IBM Security

IBM

Eliminando a complexidade do compliance regulatório

Com as ferramentas certas, o compliance pode ser um ativo valioso, não apenas um custo necessário

Tendências de regulamentações da privacidade de dados — e por que são relevantes

O medo da utilização indevida dos dados resultou em regulamentações de privacidade de dados gerais e específicas dos setores em todo o mundo que devem ser cumpridas pelas organizações, e é importante adotar suas exigências. Cada vez mais, a função das organizações detentoras de dados tem mudado para a de administradoras de informações, principalmente nos Estados Unidos e na União Europeia (UE). O não cumprimento das regulamentações pode ocasionar não apenas em danos à reputação, mas em multas significativas e, até mesmo, em prisão. No entanto, apenas cumprir as exigências de *compliance* pode não ajudar você a identificar e interromper uma violação de dados ativamente.

Avançando além das exigências regulatórias, a amplitude dos dados pessoais e confidenciais que qualquer organização detém é mais que igualada pelas ameaças que colocam essas informações em risco. Os crimes virtuais, sejam realizados por agentes internos ou por invasores externos sofisticados e mal-intencionados, têm destacado o valor inerente às informações — e os criminosos virtuais exploram as lacunas específicas que acompanham a não identificação e proteção corretas dos dados confidenciais. Mas, antes de falar sobre a segurança completa dos dados, é importante abordar primeiramente o *compliance* regulatório — e obter aprovação nas auditorias.

Este artigo examina quatro regulamentações principais, como a General Data Protection Regulation (GDPR) da UE, e descreve como as organizações podem cumpri-las com sucesso usando processos e tecnologias adequados.

Os dados... podem ser a base para fraudes financeiras devastadoras e para divulgações constrangedoras.[1]

Leia sobre 10 elementos essenciais das soluções eficazes de compliance.

1 Timothy B. Lee, "Here's how phone metadata can reveal your affairs, abortions, and other secrets", *The Washington Post*, 27 de agosto de 2013.

Como alcançar o *compliance* em um panorama regulatório dinâmico

Há muito tempo, a manutenção de registros e as declarações de privacidade dos governos e órgãos do setor em todo o mundo têm regido a forma como as organizações controlam os dados — especialmente em iniciativas de alto risco e com uso intenso de dados. Notavelmente, as áreas consideradas especialmente merecedoras de supervisão são assistência médica, seguro, controle corporativo e serviços financeiros.

As tendências recentes de regulamentações de dados, no entanto, refletem o crescente valor dos dados e o amplo ceticismo sobre a forma como as empresas os controlam. As novas regras impõem uma grande responsabilidade sobre os detentores de dados e, ao mesmo tempo, definem amplamente os indivíduos e as organizações que detêm ou controlam os dados. Como resultado, as empresas que podem ter enfrentado apenas regulamentações leves relacionadas a dados (ou nenhuma) no passado, agora, provavelmente serão responsáveis por proteger ou excluir dados que nunca criaram, ou serão obrigadas a remover dados que mantinham anteriormente.

Para cumprir com sucesso as regulamentações de controle de dados, as organizações deverão:

- **Localizar** e **classificar** registros que estejam sob seu controle e que sejam sujeitos às regulamentações
- **Avaliar** as práticas e a infraestrutura atuais, e **fortalecê-las** para cumprir as exigências técnicas e legais
- **Realizar auditorias** internamente ou para autoridades reguladoras, e **relatar** as práticas de controle de dados, bem como as violações, aos órgãos reguladores e titulares dos dados afetados, nos intervalos exigidos ou sob demanda
- **Monitorar** as transações em busca de registros auditáveis e fazer **cumprir** as políticas para investigar e reduzir violações

Expanda facilmente e avance do *compliance* à segurança dos dados

Leia sobre sobre como avaliar e fortalecer a infraestrutura do banco de dados usando o IBM® Security Guardium®.

