

Proofpoint Data Security Posture Management

Descubra e proteja dados em plataformas de SaaS, infraestrutura de nuvem e ambientes locais



Principais vantagens

- **Classificadores de IA** identificam dados confidenciais e específicos do negócio sem regras manuais em ambientes de SaaS, de nuvem e locais
- O **mapa de risco de dados** prioriza o risco com base na confidencialidade, no acesso, no impacto sobre os negócios e na movimentação dos dados
- A **governança de acesso com contexto empresarial simplifica a remediação direta e delegada e a criação de políticas de DLP**
- A **segurança de dados de IA integrada** identifica dados confidenciais expostos a aplicativos de IA e pipelines de treinamento de IA
- Dashboards de conformidade monitoram a postura em mais de 25 estruturas com relatórios decisivos
- A segurança de dados unificada compartilha inteligência entre DSPM, governança de acesso, DLP e segurança de dados para IA

A explosão de dados corporativos

A ascensão da IA, das plataformas de banco de dados como serviço (DBaaS) e do armazenamento em nuvem acelerou a proliferação de dados em ambientes de software como serviço (SaaS), de nuvem e locais. À medida que dados confidenciais se espalham por sistemas e pipelines, as equipes têm dificuldades para ver onde esses dados residem. Isso causa pontos cegos, aumenta o risco de exposição e complica a conformidade.

Acesso a dados por pessoas e IA fora de controle

A proliferação de dados é amplificada pela falta de controle sobre quem — e o que — pode acessar informações confidenciais. Usuários com privilégios excessivos, ferramentas não autorizadas e compartilhamento arriscado criam riscos associados a pessoas. Modelos de IA, agentes e fluxos de trabalho automatizados acrescentam novos caminhos de acesso não humanos. Sem uma governança forte, configurações incorretas, permissões excessivas e supervisão fraca podem causar vazamentos de dados, uso indevido e violações de conformidade.

55%

das organizações dizem que de 21% a 40% de seus dados são confidenciais.

Fonte: Proofpoint

68%

das organizações dizem que o uso inadequado de IA expôs dados confidenciais.

Fonte: Proofpoint

Descubra, classifique, governe e proteja dados

O Proofpoint Data Security Posture Management (DSPM) ajuda as equipes a recuperar o controle sobre dados espalhados e a reduzir o acesso arriscado por pessoas e IA. Ele descobre e classifica dados confidenciais, mostra quem e o que pode acessá-los e classifica os riscos. As equipes podem corrigir exposições mais rapidamente e fortalecer a segurança dos dados.

Capacidades exclusivas

Como parte do Proofpoint Data Security, o Proofpoint DSPM com governança de acesso a dados integrada compartilha sua estrutura de classificação de dados com o Proofpoint Enterprise DLP e com o Proofpoint Data Security for AI. Classificadores de IA identificam categorias de documentos confidenciais por contexto e significado, e não apenas por padrões. Isso melhora a descoberta e a classificação. Também ajuda as equipes a governar o acesso, criar políticas de prevenção de perda de dados (DLP) e proteger dados em ambientes de nuvem, de SaaS, locais e de IA.

O Proofpoint DSPM detecta permissões excessivas, acesso arriscado, configurações incorretas, dados obsoletos e caminhos de ataque. O mapa de risco de dados mostra onde os dados confidenciais residem, o quão amplamente expostos eles estão e quais usuários, aplicativos e ferramentas de IA podem acessá-los. Fluxos de trabalho de governança de acesso a dados oferecem suporte para remediação em massa e delegada. As descobertas do Proofpoint DSPM podem ser convertidas em regras de DLP com uns poucos cliques. Elas ajudam as equipes a reduzir a exposição e a aplicar o princípio de privilégios mínimos.

O Proofpoint DSPM permite uma adoção de IA mais segura. Ele encontra dados confidenciais expostos a copilotos, grandes modelos de linguagem (LLMs) e aplicativos de IA.

