COHESITY

GUIA DO COMPRADOR

ENFRENTE RISCOS DE DADOS E IA COM A SOLUÇÃO DE DSPM CERTA

Resumo executivo

Dados confidenciais estão agora distribuídos em suas plataformas de nuvem, SaaS, bancos de dados, backups, infraestrutura híbrida, NAS e diversos outros locais. Sua organização provavelmente já tem mais dados do que pode facilmente governar. Mas é difícil entender onde estão seus dados mais confidenciais, o quanto eles estão expostos, quem tem acesso a eles e se esse acesso é apropriado.

Isso cria uma tempestade perfeita que aumenta os riscos de negócios para a alta gestão. E o desafio está crescendo: enquanto as pessoas seguem acessando, alterando e movendo esses dados, os agentes de IA estão introduzindo riscos novos e cada vez maiores.

E é devido a essas lacunas de segurança e proteção que o gerenciamento da postura de segurança de dados (DSPM) se tornou uma prioridade estratégica para os líderes empresariais modernos.

89% **dos líderes de segurança indicam que o status quo da segurança de dados em sua empresa é um problema.**

39% **dos líderes de segurança indicam que as tecnologias mais antigas são insuficientes para os requisitos atuais.**

60% **das empresas não têm visibilidade em pelo menos metade de seu patrimônio de dados**[1].

[1]Relatório técnico da Omdia: Achieving Cyber Resilience With Actionable Data Intelligence [Alcançando resiliência cibernética com inteligência de dados acionável]

Uma solução de DSPM moderna deve ajudar sua organização a fazer muito mais do que inventariar dados. Ela deve ajudar a reduzir ativamente os riscos, fortalecer a resiliência cibernética e esclarecer perguntas críticas durante a resposta a incidentes, exercícios de segurança ou auditorias:

- Onde e quais são nossos dados confidenciais?
- Quem ou o que tem acesso a esses dados?
- O que devemos corrigir primeiro?
- Como reduzimos o risco sem retardar a inovação e o crescimento dos negócios?
- Os dados estão protegidos e podem ser recuperados de forma rápida, segura e em conformidade?

Para líderes de segurança, isso significa passar da visibilidade para a redução de risco acionável, antes e depois da ocorrência de um ataque.

Este guia se destina a equipes que avaliam soluções DSPM, para que sua organização possa selecionar a solução certa para suas necessidades.

Inventariar não é suficiente.

A verdadeira pergunta de compra não é se uma solução pode mostrar onde estão os dados. É preciso saber se a solução é capaz de identificar e mostrar *por que* os dados são de alto risco e o que sua organização pode fazer para remediar esse risco.

O que o DSPM soluciona

Um dos erros mais comuns que as organizações cometem ao avaliar o DSPM é tratá-lo como uma ferramenta de descoberta simples. Uma solução de DSPM envolve muito mais do que visibilidade. A solução certa deve ajudar a solucionar problemas relacionados à postura de risco dos dados.

Seguem cinco problemas que sua solução de DSPM deve ajudar a resolver:

