Informatica

Livre Blanc

Sécurité centrée sur les données pour un monde hybride

Conformité du RGPD dans les environnements Cloud et sur site

À propos d'Informatica

La transformation digitale fait évoluer les attentes : service amélioré, livraisons plus rapides, à moindre coût.
Les données sont la clé de la réussite des entreprises, 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 quel que soit le secteur, la catégorie ou la niche. Les entreprises ont besoin de solutions de données pour le Cloud, les projets Big Data, le temps réel et les flux de données en continu. 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

Aujourd'hui, la plupart des entreprises stockent des données sensibles produits, clients et autres données importantes, sur des plates-formes et dans des lieux physiques dans le monde de plus en plus nombreux et divers. Ces données critiques pour l'entreprise sont souvent situées dans des applications logicielles en tant que service (SaaS), sur site et dans le Cloud public. Avec Informatica Intelligent Cloud Services™, par exemple, Informatica garantit la sécurité des infrastructures sous forme de datacenters de basculement, d'authentification des utilisateurs et de contrôle d'accès, de protocoles de sécurité réseau, de chiffrement et de couches de sécurité au niveau du système d'exploitation, de la base de données et des niveaux d'application.[1]

Les environnements hybrides posent de nouveaux défis aux équipes de conformité et de sécurité des données. La nature dynamique des données, utilisateurs et applications impose des actions supplémentaires pour s'assurer que les données critiques de l'entreprise sont suivies, comprises et protégées en permanence. Les risques ne sont pas hypothétiques, comme démontré dans les atteintes à la sécurité sur site et dans le Cloud de grande envergure, ainsi que par les amendes de nouvelles réglementations telles que RGPD (Règlement Général sur la Protection des Données).

Dans ces environnements hybrides dynamiques, vous avez besoin de l'intelligence et de l'automatisation pour assurer une protection et une conformité durables des données, tout en répondant aux questions suivantes :

- Où se trouve l'ensemble des données à protéger ?
- Qui accède aux données et avec quelles applications ?
- L'accès et l'utilisation actuels respectent-ils les règlements et les politiques d'utilisation des données ?
- Les protections des données sont-elles appropriées, et les risques liés aux données sont-ils à des niveaux acceptables ou existe-t-il des conditions créant plus de risques à corriger ?

La prise de décisions quant aux risques liés aux données, à la sécurité et la conformité dans un écosystème de données hybrides repose sur les résultats de la découverte et de la classification des données sensibles.

Ce document fournit un cadre de stratégies et de considérations de sécurité dans des environnements hybrides avec une approche centrée sur les données qui peut :

- Appliquer l'analyse, l'automatisation et l'intelligence artificielle (IA) afin d'identifier et de protéger les données sensibles de toutes les sources dans un environnement hybride, en utilisant une interface unique pour les tableaux de bord et les rapports.
- Respecter l'évolution de la gouvernance de données et des réglementations de sécurité.
- Fournir une préparation de l'audit.
- Alerter les principaux intervenants en cas de comportement anormal de l'utilisateur.

Informatica Data Masking et Informatica Secure@Source® offrent des capacités exceptionnelles pour exécuter ces fonctions, en ajoutant une couche de sécurité intégrée et axée sur les données pour toutes les sources de données sensibles dans un écosystème hybride.

[1] Monahan, David, « Informatica Cloud Security Architecture Overview », Enterprise Management Associates (EMA), mars 2016.

Sécurité des données pour votre réalité hybride

Selon l'entreprise d'études IDC, le monde prévoit de créer 180 zettaoctets de données en 2025, contre moins de 10 zettaoctets en 2015.[2] Les entreprises de tous les secteurs comptent sur la précision, la disponibilité et la sécurité de leurs données pour générer du chiffre d'affaires, servir les clients, augmenter la productivité et soutenir d'autres processus métiers critiques.

La croissance exponentielle continue du volume de données et de leur utilisation inclut également des données sensibles sur plusieurs silos, à la fois sur site et dans le Cloud, et dans une variété de formats de données. Par conséquent, les méthodes traditionnelles de sécurité des données sont devenues obsolètes. Les entreprises ont besoin d'une nouvelle approche de la sécurité des données.[3]

Il existe également une forte tendance selon laquelle un pourcentage important des données qu'une entreprise utilise provient de sources externes. Il est essentiel de comprendre la sensibilité de ces données au moment où elles sont intégrées dans l'entreprise et avant qu'elles se prolifèrent vers plusieurs systèmes et utilisations d'analyse. Cependant, la plupart des sociétés ne peuvent pas identifier avec précision où se trouvent toutes leurs données sensibles, en particulier si elles sont dans des formats non structurés ou si elles se trouvent sur plusieurs applications sur site et dans le Cloud, bases de données relationnelles, appliances de data warehouse et sources de données de Big Data. Ce manque de connaissances augmente le risque auquel une entreprise est exposée et, par conséquent, les atteintes à la sécurité des données représentent actuellement le principal risque de sécurité informatique.[4]

