Microsoft Security

Índice de segurança de dados

Tendências, insights e estratégias para manter seus dados seguros e navegar pela IA generativa

Relatório de 2024

Prefácio

Ao iniciarmos nosso segundo ano de pesquisa sobre o cenário em constante evolução da segurança de dados, os desafios e as oportunidades à nossa frente nunca foram tão profundos. No último ano, a gravidade dos incidentes de segurança de dados aumentou. Nesta era centrada em dados, as estratégias e ferramentas usadas para manter os dados protegidos estão evoluindo rapidamente.

Neste ano, exploramos uma nova fronteira: o papel e o impacto da IA generativa (IA) nas estratégias de segurança de dados.

A IA está causando um impacto mundial com capacidades inéditas para revelar mais inovação e eficiência. Entretanto, com esse enorme potencial, as organizações também se preocupam com os riscos à segurança de dados e como isso pode moldar as responsabilidades das equipes de segurança de dados. Vemos a IA como um acelerador para que as organizações fortaleçam suas práticas fundamentais de segurança de dados, de modo a minimizar o impacto do compartilhamento excessivo de dados e vazamentos e a criar processos para uma adoção segura da IA. Por outro lado, a IA também pode ajudar as organizações a aprimorar suas práticas de segurança de dados, identificando riscos ocultos e lacunas na proteção, recomendando políticas de proteção, bem como ajudando a investigar e corrigir incidentes de segurança mais rapidamente.

O objetivo de nossa pesquisa é fornecer aos líderes de segurança de dados insights e orientações práticas para ajudar suas equipes a adaptarem com confiança suas estratégias de segurança de dados, protegendo o uso da IA de maneira eficaz, além de integrar a IA em suas estratégias de segurança de dados. Embora notável em seu alcance e potencial, a IA é somente a mais recente força transformadora a impactar as empresas, assim como o trabalho híbrido, a nuvem e a mobilidade, que, nos últimos anos, destacaram a necessidade atemporal de visibilidade para mitigar riscos e maximizar o impacto. Informados por esses aprendizados, proteger os dados usados na IA de forma adequada, bem como utilizar a IA para aprimorar as medidas de segurança de dados, permitirá maior produtividade, resiliência e agilidade à medida que as equipes enfrentam desafios futuros.

Convidamos você a explorar as últimas descobertas e esperamos que os insights ajudem a fortalecer sua postura de segurança de dados, além de inspirar você a adotar a IA e a criar uma estratégia abrangente de segurança de dados, revelando mais inovação e garantindo um futuro mais seguro para todos nós.

Rudra Mitra
Vice-presidente corporativo
Conformidade e segurança de dados da Microsoft

Introdução

Com as organizações enfrentando uma média de 156 incidentes de segurança de dados por ano, o impacto desses incidentes continua sendo uma preocupação constante para os tomadores de decisão em segurança de dados. Há um bom motivo para isso: um único incidente pode causar enormes danos financeiros e à reputação, especialmente em um cenário de ameaças em constante evolução, onde invasores exploram todas as vulnerabilidades possíveis. Isso é agravado pela rápida adoção da IA, na qual, sem proteções e medidas de segurança adequadas, os usuários podem, acidentalmente ou de forma mal-intencionada, colocar em risco dados críticos e confidenciais para os negócios (inclusive informações de funcionários e clientes, propriedade intelectual, previsões financeiras e dados operacionais). À medida que as organizações buscam novas maneiras de proteger essa ampla variedade de dados confidenciais, muitos tomadores de decisão têm direcionado sua atenção para o rápido crescimento da IA.

O desafio da IA é duplo. Considerando que dois terços das organizações admitem que seus funcionários estão usando ferramentas de IA não autorizadas, é fundamental garantir que os funcionários utilizem essas ferramentas com segurança. Ao mesmo tempo, há uma oportunidade de usar a IA como uma ferramenta eficaz em uma estratégia sofisticada de segurança de dados.

As soluções de segurança de dados alimentadas por IA já desempenham um papel fundamental na identificação e resposta a ameaças em tempo real, melhorando a velocidade e a precisão dos programas de segurança de dados e fornecendo insights que ajudam a prevenir incidentes de segurança antes que ocorram. As organizações devem gerenciar os riscos que a IA introduz, além de aproveitar seu poder para identificar padrões que podem ser desafiadores para seres humanos processarem e analisarem em velocidade de máquina, e, em última análise, combater ataques cibernéticos cada vez mais sofisticados.

Em 2023, a Microsoft encomendou à agência de pesquisa independente Hypothesis a realização de uma pesquisa multinacional com mais de 800 profissionais de segurança de dados, lançando a iniciativa do Índice de Segurança de Dados para melhor atender nossos parceiros e clientes e ajudar os líderes empresariais a desenvolverem suas próprias estratégias de segurança de dados.

