Microsoft

hypothesis

Índice de segurança de dados

tendências, insights
e estratégias para proteger dados

Prefácio

Em uma época sendo definida por uma explosão de dados, tornou-se cada vez mais claro que os dados de uma organização são nada menos do que sua força vital. A grande quantidade de dados criados e usados pelas organizações alimenta operações críticas, embasa a tomada de decisão estratégica e global e molda as possibilidades para seus futuros. Os dados não são apenas um recurso, são a força motriz das empresas modernas.

No entanto, com essa maior dependência dos dados vem a dura realidade de que as vulnerabilidades nas sombras digitais são reais e se expandem rapidamente. Ameaças cibernéticas, violações de dados e incidentes de riscos internos não são mais ocorrências raras; elas são difundidas e estão escalando, representando riscos para organizações que dependem dos dados. Dos tomadores de decisão que entrevistamos recentemente, 89% disseram que veem sua postura de segurança de dados como crítica para o sucesso geral.

Neste white paper, embarcamos em uma exploração desse imperativo fundamental: a proteção dos dados da sua organização. Minha equipe e eu estamos entusiasmados em compartilhar nossas descobertas com você e esperamos iniciar um diálogo sobre como continuar a impulsionar a segurança de dados coletivamente em direção à excelência. Nossas aprendizagens exemplificam como a segurança de dados está em um momento decisivo, enquanto os tomadores de decisão de segurança concordam que isso é essencial para a segurança de seus dados e a maioria diz estar confiante no que está fazendo, ao mesmo tempo, eles estão enfrentando uma infinidade de incidentes e desafios de segurança de dados. E 80% dos líderes com quem conversamos reconheceram que uma abordagem integrada de melhor solução do pacote é superior às soluções pontuais, mas a maioria das empresas ainda estão usando um sistema fragmentado de várias ferramentas para proteger seus dados, o que muitas vezes resulta em mais incidentes de segurança, em vez de menos.

Fique à vontade para ler e compartilhar este relatório mais recente e tratá-lo como o início de novas conversas com nossas equipes sobre como podemos ajudar melhor a proteger nosso futuro coletivo.

Rudra Mitra
Vice-presidente corporativo
Conformidade e Segurança de Dados da Microsoft

Introdução

A prevenção de violações de dados e outros incidentes de segurança continua a ser uma preocupação constante dos tomadores de decisão de segurança e risco, e um pilar de qualquer programa de segurança cibernética, pois uma única violação pode causar danos significativos à reputação e às finanças. As organizações têm a tarefa de proteger uma ampla gama de dados confidenciais, incluindo informações de funcionários e clientes, propriedade intelectual, previsões financeiras e dados operacionais.

Para entender as práticas e tendências atuais de segurança de dados, bem como identificar oportunidades para as organizações aprimorarem a segurança de dados, a Microsoft encomendou a uma agência de pesquisa independente, o Hypothesis Group, a realização de uma pesquisa multinacional entre mais de 800 profissionais de segurança de dados. Este relatório apresenta cinco conclusões principais da pesquisa, incluindo tendências, insights e estratégias para proteger dados.

Principais conclusões

1

Os tomadores de decisão acham que estão protegidos, mas a realidade não corresponde às percepções.

Embora a maioria dos tomadores de decisão digam estar satisfeitos e confiantes com suas soluções de segurança de dados, eles ainda estão enfrentando uma média de 59 incidentes de segurança de dados por ano, com impactos dispendiosos.

2

Ter mais ferramentas não significa maior segurança ou eficiência de dados, é o oposto.

80% dos tomadores de decisão concordam que as soluções abrangentes e integradas são superiores às soluções manuais e consideradas as melhores da categoria, contudo, a abordagem das organizações para as ferramentas continua a ser fragmentada, usando uma média de mais de 10 ferramentas de segurança de dados. Mas aqueles com mais ferramentas também enfrentam mais incidentes de segurança de dados, sugerindo que quanto maior a proliferação de ferramentas, mais fraca será a segurança.

3

As organizações continuam a ser atormentadas pelo estresse de incidentes de segurança de dados externos e internos, especialmente em dados de negócios.

50% das organizações entrevistadas sofreram um ataque de ransomware ou malware no último ano, e muitos tomadores de decisão não acreditam que sua organização esteja totalmente preparada para prevenir e abordar os futuros ataques. Internamente, pessoas internas mal-intencionadas são uma das principais preocupações. Além disso, as organizações estão altamente preocupadas com a vulnerabilidade de seus dados de negócios. Isso novamente ressalta a necessidade de uma plataforma de segurança que aborde os riscos de forma abrangente.

Principais conclusões

4

As organizações precisam da nuvem e da IA para promover a transformação digital, mas elas também são os locais de dados mais vulneráveis.

As aplicações de nuvem e a tecnologia de IA tornaram-se essenciais para a colaboração e a produtividade das organizações. No entanto, essa evolução também criou riscos mais dinâmicos e multifacetados. À medida que as organizações adotam a IA, o aprimoramento da segurança de dados para permitir o uso responsável e seguro torna-se fundamental.

5

A automação e a IA são caminhos promissores de maior proteção.

As organizações querem que suas equipes gastem menos tempo na detecção e mais tempo na prevenção. A automação pode permitir que as equipes se concentrem mais em medidas proativas, enquanto o uso da IA para segurança de dados ajuda as organizações a serem mais estratégicas e ficarem mais espertas em relação às futuras ameaças.

1

Os tomadores de decisão acham que estão protegidos, mas a realidade não corresponde às percepções.

Os tomadores de decisão acham que estão protegidos, mas a realidade não corresponde às percepções.

Na superfície, os tomadores de decisão projetam altos níveis de confiança e satisfação com suas soluções de segurança de dados. A maioria das organizações concordam que seus controles de segurança de dados são suficientes para impedir que os dados sejam violados, elas sentem que sabem onde a maioria de seus dados residem e que podem detectar a maioria dos riscos em torno dos dados.

Ao mesmo tempo, as organizações continuam a enfrentar um volume substancial de incidentes de segurança de dados, uma média de 59 nos últimos 12 meses, sendo que um quinto deles é considerado "grave". O impacto desses incidentes é generalizado, pois, em média, as organizações estimam que o custo financeiro total de seu incidente de segurança de dados mais grave é de cerca de USD 244 mil, o que significa que os incidentes anuais podem custar até USD 15 milhões. Além desses custos, quatro em cada dez tomadores de decisão também dizem que o custo operacional para se recuperar de um incidente de segurança de dados e a perda de negócios decorrente dos danos à reputação são uma grande preocupação.

