Informatica

Livre blanc

Limiter les risques liés à la confidentialité des données pour la gestion des données de référence

À propos d'Informatica

La transformation digitale fait évoluer les attentes : meilleurs services, livraisons plus rapides, à moindre coût. Les données sont la clé de la réussite des entreprises, et ces dernières doivent évoluer pour rester compétitives.

En tant que leader mondial dans la gestion des données Cloud d'entreprise, nous sommes prêts à vous guider de manière intelligente — quels que soient le secteur, la catégorie ou la niche. Informatica vous permet de prendre une longueur d'avance pour gagner en agilité, concrétiser de nouvelles opportunités de croissance ou même innover. Nous nous concentrons sur les données afin de vous offrir la polyvalence nécessaire pour réussir.

Découvrez nos solutions et libérez tout le potentiel de vos données en vue de la prochaine révolution intelligente.

Table des matières

Synthèse

Les entreprises investissent dans des initiatives de gestion des données de référence (MDM) afin de créer une vue d'ensemble fiable et pertinente des clients, des produits, des services, des opérations et d'autres informations stratégiques d'entreprise. Le MDM regroupe les éléments relatifs aux données essentielles dans l'ensemble de l'entreprise dans des dossiers consolidés pour créer des données fiables à partager avec les personnes et les applications qui en ont besoin. Il s'agit d'une valeur exceptionnelle pour toute entreprise désirant axer les offres sur les clients, améliorer le service client et les programmes de fidélisation, rendre efficace la gestion des produits et des solutions, migrer vers le Cloud en toute sécurité, etc.

Les données fiables deviennent l'un des piliers des initiatives clients et produits des entreprises et fournissent un avantage concurrentiel. Toutefois, la consolidation des données sensibles constitue également une cible intéressante pour les attaques extérieures, qui entraînent des violations de la sécurité des données et augmentent les abus internes potentiels. Elle est donc soumise à des réglementations relatives à la vie privée, telles que le Règlement général sur la protection des données (RGPD), le California Consumer Privacy Act (CCPA) et bien d'autres encore.

Par conséquent, nous sommes amenés à nous poser des questions sur la protection des données et la conformité de ces environnements :

- Où se trouvent toutes les données et comment prolifèrent-elles ?
- Qu'est-ce qui alimente le repository ? Qui a accès aux données et avec quelles applications ?
- L'accès et l'utilisation actuels respectent-ils les règlements et les politiques d'utilisation des données approuvés ?
- Les protections des données sont-elles appropriées ? Les risques liés aux données demeurent-ils à des niveaux acceptables ou existe-t-il des conditions créant plus de risques inappropriés qu'il faut corriger ?

La prise de décisions quant aux risques, à la protection et à la conformité réglementaire en matière de confidentialité des données de référence repose sur les résultats de la découverte et de la classification des données client sensibles.

Ce livre blanc propose un cadre pour les considérations et les stratégies à adopter d'atténuation des risques avec une solution axée sur les données qui :

- utilise l'analyse, l'intelligence pilotée par les métadonnées, l'automatisation et l'intelligence artificielle pour identifier et protéger les données de référence sensibles ;
- s'adapte à l'évolution de la gouvernance de données et des réglementations relatives à la vie privée ;
- fournit une préparation à l'audit pour attester des contrôles en place, et ;
- signale tout comportement anormal de l'utilisateur, nécessitant une enquête, aux parties prenantes.

Introduction

Selon l'institut de recherche IDC, 175 zettaoctets de données devraient être créés dans le monde d'ici 2025, contre 33 zettaoctets créés en 2018[1]. Les entreprises de tous les secteurs comptent sur la précision, la disponibilité et la protection de leurs données pour générer des revenus, servir les clients, augmenter la productivité, optimiser les opérations et mener d'autres processus métiers critiques.

La croissance exponentielle continue du volume de données et de leur utilisation inclut également des données de référence sensibles sur plusieurs silos, à la fois sur site et dans le Cloud, dans une variété de formats de données. Par conséquent, les méthodes traditionnelles de sécurité des données sont devenues obsolètes[2]. Les entreprises ont besoin d'une nouvelle approche de la sécurité des données de référence.

Cependant, la plupart des entreprises ne sont pas en mesure d'identifier avec précision l'emplacement de leurs données de référence sensibles et comment elles y accèdent, en particulier si ces dernières existent dans un format non structuré. Ce manque de visibilité augmente le risque auquel une entreprise est exposée et, par conséquent, les atteintes à la sécurité des données demeurent le principal risque de sécurité informatique[3].

La hausse des atteintes à la sécurité des données associée à la prolifération des données de référence sensibles utilisées de façon inappropriée impose aux entreprises de développer une stratégie d'atténuation des risques, qui inclut une solution de confidentialité axée sur les données, disposant des caractéristiques clés suivantes :

- visibilité dans toutes les sources de données pour découvrir et classer les données de référence sensibles réparties dans toute l'entreprise ;
- capacité à implémenter des mécanismes de protection des données de référence sensibles pour atténuer les atteintes à la sécurité des données ;
- conformité avec les réglementations actuelles en matière de confidentialité, notamment l'utilisation de l'intelligence pilotée par les métadonnées, de l'intelligence artificielle pour surveiller le comportement des utilisateurs et signaler toute anomalie en temps quasi réel ;
- outils de visualisation d'analyse riches pour l'évaluation des risques et la gestion des données sensibles ;
- capacités de création de rapports transparentes et complètes pour démontrer l'état de préparation à l'audit des contrôles.

