Forcepoint

Datasheet

Forcepoint Data Security Posture Management

Principais recursos e benefícios:

- **AI Mesh e Machine Learning –** A catalogação de AI Mesh oferece precisão e eficiência incomparáveis, evoluindo continuamente com aprendizado de máquina e melhorias constantes.
- **Discovery rápido –** execute o Forcepoint DSPM nos locais de armazenamento, na nuvem e on-prem, quantas vezes quiser.
- **Monitoramento em tempo real e análise de riscos –** Verifique as permissões de acesso e outros riscos de dados.
- **Orquestração de fluxo de trabalho –** Implementar prioridades de negócios para as partes interessadas.

A transformação digital evoluiu para a transformação com IA, impulsionada pela integração de tecnologias de inteligência artificial, especialmente aplicativos GenAI, nos processos de negócios. Juntamente com a expansão de dados de organizações que migram aplicativos e dados on-premises para a nuvem e utilizam ferramentas GenAI, como ChatGPT, Copilot e Gemini, eles enfrentam a luta contínua de acompanhar onde estão seus dados confidenciais, quem pode acessá-los e como são usados. O crescimento exponencial de "dark data" - dados escondidos em repositórios baseados na nuvem ou espalhados por dispositivos individuais e, agora, os aplicativos de IA Gen - apresenta um risco significativo. Estima-se que até 80% dos dados de uma organização exista nesse estado "obscuro", ignorando a supervisão tradicional.

A consequência desse cenário de dados obscuros é grave. Sem visibilidade e gerenciamento claros, as organizações estão expostas a altos riscos de violações, com consequências potencialmente devastadoras em todos os setores de comércio, organizações sem fins lucrativos e governamentais. Na era da transformação digital de hoje, a retomada do controle de informações confidenciais nunca foi tão urgente.

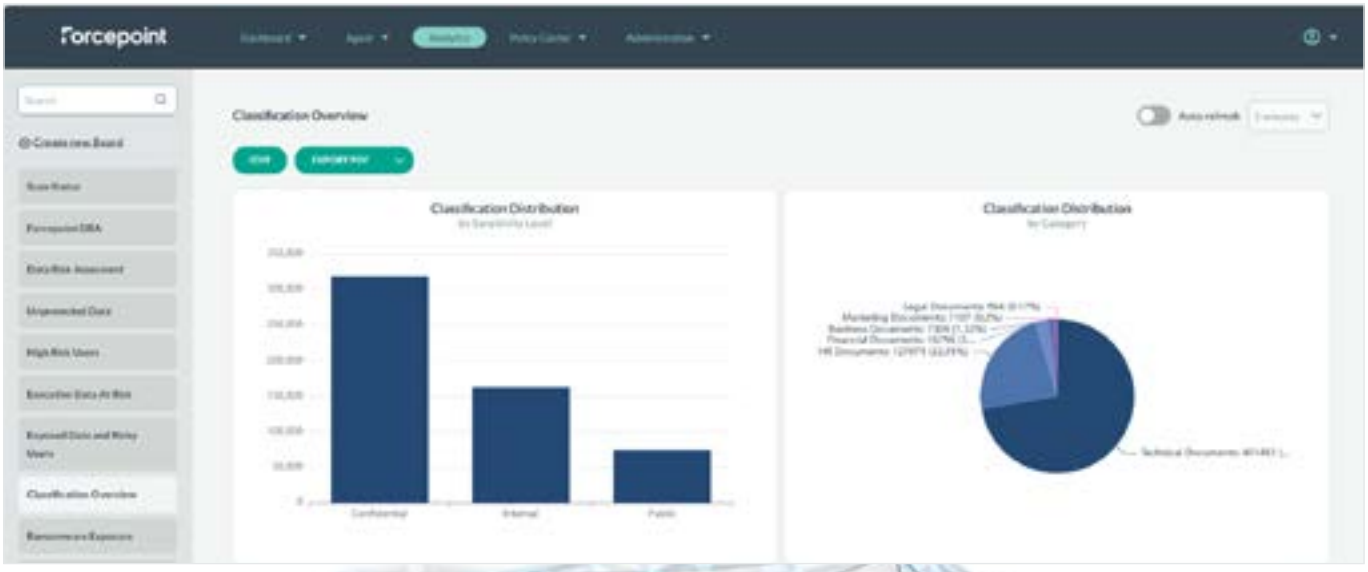
O AI Mesh do Forcepoint DSPM proporciona às organizações uma precisão superior na classificação de dados. Sua arquitetura de IA em rede, que utiliza o GenAI Small Language Model (SLM) e componentes avançados de dados e IA, captura com eficiência o contexto de textos não estruturados. Personalizável e eficiente, garante uma classificação rápida e precisa sem treinamento extensivo, aumentando a confiança e a conformidade.

Discoveryrápido e abrangente

Com uma variedade de conectores, o Forcepoint DSPM localiza dados confidenciais de forma eficiente em diversos ambientes de armazenamento, seja na nuvem ou on-premises, verificando aproximadamente um milhão de arquivos por hora nas principais plataformas, como Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) e Google (Google Drive e IAM), bem como sistemas locais de LDAP e SharePoint.

