Zscaler Data Security Posture Management (DSPM)

Resumo da solução

Visão geral: proteção de dados no mundo centrado na nuvem

Os desafios de proteger grandes quantidades de dados empresariais em ambientes multinuvem incluem gerenciar a complexidade e a escala da proteção de dados; lidar com ameaças internas, violações de dados, acesso de terceiros e fornecedores e riscos da cadeia de suprimentos; e cumprir com regulamentações de dados. As organizações lutam para inventariar, classificar, controlar e proteger ativos de dados críticos, ao mesmo tempo em que os protegem de diversas ameaças. Somando-se a essa complexidade, há uma infinidade de locais de dados fragmentados, funções e permissões em diferentes ambientes.

Ambientes complexos	Volume de dados	Ataques direcionados e sofisticados	Acesso com excesso de privilégios
82% das violações envolvem dados armazenados na nuvem[1]	Estima-se que 175 ZB de dados serão armazenados na nuvem até 2025[2]	USD 4,88 milhões: o custo médio global de uma violação de dados em 2024[3]	80% das organizações sofreram violações de identidade[4]

Infelizmente, as soluções legadas de proteção de dados não foram projetadas para ambientes multinuvem dinâmicos. Ao mesmo tempo, os fornecedores de DSPM específicos oferecem abordagens isoladas que não se integram perfeitamente aos programas de proteção de dados existentes. As organizações precisam de uma abordagem nova e unificada para proteger seus dados na nuvem.

A Zscaler resolve esses desafios de segurança de dados em ambientes multinuvem com uma solução de gerenciamento da postura de segurança de dados (DSPM) totalmente integrada e sem agentes.

O que é DSPM?

"Data Security Posture Management (DSPM) fornece visibilidade sobre onde estão os dados sigilosos, quem tem acesso a esses dados, como eles foram usados e qual é a postura de segurança dos dados armazenados ou do aplicativo." — Gartner

O DSPM às vezes é chamado de segurança "focada em dados", invertendo o modelo de proteção adotado por outras tecnologias e práticas de segurança cibernética. Em vez de proteger os dispositivos, sistemas e aplicativos que armazenam, movem ou processam dados, o DSPM se concentra em proteger os dados diretamente, ao mesmo tempo em que complementa muitas outras soluções no conjunto de segurança de uma organização.

Mais especificamente, o DSPM envolve monitoramento, avaliação e otimização contínuos de controles de segurança para proteger dados sigilosos em plataformas multinuvem. Ao automatizar a identificação de dados sigilosos, bem como possíveis vulnerabilidades associadas, erros de configuração e violações de conformidade, o DSPM garante que as organizações abordem proativamente o risco da exposição de dados. Ao fazer isso, o DSPM as ajuda a fortalecer a postura geral de segurança de dados, minimizar o risco de violações de dados e atender aos requisitos de conformidade regulatória.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

Por que DSPM?

O foco principal das ferramentas de DSPM é avaliar e gerenciar o status de segurança do ambiente de dados de uma organização, encontrando pontos fracos, monitorando configurações de segurança e identificando possíveis ameaças a dados sigilosos. O DSPM vai além da política e analisa os dados em si.

