Cinco armadilhas comuns a evitar na segurança de dados

Saiba como melhorar sua postura de segurança

IBM Security

Índice

A segurança de dados deve ser uma grande prioridade para as empresas, por um bom motivo.

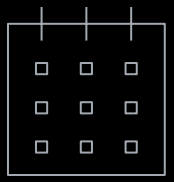
Embora o ambiente de TI esteja se tornando cada vez mais descentralizado e complexo, é importante entender que muitas violações de segurança são evitáveis. Os desafios e as metas individuais de segurança podem diferir de empresa para empresa. No entanto, as organizações frequentemente cometem os mesmos erros generalizados quando começam a lidar com a segurança de dados. Além disso, muitos líderes empresariais costumam aceitar esses erros como prática normal de negócios.

Muitos fatores internos e externos podem levar a ataques cibernéticos de sucesso, tais como:

- Erosão dos perímetros de rede
- Maiores superfícies de ataque oferecidas por ambientes de TI mais complexos
- As demandas crescentes que os serviços de nuvem impõem às práticas de segurança
- A natureza cada vez mais sofisticada dos crimes cibernéticos
- Escassez persistente de habilidades de segurança cibernética
- Falta de consciência dos funcionários a respeito dos riscos de segurança de dados

US$ 8,19 milhões

Custo médio de uma violação de dados nos Estados Unidos em 2019[1]



245 dias

Tempo médio para identificar e conter uma violação de dados nos Estados Unidos[1]

Sua prática de segurança de dados é forte?

Vamos dar uma olhada nos cinco erros mais prevalentes (e evitáveis) na segurança de dados que podem tornar as organizações vulneráveis a possíveis ataques — e como você pode evitá-los.

Acelerar a conformidade

Centralizar a segurança

Estabelecer a responsabilidade

Avaliar as vulnerabilidades

Priorizar as atividades

Armadilha nº 1

Deixar de ir além do compliance

Compliance e segurança não são necessariamente equivalentes. As organizações que usam seus recursos limitados de segurança para cumprir uma auditoria ou certificação podem se tornar complacentes. Muitas violações de dados grandes aconteceram em organizações que, no papel, possuíam o compliance adequado. Os exemplos a seguir mostram como se concentrar exclusivamente no compliance pode diminuir a eficácia da segurança:

Cobertura incompleta
Muitas vezes, as empresas se esforçam para corrigir configurações incorretas de banco de dados e políticas de acesso desatualizadas antes de uma auditoria anual. As avaliações de vulnerabilidades e riscos devem ser atividades contínuas.

Esforço mínimo
Muitas empresas adotam soluções de segurança de dados para cumprir os requisitos jurídicos ou de um parceiro de negócios. Essa mentalidade de "vamos implementar um padrão mínimo e voltar aos negócios" pode ir contra as boas práticas de segurança. Uma segurança de dados eficaz é uma maratona, não uma corrida de velocidade.

Urgência que diminui
As empresas poderão se tornar complacentes no gerenciamento de controles quando regulamentos, como a Lei Sarbanes-Oxley (SOX) e o Regulamento Geral de Proteção de Dados (RGPD), amadurecerem. Com o passar do tempo, os líderes podem dar menos atenção à privacidade, à segurança e à proteção de dados regulamentados. Entretanto, os riscos e os custos associados à falta de compliance permanecem.

1,4 por dia

Estimativa de 1,4 violação de dados de saúde por dia em 2019, apesar da legislação da Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA).[2]

Omissão de dados não regulamentados
Ativos, como propriedade intelectual, poderão colocar sua organização em risco se forem perdidos ou compartilhados com pessoal não autorizado. Concentrar-se apenas no compliance pode fazer com que as organizações de segurança negligenciem e não protejam suficientemente dados importantes.

Solução

Reconhecer e aceitar que o compliance é um ponto de partida, não a meta

As organizações de segurança de dados precisam estabelecer programas estratégicos que protejam consistentemente seus dados críticos, em vez de apenas responder a requisitos de compliance.

