IBM Security

IBM

Supere os desafios de proteger dados que estão aqui, lá e em todos os lugares

Mantendo os dados sensíveis seguros na era da computação em nuvem

Clique em um círculo para avançar para o capítulo

1

Como implementar um ambiente de nuvem

As organizações estão rapidamente migrando para a nuvem, utilizando a infraestrutura como serviço (IaaS), o software como serviço (SaaS) e a plataforma como serviço (PaaS) como novas formas de otimizar seus negócios, embora tais ambientes ofereçam novos riscos para dados sensíveis.

2

Os desafios de segurança part

Muitas vezes, as implementações na nuvem significam que os dados sensíveis são mantidos em locais que você não pode controlar e são gerenciados por terceiros que talvez tenham acesso irrestrito a eles.

3

Desafios organizacionais

Os desafios de proteger dados na nuvem incluem garantir a conformidade, monitorar os controles de acesso, assegurar a privacidade, aumentar a produtividade e enfrentar as vulnerabilidades, enquanto utiliza seus dados locais e os dados baseados na nuvem para impulsionar seus negócios adiante.

4

Abordagem de proteção de dados

As tecnologias de segurança e proteção de dados devem atuar em vários ambientes (físico, nuvem e híbrido) ao mesmo tempo. Sua solução de segurança de dados deve ser automatizada, dinâmica e adaptável, além de oferecer recursos de criptografia consistentes e flexíveis.

5

Conclusão

À medida que a computação em nuvem se populariza, os fundamentos de segurança permanecem os mesmos: proteger os dados e dar suporte à conformidade.

1.1 Como implementar um ambiente de nuvem

Alguns anos atrás, muitas organizações recorreram aos ambientes de nuvem privada para ajudar a aumentar a flexibilidade e controlar os custos, principalmente por causa da imaturidade e da falta de controle dentro dos ambientes de nuvem pública disponíveis na época. Hoje, porém, a decisão de "migrar para a nuvem" é menos binária. Existe um espectro de opções, que cobrem diferentes modelos de implementação (pública, privada e híbrida) e tipos de serviço, incluindo IaaS, PaaS e SaaS.

Com opções mais granulares, a implementação na nuvem se tornou fragmentada de acordo com a linha de negócios, deixando de ser uma decisão padronizada de TI. Embora a lista de novas opções de nuvem seja abundante, a maioria das empresas adotará um ambiente híbrido misto para aproveitar os investimentos existentes em mainframes, bancos de dados locais, distribuições de Big Data, sistemas de arquivos e muito mais.[1]

Uma nuvem privada é uma infraestrutura de TI operada exclusivamente para uma única organização, podendo ser gerenciada internamente ou por terceiros. Com as nuvens privadas, as organizações controlam toda a pilha de software, assim como a plataforma subjacente, desde a infraestrutura de hardware até as ferramentas de medição. Os serviços de nuvem privada são dedicados para uso das unidades de negócios de uma única empresa (ou compartilhados apenas com os parceiros dela).1 Entretanto, quando as cargas de trabalho migram para nuvens privadas, a proteção dos dados em ambientes virtuais se torna ainda mais importante, especialmente porque cargas de trabalho com diferentes níveis de confiança são combinadas para execução no mesmo hardware físico.

Uma pesquisa da Gartner mostra que o uso e o investimento em computação em nuvem privada continuarão sendo significativos. No entanto, quase todas as empresas que a Gartner entrevistou desejam utilizar um modelo de nuvem híbrida, com elementos de nuvens privada e pública. As empresas estão usando opções turnkey de computação em nuvem pública para possibilitar serviços mais rápidos e sem atrito, além de aumentar a agilidade dos negócios e promover a inovação. A computação em nuvem pública exerce uma função essencial para a inovação e, consequentemente, deve crescer 15,2% ao ano até 2019.[1]

No que diz respeito a ambientes de nuvem, sejam eles na nuvem pública ou um ambiente hospedado de forma privada, os controles de segurança e proteção de dados precisam proteger dados sensíveis, assim como dar suporte aos requisitos de conformidade do governo e da indústria, que crescem de modo constante.

1.2 Como implementar um ambiente de nuvem

Os tipos de serviços mais comuns são IaaS, PaaS e SaaS. A maneira mais fácil de visualizar a diferença é considerar sua pilha de TI. Na parte inferior, fica a infraestrutura (que inclui seu hardware, servidores e rede) que age como base de TI. Acima dessa infraestrutura, estão as plataformas de software ou middleware que fornecem as ferramentas de que seus desenvolvedores precisam para implementar aplicativos de negócios. Na parte superior, encontram-se os aplicativos de negócios que interagem com os funcionários internos e os clientes.