SOX: oferecendo responsabilização, controles e divulgação

Criada no despertar de escândalos corporativos que se articularam sobre a ausência de transparência organizacional, a Lei Sarbanes-Oxley de 2002 (SOX) é uma das regulamentações mais abrangentes para empresas que fazem negócios nos EUA. A SOX é mais conhecida por suas exigências de divulgação e manutenção de registros que afetam grandes empresas de capital aberto. No entanto, ela também impõe regras de práticas corporativas que afetam empresas de todos os tipos e portes. Suas disposições são respaldadas por penalidades civis e criminais.

Com o intuito de proteger os acionistas e o público contra práticas contábeis fraudulentas e relacionamentos privilegiados não divulgados — além de aumentar a confiabilidade das declarações obrigatórias de divulgações corporativas, a SOX exige a divulgação de determinados relacionamentos e decisões de controle corporativo. Ela também requer que os resultados financeiros informados sejam certificados pela gerência sênior de uma organização. Além da certificação, a SOX necessita que, juntos, a gerência e os auditores estabeleçam controles internos e métodos de geração de relatórios sobre a precisão dos controles.

A lei também fortalece a supervisão dos conselhos de administração e estabelece penalidades criminais pela interferência no trabalho de auditores externos que analisam as demonstrações financeiras corporativas. O *compliance* com a SOX requer transparência, apoiada por uma manutenção de registros e um planejamento cuidadoso.

Regulamentações semelhantes à SOX foram aprovadas em jurisdições de todo o mundo, como em Ontário, no Canadá,[1] e no Japão.[2]

▸ Assista ao vídeo para saber mais sobre como usar o Guardium para gerenciar o *compliance* com a SOX.

1 "Keeping the Promise for a Strong Economy Act, 2002", *Assembleia Legislativa de Ontário, Canadá.*
2 "Financial Instruments and Exchange Act", Financial Services Agency of Japan.

HIPAA: mantendo confidenciais as informações privadas de saúde

Os dados de pacientes médicos dos EUA devem atender às exigências da Seção II da Health Insurance Portability and Accountability Act (HIPAA). Dentre outras disposições, a HIPAA requer um tratamento superior de privacidade para as informações protegidas de saúde (PHI, na sigla em inglês) dos consumidores por parte das seguradoras de saúde, dos provedores de serviços médicos e de outras entidades cobertas. A lei se aplica às informações individualmente identificáveis sobre as condições médicas, a assistência médica ou o pagamento de plano de saúde de uma pessoa. Suas disposições são interpretadas em termos amplos para se aplicar não só às equipes médicas e de seguro, mas a uma longa lista de provedores[1] que têm qualquer acesso aos dados de pacientes.

Embora as informações sobre pacientes possam ser usadas para fins adequados e rigidamente definidos — como a realização do tratamento médico em si — os demais usos são proibidos. Nem todos os dados individualmente identificáveis são considerados como informações protegidas de saúde, mas a capacidade cada vez mais sofisticada de correlacionar dados e metadados agregados para detectar informações pessoais confidenciais, juntamente com as fortes penalidades implicadas pela lei, significa que até mesmo os dados aparentemente inofensivos devem ser controlados como se fossem privados e confidenciais. Além dos rigorosos padrões para os dados pessoais, a HIPAA define um conjunto cada vez maior de esquemas detalhados para padronizar a transmissão eletrônica de tipos específicos de informações sobre saúde entre as entidades cobertas pela HIPAA.

As penalidades da HIPAA podem chegar a US$ 50.000 por violação, com um máximo anual de US$ 1,5 milhão.[2]

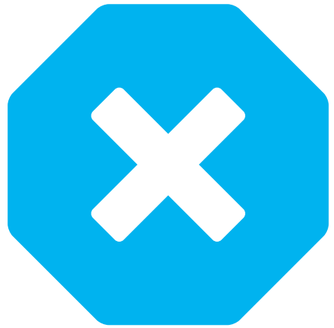
▸ Saiba mais sobre a necessidade de ir além dos padrões da HIPAA, e de proteger os dados de pacientes e de assistência médica neste vídeo curto.

