Forcepoint DSPM



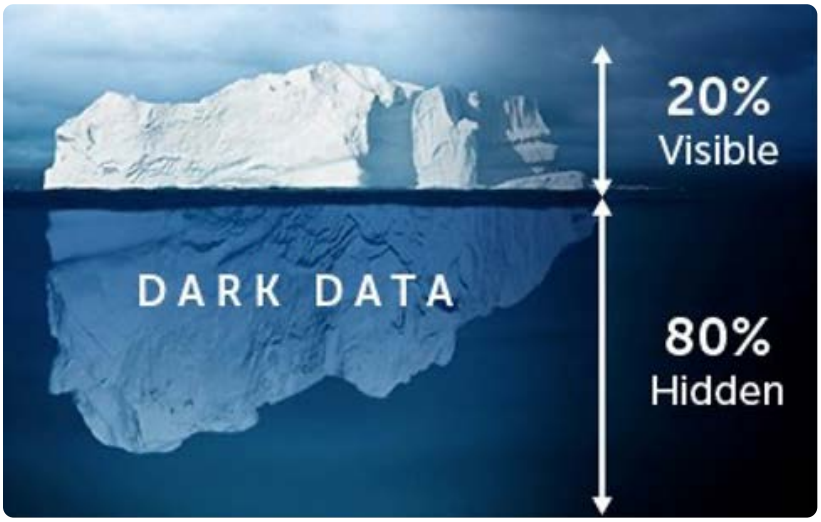
Forcepoint

Brochure

A transformação com IA é a próxima evolução da transformação digital

Seus dados estão seguros nesta nova era?

As organizações de todos os setores estão enfrentando a transformação da IA, impulsionada pela promessa de aumentar drasticamente a produtividade. Esta era aprimorada pela IA é marcada por iniciativas para incorporar serviços empresariais de IA, gerenciar o uso não autorizado de IA e mitigar os riscos associados à atividade de agentic AI. De forma geral, uma prioridade fundamental que sustenta esses esforços é a visibilidade e o controle sobre como os dados sensíveis são utilizados. No entanto, praticamente todas as organizações enfrentam dificuldades para obter visibilidade consistente, e muito menos controle, de seus dados em escala. É como um iceberg, no qual vemos apenas uma pequena fração na superfície, enquanto a grande maioria permanece imperceptível abaixo dela. Isso costuma ser chamado de "dark data" (dados obscuros): permanecem invisíveis e desconhecidos, mas contêm quantidades substanciais de informações sensíveis pelas quais a organização é diretamente responsável. Agora, as organizações estão tentando descobrir como permitir que os usuários aproveitem a IA com segurança, garantindo ao mesmo tempo a proteção de seus dados sensíveis, mas o próprio uso da IA está agravando o problema, pois ajuda a criar mais dados em uma velocidade sem precedentes.



O Data Security Posture Management (DSPM) oferece uma abordagem abrangente para proteger suas informações contra acesso não autorizado, divulgação, alteração ou destruição de dados. Diferentemente de outros métodos de segurança de dados que se concentram em aplicativos e dispositivos específicos, o DSPM pode visualizar e controlar a totalidade dos dados de uma organização, seja na nuvem ou em redes privadas, garantindo a conformidade e mitigando o risco de violações de dados.



Percentual de organizações que relataram uma violação relacionada à IA e não possuíam controles de acesso à IA adequados[1].



Equipes de segurança que utilizam IA e automação de forma extensiva reduziram o tempo de contenção de violações em 65 dias e diminuíram seus custos médios em USD 1,93 milhão, em comparação com aquelas que não utilizaram essas soluções[1].



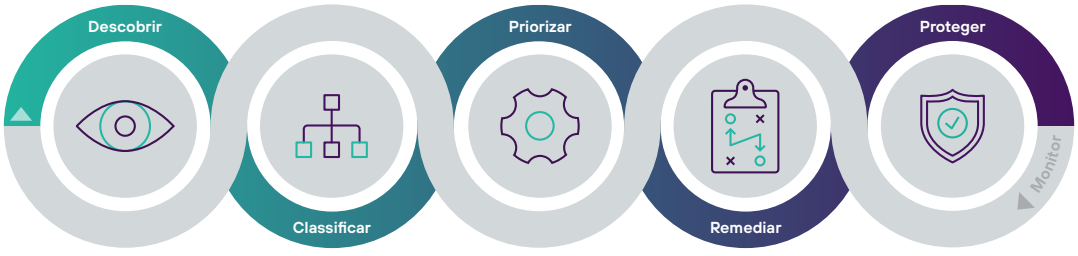
A AT&T concordou em pagar US$ 177 milhões para encerrar uma ação coletiva relacionada a duas violações ocorridas em 2024. A primeira violação expôs dados, incluindo números de Seguro Social, de 73 milhões de clientes atuais e antigos, e a segunda envolveu acesso não autorizado a um espaço de trabalho que continha informações sensíveis de clientes, hospedado em um ambiente de nuvem sem monitoramento adequado[2].