Em 2024, este relatório expande a pesquisa anterior com novos insights provenientes de uma pesquisa multinacional ampliada com mais de 1.300 profissionais de segurança de dados. Embora os dados revelem insights e tendências consistentes nos mercados pesquisados, descobrimos novos aprendizados sobre as últimas práticas e tendências em segurança de dados e IA no mundo todo.

Principais conclusões

1

O cenário da segurança de dados permanece fragmentado, aumentando a necessidade de estratégias coesas de segurança de dados para lidar com os riscos tradicionais e os novos riscos associados ao uso de IA

As organizações relatam altos níveis de satisfação e confiança em suas medidas de segurança de dados. No entanto, a gravidade dos incidentes de segurança de dados continua a aumentar, principalmente devido às lacunas que as organizações encontram entre suas políticas de segurança de dados atuais e o uso/introdução crescente de aplicações de IA. Diante desses desafios e prioridades, muitas organizações ainda dependem de diversas ferramentas de segurança de dados, o que pode aumentar sua vulnerabilidade e risco geral.

2

À medida que os usuários finais aumentam a adoção de aplicativos de IA, a integridade dos dados mais confidenciais das organizações fica em maior risco, exigindo mais visibilidade e novos controles de proteção.

Com o uso de ferramentas de IA tornando-se essencial no trabalho diário, as organizações estão preocupadas com os riscos de segurança de dados. Elas reconhecem a necessidade de fortalecer suas defesas e estão comprometidas em prevenir incidentes de segurança de dados causados pela IA, mas o uso não autorizado dessas ferramentas destaca a necessidade de uma visibilidade mais robusta.

3

Os tomadores de decisão estão otimistas com o potencial da IA para impulsionar seus esforços de segurança de dados

As organizações estão investindo de forma ativa em ferramentas de segurança de dados que incorporam a IA para melhorar as capacidades de detecção e resposta. A IA pode ajudar a identificar dados desprotegidos, recomendar políticas de proteção e investigar e remediar incidentes de segurança de dados de forma mais rápida, permitindo que as equipes de segurança de dados dediquem mais tempo e atenção a tarefas estratégicas. O uso da IA também aumenta a confiança e a satisfação com a estratégia geral de segurança de dados das organizações, especialmente em relação à capacidade de responder a incidentes de maneira rápida e precisa.

1

O cenário da segurança de dados permanece fragmentado, aumentando a necessidade de estratégias coesas de segurança de dados para lidar com os riscos tradicionais e os novos riscos associados ao uso de IA

Há uma desconexão entre a confiança dos tomadores de decisão em suas práticas de segurança de dados e o verdadeiro nível de proteção dos dados

Conforme relatado em 2023, a grande maioria dos tomadores de decisão está confiante em suas estratégias de segurança de dados, com 74% relatando satisfação com suas soluções atuais em 2024. Eles se sentem seguros em sua capacidade de rastrear e gerenciar dados confidenciais: 88% acreditam saber onde está localizada a maior parte de suas informações críticas, e 85% dizem que seus dados estão devidamente classificados e rotulados. A maioria também confia em seus controles de defesa, com 79% confiantes em sua capacidade de prevenir exfiltração de dados e 76% descrevendo sua abordagem como proativa, e não reativa.

No entanto, essa confiança está sendo testada à medida que a gravidade dos incidentes continua crescendo. **A média anual de incidentes de segurança de dados permaneceu alta, passando de 166 em 2023 para 156 em 2024, e a gravidade desses incidentes aumentou de 20% para 27% em 2024.**

156

incidentes de segurança de dados

27%

dos incidentes são considerados graves (um aumento em relação aos 20% em 2023)

63%

dos alertas são revisados diariamente

"A localização onde uma plataforma de software foi estabelecida, onde seus dados são armazenados e quem terá acesso a esses dados complicaram a segurança e o gerenciamento de dados das nossas ferramentas e fornecedores de IA. Temos mais de 100 anos de dados que devemos proteger e governar de acordo com os requisitos legais em cada jurisdição em que operamos", afirma um gerente sênior de Governança de Informações de um fabricante de equipamentos pesados.

O aumento na gravidade dos incidentes de segurança de dados levou, consequentemente, a um aumento no volume de alertas. **As organizações estão enfrentando uma média de 66 alertas por dia, em comparação aos 52 em 2023.** Esse número varia de forma significativa conforme o tamanho da organização: empresas de médio porte (500 a 999 funcionários) e grandes empresas (1.000 a 4.999 funcionários) recebem 56 alertas em média, enquanto empresas extragrandes (mais de 5.000 funcionários) recebem 80 alertas por dia, em média.