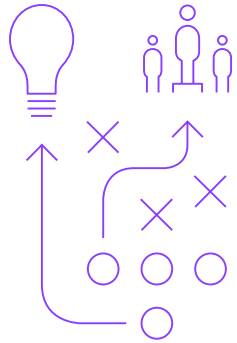
Os programas de segurança e proteção de dados devem incluir estas práticas principais:

- **Descobrir e classificar dados sensíveis** em repositórios de dados locais e na nuvem.
- **Avaliar o risco** com informações contextuais e análise.
- **Proteger dados sensíveis** por meio de criptografia e políticas flexíveis de acesso.
- **Monitorar padrões de acesso e uso de dados** para detectar atividades suspeitas rapidamente.
- **Responder a ameaças** em tempo real.
- **Simplificar o compliance** e os relatórios.

O elemento final pode incluir responsabilidades legais relacionadas ao compliance regulatória, possíveis perdas que uma empresa pode sofrer e os custos em potencial dessas perdas além das multas por falta de compliance.

Por fim, você deve pensar de forma holística sobre o risco e o valor dos dados que deseja proteger.

Veja o compliance como uma oportunidade de inovar e eleve seus padrões de segurança para dar suporte aos seus negócios.



Armadilha nº 2

Deixar de reconhecer a necessidade de uma segurança de dados centralizada

Sem obrigações mais amplas de compliance que abrangem a privacidade e a segurança de dados, os líderes da organização podem se esquecer da necessidade de uma segurança de dados consistente para toda a empresa.

No caso de empresas com ambientes de multicloud híbrida, que mudam e crescem de maneira constante, novos tipos de fontes de dados podem aparecer semanal ou diariamente e dispersar consideravelmente os dados sensíveis.

Os líderes de empresas que estão crescendo e expandindo suas infraestruturas de TI podem não reconhecer o risco representado pela superfície de ataque em transformação. É possível que não tenham a visibilidade e o controle adequados conforme seus dados sensíveis se movimentam em um ambiente de TI cada vez mais complexo e desigual. A falta de adoção de controles de privacidade, segurança e proteção de dados de ponta a ponta (especialmente dentro de ambientes complexos) pode acabar sendo um lapso muito caro.

A utilização de soluções de segurança em silos pode causar problemas adicionais. Por exemplo, organizações com uma solução de gerenciamento de eventos e informações de segurança (SIEM) e centro de operações de segurança (SOC) podem deixar de alimentar esses sistemas com informações obtidas com a solução de segurança de dados. Da mesma maneira, a falta de interoperabilidade entre profissionais, processos e ferramentas de segurança pode impedir o sucesso de qualquer programa de segurança.

Criptografia, gerenciamento da continuidade de negócios, integração da segurança no processo de desenvolvimento de software (DevSecOps) e compartilhamento de inteligência sobre ameaças podem ajudar a diminuir os custos da violação de dados.[1]

Solução

Saber onde residem seus dados sensíveis, incluindo repositórios locais e hospedados em nuvem

A proteção de dados sensíveis deve ocorrer em conjunto com esforços de segurança mais amplos. Além de entender onde seus dados sensíveis estão armazenados, você precisa saber quando e como estão sendo acessados, mesmo que tais informações mudem rapidamente. Você também deve trabalhar para integrar informações e políticas de seu programa de segurança geral, para possibilitar uma comunicação fortemente alinhada entre as tecnologias. Uma solução de segurança de dados que atue em ambientes e plataformas distintos pode ajudar nesse processo.

Qual é o momento certo para integrar a segurança de dados com outros controles de segurança como parte de uma prática de segurança mais holística? Estes são alguns sinais que sugerem que sua organização pode estar pronta para dar o próximo passo:

Risco de perder dados de valor
O valor dos dados pessoais, sensíveis e particulares da sua organização é muito significativo. A perda deles causaria danos significativos para a viabilidade da sua empresa.

Implicações regulatórias
Sua organização coleta e armazena dados com requisitos legais, como números de cartão de crédito, outras informações de pagamento ou dados pessoais.

A proteção de dados sensíveis deve ocorrer em conjunto com esforços de segurança mais amplos.

Falta de supervisão de segurança
Sua organização cresceu a um ponto em que é difícil monitorar e proteger todos os endpoints da rede, incluindo instâncias de nuvem. Por exemplo, você tem uma ideia clara de onde, quando e como os dados estão sendo armazenados, compartilhados e acessados em seus repositórios de dados locais e em nuvem?

