

Guia do CISO para segurança de dados preparada para o futuro com DSPM baseado em IA

2025

©2025 Zscaler, Inc. Todos os direitos reservados.

Índice



Como navegar no atual cenário de segurança de dados 3

A prioridade do CISO: dominar a segurança de dados na era da IA 4

Adoção do DSPM: o novo imperativo para segurança de dados em IA 6

Como os CISOs podem melhorar a postura da segurança de dados usando DSPM integrado 7

- Aborde os riscos de IA paralela, dados abandonados e paralelos 7
- Classificação de dados baseada em IA 8
- Gerenciamento de riscos proativo 9
- Simplifique a conformidade com governança em tempo real 10
- Obtenha acesso de privilégio mínimo 11
- Otimize custos de armazenamento e consumo 12
- Aplique políticas unificadas em todos os ambientes de dados 12
- Resposta rápida a incidentes 13
- Segurança de IA aprimorada 14

Como usar o DSPM para proteger um cenário de dados diversificado 15

Zscaler DSPM 16

©2025 Zscaler, Inc. Todos os direitos reservados.

Como navegar no atual cenário de segurança de dados

O crescimento exponencial e a dispersão de dados em múltiplas plataformas aumentaram a complexidade, os custos e os riscos para muitas organizações. Os líderes de segurança enfrentam agora desafios significativos para compreender e controlar profundamente seus dados críticos. Para agravar essa complexidade, há a rápida adoção da IA, que dispersa ainda mais os dados, tornando as organizações mais vulneráveis a riscos relacionados a dados e conformidade.

Para mitigar com eficácia os riscos de segurança e garantir uma conformidade sólida, as equipes de segurança de dados precisam de ferramentas inovadoras que ofereçam uma compreensão abrangente e em tempo real de todo o seu universo de dados. O gerenciamento da postura de segurança de dados (DSPM, na sigla em inglês) surgiu como a abordagem moderna definitiva, capacitando os líderes de segurança de dados a alcançar essa visibilidade e compreensão contínuas por meio de IA e automação.

Este e-book essencial explora o potencial transformador do DSPM, capacitando líderes de segurança e suas equipes a protegerem proativamente dados sigilosos. Elaborado especificamente para profissionais seniores de segurança e gerenciamento de riscos, este guia oferece informações práticas para navegar pelas complexidades do cenário moderno de segurança de dados. Como um guia completo para elevar o nível de segurança de dados da sua organização, esse recurso explora tendências críticas, aborda desafios urgentes e revela estratégias inovadoras, destacando, em última análise, o papel indispensável do DSPM na proteção de seus ativos de dados na era dinâmica da IA.



©2025 Zscaler, Inc. Todos os direitos reservados.

A prioridade do CISO: dominar a segurança de dados na era da IA

Para os diretores de segurança da informação (CISOs), a rápida adoção de tecnologias de IA e nuvem representa um dilema profundo. Ao mesmo tempo que oferece oportunidades sem precedentes para redução de custos, melhores resultados de negócios e ganhos de produtividade notáveis, essa transformação digital introduz simultaneamente um cenário complexo de desafios em relação à segurança de dados.

O cenário de dados em expansão

O cerne desse desafio reside na explosão dos dados corporativos. Informações valiosas e sigilosas não estão mais confinadas; elas estão cada vez mais fragmentadas e espalhadas por diversos ambientes: ecossistemas de IA, SaaS, PaaS, implantações multinuvem, arquiteturas de nuvem híbrida e infraestrutura tradicional local. Essa proliferação é impressionante: a IDC prevê um crescimento de dados a uma taxa composta anual de 21,2%, atingindo mais de 221.000 exabytes até 2026.

Como lidar com complexidade e risco

Isso cria uma complexidade imensa para os CISOs, que agora precisam gerenciar a segurança de dados em um ambiente de dados cada vez maior e mais volátil. Os dados são constantemente criados, compartilhados e armazenados em centenas de sistemas e aplicativos diversos em toda a empresa, tornando a proteção abrangente de dados incrivelmente difícil.

Principais riscos de segurança de dados na era da IA:

- **Riscos de vulnerabilidade e conformidade:** dados dispersos e fragmentados aumentam significativamente o risco de violações de dados e descumprimento de regulamentações. Garantir a adesão às regulamentações de governança de dados e privacidade em constante evolução (como GDPR, CCPA, etc.) torna-se uma tarefa monumental.
- **A ameaça dos dados ROT:** a proliferação descontrolada de dados paralelos (cópias de dados desconhecidas ou não autorizadas) e dados abandonados (dados obsoletos ou esquecidos) cria vulnerabilidades críticas. Isso frequentemente leva a falhas de segurança significativas e expande exponencialmente a superfície de ataque.
- **Desafios de segurança da IA generativa (GenAI) e dos LLMs:** a ascensão da IA generativa e dos grandes modelos de linguagem (LLMs) introduz uma nova onda de riscos altamente especializados. Entre eles, IA paralela, data spillage (exposição não intencional de informações sigilosas), problemas de direitos de acesso em sistemas de IA e novas vias para infrações regulatórias. Segurança de IA vigilante e governança de dados de LLM são fundamentais.

Enfrentar esses desafios multifacetados de segurança de dados exige uma abordagem estratégica e proativa por parte dos CISOs, com foco em uma governança de dados robusta, soluções avançadas de proteção de dados e estruturas abrangentes de segurança de IA para salvaguardar informações sigilosas nesta era dinâmica.

Risco de perda de dados valiosos

Com um volume cada vez maior de ataques direcionados e um cenário regulatório dinâmico, tornou-se crucial para os CISOs priorizar a segurança desses ambientes. Cerca de 44% das empresas sofreram uma violação de dados em seus ambientes na nuvem nos últimos 12 meses.[1] Uma violação de dados pode ter consequências graves, incluindo perda de dados, danos à reputação e prejuízos financeiros. À medida que o cenário de ameaças relacionadas à IA e à nuvem se torna mais perigoso, o papel do CISO torna-se ainda mais crítico.

US$ 4,44 M

O custo médio global de uma violação de dados em 2025[2]

1. Revista Infosecurity, **Violações na nuvem afetam quase metade das organizações**, 25 de junho de 2024.
2. **Relatório da IBM sobre o custo de uma violação de dados em 2025**

©2025 Zscaler, Inc. Todos os direitos reservados.