Juntos, o Proofpoint DSPM com governança de acesso a dados, o Proofpoint Enterprise DLP e o Proofpoint Data Security for AI oferecem às equipes uma maneira única de descobrir, governar e proteger dados confidenciais durante todo seu ciclo de vida.

Classifique autonomamente documentos críticos para os negócios

O Proofpoint DSPM oferece uma classificação de dados líder de mercado. Ele usa expressões regulares, processamento de linguagem natural e LLMs para melhorar o desempenho e reduzir o uso de recursos.

O Proofpoint Autonomous Custom Classification (ACC) identifica documentos específicos da organização sem regras manuais ou treinamento. Isso ajuda as equipes a descobrir dados de propriedade da empresa, eliminar pontos cegos e melhorar a detecção de riscos e a aplicação de políticas.

O Proofpoint DSPM também pode aplicar rótulos de confidencialidade do Microsoft Information Protection (MIP) com base em classificadores de IA. Isso ajuda as equipes a aplicar políticas de governança, apoiar a conformidade e proteger os dados da Microsoft contra acesso não autorizado ou uso indevido.

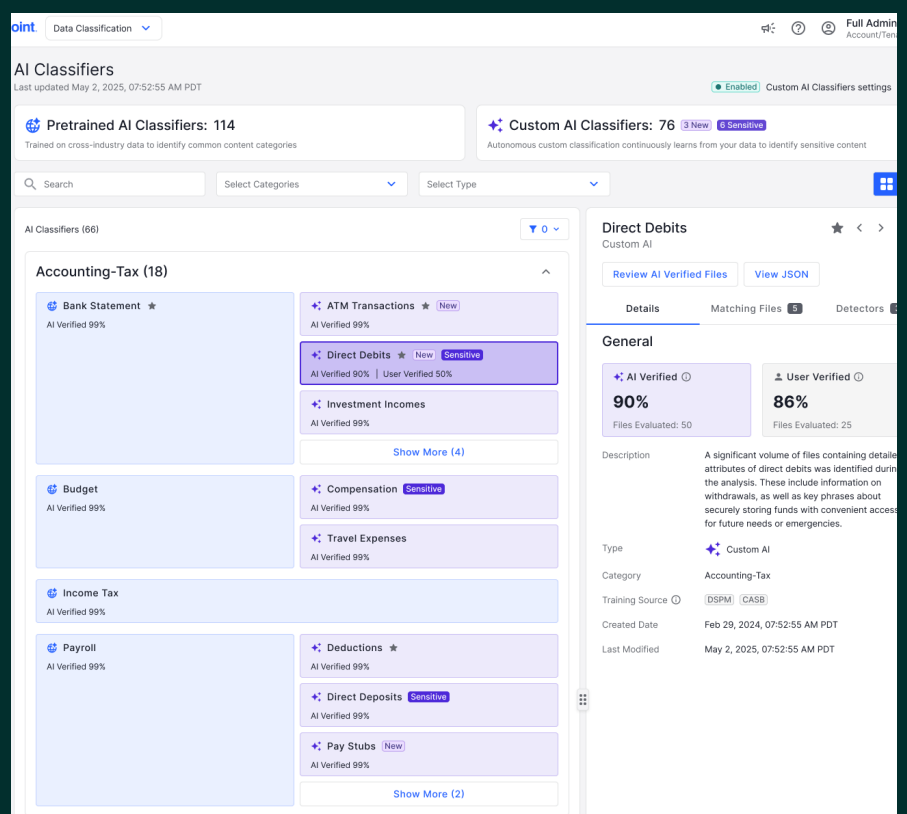


Figura 1. Classificadores de IA pré-treinados e autônomos do Proofpoint DSPM identificam documentos padrão e específicos de negócios, inclusive contratos, registros financeiros, código-fonte e registros de funcionários.