Avaliação inadequada
Sua organização adotou uma abordagem fragmentada em que não há uma compreensão clara de exatamente o que está sendo gasto em todas as atividades de segurança. Por exemplo, você tem processos em vigor que meçam com precisão o retorno sobre o investimento (ROI) em termos dos recursos alocados para reduzir o risco de segurança de dados?

Caso alguma dessas situações se aplique à sua organização, considere a possibilidade de adquirir as habilidades e soluções de segurança necessárias para integrar a segurança de dados em sua prática de segurança mais ampla existente.

Armadilha nº 3

Deixar de definir quem detém a responsabilidade pelos dados

Mesmo quando estão cientes da necessidade de segurança de dados, muitas empresas não têm nenhuma pessoa especificamente responsável por proteger os dados sensíveis. Muitas vezes, essa situação se torna aparente durante um incidente de auditoria ou segurança de dados, quando a organização está sob pressão para descobrir quem é o verdadeiro responsável.

Os altos executivos podem procurar o diretor de informações (CIO), que talvez diga: "Nosso trabalho é manter os principais sistemas funcionando. Fale com alguém da equipe de TI". Os funcionários de TI podem ser responsáveis por vários bancos de dados em que residem dados sensíveis e, no entanto, não possuir um orçamento de segurança.

Em geral, os membros da organização do diretor de segurança da informação (CISO) não são diretamente responsáveis pelos dados que atravessam a empresa como um todo. É possível que deem conselhos aos diferentes gerentes de linhas de negócios (LOB) dentro de uma empresa. Porém, em muitas empresas, ninguém é explicitamente responsável pelos dados propriamente ditos. Para uma organização, os dados estão entre os ativos de mais valor. Mas, sem responsabilidade, proteger dados sensíveis de forma adequada se torna um desafio.

74%

das organizações entrevistadas dizem que a falta de habilidades de segurança cibernética afetou a organização.[3]

"Em 2018, 67,9% das empresas entrevistadas afirmaram que têm um diretor de dados (CDO). Entretanto, a função não é bem definida."[4]

Relatório da NewVantage
Big Data and AI Executive Survey
2019, Executive Summary of Findings

Leia o estudo →

Solução

Contratar um CDO ou DPO dedicado ao bem-estar e à segurança de ativos de dados sensíveis e críticos

Em ambientes complexos de TI, é essencial responsabilizar-se pelos dados nos seguintes locais:

Compartilhados entre unidades de negócios

Localizados em infraestruturas de multicloud híbrida

Armazenados em dispositivos móveis

Um diretor de dados (CDO) ou diretor de proteção de dados (DPO) pode cumprir tais obrigações. Na realidade, empresas com sede na Europa ou que fazem negócios com proprietários de dados da União Europeia enfrentam ordens do RGPD que exigem que tenham um DPO. Esse pré-requisito reconhece que dados sensíveis (no caso, informações pessoais) têm um valor que vai além da LOB que usa os dados. Além disso, o requisito enfatiza que as empresas tenham uma função especificamente criada para ser responsável pelos ativos de dados. Considere os seguintes objetivos e responsabilidades na hora de escolher um CDO ou DPO:

Conhecimento técnico e tino comercial
Avalie o risco e crie um argumento prático que líderes de negócios não técnicos possam entender a respeito dos investimentos adequados em segurança.

Implementação estratégica
Direcione um plano em nível técnico que aplique controles de detecção, resposta e segurança de dados para oferecer proteções.

Liderança em compliance
Entenda os requisitos de compliance e saiba como mapeá-los em relação aos controles de segurança de dados para que sua empresa esteja em compliance.

Monitoramento e avaliação
Monitore o ambiente de ameaças e mensure a eficácia do programa de segurança de dados.

Flexibilidade e ajuste de escala
Saiba quando e como ajustar a estratégia de segurança de dados, como expandir políticas de acesso e uso de dados em novos ambientes por meio da integração de ferramentas mais avançadas.

Divisão do trabalho
Defina as expectativas com os provedores de serviços de nuvem a respeito de acordos de nível de serviço (SLAs) e responsabilidades associadas a risco e remediação de segurança de dados.