Com IaaS, as organizações podem manter as plataformas físicas de software e middleware e os aplicativos de negócios existentes, mas terceirizam o gerenciamento da infraestrutura subjacente. As empresas fazem isso com a intenção de tirar proveito da nuvem rapidamente, enquanto minimizam o impacto e utilizam os investimentos existentes.

Com PaaS, as empresas podem terceirizar a infraestrutura, assim como o middleware ou o software. Isso remove uma carga significativa para a empresa, por uma perspectiva de TI, e permite que ela se concentre em desenvolver aplicativos de negócios inovadores.

SaaS é a opção mais extrema, que terceiriza toda a TI e permite que as organizações se concentrem mais em seus pontos fortes (por exemplo, assistência médica, serviços financeiros) em vez de gastar muito tempo e investimento em tecnologia, o que pode ser feito pelos especialistas da área.

A cada passo, de IaaS a PaaS e SaaS, as organizações abrem mão de certo nível de controle sobre os sistemas que armazenam, gerenciam e distribuem seus dados sensíveis. Esse aumento na confiança concedida a terceiros também oferece um aumento no risco.

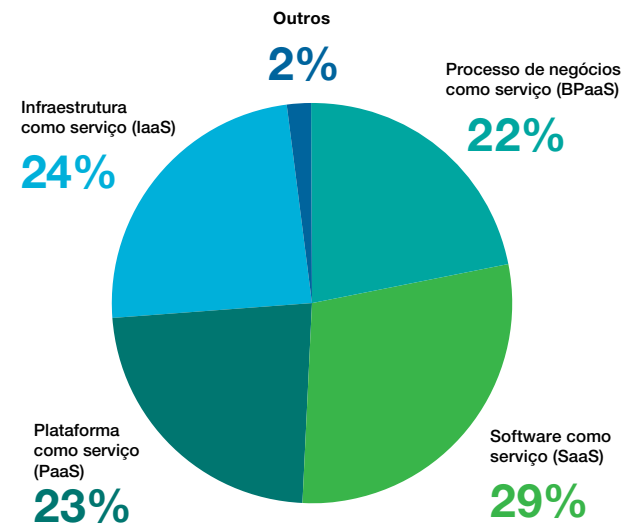


Figura 1: Pergunta da pesquisa: “Como o orçamento está alocado atualmente para serviços em nuvem “públicos” se dividido entre os seguintes tipos de nuvem?”

Fonte: Ed Anderson e Sid Nag, “Market Trends: Cloud Adoption Trends Favor Public Cloud With a Hybrid Twist”, Gartner, 4 de agosto de 2016. ID: G00294424.

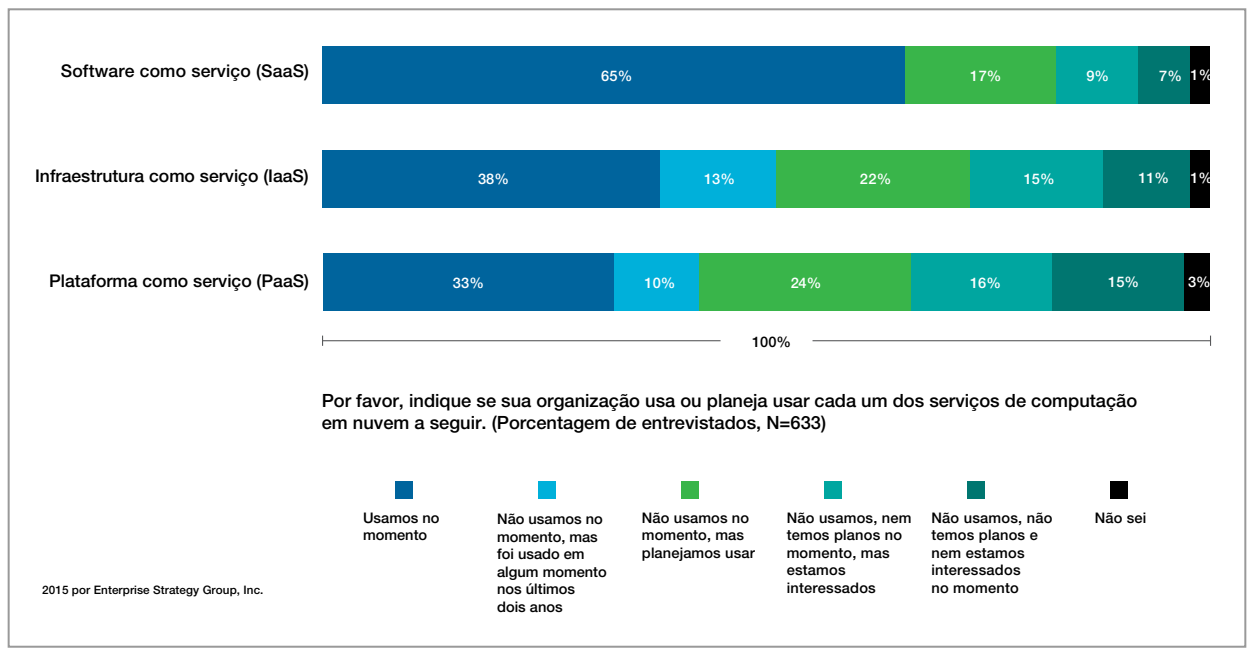
1.3 Como implementar um ambiente de nuvem

