Forcepoint DSPM

Forcepoint

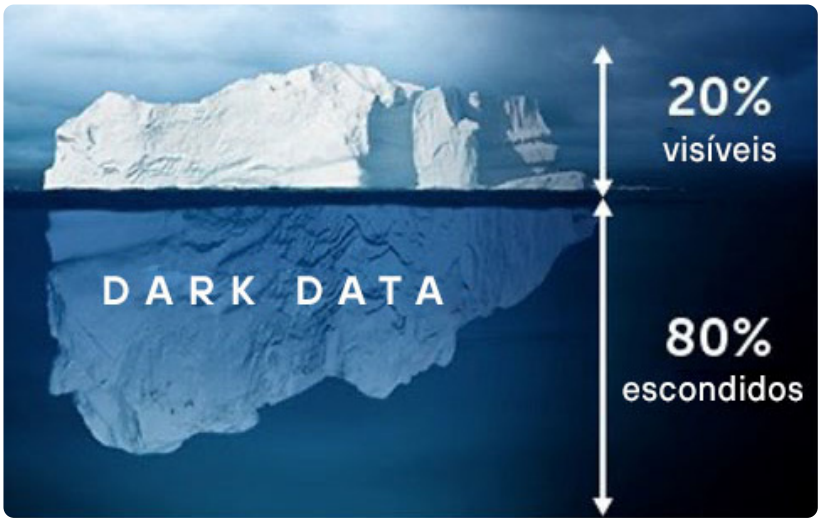
Brochure

forcepoint.com/pt-br

A transformação com IA é a próxima evolução da transformação digital

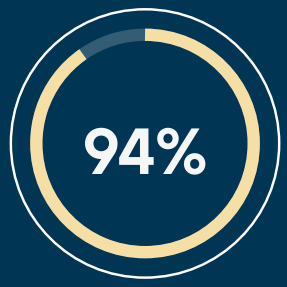
Seus dados estão seguros nesta nova era?

A maioria das organizações que passaram pela transformação digital agora estão se preparando para a próxima evolução, a transformação com IA. Essa nova era da IA é conduzida pelos inúmeros benefícios oferecidos pelos aplicativos GenAI, como ChatGPT, Copilot, Gemini, entre outros. Com base nas experiências adquiridas com a transformação digital, as organizações aprenderam que a segurança de dados deve ser uma prioridade. No entanto, para muitas organizações, os dados hoje são como um iceberg gigante, com a sua maior parte escondida sob a superfície. Muitas vezes chamados de "dark data" ou "shadow data", eles permanecem invisíveis e desconhecidos, mas contêm quantidades substanciais de informações confidenciais pelas quais as organizações têm responsabilidade direta. Agora, as organizações estão tentando descobrir como permitir que os usuários usufruam com segurança dos aplicativos GenAI para aumentar a produtividade e a eficiência, garantindo a proteção de seus dados confidenciais.



O DSPM (Data Safety Posture Management) oferece uma abordagem abrangente para proteger suas informações contra acesso, divulgação, alteração ou destruição de dados não autorizados. Ao contrário de outros tipos de métodos de segurança de dados que se concentram em sistemas e dispositivos, o DSPM concentra-se na totalidade dos dados de uma organização, estruturados ou não estruturados, de propriedade intelectual ou dados regulados, na nuvem ou em redes privadas, garantindo a conformidade e mitigando o risco de violações de dados.

De acordo com o IDC, 80% dos dados globais são não estruturados e 90% desses dados não são analisados, também chamados de "dark data".[1]



94% das organizações estão armazenando dados em vários ambientes de nuvem.[2]

A Equifax fez um acordo judicial de US$ 1,4 bilhão devido a uma violação de dados[3] ficou ainda pior quando hackers acessaram uma unidade compartilhada que armazenava várias cópias de nomes de usuários e senhas de funcionários. A empresa não tinha ferramentas para detectar e identificar arquivos redundantes e desatualizados.

