Superando desafios de segurança de dados em um mundo híbrido e multinuvem

Proteja seus dados onde quer que estejam com a plataforma de segurança de dados IBM Security Guardium

IBM **Security**

IBM

Sumário

Implementando em um ambiente híbrido e multinuvem

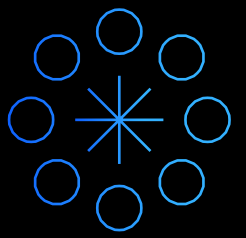
Sejamos sinceros: a computação em nuvem está evoluindo rapidamente. Hoje, existem muitas opções para migrar aplicações e dados para a nuvem. Elas incluem vários modelos de implementação, como os tipos de serviço de nuvem pública, privada e híbrida.

Como parte de uma estratégia digital mais ampla, as organizações estão buscando maneiras de utilizar diversas nuvens. Com uma abordagem multinuvem, elas podem evitar ficarem presas a um fornecedor e se beneficiarem das melhores tecnologias, como a inteligência artificial (IA) e o blockchain. Os benefícios para os negócios são claros: maior flexibilidade e agilidade, custos mais baixos e menor tempo de entrada no mercado.

De acordo com uma pesquisa feita pelo IBM Institute for Business Value com 1.106 executivos de negócios e tecnologia, até 2021, 85% das organizações já estarão utilizando ambientes em multinuvem. Noventa e oito por cento planejam usar várias nuvens híbridas até 2021. Entretanto, apenas 41% têm uma estratégia de gerenciamento de multinuvem em vigor.[1]

No que diz respeito a escolher as soluções de nuvem, há uma infinidade de opções disponíveis. É importante analisar as diferenças entre os vários tipos de modelos de implementação de nuvem e serviço de nuvem.

85%
das organizações já estão utilizando ambientes em multinuvem.[1]



98%
das organizações planejam usar diversas nuvens híbridas até 2021.[1]

Entendendo os modelos de implementação de nuvem

Na última década, a computação em nuvem amadureceu de várias maneiras e se tornou uma ferramenta para a transformação digital no mundo todo. Em geral, as nuvens usam um dentre os três modelos de implementação: pública, privada ou híbrida.

Nuvem pública
Em uma nuvem pública, os serviços são prestados por meio da internet pública. O provedor de nuvem possui, gerencia e mantém a infraestrutura, de forma integral, e a aluga para clientes com base em uso ou assinatura periódica. Os exemplos incluem Amazon Web Services (AWS) e Microsoft Azure.

Nuvem privada
Em um modelo de nuvem privada, a infraestrutura da nuvem e os recursos são implementados localmente
para uma única organização, podendo ser gerenciados internamente ou por terceiros.

Com nuvens privadas, as organizações controlam todo o conjunto de softwares, assim como a plataforma subjacente, da infraestrutura de hardware às ferramentas de mensuração.

Nuvem híbrida
Ela oferece o melhor dos dois mundos. Uma infraestrutura de nuvem híbrida conecta a nuvem privada de uma empresa e a nuvem pública de terceiros em uma única infraestrutura para que a empresa possa executar suas aplicações e cargas de trabalho.

Usando o modelo de nuvem híbrida, as organizações podem executar cargas de trabalho sensíveis e altamente reguladas em uma infraestrutura de nuvem privada e executar as cargas de trabalho menos sensíveis e temporárias na nuvem pública. No entanto, a migração de aplicações e dados para a nuvem, fora dos firewalls, os expõe a riscos.

Devem existir controles de segurança e proteção de dados para proteger os dados, estejam eles em uma nuvem privada ou em um ambiente híbrido, e para cumprir os requisitos de conformidade do governo e do setor.

Estima-se que o mercado de nuvem híbrida representa uma **oportunidade de US$ 1,2 trilhão**.[2]

Mas permanecem as preocupações com a proteção e a conformidade dos dados.

O custo da violação de dados está subindo.

Em média, as empresas levam **279 dias** para detectar e conter uma violação de dados.[3]

Tipos de modelos de serviço de nuvem

A segurança de dados varia com base no modelo de serviço de nuvem usado. Existem quatro categorias principais de modelos de serviço de nuvem: infraestrutura como serviço (IaaS), plataforma como serviço (PaaS), software como serviço (SaaS) e banco de dados como serviço (DBaaS), que é uma variante da PaaS.

A IaaS permite que as organizações mantenham as plataformas físicas existentes de software e middleware, com as aplicações de negócios na infraestrutura fornecida e gerenciada pelo provedor de serviços. Essa abordagem é benéfica para as organizações quando elas desejam beneficiar-se rapidamente da nuvem e, ao mesmo tempo, minimizar o impacto e usar os investimentos existentes.