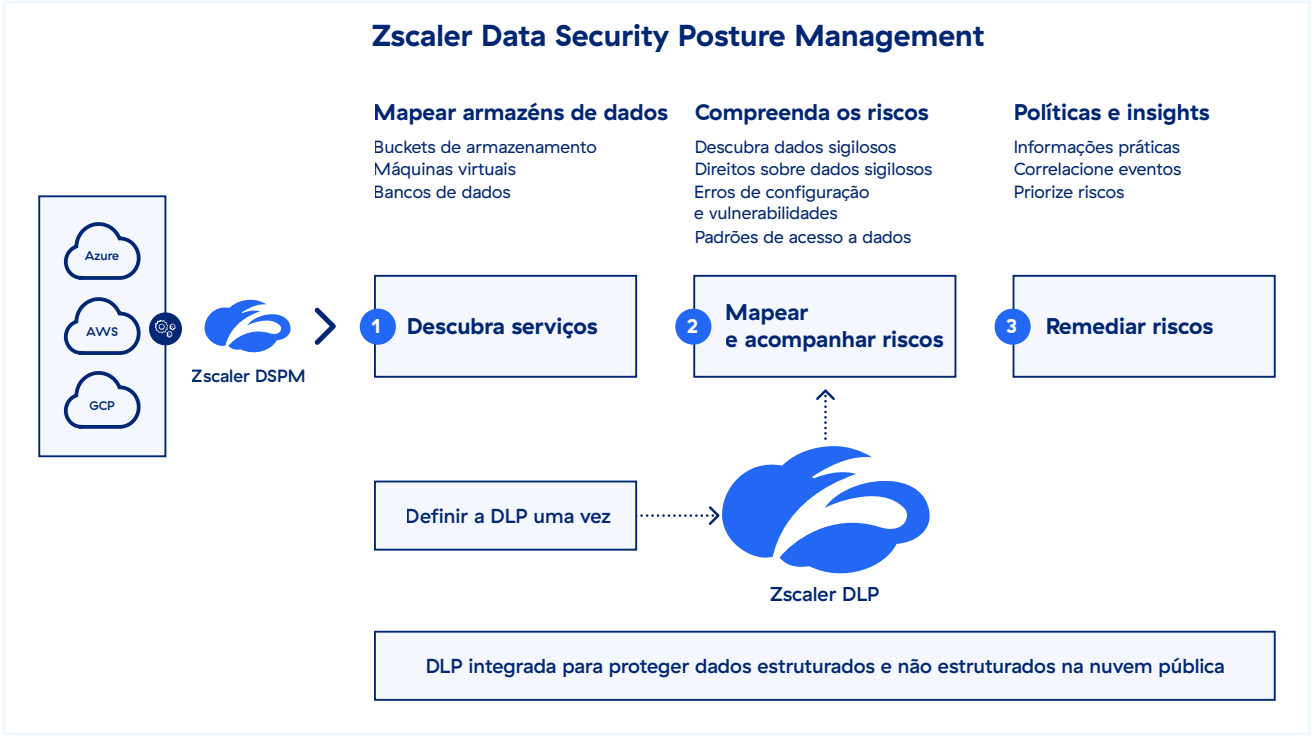
Ao verificar e categorizar dados, ele ajuda as organizações a entender completamente onde os dados sigilosos estão localizados e como estão sendo usados. Ele também ajuda a priorizar problemas identificados e evita alertas excessivos que poderiam fazer com que tais problemas fossem ignorados.

Casos de uso prático do DSPM incluem a detecção de vulnerabilidades de segurança (como criptografia) em ambientes de nuvem, a aplicação de políticas de acesso e o fornecimento de alertas e recursos de investigação para gerenciamento de incidentes.

Conheça o Zscaler DSPM

A Zscaler AI Data Protection é a plataforma de proteção de dados mais abrangente e totalmente integrada do mundo. Ela protege dados estruturados e não estruturados na web, serviços baseados em SaaS, ambientes de nuvem pública (AWS, Azure, GCP), aplicativos privados, email e terminais.

Como parte da plataforma da Zscaler, o Zscaler DSPM estende a segurança de dados robusta e de primeira classe para a nuvem pública. Ele fornece visibilidade granular em dados na nuvem, classifica e identifica dados e acesso, e contextualiza a exposição de dados e a postura de segurança, capacitando equipes de segurança a prevenir e remediar violações de dados na nuvem em larga escala.



Usando um único mecanismo de DLP unificado, o Zscaler DSPM oferece proteção de dados consistente em todos os canais. Ao seguir todos os usuários em todos os locais e controlar os dados em uso e em repouso, ele garante que os dados sigilosos sejam perfeitamente protegidos e que a conformidade seja alcançada.

Principais recursos do Zscaler DSPM

Descoberta de dados, classificação e inventário
Os métodos de verificação tradicionais são caros e exigem um esforço significativo para produzir resultados úteis. O Zscaler DSPM, com acesso mínimo a recursos em ambientes de nuvem (AWS, Azure e GCP), verifica armazenamentos de dados, descobre dados sigilosos e classifica os dados com precisão. Ele ajuda com:

- **Descoberta abrangente de dados:** o Zscaler DSPM monitora constantemente os ambientes de nuvem para descobrir automaticamente novos armazenamentos de dados à medida que são instanciados em ambientes de dados em constante mudança para economizar tempo e eliminar pontos cegos de dados.
- **Classificação precisa de dados:** o Zscaler DSPM usa mecanismos de DLP predefinidos e dicionários para classificação de dados. Ele oferece visibilidade sobre que tipo de dados sigilosos são armazenados em recursos na nuvem, a região, os arquivos que contêm dados sigilosos, a gravidade do risco associado aos dados sigilosos, etc. Ele também oferece flexibilidade para as organizações criarem ou replicarem as políticas existentes que estão disponíveis.
- **Inventário de dados preciso:** o Zscaler DSPM cria um mapa preciso e um inventário de ativos de dados, ajudando as equipes de segurança a localizar dados sigilosos e a entender quem tem acesso a eles e como estão sendo usados.

Com o Zscaler DSPM, as equipes de segurança ganham maior visibilidade dos dados na infraestrutura de nuvem. Isso torna muito mais fácil gerenciar e melhorar a postura de segurança de dados em ambientes multinuvem, abrangendo camadas complexas de SaaS, PaaS, IaaS e bancos de dados.

Mapear e rastrear exposições de dados

Os serviços e configurações de nuvem mudam com frequência, o que pode levar à exposição de dados. É essencial corrigir essas falhas de segurança antes que criminosos possam explorá-las. O Zscaler DSPM detecta recursos expostos publicamente, bem como vulnerabilidades ou configurações incorretas nos diferentes componentes (grupo de segurança de rede, balanceador de carga, rede virtual, etc.) associados ao recurso de dados. Isso ajuda com:

- **Análise de exposição:** determine a exposição pública, configurações incorretas e vulnerabilidades para armazenamentos de dados e serviços.
- **Avaliação de riscos:** agregue o nível geral de risco combinando o impacto e a probabilidade. Isso envolve categorizar os riscos em níveis alto, médio ou baixo.
- **Priorização de riscos:** ajude as equipes de segurança a filtrar o ruído e priorizar incidentes com base no risco e na gravidade.
- **Correlação avançada de ameaças:** correlacione ameaças, fatores de risco e rotas de ataque ocultas para minimizar riscos.
- **Inteligência de acesso adaptável:** obtenha uma visão granular, baseada em riscos e centrada no usuário de todos os caminhos de acesso a dados e configurações essenciais.

Correção de riscos

O Zscaler DSPM agiliza o gerenciamento de riscos com remediação orientada baseada no contexto, permitindo que as equipes de segurança corrijam facilmente problemas e violações na origem, evitando interrupções futuras. Os recursos incluem:

- **Investigação e resposta eficazes** para ajudar as equipes de segurança a entender rapidamente as possíveis causas-raiz durante investigações de eventos de segurança de dados.
- **Correção guiada e aprofundada** para ajudar equipes multifuncionais com fluxos de trabalho automatizados e orientação passo a passo com contexto completo para abordar riscos de segurança de dados e corrigir de forma eficaz.
- **Tempo de segurança mais rápido**, permitindo que as equipes configurem alertas personalizados em tempo real para acompanhar as rápidas mudanças nos dados e seu ambiente, acelerando a investigação e a resposta.
- **Integração perfeita** para fácil integração com ferramentas e plataformas ITSM, SIEM ou ChatOps existentes para alertas, correção, orientação e fluxos de trabalho.

Experimente o Zscaler DSPM

Solicite uma demonstração
Veja o Zscaler DSPM em ação com uma demonstração guiada.

Solicite uma demonstração

Baixe o guia de compras do DSPM
Saiba mais sobre os 5 principais requisitos a serem considerados ao selecionar o DSPM certo para sua organização.

Baixe agora

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

Apêndice

Glossário de termos

- Gerenciamento de postura da segurança de dados (DSPM)
- Plataforma de proteção de aplicativos nativos da nuvem (CNAPP)
- Gerenciamento de postura de segurança na nuvem (CSPM)
- Gerenciamento de direitos de infraestrutura na nuvem (CIEM)

Outras leituras

Leia o código QR para acessar os recursos do DSPM

Sessões sob demanda

- Palestra: Sessão Zenith Live '24, Zscaler DSPM: dados seguros na nuvem com uma plataforma totalmente integrada — Saiba mais sobre a jornada de DSPM da Inter&Co's.
- Webinar: Por que o DSPM pertence a sua estratégia de proteção de dados?

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