Para lidar com esses riscos e garantir a adesão às regulamentações, os líderes de segurança devem compreender completamente seus ambientes de dados. Muitas vezes, porém, o volume, a variedade e a velocidade dos dados tornam difícil protegê–los. Os líderes frequentemente não têm respostas para estas perguntas:

- Onde estão os dados?
- Quais armazenamentos de dados contêm dados valiosos ou sigilosos?
- Quem, o quê ou quais ferramentas de IA têm acesso a esses repositórios?
- Como os dados são acessados ou compartilhados com ferramentas de IA?
- Qual é o valor dos dados?
- Como os dados são tratados e qual o impacto na conformidade com as normas?

Além dos limites: por que a segurança de dados tradicional não funciona na era da IA

O cenário da segurança de dados mudou fundamentalmente. Para muitos CISOs e suas equipes, a resposta convencional ao aumento das ameaças tem sido acumular uma vasta gama de ferramentas de segurança distintas. No entanto, essas ferramentas tradicionais de segurança de dados estão se mostrando cada vez mais inadequadas, falhando em fornecer os insights e proteções cruciais realmente necessários no atual ambiente dinâmico.

Os desafios não atendidos da segurança de IA

Uma brecha significativa nas soluções legadas reside em sua incapacidade de lidar com os comportamentos únicos, os novos modos de falha e os requisitos especializados de governança de dados das tecnologias emergentes. Especificamente, elas deixam a desejar quando se trata de proteger LLMs, agentes de IA generativa e outros modelos fundamentais. Esses novos riscos da IA exigem uma abordagem fundamentalmente diferente.

A necessidade de um novo paradigma de segurança

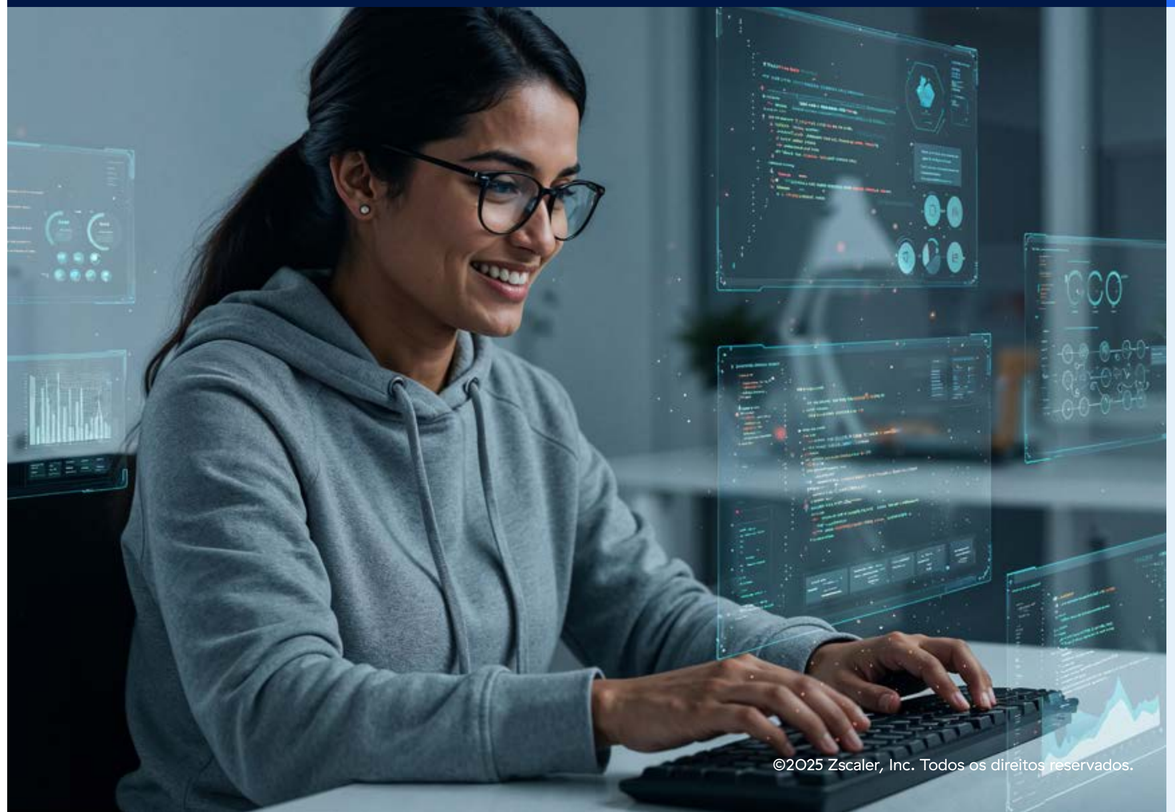
Esse cenário de ameaças emergente exige não apenas novas soluções, mas uma abordagem holística e integrada para a governança e segurança de dados na era da IA. Estamos falando de uma mudança de paradigma em que a segurança da IA não é mais algo opcional, mas um componente central da sua estratégia geral de cibersegurança.

Otimização de investimentos em meio a orçamentos mais restritos

Para agravar esses desafios, orçamentos de segurança cada vez mais apertados forçam os líderes de segurança a avaliar e otimizar criticamente seus investimentos. O foco está mudando decisivamente para a redução da complexidade operacional e a minimização de custos, ao mesmo tempo em que se aprimoram as defesas de cibersegurança e se eliminam falhas críticas de segurança. Paradoxalmente, esse investimento estratégico muitas vezes inclui o uso de soluções de segurança sofisticadas baseadas em IA. Essas ferramentas avançadas não são apenas parte do problema; elas são poderosos facilitadores que oferecem maior visibilidade, detecção acelerada de riscos e resposta a incidentes mais eficiente, fortalecendo, em última análise, toda a sua postura de segurança contra as ameaças da era da IA.

97%

das organizações que relataram uma violação relacionada à IA não possuíam controles de acesso à IA adequados[3]



3. Relatório da IBM sobre o custo de uma violação de dados em 2025

©2025 Zscaler, Inc. Todos os direitos reservados.