Plano de resposta à violação de dados
Por fim, prepare-se para exercer uma função importante na elaboração de um plano estratégico de mitigação e resposta à violação.

O CDO ou o DPO deve, em última análise, liderar a colaboração para segurança de dados em diferentes equipes e em toda a empresa, pois todos precisam trabalhar juntos para proteger os dados corporativos de modo eficaz. Essa colaboração pode ajudar o CDO ou DPO a supervisionar os programas e proteções de que sua organização precisa para ajudar a proteger os dados sensíveis.

Armadilha nº 4

Deixar de lidar com as vulnerabilidades conhecidas

Muitas vezes, violações de destaque em empresas resultaram de vulnerabilidades conhecidas que ficaram sem correção, mesmo após a liberação de correções. A falta de correção rápida de vulnerabilidades conhecidas coloca os dados da sua organização em risco, uma vez que os criminosos cibernéticos procuram ativamente esses pontos fáceis de entrada.

Entretanto, muitas empresas sentem dificuldade para implementar correções rapidamente por causa do nível de coordenação necessária entre os grupos de TI, segurança e operações. Além disso, as correções frequentemente precisam de testes para ver se não interrompem ou processo ou introduzem uma nova vulnerabilidade.

Em ambientes de nuvem, às vezes é difícil saber se um componente de serviço ou aplicativo contratado deve ser corrigido. Mesmo se uma vulnerabilidade for encontrada em um serviço, os usuários muitas vezes não terão controle sobre o processo de remediação do provedor de serviços.

51%

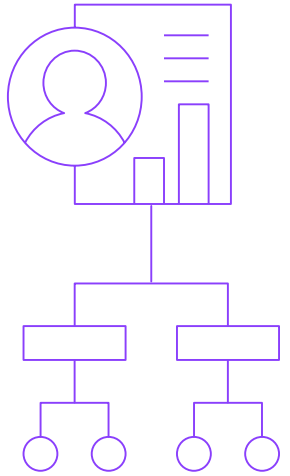
das violações registradas em 2019 foram causadas por ataques mal-intencionados. Ataques mal-intencionados são a causa mais comum e cara de violações.[1]

Solução

Estabelecer um programa eficaz de gerenciamento de vulnerabilidades com a tecnologia adequada para dar suporte ao crescimento dele

Em geral, o gerenciamento de vulnerabilidades envolve algum dos níveis de atividade a seguir:

- Manter um inventário exato e um estado de referência para seus ativos de dados.
- Realizar varreduras e avaliações de vulnerabilidades frequentes em toda a sua infraestrutura, incluindo ativos de nuvem.
- Priorizar uma remediação de vulnerabilidades que considere a probabilidade de a vulnerabilidade ser explorada e o impacto que o evento teria na sua empresa.
- Incluir o gerenciamento de vulnerabilidades e a capacidade de resposta como parte do SLA com provedores de serviços terceiros.
- Ocultar dados sensíveis ou pessoais sempre que possível. Criptografia, tokenização e edição são três opções para atingir esse objetivo.
- Utilizar um gerenciamento adequado de chaves de criptografia, garantindo que as chaves de criptografia sejam armazenadas de modo seguro e movidas adequadamente para manter os dados criptografados em segurança.



Mesmo com um programa maduro de gerenciamento de vulnerabilidades, nenhum sistema será perfeito. Presumindo que intrusões podem acontecer mesmo nos ambientes mais bem protegidos, seus dados necessitam de outro nível de proteção. O conjunto certo de técnicas e recursos de criptografia de dados pode ajudar a proteger seus dados de ameaças novas e emergentes.

Armadilha nº 5

Deixar de priorizar e utilizar o monitoramento das atividades de dados

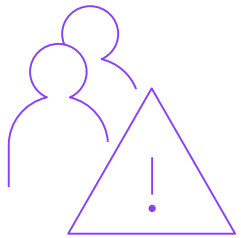
Monitorar o acesso e o uso de dados é uma parte essencial de qualquer estratégia de segurança de dados. O líder de uma organização precisa saber como e quando as pessoas estão acessando os dados, bem como quem são essas pessoas. Tal monitoramento deve considerar se essas pessoas devem ter acesso, se o nível de acesso está correto e se ele representa um risco elevado para a empresa.