1 IBM's Cost of a Data Breach Report 2026
2 Top Class Actions **acordo da ação coletiva sobre a violação de dados da AT&T**

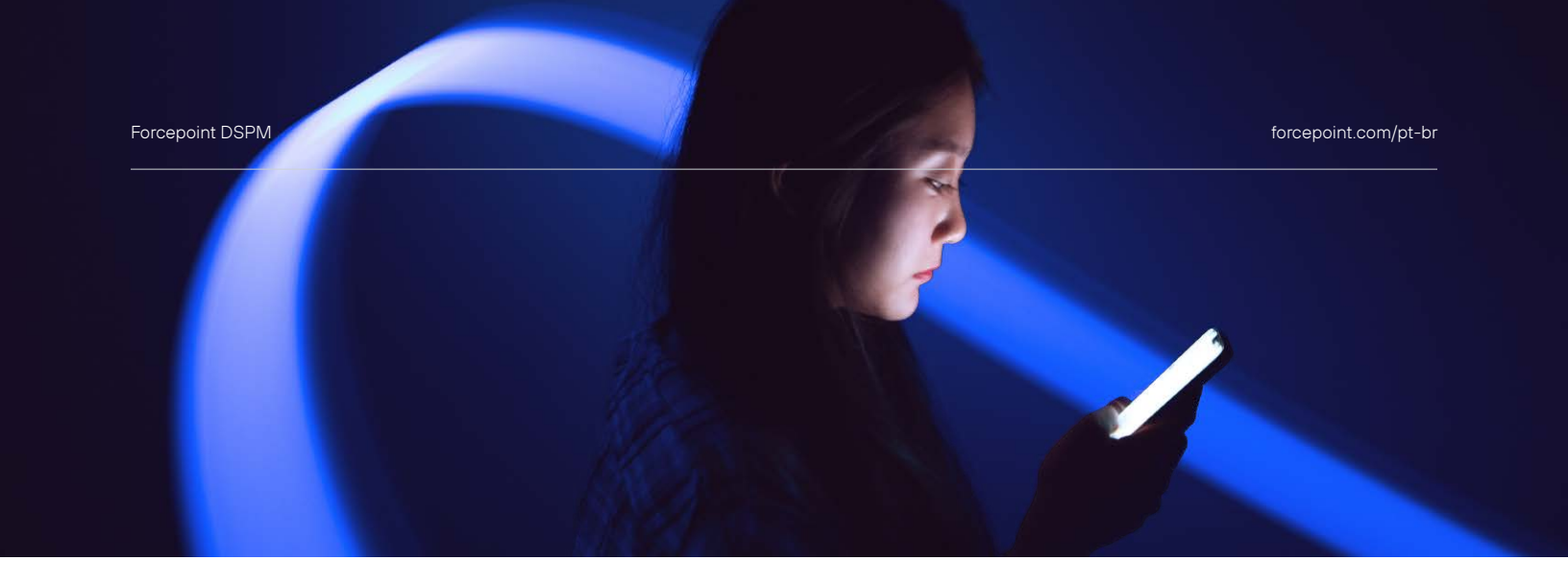
O que o DSPM faz?