Adoção do DSPM: o novo imperativo para segurança de dados em IA

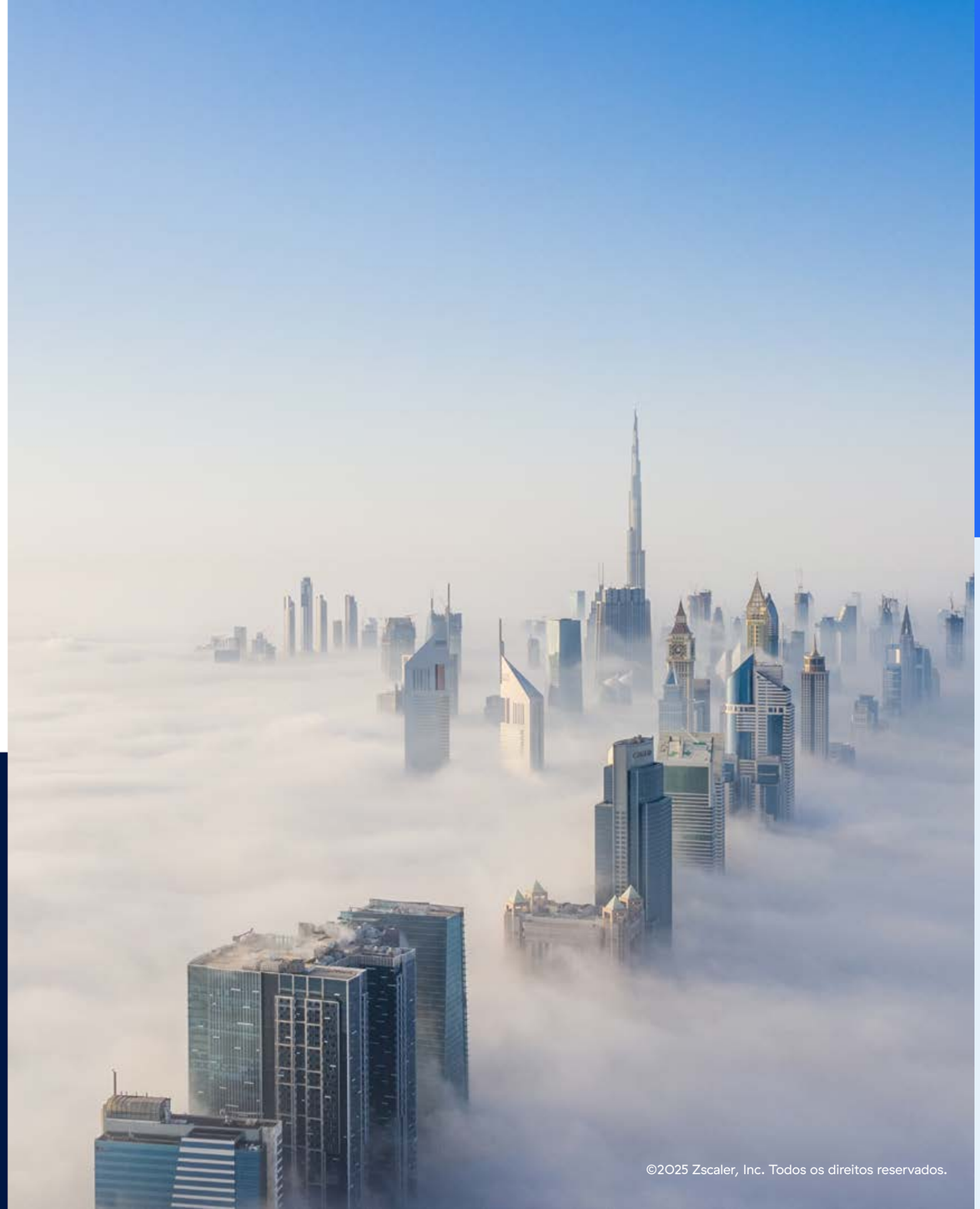
Diante dos riscos sem precedentes da IA e das reconhecidas limitações das ferramentas tradicionais de cibersegurança, uma abordagem verdadeiramente moderna para a segurança de dados não é apenas benéfica, mas essencial. É aqui que o gerenciamento da postura de segurança de dados (DSPM) surge como uma solução fundamental e indispensável.

O DSPM oferece o contexto e a automação necessários para navegar com habilidade pelas complexidades dos cenários de dados modernos. Ao adotar uma metodologia inovadora, os CISOs podem compreender seus dados de forma mais proativa, garantir a conformidade com as regulamentações e reduzir os riscos associados ao uso da IA.

4. Ibid.

US$ 1,9 M

A economia média para organizações que utilizam IA de segurança e automação extensivamente[4]



©2025 Zscaler, Inc. Todos os direitos reservados.

Como os CISOs podem melhorar a postura da segurança de dados usando DSPM integrado

Aqui estão algumas maneiras pelas quais os CISOs podem utilizar a IA de forma eficaz para melhorar a postura de segurança de dados:

Aborde os riscos de IA paralela, dados abandonados e paralelos

Dados paralelos Dados paralelos e dados abandonados representam riscos substanciais de segurança, pois frequentemente operam fora do escopo dos protocolos de segurança de TI e das estruturas de governança de dados. Segundo a IBM, 35% das violações de dados envolveram dados paralelos, e essas violações resultaram em um custo médio 16% maior. Além disso, as violações envolvendo dados paralelos levaram 26,2% mais tempo para serem identificadas e 20,2% mais tempo para serem contidas[5]. Os dados paralelos podem ser encontrados em arquivos não estruturados, bancos de dados estruturados, armazenamentos na nuvem ou em dispositivos pessoais sem a devida supervisão, enquanto os dados abandonados, sem gerenciamento de ciclo de vida, podem se tornar um passivo.
As soluções de DSPM utilizam IA para descobrir e classificar continuamente os armazenamentos de dados, melhorando a visibilidade geral do cenário de dados. A IA pode ajudar a catalogar dados obscuros e paralelos, aumentando a visibilidade dos dados. Ela também alerta as equipes de segurança sobre riscos potenciais e minimiza os riscos de violação. Ela pode monitorar anormalidades no acesso a dados, padrões, detectar anomalias e prever possíveis violações de segurança.