"Usar a nuvem" não é um binário. Um estudo feito com mais de 600 responsáveis por tomar decisões de TI em empresas mostra que a maioria das empresas entrevistadas adotou pelo menos alguns aplicativos de SaaS; menos de 20% dos entrevistados não tinham planos ou interesse em utilizar SaaS.

A implementação de PaaS, exige maior compromisso com o armazenamento de dados externos e computação, por essa razão fica atrás das aplicações fragmentarias de nuvem. No entanto, 67% dos entrevistados tinham usado, usavam ou planejavam adotar PaAs.

A adoção da infraestrutura em nuvem (IaaS), que transfere a obrigação de instalar e manter a infraestrutura física de uma empresa para um provedor dedicado, está estatisticamente posicionada entre PaaS e SaaS. No momento dessa pesquisa, 73% dos entrevistados usavam ou planejavam usar alguma forma de infraestrutura em nuvem ou já haviam experimentado.

Os desafios da proteção de dados em nuvem virtual e privada



2.1 Os desafios de segurança da nuvem

A nuvem é especialmente indicada para o armazenamento de dados em nível corporativo a longo prazo, com economia de escala em equipamentos e na administração que é capaz de transformar os datacenters baseados em nuvem em um local mais otimizado para armazenar informações críticas do que uma pilha de servidores no fim do corredor. Isso ocorre porque, enquanto a despesa de adquirir armazenamento diminui, os custos do maior uso corporativo e do pessoal para gerenciar o armazenamento continuam aumentando. No entanto, colocar o armazenamento de dados nas mãos de administradores dedicados pode ajudar a poupar tempo e dinheiro. Todavia, também pode representar desafios sérios de segurança e criar novos níveis de risco.

É importante entender que, independentemente do modelo de implementação ou tipo de serviço, os princípios fundamentais de segurança de dados não devem mudar. O que muda é que os dados sensíveis agora encontram-se em muitos locais, tanto dentro quanto fora da empresa. Isso significa que os controles de segurança precisam ir para onde os dados forem. Ao avaliar as tecnologias de segurança de dados, escolha soluções que atuem em diversos ambientes de maneira transparente e simultânea. Certifique-se de que a segurança de dados seja uma solução dinâmica e adaptável através de uma ampla gama de ambientes, para que você não precise colocar aleatoriamente peças adicionais de proteção de dados juntas.

Mantendo os dados seguros de todos, em qualquer lugar

O desafio mais importante é óbvio: agora, os dados sensíveis estão em todo lugar, dentro e fora dos seus firewalls, sendo gerenciados, de alguma forma, por seus próprios funcionários e também por terceiros. Não é mais possível proteger seus dados sensíveis simplesmente bloqueando o acesso à rede. Na verdade, você depende da rede para acessar e compartilhar seus dados. Isso deixa a segurança de dados em grande parte nas mãos de muito mais pessoas do que no passado, e muitas outras pessoas que não trabalham mais diretamente para a sua empresa. Geralmente, em ambientes de nuvem, os provedores de serviços de nuvem (CSPs) são capazes de acessar seus dados sensíveis, tornando-se a nova fronteira em ameaças internas. Além disso, os cibercriminosos sabem que os CSPs armazenam quantias enormes de dados importantes. Ambos esses riscos transformam recursos como criptografia de dados e monitoramento das atividades dos dados em uma parte especialmente importante da sua estratégia de segurança.

2.2 Os desafios de segurança da nuvem

A portabilidade dos dados é um dos motivos pelos quais o armazenamento em nuvem é uma opção econômica. As despesas de infraestrutura (desde custos com imóveis a custos com energia) variam enormemente de acordo com a geografia e até com a hora do dia. Do mesmo modo, os custos de armazenamento e o desempenho entre os tipos de mídia mudam. Os armazenamentos em fita, em disco giratório e de estado sólido estão avançando em termos de capacidade, velocidade e confiabilidade; a combinação mais econômica de tecnologias de armazenamento para determinada empresa pode mudar rapidamente. Portanto, com o armazenamento em nuvem, seus dados poderão passar o dia de amanhã em um local e uma mídia diferentes dos de hoje. Isso também ocorre com a virtualização. Assim como os dados baseados em nuvem, os recursos de computação baseados em nuvem podem mudar (de forma transparente e rápida) em termos de local e do hardware subjacente.