A PaaS permite que as empresas usem a infraestrutura, assim como o middleware ou o software fornecido e gerenciado pelo provedor de serviços. Essa flexibilidade remove um fardo significativo de uma empresa pela perspectiva de TI e permite que ela se concentre no desenvolvimento de aplicações de negócios inovadoras.

As soluções de DBaaS são ambientes de bancos de dados hospedados e totalmente gerenciados por um provedor de nuvem. Uma empresa pode, por exemplo, assinar o Amazon RDS for MySQL ou o Microsoft Azure SQL Database.

O SaaS é um modelo de serviço que terceiriza toda a TI e permite que as organizações se concentrem mais em seus principais pontos fortes, em vez de dedicar tempo e investimento à tecnologia. Ele oferece SaaS aos usuários finais. Nesse modelo de serviço de nuvem, um provedor de serviços hospeda as aplicações e as disponibiliza para as organizações.

Com cada etapa, de IaaS a PaaS, SaaS e DBaaS, as organizações abrem mão de certo nível de controle dos sistemas que armazenam, gerenciam, distribuem e protegem seus dados sensíveis. Esse aumento da confiança depositada em terceiros também oferece maior risco para a segurança de dados.

Independentemente da arquitetura escolhida, sua organização é a responsável final por garantir que as medidas adequadas de segurança de dados estejam em vigor em todos os ambientes.

Modelos de serviço de nuvem: Principais diferenças

IaaS	**PaaS**	**SaaS**	**DBaaS**
Mantém o controle completo do gerenciamento da infraestrutura;	Permite a terceirização da manutenção da infraestrutura, do middleware e do software;	Evita despesas de capital com software;	Evita despesas de capital com infraestrutura e hardware de banco de dados;
É independente da plataforma;	Libera a equipe de TI para se concentrar no desenvolvimento de aplicações;	Transfere o gerenciamento completo para o provedor de serviços;	Transfere o gerenciamento completo para o provedor de serviços;
Oferece um modelo de preço pay-as-you-go.	Não oferece o controle completo da infraestrutura de TI.	Não oferece o controle dos dados e da segurança.	Reduz o controle dos dados e da segurança.

Desafios de segurança de dados para seu ambiente em nuvem

É provável que você já tenha iniciado a jornada em direção à nuvem.

Se sua organização é como a grande maioria das empresas, seus dados sensíveis residem em locais que você não pode controlar e são gerenciados por terceiros que talvez tenham um acesso irrestrito.

Uma pesquisa do Ponemon Institute constatou que as ameaças internas estão crescendo significativamente em termos de frequência e custo. De acordo com as constatações do instituto, “o custo global médio das ameaças internas subiu 31% em dois anos, chegando a US$ 11,45 milhões, e a frequência dos incidentes aumentou 47% no mesmo período de tempo”. [4] As organizações entrevistadas tinham um total global de 1.000 funcionários ou mais.

US$ 11,45 milhões

é o custo médio global de uma ameaça interna.[4]

Determinar a melhor forma de armazenar os dados é uma das decisões mais importantes que uma organização pode tomar. A nuvem é bastante adequada para o armazenamento de dados em nível organizacional a longo prazo que permite que as organizações aproveitem enormes economias de escala, as quais se convertem em despesas mais baixas. Além disso, esse recurso normalmente transforma os data centers baseados em nuvem em um local mais inteligente do que um conjunto de servidores locais para o armazenamento de informações críticas.

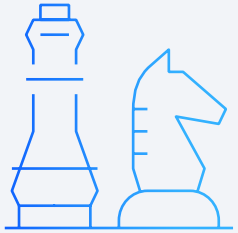
Embora a despesa de adquirir o armazenamento diminua, ele pode custar caro no longo prazo por conta do aumento do uso para negócios e do número de profissionais que gerenciam os sistemas de armazenamento. Colocar o armazenamento de dados nas mãos de provedores de serviços terceirizados pode ajudar a economizar tempo e dinheiro. Todavia, isso também pode apresentar sérios riscos de segurança e criar novos níveis de risco.

As implementações de nuvem seguem um modelo de responsabilidade compartilhada entre o provedor de nuvem e o consumidor. No caso de um modelo de IaaS, o consumidor de nuvem tem espaço para implementar medidas de segurança de dados parecidas com as que normalmente implementaria localmente, bem como para exercer controles mais rigorosos.

Por outro lado, com serviços de SaaS, os consumidores de nuvem precisam confiar, em grande parte, na visibilidade oferecida pelo provedor de nuvem. Em essência, isso limita a capacidade de exercer controles mais granulares.