Gartner estime que les produits de protection intégrés axés sur les données remplaceront les outils en silos et disparates consacrés à la sécurité des données dans 40 % des grandes entreprises, ce qui est le cas pour 5 % d'entre elles[4]. Ces solutions de protection axées sur les données offrent une vue centralisée des données à risque, de sorte que tous les intervenants principaux d'une entreprise internationale puissent suivre la circulation des données sensibles et appliquer des mécanismes de protection, comme imposé par les politiques et les réglementations de gouvernance.

[1] Livre blanc IDC, « The Digitization of the World – From Edge to Core » (novembre 2018).
[2] Gartner, « Market Guide for Data-Centric Audit and Protection », 21 mars 2017.
[3] Ponemon Institute LLC, « Data Breaches and Sensitive Data Risk », février 2016.
[4] Gartner, « Market Guide for Data-Centric Audit and Protection », 21 mars 2017.

Une stratégie en 4 étapes pour limiter les risques liés à la confidentialité des données sensibles

Les risques liés à la confidentialité des données sensibles découlent de la perte de ces dernières à cause d'une exposition inappropriée. La principale cause de cette perte est une atteinte à la sécurité des données ou une utilisation abusive en interne. L'idée reçue selon laquelle la simple action d'identifier l'emplacement des données de référence sensibles suffit à remédier aux risques est courante. Toutefois, la localisation et la classification de ces données ne représentent que la première étape d'une stratégie globale de correction des risques.

Les étapes suivantes consistent à évaluer les priorités en matière de risques auxquelles doit faire face votre entreprise en fonction des résultats de l'analyse de l'emplacement et de la classification. Vous devez déterminer une stratégie pour réduire les risques principaux – avec des contrôles automatisés veillant au respect des politiques de gouvernance des données et impliquant tous les intervenants principaux – pas seulement les membres de l'équipe informatique. Votre stratégie doit inclure l'implémentation d'une solution de protection et de confidentialité fiable et axée sur les données qui offre des capacités de conformité réglementaire, notamment des visualisations d'analyses enrichies des données sensibles pour les tableaux de bord et des rapports d'audit des contrôles de conformité, ainsi qu'une protection de tous les types de données de référence sensibles à travers l'entreprise.

1. Découverte et classification

Une approche ad hoc de la découverte consiste à examiner les sources existantes et envoyer des questionnaires. Cependant, une approche manuelle est inadéquate, car elle monopolise du temps et des ressources précieuses. Par ailleurs, elle est souvent inexacte et rapidement obsolète, et repose sur les rapports automatiques plutôt que sur la surveillance réelle en temps réel du comportement des utilisateurs et des flux de données.

Les entreprises doivent se demander :

- Quelles données stockons-nous, qui peut y accéder et à quelles fins ?
- Comment gérez-vous les privilèges d'un utilisateur et l'approvisionnement des droits de données ?
- Comment protégerons-nous les données de référence sensibles et nous assurerons-nous que les contrôles appropriés sont en place ?

Les autres considérations en matière de conformité de la découverte et la classification incluent :

- la définition et la compréhension de l'environnement de données, y compris les bases de données et les données non structurées ;
- le mapping des systèmes contenant des données de référence sensibles et le mapping des données aux identités ;
- l'acquisition d'une solution pouvant mapper la circulation de ces données à travers l'écosystème, tout en conservant une vue en temps quasi réel avec des outils d'analyse et de rapports.

2. Conformité

Les entreprises luttent pour identifier, surveiller et atténuer les risques liés aux données pour se conformer aux réglementations sur la confidentialité des données. De plus, elles doivent établir une surveillance, une analyse et un système d'alerte quant à l'accès aux données ou au mouvement qui pourrait compromettre la conformité.

Le RGPD, obligatoire depuis le 25 mai 2018, a été adopté afin de renforcer et d'unifier la protection des données pour toutes les personnes au sein de l'Union européenne, simplifiant ainsi l'environnement réglementaire des activités internationales. De même, la CCPA, qui est entrée en vigueur le 1er janvier 2020, place la barre plus haut en élargissant la protection de la confidentialité pour y inclure les données sur les ménages.

De nombreuses entreprises ne sont pas totalement prêtes pour ces deux réglementations et ne sont pas suffisamment conformes. Or la non-conformité pourrait entraîner des amendes importantes et nuire à leur réputation. D'autre part, la conformité peut favoriser l'avantage concurrentiel en tant que différentiateur de confidentialité des données de référence pour renforcer la fidélité des clients, tout en améliorant également les résultats de la transformation digitale. En outre, les entreprises qui font preuve de diligence en protégeant les données peuvent accéder 5 fois plus facilement aux informations personnelles de leurs clients qui leur font confiance pour les gérer de manière responsable[5].

