vigueur. Un **audit de permissions** peut être un premier pas, réalisé sur la base d'une méthode éprouvée. Les résultats de l'audit peuvent être utilisés pour mettre en place une **consolidation automatique de la gestion des accès aux systèmes de fichiers**.

Modèle en trois phases :

1. **Analyse & rapport :**
   - Analyse des permissions : identification et analyse automatiques des schémas d'autorisations et des droits d'accès aux données non structurées incluant un rapport sur « qui a le droit de faire quoi et qui a attribué quels droits et quand? »
   - Analyse de sécurité : évaluation des dangers potentiels par niveau de risque grâce à des indicateurs de risque.
   - Rapports de résultats : évaluation des efforts pour résoudre les failles de sécurité, avec les recommandation associées.

2. **Consolidation et migration:** phase de « **clean-up »**
   - Nettoyage, restructuration et consolidation des schémas d'autorisation et des permissions (prestation outillée).
   - Migration des données et des droits vers la nouvelle structure sans perturber les processus commerciaux (prestation outillée)

3. **Data Access Governance : Contrôle et gestion des droits d'accès**
   - Gestion sûre des informations, autorisations et ressources des systèmes contenant des données non structurées.
   - Délégation du contrôle des droits d'accès aux propriétaires des données, sans intervention de l'équipe IT
   - Plus d'attribution de droits en violation des règles : gestion des droits via des workflows couvrant l'ensemble du cycle de vie des utilisateurs et de leur permission, de la requête à l'attribution par validation ou à la révocation.
   - Contrôles de conformité intégrés : respect automatisé des directives légales et internes à l'entreprise concernant la gestion de l'accès aux données critiques (SOX, lois BDSG, MaRisk, GoBS/GDPdU, KonTraG, etc.).
   - Comparaison des droits théoriques et des droits réels: identification des écarts à risque.

Intégration totale avec IAM GARANCY

Le module Data Access Governance GARANCY prend encore plus de sens lorsqu'il est couplé avec la suite GARANCY IAM. Toutes les informations relatives aux données structurées et non structurées sont alors mises à disposition sur le système IAM principal.

- Administrateurs, opérateurs et utilisateurs restent dans leur environnement habituel et n'ont pas besoin de se former à une nouvelle solution.
- Point d'administration unique.
- Intégration aux portails libre-service et aux rapports existants.

Contactez-nous !

_betasystems

Beta Systems Software France SARL

5 avenue de Verdun
94200 Ivry-sur-Seine
Tél. : +33 6 76 09 57 78
info-f@betasystems.com

Partenaire