É importante entender que, independentemente do modelo de implementação ou do tipo de serviço de nuvem, a segurança de dados precisa ser uma prioridade. O mais preocupante é que, agora, seus dados sensíveis encontram-se em muitos locais, tanto dentro da empresa quanto fora delas. Além disso, seus controles de segurança precisam ir aonde os dados forem.

Determinar a melhor forma de armazenar os dados é uma das decisões mais importantes que uma organização pode tomar.



Manter seus dados sensíveis em segurança essencialmente em qualquer lugar

Quem tem acesso aos dados sensíveis na sua organização? Você tem certeza de que seus funcionários ou usuários privilegiados não acessaram inadequadamente dados sensíveis de clientes?

Em outras palavras, você não pode proteger algo que não conhece. Simplesmente bloquear o acesso à rede pode não ser o ideal. Afinal, os funcionários necessitam dessa rede para acessar e compartilhar dados. Tal acesso significa que a eficácia da sua segurança de dados está principalmente nas mãos dos funcionários, alguns dos quais podem não trabalhar mais diretamente para a empresa, mas ainda mantêm o acesso. A descoberta, a classificação e o monitoramento automatizados dos dados sensíveis em todas as plataformas são cruciais para impor políticas de segurança eficazes no contexto e para ajudar na conformidade com os regulamentos.

Em geral, nos ambientes em nuvem, os provedores de serviços de nuvem (CSPs) têm a capacidade de acessar seus dados sensíveis, o que os transforma em uma nova fronteira de ameaças internas. Além disso, os cibercriminosos sabem que os CSPs armazenam enormes quantidades de dados importantes. Isso transforma tais ambientes nos principais alvos de ataques. Para combater essas ameaças, é necessário utilizar ferramentas sofisticadas com base em análise de dados que verifiquem o acesso normal e o autorizado.

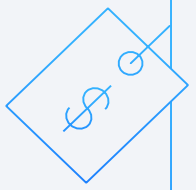
Saiba mais →

95% maior

foi o custo médio da violação de dados em organizações sem automação de segurança em 2019.[3]

US$ 5,16 milhões

foi o custo **sem automação**.[3]



US$ 2,65 milhões

foi o custo **com automação totalmente implementada**.[3]

Considerar a criptografia para o armazenamento em nuvem

Com o armazenamento em nuvem, seus dados podem ser transferidos para um local diferente do atual, em uma mídia diferente. Isso também acontece com a virtualização. Assim como os dados baseados em nuvem, os recursos de computação baseados em nuvem podem mudar rapidamente em termos de fundamentos de hardware e localização. A natureza mutável da nuvem significa que sua abordagem de segurança precisa lidar com diferentes tipos de armazenamento baseado em nuvem. Sua abordagem também precisa contemplar as cópias, sejam elas cópias temporárias ou backups de longo prazo, criadas durante a movimentação dos dados.

Para enfrentar esses desafios, você deve implementar soluções em diferentes plataformas e utilizar uma criptografia forte que ajude a garantir que seus dados sejam inúteis para pessoas não autorizadas em caso de uso indevido.

Mesmo se seus dados não estiverem armazenados principalmente na nuvem, tanto a forma em que saem da empresa e retornam a ela quanto a rota percorrida serão preocupações importantes. A segurança dos dados é determinada pelo elo mais fraco na corrente de processamento. Portanto, mesmo se os dados forem principalmente mantidos criptografados e atrás de um firewall local, poderão ser expostos caso sejam transmitidos para backup externo ou para processamento por terceiros.

A detecção de malware ou análise comportamental desenvolvida para identificar atividades suspeitas pode ajudar a evitar uma violação de dados interna ou externa, além de exercer funções importantes por conta própria.

No entanto, a criptografia ajuda a proteger os dados em qualquer lugar, estejam eles em repouso ou em movimento.

A segurança eficaz do armazenamento em nuvem não se limita a um simples backup de arquivos. É necessário proteger seus dados com medidas preventivas contra o uso não autorizado.

Melhores práticas de segurança do armazenamento em nuvem

- Bloquear o acesso por portas não aprovadas
- Avaliar vulnerabilidades proativamente
- Examinar continuamente o acesso a dados suspeitos
- Criptografar dados sensíveis, manter uma boa higiene das chaves de criptografia e armazenar as chaves localmente em uma rede separada dos dados criptografados
- Usar uma plataforma unificada que integre as informações de segurança em diferentes ambientes híbridos e multinuvem

Desafios organizacionais para seu ambiente em nuvem

Com os dados aumentando de forma exponencial, as organizações precisam lidar com uma lista crescente de leis e regulamentos de proteção de dados. Quais estão em risco? Informações pessoais de clientes, como informações de cartão de crédito, endereços, números de telefone e números de seguridade social, entre outras. Para ter uma solução de segurança eficaz, as organizações devem adotar uma abordagem baseada em risco para proteger os dados dos clientes em diferentes ambientes.