1 "Emptoris Contract Management for Healthcare HIPAA Compliance", *IBM Corp., 2012.*
2 "HIPAA Violations and Enforcement", Associação Médica Americana.

PCI DSS: protegendo os dados de cartões e as transações de crédito

As transações que usam os principais cartões de crédito (como Visa, MasterCard, American Express e Discover) se enquadram no Payment Card Industry Data Security Standard (PCI DSS). Essa regulamentação estabelece uma estrutura de medidas e práticas de segurança que os estabelecimentos comerciais e outras organizações devem adotar e manter para processar cartões de crédito. O PCI DSS é um padrão patenteado administrado não por um órgão governamental, mas por um consórcio do setor, o Conselho de Normas de Segurança da Indústria de Meios de Pagamento (PCI Security Standards Council), que foi estabelecido para padronizar os padrões dos principais emissores de cartão. No entanto, as disposições do PCI DSS ou disposições quase semelhantes também foram adotadas como lei por alguns estados dos EUA. Os dados em risco nos termos do PCI DSS também podem ser cobertos separadamente pode outras regulamentações.

Embora já seja amplamente utilizado, o PCI DSS é um padrão em evolução; ele tem sido atualizado continuamente desde seu surgimento, já que as ameaças à infraestrutura de cartão de crédito aumentaram e já que as ferramentas para combater as ameaças foram aprimoradas. Para possibilitar a vigilância e acompanhar as mudanças do padrão, os estabelecimentos comerciais que lidam com dados de cartão de crédito devem ter seu *compliance* validado anualmente.



O PCI DSS v3.2 introduziu a autenticação de diversos fatores para ajudar a combater o acesso não autorizado.[1]

- Leia mais sobre como atender às exigências para *compliance* com o PCI DSS.

1 "PCI DSS 3.2: What's New?" *Conselho de Normas de Segurança da Indústria de Meios de Pagamento, 28 de abril de 2016.*

GDPR: possibilitando a privacidade dos dados além da segurança dos dados

A abrangente diretiva europeia conhecida como General Data Protection Regulation (GDPR) foi criada para realizar três tarefas fundamentais: 1) Criar uma lei unificada de proteção de dados para todos os 28 países europeus; 2) Aprimorar o nível de proteção dos dados para titulares de dados da UE; e 3) Modernizar a lei para acompanhar o ritmo das tecnologias atuais e emergentes. A legislação foi adotada em 2016 pelo Conselho Europeu, e as organizações devem cumprir as normas da GDPR até 25 de maio de 2018.

A GDPR impõe às organizações uma grande responsabilidade pela proteção dos dados pessoais de qualquer residente da UE (que vivem na área) e, se violada, ocasionará grandes penalidades. Ela exige, dentre outras coisas:

- Para grandes organizações, a contratação de um diretor dedicado de proteção de dados
- A implementação do chamado direito de eliminação (às vezes, chamado de “direito de esquecimento”), que permite a exclusão de informações pessoais armazenadas
- Sólidas medidas de segurança que protejam as informações pessoalmente identificáveis dos indivíduos, inclusive informações que poderão ser pessoalmente identificáveis se agregadas

No entanto, para compreender a GDPR, é crucial perceber que seu impacto tem um alcance muito maior que apenas a Europa. A GDPR se aplica aos dados pessoais que pertencem a qualquer pessoa que viva em solo da UE, independentemente de onde os dados sejam armazenados ou processados. Como resultado, qualquer organização (inclusive as organizações não estabelecidas na UE) que detenha dados sobre indivíduos que vivem em solo da UE, ou que comercializem a esses indivíduos, será afetada pela GDPR.

Os residentes da UE cujos dados pessoais estão sujeitos às proteções da GDPR totalizam quase 510 milhões de pessoas.[1]

Saiba mais sobre a GDPR além de cinco dicas importantes para ajudar você a iniciar a jornada da GDPR.

