FICHE TECHNIQUE

Identity Manager – Data Governance Edition

Contrôlez l'accès aux données sensibles avec la gouvernance des données

Avantages

- Il trouve et assigne les propriétaires aux données non structurées
- Il fournit une vue depuis un seul écran des informations d'utilisation des donnes, ce qui n'était pas disponible auparavant
- Il réduit l'exposition aux failles de sécurité en permettant aux propriétaires des données de déterminer quels utilisateurs doivent avoir accès aux données sensibles
- Il améliore l'efficacité en allégeant la charge de travail des équipes informatiques pour répondre aux demandes d'accès
- Il fournit une preuve de conformité aux auditeurs avec les rapports d'accès des utilisateurs et d'attestations

Configuration système requise

Pour consulter la liste complète des exigences système, visitez oneidentity.com/products/identity-manager-data-governance/

Actuellement, de nombreuses entreprises sont vulnérables en raison d'une protection des données inadéquate. Les responsables de la sécurité et de la conformité rencontrent de plus en plus de difficultés à assurer la sécurité des données sensibles, car ils ne disposent pas d'un système d'accès approprié. Par conséquent, la conformité n'est pas respectée, ce qui place les entreprises en mauvaise posture.

Alors que les responsables des départements informatiques ont la permission d'accorder l'accès à des données spécifiques, ils le font souvent sans comprendre les répercussions que cela peut avoir. Ceci conduit dans de nombreux cas à autoriser l'accès à un collaborateur tout en exposant potentiellement d'autres comptes à des menaces extérieures. En multipliant les contrôles internes, il est possible d'assurer que l'accès aux données structurées reste entre les bonnes mains afin de ne pas créer de failles de sécurité ni de violation des réglementations. Identity Manager – Data Governance Edition, faisant partie des solutions One Identity, protège votre organisation en donnant le contrôle des accès aux propriétaires des entreprises, qui eux savent qui doit avoir accès aux données sensibles. La solution leur donne la possibilité d'analyser, d'approuver et de répondre aux demandes d'accès aux données non structurées aux fichiers, dossiers et partages sur les appareils NTFS, NAS et SharePoint.

ONE IDENTITY™

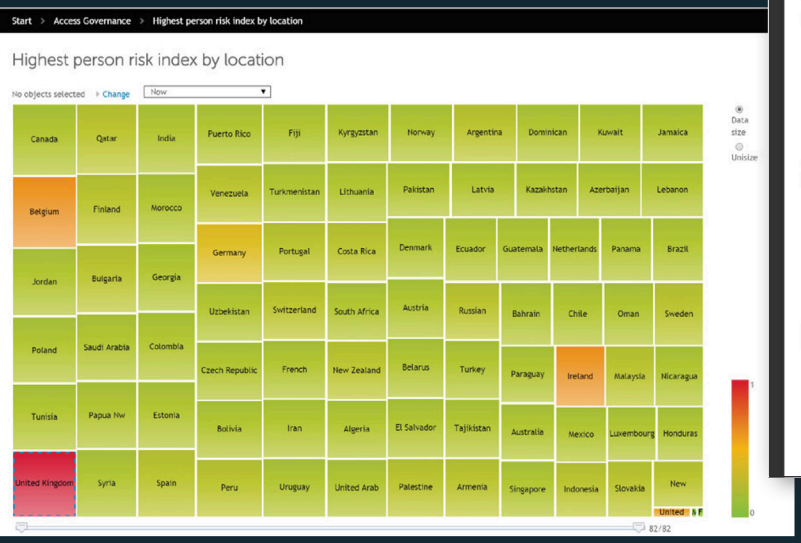

Figure 1. Carte thermique : les cartes thermiques fournissent un indice de risque et de violation des stratégies pour les données courantes ainsi qu'une comparaison avec les données passées.