Ademais, 92% enfrentam desafios, principalmente nas áreas de custo, integração e tempo de implementação, o que inibe sua capacidade de investir mais em segurança de dados, ressaltando a necessidade de soluções mais econômicas e eficientes no trabalho.

A percepção de confiança na preparação para a segurança de dados difere da realidade dos incidentes que as organizações estão enfrentando. Embora seja importante para as organizações saber onde os dados estão localizados e detectar riscos, essas medidas de forma individual ou separada não são suficientes para ajudar as organizações a evitar os incidentes que tiram o sono dos tomadores de decisão de risco e segurança de dados.

Como diz um CISO (diretor de segurança da informação) em serviços financeiros: "Não posso dizer ao meu conselho administrativo 'Cuidei dos dados, apenas não os protegi'... a última coisa que queremos ver é nosso banco falhando na primeira página do Wall Street Journal."

59

Número médio de incidentes de segurança de dados nos últimos 12 meses

ATÉ

USD 15 mi

Custo anual de incidentes de segurança graves

2

Ter mais ferramentas não significa maior segurança ou eficiência de dados, é o oposto.

Ter mais ferramentas não significa maior segurança ou eficiência de dados, é o oposto.

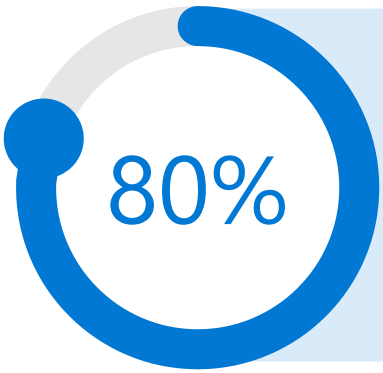
As organizações estão percebendo que anos de uma abordagem de soluções pontuais criaram lacunas na visibilidade e na eficiência devido às ferramentas de segurança de dados em silos. Essa tendência agora está dando lugar ao desejo de ter uma solução integrada para a segurança de dados, com 80% concordando que uma plataforma de segurança de dados abrangente com soluções integradas é superior ao uso de várias soluções consideradas as melhores da categoria que precisam ser integradas e gerenciadas manualmente.

No entanto, embora a grande maioria considere as soluções integradas superiores, o uso de ferramentas de segurança de dados é prolífico e fragmentado.

Como resultado, as organizações relatam o uso de 10 ferramentas de segurança de dados em média para abordar os riscos à segurança de dados, incluindo Prevenção contra Perda de Dados, Proteção de Informações, Gerenciamento de Riscos Internos, Gerenciamento de Eventos e Informações de Segurança (SIEM), Agente de Segurança de Acesso à Nuvem e muito mais. Para organizações com mais de 5.000 funcionários, o número médio de ferramentas é ainda maior.

Ter mais ferramentas pode estar criando uma falsa sensação de segurança, pois aqueles que usam mais ferramentas (mais de 16) sentem mais confiança em sua postura de segurança de dados em comparação com aqueles que usam menos ferramentas (61% vs. 56%).

No entanto, a pesquisa contradiz essa sensação de segurança, pois as organizações com 16 ou mais ferramentas também enfrentaram mais incidentes de segurança de dados no ano passado, uma média de 133, em comparação com 48 incidentes para organizações com menos ferramentas.