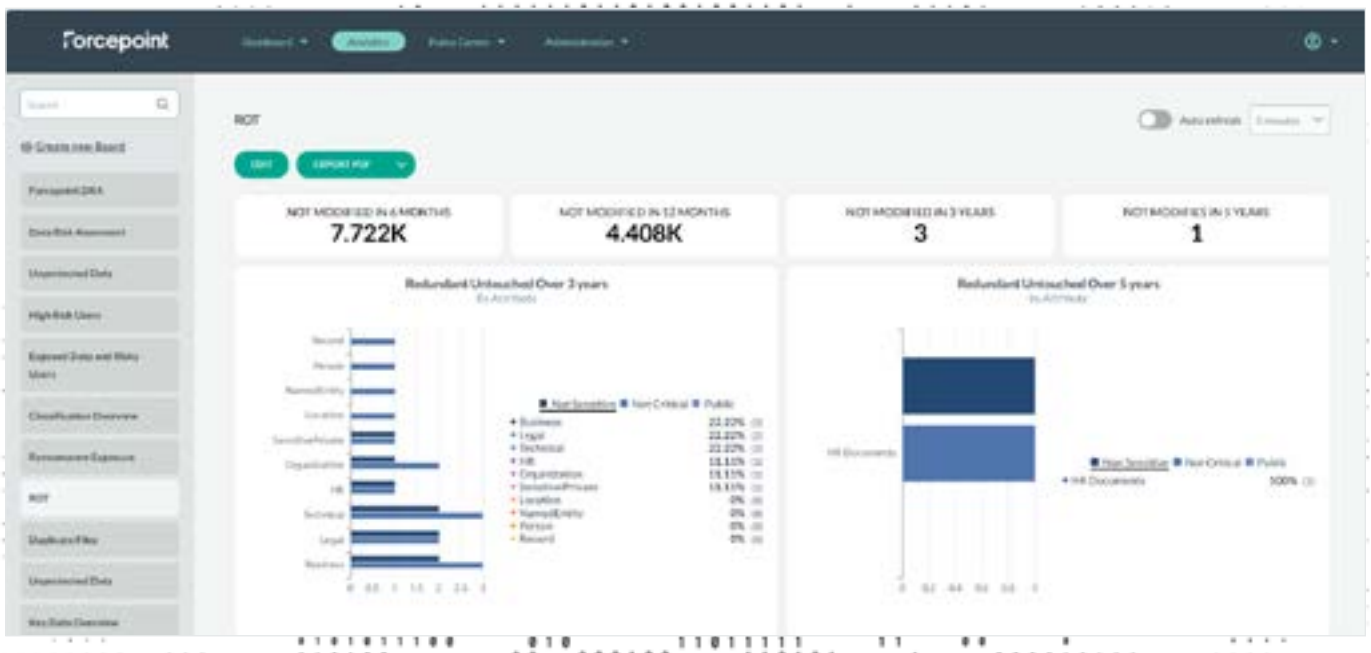
Precisão com o AI Mesh

O AI Mesh do Forcepoint DSPM se destaca por capacitar as organizações com maior precisão nos processos de Data Classification. Ao contrário de outras soluções de DSPM, oferece uma arquitetura de IA conectada e multi-nó, aproveitando um GenAI SLM e uma rede de componentes avançados de dados e IA. Essa estrutura captura o contexto de forma eficiente e transforma texto não estruturado em classificações precisas de documentos. O recurso AI Mesh é personalizável, adaptando-se às necessidades do setor e ambientes regulatórios. Funciona de forma eficiente em recursos padrão sem exigir GPUs enquanto fornece classificação de alto desempenho. A alta precisão é alcançada sem necessidade de treinamento extensivo de ML, reduzindo os gastos de manutenção. A explicabilidade do AI Mesh aumenta a confiança e a conformidade, garantindo uma postura de dados altamente segura e aderência aos regulamentos de privacidade.



Monitoramento em tempo real e análise de riscos para dados

À medida que o Forcepoint DSPM verifica e descobre dados, fornece informações detalhadas, como o número de arquivos contendo informações importantes compartilhados internamente, a quantidade de arquivos PII em risco e a contagem de arquivos de dados redundantes, obsoletos e triviais (ROT).



Orquestração de fluxo de trabalho

Simplifique a governança de segurança de dados sem esforço com o Forcepoint DSPM. Sua orquestração de fluxo de trabalho intuitiva garante um rastreamento eficiente da propriedade e responsabilidade de dados. Ao derrubar barreiras e facilitar a colaboração entre as partes interessadas, alinha as responsabilidades, aumentando a eficiência operacional e promovendo clareza em toda a organização.