Mapeamento de riscos de acesso a dados

O mapa de risco de dados mostra onde residem os dados confidenciais em sistemas de SaaS e locais. Ele mostra o quão amplamente compartilhados estão os dados e quais usuários, aplicativos ou ferramentas de IA podem acessá-los. Ele combina classificação de IA com insights sobre acesso e uso.

As equipes de segurança podem encontrar dados superexpostos, classificar riscos, validar correções e manter o acesso apropriado à medida que o uso de IA cresce. As descobertas de risco de dados consideram a confidencialidade dos dados, os padrões de acesso e a exposição. Isso ajuda as equipes a se concentrarem em dados de alto valor e alto risco, ao mesmo tempo em que reduzem custos e diminuem a superfície de ataque da empresa.

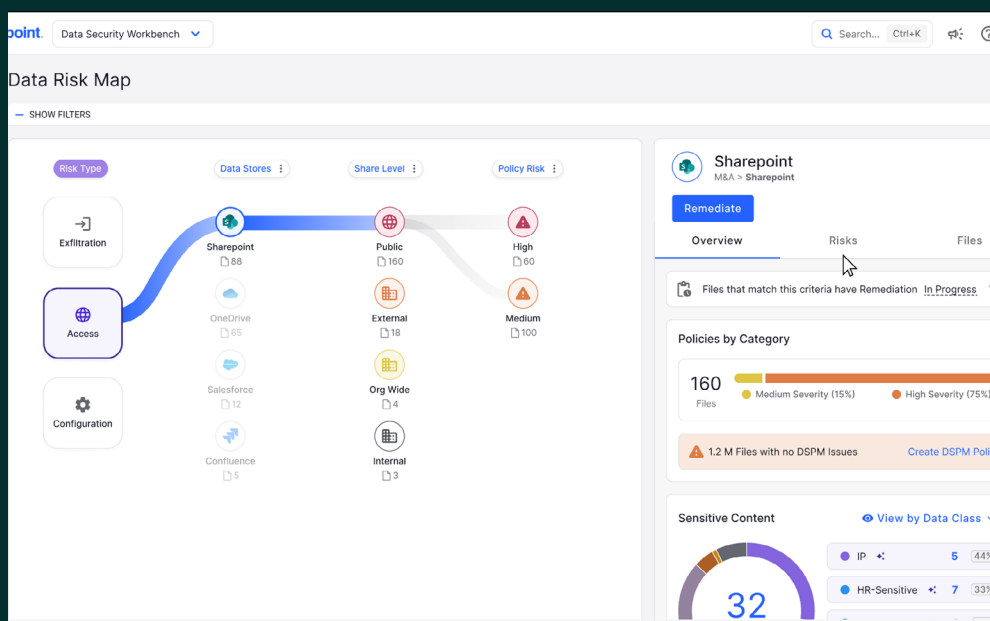


Figura 2. O mapa de risco de dados mostra quais repositórios contêm dados confidenciais, o escopo do compartilhamento de dados e o acesso por usuários, aplicativos e ferramentas de IA.

Priorize o risco com base no valor monetário dos dados

As equipes de segurança de dados precisam proteger muitos armazenamentos de dados. Porém, nem todo armazenamento tem o mesmo valor ou risco. O Proofpoint DSPM usa tecnologia de avaliação de dados para estimar o custo de violação para cada armazenamento de dados. Isso ajuda as equipes a se concentrarem no que é mais importante. O Proofpoint DSPM também inclui mais de 200 descobertas predefinidas de acesso e exposição com detecção de combinações tóxicas. Essa matriz de risco destaca armazenamentos de alto risco e alto impacto financeiro.

Minimize dados obsoletos

Em sistemas de SaaS e locais, o Proofpoint DSPM encontra e remove arquivos que não foram acessados recentemente. Classificadores de IA ajudam as equipes a manter dados críticos para os negócios quando necessário. Em ambientes de infraestrutura como serviço (IaaS), o Proofpoint DSPM encontra armazenamentos de dados desnecessários. Isso inclui dados ocultos, duplicados e abandonados, como amostragens e backups obsoletos.