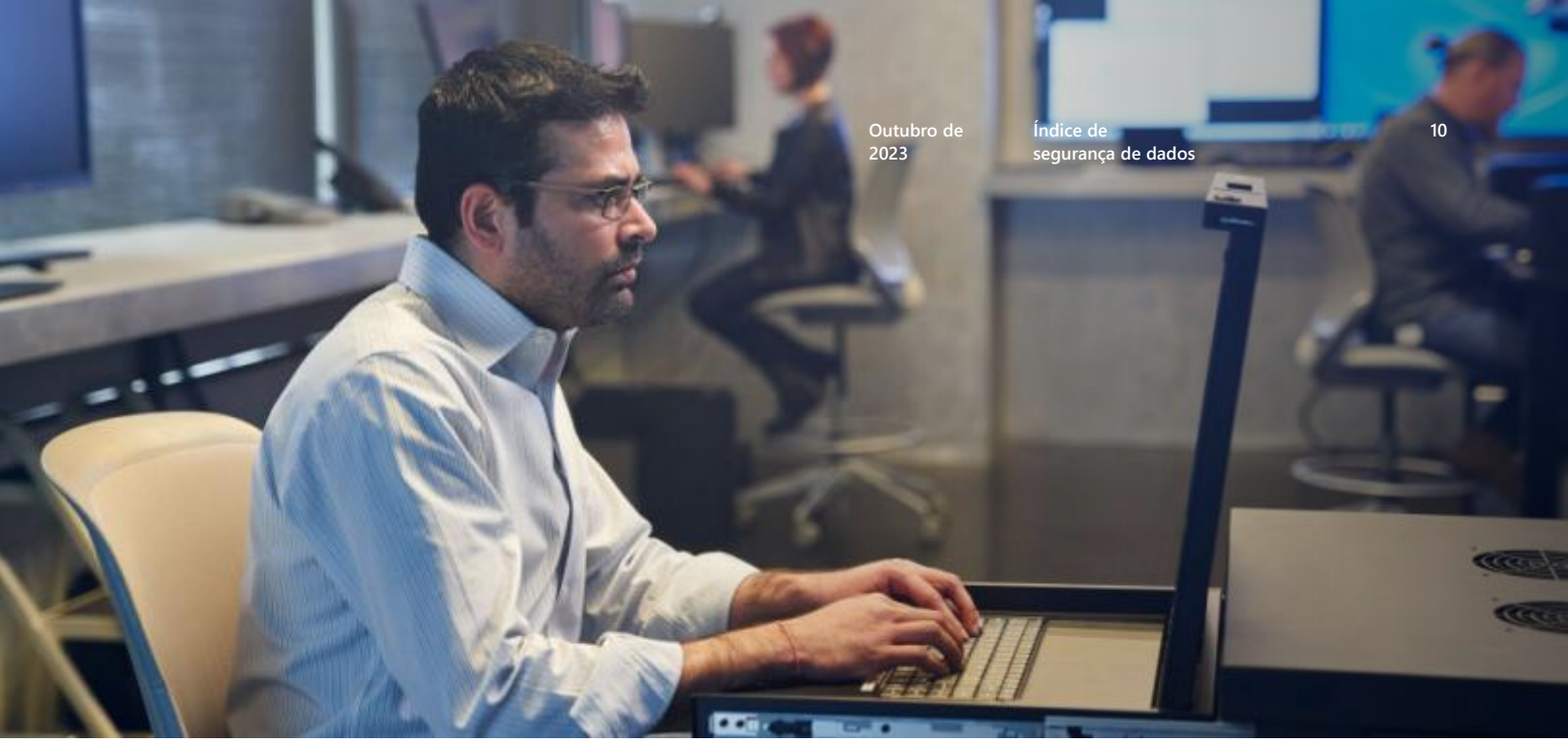


Concordam que uma plataforma de segurança abrangente com soluções integradas é superior ao uso de várias soluções consideradas as melhores da categoria que precisam ser integradas e gerenciadas manualmente.

2,8x

Mais incidentes de segurança de dados no ano passado

Para organizações com 16 ou mais ferramentas (em comparação com organizações com menos ferramentas)



A defesa de uma maior segurança de dados por meio de soluções mais integradas e menos ferramentas torna-se ainda mais robusto ao analisar os sentimentos e as práticas daqueles que preferem as melhores soluções da categoria ou mais ferramentas.

"Como os dados serão coletados, agregados e usados de vários sistemas? Muitos pontos de dados diferentes precisam ser reunidos em um ecossistema para que ele realmente funcione. Caso contrário, você terá uma versão de queijo suíço da segurança de dados."

VP de TI
Manufatura/Produção

Em primeiro lugar, várias ferramentas de segurança de dados diferentes podem levar a lacunas na visibilidade e mais dados de sombra. Na verdade, aqueles que se preocupam com dados de sombra são mais propensos a preferir as melhores soluções da categoria. Isso provavelmente ocorre porque as organizações com uma abordagem de melhor solução da categoria precisam se esforçar mais para obter uma visibilidade abrangente de sua postura de segurança de dados.

Em segundo lugar, o gerenciamento de soluções em silos traz mais complexidade para as equipes de segurança de dados, pois cada solução diferente requer uma equipe dedicada, instalação e manutenção de agentes de ponto de extremidade e vários novos processos. Tome a revisão e a triagem de alertas, uma das tarefas que precisam de funcionários e recursos, como exemplo. Um número crescente de alertas significa esforços extras exigidos das equipes de segurança de dados ao gerenciar soluções isoladas. As organizações com mais ferramentas recebem uma média de 96 alertas de segurança de dados por dia, enquanto as equipes com menos ferramentas recebem menos da metade dessa quantidade, com 44. Além disso, elas não são capazes de examinar tantos alertas quanto as equipes com menos ferramentas (61%, em comparação com 68%). Isso muitas vezes também resulta em organizações com mais ferramentas serem mais reativas em comparação com organizações que usam um volume menor de ferramentas.

Por fim, mais ferramentas também indicam que as organizações devem empregar um grande esforço para integrar insights e planos de correção, e as informações podem se perder na tradução. Em relação aos principais desafios da segurança de dados, o custo de implementação ou manutenção das soluções de segurança de dados e os desafios da integração de soluções de segurança de dados são classificados como os dois primeiros.

Isso se traduz em processos mais longos e mais lentos, com 37% dos que usam 16 ou mais ferramentas relatando a necessidade de um mês ou mais para concluir uma investigação de segurança de dados em comparação com apenas 21% daqueles com menos ferramentas.

"No momento, estamos engatinhando. Cada um dos sistemas que temos, todos eles têm seus próprios portais, suas próprias ferramentas, suas próprias maneiras de lidar com as coisas. Cada pessoa segue seu próprio caminho, no qual é especialista. Depois, todos se reúnem e decidem o que está acontecendo, e nós cuidamos da questão a partir daí. Portanto, é um trabalho manual neste momento", afirmou um diretor de infraestrutura e operações em manufatura e produção.

Em última análise, ao optar por continuar com várias soluções, as organizações estão ignorando seu próprio discurso sobre entender que as soluções integradas são superiores e caminhando na direção oposta, custando-lhes tempo e dinheiro.

RESULTADOS DAQUELES QUE USAM MENOS (<16) VERSUS MAIS (16+) FERRAMENTAS DE SEGURANÇA DE DADOS	Baixo volume de ferramentas	Alto volume de ferramentas
Número de **incidentes de segurança de dados** nos últimos 12 meses	**48**	**133**
Proporção de incidentes de segurança de dados **graves**	**19%**	**26%**
Nossa estratégia de segurança de dados atual é mais **reativa**	**31%**	**40%**
Desafios com a **integração** de soluções	**24%**	**39%**
A equipe de segurança de dados gasta a maior parte do tempo em **resposta**	**19%**	**26%**
Estamos **confiantes** com a nossa postura de segurança de dados	**56%**	**61%**
Número de alertas **recebidos** por dia, em média	**44**	**96**
Proporção de alertas que podemos **examinar** por dia	**68%**	**61%**
É necessário um mês ou mais para concluir uma investigação de segurança de dados	**21%**	**37%**

3

As organizações continuam a ser atormentadas pelo estresse de incidentes de segurança de dados externos e internos, especialmente em dados de negócios.

As organizações continuam a ser atormentadas pelo estresse de incidentes de segurança de dados externos e internos, especialmente em dados de negócios.

Como os fatores em torno dos dados, incluindo as pessoas que interagem com os dados, as atividades relacionadas aos dados e os dispositivos e aplicativos usados para processar os dados, estão constantemente evoluindo, incidentes de segurança de dados e violações de dados podem ocorrer a qualquer hora e em qualquer lugar. E essas ameaças vêm de invasores externos e também de pessoal de confiança, incluindo funcionários, prestadores de serviços e parceiros. Seja de forma mal-intencionada ou inadvertida, todos os envolvidos podem causar incidentes de segurança de dados, o que significa que há uma necessidade constante de proteção em uma infinidade de áreas.

