Informatica

white paper

Mitigando o risco à privacidade de dados para o gerenciamento de dados mestres

Sobre a Informatica

A transformação digital muda expectativas: melhor serviço, entrega mais rápida e com menos custos. As empresas devem mudar para continuar competitivas, e a solução está nos dados.

Como líder mundial em gerenciamento de dados corporativos na nuvem, estamos preparados para ajudar você a ocupar de maneira inteligente uma posição de liderança — em qualquer setor, categoria ou nicho. A Informatica oferece a perspectiva para que você se torne mais ágil, aproveite novas oportunidades de crescimento ou invente coisas novas. Estamos 100% focados em todos os tipos de dados para oferecer a versatilidade de que você precisa para prosperar.

Convidamos você a explorar tudo o que a Informatica tem a oferecer — e estimular o poder dos dados para impulsionar sua próxima revolução com inteligência.

Índice

Resumo executivo

As organizações investem em iniciativas de gerenciamento de dados mestres (Master Data Management, MDM) para criar uma visão confiável e precisa do cliente, produto e serviço, informações operacionais e outras informações empresariais essenciais para os negócios. O MDM combina elementos de dados essenciais em toda a empresa em registros consolidados para criar dados confiáveis para serem compartilhados com as pessoas e os aplicativos que necessitam deles. Isso tem um enorme valor para qualquer empresa que queira criar mais ofertas com foco no cliente; melhorar o atendimento ao cliente e programas de fidelidade; gerar eficiência no gerenciamento de produtos e soluções; migrar para a nuvem com segurança; e assim por diante.

Os dados confiáveis tornam-se a maior riqueza das iniciativas de clientes e produtos da organização, e fornecem vantagem competitiva. No entanto, a consolidação de dados sensíveis também fornece um alvo atraente para ataques externos, resultando em violações da segurança dos dados e aumentando possíveis abusos internos, portanto, está sujeita a regulamentos de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Privacidade do Consumidor da Califórnia (CCPA), entre outros.

Surgem questões naturais de proteção de dados e conformidade para esses ambientes:

- Onde estão localizados todos os dados e como eles proliferam?
- O que está alimentando o repositório, quem está acessando dados e com quais aplicativos?
- O acesso e uso atuais estão de acordo com as regulamentações e políticas de uso de dados aprovadas?
- As proteções de dados são apropriadas e o risco de dados permanece em níveis aceitáveis ou há condições que criam riscos inapropriados que deveriam ser remediados?

Os resultados da descoberta e classificação de dados sensíveis do cliente tornam-se a base do suporte à decisão em relação ao risco, à proteção e à conformidade regulatória de privacidade dos dados mestres.

Este white paper fornece uma estrutura de considerações e estratégias para reduzir riscos com uma solução centrada em dados que:

- aplica análises, inteligência orientada por metadados, automação e IA para identificar e proteger dados mestres sensíveis
- cumpre os regulamentos de governança e privacidade de dados em evolução
- fornece prontidão de auditoria para atestar os controles em vigor, e
- alerta as partes interessadas quando ocorre um comportamento anormal do usuário, exigindo investigação

Apresentação

De acordo com a empresa de pesquisa IDC, estima-se que sejam criados 175 zettabytes de dados em 2025, contra 33 zettabytes em 2018.[1] Organizações de todos os setores confiam na precisão, disponibilidade e proteção de seus dados para gerar receita, atender clientes, aumentar a produtividade, otimizar operações e conduzir outros processos de negócios de missão crítica.

O crescimento exponencial contínuo do volume e uso de dados também inclui dados mestres confidenciais em vários silos, tanto locais quanto na nuvem, e em vários formatos de dados. Essas condições tornaram obsoletos os métodos tradicionais de segurança,[2] exigindo uma nova abordagem da segurança de dados em toda a organização.

No entanto, a maioria das empresas não consegue identificar com precisão onde estão localizados todos os dados mestres sensíveis, principalmente se estiverem em formatos não estruturados. Essa falta de visibilidade aumenta o risco de uma organização e, por isso, a violação de dados permanece sendo um dos principais riscos de segurança de TI.[3]

Com as violações de segurança de dados em ascensão, junto com a proliferação de dados mestres sensíveis usados de forma inadequada, as organizações devem desenvolver uma estratégia de mitigação de riscos que inclua uma solução de privacidade centrada em dados com os seguintes principais recursos:

- visibilidade em todas as fontes de dados para descobrir e classificar dados mestres sensíveis localizados na organização
- capacidade de implementar mecanismos de proteção de dados mestres sensíveis para mitigar violações de segurança de dados
- conformidade com os regulamentos atuais de privacidade, incluindo o uso de inteligência orientada por dados, automação e IA para monitorar o comportamento do usuário e alertar sobre anormalidades quase em tempo real
- ferramentas de visualização analítica completas para avaliação de riscos e gerenciamento de dados sensíveis
- recursos de relatório transparentes e abrangentes para demonstrar controles com prontidão para auditoria

A Gartner prevê que os produtos de proteção integrada substituirão as diferentes ferramentas de segurança de dados em silos em 40% das grandes empresas, em comparação aos menos de 5%.[4] Essas soluções de proteção com foco em dados fornecem uma visão centralizada dos dados em risco, para que as principais partes interessadas em uma organização global possam rastrear a movimentação de dados sensíveis e aplicar mecanismos de proteção, conforme exigido pelas políticas e regulamentos de governança.

Uma estratégia de quatro pontos para mitigar os riscos à privacidade de dados sensíveis

O risco à privacidade de dados sensíveis é o impacto da perda de dados sensíveis com exposição inadequada, e a causa mais comum é a violação de dados ou o uso indevido de informações privilegiadas. Um equívoco comum é pensar que simplesmente localizar dados mestres confidenciais é o suficiente para remediar o risco. Localizar e classificar esses dados é apenas o primeiro passo de uma estratégia abrangente de remediação de riscos.

[1] White Paper da IDC, "The Digitization of the World – From Edge to Core" (Novembro de 2018).
[2] Gartner, "Market Guide for Data-Centric Audit and Protection", 21 de março de 2017.
[3] Ponemon Institute LLC, "Data Breaches and Sensitive Data Risk", fevereiro de 2016.
[4] Gartner, "Market Guide for Data-Centric Audit and Protection", 21 de março de 2017.

As próximas etapas envolvem avaliar as prioridades de risco da organização a serem abordadas, com base nos resultados da análise de localização e classificação. Você precisa determinar uma estratégia para reduzir os principais riscos – com controles automatizados que aplicam políticas de governança de dados e envolvem as principais partes interessadas – não apenas a TI. Sua estratégia deve incluir a implementação de uma solução confiável de privacidade e proteção centrada em dados que ofereça recursos para conformidade regulatória, incluindo ricas visualizações analíticas de dados sensíveis para painéis de visibilidade de risco e relatórios de auditoria de controles de conformidade; e proteção para todos os tipos de dados mestres sensíveis em toda a organização.

1. Descoberta e classificação

Uma abordagem ad hoc comum para a descoberta é revisar as fontes existentes e enviar questionários. No entanto, uma abordagem manual é inadequada porque consome tempo e recursos valiosos, e geralmente é imprecisa e se torna desatualizada rapidamente, com dependência de autorrelatórios em vez de monitoramento real em tempo real do comportamento do usuário e fluxo de dados.

As organizações precisam se perguntar:

- Quais dados você armazena, quem tem acesso a eles e com quais objetivos?
- Como você gerencia privilégios de usuários e fornece direitos de dados?
- Como você protegerá dados mestres sensíveis e garantirá que os controles apropriados estejam em vigor?

Outras considerações de conformidade de descoberta e classificação incluem:

- Definir e entender seu cenário de dados, incluindo bancos de dados e dados não estruturados
- Mapear quais sistemas contêm dados mestres sensíveis e mapear dados para identidades
- Adquirir uma solução que possa mapear o movimento dos dados em todo o ecossistema, mantendo uma exibição próxima ao tempo real com ferramentas de análise e relatórios

2. Conformidade

As organizações realizam grandes esforços para identificar, monitorar e remediar riscos de dados e cumprir os regulamentos de privacidade de dados. Além disso, devem monitorar, analisar e alertar sobre o acesso ou movimentação de dados que possam comprometer a conformidade.

O GDPR, em vigor a partir de 25 de maio de 2018, foi adotado com a intenção de fortalecer e unificar a proteção de dados para todos os indivíduos dentro da União Europeia, simplificando assim o ambiente regulatório para negócios internacionais. Da mesma forma, a CCPA, que entrou em vigor em 1º de janeiro de 2020, eleva o nível, ampliando a privacidade para incluir dados domésticos.

Muitas empresas ainda não se prepararam totalmente para nenhum dos regulamentos e não estão em conformidade de maneira suficiente, o que pode resultar em multas significativas e danos à reputação. Por outro lado, a conformidade pode oferecer a oportunidade de vantagem competitiva como um diferencial de privacidade de dados mestres para aumentar a fidelidade do cliente e, ao mesmo tempo, impulsionar resultados de transformação digital. Além disso, as empresas que demonstram diligência ao proteger os dados podem obter 5 vezes mais acesso às informações pessoais de clientes que confiam nelas para administrá-las de forma responsável.[5]

[5] Trecho, Boston Consulting Group, "Bridging the Trust Gap in Personal Data"

As organizações precisam desenvolver políticas inteligentes que identifiquem armazenamentos de dados que contenham GDPR, CCPA e "domínios de dados" de privacidade relevantes obrigatórios semelhantes Essas políticas são multifatoriais, com lógica de inteligência de dados que determina quais combinações representam uma ameaça de exposição ao risco de privacidade.