Identificações de usuários privilegiados costumam ser culpadas em casos de ameaças internas.5 Um plano de proteção de dados deve incluir monitoramento em tempo real para detectar contas de usuários privilegiados usadas em atividades suspeitas ou não autorizadas. Para evitar possíveis atividades mal-intencionadas, uma solução precisa realizar estas tarefas:

- Bloquear atividades suspeitas e colocá-las em quarentena, com base em violações de políticas.
- Suspender ou encerrar sessões com base em comportamentos anômalos.
- Usar fluxos de trabalho predefinidos, de regulamentos específicos, em diferentes ambientes de dados.
- Enviar alertas acionáveis a sistemas de TI, segurança e operações.

O custo médio global de uma ameaça interna é

US$ 11,45 milhões.[6]



Levar em conta as informações relacionadas ao compliance e de segurança de dados, além de saber quando e como responder a possíveis ameaças, pode ser muito difícil. Com usuários autorizados acessando várias fontes de dados, incluindo bancos de dados, sistemas de arquivos, ambientes de mainframe e ambientes de nuvem, monitorar e salvar dados de todas essas interações pode parecer algo excessivo. O desafio está em monitorar, capturar, filtrar, processar e responder de maneira eficaz a um enorme volume de atividades de dados. Sem um plano adequado em vigor, sua organização pode ter mais informações sobre atividades do que consegue razoavelmente processar. Isso diminui o valor do monitoramento das atividades de dados.

Solução

Desenvolver uma estratégia abrangente de detecção e proteção de dados

Para esse fim, ao iniciar uma jornada de segurança de dados, você precisa dimensionar e definir o escopo dos esforços de monitoramento se quiser lidar adequadamente com os requisitos e riscos. Essa atividade envolve, muitas vezes, a adoção de uma abordagem em fases que possibilita melhores práticas de desenvolvimento e ajuste de escala na empresa. Além disso, é essencial conversar com as principais partes interessadas nas áreas de negócios e TI ainda no início do processo, para entender os objetivos de negócios a curto e longo prazo.

Essas conversas também devem capturar a tecnologia que será necessária para dar suporte às iniciativas principais. Por exemplo, se a empresa estiver planejando montar escritórios em uma nova região usando uma combinação de repositórios de dados locais e hospedados em nuvem, sua estratégia de segurança de dados deve avaliar como esse plano afetará a postura de compliance e segurança de dados da organização. Se, por exemplo, os dados de propriedade da empresa passarem a estar sujeitos a novos requisitos de conformidade e segurança de dados, como o RGPD, o Lei de Privacidade do Consumidor da Califórnia (CCPA), a Lei Geral de Proteção de Dados (LGPD) do Brasil etc.

Você também deve priorizar e se concentrar em uma ou duas fontes que provavelmente terão os dados mais sensíveis. Confira se suas políticas de segurança de dados são claras e detalhadas para essas fontes antes de levar as práticas para o restante da infraestrutura.

O custo médio total de uma violação de dados foi

95% maior

em organizações sem automação de segurança implementada em 2019.[1]

US$ 5,16 milhões **sem automação**.[1]

US$ 2,65 milhões **com automação totalmente implementada**.[1]

Procure uma solução automatizada de monitoramento de atividades de arquivos ou dados, com uma análise rica que possa se concentrar nos principais riscos e em comportamentos incomuns por parte de usuários privilegiados. É essencial receber alertas automatizados quando uma solução de monitoramento de atividades de arquivos ou dados detectar um comportamento anormal. Entretanto, você também deve ser capaz de agir rapidamente em caso de descoberta de anomalias ou desvios em relação às suas políticas de acesso a dados. As ações de proteção devem incluir bloqueio ou mascaramento dinâmico de dados.