Um VP de TI em serviços financeiros disse: "A ameaça contra a qual você está tentando se proteger está sempre mudando. É um alvo em movimento. Sempre estará evoluindo, mudando e será flexível. O que você está protegendo e onde isso reside só vai ficar mais variado."

Embora os incidentes de segurança de dados possam vir de várias fontes, a ameaça externa de incidentes de malware ou ransomware, instâncias em que o software mal-intencionado se infiltra em um sistema fornecendo aos invasores acesso não autorizado a sistemas ou redes, é de longe a mais comum, com 50% das organizações entrevistadas tendo enfrentado pelo menos um incidente no ano passado.

Além disso, esses ataques são onde as organizações se sentem mais vulneráveis, com 41% dizendo que se sentem menos preparadas para lidar com futuros ataques de malware ou ransomware no próximo ano. Essa sensação de vulnerabilidade é ainda maior entre aqueles que preferem uma abordagem de melhor solução da categoria, 44% se sentem despreparados para um ataque dessa natureza, em comparação com apenas 36% daqueles que preferem uma solução integrada.

Proteger-se contra e prevenir os riscos internos também é uma prioridade para os tomadores de decisão. 35% dizem que precisam fortalecer as defesas contra pessoas internas mal-intencionadas e contas comprometidas, e um terço estão preocupados com incidentes internos inadvertidos. Embora os incidentes internos mal-intencionados não sejam a principal causa de violações de segurança de dados, eles são o segundo tipo mais comum de incidentes que os tomadores de decisão se sentem menos preparados para evitar.

"Pelo menos uma vez por mês, recebo uma chamada de um diretor em pânico... 'tivemos um evento, descobri um evento, ou a equipe de ameaças descobriu um evento.' Alguns deles não são intencionais, outros ocorrem porque as pessoas não sabem ou entendem o que seus privilégios permitem."

CISO do Governo dos EUA

Pessoas internas são indivíduos confiáveis que normalmente recebem acesso a, ou possuem conhecimento de, recursos, dados ou sistemas da empresa que não estão disponíveis para o público em geral. Consequentemente, os riscos à segurança de dados associados às pessoas internas tendem a ser mais elusivos e difíceis de detectar. Como Bret Arsenault, o CISO da Microsoft, indicou: "Em última análise, não importa se a violação foi intencional ou acidental. Programas de riscos internos devem fazer parte da estratégia de segurança de todas as empresas."

RESUMO DOS INCIDENTES DE SEGURANÇA DE DADOS

Causas de incidentes de segurança de dados	Incidentes mais comuns nos últimos 12 meses	Menor preparação para prevenir nos próximos 12 meses
Malware ou ransomware	50%	41%
Contas comprometidas	38%	35%
Ataques de negação de serviço (DoS)	35%	33%
Pessoas internas negligentes	32%	29%
Pessoas internas inadvertidas	31%	32%
Pessoas internas mal-intencionadas	31%	35%
Propriedade física	29%	29%

As soluções de segurança de dados que as organizações escolhem também devem funcionar para uma variedade de dados confidenciais, incluindo dados de negócios de alto valor, dados operacionais e dados pessoais. Durante incidentes de segurança de dados nos últimos 12 meses, 74% das organizações tiveram dados de negócios expostos, 65% tiveram dados operacionais comprometidos e 58% viram dados pessoais se tornarem vulneráveis. Entre os vários tipos de dados, propriedade intelectual, TI e design de rede e PII foram comprometidos ou expostos com mais frequência.

Olhando para o futuro, 77% das organizações percebem os dados de negócios, como a propriedade intelectual e o código-fonte, como os mais vulneráveis. Isso ocorre principalmente porque os dados de negócios desempenham um papel crucial no estabelecimento de vantagens competitivas e geração de receita. No entanto, identificar e classificar esses dados pode ser desafiador, pois o reconhecimento tradicional de padrões, a expressão regular ou a tecnologia de correspondência de funções podem não identificar de forma eficaz o conteúdo que carece de formatos de cadeia de caracteres ou palavras-chave específicos. Por sua vez, as organizações precisam de tecnologias mais avançadas para ajudar a descobrir e proteger esses dados confidenciais vulneráveis.

TIPOS DE DADOS EM MAIOR RISCO NOS PRÓXIMOS 12 MESES

77% **Dados de negócios**		64% **Dados operacionais**		63% **Dados pessoais**	
Propriedade intelectual	**30%**	TI e design de rede	**29%**	Informações de Identificação Pessoal (PII)	**31%**
Código-fonte	**28%**	Demonstrações financeiras	**18%**	Informações de recursos humanos (folha de pagamento, currículo etc.)	**21%**
Planos de negócios	**27%**	Relatórios de vendas e receita	**15%**	Dados da indústria de cartões de pagamento (PCI)	**18%**
Segredos comerciais	**24%**	Compras e faturas	**12%**	Informações de Saúde Protegidas (PHI)	**18%**
Arquivos de fusão e aquisição	**20%**	Documentos legais/ contratos	**12%**	Credenciais	**17%**
Especificações de construção	**18%**	Processos de manufatura/ arquivos em lotes	**11%**		

4

As organizações precisam da nuvem e da IA para promover a transformação digital, mas elas também são os locais de dados mais vulneráveis.

As organizações precisam da nuvem e da IA para promover a transformação digital, mas elas também são os locais de dados mais vulneráveis.

A colaboração por meio de aplicações e plataformas de nuvem, combinada com a nova tecnologia de IA, aumenta significativamente a produtividade dos funcionários e permite arranjos de trabalho flexíveis, tornando as aplicações de nuvem e a tecnologia de IA essenciais para as organizações. Em média, as organizações agora utilizam 147 serviços de nuvem pública que abrangem SaaS, PaaS e IaaS.[1] E 66% das organizações desenvolveram uma estratégia de IA, com 36% já implementando-a.[2] No entanto, essa evolução criou riscos mais dinâmicos e multifacetados, devido à dificuldade de definir claramente os limites de dados entre vários ambientes.