Dado o grande volume de alertas de segurança de dados, não é surpreendente que a maioria das organizações simplesmente não consiga acompanhar. Em média, as equipes de segurança de dados revisam 63% de seus alertas diários. 35% desses alertas acabam sendo falsos positivos. Essa incompatibilidade entre a percepção de controle e a realidade operacional deixa as equipes de segurança de dados sobrecarregadas, tentando avaliar se possuem as proteções corretas ou como ajustá-las, ao mesmo tempo em que se preocupam com a possibilidade de que incidentes potencialmente graves passem despercebidos.

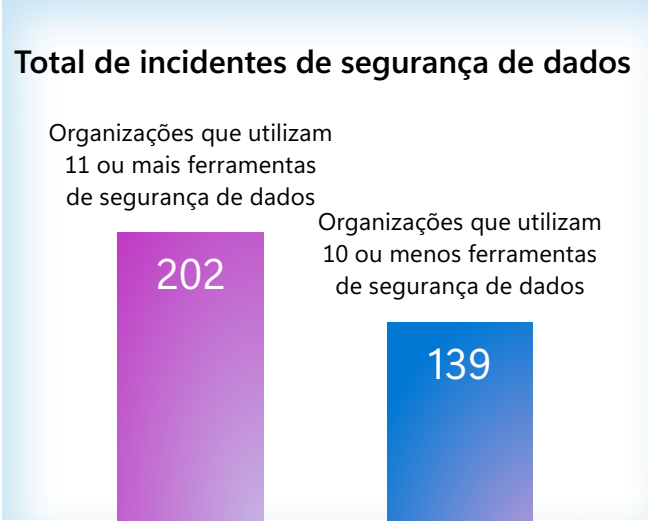
Para combater os riscos tradicionais e emergentes de dados associados ao uso de ferramentas de IA, há uma necessidade crescente de estratégias de segurança de dados mais robustas e coesas.

Apesar do aumento no número de ferramentas disponíveis, muitos tomadores de decisão continuam a reconhecer que mais ferramentas nem sempre significam melhores resultados. De fato, 21% apontam a falta de visibilidade consolidada e abrangente (e a compreensão compartilhada dos riscos) causada por ferramentas isoladas como seu maior desafio/risco.[1]

A maioria dos tomadores de decisão (82%) concorda que uma plataforma abrangente e totalmente integrada é superior ao gerenciamento de diversas ferramentas isoladas. **Em média, as organizações lidam com 12 soluções diferentes de segurança de dados, o que aumenta a complexidade e sua vulnerabilidade.** Isso é especialmente evidente em grandes organizações: em média, empresas de médio porte utilizam 9 ferramentas, grandes empresas usam 11 e empresas extragrandes utilizam 14 ferramentas.

Os dados mostram uma forte correlação entre o número de ferramentas de segurança de dados utilizadas e a frequência de incidentes de segurança de dados. Empresas de médio e grande portes relatam uma média de 89 incidentes por ano, enquanto as empresas extragrandes enfrentam impressionantes 248 incidentes por ano. Essa diferença significativa destaca o alto risco enfrentado pelas maiores organizações, mesmo quando expressam considerável confiança em suas medidas de segurança de dados.

Em 2024, organizações que utilizam mais ferramentas de segurança de dados (11 ou mais) experimentaram uma média de 202 incidentes de segurança de dados, em comparação com 139 incidentes para aquelas com 10 ou menos ferramentas.



Soluções fragmentadas dificultam a compreensão do estado de segurança de dados, já que os dados ficam isolados e fluxos de trabalho distintos podem limitar a visibilidade abrangente dos possíveis riscos. Quando as ferramentas não se integram, as equipes de segurança de dados precisam criar processos para correlacionar os dados e estabelecer uma visão coesa dos riscos, o que pode levar a pontos cegos e dificultar a detecção e mitigação eficaz de riscos.

Uma área de preocupação crescente é o aumento de incidentes de segurança de dados decorrentes do uso de aplicações de IA, que quase dobraram, de 27% em 2023 para 40% em 2024. Esse aumento nos incidentes é impulsionado por um aumento nos ataques de malware e ransomware, que subiram de 50% em 2023 para 59%. Os ataques associados ao uso de aplicativos de IA não só expõem dados confidenciais, como também comprometem a funcionalidade dos próprios sistemas de IA, complicando ainda mais o já fragmentado cenário de segurança de dados. Em resumo, há uma necessidade cada vez mais urgente de estratégias de segurança de dados mais fortes e coesas, capazes de lidar com os riscos tradicionais e emergentes associados ao uso de ferramentas de IA.

1. Pesquisa de setembro de 2024 com tomadores de decisão em segurança de dados, governança, conformidade e privacidade, encomendada pela Microsoft à agência MDC Research

O caminho adiante

O aumento na gravidade dos incidentes de segurança de dados revela uma oportunidade para a IA ajudar. Organizações na vanguarda estão implementando segurança de dados com IA para auxiliar na priorização de incidentes, automatizar a classificação de dados e identificar maneiras de aprimorar as políticas de proteção atuais. A IA pode sintetizar automaticamente a gravidade potencial dos alertas de incidentes, fornecendo às equipes de segurança de dados insights práticos para uma resposta rápida e reduzindo o tempo gasto em falsos positivos. Isso simplifica os fluxos de trabalho e permite que as equipes de segurança de dados se concentrem em melhorias estratégicas e em medidas proativas de segurança de dados.