Problema	Como o DSPM resolve
Não sei onde estão meus dados confidenciais.	Muitas organizações não podem responder com confiança onde residem seus dados de maior valor ou regulamentados em ambientes de nuvem, SaaS e híbridos. Por que este é o status quo? As ferramentas tradicionais de segurança de dados estão isoladas em tipos específicos de dados, determinados modelos de implantação ou casos de uso específicos. Mesmo quando há algum inventário, ele geralmente está incompleto, desatualizado ou desconectado do contexto de risco. É preciso contar com uma arquitetura moderna e nativa da nuvem para acompanhar o volume e a expansão dos dados.
Não sei quem ou o que está acessando (ou pode acessar) meus dados.	O funcionário típico interage com aproximadamente 36 serviços em nuvem por dia, em mais de 200 ferramentas de colaboração. As informações confidenciais se espalham pelas plataformas e são frequentemente compartilhadas fora dos controles de governança estabelecidos. Os dados confidenciais ficam ainda mais arriscados quando são superexpostos, têm permissões excessivas, são compartilhados de forma muito ampla, armazenados no local errado ou acessíveis a mais identidades (inclusive não humanas) do que o pretendido. Sua solução de DSPM deve ajudar a entender quais dados estão em risco, e não só quais correspondem a uma política de classificação.
Não sei quais riscos de dados devo priorizar primeiro para remediação.	A maioria dos ambientes empresariais contém grandes volumes de dados confidenciais. No entanto, nem todos os riscos de dados têm a mesma urgência. As equipes precisam de uma maneira de distinguir o ruído de fundo da exposição significativa. A solução certa deve ajudar sua organização a se concentrar nos problemas com o maior impacto potencial nos negócios, com base em sensibilidade, acesso, exposição, ambiente e contexto de negócios aprendido.
Não consigo remediar riscos de dados de forma rápida ou automática.	O contexto de dados – combinado com uma integração profunda em toda a cadeia de ferramentas de segurança – é essencial para reduzir o tempo médio de resposta (MTTR) na remediação de dados que estão em alto risco. Os métodos tradicionais de segurança de dados dependem muito de padrões e tags, sobrecarregando as equipes com alertas ruidosos que muitas vezes não têm credibilidade. As soluções de DSPM devem promover a ação. As descobertas devem ser compreensíveis, atribuíveis e rastreáveis. As equipes de segurança e TI devem ser capazes de agir sobre elas com confiança.
Quando preciso recuperar dados, é lento, arriscado e caro.	Os dados secundários (como backups) são críticos em matéria de resposta e recuperação de incidentes. Esses dados também podem introduzir riscos e possíveis violações de conformidade que precisam ser abordados. As soluções modernas de DSPM devem fortalecer os resultados de resiliência cibernética e fornecer inteligência de dados para ajudar a assegurar a aplicação dos níveis certos de proteção. Os dados confidenciais devem ser priorizados e recuperados em conformidade durante a resposta a incidentes.

Qual é a “boa” abordagem

Antes de avaliar fornecedores, sua organização precisa decidir qual seria a “boa” abordagem. Seguem cinco áreas em que uma solução de DSPM moderna deve se destacar:

Implementar rapidamente e dimensionar perfeitamente, sem limites

Uma boa descoberta deve ajudar a obter rapidamente uma visão mais completa de sua exposição sem exigir um ciclo de implementação longo e pesado antes que o valor apareça.

As organizações devem esperar uma varredura contínua de centenas de petabytes, sem que isso comprometa o desempenho. O fornecedor certo oferecerá cobertura ampla nos principais ambientes, inclusive armazenamentos de dados em nuvem, aplicativos SaaS, sistemas de arquivos e bancos de dados no local, quando for o caso.

Eliminar pontos cegos com descoberta e classificação precisas

Uma descoberta robusta ajuda a evitar que resultados inferiores contaminem todos os resultados posteriores. Se a ferramenta de DSPM perder locais críticos, classificar informações confidenciais incorretamente ou exigir ajuste manual demais, as descobertas serão menos úteis ou até mesmo irrelevantes.

A solução de DSPM certa revela pontos cegos adaptando-se a seu ambiente e classificando dados automaticamente (inclusive propriedade intelectual e dados exclusivamente importantes para seus negócios).

Priorizar o risco real, não o ruído

O tempo é limitado, e nenhuma equipe pode remediar tudo de uma vez. Uma solução de DSPM forte combina exposições e contexto para se concentrar nos maiores perigos. Ela deve priorizar o risco de dados altamente confidenciais com exposições amplas.

Isso requer recursos avançados para correlacionar sensibilidade dos dados, finalidade do negócio, identidades, atividade de acesso e exposição para revelar o risco real para os negócios.

Automatizar a remediação em escala

Soluções de DSPM modernas precisam ajudar as organizações a reduzir a exposição, e não só a observá-la. As organizações devem buscar opções de DSPM que forneçam remediações prontas para uso. Por exemplo, as principais soluções oferecem controles com um único clique para revogar acesso, mascarar dados, disparar fluxos de trabalho predefinidos e encaminhar problemas diretamente aos proprietários de dados, tudo com o contexto necessário para resolver problemas rapidamente.