Estes são cinco desafios que podem afetar a postura de segurança da sua organização:

- Garantir a conformidade
- Proteger a privacidade
- Aumentar a produtividade
- Monitorar os controles de acesso
- Solucionar as vulnerabilidades

A plataforma de proteção de dados IBM Security™ Guardium® foi desenvolvida para ajudar sua organização a enfrentar esses desafios com recursos de proteção de dados mais inteligentes em todos os ambientes.

Manter a conformidade

As realidades da computação e do armazenamento com base em nuvem significam que seus dados sensíveis em diferentes sistemas híbridos em multinuvem podem estar sujeitos a regulamentos do governo e do setor.

Caso seus dados estejam em uma nuvem pública, você precisa saber como o CSP planeja proteger os dados sensíveis. Por exemplo, segundo o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UE), as informações que revelam a origem racial ou étnica de uma pessoa são consideradas sensíveis e podem estar sujeitas a condições específicas de processamento.5 Esses requisitos aplicam-se até mesmo a empresas localizadas em outras regiões do mundo que detêm e acessam os dados pessoais de residentes da UE.

Entender onde residem os dados de uma organização, em quais tipos de informações eles consistem e como estão relacionados dentro da empresa pode ajudar os líderes de negócios a definir as políticas certas para proteger e criptografar os dados.

Além disso, também pode ajudar a demonstrar a conformidade com regulamentos, tais como:

- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Security Content Automation Protocol (SCAP)
- Federal Information Security Management Act (FISMA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA).

As soluções IBM Security Guardium foram desenvolvidas para monitorar e auditar a atividade de dados em diferentes bancos de dados, arquivos, implementações de nuvem, ambientes de mainframe, repositórios de Big Data e contêineres. O processo é simplificado graças à automação, diminuindo os custos e o tempo para os requisitos de conformidade.

Learn more →

"Agora, o Guardium tem muitos relatórios e recursos incorporados, concentrando-se em coisas como a GDPR. Podemos aproveitar essas funcionalidades integradas para começar rapidamente, sem precisar construir tudo do zero."

Especialista sênior em governança de uma organização de seguros, em um estudo Total Economic Impact (TEI) da Forrester.[6]

Leia o estudo TEI sobre o Guardium →

Resolver os problemas de privacidade

Com a proliferação de smartphones, tablets e smart watches, o gerenciamento dos controles de acesso e da privacidade pode se tornar uma tarefa desafiadora. Um dos desafios para os administradores de segurança é garantir que apenas pessoas com um motivo de negócios válido tenham acesso a informações pessoais. Por exemplo, os médicos devem ter acesso a informações sensíveis, como os sintomas e dados de prognóstico de um paciente, enquanto um agente de cobrança precisa apenas do número do plano de saúde e do endereço de cobrança do paciente.

Seus clientes esperam que a privacidade deles seja uma prioridade para você. Comece desenvolvendo uma política de privacidade, descrevendo as informações que coleta sobre os clientes e o que pretende fazer com elas.

O IBM Security Guardium Insights fornece às equipes de segurança visualizações e alertas com base em risco, bem como análise de dados avançada baseada na própria tecnologia de aprendizado de máquina (ML), para lhes ajudar a revelar ameaças ocultas dentro de grandes volumes de dados em ambientes híbridos.

Saiba mais →

Kevin Baker, Chief Information Security Officer da Westfield, fala sobre os desafios de privacidade de dados enfrentados por sua organização, assim como sobre sua abordagem para enfrentá-los usando a automação e os insights necessários, enquanto amplia para apoiar a inovação com o IBM Security Guardium Insights.

Assista ao vídeo →

Aumentar a produtividade

As políticas de segurança e privacidade devem habilitar e aprimorar as operações de negócios, não interferir nelas. As políticas devem ser incorporadas às operações e ao trabalho diário de forma contínua dentro de todos os ambientes e entre eles (em ambientes públicos, locais e híbridos), sem afetar sua produtividade. Por exemplo, quando nuvens privadas são implementadas para facilitar o teste de aplicações, considere o uso de criptografia ou tokenização para mitigar o risco de exposição dos dados sensíveis.

As soluções IBM® Guardium podem ajudar suas equipes de segurança a monitorar a atividade dos usuários e responder a ameaças em tempo real. Esse processo é simplificado com controles automatizados e centralizados, reduzindo, assim, o tempo dedicado a investigações e capacitando os administradores de banco de dados e os especialistas em privacidade de dados a tomar decisões mais informadas.