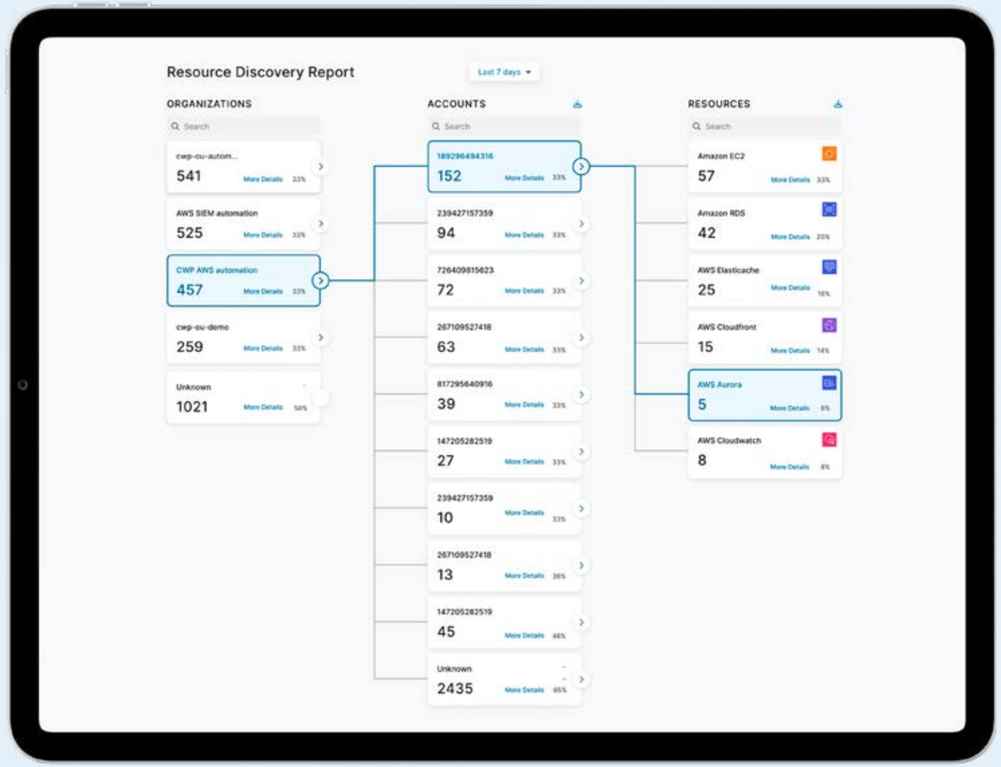
IA paralela IA paralela, assim como a TI paralela, refere-se principalmente ao uso de ferramentas de IA não autorizadas para interagir com dados sigilosos da empresa, o que pode ter consequências de longo alcance para a segurança e conformidade dos dados. À medida que essas ferramentas de IA se tornam mais acessíveis e produtivas, os funcionários as adotam sem a supervisão da TI. Embora possa parecer algo inofensivo, isso pode criar riscos em cascata que as estruturas de segurança tradicionais não conseguem mitigar simplesmente proibindo as ferramentas de IA.

Com o DSPM, as organizações podem colher os benefícios da IA. Em vez de bloquear ou proibir ferramentas de IA, as organizações podem gerenciar os riscos da IA paralela com o DSPM, aproveitando os benefícios da IA. Os recursos de segurança de IA integrados ao DSPM ajudam as equipes a obter visibilidade e controle de ponta a ponta sobre dados e modelos de IA para se protegerem proativamente contra riscos de IA. Isso ajuda a

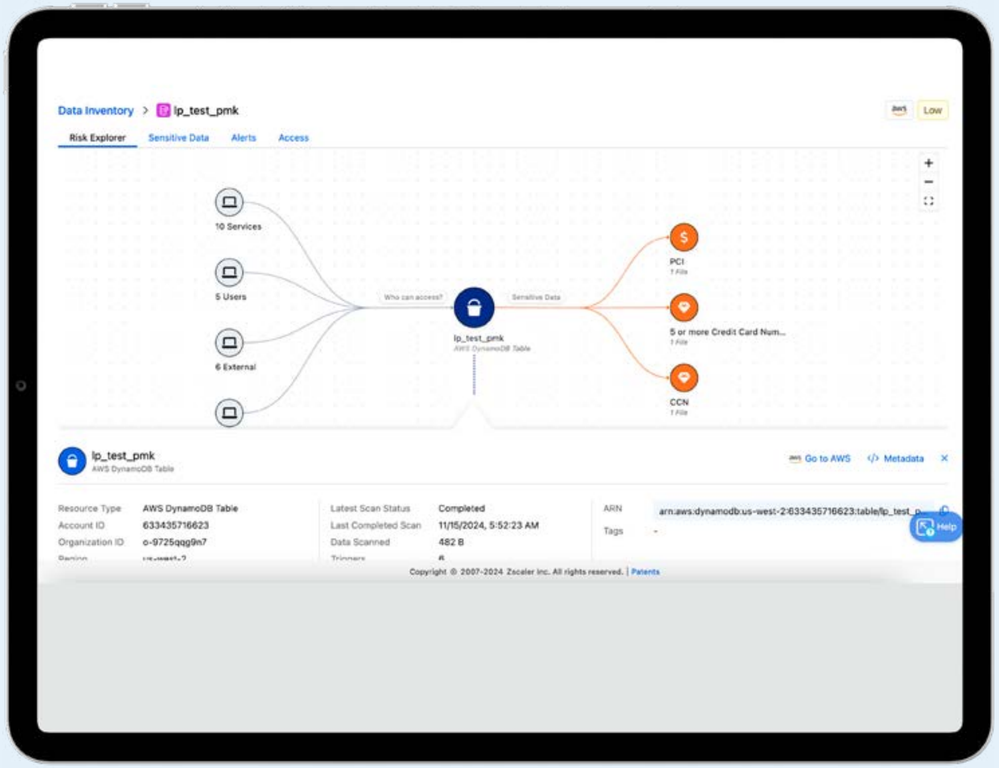
- Obtenha uma visão de 360 graus dos seus modelos, agentes e serviços de IA
- Identifique e proteja dados de treinamento de IA contra envenenamento de dados, configurações incorretas e exposição
- Garanta o alinhamento com estruturas de conformidade de IA novas e emergentes

Com o DSPM, os líderes de segurança podem transformar o caos da segurança em inovação controlada, fornecendo descoberta de dados unificada, avaliação contextual de riscos e governança automatizada em todas as interações com IA.