3. Proteção

No terceiro bimestre de 2019, houve mais de 5.000 violações de dados, com quase 8 bilhões de registros expostos.[6] Claramente, apesar de grandes investimentos em privacidade e segurança de dados, dados pessoais críticos permanecem vulneráveis. As organizações precisam proteger dados de alto risco de forma contínua; identificar comportamento suspeito e uso ou movimento não autorizado, enquanto automatizam e planejam a correção.

As organizações devem priorizar os riscos de dados mais críticos e remediá-los com controles centrados em dados que suportem a mobilidade de dados, em vez de depender de controles históricos de acesso ao servidor, firewalls e ferramentas semelhantes de segurança cibernética com foco no sistema. Por exemplo, controles com foco em dados incluem mascaramento, controles baseados em identidade e criptografia.

Além dos controles de privacidade de dados, as organizações devem monitorar o acesso e o comportamento dos dados baseados em identidade. O acesso excessivo ou comportamento incomum podem indicar que os usuários não estão aderindo às políticas de privacidade ou que suas credenciais de usuário foram comprometidas.

4. Prontidão e resposta à auditoria

As empresas estão passando por mais auditorias e avaliações de dados confidenciais do que nunca. Elas empenham grandes esforços para fornecer provas aos auditores de que têm visibilidade e proteção de dados críticos.

As organizações devem ser capazes de responder imediatamente aos auditores e fornecer evidências de que sabem onde existem dados, quais são seus riscos, como são protegidos e estão sendo usados. Também, devem considerar que os auditores desejarão relatórios e visualizações que sejam extraídas de departamentos ou locais e que forneçam a possibilidade de busca detalhada de domínios de dados específicos.

Conclusão

O poder do MDM pode ajudar as organizações a transformar suas operações e serviços. O poder desses dados é claro, mas também representa um alvo tentador para o seu mau uso por parte de atores internos ou externos. Devido às contínuas investidas de violações de dados e os crescentes requisitos de conformidade, as organizações devem repensar seus processos e ferramentas para identificar, analisar e proteger dados confidenciais.

No clima atual de elevado risco à privacidade e violações rotineiras de dados, as empresas precisam desenvolver uma estratégia digital robusta para monitorar, analisar e corrigir de forma contínua o risco dos dados mestre sensíveis. Elas precisam monitorar os dados quase em tempo real quanto a sinais de uso indevido ou violação da segurança dos dados, acesso e comportamento incomuns ou transferências transfronteiriças inadequadas. Com essa diligência, as organizações podem aproveitar o MDM e melhorar sua postura de risco de dados para ajudar a reduzir o impacto de violações de dados ou o mau uso interno e atender aos rigorosos regulamentos regionais e do setor.

[6] Relatório QuickView de violação de dados do terceiro trimestre de 2019 de segurança baseada em risco

Recomendações

1. Realize uma avaliação de risco de privacidade de dados para obter um entendimento claro de onde estão localizados os dados mestres sensíveis, até que ponto eles proliferam no seu ecossistema de dados, e quais conjuntos de dados sensíveis são mais vulneráveis à correção.
2. Com base nos resultados da avaliação, priorize as principais fontes de dados mestres mais sensíveis da organização; determine uma estratégia e cronograma para protegê-los; e implemente essa estratégia como uma solução piloto para sua abordagem à proteção e à privacidade dos dados.
3. Defina, documente e distribua as políticas de conformidade de privacidade da organização e as principais partes interessadas que são responsáveis pela conformidade regulatória com a privacidade. Elabore um plano estratégico para este ano e para os próximos.

Pesquisa adicional

Para obter mais informações sobre riscos de segurança de dados confidenciais e considerações de proteção, consulte as seguintes publicações:

Informatica Data Privacy Management

Informatica Master Data Management – Customer 360

White Paper: Intelligent Data Privacy

Bloor Research: Descobrindo dados sensíveis

Sede mundial Av. Das Nações Unidas, 12901 - 3º, Andar - Torre Norte - Brooklin Novo, 04578-000 - São Paulo, SP Tel.: 0800-878-3060
Ligação gratuita nos EUA: 1.800.653.3871

IN09_0520_03409