De acordo com o Ponemon Institute, as soluções IBM Guardium podem ajudar a tornar as equipes de segurança de TI mais eficientes.7 Antes de implementarem a solução Guardium, cerca de 61% do tempo das equipes de segurança de TI entrevistadas era usado para identificar e corrigir problemas de segurança de dados. Após a implementação, a porcentagem média de tempo dedicado a essas atividades foi de 40%, com uma diminuição de 42%.

Antes da implementação da solução Guardium

61%

do tempo era usado anualmente para identificar e corrigir problemas de segurança de dados.[7]

Depois da implementação da solução Guardium

40%

do tempo foi usado anualmente para identificar e corrigir problemas de segurança de dados.[7]

Monitorar os controles de acesso

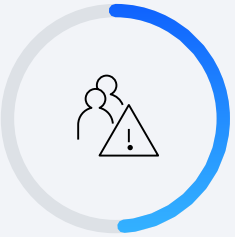
O ciclo de vida de uma violação de dados está ficando mais longo, afirma um estudo do Ponemon Institute. Na verdade, a pesquisa do instituto constatou que 49% das violações de dados estudadas foram causadas por erro humano, incluindo falhas no sistema e "usuários descuidados" que podem ser comprometidos por ataques de phishing ou ter dispositivos infectados ou perdidos/roubados.[3]

Os cibercriminosos podem variar de pessoas físicas a hackers patrocinados pelo estado com más intenções. Podem ser cientistas da computação desonestos tentando se exibir ou fazer uma declaração política ou podem ser intrusos organizados e difíceis. Podem ser funcionários insatisfeitos ou até mesmo um hacker patrocinado por um estado estrangeiro que deseja coletar inteligência de organizações do governo.

As violações também podem ser acidentais, como credenciais roubadas, erro humano ou configurações incorretas (por exemplo, quando as permissões são definidas incorretamente em uma tabela de banco de dados ou quando as credenciais de um funcionário são comprometidas). Uma maneira de evitar esse problema é autorizar usuários finais privilegiados e comuns com o "mínimo privilégio possível" para minimizar o abuso de privilégios e erros. As organizações devem proteger os dados de ataques internos e externos em ambientes em nuvem física, virtual e privada.

As defesas do perímetro são importantes. Entretanto, o mais importante é proteger os dados sensíveis onde quer que eles estejam. Dessa forma, se o perímetro for invadido, os dados sensíveis permanecerão seguros e não poderão ser usados por um ladrão. O declínio dos perímetros torna fundamental a proteção dos dados na origem.

Uma solução de segurança de dados em camadas pode ajudar os administradores a examinar os padrões de acesso a dados e os comportamentos dos usuários privilegiados de modo a entender o que está acontecendo dentro do ambiente em nuvem particular. O desafio é implementar soluções de segurança sem prejudicar a capacidade da empresa de crescer e se adaptar, fornecendo, assim, as proteções adequadas de acesso e dados para garantir que os dados sejam gerenciados conforme a necessidade de saber, onde quer que estejam.



49%

Quase metade das violações de dados causadas foram resultado de violações acidentais de erro humano e falhas do sistema.[3]

Lidar com as avaliações de vulnerabilidade

Na hora de se defender dos invasores, o que funcionou no passado pode não funcionar hoje. Muitas organizações usam tecnologias de segurança distintas que podem estar trabalhando isoladamente. Segundo um estudo da Forrester Consulting, em média, as organizações estão gerenciando 25 produtos ou serviços de segurança diferentes de 13 fornecedores.[8]

O número de vulnerabilidades no repositório de dados é grande e os criminosos podem explorar até mesmo a menor janela de oportunidade. Algumas dessas vulnerabilidades incluem ausência de correções, configurações indevidas e configurações padrão do sistema que podem deixar as lacunas de segurança que os cibercriminosos estão esperando. Essa complexidade fica cada vez mais difícil de monitorar e gerenciar à medida que os repositórios de dados se tornam virtualizados.

Ademais, as empresas que migram para a nuvem frequentemente têm dificuldades para aprimorar as práticas de segurança de dados de uma maneira que lhes permita proteger os dados sensíveis e, ao mesmo tempo, aproveitar os benefícios da nuvem. Quanto mais serviços de nuvem sua organização usa, de mais controle você talvez precise para gerenciar os diferentes ambientes.

Pense no uso das ferramentas desenvolvidas internamente que estão em vigor hoje para a segurança de dados. As ferramentas desenvolvidas internamente que você usa hoje funcionarão amanhã? Por exemplo, no caso de rotinas de mascaramento de dados ou scripts de monitoramento de atividades do banco de dados, mudanças de codificação serão necessárias para que funcionem em um banco de dados virtual? É provável que seja preciso um investimento significativo para atualizar tais soluções. Em resumo, as organizações necessitam de uma abordagem de segurança centrada em dados em que as estratégias de segurança estejam incorporadas na malha dos ambientes híbridos e multinuvem.