A implementação de uma solução de DSPM robusta é crucial para organizações que visam simplificar seu patrimônio de dados e proteger dados confidenciais armazenados em nuvem e on-premises. Usando o Forcepoint DSPM, diversas organizações podem aumentar sua produtividade e a confiabilidade do acesso e compartilhamento de dados. Desta forma, promovem inovação e incentivam a colaboração. Simultaneamente, podem mitigar riscos identificando e abordando proativamente o uso indevido de dados confidenciais, evitando violação e vazamento de dados. Em última análise, as organizações podem simplificar os esforços de conformidade ao obter visibilidade e controle genuínos sobre dados confidenciais em todos os ambientes.

Discovery robusto

RECURSO	BENEFÍCIO
Descoberta e catalogação rápida	Funciona em várias fontes para verificar maiores volumes de arquivos por segundo/hora e sintetiza detalhes sobre ativos de dados não estruturados, organizando-os em um formato de fácil entendimento.
Conectores de fonte de dados extensos	Visibilidade robusta de mais dados não estruturados, oferecendo uma ampla gama de conectores de fontes de dados.
Análise de dados superexpostos	Identifique dados com alta exposição, compartilhados de forma pública, com terceiros, ou internamente.
Visualize as permissões para todos os arquivos de dados não estruturados	Visualize o acesso de forma individualizada, para cada arquivo, e quais são os usuários com maior acesso aos arquivos.
Elimine os riscos de dados ROT (redundantes, obsoletos e triviais)	Identifique e elimine arquivos que são redundantes, obsoletos ou triviais (ROT).
Visibilidade de acesso e permissões	As integrações com o Active Discovery e outras soluções de IRM aprimoram a segurança de acesso dentro de organizações.

AI Mesh Data Classification

RECURSO	BENEFÍCIO
Classificação de dados não estruturados com AI Mesh e Aprendizado de Máquina	Sugestões de classificação altamente precisas, recomendadas com base na verificação de dados não estruturados existentes.
Treinamento de modelos personalizados	As organizações podem adaptar o modelo de AI Mesh para atender a necessidades de dados exclusivas (por exemplo, IP, segredos comerciais, etc.). Por meio de machine learning, pode ser aprimorado ao longo do tempo e aumentar a precisão.
Mapeamento de tags para a marcação de IP do Microsoft Purview.	Camada adicional de granularidade de classificação, complementando as tags MPIP. Correção de tags de MPIP.
Data tagging	A simplificação da implementação de DLP aumenta a eficiência através da marcação de arquivos após sua verificação e classificação, com rótulos legíveis por DLP com tags típicas (confidencial, muito confidencial, público), bem como catalogação/marcação comercial (RH, marketing, finanças, desenvolvedores - com sub tags como currículos, ordens de pagamento, e outros).
Integração com o Forcepoint DLP	Pode ser integrado para utilizar o tagging de arquivos (classificação) do DSPM AI Mesh para criar políticas mais fortes.

Monitoramento em tempo real e avaliação de riscos

RECURSO	BENEFÍCIO
Análises de Risco de Dados (DRA)	Análises de risco gratuitas para dados estão disponíveis para determinar a postura atual de uma organização em relação a riscos de dados em várias categorias.
Dashboard interativo detalhado	Veja detalhes abrangentes dos arquivos em uma tela. Detalhamento de dados cruciais sobre arquivos, como nível de risco, permissões e locais (endereço IP, caminho).
Função de relatórios	Gere relatórios que mostram a aptidão de conformidade geral e para regulamentos de privacidade específicos.
Sistema de alertas avançado	Fornece controles de dados sofisticados e alertas, encontrados por meio de verificações para quaisquer anomalias ou possíveis vazamentos.
Busca de Data Subject Access Request (DSAR)	Simplifique a geração de DSAR para atender rapidamente às solicitações de regulamentos de privacidade.
Suite de Analytics	Experimente um pacote de análises avançadas para acesso fácil a insights de segurança e classificação em um piscar de olhos. Escolha entre vários dashboards predefinidos ou crie os seus próprios modelos, e exporte facilmente snapshots de PDF com apenas um clique. Os painéis predefinidos incluem análise de sobre-exposição e ransomware, duplicação de dados críticos, detecção de usuários de risco, retenção de dados, dados extraviados, análise de riscos, soberania e rastreamento de incidentes para violações de controle.
Análise de exposição a ransomware	Identifique dados críticos que estão expostos a ataques de ransomware.
Relatórios sem linguagem de programação e compilador de analytics	Crie casos de uso personalizados e relatórios de analytics sem precisar aplicar linguagens de programação.
Identificação de usuários de risco	Identifique usuários com perfis de risco elevado que têm acesso a quantidades significativas de informações críticas.
Incidente de controle de dados	Fornece uma visão clara de quaisquer violações de controle de dados e um status de resolução de incidentes.

Orquestração de fluxo de trabalho

RECURSO	BENEFÍCIO
Propriedade de dados	Define responsabilidades com facilidade e garante o alinhamento de stakeholders
Gerenciador de tarefas	Defina tarefas para proprietários e custodiantes de dados, permitindo o rastreamento de estatísticas de DSPM (como tickets abertos, resolvidos e fechados, tempo de resolução).