5. Ibid.



©2025 Zscaler, Inc. Todos os direitos reservados.



Classificação de dados baseada em IA

A classificação de dados é um aspecto fundamental da segurança de dados robusta. Mapear proativamente os dados sigilosos aos riscos associados é essencial para evitar possíveis exposições causadas por configurações incorretas ou práticas inseguras. As abordagens convencionais, muitas vezes dependentes de procedimentos manuais ou reconhecimento de padrões simplistas, são suscetíveis a um aumento de falsos positivos e a uma alocação inadequada de recursos de segurança. Frequentemente, as organizações dependem muito de soluções baseadas em expressões regulares; uma abordagem rígida e sujeita a falsos positivos, que se mostrou frágil e ineficiente. Mesmo as abordagens atuais baseadas em produtos específicos não conseguem integrar a classificação em uma plataforma centralizada e unificada, o que leva a alertas inconsistentes e visibilidade fragmentada, especialmente à medida que os dados se movem pelo ecossistema de uma organização.

Os líderes de segurança podem aproveitar o DSPM com a classificação de LLM baseada em IA, que aprimora as operações em torno dos fluxos de trabalho tradicionais de expressões regulares, proporcionando visibilidade e flexibilidade incríveis, permitindo que eles protejam dados sigilosos, conhecidos ou desconhecidos, como nunca antes. Ao contrário das técnicas que dependem de palavras-chave, a classificação de LLM permite uma identificação de conteúdo mais profunda. Ela utiliza processamento de linguagem avançado para classificação de dados, a fim de compreender a intenção e o contexto do conteúdo, sem a necessidade de padrões ou palavras-chave predefinidas. Isso permite que as organizações não apenas aprimorem suas práticas existentes, mas também descubram e protejam novos tipos de dados sigilosos anteriormente negligenciados ou indetectáveis.

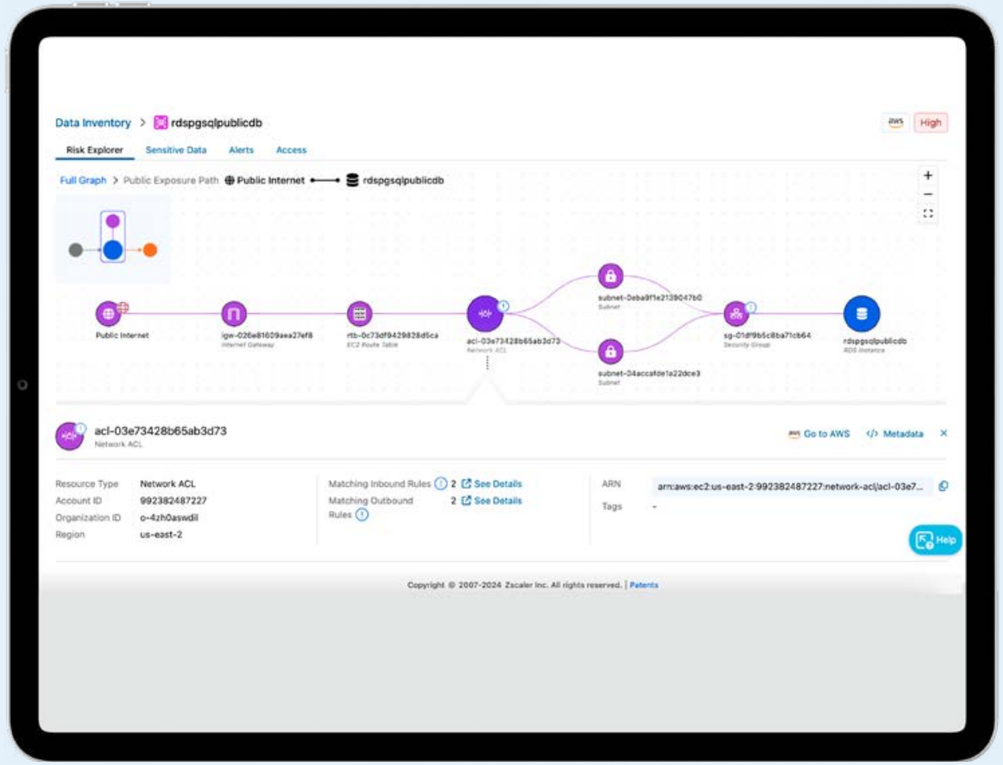
©2025 Zscaler, Inc. Todos os direitos reservados.

Gestão proativa de riscos

Para controlar riscos de segurança de forma eficaz e garantir a conformidade, os líderes de segurança precisam de uma maneira proativa de gerenciar sua postura de segurança de dados. Uma das aplicações mais interessantes da IA na segurança de dados é a abordagem proativa de segurança e a análise preditiva. Ao analisar e correlacionar dados, os algoritmos de IA podem prever potenciais riscos de segurança. Essa abordagem proativa permite que as organizações estejam um passo à frente das ameaças e dos riscos críticos.

O DSPM utiliza IA e técnicas avançadas de correlação para ajudar a identificar padrões e tendências nos dados que podem indicar incidentes de segurança iminentes. Além disso, ele pode priorizar armazenamentos de dados com base em seu valor (gravidade do risco), garantindo assim que os esforços de segurança sejam direcionados aos ativos mais críticos. Ademais, ao automatizar vários processos de segurança, ele reduz a carga de trabalho dos profissionais de segurança, permite uma abordagem de segurança proativa e melhora a eficiência operacional geral.

Por exemplo, a correlação avançada do Zscaler DSPM pode conectar pontos proativamente e detectar riscos ocultos, permitindo a priorização dos esforços de segurança nos dados mais críticos.



49%

das organizações investem em segurança após violação[6]

6. Relatório da IBM sobre o custo de uma violação de dados em 2025

©2025 Zscaler, Inc. Todos os direitos reservados.