2

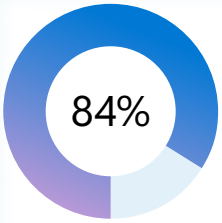
À medida que os usuários finais aumentam a adoção de aplicativos de IA, a integridade dos dados mais confidenciais das organizações fica em maior risco, exigindo mais visibilidade e novos controles de proteção.

A IA está rapidamente se tornando essencial para o trabalho diário, e as organizações devem adotar e se adaptar ativamente a essa nova realidade

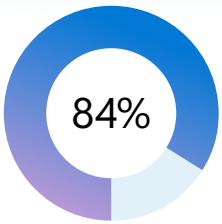
A rápida adoção de ferramentas de IA pelos funcionários tem promovido grandes mudanças na abordagem das organizações em relação à segurança de dados. Embora a IA esteja transformando a produtividade e os fluxos de trabalho, como qualquer tecnologia emergente, ela também pode amplificar riscos existentes ou introduzir novos riscos que exigem uma abordagem diferente para proteger informações confidenciais. Como resultado, as empresas ainda estão encontrando seu caminho em um cenário que muda rapidamente. Um diretor de engenharia e análise do setor de transporte afirma: "estamos monitorando os dados mais cuidadosamente no lado da IA. Há uma tensão entre produtividade e segurança, precisão e privacidade."

A confiança na segurança do uso de IA pelos funcionários varia. A maioria (84%) gostaria de se sentir mais confiante sobre o gerenciamento e a descoberta de dados inseridos. Enquanto 22% das organizações se sentem extremamente confiantes em sua capacidade de manter os dados seguros, a maioria (59%) está apenas "muito confiante", indicando que há espaço para melhorias. Além disso, a maioria das empresas (86%) reconhece que gostaria de se sentir mais segura em relação ao gerenciamento e à descoberta de dados gerados por ferramentas de IA.

À medida que a IA se torna mais essencial para a produtividade diária, o uso de aplicativos de IA também aumentou as preocupações com incidentes de segurança de dados. **Quase um terço (31%) das organizações prevê um aumento nos incidentes de segurança de dados devido ao uso de IA pelos funcionários, e 84% admitem que precisam fazer mais para se proteger contra esses riscos.** Essas preocupações são especialmente altas entre as maiores organizações: enquanto 26% das empresas de médio porte esperam ver um aumento em incidentes de segurança de dados relacionados à IA e 29% das grandes empresas projetam um crescimento, um grupo significativamente maior, representando 36% das empresas extragrandes, prevê um aumento.



desejam se sentir mais confiantes sobre o gerenciamento e a descoberta dos dados inseridos em aplicativos e ferramentas de IA



concordam que precisam fazer mais para se proteger contra o uso arriscado de aplicativos e ferramentas de IA pelos funcionários

O uso não autorizado de IA é generalizado

Quarenta por cento das organizações relatam que seus aplicativos de IA já foram violados ou comprometidos em um incidente de segurança de dados. Esse índice é ainda mais alto entre as organizações maiores: empresas de médio porte relatam uma taxa de incidentes de 36%, empresas grandes relatam 38% e empresas extragrandes registram o maior número de ocorrências, com 44%.

O uso não autorizado de IA frequentemente ocorre quando funcionários fazem login com credenciais pessoais ou usam dispositivos pessoais para tarefas relacionadas ao trabalho. **Em média, 65% das organizações admitem que seus funcionários estão usando ferramentas de IA não autorizadas.** As maneiras como os funcionários utilizam ferramentas de IA não autorizadas incluem:

- 53% que fazem login com credenciais pessoais para fins de trabalho
- 48% que usam seus dispositivos pessoais ao utilizarem IA para trabalho
- 47% que usam suas credenciais de trabalho para utilizar IA para fins pessoais