- **Jornada de transformação da IA:** libere o potencial da IA com o Forcepoint DSPM, protegendo seus dados em todos os lugares com nossa avançada tecnologia de AI Mesh. Com visibilidade e correção centralizadas do Forcepoint DSPM e controles de bloqueio em tempo real do Forcepoint DLP, protegemos suas informações confidenciais em canais importantes, incluindo aplicativos GenAI como ChatGPT, Copilot, Gemini e muitos outros — possibilitando inovação ousada, aumentando a produtividade e reduzindo os riscos.
- **Identificação de dados confidenciais:** O DSPM ajuda as organizações a identificar dados confidenciais em vários ambientes e serviços de nuvem, bem como em locais on-prem, incluindo dados estruturados e não estruturados. Isso inclui entender onde dados confidenciais residem, como eles são acessados e quem tem permissões para interagir com eles.
- **Avaliação de vulnerabilidades e riscos:** o DSPM avalia a vulnerabilidade de dados sensíveis a ameaças de segurança e o risco de não conformidade com regulamentações vigentes. Ao analisar a postura de segurança dos dados, as organizações podem abordar proativamente possíveis riscos.
- **Foco nos dados na fonte:** ao contrário de outras ferramentas de segurança de dados que protegem principalmente dispositivos, sistemas e aplicativos, o DSPM se concentra diretamente na proteção da totalidade dos dados de uma organização. O objetivo é evitar violações de dados e garantir a conformidade, protegendo os dados em seu núcleo.
- **Abordando o dark data e dados redundantes, obsoletos e triviais (ROT):** o DSPM aborda diretamente o dark data (dados invisíveis e sem uso em processos normais das empresas). Da mesma forma, o DSPM pode abordar dados ROT (redundantes, obsoletos e triviais) que também tendem a se proliferar dentro das organizações, à medida que as empresas continuam guardando grandes quantidades de dados por vários motivos, pensando que isso vai ajudar a manter a conformidade. Na verdade, guardar esses dados cria ainda mais riscos e o DSPM ajuda a gerenciar essas ameaças.
- **Tratativa de dados com permissões/exposições excessivas:** devido à maneira como os dados se proliferam por meio da cópia e edição de novas versões de dados, as permissões para dados geralmente também podem aumentar exponencialmente para usuários, grupos e até mesmo para toda a organização. O DSPM ajuda a aplicar o "princípio do menor privilégio" do conceito de Zero Trust que reduz drasticamente os dados com excesso de permissões para evitar violações de dados.
- **Ambientes de nuvem múltipla e híbrida:** à medida que as organizações adotam ambientes de nuvem múltipla e híbrida, o risco de violações de dados aumenta drasticamente. O DSPM fornece visibilidade e controle sobre dados confidenciais nesses diversos ambientes de computação, além de ambientes on-premises.
- **Monitoramento contínuo de riscos:** o complemento do Forcepoint Data Detection and Response (DDR) permite que o Forcepoint DSPM detecte e corrija novos riscos de dados à medida que eles surgem. Não é necessário esperar pela próxima varredura completa do DSPM, identifique dinamicamente os riscos da sua postura de data security para corrigi-los.

O **Forcepoint DSPM** foi projetado para organizações modernas que precisam de forte visibilidade e controle de seus dados confidenciais. Fornece visibilidade em vários ambientes e servidores de nuvem para evitar violações de dados e reduzir o risco de não conformidade com os regulamentos de privacidade. A Forcepoint oferece total visibilidade e controle em todo o ciclo de vida dos dados, fornecendo o Data Security Everywhere ao combinar a **descoberta proativa de riscos** (DSPM) com **controles ativos sobre como os dados são usados** (DLP) enquanto **se adapta continuamente às ações de cada usuário** (Risk-Adaptive Protection). Descoberta dinâmica de ganhos de riscos de dados com monitoramento contínuo (Forcepoint DDR) para evitar vazamentos de dados e proteger sua postura de segurança de dados.



Descoberta, classificação e orquestração com tecnologia de IA



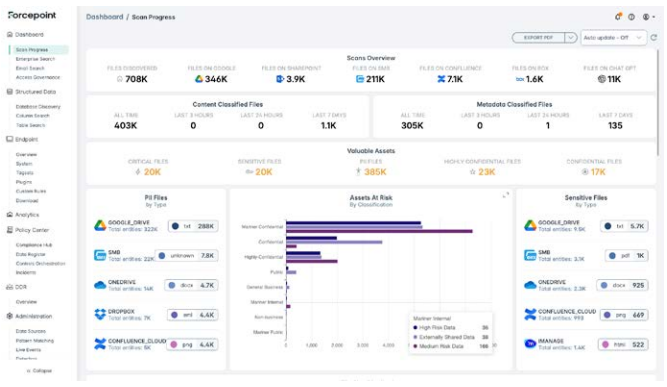
Combine a visibilidade e o controle do seu universo de dados com o Forcepoint DSPM

Gerenciar e proteger os dados da sua organização nunca foi tão complexo. O Forcepoint DSPM oferece uma solução poderosa para obter visibilidade e controle abrangentes sobre seus dados, independentemente da localização. Com uma classificação de dados líder do setor, que utiliza inspeção completa de conteúdo baseada no AI Mesh da Forcepoint e em classificadores DLP avançados, o Forcepoint DSPM permite que você tome decisões informadas sobre sua postura de segurança de dados e resolva riscos potenciais de forma proativa.

Os principais benefícios do Forcepoint DSPM incluem:

Descoberta rápida e abrangente: o Forcepoint DSPM realiza uma varredura rápida e de alto desempenho de arquivos e bancos de dados em ambientes multi cloud e on-premises, executando inspeção completa de conteúdo em vez de depender apenas de marcação de metadados ou amostragem. Essa profundidade de análise garante que os dados sensíveis sejam identificados com precisão, e não apenas estimados. A descoberta e classificação de alto desempenho da Forcepoint permitem que as organizações obtenham visibilidade rápida e abrangente do seu cenário de dados em escala, abrangendo repositórios estruturados e não estruturados, incluindo dados hospedados em plataformas de IA generativa, como ChatGPT Enterprise, Anthropic Claude e Microsoft Copilot, ajudando as equipes de segurança a se anteciparem aos riscos emergentes de exposição de dados impulsionados por IA.