A natureza mutável da nuvem significa que as abordagens de segurança para o armazenamento baseado em nuvem precisam lidar com tipos diferentes de armazenamento. A abordagem também precisa considerar as cópias, sejam elas backups de longo prazo ou cópias temporárias criadas durante a movimentação dos dados. Para enfrentar tais desafios, escolha soluções de plataforma cruzada e utilize uma criptografia forte.

Mesmo se seus dados não estiverem armazenados substancialmente na nuvem, tanto a forma em que os dados saem e retornam para a empresa quanto a rota que eles percorrem serão preocupações importantes. Até mesmo para os dados que são mantidos principalmente criptografados e protegidos por firewall no local, se partes deles forem expostas durante a transmissão para backup externo ou processamento por um terceiro, a segurança dos dados sensíveis será determinada pelo elo mais fraco na corrente de processamento de dados.

Uma proteção eficaz dos dados quando estão na nuvem adota medidas preventivas e passivas (como bloquear o acesso por portas não aprovadas) e medidas ativas, como fazer varredura contínua em busca de acesso a dados suspeitos. A principal medida que a ser adotada é a utilização de criptografia para seus dados sensíveis. Enquanto a detecção de malware ou análise comportamental criada para identificar o acesso suspeito pode ajudar a impedir uma violação de dados interno ou externo (e exercerem valiosas funções próprias), a criptografia auxilia a proteger os dados onde quer que estejam, seja em repouso ou em movimento.

2.3 Os desafios de segurança da nuvem

Implicações administrativas e regulamentares

As realidades do armazenamento e da computação baseados em nuvem significam que a proteção de dados sensíveis na nuvem e em sistemas de nuvem híbrida raramente é tão perfeita quanto os administradores gostariam. Ferramentas de segurança que oferecem interfaces unificadas em terminais de nuvem (de um parque de servidores externo dedicado a máquinas virtuais em uma infraestrutura de nuvem pública) são um bom começo para cumprir a promessa de uma administração remota eficiente.

Igualmente importantes são os requisitos regulamentares e a soberania de dados, em outras palavras, as regras que tratam da segurança e da proteção de dados quando dados sensíveis são armazenados fisicamente em um local específico. O armazenamento de dados na nuvem poderá resultar em armazenamento de dados sensíveis em locais onde estão em vigor leis mais rigorosas do que as do lugar de origem dos dados. Uma proteção mais rigorosa para os dados pessoais de indivíduos de países dentro da União Europeia (UE), por exemplo, é exigida no âmbito do Regulamento Geral de Proteção de Dados (GDPR) da UE. Esses requisitos aplicam-se até mesmo a empresas situadas em outras regiões do mundo que detêm e acessam dados pessoais de residentes da UE.

Saiba quem está acessando seus dados:
o IBM® Security Guardium® pode ajudar sua infraestrutura em nuvem e em nuvem híbrida com ferramentas de monitoramento e avaliação que revelam anomalias e vulnerabilidades.

3.1 Desafios organizacionais

3

As organizações ainda enfrentam muitos desafios quando tentam proteger seus dados sensíveis. Um dos motivos são os regulamentos complexos. A Forrester destaca que, atualmente, "a maioria dos arquitetos e profissionais de segurança das empresas têm dificuldades para melhorar a segurança dos dados ou cumprir os requisitos de conformidade, por causa do aumento dos silos e dos volumes de dados. A aplicação de políticas uniformes de controle de acesso em bancos de dados, data warehouses, Hadoop, NoSQL e arquivos tornou-se extremamente desafiadora."[2]

A virtualização terá o potencial de facilitar a aplicação dos controles de segurança e dos mecanismos de conformidade, mas somente se o ambiente de nuvem virtual ou privado for capaz de apoiar a proteção de dados sensíveis tratando uniformemente os requisitos de conformidade, as necessidades de controle de acesso, os requisitos de privacidade, os requisitos de vulnerabilidade e as necessidades de produtividade.

Os desafios da proteção de dados em nuvem virtual e privada

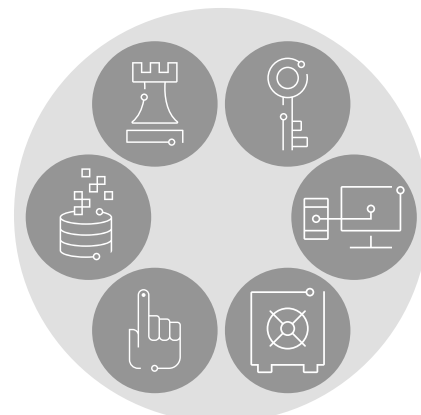


Figura 2: A proteção de dados armazenados em nuvem ainda exige que os administradores prestem atenção a aspectos de segurança, que vão desde segurança e privacidade até conformidade regulamentar em diversos domínios.