1 “Living in the EU”, *Europa.eu.*

Planeje sua jornada de segurança de dados

Você pode pensar no alcance da segurança como uma jornada que já está sendo seguida por sua organização. A necessidade de compliance é uma preocupação prática e legal — uma etapa importante ao longo do caminho — mas é apenas parte do todo. Realizar o *compliance* com as exigências regulatórias pode significar que sua organização evita penalidades legais, mas não garante que os criminosos virtuais não consigam uma forma de entrar em seu sistema.

A boa notícia é que as ações e o planejamento necessários para lidar com as exigências de compliance também podem oferecer um panorama sobre as ferramentas e os objetivos adequados para proporcionar uma proteção mais abrangente dos dados. Geralmente, o *compliance* regulatório está relacionado a um tipo de instantâneo da segurança específica do domínio — ela mostra que, em determinado momento, sua organização protegeu corretamente os dados dos usuários e preservou registros adequados.

Mas, como parte do cumprimento das exigências de *compliance*, as organizações precisam inspecionar todo o seu panorama de dados. Isso significa fazer perguntas com implicações de segurança que vão além de quaisquer regulamentações específicas. Quantos dados você usa ativamente, e quantos estão armazenados, mas estão em repouso? Quantas pessoas têm acesso a esses dados, e o acesso é examinado? Você sabe quando os repositórios de dados confidenciais são acessados? Equipada com esses tipos de informações, sua equipe de segurança pode implementar as práticas recomendadas para proteger os dados e os usuários, prever possíveis violações e planejar ativamente defesas e reações em caso de ocorrência de uma violação.

A jornada à proteção abrangente dos dados começa com o atendimento das necessidades imediatas de *compliance* e continua com a detecção e a classificação de informações em todo o ambiente de dados.

- Saiba mais sobre o que você precisa pensar para preparar-se para o compliance e como você poderá avançar se planejar corretamente!

Por que o *compliance* é difícil

O compliance regulatório é um monstro de muitas cabeças, o que pode dificultar dar os primeiros passos. A estratégia de *compliance* de uma organização deve considerar jurisdições sobrepostas, portabilidade de dados e responsabilidades por privacidade que mudam com frequência. Ela também deve abranger não apenas o monitoramento do acesso aos dados, mas os relatórios regulares e as trilhas de auditoria reais. Inevitavelmente, esses fatores interagem entre si. Eles afetam o provisionamento de hardware e software, os processos corporativos, as práticas de segurança, as políticas de funcionários, os relacionamentos com os clientes e muito mais.

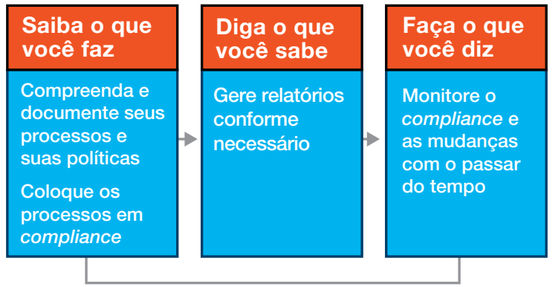
Com tantas facetas e partes interessadas a considerar, as organizações presas em modo reativo — e não em modo proativo — não conseguem fazer muito progresso em termos de *compliance*. É desafiador, mas essencial, primeiramente entender o panorama geral: o tipo de dados que você tem, onde eles estão armazenados e como eles estão sendo usados.

Em um mundo de dados portáteis, forças de trabalho geograficamente distribuídas e bases de clientes internacionais, essas são questões complicadas.

Mas, à medida que iniciar a jornada rumo ao compliance, faça estas perguntas:

- Onde estão seus dados relacionados ao *compliance*? No local, na nuvem, híbridos?
- Os aplicativos de software como serviço (SaaS) usam seus dados?
- Quais são as regulamentações aplicáveis? Sua organização é coberta por regras específicas de domínio?
- Você tem necessidades desafiadoras de rede, acesso ou fluxo de dados?