Ao contrário de uma solução pontual, o IBM Security Guardium Insights oferece suporte à integração heterogênea com outras soluções de segurança líderes no setor. A proteção de dados Guardium também fornece a melhor integração com soluções IBM Security, como IBM QRadar® SIEM para proteção proativa de dados.

Learn more →

"O Guardium pega todos os diferentes sistemas de gerenciamento de banco de dados e os consolida em uma ferramenta para que não precisemos usar sistemas separados para Oracle, SQL Server e afins. Podemos examinar todas as informações em um único painel."

VP, gerenciamento de segurança cibernética, serviços financeiros, estudo TEI[6]

Leia o estudo TEI sobre o Guardium →

Uma abordagem de segurança de dados mais inteligente

Como as nuvens amadurecem e se expandem rapidamente, precisamos compreender que uma segurança de dados eficaz não é **uma prova de 100 metros rasos, mas uma maratona**. Trata-se de um processo contínuo que se estende ao longo da vida dos dados.

Apesar de não existir uma abordagem genérica para a segurança de dados, é fundamental que as organizações busquem centralizar os controles de segurança e proteção de dados que podem funcionar bem juntos. Essa abordagem pode ajudar as equipes de segurança a melhorar a visibilidade e o controle dos dados em toda a empresa e na nuvem.

O que constitui uma estratégia de segurança de nuvem eficaz?

Descubra e classifique seus dados sensíveis estruturados e desestruturados, tanto online quanto offline, independentemente de onde se encontram. Além disso, classifique as informações pessoais e os dados sensíveis que estão sujeitos a regulamentos, como PCI, HIPAA, Lei Geral de Proteção de Dados (LGPD), CCPA e GDPR.

Proteja as origens de dados sensíveis com base em uma profunda compreensão de quais dados você possui e quem tem e deve ter acesso a eles. Os controles de proteção precisam acomodar os diferentes tipos de dados e perfis de usuário dentro do seu ambiente. Políticas de acesso flexíveis, criptografia de dados e gerenciamento de chaves de criptografia devem ajudar a manter seus dados sensíveis protegidos.

Responda às ameaças em tempo real. Depois de ser alertado sobre possíveis vulnerabilidades e riscos, você precisará da capacidade de responder rapidamente. As ações podem incluir bloqueio e quarentena de atividades suspeitas, suspensão ou desativação de sessões de usuários ou acesso a dados e envio de alertas acionáveis aos sistemas de operações e segurança de TI.

Avalie o risco com análise de dados e insights contextuais. Como seus dados críticos estão sendo protegidos? As autorizações de acesso estão em conformidade com os requisitos regulamentares e do setor? Os dados estão vulneráveis a acesso não autorizado e riscos de segurança com base na ausência de controles de proteção?

Monitore os padrões de acesso e uso de dados para revelar atividades suspeitas rapidamente. Depois que os controles adequados estiverem em vigor, você precisará ser rapidamente alertado sobre atividades suspeitas e desvios das políticas de acesso e uso de dados. Além disso, deve ser capaz de visualizar centralmente sua postura de conformidade e segurança de dados em diferentes ambientes de dados sem depender de vários consoles desarticulados.

Simplifique a conformidade e os relatórios. Você precisa ser capaz de demonstrar a conformidade e a segurança de dados a partes internas e externas, assim como de realizar as modificações adequadas com base nos resultados. A demonstração de conformidade com as exigências regulamentares normalmente requer armazenamento e relatórios equivalentes a anos de dados de auditoria e segurança de dados. Os relatórios de conformidade e segurança de dados devem ser abrangentes, cobrindo todo o ambiente de dados.

Criptografe dados em ambientes híbridos em multinuvem

Como não podemos mais confiar no perímetro para proteger os dados sensíveis de uma organização, é crucial que os líderes de negócios atuais confiram proteção aos dados propriamente ditos.

O IBM Security Guardium Data Encryption é um conjunto de soluções modulares, integradas e altamente escaláveis em criptografia, tokenização, gerenciamento de acesso e gerenciamento de chaves de criptografia que pode ser implementado essencialmente em todos os ambientes. Essas soluções codificam suas informações sensíveis e fornecem controle granular de quem tem a capacidade de codificá-las.

Saiba mais →

Uma criptografia forte é a resposta comum para o desafio de proteger dados sensíveis onde quer que estejam. Entretanto, a criptografia gera questões complicadas de portabilidade e garantia de acesso. Os dados serão bons se as chaves que os protegem forem seguras e confiáveis. Como é feito o backup das chaves? É possível mover os dados de forma transparente entre provedores de nuvem ou compartilhá-los entre o armazenamento local e o baseado em nuvem?