Simplifique a conformidade com governança em tempo real

Manter a conformidade com os regulamentos e protocolos de segurança interna em constante evolução é um dos pilares da segurança de dados, do GDPR à SEC. Atualmente, as organizações precisam lidar não apenas com regulamentações já estabelecidas, como GDPR e HIPAA, mas também com estruturas emergentes voltadas especificamente para a IA, incluindo a lei de IA da UE, o NIST AI 600 e outras. A segurança e o risco de conformidade compartilham um vínculo inquebrável, influenciando profundamente um ao outro e moldando a trajetória de uma organização. Violações podem desencadear sanções por não conformidade, levando a repercussões severas, multas substanciais e manchando a reputação de uma organização. Por outro lado, adotar regulamentações pode servir como um escudo, fortalecendo a IA e os dados contra vulnerabilidades e ameaças à segurança.

Muitas regulamentações se resumem a conhecer a IA e os dados sigilosos, limitar quem pode acessá–los e monitorar continuamente os riscos. Embora possa parecer simples, a complexidade da IA e dos ambientes de dados pode tornar isso em uma tarefa desafiadora. Além disso, as regulamentações estão em constante evolução, impulsionadas por novas tecnologias, mudanças nas preocupações com privacidade e pela crescente interconexão da economia global. Esse cenário regulatório em constante mudança exige vigilância e adaptação constantes das organizações que desejam permanecer em conformidade. As abordagens tradicionais de conformidade, com visões fragmentadas, avaliações manuais e respostas reativas, têm dificuldade em proporcionar clareza e eficiência.

O DSPM pode simplificar os processos de conformidade com recursos de governança e conformidade de dados em tempo real. A solução de DSPM oferece às organizações uma visão ampla do status de conformidade de dados, análises abrangentes, benchmarking, remediação e relatórios para que possam agir rapidamente em relação às suas brechas de conformidade. Isso é especialmente importante em setores altamente regulamentados, onde uma compreensão clara do status dos dados e da mitigação de riscos é essencial. Desde etapas de correção guiadas até fluxos de trabalho automatizados, o painel de conformidade capacita as equipes de segurança a agir com rapidez e eficácia. A aplicação da IA na governança de dados garante que as organizações possam atender às exigências regulatórias, mantendo ao mesmo tempo medidas de segurança robustas.

63%

das organizações não possuem políticas de governança de IA[7]



7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

©2025 Zscaler, Inc. Todos os direitos reservados.

Obtenha acesso de privilégio mínimo

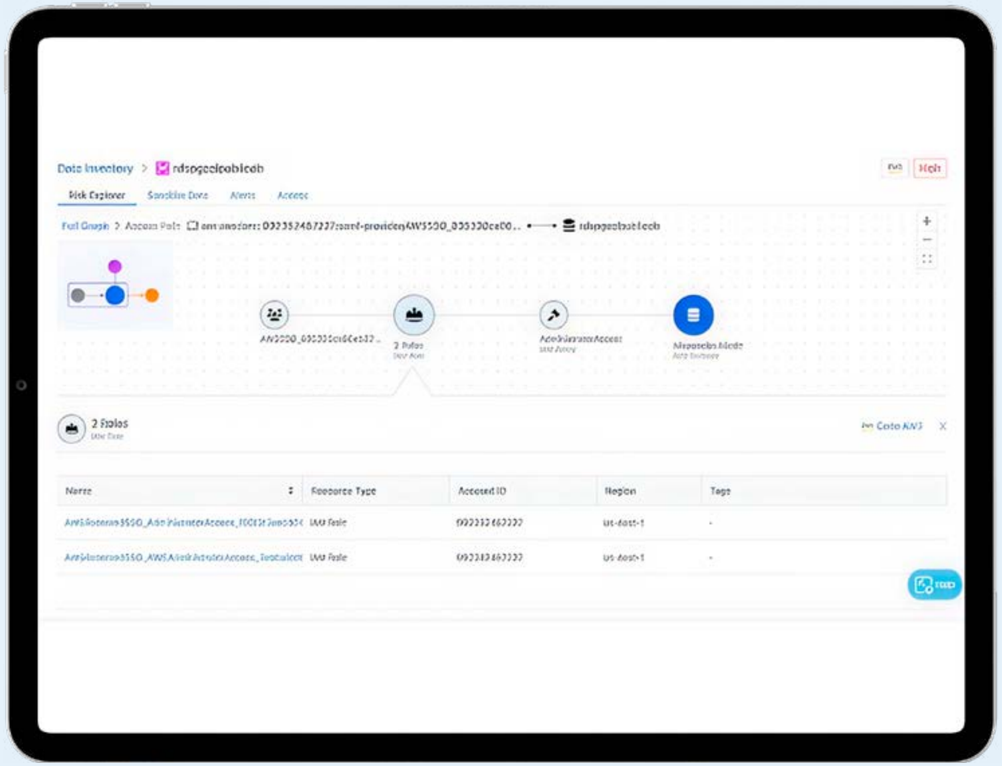
Devido ao enorme volume de usuários, aplicativos e recursos, os ambientes de dados apresentam riscos significativos de controles de acesso inadequados, proliferação de identidades e repositórios órfãos. Aproximadamente 90% das organizações sofreram violações de identidade, resultando em incidentes de segurança dispendiosos.

Além disso, os modelos de IA e as ferramentas baseadas em LLM introduzem riscos adicionais relacionados ao acesso não autorizado a dados. Os principais riscos incluem divulgações não intencionais ou não autorizadas de dados sigilosos, exfiltração de dados (onde dados sigilosos são roubados por meio de resultados de IA) e ataques sofisticados, onde identidades comprometidas exploram sistemas de IA para obter acesso não autorizado.

Por isso, garantir o acesso de privilégio mínimo aos repositórios de dados é um princípio fundamental da segurança de dados. A governança do acesso a dados é mais desafiadora devido à dispersão de dados, à dispersão de permissões e às arquiteturas complexas de IA e multinuvem. Ainda assim, ela continua sendo um componente essencial da segurança de dados, uma vez que a exposição não autorizada de dados sigilosos é normalmente o primeiro passo de um ataque sofisticado.