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. Pesquisa de IA de segurança de dados da Microsoft, Hypothesis, março de 2023

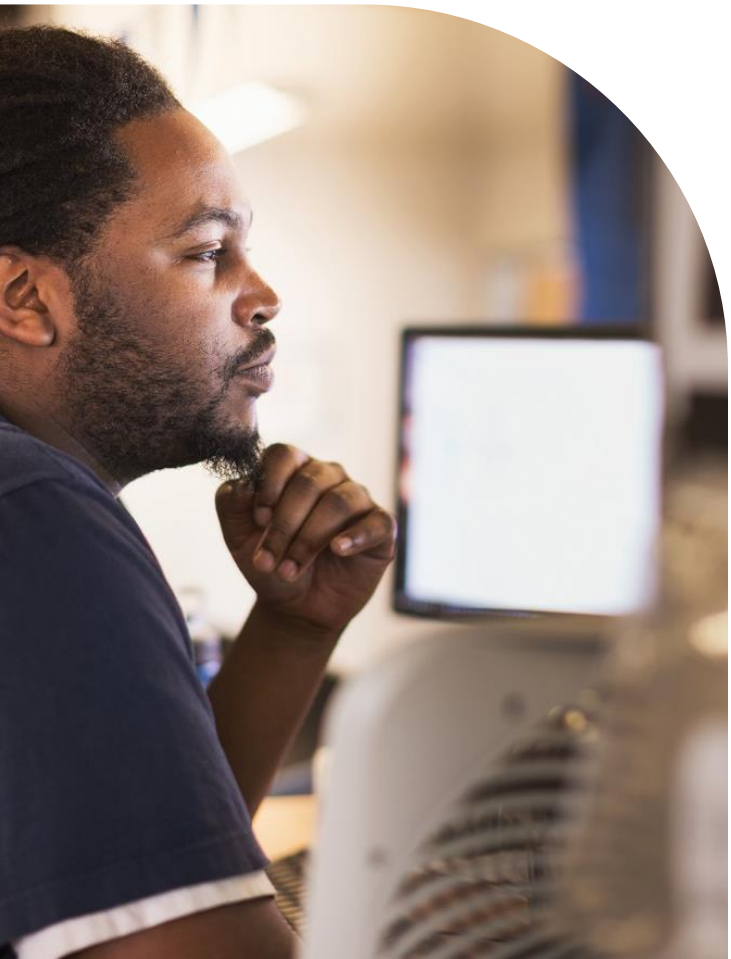
Agora é ainda mais crucial ter a solução de segurança de dados certa para esses locais de dados de alta produtividade. Nos últimos 12 meses, 42% das organizações relataram incidentes de segurança no armazenamento na nuvem e 31% em emails, mensagens instantâneas ou ferramentas de reunião online. Os incidentes parecem ser mais comuns onde há mais produtividade e colaboração.

O gerenciamento desses tipos de incidentes exige recursos, e 79% das organizações relatam que sua equipe de segurança de dados precisa de mais pessoas para gerenciar efetivamente as responsabilidades de segurança de dados críticas. No entanto, entre as organizações que afirmam precisar de mais pessoas, a maioria (57%) prefere uma abordagem de melhor solução da categoria. Essa preferência destaca que as organizações que usam mais soluções podem ter mais dificuldade para identificar os verdadeiros riscos entre as inúmeras atividades dos usuários.

RESUMO DOS LOCAIS DE DADOS

Locais de dados	Comprometimento nos últimos 12 meses	Em maior risco
Armazenamento na nuvem (por exemplo, Box, OneDrive, Google Drive)	42%	54%
Emails/Mensagens instantâneas/Ferramentas de reunião online	31%	39%
Plataforma como Serviço (PaaS)	29%	34%
Infraestrutura como Serviço (IaaS)	28%	36%
IA (por exemplo, ChatGPT, Bard etc.)	27%	38%
Data lakes/bancos de dados baseados em SaaS	27%	41%
Pontos de extremidade/dispositivos	25%	36%
Bancos de dados/compartilhamentos de arquivos/repositórios na infraestrutura local	24%	28%
Dados de sombra	21%	23%
Aplicações de linha de negócios	17%	25%
Ferramentas para desenvolvedores	16%	23%

Com mais de um terço das organizações implementando uma estratégia de IA, e mais a caminho, a IA está sendo adotada a um ritmo sem precedentes, com muito mais rapidez do que a adoção da nuvem e do email no passado. À medida que as organizações adotam a IA, o aprimoramento da segurança de dados para permitir o uso responsável e prevenir riscos torna-se essencial. A IA é considerada um dos principais locais de risco para incidentes de segurança de dados, em comparação com outros locais, e 27% das organizações sofreram uma violação de segurança de dados de IA. As preocupações da organização com os riscos do uso da IA estão centradas na falta de controle sobre os dados compartilhados com a IA, na falta de controles para detectar e mitigar o uso arriscado da IA, na falta de transparência sobre como os modelos de IA generativa são treinados e no vazamento de informações confidenciais por meio da IA.



"A IA é boa para produtividade e eficiência, mas oferece riscos potenciais a segurança e dados", afirmou o tomador de decisão de segurança de uma empresa.

Embora existam preocupações relacionadas à IA, os tomadores de decisão também podem ver o potencial, especialmente porque os fornecedores no mercado estão desenvolvendo inovações para ajudar a capacitar as empresas por meio do uso da IA responsável. No entanto, para utilizar ainda mais a IA, as organizações relatam os principais controles necessários para detectar conteúdo mal-intencionado ou arriscado na IA, criptografar, mascarar ou anonimizar dados antes que eles possam ser carregados para a IA e identificar dados confidenciais gerados pela IA.

OS 5 PRINCIPAIS CONTROLES DE SEGURANÇA DE DADOS NECESSÁRIOS PARA A IA

1. **Detectar conteúdo mal-intencionado ou arriscado** na IA
2. **Criptografar, mascarar ou anonimizar dados** antes que eles possam ser carregados para a IA
3. **Identificar dados confidenciais** gerados pela IA
4. **Impedir que dados confidenciais sejam carregados** para a IA
5. **Detectar manipulação de modelos ou dados** na IA

5

A automação e a IA são caminhos promissores de maior proteção.

A automação e a IA são caminhos promissores de maior proteção.