3.2 Desafios organizacionais

Conformidade

Pense sobre onde os dados sensíveis residem em um ambiente de nuvem. É importante identificar e classificar os tipos de dados sensíveis, assim como estabelecer políticas para o uso deles, seja na nuvem pública ou em um ambiente de nuvem privada. Se os dados estiverem em uma nuvem pública, você precisará entender como o provedor da infraestrutura em nuvem planeja proteger seus dados sensíveis.

Em qualquer caso, entender onde os dados residem, quais domínios de informações existem e como estão relacionados em toda a empresa ajudará as organizações a definir as políticas certas para proteger e criptografar esses dados, além de demonstrar o cumprimento de regulamentos como Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Security Content Automation Protocol (SCAP), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA) e Health Information Technology for Economic and Clinical Health Act (HITECH). Os regulamentos de confomidade continuam surgindo, e as organizações permancem responsáveis, mesmo quando os dados são movidos em nuvem.

Privacidade

Outro desafio para os administradores do acesso a dados é garantir que apenas as pessoas com um motivo de negócios válido tenham acesso a informações pessoais. Por exemplo, os médicos precisam ver informações sensíveis como os sintomas e dados de prognóstico de um paciente, enquanto um caixa necessita apenas do número do plano de saúde e do endereço de cobrança do paciente.

3.3 Desafios organizacionais

Controles de acesso

Os cibercriminosos têm intenções inescrupulosas e disruptivas. Podem ser cientistas da computação desonestos tentando se exibir ou fazer uma declaração política ou mesmo invasores organizados e malignos. Estados estrangeiros já patrocinaram hackers para coletar inteligência de organizações do governo. Os invasores podem ser até mesmo funcionários descontentes. As violações também podem ser acidentais, por exemplo, quando permissões são definidas incorretamente em uma tabela de banco de dados ou quando as credenciais de um funcionário são comprometidas. As boas práticas sugerem autorizar usuários finais privilegiados e comuns com o "menor privilégio possível" para minimizar o abuso de privilégios e os erros. As organizações devem proteger os dados de ataques internos e externos em ambientes de nuvem física, virtual e privada.

As defesas do perímetro são importantes, mas também é importante proteger os próprios dados sensíveis. Se o perímetro for violado, os dados sensíveis já precisarão estar protegidos (sem poder ser usados por um ladrão) a fim de minimizar o impacto da violação e impedir que o hacker tenha o caminho livre. As defesas devem incluir uma solução de segurança de dados em camadas para que os administradores possam entender o que está acontecendo dentro da nuvem privada, por exemplo, compreendendo os padrões de acesso a dados e os comportamentos do usuário privilegiado.

O desafio é fornecer as proteções adequadas de acesso e dados e, ao mesmo tempo, atender às necessidades de negócios e garantir que os dados sejam gerenciados conforme a "necessidade de saber", não importa onde estejam.

Produtividade

As políticas de segurança e privacidade devem habilitar e aprimorar, sem interferir com as operações de negócios. Devem ser integradas nas operações diárias e trabalhar de forma contínua dentro de todos os ambientes e entre eles (em ambientes de nuvem privada, ambientes de nuvem pública, ambientes locais e ambientes híbridos) sem afetar a produtividade do usuário. Por exemplo, quando nuvens privadas são implementadas para facilitar os testes de aplicativos, considere a possibilidade de usar criptografia ou tokenização para mitigar o risco de exposição dos dados sensíveis.

3.4 Desafios organizacionais

Vulnerabilidade

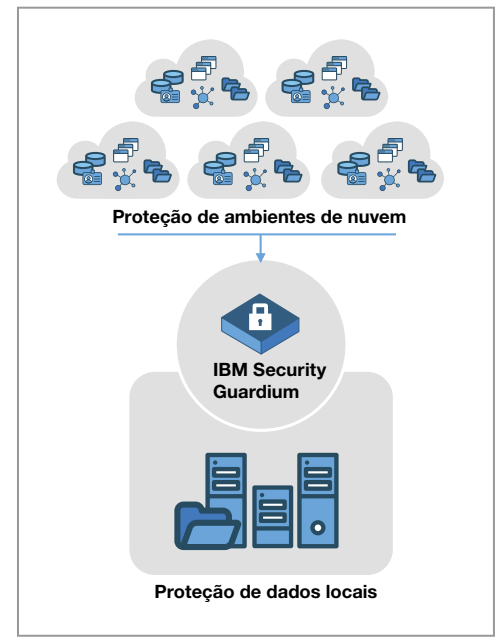
Atualmente, as organizações têm diversas tecnologias de segurança em vigor para proteger os dados corporativos e dar suporte à conformidade. No entanto, o número de vulnerabilidades no repositório de dados é vasto; os criminosos podem explorar até mesmo a menor janela de oportunidade. É importante entender as vulnerabilidades de todos os ângulos e desenvolver uma abordagem para lidar com elas. As vulnerabilidades comuns incluem ausência de correções, configurações incorretas e configurações de sistema padrão. Está ficando cada vez mais difícil monitorar e gerenciar essa complexidade conforme os repositórios de dados se tornam virtualizados.