O DSPM oferece uma abordagem unificada para a governança de acesso a dados, com monitoramento contínuo da postura de segurança dos dados e do comportamento dos usuários. O DSPM examina minuciosamente as funções, permissões e atributos relacionados ao gerenciamento de identidade e acesso a dados para identificar rapidamente rotas de acesso de risco aos repositórios de dados. O DSPM é compatível com dados estruturados e não estruturados em ambientes locais, multinuvem e SaaS, permitindo que as organizações identifiquem e abordem consistentemente os riscos de acesso e apliquem políticas de acesso em diversos conjuntos de dados e ecossistemas de IA. Ao fornecer insights detalhados sobre padrões de acesso e possíveis vulnerabilidades, as equipes de segurança de dados podem aplicar o acesso de privilégio mínimo de forma mais eficaz. Essa abordagem reduz os riscos de acessos não autorizados e aumenta a segurança geral do ambiente de dados.

8. Security Today, estudo: **90% das organizações sofreram um incidente relacionado à identidade no último ano**, 5 de junho de 2024.



90%

das organizações sofreram um incidente relacionado à identidade.[8]

©2025 Zscaler, Inc. Todos os direitos reservados.

Otimize custos de armazenamento e consumo

As equipes de dados precisam otimizar os custos de armazenamento e consumo, identificando repositórios de dados duplicados ou negligenciados que podem ser eliminados ou transferidos para soluções de armazenamento mais econômicas. Os métodos convencionais frequentemente falham na identificação e gerenciamento desses dados, resultando em despesas de armazenamento supérfluas.

Soluções de DSPM podem enfrentar esse problema fornecendo insights sobre armazenamentos de dados duplicados ou abandonados, permitindo que as organizações tomem as medidas apropriadas. O Zscaler DSPM fornece uma visão abrangente de armazenamentos de dados duplicados ou abandonados, permitindo que as equipes identifiquem dados que podem ser excluídos ou migrados com segurança.

Com insights baseados em IA, as organizações podem reduzir despesas excessivas com armazenamento e garantir o gerenciamento e a proteção adequados de informações sigilosas.

Aplique políticas unificadas em todos os ambientes de dados

Com métodos tradicionais, o desafio de manter políticas de segurança de dados consistentes em diversos ambientes é enorme. As soluções de DSPM podem superar isso oferecendo uma abordagem unificada à segurança de dados em ambientes multinuvem, permitindo que as organizações apliquem políticas uniformes em todos os ambientes de dados.

O Zscaler DSPM apresenta uma estratégia unificada para segurança de dados. Ele capacita as organizações a estabelecer políticas uniformes em todos os cenários de dados, garantindo vigilância abrangente sobre dados na nuvem e simplificando o processo de identificação e resolução de riscos. Ao usar insights baseados em IA/ML, as organizações podem reduzir o risco de violações de dados e seguir melhor as regras de proteção de dados.



©2025 Zscaler, Inc. Todos os direitos reservados.

Resposta rápida a incidentes

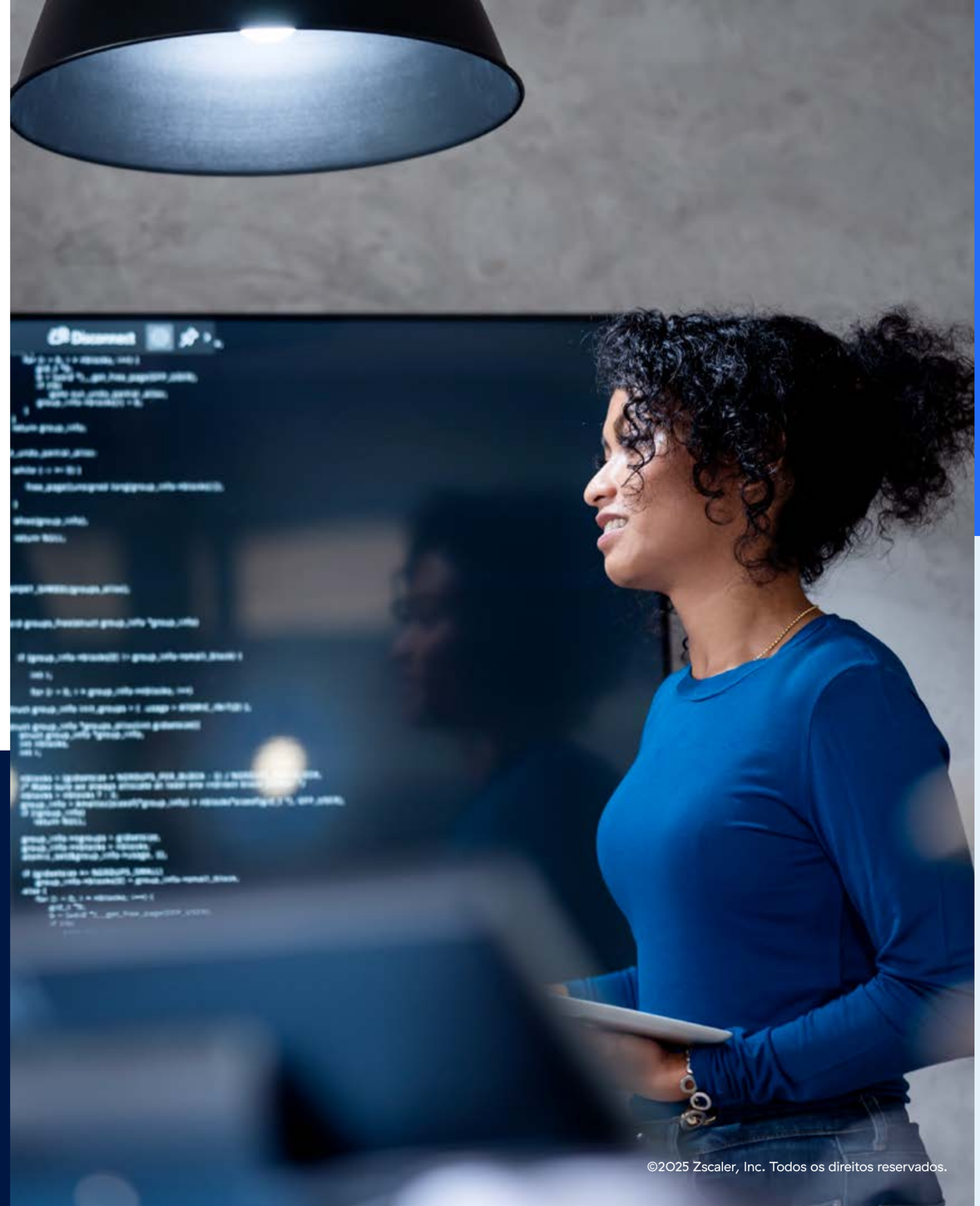
Identificar e mitigar riscos são tarefas fundamentais para profissionais de segurança de dados. A velocidade com que as ameaças evoluem exige respostas em tempo real. No entanto, as metodologias convencionais podem falhar diante de um ambiente de ameaças dinâmico impulsionado pela IA. A automação de segurança orientada por IA é a resposta para esse desafio.

