Forcepoint

Datasheet

Forcepoint Data Security Posture Management

Principais recursos e benefícios:

- **Classificação de AI Mesh –** Arquitetura de classificação em rede altamente precisa e eficiente usando GenAI, IA preditiva e recursos de ciência de dados.
- **Discovery rápido –** execute o Forcepoint DSPM nos locais de armazenamento, na nuvem e on-prem, quantas vezes quiser.
- **Avaliação de riscos em tempo real –** Verifique 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.

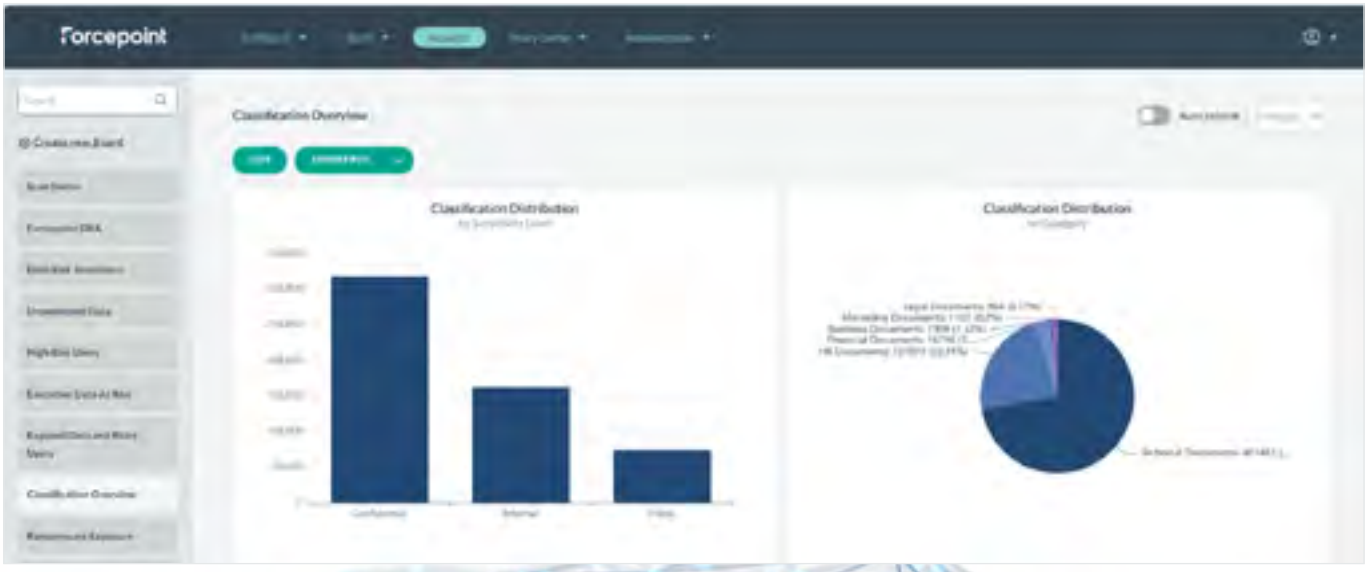
O AI Mesh do Forcepoint DSPM proporciona às organizações uma precisão superior na classificação de dados. Sua arquitetura de IA em rede, que utiliza o GenAI Small Language Model (SLM) e componentes avançados de dados e IA, captura com eficiência o contexto de textos não estruturados. Personalizável e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

Discoveryrápido e abrangente

Com uma infinidade de conectores, o Forcepoint DSPM localiza com eficiência dados confidenciais em diversos ambientes de armazenamento, seja na nuvem ou on-premises, usando as principais plataformas, como Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) e Google (Google Drive e IAM), bem como sistemas LDAP e SharePoint locais.

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 de alto desempenho e avaliação de risco de 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 tornar sua postura de dados mais segura 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.
Conexão com fontes de dados importantes	Visibilidade robusta para 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.
Visualizar e corrigir permissões	Veja o acesso para cada arquivo e corrija as alterações para estabelecer o princípio de zero trust security com base no princípio de privilégio mínimo (POLP).
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 pelo sistema AI Mesh	Classificação de IA altamente precisa para dados não estruturados.
Treinamento de modelos personalizados	As organizações podem adaptar o modelo AI Mesh para atender às necessidades de dados exclusivas (por exemplo, IP, segredos comerciais, etc.), para uma classificação de dados altamente precisa, reduzindo falsos positivos/negativos de DSPM e DLP.
Mapeamento de tags para a marcação de IP do Microsoft Purview.	Fornece uma camada adicional de granularidade de classificação, complementando as tags MIP. Capaz de corrigir marcações MIP.
Data tagging	Marca todos os arquivos digitalizados e classificados com rótulos persistentes que podem ser lidos pelo DLP com marcação padrão (confidencial, altamente confidencial, público), bem como catalogação/marcação de negócios (RH, marketing, finanças, devops - com subtags, como currículos, POs, etc.).
Integração com o Forcepoint DLP	Pode ser integrado ao Forcepoint DLP para utilizar a marcação de arquivos (classificação) pelo DSPM AI Mesh para criar políticas fortes.

Monitoramento em tempo real e avaliação de riscos

RECURSO	BENEFÍCIO
Análises de Risco de Dados (DRA)	Data Risk Assessments Gratuitos estão disponíveis para analisar a postura atual de segurança de dados de qualquer organização 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 um DSAR para cumprir rapidamente as solicitações de regulamentação 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 seus próprios modelos, além de exportar facilmente snapshots de PDF com apenas um clique. Os dashboards predefinidos incluem análise de exposição excessiva e ransomware, duplicação de dados críticos, detecção de usuários arriscados, retenção de dados, dados extraviados, avaliação de risco de dados, soberania, rastreamento de incidentes para violações de controle de dados e muito mais.
Análise de exposição a ransomware	Identifique dados críticos que poderiam ser expostos a um ataque de ransomware.
Relatórios sem linguagem de programação e compilador de analytics	Crie facilmente casos de uso personalizados e relatórios analíticos, sem precisar saber linguagem 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.