Precisão viabilizada pelo AI Mesh: o Forcepoint DSPM descobre dados em fontes de nuvem e de rede e classifica automaticamente esses dados usando um mecanismo avançado de classificação por IA. O AI Mesh do Forcepoint DSPM oferece às organizações uma precisão de classificação de dados superior. Sua arquitetura de IA em rede, que utiliza um GenAI Small Language Model (SLM) e os classificadores DLP da Forcepoint, confiáveis há muito tempo e cuidadosamente selecionados, captura com eficiência o contexto de textos não estruturados. Personalizável e eficiente, garante uma classificação rápida e precisa sem a necessidade de treinamento extenso, aumentando a confiança e a conformidade. Por fim, essa alta precisão permitiu que organizações que enfrentavam dificuldades com outros métodos populares de classificação reduzissem drasticamente os falsos positivos/negativos, protegendo com sucesso sua propriedade intelectual e economizando grandes quantidades de tempo e recursos.



Visibilidade dos dados em todo o seu cenário de dados: o Forcepoint DSPM permite que você inspecione as permissões para todos os arquivos e usuários. Os administradores de dados podem ver quais os indivíduos que têm acesso a ficheiros e bases de dados em toda a organização. Com um único clique, você pode visualizar imediatamente as permissões para todos os arquivos sendo verificados. O Forcepoint DSPM fornece um painel com extensos detalhes que dão uma visão panorâmica sobre dados obscuros, além de fornecer uma visão geral da avaliação de riscos de dados para ajudar você a entender as áreas com maior risco para os dados.

Orquestração do fluxo de trabalho: defina facilmente a propriedade e a responsabilidade para diferentes conjuntos de dados, agilizando o processo de alinhamento das partes interessadas. Isso proporciona fluxos de trabalho mais eficientes nas ações realizadas em cada fonte e ativo de dados. A correção eficaz requer ampla adesão e colaboração além da organização de segurança, estendendo-se ao grupo de CDO/ Governança, Risk and Compliance (GRC), bem como a funções como marketing, finanças, DevOps e muitas outras. O Forcepoint DSPM considera a segurança da postura de dados não apenas como uma questão de segurança, mas como uma prioridade empresarial.

Forcepoint DDR: um poderoso complemento do Forcepoint DSPM, é uma solução essencial para resolver problemas de vazamentos de dados. Ele fornece detecção de ameaças contínua e visibilidade avançada de riscos aos dados, garantindo que as organizações possam ver com eficácia as alterações nos dados que provavelmente estão permitindo que os vazamentos de dados ocorram. Ao utilizar respostas orientadas por IA, o Forcepoint Data Detection and Response (DDR) oferece uma neutralização precisa de ameaças, ajudando as organizações a manter medidas de segurança robustas. Sua ampla visibilidade na nuvem e nos endpoints, combinada com o rastreamento de linhagem de dados, faz dele uma ferramenta essencial para proteger informações confidenciais, reduzir prejuízos financeiros e manter a confiança do cliente.



Não deixe que os dados prejudiquem o seu negócio. A Forcepoint pode ajudar!

Na atual era digital, os dados são o ativo mais valioso de uma organização, mas também podem ser um enorme risco se não forem gerenciados adequadamente. O Forcepoint DSPM oferece uma abordagem proativa para proteger seus dados confidenciais, mitigando os riscos de violações de dados e garantindo a conformidade com regulamentações. Com a implementação do Forcepoint DSPM, você pode obter visibilidade abrangente do seu cenário de dados, identificar e solucionar vulnerabilidades e proteger proativamente a sua organização contra prejuízos financeiros e danos à reputação causados por violações de dados e não conformidades regulatórias, tudo isso enquanto protege seus dados nos aplicativos GenAI. Assuma o controle de sua postura de segurança de dados hoje mesmo. Comece a explorar como o DSPM pode proteger suas informações valiosas. Acesse www.forcepoint.com/pt-br/dspm para solicitar uma demo.

Forcepoint

forcepoint.com/contact

About Forcepoint

A Forcepoint viabiliza a Self-Aware Data Security, uma abordagem nativa de IA que ajuda empresas e governos a conhecer seus dados em todos os lugares, se adaptar a riscos e regulamentações em evolução em tempo real e proteger em escala com uma estrutura de política única e unificada. Sediada em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para clientes e seus funcionários em mais de 150 países. Conecte-se com a Forcepoint em www.forcepoint.com/pt-br, LinkedIn, Instagram e YouTube.

© 2026 Forcepoint. Forcepoint e o logotipo FORCEPOINT são marcas comerciais da Forcepoint.
Todas as outras marcas utilizadas neste documento são propriedade dos seus respectivos proprietários.
[FP-DSPM-Brochure-PT-BR] 21Aug2026