O IBM Security Guardium Key Lifecycle Manager pode ajudar os clientes que necessitam de uma proteção de dados mais rigorosa. A solução oferece armazenamento de chave, fornecimento de chave e gerenciamento de ciclo da vida da chave robustos e seguros para soluções de armazenamento IBM e não IBM usando o OASIS Key Management Interoperability Protocol (KMIP). Com gerenciamento centralizado de chaves de criptografia, as organizações serão capazes de cumprir regulamentos como PCI DSS, SOX e HIPAA.

Descubra mais →

A plataforma IBM Security Guardium foi nomeada líder no Forrester Wave: Data Security Portfolio Vendors, Q2 2019. De acordo com o relatório, a plataforma Guardium é “indicada para compradores que desejam reduzir e gerenciar centralmente os riscos de dados em ambientes de banco de dados distintos”.

Leia o relatório →

Descubra uma nova abordagem de segurança de dados

Para proteger um ambiente híbrido e multinuvem, é essencial que as organizações adotem soluções que ofereçam a máxima visibilidade e continuidade de negócios, além de ajudarem a alcançar a conformidade e a confiança dos clientes.

A plataforma IBM Security Guardium fundamenta-se na abrangente proposta de valor de uma "abordagem mais inteligente e mais adaptável" de segurança de dados. Além disso, a solução oferece suporte a uma grande variedade de ambientes em nuvem, incluindo nuvens privadas e públicas, em ambientes PaaS, IaaS e SaaS, para operações contínuas e segurança.

O Ponemon Institute realizou uma pesquisa com organizações que usam a solução Guardium para monitorar e defender os dados e bancos de dados da sua empresa. Constatou que 86% dos entrevistados afirmaram que a capacidade de usar a solução Guardium para gerenciar o risco de dados em ambientes complexos de TI, como um ecossistema em multinuvem ou nuvem híbrida, é de grande valor. Do mesmo modo, o aprendizado de máquina e a automação são benefícios significativos no gerenciamento de riscos de dados em toda a empresa.[7]

Com a solução Guardium, sua equipe de segurança pode escolher a arquitetura de sistema que funciona para a empresa. Por exemplo, sua equipe pode implementar todos os componentes do Guardium na nuvem ou optar por manter alguns dos componentes, como um gerenciador central, no local. Essa flexibilidade permite que os clientes existentes levem facilmente sua estratégia de proteção de dados para a nuvem sem afetar as implementações existentes.

Saiba mais →

Principais recursos do IBM Security Guardium:

Descubra e classifique dados sensíveis automaticamente.

Criptografe dados em todos os ambientes.

Identifique dados em risco e obtenha recomendações de remediação.

Use análises de dados e insights contextuais.

Simplifique os relatórios de segurança e conformidade.

Receba uma perspectiva de negócios sobre o risco dos dados.

Monitore o acesso e proteja os dados.

Conclusão

Dada a evolução das ameaças, as organizações precisam adotar uma abordagem consistente e unificada para a segurança de dados em multinuvem híbrida. Considere estas perguntas:

- Quais dados permanecerão no local?
- Quais dados serão transferidos para a nuvem?
- Como é possível monitorar o acesso a dados?
- Quais tipos de vulnerabilidades devem ser considerados?
- Como podemos demonstrar a conformidade com os requisitos regulamentares e de segurança de dados?

Ao escolher soluções de proteção e segurança de dados, selecione soluções que possam ser ampliadas em infraestruturas de TI distintas, protegendo ambientes físicos, virtuais e em nuvem de ataques externos mal-intencionados, fraude, acesso não autorizado e violações internas. Essas soluções precisam funcionar em um ambiente em nuvem sem configurações caras e complexas. Tal abordagem fornecerá uma plataforma eficiente para a disponibilização de privacidade e segurança de dados, ajudando você a gerenciar os custos reduzindo os recursos e proporcionando mais agilidade e flexibilidade.

O software Guardium oferece uma solução abrangente para infraestruturas físicas, virtuais e em nuvem por meio de controles automatizados de segurança em ambientes heterogêneos. A solução ajuda a simplificar a conformidade, reduz riscos e é compatível com as principais plataformas de nuvem, incluindo IBM Cloud®, Microsoft Azure e AWS. Além disso, funciona em ambientes Microsoft Windows, UNIX e Linux®.