Isso reduz os custos de armazenamento, diminui a superfície

de ataque e simplifica o gerenciamento de dados. As equipes mantêm apenas dados relevantes e ativos.

Imponha acesso com privilégios mínimos

O Proofpoint DSPM oferece suporte para acesso com privilégios mínimos ao encontrar usuários com permissões excessivas, acesso não utilizado e contas de risco em armazenamentos de dados. Isso dá suporte a uma governança de acesso a dados mais forte e a Zero Trust.

O Proofpoint DSPM analisa funções de gerenciamento de identidade e acesso (IAM), permissões, concessões de banco de dados e outros controles de acesso para identidades humanas e de máquina. Ele mostra quem pode acessar dados confidenciais, quase em tempo real. As equipes podem remover permissões desnecessárias e reduzir a exposição.

O Proofpoint DSPM também sinaliza contas com proteção insuficiente em ambientes de SaaS e de plataforma como serviço (PaaS). Exemplos incluem usuários com acesso a dados confidenciais, mas sem autenticação por múltiplos fatores (MFA), contas inativas e aplicativos com privilégios de administrador excessivos.

Detecte caminhos de ataque em ambientes de nuvem

O Proofpoint DSPM coleta informações sobre recursos de computação e rede, bem como serviços de PaaS e SaaS, entre provedores de nuvem. Ele detecta configurações incorretas e vulnerabilidades nesses recursos. Um gráfico mostra os caminhos que um atacante poderia usar para alcançar dados confidenciais. O monitoramento quase em tempo real ajuda as equipes a identificar alterações que aumentam a exposição.

Insights sobre confidencialidade dos dados, padrões de acesso e riscos também ajudam ferramentas de DLP e de detecção e resposta a dados (DDR).

Governe o acesso diretamente ou por delegação

Em sistemas de SaaS e locais, os fluxos de trabalho do Proofpoint DSPM transformam insights de exposição em ação. À medida que ferramentas de IA como o Microsoft Copilot aumentam o impacto do conteúdo compartilhado em excesso, a redução do acesso excessivo torna-se crítica. Administradores podem revogar links públicos, compartilhamentos externos e acesso em nível de domínio no Google Workspace e no Microsoft

365. Isso permite remediação em escala empresarial.

As equipes de segurança não podem julgar o nível de acesso correto para cada arquivo. Fluxos de trabalho de governança de acesso a dados permitem que elas atribuam revisões de acesso aos proprietários do conteúdo. Campanhas automatizadas, lembretes e rastreamento tornam a governança mais fácil de sustentar.

A integração com o Proofpoint Enterprise DLP estende as proteções além dos dados estacionários. Dados confidenciais classificados e riscos priorizados pelo Proofpoint DSPM podem ser mapeados para políticas de DLP. Isso oferece suporte a uma proteção consistente e remediação automatizada em canais de e-mail, endpoint, nuvem e colaboração.

Em ambientes de IaaS e PaaS, recomendações e insights decisivos ajudam as equipes a reduzir exposições rapidamente. Integrações com plataformas de tíquetes, notificações e automação ajudam operadores de segurança a colaborar com equipes de DevOps e de engenharia de plataforma por meio de fluxos de trabalho já existentes.

Mantenha-se alinhado com estruturas de conformidade

O Proofpoint DSPM encontra lacunas de privacidade e segurança em mais de 25 estruturas de conformidade regulatória. Estas incluem a lei de IA da UE, RGPD, HIPAA, NIST, CMMC e SOC 2, entre outras.

As violações são marcadas por estrutura e por controle, para que os analistas possam ver o impacto sobre a conformidade.