Les entreprises doivent élaborer des politiques intelligentes qui identifient les magasins de données qui contiennent des « domaines de données » pertinents pour le RGPD, la CCPA et autres obligations similaires en matière de confidentialité. Ces politiques sont multifactorielles, avec une logique d'intelligence de données qui détermine quelles combinaisons constituent une menace d'exposition aux risques d'atteinte à la confidentialité.

[5] Extrait, Boston Consulting Group, « Bridging the Trust Gap in Personal Data »

3. Protection

En 2019, au troisième trimestre, plus de 5 000 failles de sécurité des données, avec près de 8 milliards d'enregistrements exposés[6]. De toute évidence, malgré d'importants investissements dans la confidentialité et la sécurité des données, les données personnelles stratégiques restent vulnérables. Les entreprises doivent en permanence protéger les données à haut risque, identifier les comportements suspects et l'utilisation ou la circulation non autorisée, tout en automatisant et orchestrant le processus de correction.

Les entreprises devraient donner la priorité aux risques les plus critiques liés aux données et y remédier par des contrôles axés sur les données qui favorisent la mobilité des données, plutôt que de se fier uniquement aux contrôles d'accès aux serveurs traditionnels, aux pare-feu et aux outils de cybersécurité similaires axés sur les systèmes. Par exemple, les contrôles centrés sur les données incluent le masking, les contrôles basés sur l'identité et le chiffrement.

Outre les contrôles de confidentialité des données, les entreprises doivent surveiller l'accès aux données et leur comportement basés sur l'identité. Un accès excessif ou un comportement inhabituel peut indiquer que les utilisateurs ne respectent pas les politiques de confidentialité ou que leurs identifiants ont été divulgués.

4. Préparation de l'audit et réponse

Les sociétés subissent plus que jamais des audits et des évaluations des données sensibles. Elles luttent pour fournir une preuve aux auditeurs qu'elles ont de la visibilité et que leurs données critiques sont protégées.

Les entreprises doivent pouvoir répondre immédiatement aux auditeurs et démontrer qu'elles connaissent l'emplacement des données et les risques connexes, la forme de protection des données et leur utilisation. Elles doivent savoir que les auditeurs souhaiteront obtenir des rapports et des visualisations extraits pour les services ou les emplacements, et qu'elles devront leur permettre d'approfondir certains domaines de données spécifiques.

Conclusion

Grâce à leur potentiel, les données MDM peuvent permettre aux entreprises de transformer leurs activités et leurs services. Leur potentiel est indéniable. Cependant, ces données représentent également une cible intéressante pour une utilisation abusive de la part d'intervenants internes ou externes. En raison des atteintes à la sécurité des données incessantes et des exigences de conformité de plus en plus nombreuses, les entreprises doivent réinventer leurs processus et leurs outils pour identifier, analyser et protéger les données sensibles.

[6] Rapport QuickView du 3e trimestre 2019 sur l'atteinte à la sécurité des données de Risk Based Security

Dans le climat actuel d'augmentation des risques en matière de confidentialité et d'atteintes courantes à la sécurité des données, les entreprises doivent élaborer une stratégie digitale fiable pour surveiller, analyser et corriger en permanence les risques liés à leurs données de référence sensibles. Elles doivent surveiller les données en temps quasi réel, à la recherche de signaux d'abus ou d'atteintes à la sécurité des données, d'accès ou de comportements inhabituels ou de transferts transfrontaliers inappropriés. Si elles s'y appliquent, les entreprises peuvent tirer profit des données MDM et améliorer leur position face aux risques liés aux données afin de réduire l'impact des atteintes à la sécurité des données ou des utilisations abusives internes, et répondre aux exigences rigoureuses des réglementations régionales et sectorielles.

Recommandations

1. Effectuer une évaluation des risques liés à la confidentialité des données pour comprendre parfaitement où se trouvent vos données de référence sensibles, la portée de leur prolifération dans votre écosystème de données et quels sont les ensembles de données sensibles les plus vulnérables pour la correction.
2. En fonction des résultats de l'évaluation, hiérarchiser les sources principales de données de référence les plus sensibles, définir une stratégie et une échéance pour les protéger et implémenter cette stratégie comme une solution pilote pour votre approche de la protection et la confidentialité des données.
3. Définir, documenter et distribuer les politiques de conformité à la confidentialité de votre entreprise et les principaux intervenants qui sont chargés de la conformité réglementaire en matière de confidentialité. Élaborer un plan stratégique pour cette année et pour les suivantes.

Plus de recherches

Pour en savoir plus sur les risques liés à la sécurité des données sensibles et les considérations relatives à la protection, consultez les publications et vidéos suivantes :

Informatica Data Privacy Management

Informatica Master Data Management – Customer 360

Livre Blanc : Protection intelligente de la vie privée

Bloor Research : Discovering Sensitive Data

Siège mondial Tour CB 21, 16 Place de l'Iris, 92040 Paris La Défense Cedex Tél : +33 01 42 04 89 00
Numéro gratuit aux États-Unis : 1.800.653.3871

IN09_0520_03409