Avec la hausse des atteintes à la sécurité des données, associée à la prolifération des données sensibles, les entreprises doivent développer une stratégie d'atténuation des risques qui inclut un produit de sécurité centré sur les données, avec ces caractéristiques clés :

- Visibilité dans toutes les sources de données pour localiser et classer les données sensibles de toute l'entreprise.
- Capacité à implémenter des mécanismes de protection des données sensibles pour atténuer les atteintes.
- Conformité avec les réglementations sur la confidentialité et la sécurité des données actuelles, y compris l'utilisation de l'automatisation et de l'IA pour surveiller le comportement des utilisateurs et signaler les anomalies en temps quasi réel.
- Outils de visualisation d'analyse enrichie pour la gestion de données sensibles.
- Capacités de produire des fonctionnalités de rapport transparentes et robustes pour la préparation de l'audit.

Gartner prédit que d'ici 2020, les produits de vérification et de protection des données remplaceront les outils de sécurité des données cloisonnés disparates dans 40 % des grandes entreprises, contre moins de 5 % aujourd'hui.[5] Ces solutions de protection axées sur les données, y compris Informatica Data Masking and Informatica Secure@Source, offrent une vue centralisée des données à risque, de sorte que tous les intervenants clés d'une entreprise puissent suivre les mouvements des données sensibles et appliquer des mécanismes de protection tel que requis par les politiques et réglementations de gouvernance.

2 « 2016 IoT Midyear Review – The Report Card for Everyone », IDC, 4 août 2016.
3 « Market Guide for Data-Centric Audit and Protection », Gartner, 21 mars 2017.
4 « Data Breaches and Sensitive Data Risk », Ponemon Institute, février 2016.
5 « Market Guide for Data-Centric Audit and Protection », Gartner, 21 mars 2017.

Stratégie à quatre étapes pour la protection des données sensibles

« Risque de données sensibles » est l'impact de la perte de données sensibles, et la principale cause de cette perte est une atteinte à la sécurité des données. Localiser simplement les données sensibles suffit à remédier aux risques, et représente une idée reçue courante. Toutefois, la localisation et la classification de ces données n'est que la première étape d'une stratégie globale d'atténuation des risques.

Les étapes suivantes impliquent l'évaluation des risques de l'entreprise sur la base des résultats de l'emplacement et de l'analyse de classification, ainsi que l'élaboration d'une stratégie de réduction des risques qui implique tous les intervenants clés — pas seulement le service informatique — avec les contrôles automatisés qui mettent en application les politiques de gouvernance de données. Votre stratégie doit également inclure l'acquisition et l'implémentation d'un produit de sécurité robuste et axé sur les données, qui améliore les capacités de conformité réglementaire, les visualisations d'analyses enrichies des données sensibles pour les tableaux de bord et les rapports d'audit, ainsi que la protection de tous les types de données sensibles à travers l'entreprise. Le produit de sécurité axé sur les données choisi doit également protéger les données sensibles de toutes les sources dans votre environnement hybride : Cloud public, applications SaaS, applications et bases de données sur site, données non structurées et appliances de data warehouse.

1. Découverte et classification

Une approche courante de la découverte consiste à examiner les sources existantes et envoyer des questionnaires. Cependant, cette approche hautement manuelle est inadéquate car elle monopolise du temps et des ressources précieuses. Par ailleurs, elle est souvent inexacte et obsolète, et repose sur l'auto-reporting plutôt que sur la surveillance réelle du comportement de l'utilisateur.

Les entreprises doivent se demander :

- Quelles données stockent-elles, qui a accès à quoi et à quelles fins ?
- Comment gérer les privilèges d'un utilisateur et les droits des données ?
- Comment protégerons-nous les données 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 votre paysage de données (y compris les bases de données, les applications et les données non structurées sur site et dans le Cloud).
- La construction d'un plan pour gérer les données provenant de sources externes.
- Le mappage des systèmes qui contiennent des données sensibles.
- La fourniture d'une solution qui peut mapper le mouvement des données à travers votre 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 et la sécurité 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 à compter du 25 mai 2018, a été adopté dans l'intention de renforcer et d'unifier la protection des données pour toutes les personnes au sein de l'Union européenne, ce qui simplifie l'environnement réglementaire des activités internationales. De nombreuses entreprises ne sont pas encore prêtes pour cette réglementation, et ne seront pas suffisamment conformes. Par ailleurs, 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 sécurité et de confidentialité des données sensibles, tout en dirigeant également les résultats de la transformation numérique pilotée par les données.