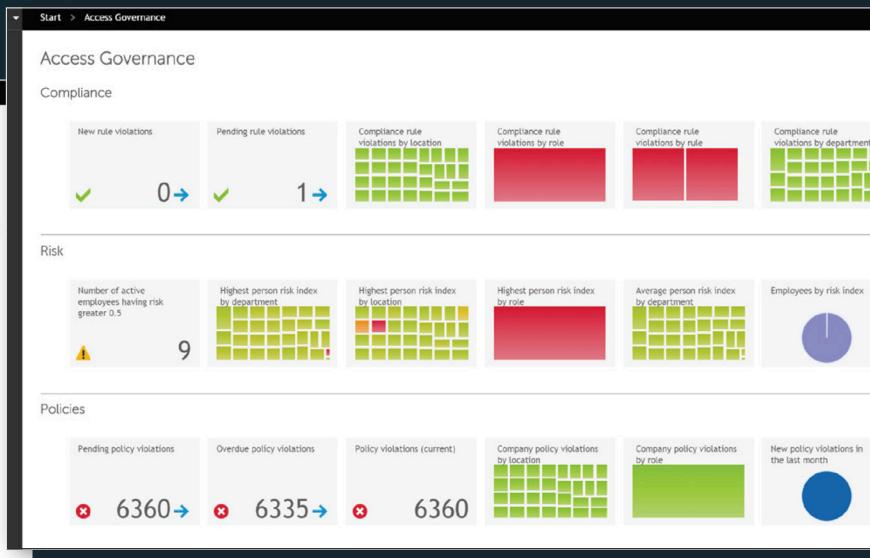

Figure 2. Données gérées : le propriétaire des données approuve la demande d'accès, crée les rapports, réalise les audits et gère le cycle de vie des données gérées.

Identity Manager – Data Governance Edition aide les propriétaires des données (ne faisant pas partie de l'équipe informatique) à déterminer qui doit avoir accès et à automatiser le workflow de demande et d'approbation. De cette manière, votre entreprise ne fera pas les gros titres des journaux en raison d'une faille de sécurité, et cela réduit en outre la charge de travail pour l'équipe informatique.

Fonctionnalités

Gouvernance du Cloud
Gérez le Cloud et effectuez des rapports d'accès avec la prise en charge de Microsoft SharePoint Online et OneDrive.

Classification des données
Classifiez manuellement les données gérées. Le chef d'entreprise peut définir la classification sur le portail Web. L'outil fournit une solution prête à l'emploi de stratégies et de calcul des risques en fonction du niveau de classification attribué.

Accès restreint
Définissez les politiques d'accès pour votre entreprise afin d'assurer que seuls les utilisateurs approuvés ont accès aux données sensibles non structurées. La solution Identity Manager – Data Governance Edition verrouille les données sensibles telles que les fichiers, les dossiers et les partages sur les appareils NTFS, NAS et SharePoint.

Attribution du propriétaire des données
Déterminez et assignez un propriétaire des données approprié pour l'ensemble des futures demandes d'accès en évaluant les schémas d'utilisation et les accès de lecture et d'écriture.

Audit simplifié
Identifiez les accès utilisateurs aux ressources de l'entreprise, telles que les fichiers, les dossiers et les partages sur les appareils NTFS, NAS et SharePoint afin de fournir des informations clés au cours de la préparation des audits.

Demandes d'accès automatisées
Utilisez les workflows intégrés pour orienter automatiquement les demandes d'accès du portail de demande au propriétaire des données concerné par la demande. Les demandes approuvées sont traitées automatiquement et correctement sans intervention de l'équipe informatique.

Vérification des accès
Assurez-vous que seuls les utilisateurs approuvés ont accès à des ressources spécifiques, notamment ceux qui ont quitté l'entreprise ou le département ou qui ont changé de poste. Identity Manager – Data Governance Edition vous permet de surveiller l'activité des utilisateurs et des ressources et de configurer et planifier un processus de recertification pour les propriétaires des données afin de vérifier et d'attester l'accès des collaborateurs.

Tableau de bord personnalisé
Affichez les tendances, l'historique et les données actuelles des activités d'accès aux données et l'état d'attestation sur un tableau de bord personnalisé avec des rapports pouvant servir à prouver la conformité aux auditeurs.

À propos de One Identity

La gamme One Identity de solutions de gestion des accès et des identités (IAM) inclut une offre de solutions IAM concrètes de gouvernance des identités, de gestion des accès et de gestion des comptes à privilèges axées sur l'entreprise, modulaires, intégrées et tournées vers l'avenir.

Pour en savoir plus, visitez OneIdentity.com

Datasheet-IdentityMgr-DataGovEd-US-CW-FR-WL-24725

ONE IDENTITY™