Informatica

White Paper

Segurança centrada em dados para um mundo híbrido

Conformidade com GDPR em ambientes locais e na nuvem

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 corporativo de dados em nuvem, estamos preparados para ajudar você a assumir a liderança de qualquer setor, categoria ou nicho de maneira inteligente. 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 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

Atualmente, a maioria das organizações armazena dados confidenciais de clientes, produtos e outros dados essenciais em um número e variedade cada vez maior de plataformas e locais físicos no mundo inteiro. Esses dados críticos para os negócios geralmente estão localizados em aplicativos locais, de nuvem pública e de SaaS (Software as a Service, Software como Serviço). Com o Intelligent Cloud Services™, por exemplo, a Informatica fornece segurança de infraestrutura na forma de data centers de failover, autenticação de usuário e controle de acesso, protocolos de segurança de rede, criptografia e camadas de segurança nos níveis de sistema operacional, banco de dados e aplicativo.[1]

Ambientes híbridos fornecem novos desafios para equipes de conformidade e segurança de dados. A natureza dinâmica de dados, usuários e aplicativos exige medidas adicionais para garantir que os dados críticos da organização sejam rastreados, entendidos e protegidos sempre. Conforme demonstrado nas violações locais e de nuvem de alto perfil e pelas multas das novas regulamentações, como a GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados), os riscos não são hipotéticos.

Nesses ambientes híbridos dinâmicos, você precisa da inteligência e da automação para garantir proteção e conformidade de dados sustentadas, com a capacidade de responder perguntas como as seguintes:

- Onde estão todos os dados que precisam ser protegidos?
- Quem está acessando dados com quais aplicativos?
- O acesso e uso atual estão de acordo com as regulamentações e políticas de uso de dados?
- As proteções de dados são apropriadas e o risco de dados permanece em níveis aceitáveis ou há condições criando mais riscos que devemos remediar?

Os resultados da descoberta e classificação de dados confidenciais tornam-se a base para o apoio à decisão em relação ao risco, segurança e conformidade de dados em um ecossistema de dados híbrido.

Este documento fornece uma estrutura de considerações e estratégias de segurança em ambientes híbridos com uma abordagem centrada em dados que pode:

- Aplicar analytics, automação e AI (Artificial Intelligence, Inteligência Artificial) para identificar e proteger dados confidenciais de todas as origens em um ambiente híbrido, usando uma única interface para painéis e relatórios.
- Cumprir as regulamentações de governança e segurança de dados em evolução.
- Fornecer prontidão de auditoria
- Alertar as principais partes interessadas quando ocorrer um comportamento anormal do usuário.

O Data Masking e o Secure@Source® da Informatica fornecem recursos excepcionais para executar essas funções, adicionando uma camada de segurança integrada e centrada em dados para todas as fontes de dados confidenciais em um ecossistema híbrido.

[1] Monahan, David, "Informatica Cloud Security Architecture Overview", Enterprise Management Associates (EMA), March 2016.

Segurança de dados para sua realidade híbrida

De acordo com a empresa de pesquisa IDC, estima-se que o mundo crie 180 zettabytes de dados em 2025, diante os menos de 10 zettabytes em 2015.[2] Organizações de todos os setores confiam na precisão, disponibilidade e segurança de seus dados para gerar receita, atender clientes, aumentar a produtividade e oferecer suporte a outros processos de negócios de missão crítica.

O crescimento exponencial contínuo do volume e uso de dados também inclui dados confidenciais em vários silos, tanto locais quanto na nuvem, e em vários formatos de dados. Essas condições tornaram obsoletos os métodos tradicionais de segurança, exigindo uma nova abordagem da segurança de dados em toda a organização.[3]

Há também uma forte tendência de que grande porcentagem dos dados que uma organização usa tem origens externas. É fundamental entender a confidencialidade desses dados no momento em que eles são incorporados à organização e antes de serem propagados para vários sistemas e usos analíticos. No entanto, a maioria das empresas não consegue identificar com precisão onde estão localizados todos os dados confidenciais, principalmente se estiverem em formatos não estruturados ou em vários aplicativos locais e na nuvem, bancos de dados relacionais, dispositivos de data warehouse e grandes fontes de dados. Essa falta de conhecimento aumenta o risco de uma organização e, por essas razões, as violações de dados são atualmente o principal risco de segurança de TI.[4]

Com as violações de dados em ascensão, em conjunto com a propagação de dados confidenciais, as organizações devem desenvolver uma estratégia de mitigação de riscos que inclua um produto de segurança centrado em dados com esses principais recursos:

- Visibilidade em todas as fontes de dados para localizar e classificar dados confidenciais de toda a organização.
- Capacidade de implementar mecanismos de proteção de dados confidenciais para mitigar violações.
- Conformidade com os regulamentos atuais de segurança e privacidade de dados, incluindo o uso de automação e AI para monitorar o comportamento do usuário e relatar anormalidades de maneira próxima ao tempo real.
- Ferramentas de visualização analítica completas para gerenciamento de dados confidenciais.
- Recursos de relatórios transparentes e robustos para prontidão de auditoria.

O Gartner prevê que até 2020, produtos de proteção e auditoria centrados em dados substituirão diferentes ferramentas de segurança de dados em silos em 40% das grandes empresas, diante os menos de 5% atuais.[5] Essas soluções de proteção centradas em dados, incluindo o Data Masking e o Secure@Source da Informatica, fornecem uma visão centralizada dos dados em risco para que todos os principais interessados em uma organização possam rastrear a movimentação de dados confidenciais e aplicar mecanismos de proteção conforme exigido pelas políticas de governança e regulamentações.