Em um mundo ideal, sem restrições baseadas em prioridades organizacionais ou orçamentos, metade das organizações gostariam de ser mais proativas em relação ao gerenciamento de segurança de dados, gastando mais tempo em tarefas como a descoberta de dados confidenciais e os riscos associados a isso e a prevenção de incidentes de segurança de dados. Atualmente, no entanto, mais da metade das organizações gastam mais tempo concentrando-se em medidas reativas, como detecção de incidentes, resposta e investigações. E essa detecção e resposta a incidentes de segurança de dados é demorada. A maioria das organizações levam cerca de um mês para resolver um incidente de segurança de dados e, para algumas, a resolução pode levar até seis meses.

O benefício da adoção de uma estratégia mais proativa é evidente, pois as organizações entrevistadas que são mais proativas já enfrentam incidentes de segurança de dados menos dispendiosos, têm maior probabilidade de conseguir investigar esses incidentes em menos de um mês e são mais propensas a acreditar que seus controles de defesa são suficientes para evitar violações de dados.

Embora as organizações estejam cientes de que medidas proativas de segurança de dados podem ajudar a reduzir os riscos à segurança de dados, elas não estão progredindo na implementação dessas medidas. Por exemplo, aquelas que buscam ser mais proativas alocando mais tempo para a prevenção são mais propensas a escolher as melhores soluções da categoria, que exigem maiores esforços no tratamento de medidas reativas ao reunir sinais de detecção e controles de resposta.

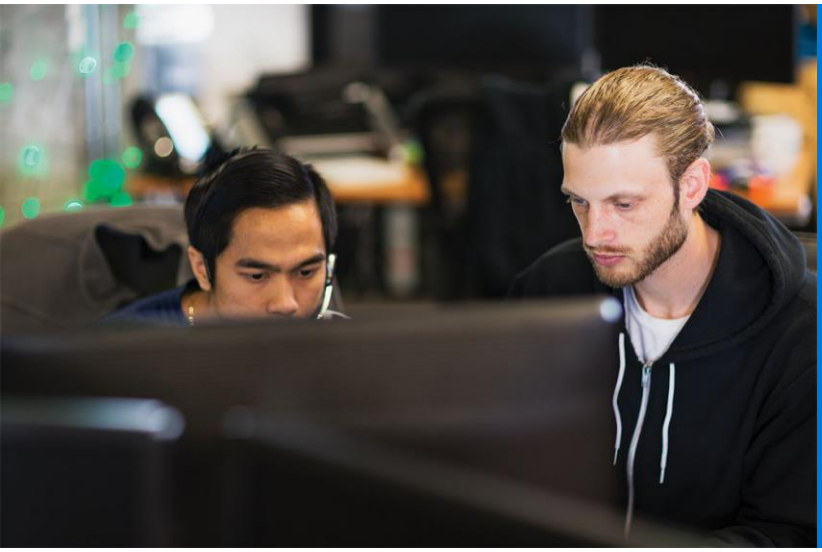
RESULTADOS DE ORGANIZAÇÕES QUE SÃO MAIS PROATIVAS VS. REATIVAS

	Mais proativas	Mais reativas
Impacto médio de custo de um incidente de segurança de dados nos últimos 12 meses	**USD 207 mil**	**USD 330 mil**
Conclusão de uma investigação de segurança de dados em menos de um mês, em média	**80%**	**68%**
Controles de defesa suficientes para evitar violações de dados	**77%**	**68%**

Como os recursos e os funcionários são limitados e a alocação de esforço entre as atividades pode não ser ideal, as organizações estão procurando tecnologias para ajudá-las a reservar mais tempo para atividades proativas. A automação é uma maneira de as organizações ganharem tempo para uma abordagem mais proativa à segurança de dados. 74% das organizações entrevistadas prefeririam uma mitigação de riscos semi ou totalmente automatizada, que permite às equipes de segurança minimizar o impacto de possíveis incidentes de segurança de dados de forma antecipada em comparação com análises manuais. Além disso, as organizações reconhecem muitas outras tarefas que poderiam se beneficiar da automação, como a criação de relatórios de segurança de dados, a automação do fluxo de trabalho de gerenciamento de incidentes e a resposta e a investigação de incidentes. A maioria das principais tarefas que as equipes de segurança desejam automatizar são medidas reativas. Ao automatizar essas tarefas, as organizações podem aliviar a carga sobre suas equipes de segurança de dados, permitindo que elas adotem uma postura mais proativa.

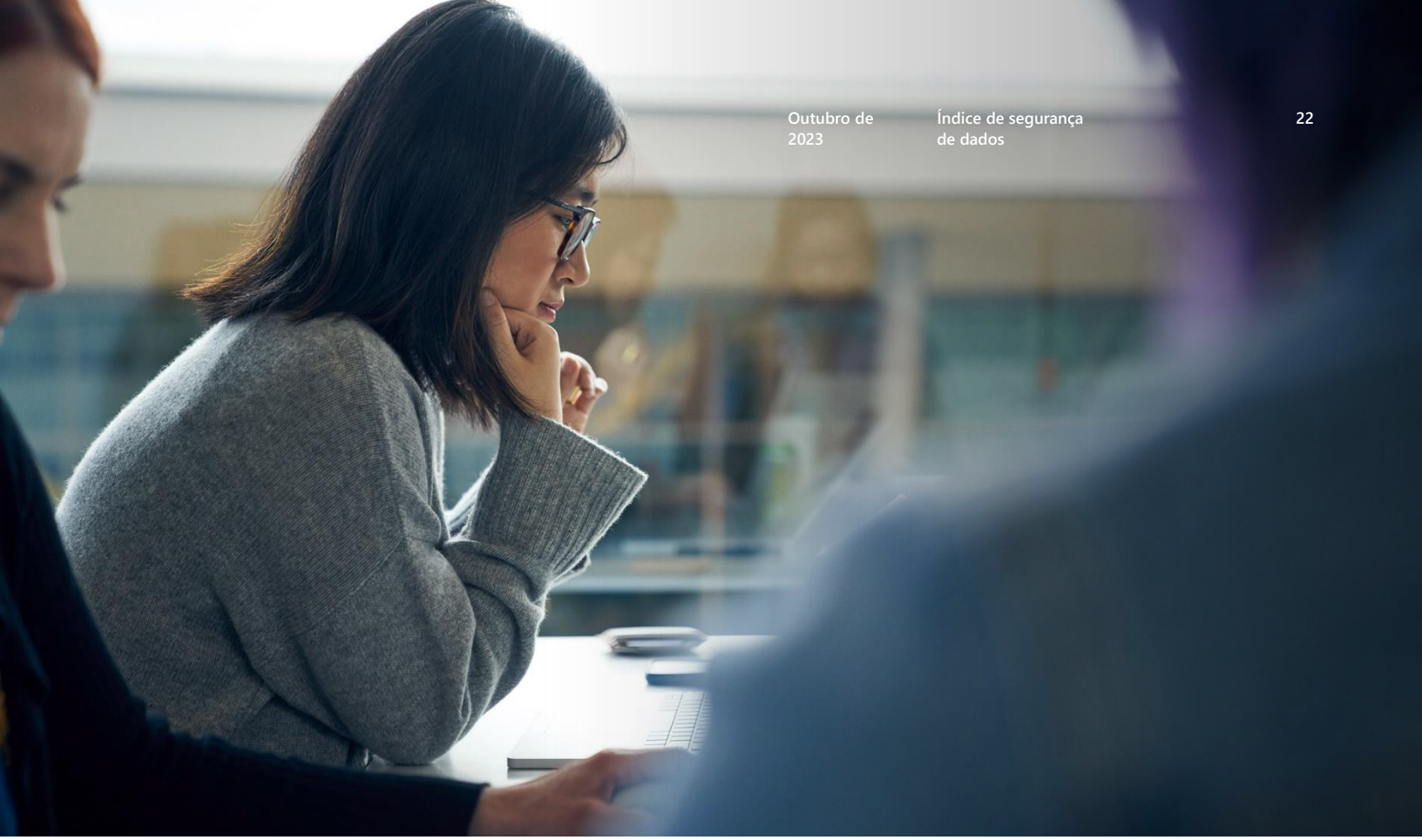
AS 5 PRINCIPAIS ÁREAS QUE AS EQUIPES DE SEGURANÇA DE DADOS PREFEREM AUTOMATIZAR/ALIVIAR