À medida que as organizações migram para nuvens privadas e públicas, por exemplo, as soluções nem sempre são ampliadas. Além disso, algumas abordagens de criptografia estão vinculadas a um recurso específico de hardware ou rede. Em um ambiente de nuvem, os administradores não podem depender de acesso à infraestrutura de hardware de baixo nível.

Outro problema costuma surgir quando uma nuvem privada é usada para teste ou desenvolvimento de aplicativos. Bancos de dados novos são criados e descomissionados regularmente. Os dados precisam ser protegidos, pois esses bancos de dados são criados de forma dinâmica para apoiar o teste e o desenvolvimento. Uma abordagem escalável de segurança de dados para tal ambiente de nuvem privada significa que, conforme são criados, os novos bancos de dados são descobertos automaticamente, enquanto os dados que vivem neles são classificados, monitorados e protegidos automaticamente.

Por fim, reflita sobre o uso de ferramentas próprias em vigor atualmente para a segurança de dados (como rotinas de mascaramento de dados ou scripts de monitoramento das atividades de banco de dados). Mudanças na codificação são necessárias para que funcionem em um banco de dados virtual? É provável que um investimento significativo seja necessário para atualizar essas soluções próprias, e você ainda enfrentará desafios significativos depois disso. Preferencialmente, à medida que novos bancos de dados ou outras origens de dados são adicionados, os processos e procedimentos de segurança devem ser realizados sem intervenção manual. Em resumo, é necessário incorporar estratégias de segurança na malha de qualquer ambiente de nuvem.

Abordagem de proteção de dados



4.1 Abordagem de proteção de dados

As organizações devem tentar centralizar os controles de segurança e proteção de dados em ambientes de nuvem privada e pública, assim como no restante da empresa, e assegurar uma separação de funções para que os administradores de dados não se tornem também administradores ou auditores de segurança. Os principais elementos de uma estratégia de nuvem segura incluem:

- Entender onde os dados sensíveis existem e quem tem acesso a eles. As organizações não podem proteger dados sensíveis com criptografia ou aplicar controles de acesso rigorosos a menos que saibam onde eles residem e como estão relacionados em toda a empresa.
- Proteger dados sensíveis estruturados e desestruturados, online e offline, com as tecnologias adequadas, além de estabelecer os requisitos de acesso corretos.
- Proteger os dados após a produção, em ambientes de desenvolvimento, teste e garantia de qualidade.
- Monitorar o acesso a dados sensíveis, onde quer que residam, de maneira segura e contínua.
- Demonstrar a conformidade com auditorias de aprovação por meio de relatórios criados previamente para auditores e fluxo de trabalho automatizado. Assim, será possível levar os relatórios corretos às pessoas corretas no momento correto para a aprovação.

Estratégias de proteção abrangentes para todos os ambientes de nuvem e nuvem híbrida devem fornecer alertas sobre comportamentos suspeitos para administradores de segurança. As organizações também devem considerar soluções de segurança de dados que forneçam suporte de conformidade automatizado para simplificar o processo de conformidade.

Os processos de segurança de dados para ambientes de nuvem precisam rastrear os dados continuamente e fornecer insights sobre quem os está acessando em aplicativos, bancos de dados, warehouses, compartilhamentos de arquivos, ambientes de Big Data e muito mais. Uma abordagem como essa pode ajudar a garantir proteção 360 graus para dados organizacionais sensíveis, não importa onde estejam.