Todas as regulamentações são iguais...



A maioria das regulamentações aborda processos, controle e relatórios, não tecnologia.

Leia este blog para saber mais sobre como ter uma visão geral de seus dados e enfrentar o desafio de *compliance*.

Do que você precisa para dar início ao *compliance*

Dar os primeiros passos com ao *compliance* regulatório requer um plano abrangente. Antes, a readaptação dos registros do banco de dados e outras abordagens específicas podem ter sido etapas suficientes, mas a necessidade atual por práticas auditáveis de controle de dados significa que não vale a pena arriscar usando soluções internas. Um plano eficaz de *compliance* deve abordar diversos requisitos fundamentais com eficiência, tais como:

- **Localizar e classificar dados:** dados relevantes podem residir em um número surpreendente de fontes de dados: bancos de dados, *data warehouses*, ambientes de Big Data, arquivos e sistemas de arquivos, ambientes em nuvem e muito mais. Você deve ser capaz de detectar e classificar seus dados automaticamente.
- **Atividade de monitoramento:** o uso de uma solução de que possa monitorar padrões e atividades de acesso a dados (leitura, alteração ou exclusão de dados) permite que você estabeleça um registro do acesso e do uso; assim, poderá relatar atividades relacionadas aos dados relevantes.
- **Criar um registro auditável:** Nem todos os registros são criados da mesma forma. Os requisitos de relatórios variam entre as regulamentações, tanto em termos dos dados necessários e do formato em que os dados devem ser armazenados ou apresentados.
- **Automatizar o *compliance*:** como o *compliance* tem restrições de prazo, é importante que os relatórios e os processos de entrega sejam regulamentados e automatizados sempre que possível.
- **Fortalecer os repositórios de dados confidenciais:** classificar e monitorar os dados existentes não é o fim da história; a proteção dos repositórios de dados é uma tarefa contínua, não um evento único.

A automatização do compliance pode ajudar a simplificar a avaliação e a correção de vulnerabilidades, o monitoramento das atividades de dados, a distribuição e aprovação de relatórios, a escalação e muito mais.[1]

▸ Saiba como estabelecer a base ideal para *compliance* — uma que possa facilitar o caminho à segurança de dados.

1 "Compliance Workflow Automation", *IBM Knowledge Center.*

Primeiros passos do *compliance* com o IBM Security Guardium

Guardium é uma solução abrangente de segurança de dados; mas, como uma base, ele oferece suporte aos principais recursos necessários para simplificar e automatizar as iniciativas de *compliance*. O Guardium oferece detecção e classificação automatizadas dos dados relevantes ao *compliance*. Ele também oferece monitoramento de atividades de arquivos e dados em tempo real; assim, você sabe e pode documentar quem está lendo e alterando dados, ajudando a criar um registro auditável com o mínimo de impacto sobre a performance. Por fim, a solução ajuda você a realizar avaliações de vulnerabilidade e, depois, fortalecer suas fontes de dados para que possa demonstrar que ninguém está acessando os dados confidenciais por meio de uma "porta dos fundos".

Para ajudar a acelerar ainda mais o caminho ao *compliance*, o Guardium oferece centenas de relatórios personalizáveis e criados previamente, bem como aceleradores. Os aceleradores do Guardium, gerados a partir das necessidades e da experiência de milhares de usuários do Guardium, oferecem relatórios, políticas e grupos de uso específico para simplificar o processo de alcançar o *compliance* regulatório, abordando PCI DSS, privacidade de dados, SOX, Basel, a GDPR e muito mais. Os aceleradores ajudam sua organização a reunir e centralizar dados auditáveis rapidamente. O Guardium também automatiza os fluxos de trabalho de compliance, eliminando o tedioso trabalho manual para simplificar e acelerar o processo de análise e aprovação.

Ele ajuda as organizações a alcançar o *compliance* regulatório e, depois, a avançar além do *compliance*, chegando à segurança total dos dados.