O DSPM pode monitorar dados continuamente, detectar anomalias e ajudar a responder a ameaças. As soluções de DSPM reforçam a mitigação de riscos oferecendo correlação de riscos sofisticada e inteligência de acesso adaptativa. Algumas soluções de DSPM, como o Zscaler DSPM, incorporam inteligência sobre ameaças da Zscaler ThreatLabz, remediação guiada meticulosa e implementação de segurança acelerada. Por meio da correlação de ameaças sofisticada orientada por IA , as organizações podem revelar riscos latentes e vetores de ataque cruciais, permitindo um esforço concentrado nos riscos mais críticos.

9. Statista, **Tempo médio para identificar e conter violações de dados em todo o mundo, de 2017 a 2024**, acessado em 9 de dezembro de 2024.

194 dias

O tempo médio para identificar uma violação de dados[9]



©2025 Zscaler, Inc. Todos os direitos reservados.

Segurança de IA melhorada

As organizações estão adotando aplicativos de IA em ritmo acelerado. Infelizmente, aplicativos de IA como IA generativa (GenAI) e grandes modelos de linguagem (LLMs) introduziram riscos relevantes de violação de dados e não conformidade. Um relatório recente afirmou que 13% das organizações relataram violações de modelos ou aplicativos de IA[10], destacando que a IA está se tornando um alvo de alto valor.

As organizações que integram a GenAI em suas operações devem tomar medidas para evitar o uso negligente de dados sigilosos nesses modelos. As equipes de segurança devem priorizar a sinalização, marcação e classificação de dados para garantir que as equipes multifuncionais estejam utilizando a GenAI de forma responsável.

O DSPM pode aprimorar o controle e a proteção de dados em ambientes de GenAI com recursos integrados de AI-SPM. Ao identificar e categorizar dados meticulosamente, o DSPM impede que informações sigilosas sejam enviadas para LLMs, reduzindo o risco de violações de dados e não conformidade. O DSPM adota uma abordagem de “priorizar os dados", focando na segurança das informações que alimentam a IA, e não apenas na infraestrutura. Ao descobrir, classificar e monitorar dados continuamente ao longo de seu ciclo de vida, o DSPM ajuda a mitigar riscos de segurança exclusivos da IA, como envenenamento de dados, exposição de dados sigilosos e roubo de modelos.

Adotar um DSPM com recursos integrados de AI-SPM pode capacitar as organizações a inspirar confiança em seus aplicativos de IA. Ao fazer isso, elas não apenas protegem seus dados importantes, mas também tornam os aplicativos de IA mais confiáveis e seguros.



10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

©2025 Zscaler, Inc. Todos os direitos reservados.

Como usar o DSPM para proteger um cenário de dados diversificado

O uso estratégico do DSPM é fundamental na busca por uma segurança de dados mais robusta. Essas tecnologias oferecem o contexto e a automação necessários para gerenciar com eficiência as complexidades dos ambientes de dados modernos. Por meio de uma postura proativa, os líderes de segurança podem proteger dados sigilosos de forma mais eficaz, garantir a conformidade e mitigar os riscos associados a tecnologias progressivas como a GenAI.



“Até 2026, mais de 20% das organizações implantarão tecnologia de DSPM, devido aos requisitos urgentes para identificar e localizar repositórios de dados anteriormente desconhecidos e para mitigar os riscos de segurança e privacidade associados.”

Gartner, Análise de inovação: gerenciamento da postura de segurança de dados,
Brian Lowans, Joerg Fritsch, Andrew Bales,
28 de março de 2023

Gartner é uma marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e no mundo, e é usada aqui com a devida permissão. Todos os direitos reservados.

©2025 Zscaler, Inc. Todos os direitos reservados.

Zscaler DSPM

O Zscaler DSPM é a plataforma de proteção de dados integrada mais abrangente do mundo para proteger dados estruturados e não estruturados em SaaS, ambientes de nuvem pública (AWS, Azure, GCP), ambientes locais e terminais.

O Zscaler DSPM fornece visibilidade granular dos dados na nuvem, classifica e identifica dados e acesso e contextualiza a exposição dos dados e a postura de segurança, capacitando organizações e equipes de segurança a prevenir e remediar violações de dados na nuvem em grande escala.

O Zscaler DSPM adota uma abordagem unificada e baseada em IA para garantir uma forte higiene de dados em todos os armazenamentos de dados, incluindo IaaS, SaaS, ambientes locais, terminais e outros. Integrado nativamente à plataforma de segurança de dados da Zscaler, ele permite que você compreenda e controle totalmente todos os seus dados em uma única plataforma.

O Zscaler Data Security usa um mecanismo de DLP único e unificado para fornecer a melhor proteção de dados consistente em todos os canais. Ao seguir todos os usuários em todos os locais e controlar os dados em trânsito e em repouso, ele garante que os dados sigilosos sejam perfeitamente protegidos e que a conformidade seja alcançada

Para mais informações, visite zscaler.com/br/dp/dspm.

Explore o tour interativo do produto DSPM



Por que o DSPM pertence a sua estratégia de proteção de dados?

Assistir ao webinar sob demanda⟶

Leia o código QR para acessar recursos úteisdo DSPM:

©2025 Zscaler, Inc. Todos os direitos reservados.



zscaler™ | Experience your world, secured.™

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange™ baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos os direitos reservados. Zscaler™ e outras marcas registradas listadas em **zscaler.com/br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

+1 408.533.0288 **Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/br**