Isso é particularmente importante em escala empresarial, quando há o envolvimento de muitas equipes. Geralmente, as equipes de segurança identificam o problema, mas a remediação pode depender de diferentes grupos, como administradores de armazenamento, proprietários de dados, equipes de identidade ou partes interessadas do negócio. Quanto mais claramente uma solução oferecer suporte a essa transferência, maior a probabilidade de gerar resultados significativos que melhorem sua postura de segurança.

Fortalecer a segurança antes e depois dos incidentes

Já abordamos a redução proativa de riscos antes que uma violação ocorra. A solução de DSPM certa também pode fornecer a inteligência de dados e o contexto necessários para fortalecer os esforços de recuperação, assegurando que as equipes de segurança e proteção de dados entendam onde residem os dados confidenciais, quais ativos são mais críticos e se as proteções apropriadas foram aplicadas às joias da coroa da organização.

Com uma visão clara dos dados sensíveis e críticos para os negócios, sua ferramenta de DSPM deve orientar e aprimorar as estratégias de proteção de dados que sustentam a resiliência cibernética. Isso ajudará a priorizar os dados mais importantes durante a recuperação, acelerar a resposta a incidentes com melhor contexto e reduzir custos e complexidade ao identificar e eliminar dados obsoletos, redundantes ou de baixo valor.

O resultado é um ciclo de feedback contínuo entre visibilidade, proteção, resposta e recuperação. Com a solução de DSPM certa, sua organização deve ser capaz de conectar essas funções para ser capaz de, em lugar de esforços de segurança isolados, passar a adotar uma estratégia mais holística e completa de segurança de dados e resiliência cibernética.

Kit de avaliação de fornecedores

Perguntas críticas a fazer aos fornecedores

Estas perguntas ajudarão sua organização a avaliar sua lista de produtos de DSPM pré-selecionados.

Sobre descoberta e cobertura:

- Para quais ambientes de nuvem, SaaS, IA, bancos de dados e híbridos vocês oferecem cobertura hoje?
- Como vocês identificam e classificam dados confidenciais em diferentes tipos de dados? Quanto tempo isso leva normalmente?
- Como vocês lidam com dados estruturados e não estruturados? Vocês oferecem melhor suporte para um tipo ou para o outro?
- Que nível de ajuste é necessário antes que os resultados sejam utilizáveis?
- Como vocês ajudam os clientes a validar a cobertura e a confiança logo no início?

Sobre controles de exposição e acesso:

- Como vocês determinam se dados confidenciais estão superexpostos? Vocês podem mostrar quais identidades, grupos ou usuários têm acesso a dados confidenciais?
- Como vocês identificam acesso amplo, excessivo ou arriscado?
- Como vocês conectam o contexto de acesso à sensibilidade dos dados?
- Vocês são capazes de impedir que dados confidenciais sejam inseridos ou saiam de modelos e sistemas de IA?
- Vocês podem mostrar como sua solução destaca os problemas de maior risco?

Sobre priorização e remediação de riscos:

- Como vocês classificam ou priorizam as descobertas? Quais fatores influenciam a gravidade ou a pontuação de risco?
- Vocês podem mostrar como as equipes passam de muitas descobertas para um plano de ação gerenciável?
- Como sua solução orienta a remediação?
- As descobertas podem ser atribuídas às equipes certas ou aos responsáveis?
- Os insights podem ser totalmente integrados às plataformas de proteção de dados e fornecer melhores resultados de segurança e recuperação?

Sobre tempo de retorno e implantação:

- O que a implantação inicial exige da nossa equipe?
- Com que rapidez podemos esperar descobertas úteis?
- Como deve ser o sucesso nos primeiros 30, 60 e 90 dias?