As organizações que implementam o Guardium obtiveram um retorno sobre o investimento de 218%.[1]

- Use uma ferramenta interativa para estimar os benefícios que o Guardium pode oferecer à sua organização.

1 "The Total Economic Impact of IBM Security Guardium", *Forrester Research*, setembro de 2015.

O Guardium pode ajudar você a se tornar um defensor da segurança de dados, ultrapassando o *compliance*

Ao expandir o uso dos mesmos recursos que o Guardium oferece para dar suporte ao *compliance* (automatização da detecção e classificação de dados confidenciais, monitoramento, monitoramento do acesso aos dados confidenciais e envio de alertas em caso de comportamento anormal) e ao aplicá-los a todos os dados confidenciais do ambiente (inclusive algoritmos patenteados, registros de RH, dados de parceiros comerciais, etc.), e adicionar a capacidade de proteger dados confidenciais em repouso e em movimento por meio de bloqueio, colocação em quarentena, criptografia, mascaramento e edição de dados, sua organização poderá dar os próximos passos e proteger de fato os dados confidenciais em todo o ambiente.

O Guardium ajuda a analisar dados e riscos — detectando dados confidenciais automaticamente e revelando riscos, protegendo dados em repouso e em movimento, e adaptando-se às mudanças de TI — quer você esteja adicionando novos usuários, novos tipos e volumes de dados ou novas tecnologias. Ele oferece suporte a uma ampla variedade de fontes de dados, como mainframes, plataformas de Big Data, ambientes em nuvem, e arquivos e sistemas de arquivos. O Guardium também oferece análise de dados avançada, aprendizado de máquina e análise de dados especializada em detecção de ameaças — como a capacidade de bloquear automaticamente as injeções SQL e os procedimentos mal-intencionados armazenados — para ajudar as organizações a identificar proativamente e interromper os ataques desde o início. Não desperdice seu tempo em tentativas falhas de alcançar o *compliance*. Lide com ela, tenha sucesso e utilize sua solução e seus conhecimentos para avançar e conquistar também a segurança dos dados.

O Guardium pode oferecer controle granular do acesso, com uma interface que pode ser usada até mesmo por quem não é especialista.[1]

- Leia o artigo da Forrester, intitulado “The Total Economic Impact Of IBM Security Guardium”, para entender o ROI e os benefícios que ele oferece em termos de *compliance* e segurança de dados.

1 “Demo: Fine-grained access control with IBM Security Guardium V10” , IBM Corp., 16 de outubro de 2015.

Estudos de caso: Guardium no mundo real

As organizações estão usando o Guardium para abordar o compliance regulatório em uma grande variedade de cenários. Estas são algumas formas como os clientes da IBM estão enfrentando seus desafios de compliance:

Automatizando os relatórios de compliance

Um grande pagador de assistência médica queria monitorar seus bancos de dados essenciais em busca de invasões, além de ter acesso aos usuários internos privilegiados. Ele também precisava criar uma trilha de auditoria centralizada do banco de dados em um ambiente heterogêneo existente. A performance era fundamental; a organização queria evitar funções residentes no banco de dados, como acionadores ou registros de transação que pudessem afetar a velocidade e estabilidade do banco de dados. Igualmente importante para a empresa era criar relatórios prontos para auditoria, para fins de *compliance* com a SOX e a HIPAA. Ao implementar uma solução Guardium, a empresa conseguiu manter a alta performance de seu banco de dados e automatizar seus relatórios de *compliance*.

Impedindo violações de agentes internos

Uma empresa global com 75 milhões de clientes descobriu violações de política por agentes internos e realizou aprimoramentos em seu *compliance* com a SOX e em seu controle de dados. Essa não foi uma tarefa fácil, já que ela tinha mais de cem servidores, um número ainda maior de instâncias de banco de dados, e um ambiente multiplataformas que incluía IBM AIX®, HP-UX e Microsoft Windows. Então, a empresa adotou uma abordagem em fases — primeiramente, monitorar as atividades dos usuários privilegiados e, depois, concentrar-se em privacidade dos dados. Com uma solução baseada no Guardium, ela pode auditar mais de um milhão de sessões por dia e produzir relatórios automatizados de *compliance* com a SOX, prontos para aprovação.