Enquanto você desenvolve seus planos de proteção e monitoramento das atividades de dados, muitas vezes é útil refletir sobre estas perguntas:

- Quais são minhas duas fontes de dados mais sensíveis?
- Quais são as cinco a dez fontes de dados que devo priorizar em seguida, com base no volume de dados sensíveis?
- Alguns endpoints ou ativos de nuvem estão associados a dados de maior risco?
- Dados sensíveis estão se movendo livremente entre ambientes locais, híbridos e de nuvem?
- Quais usuários devem ter acesso à fonte de dados e em quais condições?
- Quais usuários de alto risco ou contas privilegiadas precisam ser desativados ou necessitam de um exame mais minucioso?
- Minha solução de segurança de dados dá suporte a recursos de monitoramento de atividades em tempo real e proteção automatizada de dados?
- Há monitoramento em tempo real para rastrear dados em arquivos que residem em repositórios de dados, tais como bancos de dados Structured Query Language (SQL), distribuições do Hadoop, plataformas Not Only SQL (NoSQL) e assim por diante.
- Minha solução de monitoramento contempla repositórios de dados distribuídos em ambientes de multicloud híbrida e permite que eu gere relatórios personalizados que sejam enviados às pessoas certas, no momento certo?
- Tenho os recursos de análise de risco e monitoramento filtrado de que preciso para priorizar os esforços de risco, vulnerabilidades e remediação de forma eficaz?

Quanto mais específico você for sobre as prioridades de monitoramento e os requisitos de proteção, mais eficaz será a solução em termos de aplicação dos recursos disponíveis de detecção e resposta?

Quais são os próximos passos?

Como é possível evitar essas cinco armadilhas comuns de segurança de dados, especialmente à medida que mais empresas buscam ambientes de multicloud híbrida? Para começar, reconheça o problema e prepare sua organização para adotar uma abordagem proativa e holística de proteção de dados, independentemente de onde eles residem.

Caso sua empresa tenha um ambiente de TI híbrido e complexo, você não pode se dar ao luxo de usar uma abordagem de segurança de dados em silos. Precisa adicionar estratégias de proteção de dados que cubram a infraestrutura de dados por inteiro e deem suporte a todos os tipos de dados.

Os próximos passos imediatos que você pode dar para proteger os dados de valor da sua organização incluem:

- Criar uma estratégia de segurança de dados que dê suporte aos objetivos de tecnologia e negócios de curto e longo prazo da organização
- Implementar essa estratégia com as pessoas, os processos e as ferramentas certos
- Planejar seus recursos para garantir que o programa de compliance e segurança de dados possa ser ampliado de maneira eficaz conforme a organização adota tecnologias modernas

A plataforma de proteção de dados IBM® Security Guardium® foi desenvolvida para ajudar as organizações a adotar uma abordagem mais inteligente e adaptável para proteger dados críticos, onde quer que residam. Descubra por que ela pode ser a escolha certa para sua organização.

Saiba mais em ibm.com/guardium.

>4 semanas

A maioria das organizações reconhece o valor da Guardium em menos de um mês.[7]

Por que escolher a IBM Security?

A IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança empresarial. 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 aplicativos. Ele oferece soluções para gerenciamento de identidade e de acesso, segurança de banco de dados, desenvolvimento de aplicativos, 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 opera em uma das maiores organizações de pesquisa, desenvolvimento e entrega do mundo, monitorando mais de

60 bilhões

de eventos de segurança por dia em mais de 130 países.

A IBM detém mais de 3.700 patentes de segurança

Para obter mais informações sobre IBM Security, visite o nosso site.

Dê o próximo passo

Entre em contato com nosso especialista que o ajudará a superar os desafios de segurança cibernética.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América
Abril de 2020

1 "Cost of a Data Rreach report 2019." *IBM Security*. databreachcalculator.mybluemix.net/executive-summary

2 "Healthcare Data Breach Statistics." *HIPAA Journal*. www.hipaajournal.com/healthcare-data-breach-statistics

3 Jon Oltsik. "The Life and Times of Cybersecurity Professionals 2018." *Enterprise Strategy Group and Information Systems Security Association International*, April 2019. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 NewVantage Report, "Big Data and AI Executive Survey 2019 Executive Summary of Findings." *NewVantage Partners*, 2019. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. "Why Privileged Account Management Is Key to Preventing Insider Threats." *Security Intelligence*, June 20, 2018. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 "Cost of Insider Threats: Global Report 2020." *Ponemon Institute*, 2020. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

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

SEL03144-BRPT-02