Os relatórios mostram o status de conformidade em toda a infraestrutura, com visualizações por conta, por recurso e por estrutura. Isso ajuda as equipes a corrigir vulnerabilidades, preparar-se para auditorias e manter a conformidade.

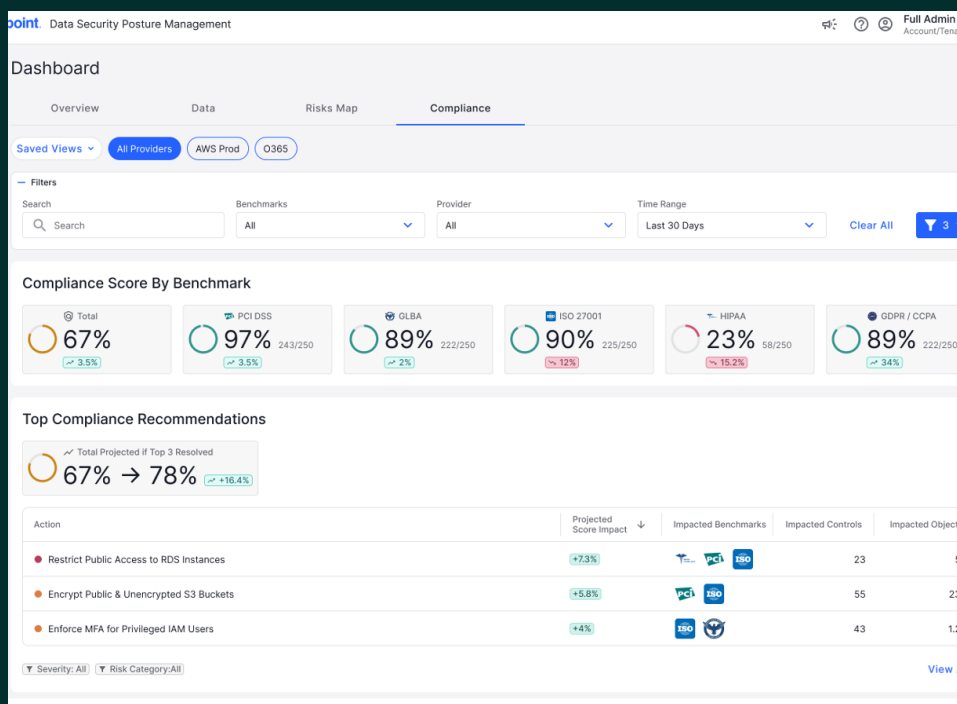


Figura 3. Dashboard que destaca a postura de conformidade.

Reduza os riscos de exposição de dados na IA

O Proofpoint DSPM ajuda as organizações a expandir a IA encontrando dados confidenciais expostos a aplicativos e fluxos de trabalho de IA.

O Proofpoint DSPM fornece insights sobre exposição para o dashboard do Proofpoint Data Security for AI. O dashboard proporciona uma visão central dos riscos de dados em aplicativos de IA aprovados e não aprovados. O Proofpoint DSPM também monitora configurações incorretas de aplicativos de IA e ajuda as equipes a corrigi-las. Isso reduz o risco de vazamento, fortalece a governança de dados de IA e apoia uma adoção segura.

O Proofpoint DSPM protege LLMs personalizados e aplicativos de IA em plataformas como AWS Bedrock e Azure ML. Ele detecta dados confidenciais inseridos em modelos de base, modelos personalizados e fluxos de trabalho de geração aumentada por recuperação (RAG).

O Proofpoint DSPM também fornece APIs especializadas para segurança de LLM. Elas analisam os dados confidenciais que fluem para dentro e para fora de LLMs em tempo real. Elas também proporcionam governança e visibilidade sobre o uso de dados e se integram aos fluxos de trabalho dos clientes.

Plataformas e tecnologias suportadas

O Proofpoint DSPM descobre e classifica dados em muitas plataformas e serviços. Ele oferece suporte a uma ampla gama de armazenamentos de dados, desde bancos de dados relacionais até NoSQL e armazenamentos de chave-valor. Isso proporciona às equipes visibilidade sobre dados estruturados, não estruturados e semiestruturados.