O Guardium oferece suporte a fontes de dados como IBM DB2®, Oracle, Teradata, Sybase e Microsoft SQL Server, executadas em plataformas Windows, UNIX, Linux, IBM AS/400, IBM z/OS®, sistemas de arquivos, ambientes Hadoop e NoSQL, ambientes em nuvem e muito mais.[1]

▸ Saiba mais sobre como um cliente usou o Guardium para começar a proteger dados confidenciais.

1 "IBM Security Guardium Data Activity Monitor", IBM Corp., fevereiro de 2016.

Por que escolher a IBM?

Organizações de todo o mundo confiam nas soluções IBM Security para gerenciamento de identidade e acesso, soluções de proteção de dados e ferramentas para ajudar a gerenciar a *compliance* regulatório. Essas tecnologias comprovadas permitem que as organizações protejam seus recursos mais essenciais das mais recentes ameaças de segurança e demonstrem aos auditores e órgãos reguladores que cumpriram os padrões exigidos de manutenção de registros e proteção de dados.

À medida que novas ameaças e regulamentações surgem em um panorama de dados em constantes mudanças, a IBM pode ajudar as organizações a desenvolver sua principal infraestrutura de segurança com um portfólio completo de produtos, serviços e soluções de parceiros comerciais. Além disso, as soluções IBM Security podem se integrar a ambientes de terceiros, como Oracle, Microsoft e SAP, para proporcionar uma sólida proteção. As soluções IBM Security são respaldadas pelas pesquisas internacionalmente reconhecidas da X-Force, que ajudam a proteger dados e infraestruturas em produtos de hardware que variam de telefones celulares e mainframes a dispositivos de Internet das Coisas (IoT).

A IBM tem experiência em todo o mundo com um parceiro estratégico em setores altamente regulamentados, como os setores governamental, de assistência médica e de serviços financeiros. Ela permite que as organizações reduzam as vulnerabilidades de segurança e gerenciem riscos nos ambientes de TI mais complexos.

A IBM opera em uma das maiores organizações de pesquisa, desenvolvimento e entrega do mundo, monitora bilhões de eventos de segurança por dia em mais de 130 países e tem mais de 3 mil patentes de segurança.

O Guardium pode ajudar as organizações de qualquer porte a se adaptar aos ambientes regulatórios em constante evolução — em diferentes plataformas, topologias de rede e tipos de dados.

Sobre o Guardium

O Guardium oferece uma solução completa de compliance e segurança de dados para proteger dados confidenciais em todo o ambiente. Além de poder analisar os riscos, proteja os dados confidenciais e adapte-se aos dinâmicos de requisitos de TI, como a adição de novas tecnologias e novos tipos e volumes de dados. O Guardium também oferece uma profunda integração a outras ferramentas da IBM Security, como IBM QRadar®, IBM Security Privileged Identity Manager e muito mais, para ajudar a cumprir as exigências de compliance e proteger o ambiente.

Para mais informações

Para saber mais sobre as soluções IBM Security, fale com o especialista da IBM ou acesse **ibm.com**/security

Para saber mais sobre as soluções IBM Security Guardium, acesse **ibm.com**/software/products/en/ibm-security-guardiumfamiliy

Além disso, a IBM Global Financing oferece diversas opções de pagamento para ajudá-lo a adquirir a tecnologia de que você precisa para expandir sua empresa. Nós fornecemos gerenciamento completo do ciclo de vida de produtos e de serviços de TI, desde a aquisição até o descarte. Para obter mais informações, visite: **ibm.com**/financing

IBM

IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América Janeiro de 2017

WGW03244-USEN-03