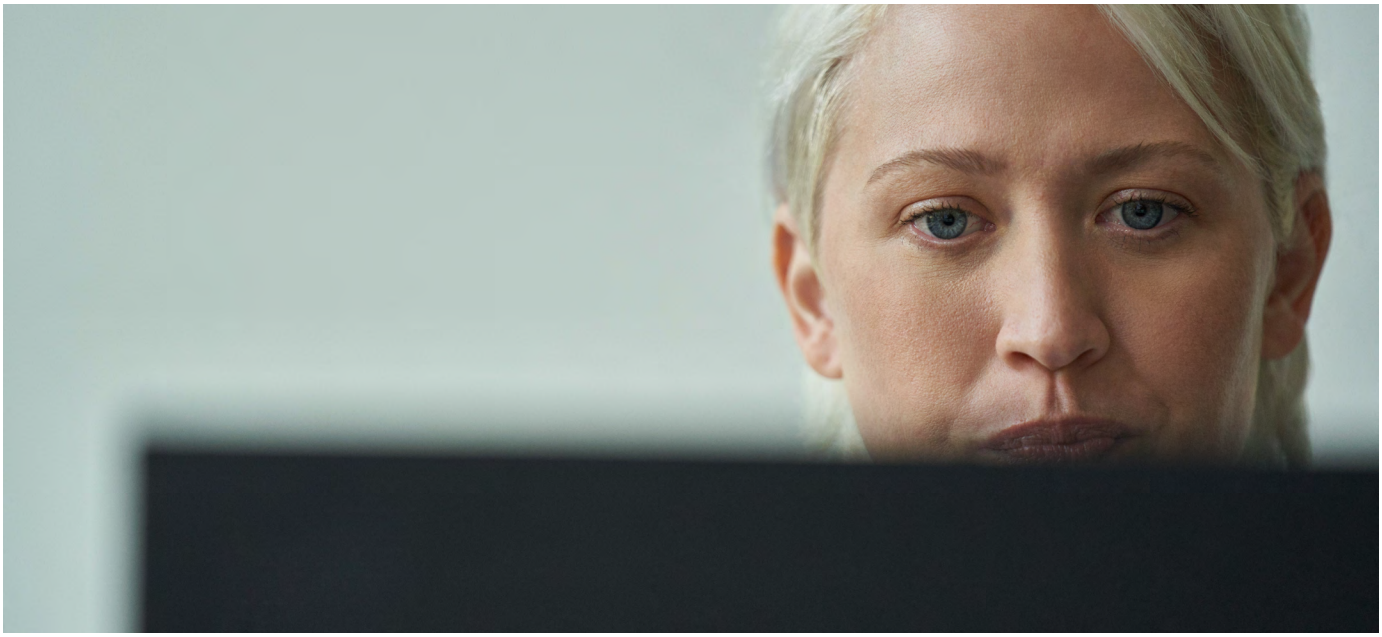
Metade de todas as organizações afirma estar preocupada com a falta de controles para detectar e mitigar riscos quando os funcionários usam aplicativos de IA de forma insegura. Esse índice varia conforme o tamanho da empresa, com 43% das empresas de médio porte, 50% das grandes empresas e 54% das empresas extragrandes expressando preocupação quanto à sua capacidade de gerenciar esses riscos.

Considerando o aumento no uso de IA, são necessários mais controles de segurança de dados

À medida que a IA se torna mais integrada nas operações diárias, as organizações reconhecem a necessidade de uma proteção mais robusta. **Embora 96% das empresas estejam preocupadas com o uso dessas ferramentas por seus funcionários, quase o mesmo percentual está disposto a investir em soluções para enfrentar essas preocupações.**

"O grande foco será como você se antecipa à IA? O foco de segurança é reduzir o volume de dados e monitorar os dados de forma mais cuidadosa. Do lado da IA, para que seus modelos sejam mais representativos e identifiquem vieses, você precisa de mais dados. Então, como reconciliar isso?" afirma um diretor de engenharia, arquitetura e análise no setor de transporte. A grande maioria dos tomadores de decisão (87%) está disposta a investir tempo e dinheiro no treinamento de funcionários em práticas seguras para o uso de ferramentas de IA. **Isso ocorre porque 85% consideram essencial que os funcionários utilizem essas ferramentas para se manterem competitivos.**

Quase todas as organizações (93%) estão em alguma etapa de desenvolvimento ou implementação de controles para o uso de IA, mas muitas ainda estão nas fases iniciais. Apenas 39% implementaram completamente controles de segurança de dados para IA, enquanto 24% desenvolveram políticas, mas ainda não as colocaram em prática. Vice-presidente de segurança de dados no setor de hospitalidade afirma: "precisamos alinhar os controles para a IA, mas estamos abraçando o uso da IA enquanto isso. Ela realmente facilita a vida e nos ajuda a ser mais eficientes."



Embora as organizações estejam tomando medidas para proteger dados confidenciais contra o uso indevido em aplicativos de IA, há uma necessidade evidente de controles mais abrangentes. Atualmente, 43% das empresas estão focadas em impedir que dados confidenciais sejam carregados em aplicativos de IA. Além disso, outros 42% registram todas as atividades e conteúdos nesses aplicativos para potenciais investigações ou respostas a incidentes. Da mesma forma, 42% bloqueiam o acesso de usuários a ferramentas não autorizadas, e um percentual equivalente investe no treinamento de funcionários sobre o uso seguro da IA.