Les entreprises doivent élaborer des politiques intelligentes qui permettent d'identifier les magasins de données qui contiennent des « domaines de données » qui s'appliquent à RGPD. Ces politiques sont multifactorielles, avec une logique qui détermine quelles combinaisons posent une menace de confidentialité.

3. Protection

En 2017, 1 120 cas d'atteintes à la sécurité des données ont été recensés avec près de 171 millions d'enregistrements exposés.[6] Malgré d'importants investissements dans la sécurité au niveau de l'infrastructure, les données critiques restent clairement vulnérables. Les entreprises doivent sécuriser en permanence les données à haut risque, identifier les comportements suspects et l'utilisation non autorisée ou la circulation des données critiques, et automatiser et orchestrer la correction.

Les entreprises devraient identifier les risques critiques et les corriger avec des contrôles axés sur les données (plutôt que des outils classiques de cybersécurité). Par exemple, ces contrôles comprennent des solutions de masquage et de chiffrement des données. En outre, les entreprises doivent surveiller l'accès des utilisateurs et leur comportement. L'accès à un trop grand nombre de données ou un comportement inhabituel peut indiquer que les utilisateurs ne se conforment pas aux politiques de confidentialité ou que leurs identifiants ont été volés.

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 devraient être en mesure de répondre immédiatement aux auditeurs et fournir la preuve qu'elles savent où sont les données, quels sont les risques auxquels elles sont exposées, comment elles sont protégées et comment elles sont utilisées. Elles devraient prendre en compte le fait que les auditeurs souhaiteront des rapports et des visualisations extraits pour les services ou les emplacements, et permettant d'explorer en profondeur les domaines de données spécifiques.

[6] « 2016 Data Breach Category Summary », Identity Theft Resource Center, 31 décembre 2016.

Conclusion

Les protocoles de sécurité de l'infrastructure de haut niveau sont indispensables pour protéger tout environnement hybride qui transmet des données confidentielles aux utilisateurs, aux serveurs de datacenter à travers le globe et à travers les applications Cloud. L'assaut continu des atteintes à la sécurité des données et les exigences de conformité de plus en plus nombreuses indiquent que les entreprises doivent implémenter des processus et des outils adéquats pour identifier, analyser et protéger les données sensibles.

Dans le climat actuel d'intensification du risque pour la sécurité et des atteintes régulières à la sécurité des données, les sociétés doivent élaborer une stratégie de sécurité numérique robuste pour surveiller et analyser en permanence les risques pour leurs données sensibles. Elles doivent surveiller les données en temps quasi réel, à la recherche de signaux d'abus ou d'atteintes, d'accès excessif, de comportement inhabituel ou de transferts transfrontaliers. Les solutions de sécurité axées sur les données telles qu'Informatica Data Masking et Informatica Secure@Source permettent aux entreprises d'améliorer leur exposition aux risques liés aux données, afin d'atténuer l'impact des atteintes à la sécurité ou de la mauvaise utilisation en interne et répondre aux exigences rigoureuses des réglementations régionales et de l'industrie.

Recommandations

1. Effectuer une évaluation des risques pour mieux comprendre où se trouvent vos données sensibles, la portée de leur propagation sur votre écosystème de données et quels ensembles de données sensibles sont les plus vulnérables.
2. En fonction des résultats de votre évaluation, hiérarchiser les 10 sources principales de données les plus sensibles de votre entreprise, déterminer une stratégie et un produit pour la protéger et implémentez la stratégie de sécurité des données.
3. Définir, documenter et distribuer les politiques de conformité de votre entreprise et les principaux intervenants qui sont responsables de la conformité du RGPD. Construire un plan stratégique pour mai 2018 et au-delà.

Pour plus d'informations

Pour plus d'informations sur les risques liés à la sécurité des données sensibles et les considérations relatives à la protection, consultez les publications suivantes :

- « Detect and Protect: A Data-Centric Approach to Security », Informatica, avril 2017.
- « Data Breaches and Sensitive Data Risk », Ponemon Institute, février 2016.

Informatica

Siège mondial 2100 Seaport Blvd., Redwood City, CA 94063, États-Unis Téléphone : +33 1 42 04 89 00 (France), numéro gratuit aux États-Unis : 1.800.653.3871

IN09_0418_03429