1 O enigma dos dados invisíveis, Forbes, fevereiro de 2022

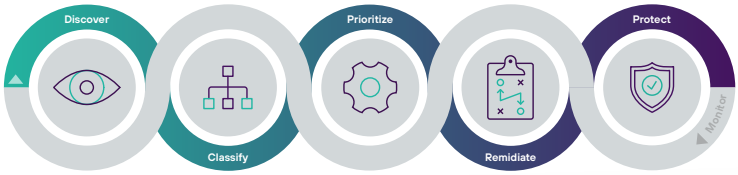
2 Dark Data: o risco desconhecido de segurança e privacidade da nuvem, Forbes, junho de 2023

3 A Equifax aceita acordo de ação judicial de violação de dados de US $ 1,38 bilhão, Finextra, janeiro de 2020

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

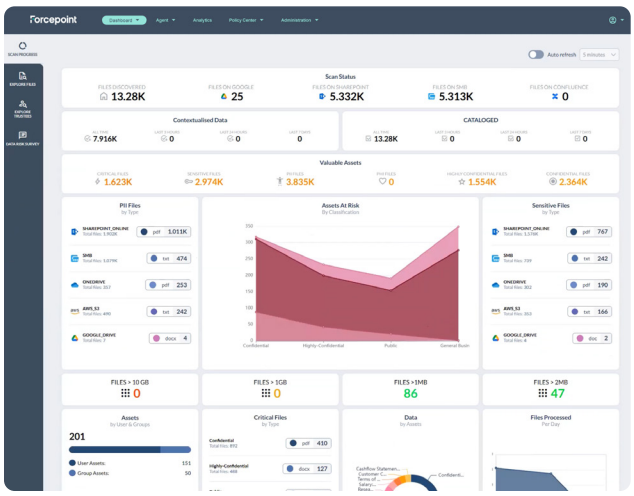
Gerenciar e proteger os dados da sua organização nunca foi tão complexo. O Forcepoint DSPM oferece uma solução poderosa para conseguir obter total visibilidade e controle sobre seus dados, independentemente de onde eles estão localizados. Com velocidades de descoberta líderes do setor e recursos avançados de classificação de dados por AI Mesh, o Forcepoint DSPM possibilita que você tome decisões informadas sobre sua postura de segurança de dados e aborde proativamente os riscos potenciais.

Os principais benefícios do Forcepoint DSPM incluem:

Descoberta rápida e abrangente: Em várias nuvens e on-prem, o Forcepoint DSPM é capaz de verificar rapidamente arquivos e bancos de dados. É comum que organizações tenham muitos terabytes sob sua responsabilidade, algumas podendo chegar a níveis maiores, como petabytes e exabytes em organizações muito grandes. Com a descoberta de alto desempenho, a Forcepoint permite que as organizações obtenham uma visão rápida dos dados em um vasto panorama, incluindo o ChatGPT Enterprise. Ao contrário de outros provedores de DSPM, a Forcepoint não cobra por varreduras de descoberta — os clientes podem executar varreduras com a frequência que quiserem, sem custos adicionais.

Precisão garantida pelo AI Mesh: o Forcepoint DSPM descobre dados em fontes de nuvem e de rede e classifica automaticamente esses dados, utilizando um mecanismo avançado de classificação com IA. O AI Mesh do Forcepoint DSPM proporciona às organizações uma precisão superior na classificação de dados. Sua arquitetura de IA em rede, que utiliza o GenAI Small Language Model (SLM) e componentes avançados de dados e IA, captura com eficiência o contexto de textos não estruturados. Personalizável e eficiente, garante uma classificação rápida e precisa sem treinamento extensivo, aumentando a confiança e a conformidade. Em última análise, essa alta precisão permite que as organizações que tiveram problemas com outros métodos de classificação possam reduzir drasticamente os falsos positivos/negativos, protegendo com sucesso sua propriedade intelectual e economizando muito 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 indivíduos têm acesso a um arquivo ou compartilhamentos de arquivos 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 ou inscreva-se para um data risk assessment gratuito, na qual especialistas em engenharia de segurança fornecerão uma amostra de seus próprios dados para ver quais tipos de risco você pode estar enfrentando no momento.

Forcepoint

forcepoint.com/contact

Sobre a Forcepoint

O Forcepoint simplifica a segurança para empresas e governos do mundo todo. A plataforma totalmente integrada e totalmente nativa na nuvem da Forcepoint facilita a adoção do Zero Trust e evita o roubo ou a perda de dados confidenciais e de propriedade intelectual, independentemente de onde as pessoas estejam trabalhando. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para os clientes e seus funcionários em mais de 150 países. Conheça mais do Forcepoint em www.forcepoint.com, Twitter e LinkedIn.