[2] "2016 IoT Midyear Review – The Report Card for Everyone", IDC, August 4, 2016.
[3] "Market Guide for Data-Centric Audit and Protection", Gartner, March 21, 2017.
[4] "Data Breaches and Sensitive Data Risk", Ponemon Institute, February 2016.
[5] "Market Guide for Data-Centric Audit and Protection", Gartner, March 21, 2017.

Estratégia de quatro pontos para proteger dados confidenciais

O "risco dos dados confidenciais" é o impacto da perda de dados confidenciais, e a principal causa dessa perda é a violação de dados. Um equívoco comum é pensar que simplesmente localizar dados 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.

As próximas etapas envolvem avaliar o risco da sua organização com base nos resultados da análise de localização e classificação, e determinar uma estratégia para reduzir o risco que envolva todas as principais partes interessadas — não apenas a organização de TI — com controles automatizados que reforcem as políticas de controle de dados. Sua estratégia também deve incluir a aquisição e implementação de um produto de segurança robusto e centrado em dados que ofereça recursos para conformidade com as regulamentações, visualizações analíticas completas de dados confidenciais para painéis e relatórios de auditoria e proteção para todos os tipos de dados confidenciais em toda a organização. O produto de segurança centrado em dados escolhido também deve proteger dados confidenciais de todas as origens em seu ambiente híbrido: nuvem pública, aplicativos SaaS, aplicativos e bancos de dados locais, dados não estruturados e dispositivos de data warehouse.

1. Descoberta e classificação

Uma abordagem comum para a descoberta é revisar origens existentes e enviar questionários. No entanto, essa abordagem altamente manual é inadequada porque consome tempo e recursos valiosos e, muitas vezes, é imprecisa e desatualizada, confia mais no autorrelato do que no monitoramento real do comportamento do usuário.

As organizações precisam se perguntar:

- Quais dados armazenamos, quem tem acesso a eles e com quais objetivos?
- Como gerenciamos privilégios de usuários e direitos de dados?
- Como protegeremos os dados confidenciais e garantiremos 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 locais e na nuvem, aplicativos e dados não estruturados).
- Criar um plano para gerenciar dados de origem externa.
- Mapear quais sistemas contêm dados confidenciais.
- Adquirir uma solução que possa mapear o movimento dos dados em todo o ecossistema, mantendo uma visualização 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 as normas de privacidade e segurança 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. Muitas empresas ainda não se prepararam para esse regulamento e não estarão em conformidade de maneira adequada. Apesar disso, a não conformidade pode resultar em multas e danos à reputação significativos. Por outro lado, a conformidade pode oferecer a oportunidade da vantagem competitiva como um diferencial em privacidade e segurança de dados confidenciais, ao mesmo tempo em que impulsiona os resultados de transformação digital orientados por dados.

As organizações precisam desenvolver políticas inteligentes que identifiquem armazenamentos de dados que contenham "domínios de dados" relevantes para GDPR. Essas políticas são multifatoriais, com lógica que determina quais combinações representam uma ameaça à privacidade.

3. Proteção

Em 2017, houve 1.120 violações de dados, com um total de quase 171 milhões de registros expostos.[6] Claramente, apesar dos grandes investimentos em segurança em nível de infraestrutura, os dados críticos permanecem vulneráveis. As organizações precisam proteger continuamente dados de alto risco, identificar comportamentos suspeitos e uso ou movimentação não autorizados de ativos de dados críticos e automatizar e orquestrar a remediação.

As organizações devem identificar riscos críticos de dados e remediá-los com controles centrados em dados (em vez de ferramentas clássicas de segurança cibernética). Por exemplo, esses controles incluem soluções de mascaramento e criptografia de dados. Além disso, as organizações devem monitorar o acesso e o comportamento do usuário. O acesso excessivo a dados ou comportamento incomum podem indicar que os usuários não estão aderindo às políticas de privacidade ou que suas credenciais foram roubadas.

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.

[6] "2016 Data Breach Category Summary", Identity Theft Resource Center, December 31, 2016.

Conclusão

Protocolos de segurança de infraestrutura de alto nível são necessários para proteger qualquer ambiente híbrido que transmita dados confidenciais para usuários, servidores de data center em todo o mundo e para aplicativos em nuvem. As contínuas investidas de violações de dados e os crescentes requisitos de conformidade indicam que as organizações devem implementar processos e ferramentas adequadas para identificar, analisar e proteger dados confidenciais.

No atual clima de maior risco de segurança e violações frequentes de dados, as empresas precisam desenvolver uma estratégia robusta de segurança digital para monitorar, analisar e remediar continuamente os riscos relacionados aos seus dados confidenciais. Precisam monitorar os dados de maneira próxima ao tempo real quanto a sinais de uso indevido ou violação, acesso excessivo, comportamento incomum ou transferências internacionais. Com soluções de segurança centradas em dados, como o Data Masking e o Secure@Source da Informatica, as organizações podem 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.

Recomendações

1. Realize uma avaliação de risco para obter um entendimento claro de onde seus dados confidenciais estão localizados, em que extensão são propagados por meio do ecossistema de dados e quais conjuntos de dados confidenciais são mais vulneráveis.
2. Com base nos resultados de sua avaliação, priorize as dez principais origens dos dados mais críticos da sua organização; determine uma estratégia e um produto para protegê-los; e implemente a estratégia de segurança de dados.
3. Defina, documente e distribua as políticas de conformidade da sua organização e as principais partes interessadas que são responsáveis pela conformidade com o GDPR. Construa um plano estratégico para a partir de maio de 2018.

Mais informações

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

- "Detect and Protect: A Data-Centric Approach to Security", Informatica, April 2017.
- "Data Breaches and Sensitive Data Risk", Ponemon Institute, February 2016.

Informatica

Sede no Brasil 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_0418_03429