As empresas com funcionários que fazem uso não autorizado de IA têm uma maior necessidade de determinados tipos de controle. **Entre aquelas com uso não autorizado de IA, 42% necessitam de controles para identificar usuários de risco com base nas consultas de IA, em comparação com 30% para aquelas sem uso não autorizado. Além disso, 40% das organizações que lidam com uso não autorizado de IA precisam de controles para gerenciar o ciclo de vida dos dados (como protocolos de retenção e exclusão), em comparação com 27% das empresas sem esse problema.**

Os 5 principais controles de IA necessários

Impedir que dados confidenciais sejam carregados para a IA	43%
Registrar todas as atividades e conteúdos nas ferramentas de IA para possíveis investigações ou respostas a incidentes	42%
Bloquear o acesso do usuário a ferramentas de IA não autorizadas	42%
Treinar funcionários sobre o uso seguro das ferramentas de IA	42%
Identificar usuários de risco com base nas consultas em IA	41%

O caminho adiante

Para manter uma postura robusta de segurança de dados, as equipes precisam de um conjunto completo de controles para descobrir, proteger e governar seus dados em aplicativos de IA. Aqui estão três estratégias-chave que as equipes podem adotar:

Aumentar a visibilidade do uso de aplicativos de IA e do fluxo de dados nesses aplicativos: utilize ferramentas de segurança de dados que possam detectar o uso de aplicativos de IA. Essas ferramentas fornecem insights sobre uma lista abrangente de aplicativos de IA utilizados, juntamente com seus perfis de risco, inclusive detalhes sobre os controles de segurança de dados compatíveis e conformidade com regulamentações. Use ferramentas que forneçam uma classificação consistente para dados confidenciais em interações com IA e mostrem tendências de como os dados estão fluindo por meio de aplicativos de IA.

Desenvolver e aplicar políticas: crie políticas com base nos insights obtidos da análise. Essas políticas podem incluir diretrizes para aplicativos de IA aprovados e procedimentos para bloquear ou restringir o uso de aplicativos não autorizados por funcionários. Mesmo em aplicativos de IA sancionados, é possível criar políticas granulares para permitir que dados não confidenciais circulem enquanto se restringe o uso de dados sensíveis e críticos para os negócios. Isso pode incluir o bloqueio de determinadas ações, como colar dados confidenciais em ferramentas de IA baseadas em navegador para garantir a segurança dos dados.

Avaliar riscos e ajustar políticas regularmente: gere relatórios regularmente que mostrem os níveis de risco dos aplicativos de IA em uso, tendências sobre como dados confidenciais estão fluindo por esses aplicativos e a atividade dos usuários nesses aplicativos. Isso auxilia na avaliação do panorama geral de riscos e na tomada de decisões informadas sobre as políticas de segurança de dados mais relevantes.

3

Os tomadores de decisão estão otimistas com o potencial da IA para impulsionar seus esforços de segurança de dados

Investigações de segurança de dados dependem fortemente da IA

A grande maioria (88%) das organizações já está investindo em IA para aprimorar seus esforços de detecção e resposta, identificando dados confidenciais, detectando atividades anômalas e protegendo automaticamente dados em risco. **77% das organizações acreditam que a IA acelerará esses processos, e 76% acham que ela melhorará a precisão de suas estratégias de detecção e resposta.**

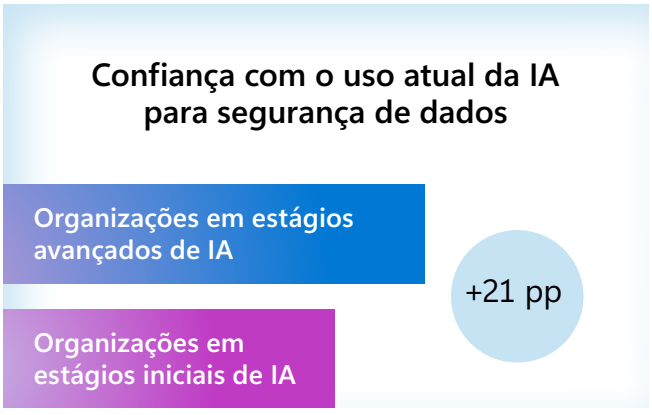
Apesar de 73% dos tomadores de decisão expressarem preocupações sobre o uso da IA para reforçar a segurança de dados, 50% afirmam que essas preocupações não inibiram o uso de IA para essa finalidade, e apenas 23% dizem que essas preocupações os impediram. No total, uma esmagadora maioria de 93% está, no mínimo, planejando usar IA para reforçar a segurança de dados, apesar das preocupações.