O suporte abrange as principais plataformas de nuvem e de SaaS. Exemplos incluem AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, LLMs e copilotos.

A estrutura comum de descoberta e classificação ajuda a Proofpoint a adicionar suporte a novos armazenamentos de dados rapidamente.

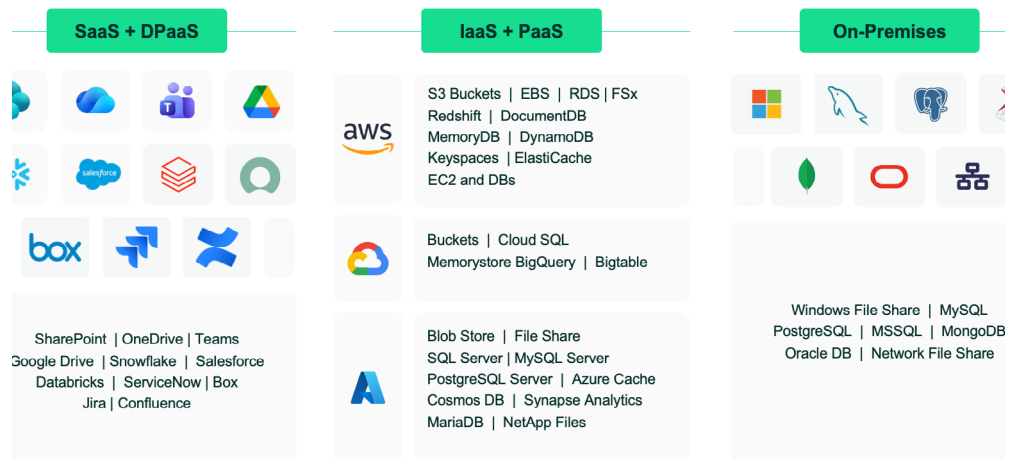


Figura 4. O Proofpoint DSPM descobre e classifica dados em uma ampla gama de plataformas e serviços.

Conclusão

À medida que as organizações adotam a IA e gerenciam mais dados, elas precisam saber onde os dados confidenciais se encontram, quem pode acessá-los e como eles são usados. O Proofpoint DSPM reduz a exposição classificando dados confidenciais, avaliando riscos, encontrando acesso excessivo e aplicando o princípio de privilégios mínimos em ambientes de nuvem, de SaaS, locais e de IA.

Como parte do Proofpoint Data Security, o Proofpoint DSPM trabalha com o Proofpoint Enterprise DLP. Juntos, eles ajudam as equipes a descobrir, classificar, governar e proteger dados confidenciais. As organizações podem fortalecer a conformidade, assegurar a adoção da IA, reduzir riscos e proteger suas informações mais valiosas.

Sobre a Proofpoint, Inc. A Proofpoint, Inc. é líder global em cibersegurança centrada em pessoas e agentes, protegendo a forma como pessoas, dados e agentes de IA se conectam por e-mail, nuvem e ferramentas de colaboração. A Proofpoint é uma parceira confiável de mais de 80 empresas da Fortune 100, mais de 10.000 grandes corporações e milhões de organizações menores, ajudando a combater ameaças, prevenir perda de dados e desenvolver resiliência, tanto de pessoas quanto de fluxos de trabalho de IA. A plataforma de segurança de colaboração e de dados da Proofpoint ajuda organizações de todos os tamanhos a proteger e capacitar suas equipes para que possam adotar a IA de forma segura e confiante. Saiba mais em www.proofpoint.com/br.

Conecte-se com a Proofpoint: [LinkedIn](#)

Proofpoint é uma marca registrada ou marca comercial da Proofpoint, Inc. nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais contidas neste documento são propriedade de seus respectivos donos.