Sinais de alerta a observar

Visibilidade limitada sobre o risco de acesso

O acesso a dados confidenciais é o maior risco. Se um fornecedor não puder mostrar claramente quem (ou o que) pode acessar os dados e quais riscos existem, essa é uma limitação séria.

As constatações não estão conectadas ao risco e ao contexto de negócios individuais

Cada empresa é diferente. O risco representado por dados confidenciais ou propriedade intelectual exposta pode variar com base no que é importante para essa organização. As constatações devem se basear no contexto aprendido e em classificadores para fornecer recomendações precisas de correção de riscos.

Incapacidade de vincular o risco de dados aos resultados de resiliência cibernética

Otimizar a postura de risco de dados e IA é fundamental para a resiliência cibernética. A inteligência de dados deve ser utilizada para orientar a segurança de dados proativa e permitir melhores resultados de recuperação. As constatações não devem ficar em silos, especialmente porque a correção geralmente envolve equipes multifuncionais.

O valor depende de esforço manual excessivo

Um produto que requer ajuste extensivo, interpretação ou design de processo do cliente pode adicionar custo operacional e complexidade contínuos.

Tabela de comparação de fornecedores

Use esta tabela para comparar fornecedores quanto aos principais recursos necessários para uma estratégia eficaz de DSPM. Ao analisar cada linha, considere não apenas a existência de um recurso, mas como ele é fornecido na prática*.

Para tornar as comparações de fornecedores mais consistentes e objetivas, cada capacidade pode ser avaliada usando um modelo de pontuação simples de 0 a 5. Essa abordagem ajuda as equipes a ir além de uma comparação básica do tipo "lista de verificação" e avaliar a força relativa, a maturidade e a usabilidade prática de cada capacidade. Uma pontuação mais elevada deve indicar que a capacidade não está apenas disponível, mas também pronta para uso em empresas, é operacionalmente eficiente e comprovadamente proporciona valor em escala.

Pontuação	Definição
5	A melhor capacidade da categoria que é totalmente entregue, altamente automatizada, escalável e bem integrada
4	Capacidade forte com funcionalidade sólida e pequenas lacunas
3	Capacidade adequada que atende aos requisitos essenciais, mas tem limitações de profundidade, escala ou usabilidade
2	Cobertura básica ou parcial com lacunas perceptíveis, esforço manual ou aplicabilidade limitada
1	Capacidade mínima, funcionalidade em estágio inicial ou suporte altamente restrito
0	Sem suporte ou sem evidência significativa fornecida

Categoria	Fornecedor 1	Fornecedor 2	Fornecedor 3	Observações
Arquitetura nativa da nuvem para implementação rápida e sem agente				
Descoberta contínua de dados em escala e velocidade				
Classificação de dados com tecnologia de IA				
Contextualização de dados				
Riscos mapeados para regulamentos				
Controles de acesso e aplicação adaptáveis				
Detecção e resposta de dados em tempo real				
Alertas contextualizados				
Fluxos de trabalho de remediação integrados				
Integração perfeita com plataformas de proteção de dados				
Total				

**As pontuações devem se basear no que está geralmente disponível hoje, não em afirmações do roadmap. Cada pontuação deve ser validada com demonstrações de produtos, referências de clientes, documentação, requisitos de implantação e prova da profundidade de integração.*

O resultado

Selecionar uma solução de DSPM é mais do que uma simples decisão de ferramenta. Os riscos são bem elevados. Os dados continuam se proliferando e espalhando a uma taxa alarmante, e abordagens manuais ou tecnologia legada não conseguem acompanhar o ritmo. A solução de DSPM certa ajudará sua organização a gerar clareza, concentrar suas equipes, reduzir riscos e fortalecer os resultados de segurança de dados e resiliência cibernética. Essa solução gerará retorno no longo prazo, pois ajudará sua organização a proteger e assegurar os dados que sustentam modelos, sistemas e agentes de IA.

Saiba mais sobre nossa solução de DSPM e como ela pode otimizar sua postura de risco de dados e de IA. Ou entre em contato conosco hoje mesmo.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-PT 5-2026