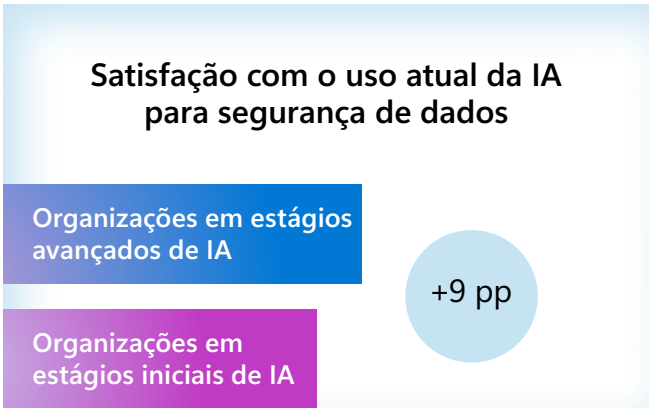
O uso de IA para reforçar a segurança de dados aumenta a visibilidade, a confiança e a satisfação

Um dos principais benefícios do uso da IA para reforçar a segurança de dados é sua capacidade de aumentar a visibilidade em todos os sistemas, mitigando uma preocupação comum entre os tomadores de decisão: saber onde os dados estão armazenados e como estão classificados (20%).[1] 88% dos tomadores de decisão de segurança de dados acreditam que a integração da IA nas soluções de segurança de dados permitirá que as equipes tenham mais visibilidade, possibilitando às organizações processar e analisar muito mais dados do que seria possível de outra maneira. As organizações de médio porte estão focadas principalmente em reduzir riscos de curto prazo, como a minimização de erros humanos em seus processos de segurança de dados. De fato, 43% das empresas de médio porte priorizam a redução de riscos causados por erros humanos, em comparação com apenas 37% das empresas extragrandes.

Em contraste, as empresas maiores adotam uma abordagem mais avançada, com ênfase nos riscos de longo prazo e na necessidade de adaptabilidade. Esse nível elevado de sofisticação permite que as equipes de segurança de dados se adaptem melhor aos riscos em evolução, uma prioridade para 49% das empresas extragrandes, em comparação com 43% das organizações de médio porte.

No geral, as organizações que estão mais avançadas no uso de IA para reforçar a segurança de dados relatam níveis muito mais altos de confiança e satisfação com suas estratégias de segurança de dados. **Entre aquelas em estágios avançados de implementação de IA, 90% se sentem extremamente ou muito confiantes no uso de IA para reforçar a segurança de dados, comparado a 69% nas fases iniciais. Da mesma forma, 76% das organizações com uso avançado de IA expressam satisfação com suas soluções de segurança de dados, enquanto apenas 67% das que estão em fases iniciais relatam o mesmo.**





1. Pesquisa de setembro de 2024 com tomadores de decisão em segurança de dados, governança, conformidade e privacidade, encomendada pela Microsoft à agência MDC Research

As organizações estão reduzindo o número de incidentes de segurança de dados e aprimorando o gerenciamento de alertas com a IA

As organizações que utilizam IA para reforçar suas operações de segurança de dados relatam significativamente menos alertas. **Em média, aquelas que implementaram ferramentas de segurança de dados com IA recebem 47 alertas por dia, contra 79 alertas para quem não usa IA. Além disso, as organizações que utilizam IA conseguem revisar 66% dos alertas diários, enquanto as demais revisam apenas 60%.**

Além disso, as organizações que usam IA para reforçar a segurança dos dados têm maior probabilidade de também usar IA para mitigar riscos (56% contra 26%). A redução no volume de alertas, juntamente com a maior capacidade de mitigá-los por meio da IA, parece ter tido um impacto significativo no número total de incidentes de segurança de dados. As organizações que implementaram IA para reforçar a segurança de dados registram uma redução de 65% nos incidentes de segurança de dados, em comparação com aquelas que não utilizam IA para reforçar a segurança.

Espera-se que a IA tenha o maior impacto na resposta

Em termos de detecção, 33% dos tomadores de decisão esperam que a IA ajude a detectar atividades anômalas, enquanto 23% acreditam que ela ajudará a investigar potenciais incidentes de segurança de dados. Outros 22% veem o potencial da IA para fazer recomendações para melhorar a segurança de seus ambientes de dados.

No entanto, a resposta é onde os tomadores de decisão esperam que a IA tenha o impacto mais profundo. 34% acreditam que a IA pode bloquear automaticamente o compartilhamento inadequado de dados confidenciais, e 32% afirmam que ela protegerá dados em risco. Outros 26% veem a IA ajudando a mitigar os riscos de segurança de dados e aplicar controles apropriados, enquanto o mesmo número espera que a IA flagre automaticamente comportamentos arriscados de usuários.