Reativa	1	Criação de fluxos de trabalho automatizados para gerenciamento e resposta a incidentes
	2	Criação de relatórios de segurança de dados
Reativa	3	Resposta e contenção de incidentes de segurança de dados
	4	Encaminhamento de incidentes para as equipes certas (por exemplo, SOC, jurídica, RH) durante as investigações
	5	Investigação de incidentes de segurança de dados



"Há muitos dados arriscados para avaliar manualmente. A IA pode ajudar a acelerar os tempos de resposta da nossa equipe e proteger os dados, pois não temos recursos suficientes."

Tomador de decisão de segurança do Reino Unido



O uso da IA para segurança de dados também pode ajudar as organizações a serem mais estratégicas e ficarem mais espertas em relação a futuras ameaças. A tecnologia acelera a resposta a incidentes detectados, ganhando tempo para os profissionais de segurança de dados investigarem mais. De forma semelhante à automação, as organizações citam muitos cenários em que a IA pode ajudar a fornecer uma segurança mais robusta, **economizando assim o tempo de sua equipe**. Os principais cenários de uso da IA incluem bloquear automaticamente o compartilhamento inadequado de dados, detectar riscos críticos à segurança de dados/atividades de dados anômalas e investigar possíveis incidentes de segurança de dados.

Ao aproveitar os benefícios da IA e da automação e avançar em direção a soluções mais integradas, as organizações podem adotar uma estratégia de segurança de dados mais proativa e se preparar para um futuro mais seguro.

PRINCIPAIS CENÁRIOS EM QUE A IA É USADA

Bloqueio automático do compartilhamento inadequado de dados

Detecção de riscos críticos à segurança de dados/atividades de dados anômalas

Recomendações para proteger melhor seu ambiente de dados

Investigação de possíveis incidentes de segurança de dados

Ajuste de políticas de segurança de dados

Recomendações finais

- Adotar uma plataforma integrada para fortalecer a postura de segurança de dados
- Proteger-se contra incidentes de segurança de dados de fora para dentro e de dentro para fora com uma abordagem de defesa em profundidade
- Atualizar suas estratégias de segurança de dados com a IA e a automação

Adotar uma plataforma integrada para fortalecer a postura de segurança de dados

De acordo com as conclusões desta pesquisa, menos soluções podem trazer mais segurança. Pode parecer contraintuitivo, mas as organizações devem combater a falsa sensação de confiança que surge de uma infinidade de soluções isoladas. A consolidação de fornecedores oferece uma abordagem estratégica que não só reduz os custos, mas também aprimora a segurança.

Os tomadores de decisão de segurança de dados podem iniciar essa transformação capacitando suas equipes a dedicar mais tempo a trabalhos estratégicos, como pesquisa e planejamento de novos controles de segurança e otimização de políticas de segurança, algo que 84% dos tomadores de decisão concordam que desejam fazer. Esse processo envolve a substituição de soluções em silos herdadas, que muitas vezes são consideradas "as melhores da categoria", mas não conseguem se integrar de forma eficaz a outras ferramentas.

Os tomadores de decisão podem promover uma estreita colaboração com suas equipes para estabelecer indicadores-chave de performance (KPIs) e metas para o programa de segurança de dados. Eles podem então progredir definindo os requisitos da solução e identificando os recursos não negociáveis. Essa abordagem permite que eles identifiquem os fornecedores capazes de oferecer ferramentas que se alinhem com seus objetivos abrangentes. Crucialmente, ela promove uma mentalidade inovadora e ajuda as equipes a evitar a fixação excessiva em práticas existentes ou casos de uso isolados, permitindo que implementem as mudanças necessárias em direção a uma abordagem mais integrada.

Uma plataforma de segurança de dados integrada deve capacitar as equipes de segurança a realizar todas estas tarefas críticas facilmente:

1. Descobrir e proteger dados confidenciais dentro de seu cenário digital.
2. Detectar riscos críticos associados a esses dados.
3. Evitar o uso não autorizado de dados confidenciais sem afetar atividades comerciais legítimas.

Ao implementar uma estratégia de segurança de dados integrada, as organizações podem alcançar um nível mais elevado de proteção e, ao mesmo tempo, simplificar sua infraestrutura de segurança.