Quais são os próximos passos?
Descubra como as soluções IBM Security Guardium podem ajudar você a adotar uma abordagem integrada e mais inteligente para proteger dados críticos em seus ambientes híbridos e multinuvem. Visite ibm.com/security/data-security/guardium

O estudo TEI da Forrester mostra que estes benefícios importantes para os negócios são gerados pela plataforma IBM Security Guardium:[6]

OI de 3 3

US 3,3 milhões em benefícios totais

Retorno em <6 meses em média

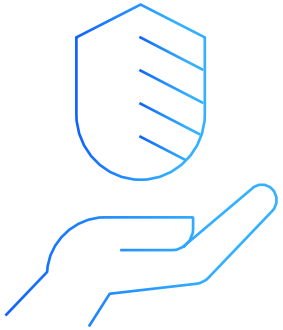
Leia mais →

Por que escolher as soluções IBM Security?

As soluções IBM Security oferecem um dos portfólios mais avançados e integrados de produtos e serviços de segurança organizacional. O portfólio, apoiado pela pesquisa e desenvolvimento de renome mundial da IBM X-Force®, fornece inteligência de segurança para ajudar as organizações a proteger integralmente seus funcionários, infraestruturas, dados e aplicações, oferecendo soluções para gestão de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicações, gerenciamento de risco, gerenciamento de endpoint, segurança de rede e muito mais.

Essas soluções permitem que as organizações gerenciem efetivamente os riscos e implementem segurança integrada para dispositivos móveis, nuvem, redes sociais e outras arquiteturas empresariais de negócios.

A IBM administra uma das organizações mais amplas de pesquisa, desenvolvimento e fornecimento de segurança do mundo, monitora mais de 60 bilhões de eventos de segurança por dia em mais de 130 países e detém mais de 3.700 patentes de segurança.



IBM Corporation
New Orchard R
oad Armonk, NY 10504

Produzido nos Estados Unidos da América
Junho de 2020

Este documento é considerado atual na data inicial da publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países em que a IBM atua.

Os dados de desempenho e os exemplos de clientes citados têm fins somente ilustrativos. Os resultados reais de desempenho poderão variar dependendo das configurações e das condições operacionais específicas. O usuário é responsável por avaliar e verificar o funcionamento de outros produtos ou programas com produtos e programas IBM. AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUSIVE NENHUMA GARANTIA DE COMERCIABILIDADE, ADEQUAÇÃO A UM FIM ESPECÍFICO E GARANTIAS OU CONDIÇÕES DE NÃO INFRAÇÃO. As garantias dos produtos IBM estão de acordo com os termos e as condições dos contratos segundo os quais foram fornecidos.

O cliente é responsável por assegurar o cumprimento das leis e dos regulamentos aplicáveis a ele. A IBM não oferece orientação jurídica nem declara ou garante que seus serviços ou produtos assegurarão o cumprimento de qualquer lei ou regulamento pelo cliente.

Declaração de boas práticas de segurança: A segurança de sistemas de TI envolve a proteção de sistemas e de informações por meio de prevenção, detecção e resposta ao acesso inadequado de dentro e de fora da sua empresa. O acesso indevido pode resultar em alteração, destruição emprego indevido ou uso incorreto de informações, ou pode causar danos ou uso indevido dos seus sistemas, inclusive para uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção do uso ou acesso inadequado. Os sistemas, produtos e serviços da IBM são desenvolvidos para fazer parte de uma abordagem de segurança legal e abrangente, o que implicará, necessariamente, em procedimentos operacionais adicionais e poderá exigir que outros sistemas, produtos ou serviços sejam mais eficazes. A IBM NÃO GARANTE QUE NENHUM SISTEMA, PRODUTO OU SERVIÇO ESTEJA IMUNE, OU TORNARÁ SUA EMPRESA IMUNE, À CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

1 "Assembling your cloud orchestra." *IBM Institute for Business Value*, outubro de 2018. ibm.com/thought-leadership/institute-business-value/report/multicloud/#

2 Jim Comfort, "How a Hybrid Multicloud Strategy Can Overcome the Cloud Paradox." *IBM*, 5 de novembro de 2019. ibm.com/blogs/think/2019/11/how-a-hybrid-multicloud-strategy-can-overcome-the-cloud-paradox/

3 "Cost of a Data Breach Report 2019." *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

4 "2020 Cost of Insider Threats Global Report", *Ponemon Institute, ObserveIT*. observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

5 "What personal data is considered sensitive?" *European Commission*. ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

6 "The Total Economic Impact Of IBM Security Guardium." *Forrester*, abril de 2018. ibm.com/downloads/cas/QA8XWPBA

7 "Ponemon Report: Client Insights on Data Protection with Guardium." *Ponemon Institute*, agosto de 2019. ibm.com/account/reg/us-en/signup?formid=urx-40683

8 "Complexity In Cybersecurity Report 2019." *Forrester Consulting*, maio de 2019. ibm.com/downloads/cas/QK1YD49A

GWB3E8ZV