O caminho adiante

Integrar a IA nas soluções de segurança de dados pode ajudar oferecendo às equipes orientações em tempo real, recursos de resumo e suporte em linguagem natural para destacar áreas que poderiam passar despercebidas. Isso também pode acelerar investigações e fortalecer a experiência nas equipes de segurança de dados. Veja como esses recursos podem fazer a diferença:

Resumo do alerta: as investigações podem ser desafiadoras devido ao volume de fontes a analisar e às diversas regras de políticas. Ao integrar a IA em prevenção contra perda de dados (DLP) e gerenciamento de riscos internos (IRM), as equipes podem rapidamente receber um resumo dos alertas, inclusive a origem, as regras de políticas e os insights de risco do usuário, para entender quais dados confidenciais foram comprometidos e o risco associado ao usuário.

Comunicações contextuais: as organizações devem aderir aos requisitos regulatórios em torno das comunicações empresariais, o que frequentemente exige uma revisão extensa de violações. A IA pode ajudar as equipes de segurança de dados a avaliar o conteúdo em relação às regulamentações e políticas corporativas, destacando comunicações de alto risco que poderiam resultar em um incidente de segurança de dados.

Linguagem natural para consulta de palavras-chave: a pesquisa pode ser um fluxo de trabalho complexo e demorado durante investigações, normalmente exigindo o uso de linguagem de consulta por palavras-chave. A IA permite que as equipes de segurança de dados insiram solicitações de pesquisa em linguagem natural para agilizar o início da busca e possibilitar investigações mais avançadas.

Recomendações finais

1 Proteja-se contra incidentes de segurança de dados adotando uma plataforma integrada

Adotar uma plataforma integrada de segurança de dados oferece uma estratégia mais segura e simplificada em um cenário em constante evolução, reduzindo a complexidade, aumentando a visibilidade e melhorando a proteção. Uma abordagem integrada pode ajudar as organizações a aprimorar o gerenciamento da postura de segurança de dados, centralizando os controles de segurança e fornecendo visibilidade unificada sobre dados, usuários e atividades, fortalecendo e agilizando a detecção e a proteção contra riscos de dados. Com 82% das organizações concordando que uma plataforma integrada é superior, a migração para a consolidação não é apenas benéfica, é essencial.

2 Aumente a visibilidade sobre o uso interno da IA para avaliar os controles necessários para o uso dos funcionários sem impactar a produtividade

À medida que a IA se torna mais comum no ambiente de trabalho, ela pode amplificar os riscos existentes e introduzir novos riscos. As organizações admitem que precisam fazer mais para se proteger contra o uso inseguro da IA. Utilizar controles integrados e visibilidade sobre aplicativos de IA é fundamental para manter a segurança de dados sem interromper a produtividade. Treinar os funcionários para o uso seguro da IA pode ajudar as organizações a minimizar comportamentos arriscados, garantindo que as equipes continuem a se beneficiar dessas ferramentas poderosas.

3 Aprimore sua estratégia de segurança de dados com a ajuda da IA

A IA permite que as equipes de segurança de dados se concentrem em iniciativas mais estratégicas, em vez de reagir constantemente a ameaças e a um alto volume de alertas. As empresas em estágios avançados de implementação da IA estão mais confiantes e satisfeitas com suas soluções de segurança de dados do que aquelas que estão apenas começando. Ao implantar a IA como parte de uma estratégia abrangente de segurança de dados, as organizações podem aumentar sua visibilidade, o que fortalece sua capacidade de detectar e responder a riscos, reforçando, em última análise, sua postura geral de segurança de dados.

Objetivos da pesquisa

Os objetivos da pesquisa incluíam:

1. Compreender o panorama da segurança de dados, incluindo prioridades, mentalidades, desafios e as causas e consequências de incidentes de segurança de dados.
2. Explorar o futuro da segurança de dados, incluindo as estratégias e inovações emergentes e como as organizações pretendem investir no futuro.
3. Descobrir o papel da IA no fortalecimento da segurança de dados e sua função na proteção dos dados.

Metodologia

Uma pesquisa multinacional online de 20 minutos foi conduzida entre 5 e 23 de agosto de 2024, com 1.376 tomadores de decisão de segurança de dados.

As perguntas se concentraram no panorama da segurança de dados e em incidentes de segurança de dados em comparação com 2023. Além disso, a pesquisa deste ano incluiu questões sobre como garantir o uso seguro da IA pelos funcionários e o uso da IA para reforçar a segurança de dados.

Recrutamento de público-alvo

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

- CISO e tomadores de decisão adjacentes (nível C-2 e acima) com responsabilidade sobre a segurança de dados
- Trabalhar em organizações empresariais (mais de 500 funcionários; variados tamanhos)
- Indústrias regulamentadas e não regulamentadas (excluindo educação, governo e organizações sem fins lucrativos)

Dos 1.376 tomadores de decisão de segurança de dados entrevistados para a pesquisa, as conclusões por país foram:

- EUA: 302
- Reino Unido: 305
- Índia: 301
- Brasil: 158
- França: 156
- Austrália: 154

hypothesis Microsoft Security