Proteger-se contra incidentes de segurança de dados de fora para dentro e de dentro para fora com uma abordagem de defesa em profundidade

Os incidentes de segurança de dados geralmente resultam de invasores externos, pessoas internas mal-intencionadas ou pessoas internas inadvertidas. As organizações devem tomar medidas para proteger seus dados, impedindo o acesso não autorizado de ameaças externas e mitigando os riscos de roubo interno ou exposição acidental dos dados.

Para enfrentar esses desafios, as organizações podem adotar uma abordagem de defesa em profundidade para a segurança de dados. Essa estratégia é análoga à proteção de obras de arte inestimáveis de um museu: câmeras de segurança de ponta equipadas com inteligência contra ameaças monitoram visitantes, sistemas de ingressos gerenciam identidades e acessos ao museu e medidas de segurança rigorosas em torno das obras de arte operam de forma semelhante aos controles de segurança de dados que protegem seus dados valiosos. Essas medidas desencorajam possíveis incidentes, sejam eles provenientes de agentes mal-intencionados externos ou indivíduos já dentro do ambiente da organização.

Combater os riscos à segurança de dados em evolução requer um esforço conjunto em toda a organização para implementar essa estratégia de defesa em profundidade. A colaboração da equipe de segurança de dados com outros departamentos, como o Centro de Operações de Segurança (SOC), pode otimizar o investimento em segurança de dados. Notavelmente, 66% das organizações que se consideram proativas interagem com sua equipe de SOC, em comparação com 54% que não interagem.

Como o trabalho em equipe entre equipes de segurança, as soluções de segurança de dados também devem integrar-se perfeitamente a outros sistemas, como soluções de Detecção e Resposta Estendida (XDR) ou Gerenciamento de Identidades e Acesso (IAM), para evitar de forma eficaz os incidentes de segurança de dados de fontes externas e internas. Essas integrações permitem que as organizações realizem investigações abrangentes e respostas a incidentes de segurança, obtendo uma compreensão completa dos dados, agentes e atividades afetados e respondendo com vários controles de mitigação. Consequentemente, isso permite que elas implementem respostas embasadas, precisas e imediatas para minimizar o impacto de possíveis incidentes de segurança.

Atualizar suas estratégias de segurança de dados com a IA e a automação

A automação e a IA podem ajudar as organizações a serem mais proativas na segurança de dados. Veja algumas recomendações para sua organização embarcar na jornada de automação e IA:

- Descobrir dados confidenciais: utilize a IA para ajudar a identificar dados confidenciais e aplicar políticas de proteção, incluindo criptografia e gerenciamento de direitos. Isso é particularmente valioso para dados de negócios que podem representar desafios para a detecção por meio de tecnologias tradicionais de reconhecimento de padrões. As organizações podem aproveitar tecnologias de classificação, como machine learning ou classificadores habilitados por IA, conhecidas por sua inteligência e capacidade de localizar rapidamente conteúdo confidencial com base no contexto de dados ou na categoria de negócios. Como alternativa, as organizações podem empregar tecnologias de correspondência exata de dados para descobrir dados operacionais ou pessoais.

  Além disso, à medida que os regulamentos da indústria evoluem (por exemplo, GDPR, HIPAA ou PCI DSS) e o cenário de dados se torna mais dinâmico, é crucial possuir uma tecnologia de classificação avançada que seja personalizável e facilmente adaptável para identificar novas categorias de dados confidenciais.

- Detectar riscos críticos à segurança de dados: aproveite o poder da IA para identificar riscos críticos associados aos seus dados confidenciais e alocar recursos estrategicamente para lidar com possíveis incidentes de alto risco. As tecnologias de IA podem gerar alertas de alta fidelidade, permitindo que as equipes de segurança economizem um tempo valioso que, de outra forma, seria gasto examinando uma abundância de falsos positivos. Além disso, a IA pode ajudar as organizações a identificar riscos elusivos, especialmente quando agentes mal-intencionados tentarem evitar a detecção. É imperativo utilizar a velocidade das máquinas para superar esses agentes de ameaça.

- Evitar incidentes de segurança de dados dinamicamente: use a IA e a automação para adaptar seus controles de prevenção e mitigação de forma automática com base nos riscos avaliados, permitindo uma estratégia de segurança de dados mais adaptável e proativa. Quando as soluções habilitadas por IA detectam e avaliam riscos, os controles de prevenção automatizados podem se envolver com rapidez para proteger os dados, aplicando controles de mitigação precisamente às áreas de alto risco. Por exemplo, nos casos em que indicadores iniciais de intenção de exfiltração dos dados são detectados por usuários de alto risco, as organizações podem aplicar políticas mais rigorosas de Prevenção contra Perda de Dados (DLP), proativamente ficando à frente de possíveis incidentes de segurança de dados.

Esperamos que os insights e as recomendações neste relatório sejam úteis para aprimorar sua postura de segurança de dados e fortalecer sua organização contra riscos em evolução.

Para saber mais sobre a Segurança de Dados da Microsoft, acesse https://aka.ms/DataSecurityNews

Objetivos, metodologia e recrutamento de público-alvo detalhados da pesquisa

Os objetivos da pesquisa incluíam:

1. Entender o cenário de segurança de dados, incluindo prioridades, mentalidades e desafios
2. Mapear a causa e o efeito de incidentes de segurança de dados e identificar ações que as equipes de segurança de dados podem executar para aprimorar a postura de segurança de dados
3. Explorar o futuro da segurança de dados, incluindo estratégias emergentes e inovações no uso da IA para segurança de dados

A metodologia foi:

Uma pesquisa multinacional online de 15 minutos realizada entre 28 de julho e 9 de agosto de 2023, com 822 tomadores de decisão de segurança de dados.

Perguntas centradas no cenário de segurança de dados, como as equipes de segurança de dados alocam seus recursos, incidentes de segurança de dados e atitudes e uso da inteligência artificial (IA) para a segurança de dados.

Para atender aos critérios de triagem, os tomadores de decisão de segurança de dados precisavam:

Ser CISOs e tomadores de decisão adjacentes (C-2 e acima) com alcance sobre a segurança de dados

Trabalhar em organizações empresariais (mais de 500 funcionários; variedade de portes)

Ser provenientes de uma combinação de indústrias regulamentadas e não regulamentadas (exceto educação, governo ou sem fins lucrativos)

Dos 822 tomadores de decisão de segurança de dados entrevistados para a pesquisa, as conclusões por país foram:

EUA	329
Reino Unido	322
Austrália	171