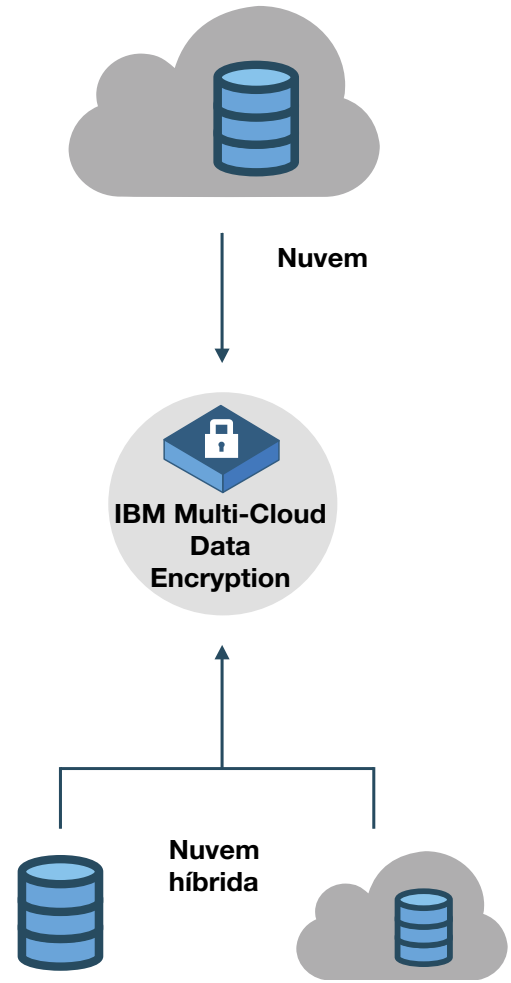
4.2 Abordagem de proteção de dados

Os fardos regulatórios para detentores de dados (assim como os riscos de uma violação) podem deixar desconfiadas as empresas que estão pensando em começar ou expandir o armazenamento baseado em nuvem. Uma criptografia forte é a resposta mais óbvia para o desafio de proteger dados sensíveis, interna ou externamente. No entanto, 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? Os dados podem ser movidos de forma transparente entre provedores de nuvem ou compartilhados entre o armazenamento local e o baseado em nuvem?

O IBM Multi-Cloud Data Encryption protege dados de nuvem (e nuvem híbrida) e faz isso pensando nos requisitos de portabilidade e conformidade. Para manter as chaves de criptografia acessíveis e prontamente disponíveis, ele pode ser integrado com um gerenciador de chaves avançado.

Além disso, o IBM Security Key Lifecycle Manager consegue ajudar clientes que necessitam de uma proteção de dados mais rigorosa, baseada em armazenamento criptografado de hardware, para simplificar e centralizar o gerenciamento de chaves de criptografia, sem medo de exposição de dados em ambientes de nuvem virtual.

O gerenciamento de chaves é o coração de um ambiente de criptografia seguro.



5.1 Conclusão

Para assegurar a proteção dos dados em ambientes virtuais e de nuvem, as organizações precisam entender quais dados entrarão em tais ambientes, como o acesso a esses dados pode ser monitorado, quais tipos de vulnerabilidades existem e como é possível demonstrar a conformidade. As proteções devem ser incorporadas nos ambientes de nuvem desde o início; o objetivo da primeira fase é ajudar as organizações a demonstrar a conformidade.

Ao escolher as soluções de segurança e proteção de dados, selecione as soluções que sejam escaláveis e extensíveis em infraestruturas de TI, protegendo ambientes físicos, virtuais e de nuvem de ataques externos maliciosos, fraude, acesso não autorizado e violações internas. Essas soluções precisam funcionar em um ambiente de nuvem sem instalação, configuração ou despesa adicional especial. Uma abordagem assim fornecerá uma plataforma eficiente para a entrega de segurança e privacidade de dados, ajudará a gerenciar os custos reduzindo os recursos de segurança de dados e proporcionará maior agilidade e flexibilidade com serviços de autoatendimento para segurança e privacidade.

O Guardium pode ajudar a apoiar sua estratégia de nuvem com:

- Monitoramento das atividades de dados e arquivos, avaliações de vulnerabilidade, edição de dados, criptografia de dados, bloqueio dinâmico, quarentena e alertas
- Descoberta e classificação automáticas de dados sensíveis na nuvem
- Mascaramento estático e dinâmico de dados para garantir um modelo de acesso menos privilegiado para recursos de nuvem
- Relatórios de auditoria e conformidade criados previamente, personalizados para diferentes regulamentos, a fim de demonstrar a conformidade e automatizar o fluxo de trabalho de conformidade, em ambientes locais e de nuvem

5.2 Conclusão

O software Guardium fornece uma solução abrangente para infraestruturas físicas, virtuais e em nuvem por meio de controles de segurança centralizados e automatizados em ambientes heterogêneos. O Guardium ajuda a simplificar a conformidade e reduzir o risco, além de oferecer imagens prontas para instalar para implementações de IaaS em grandes plataformas de nuvem, como IBM SoftLayer®, Microsoft Azure e Amazon Web Services, funcionando em ambientes Microsoft Windows, UNIX e Linux.

A arquitetura flexível do Guardium possibilita vários modelos diferentes de implementação. É possível escolher a arquitetura do sistema que funciona para sua empresa: Todos os componentes do Guardium podem ser implementados na nuvem ou alguns deles podem ser mantidos no local, como um gerenciador central.

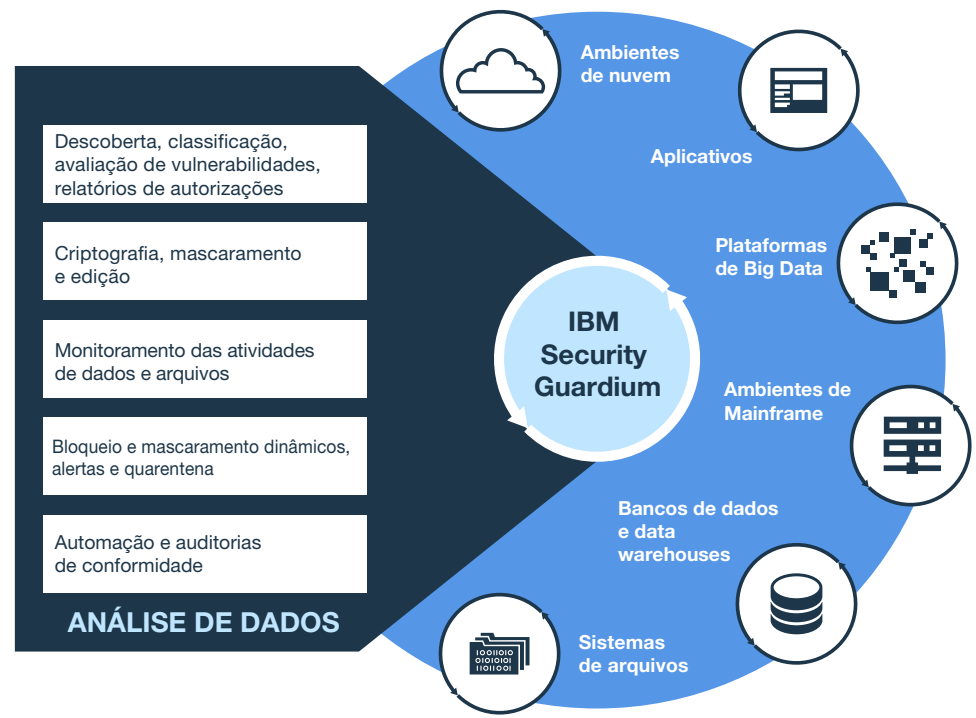


Figura 3: O Guardium fornece proteção de dados de ponta a ponta em uma grande variedade de ambientes e plataformas tecnológicas.

5.3 Conclusão

Graças a essa flexibilidade, clientes atuais podem facilmente levar sua estratégia de proteção de dados para a nuvem, sem afetar as implementações existentes.

Os coletores de monitoramento de entrada implementados na nuvem são capazes de transmitir facilmente os dados para o gerenciador central, assegurando uma única visualização consolidada das ameaças à proteção dos dados, independentemente de onde os dados residem.

Os controles de segurança que mantêm os cibercriminosos fora de um armazenamento de dados (ou que detectam rapidamente uma intrusão bem-sucedida) são ferramentas importantes. No entanto, na era dos dados portáteis, das cargas de trabalho mutáveis e da virtualização, manter os dados seguros com criptografia é igualmente importante.

As soluções da IBM para segurança de dados ajudam a proteger dados sensíveis para que as organizações possam ficar tranquilas de que seus dados estarão protegidos em ambientes virtualizados e de nuvem complexos.

5.4 Recursos adicionais

Sobre as soluções do IBM Security

O IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança corporativa. Apoiado pela pesquisa e desenvolvimento de renome mundial da IBM X-Force®, o portfólio fornece inteligência de segurança para ajudar as organizações a proteger integralmente seus funcionários, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de identidade e de acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de riscos, gerenciamento de terminais, segurança de rede e muito mais.

Essas soluções permitem que as organizações gerenciem efetivamente os riscos e implementem segurança integrada para dispositivos móveis, nuvem, mídias sociais e outras arquiteturas empresariais de negócios. A IBM opera uma das organizações mais amplas de pesquisa, desenvolvimento e fornecimento de segurança do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e detém mais de 3.000 patentes de segurança.

Para obter mais informações sobre segurança de dados, conformidade e nuvem, acesse **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, EE. UU.

Produzido nos Estados Unidos da América
Maio de 2017

1. Thomas J. Bittman, "Internal Private Cloud Is Not for Most Mainstream Enterprises," *Gartner*, 22 de maio de 2015.
2. Noel Yuhanna, "Enterprise Data Virtualization, T1 2015," *The Forrester Wave*, 11 de março de 2015.

Recicle

WGM12362-BRPT-00